servicenow

Yokohama 市セキュリティマネジメント

最終更新日: **2025**年**12**月**17**日

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

これらの資料は、翻訳ソフトウェアを使用してお客様の便宜のために翻訳されています。正確な翻訳をご提供できるよう相当な努力を払っておりますが、いかなる自動翻訳も人間の翻訳者に代わることはなく、そのようなことは意図されておりません。翻訳は「現状のまま」提供されています。他言語への翻訳の的確性、信頼性または正確性については、明示または黙示を問わず、いかなる保証も行われません。翻訳ソフトには限界があるため、一部のコンテンツが正確に翻訳されていない場合があります。これらの資料の公用言語は英語です。翻訳の際に生じる相違または不一致は、コンプライアンスまたは履行の目的に関しては拘束力を有さず、法的効力はないものとします。

ここで示したいくつかの例と図は、説明の目的でのみ提供されています。ServiceNow 製品またはサービスへの実際の関連付けやつながりは意図されておらず、推測されるものではありません。

ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは米国および/またはその他の国における ServiceNow, Inc. の商標または登録商標です。その他の会社名および製品名は、それぞれの所有者の商標です。

下記の ServiceNow ウェブサイト利用規約をお読みください。 www.servicenow.com/terms-of-use.html

自動翻訳

本社
2225 Lawson Lane
Santa Clara, CA 95054
United States
(408) 501-8550

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

servicenow

目次

セキュリティオペレーション 6
セキュリティオペレーションの詳細 8
セキュリティインシデントレスポンス向け Now Assist 14
セキュリティインシデントレスポンス向け Now Assist の探索 17
セキュリティインシデントレスポンス向け Now Assist の構成 20
セキュリティインシデントレスポンス向け Now Assistを使用したセキュリティインシデントのクローズ 27
Now Assistでの AI エージェントのユースケースの使用セキュリティインシデントレスポンス 38
攻撃対象領域管理アプリケーション 40
脆弱性対応 41
アプリケーション脆弱性対応 772
コンテナ脆弱性対応 966
コンフィグレーションコンプライアンス 1039
脆弱性対応 ワークスペース 1286
ソフトウェア部品表 1471
エンタープライズセキュリティケース管理のアプリケーション 1509
セキュリティインシデントレスポンス 1511
脅威インテリジェンス 2942
セキュリティポスチャコントロール 3174
セキュリティポスチャコントロール の詳細 3176
セキュリティポスチャコントロール ワークスペースの使用 3190
での緩和コントロールモニタリングの使用 セキュリティポスチャコントロール 3207
セキュリティポスチャコントロール におけるユースケース、ポリシー例、サポートされるサービスグラフコネクタ 3228
Cloud Security Posture Management と Amazon Web サービス の統合 3242
Microsoft Azure を使用した Cloud Security Posture Management 3253
サイバーセキュリティエグゼクティブダッシュボード 3262
ベンチマークスコアのオプトイン 3279
ターゲットを設定 3280
Security Operations のためのセキュリティシミュレーションとトレーニングの統合 3281
GRC：メトリクス のリスクとコンプライアンスダッシュボード 3283
脅威インテリジェンスセキュリティセンター 3292
脅威インテリジェンスセキュリティセンター の詳細 3294
ドメインセパレーションと脅威インテリジェンスセキュリティセンター 3296
脅威インテリジェンスセキュリティセンターの設定 3297
脅威インテリジェンスセキュリティセンターホームページの表示 3299
脅威インテリジェンスセキュリティセンターの統合 3301
SIR ワークスペースとの TISC 統合 3373
管理 3373

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データインポートの使用 3414
脅威インテリジェンスのインポート 3416
脅威アナリストワークベンチ 3425
脅威インテリジェンスセキュリティセンター ライブラリ 3440
MITRE-ATT&CK™ リポジトリ 3566
データの管理と保持 3574
TISC データ処理機能フロー 3584
Data Loss Prevention Incident Response 3586
Data Loss Prevention Incident Response の詳細 3587
DLP IR インシデント応答のインストールと構成 3590
DLP インシデント応答の管理 3591
Data Loss Prevention Incident Response Incident Management 3643
Data Loss Prevention Incident Response のインバウンド統合 3664
DLP 統合 3667
セキュリティオペレーション の共通機能 3742
Security Operations でのフィルターグループの作成と定義 3744
共有データ変換 3746
セキュリティオペレーション メール処理 3750
セキュリティオペレーション フィールドマッピング 3760
セキュリティオペレーション フィールド値変換 3764
セキュリティオペレーション 拡張データマッピング 3765
セキュリティオペレーション のユーザー定義のエスカレーション 3768
ドメインセパレーションプロパティの上書きの作成 3769
オペレーティングシステムグループの作成 3771
セキュリティタググループとタグのセットアップ 3772
セキュリティ注釈 3776
一緒にインストールされるコンポーネント Security Support Common 3778
Security Operations アプリケーションのロール別モジュールアクセス 3779
[store-future: BEGIN review]
[End]
セキュリティオペレーション の検索 4405
Security Operations Integration の参考文献 4406
セキュリティオペレーション ワークフロートリガー 4504
Security Operations オーケストレーション 4506
セキュリティオペレーション のシナリオと例 4506
[store-future: BEGIN review]
自動化を使用した脅威の分析時間の短縮 4506
[store-future: BEGIN review]
[End]
注目度の高い脆弱性を優先 4512
[store-future: BEGIN review]
[End]
[End]
セキュリティオペレーション および ServiceNow Store 4514

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ServiceNow Store からのアプリケーションの初回ダウンロード.....4515
セキュリティオペレーション 統合のインストール..... 4520
以前に ServiceNow Store からダウンロードしたアプリケーションの更新..... 4524
インスタンスの次のファミリリリースへのアップグレード..... 4525

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティオペレーション

ServiceNow® セキュリティオペレーション アプリケーションは、インシデントデータをセキュリティツールから構造化されたレスポンスエンジンにインポートします。このエンジンは、インテリジェントなワークフロー、自動化、データの可視化、および IT との緊密な連携を使用して、脅威が組織に与える影響に基づいて、脅威の優先順位付けと解決を行います。

いずれかのタイルを選択して開始します。

Security Operations アプリケーションとそのワークスペース

セキュリティオペレーションアプリケーションがセキュリティ体制の改善にどのように役立つかについて説明します。

セキュリティインシデントレスポンスの **Now Assist**

セキュリティインシデントレスポンスの Now Assist が、セキュリティインシデントレスポンスワークスペースとコア UI® (UI16) で ServiceNow 生成 AI (GenAI) スキルをどのようにサポートするかについて説明します。

攻撃対象領域管理アプリケーション

サイバー攻撃対象領域全体の脆弱性を特定して修正するのに役立つ脆弱性対応のアプリケーションについて説明します。

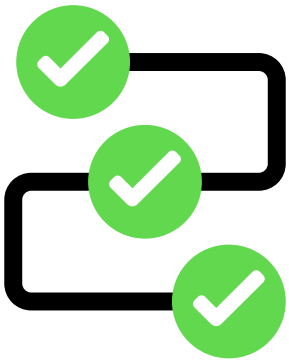
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エンタープライズセキュリティケース管理のアプリケーション

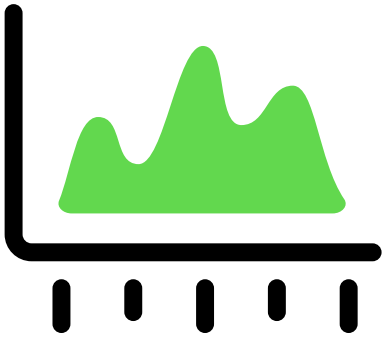
重大なセキュリティインシデントの進化に合わせて分析、切り分け、修正するのに役立つセキュリティインシデントレスポンスのアプリケーションについて説明します。

セキュリティポスチャコントロールアプリケーション



全体的なセキュリティ体制に関するインサイトを得るのに役立つアプリケーションについて説明します。

サイバーセキュリティエグゼクティブダッシュボード

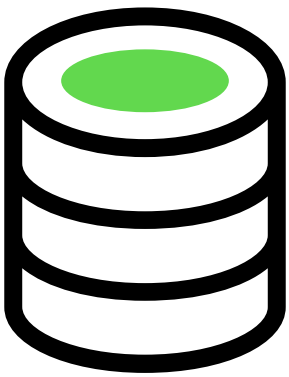


サイバーセキュリティエグゼクティブダッシュボードが、さまざまな SecOps 製品のデータを統合ダッシュボードに統合する方法について説明します。

脅威インテリジェンスセキュリティセンター

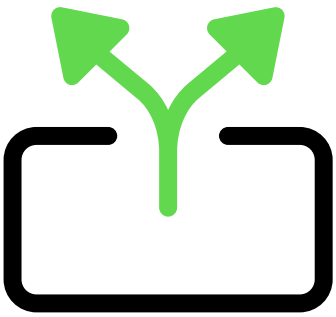
脅威インテリジェンスセキュリティセンター (TISC) プラットフォームが、脅威インテリジェンスの集約と管理のためのテクノロジーソリューションを提供する方法について説明します。

Data Loss Prevention Incident Response



顧客の機密情報を管理し、データ損失チャネルを特定して保護する方法について説明します。

Security Operations 共有アプリケーション



セキュリティオペレーション共通の機能を提供する機能とモジュールについて説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Security Operations
のシナリオと例

ServiceNow® Storeからセキュリティオペレーションアプリケーションを取得する方法と、製品の使用中に使用できるアプリケーションのシナリオについて詳しく説明します。

自動翻訳

トラブルシューティングとサポート

- セキュリティオペレーションリソースライブラリ
- セキュリティオペレーションコミュニティ
- 既知のエラーポータルで既知のエラー記事を検索する
- 連絡先 カスタマーサービス & サポート

セキュリティオペレーションの詳細

ServiceNow セキュリティオペレーション アプリケーションと Now Platform® の機能で資産やエンタープライズ環境を保護します。セキュリティチームや IT チームと連携して、組織に及ぼす影響度に基づいて脅威の優先順位を付けた上で解決します。

セキュリティオペレーションの概要

セキュリティオペレーション のアプリケーションスイートを使用して、全体的なセキュリティ体制を改善することで資産を保護できるようになります。たとえば、セキュリティインシデントレスポンス、脆弱性対応、セキュリティポスチャコントロール などのアプリケーションを既存のセキュリティツールと統合することで、セキュリティオペレーションセンター (SOC) のアナリスト、マネージャー、IT チームは次のことができるようになります。

- 急速に進化するサイバー脅威やセキュリティ脅威に対応
- 脆弱性を特定し、優先順位を付けて修復
- 完全性のある資産インベントリを表示

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

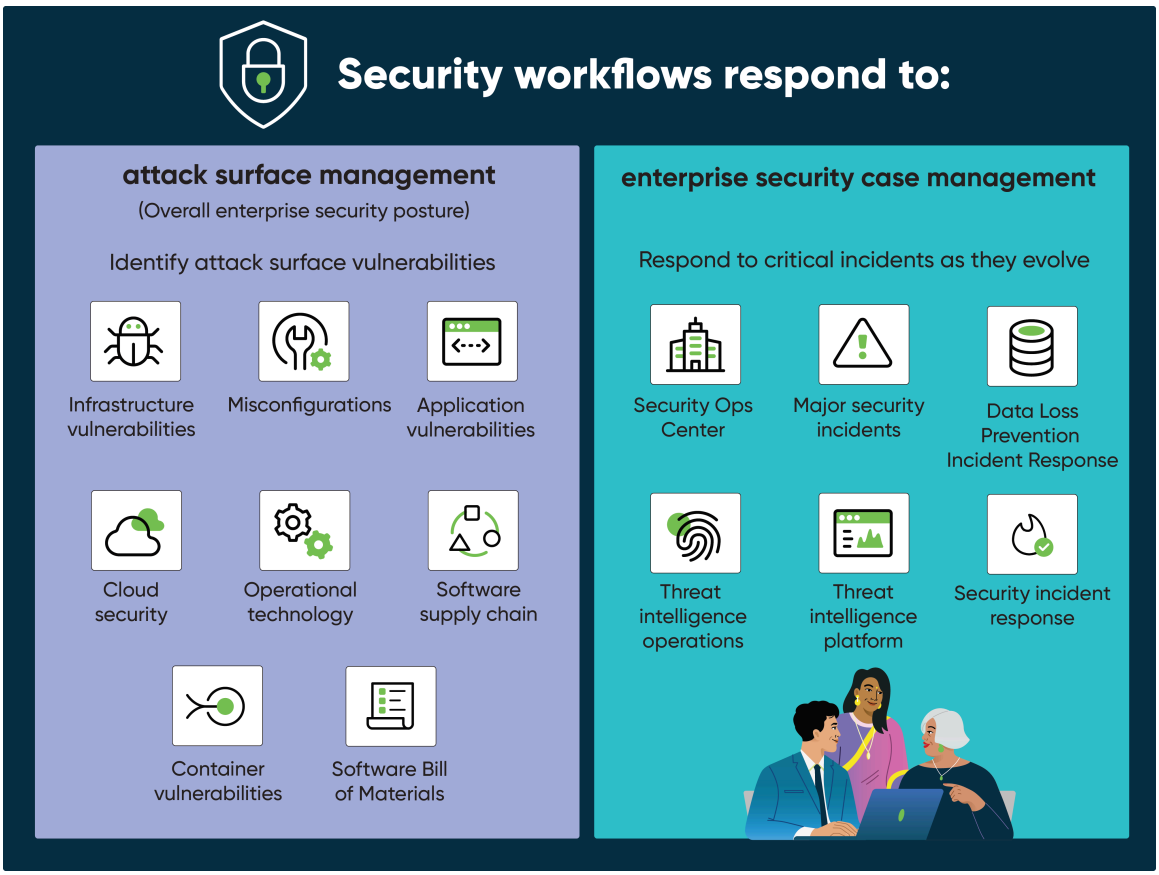
- 全体的なセキュリティツール範囲を決定する
- インテリジェントなワークフローや ServiceNow の生成 AI スキル (GenAI) を活用して、セキュリティインシデントをより迅速に解決します。詳細については、「セキュリティインシデントレスポンス向け Now Assist」を参照してください。

ワークフロー用の セキュリティオペレーション アプリケーション

セキュリティオペレーション アプリケーションは、セキュリティオペレーション のワークフローにおいて 2 つの大きなカテゴリに分類されます。

- 攻撃対象領域管理 - 脆弱性の予測、理解、クローズに役立つアプリケーションとツール。
- エンタープライズセキュリティケース管理：重大なインシデントへの迅速な対応に役立つアプリケーションとツール。

セキュリティワークフロー



SecOps アプリケーションの 2 つのカテゴリとユースケースは、エンタープライズ環境での対処に役立ちます。

セキュリティオペレーション アプリケーションのメリット

次世代ユーザーインターフェイス (ワークスペース) で セキュリティオペレーション アプリケーションやデータを表示します。ワークスペースを使用すると、組織のセキュリティアナリスト、セキュリティオペレーションセンター (SOC) のマネージャー、修復スペシャリストが、以下のタイプのワークフローを 1 か所で監視および管理できるようになります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 初期分析から封じ込め、除去、復旧までのセキュリティインシデントのライフサイクル。
- 最も心配される脆弱性。どの脆弱性を IT チームに送信して修復するかを戦略的に判断できるようになります。
- 資産に関するインポート情報を報告および監視するセキュリティツール範囲や資産の健全性に関する重要なインサイトや主要なユースケース。

攻撃対象領域管理アプリケーション

脅威の予測や脆弱性の特定に役立つアプリケーション

アプリケーション	説明	ユーザー
セキュリティポスチャコントロール	資産インベントリやインポートデータに基づいて、セキュリティツールがどの程度適切に展開され、資産をカバーできるのか考察できるようになります。データのインポートでは、サービスグラフコネクタをはじめ、 ハードウェア資産管理 (HAM) や ITOM Discovery などの ServiceNow 製品がサポートされています。 ポリシーに基づく監査により、「インターネットへの露出と既知の脆弱性」など、リスクの高い組み合わせの修復に優先順位を置くことができるようになります。カスタムのポリシーやインサイトを作成して、資産が内部セキュリティツールの構成標準に準拠しているか監視します。	• CISO • 情報セキュリティアナリスト • セキュリティオペレーションマネージャー • IT 運用エンジニア • サービスオーナー (修復オーナーペルソナ)
脆弱性対応	サードパーティの脆弱性スキャナーやアセスメントツールにより、次のタイプの資産に対して脆弱性がもたらすリスクを特定できるようになります。 • インフラストラクチャ (ホスト) • コンテナ • アプリケーション • ソフトウェア部品表 これらのツールによって特定された脆弱性は、組織の資産の維持と保護を担当するセキュリティチームと IT チームにとってはリスクとなります。	• CISO • 情報セキュリティアナリスト • セキュリティオペレーションマネージャー • IT 運用エンジニア • サービスオーナー (修復オーナーペルソナ)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威の予測や脆弱性の特定に役立つアプリケーション (続く)

アプリケーション	説明	ユーザー
コンフィグレーションコンプライアンス	セキュリティまたは企業ポリシーへの準拠を検証します。 サードパーティの SCA (Secure Configuration Assessment) 統合から得られたテスト結果を使用して非準拠構成アイテムを特定し、優先順位を付けて修復します。	• CISO • 情報セキュリティアナリスト • セキュリティオペレーションマネージャー • IT 運用エンジニア • サービスオーナー (修復オーナーペルソナ)

エンタープライズセキュリティケース管理のアプリケーション

重大なセキュリティ侵害やインシデントへの対応に役立つアプリケーション

アプリケーション	説明	ユーザー
セキュリティインシデントレスポンス	修復を迅速化する強力なワークフローと自動化ツールを適用することで、重大なインシデントを特定するプロセスを簡素化します。 既存のセキュリティ情報およびイベント管理 (SIEM) ツールをセキュリティインシデントレスポンス アプリケーションおよび Security Operations アプリケーションと統合し、さまざまなソースから脅威データをインポートして、優先順位付けされたセキュリティインシデントを自動的に作成します。	• CISO • 情報セキュリティアナリスト • セキュリティオペレーションマネージャー • 脅威インテリジェンスアナリスト
重大セキュリティインシデント管理	重大セキュリティインシデント管理の機能は、既存のセキュリティインシデントレスポンス製品の機能と連携します。セキュリティアナリストが標準のセキュリティインシデントを重大なセキュリティインシデントへエスカレーションし、新しい製品機能を利用して修復プロセスをサポートできるようにするといったことも含まれます。 重大なセキュリティインシデント (MSI) の検出から分析までの進捗状況を追跡します。ソリューションを提案し、セキュ	• CISO • 情報セキュリティアナリスト • セキュリティオペレーションマネージャー • IT 運用エンジニア • サービスオーナー (修復オーナーペルソナ) • 総協議会

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重大なセキュリティ侵害やインシデントへの対応に役立つアプリケーション (続く)

アプリケーション	説明	ユーザー
	リティインシデントを昇格およびリンクさせて、クローズします。	
Data Loss Prevention Incident Response	Data Loss Prevention Incident Response (DLP IR) により、エンドポイントやネットワーク、メール、クラウドといった複数のソースから発生した DLP インシデントの修復ワークフローを確認および管理できるようになります。 DLP アプリケーションを使用して、データ損失の経路を特定、対応、および保護できます。	• CISO • 情報セキュリティアナリスト • セキュリティオペレーションマネージャー
脅威インテリジェンス	インシデント対応チームは、脅威のルックアップ、検索、相関を自動化できるようになります。MITRE ATT&CK との統合により、検出や緩和の範囲を測定および把握し、脅威ハンティングをサポートできるようになります。	• CISO • 情報セキュリティアナリスト • セキュリティオペレーションマネージャー • 脅威インテリジェンスアナリスト
脅威インテリジェンスセキュリティセンター (TISC)	複数のソースからの脅威インテリジェンスを集約、キュレーション、管理し、脅威インテリジェンスのケース管理を実施します。キャンペーンを追跡し、脅威インテリジェンスを運用化し、実用的なインテリジェンスに対応します。	• CISO • 情報セキュリティアナリスト • セキュリティオペレーションマネージャー • 脅威インテリジェンスアナリスト

次に探索する内容

タイルを選択して セキュリティオペレーション のワークスペースを始めます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンスワークスペース	脆弱性マネージャーワークスペース	セキュリティポスチャコントロールワークスペース
セキュリティインシデントレスポンスワークスペースの詳細	脆弱性マネージャーワークスペースの詳細	セキュリティポスチャコントロールワークスペースの詳細
脆弱性アセスメントのワークスペース	**IT** 修復ワークスペース	ソフトウェア部品表ワークスペース
脆弱性アセスメントのワークスペースの詳細	IT 修復ワークスペースについて学ぶ	ソフトウェア部品表ワークスペースの詳細

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威インテリジェンス セキュリティセンター **(TISC)** ワークスペース	データ損失防止 **(DLP)** インシデントレスポンスワークスペース	重大セキュリティインシデント管理 **(MSIM)** ワークスペース
TISC ワークスペースの詳細を見る	DLP ワークスペースの詳細	MSIM ワークスペースの詳細

トラブルシューティングとサポート

- セキュリティオペレーションリソースライブラリ
- セキュリティオペレーションコミュニティ
- 既知のエラーポータルで既知のエラー記事を検索する
- 連絡先 カスタマーサービス & サポート

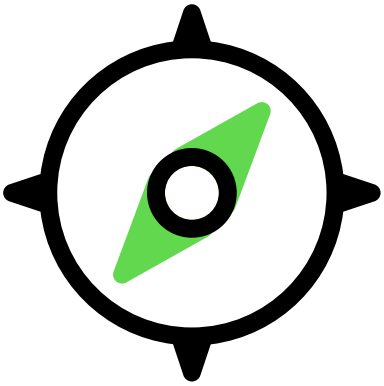
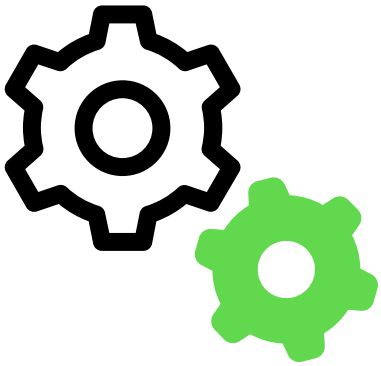
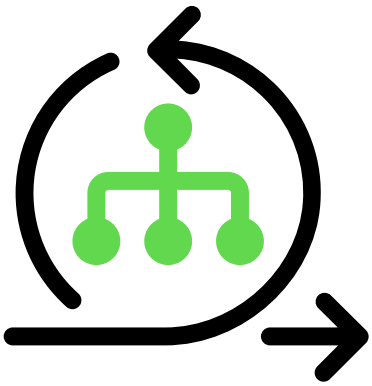
セキュリティインシデントレスポンス向け **Now Assist**

セキュリティアナリストは、インテリジェントなワークフローと ServiceNow 生成 AI スキルを使用して、セキュリティインシデントの解決に役立てることができます。セキュリティマネージャーは、セキュリティインシデントとクローズメモのコンテキストを簡潔で読みやすい形式ですばやく確認し、インシデントの事後分析データを表示し、セキュリティインシデントレスポンス向け Now Assistアプリケーションで推奨される修復手順を確認できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

開始するには

探索	構成	使用
		
「セキュリティインシデントレスポンス向け Now Assist」を参照してください。	のスキルを構成してアクティブ化する方法を学習する セキュリティインシデントレスポンス向け Now Assist	生成 AI を使用して詳細を要約し、セキュリティインシデントのクローズメモを生成する方法を学びます。 セキュリティインシデントレスポンス向け Now Assist
	セキュリティインシデントレスポンス AI エージェントコレクションの使用 セキュリティインシデントレスポンス向け Now Assist で AI エージェントのユースケースを使用する	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重要:

- 現在、一部の Now Assist 製品/機能は、FedRAMP、NSC DOD IL5、オーストラリアの IRAP で保護されたデータセンターのお客様、セルフホスト型のお客様、またはその他の制限された環境のお客様はご利用いただけません。詳細については、Now Support ナレッジベース 記事「KB0743854」を参照してください。将来のリリースで可用性の更新を必ず確認してください。
- 現在、一部の Now Assist 製品/機能は、一部の地域のお客様にのみご利用いただけます。詳細については、Now Support ナレッジベースの記事「KB1699552」を参照してください。将来のリリースで可用性の更新を必ず確認してください。

トラブルシューティングとサポート

- セキュリティオペレーションリソースライブラリ
- セキュリティオペレーションコミュニティ
- 既知のエラーポータルで既知のエラー記事を検索する
- 連絡先 カスタマーサービス & サポート

AI の制限事項

このアプリケーションは、データ内のパターンに基づいて予測を生成する急速に進化している研究分野である人工知能 (AI) と機械学習を使用しています。その結果、このアプリケーションは必ずしも正確、完全、または適切な情報を生成するとは限りません。さらに、このアプリケーションがユースケースに合わせて完全にトレーニングまたはテストされているという保証はありません。これらの問題を軽減するために、このアプリケーションの使用の正確性、害、ユースケースへの適合性をテストおよび評価し、出力を人間が監視し、意思決定の目的で AI で生成された出力のみに依存しないようにすることは、お客様の責任です。これは、医療、ファイナンス、法務、雇用、セキュリティ、インフラストラクチャなど、結果が影響を与える分野にこのアプリケーションを展開することを選択した場合に特に重要です。お客様は、ServiceNow によって更新される可能性のある ServiceNow の AI 利用規定 に従うことに同意するものとします。

データ処理

このアプリケーションでは、ServiceNow 顧客の個々のインスタンスから一元化された ServiceNow 環境にデータを転送する必要があります。この環境は、インスタンスが存在するデータセンターとは異なるデータセンターリージョンに配置されている可能性があり、場合によっては Microsoft Azure などのサードパーティクラウドプロバイダーにも転送されます。このデータは、コアコンプライアンスポータル から利用可能なポリシーを含む、ServiceNow の内部ポリシーと手順に従って処理されます。

データコレクション

ServiceNow は、このアプリケーションの入力、出力を収集して使用し、出力を編集して、ServiceNow モデルや AI 製品などの ServiceNow テクノロジーを開発および改善します。さらに、このアプリケーションは セキュリティインシデント、 インシデント、変更要求、問題、および脆弱性一致アイテムからのデータ。 お客様は、「Now Assistオプトアウトに関するページ」の説明に従って、いつでも将来のデータコレクションをオプトアウトできます。

詳細については、 Now Assist のドキュメント を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンス向け **Now Assist** の探索

セキュリティアナリストは、インテリジェントなワークフローと ServiceNow 生成 AI スキルを使用して、 セキュリティインシデントレスポンス向け Now Assist アプリケーションを使用した作業のフロー内でセキュリティインシデントのトリアージ、調査、クローズを支援できます。

セキュリティインシデントレスポンス向け **Now Assist**の概要

生成 AI スキルを使用すると、セキュリティアナリストは次のことができます。

- セキュリティインシデントの詳細を要約し、簡潔で読みやすい形式でコンテキストをすばやく確認します。
- セキュリティインシデントの推奨される次のステップを生成します。
- インシデントの事後分析データを生成します。
- クローズメモを生成します。
- 相関インサイトを生成

セキュリティアナリストは、結果、インシデントの詳細、およびクローズメモを他のアナリスト、マネージャー、および主要なステークホルダーと共有できます。

セキュリティインシデントレスポンス向け **Now Assist** ユーザー

ユーザー

ユーザー	説明
セキュリティアナリストとマネージャー	生成 AI を使用して、セキュリティインシデントの詳細をプレビューし、その潜在的な影響を確認し、既に実行された主要な修復アクションをセキュリティインシデントサマリーで表示します。サマリーと推奨される次のステップ (アクション) により、アナリストとマネージャーは調査を有利に開始し、セキュリティインシデントのクローズに役立ちます。 生成 AI を使用して、クローズメモの下書きを自動的に生成します。セキュリティインシデントのクローズメモは、クローズに関連するその他の詳細に加えて、修復および封じ込めアクティビティに基づいて迅速に作成されます。

セキュリティインシデントレスポンス向け **Now Assist** のメリット

セキュリティインシデントレスポンス向け **Now Assist** の機能

メリット	機能	ユーザー
作業メモとコンテキスト情報を簡潔で読みやすい形式ですばやく確認することで、アクティビティストリームが長いセキュリティインシデントのトリアージを迅速化します。	次の情報を含むセキュリティインシデントのサマリーを生成します。 • 問題 • 詳細 • 観察事項	• セキュリティアナリスト • セキュリティマネージャー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンス向け **Now Assist** の機能 (続く)

メリット	機能	ユーザー
	• 実行された主なアクション • クローズの詳細	
セキュリティインシデントをクローズする準備ができたら、クローズメモのドラフトを自動的に生成します。アナリストは、セキュリティインシデントをクローズする前に、AI スキルによって生成されたコンテンツを編集、削除、または独自のメモを追加することで変更できます。	セキュリティインシデントのクローズメモの生成	• セキュリティアナリスト • セキュリティマネージャー
要求に応じて、セキュリティインシデントのクローズに役立つ、ワークフロー内で推奨される次のステップを生成します。	セキュリティインシデントの推奨アクションを生成	• セキュリティアナリスト • セキュリティマネージャー
根本原因分析、影響度アセスメント、およびセキュリティインシデントをクローズするワークフロー内で得られた教訓を含む、インシデントの事後分析を生成します。	インシデントの事後分析を生成	• セキュリティアナリスト • セキュリティマネージャー
現在のインシデントを、影響を受ける同じユーザー、構成アイテム (CI)、または観測事象が関与する過去のイベントに結び付けます。	相関インサイトを生成	• セキュリティアナリスト • セキュリティマネージャー
Now Assist パネルからサマリーとクローズメモにアクセスして、セキュリティインシデントの詳細をすばやく把握できます。	Now Assist パネルから生成 AI のサマリーとクローズメモにアクセスします。パネルにセキュリティインシデントに関するより基本的な情報の要求を入力します。	• セキュリティアナリスト • セキュリティマネージャー
サマリーとクローズメモの生成 AI スキルをニーズに合わせてカスタマイズします。	スキルをコピーして、選択した関連テーブルフィールドを変更し、スキルの可用性を定義して、スキルを表示する場所を選択します。	admin

次に探索する内容

セキュリティインシデントレスポンス向け Now Assistを構成して使用する方法の詳細については、以下を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- セキュリティインシデントレスポンス向け Now Assist の構成
- セキュリティインシデントレスポンス向け Now Assist でセキュリティインシデントを要約
- セキュリティインシデントレスポンス向け Now Assist を使用したセキュリティインシデントのクローズメモの生成
- との相関インサイトの生成 セキュリティインシデントレスポンス向け Now Assist
- を使用したセキュリティインシデントの推奨アクションの生成 セキュリティインシデントレスポンス向け Now Assist
- を使用したセキュリティインシデントのインシデントの事後分析の生成 セキュリティインシデントレスポンス向け Now Assist
- セキュリティインシデントレスポンスの Now Assist の入力とトリガー

セキュリティインシデントレスポンス向け **Now Assist** に関するサポート情報

セキュリティインシデントレスポンス向け Now Assist アプリケーションに関連する重要な情報の簡単な概要を把握できます。

サポート対象のバージョン

セキュリティインシデントレスポンス向け Now Assist のバージョン 2.0.1 は以下をサポートしています。

- 従来 UI (UI16): セキュリティインシデントレスポンス コアアプリケーション、v13.6.4
- セキュリティインシデントレスポンスワークスペース (SIR ワークスペース)、v1.7.0
- Now Assist for Now Platform® v6.0.1

サポート対象のユーザーインターフェイス

セキュリティインシデントレスポンス向け Now Assist が有する生成 AI のスキルは、次のテーブルのとおりです。

セキュリティインシデントレスポンス向け **Now Assist** でサポートされるインターフェイスとスキル

インターフェイス	機能
セキュリティインシデントレスポンス	• セキュリティインシデントの要約。 • セキュリティインシデントに対して推奨される次のステップの生成。 • 根本原因分析、影響度評価、得られた教訓を含むインシデントの事後分析の生成。 • Now Assist パネル。 • クローズメモの生成。 • パネルからの相関インサイトNow Assist。
従来 UI16	• セキュリティインシデントの要約 • セキュリティインシデントに対して推奨される次のステップの生成。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンス向け **Now Assist** でサポートされるインターフェイスとスキル (続く)

インターフェイス	機能
	• 根本原因分析、影響度評価、得られた教訓を含むインシデントの事後分析の生成。 • Now Assist パネル。 • クローズメモの生成。 • パネルからの相関インサイトNow Assist。

セキュリティインシデントレスポンス向け **Now Assist** の構成

セキュリティインシデントレスポンス向け Now Assist アプリケーションは、セキュリティインシデントレスポンスワークスペースおよび従来 コア UI (UI16) でサポートされています。Now Assist アドミンコンソールのガイド付き設定を使用して、セキュリティインシデントレスポンス向け Now Assist を構成できます。

構成の概要

ServiceNow® AI 開発プログラムとデータを共有することで、予測精度やユーザーエクスペリエンスの向上、ビジネスニーズに合わせた製品のカスタマイズ、活性化された Now Assist のスキルのハルシネーションの低減に役立つ関連データを得ることができます。

共有に参加しない場合は、Now Assist アドミンコンソールから ServiceNow インスタンスのデータ共有をオプトアウトすることを選択できます。「Opt out of data sharing for Now Assist」を参照してください。Now Assist の機能を使用するすべてのインスタンスに対してオプトアウトプロセスを繰り返します。

Now Assist アドミンコンソールを使用して、セキュリティインシデントレスポンス向け Now Assist を構成します。このコンソールには、アプリケーションのインストールと生成 AI スキルの構成に必要なものがすべて含まれています。詳細については、「Configuring Now Assist settings and features」を参照してください。

次の表に、Now Assist アドミン コンソールからアクセスできる機能とスキルを示します。

Now Assist アドミン コンソールの セキュリティインシデントレスポンス向け **Now Assist** の機能とスキル

Now Assist テクノロジー製品	セキュリティインシデントスキル
セキュリティインシデントレスポンス向け Now Assist	セキュリティインシデントの要約 **注:** インシデントの要約は、[ドラフト] 以外のすべてのステータスのセキュリティインシデントをサポートします。
	解決メモの生成。
	セキュリティインシデントの推奨アクション セキュリティインシデント推奨アクションスキルは、[クローズ済み] および [キャンセル] 以

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Now Assist アドミン コンソールの セキュリティインシデントレスポンス向け **Now Assist** の機能とスキル (続く)

Now Assist テクノロジー製品	セキュリティインシデントスキル
	外のステータスのセキュリティインシデントをサポートします。 **注:** セキュリティインシデントに対して推奨アクションスキルが機能するように、AI 検索アプリケーションを有効にする必要があります。インスタンスで AI 検索が有効になっていることを確認するには、 **All** (すべて) > **AI** 検索 > **AI** 検索ステータス. ページに AI 検索が有効になっていないことが示されている場合は、サポートに連絡してください。 相関インサイトは、すべての状況のセキュリティインシデントをサポートします。
	インシデントの事後分析の生成

1. Install Now Assist plugins .

   セキュリティインシデントレスポンス向け Now Assist アプリケーション (sn_sec_gen_ai) をインストールします。

2. セキュリティインシデントレスポンス向け Now Assist のスキルを設定してアクティブ化する

   スキルの詳細を構成および確認します。ガイド付きセットアップ からスキルをアクティブ化します。

ガイド付きセットアップ による セキュリティインシデントレスポンス向け **Now Assist** の実装

ガイド付きセットアップ には一連のタスクがあり、ご利用の ServiceNow インスタンスで セキュリティインシデントレスポンス向け Now Assist を設定するのに役立ちます。セキュリティインシデントレスポンス向け Now Assistのガイド付きセットアップを開くには、 **All** (すべて) > **Now Assist** アドミン > 機能.

詳細については、「セキュリティインシデントレスポンス向け Now Assist のスキルを設定してアクティブ化する」を参照してください。

セキュリティインシデントレスポンス向け **Now Assist** のスキルを設定してアクティブ化する

ガイド付きセットアップでスキルの詳細を設定および確認します。ガイド付きセットアップからスキルをアクティブ化できます。

始める前に
必要なロール：admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 **All** (すべて) > **Now Assist** アドミン > 機能.
2. ナビゲーションパネルで [テクノロジー] を選択した状態で、リストから **[Security Operations]** を選択します。
   これらのセキュリティインシデントスキルは、次のセキュリティインシデントカードに表示されます。
   - セキュリティインシデントの推奨アクション

     セキュリティインシデントに対して推奨アクションスキルが機能するように、AI 検索アプリケーションを有効にする必要があります。インスタンスで AI 検索が有効になっていることを確認するには、 **All** (すべて) > **AI** 検索 > **AI** 検索ステータス. ページに AI 検索が有効になっていないことが示されている場合は、サポートに連絡してください。
   - インシデントの事後分析
   - 相関インサイトの生成
   - セキュリティインシデントの要約
   - 解決メモ生成
3. [詳細を表示] を選択します。
   アプリケーションに含まれているスキルは編集できません。デフォルト設定を編集するには、コピーを作成する必要があります。スキルのカスタマイズの詳細については、「 セキュリティインシデントレスポンス向け Now Assist スキルをカスタマイズする」を参照してください。
4. 必要なスキルの [スキルをアクティブ化 **(Activate skill)]** を選択します。
5. ガイド付きセットアップを使用してスキルを設定し、アクティブ化する手順に従います。

   注:
   一部のスキルでは、以下にリストされているすべての構成手順は必要ありません。左側のパネルに表示されているタスクのみを選択し、プロンプトに従います。タスクを完了したら、スキルをアクティブ化します。

   a. ナビゲーションパネルで、[入力を選択 **(Choose input)]** を選択して、選択したスキルの入力またはトリガーを構成します。

      スキルの入力テンプレート (一部、またはすべて) がリストされます:対応中、レビュー、クローズ済み。[対応中] テンプレートが選択されています。

      これらの入力テンプレートは、セキュリティオペレーション向け Now Assist のスキルの動作に慣れるまで、デフォルト設定のままにしておくことをお勧めします。

      ただし、 一部のスキルでは 、特定の関連テーブルフィールドを変更したり、セキュリティインシデントでプロンプトをテストしたり、スキルの可用性を定義したり、スキルを表示する場所を選択したりできます。

      フィールドを変更する場合、入力データの一部として提供されるリストから、サポートされているオプションのみを選択します。

      スキルの入力またはトリガーを変更する場合、スキルをいつどのように使用するかを決定できます。スキルの入力データソースは変更できません。データソースには、スキルが依存するテーブルとフィールドが含まれています。ただし、スキルをコピーしてカスタマイズすることはできます。詳細については、「セキュリティインシデントレスポンス向け Now Assist スキルをカスタマイズする」を参照してください。

6. [保存して続行] を選択して、ガイド付きセットアップ の次の手順に進みます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

7. オプション: セキュリティインシデントレコードのプロンプトをテストします。
8. [保存して続行] を選択して、ガイド付きセットアップ の次の手順に進みます。
9. オプション: 次のいずれかのオプションを選択して、可用性を定義します。

10. [保存して続行] を選択して、ガイド付きセットアップ の次の手順に進みます。
11. [表示を選択 **(Select display)**] を選択して、スキルを表示する場所を決定します。

12. [保存して続行] を選択して、次の手順に進みます。
13. オプション: ロールを追加または削除します。

    (Optional) デフォルトでは、sn_si.analyst ロールと sn_si.manager ロールが追加され、自動スキル生成の結果を確認できます。ロールを追加または削除できるのは、 セキュリティインシデントレスポンス向け Now Assist スキルをカスタマイズする場合のみです。

14. 選択内容を確認し、[アクティブ化] を選択してスキルの構成を完了します。
15. [セキュリティインシデントに戻る **(Return to Security Incident)**] を選択します。
    スキルは [Active skills (アクティブなスキル)] セクションに表示されます。

セキュリティインシデントレスポンス向け **Now Assist** スキルをカスタマイズする

環境の要件に合わせて、生成 AI スキルの一部の入力フィールドをカスタマイズします。

始める前に
必要なロール：admin

手順

1. に移動します **All** (すべて) > **Now Assist** アドミン > 機能 Now Assist アドミンコンソールのタブ。
2. ナビゲーションパネルで [テクノロジー] を選択した状態で、リストから **[Security Operations]** を選択します。
   次のセキュリティインシデントスキルが表示されます。
   - セキュリティインシデントの推奨アクション
   - インシデントの事後分析
   - 相関インサイトの生成
   - セキュリティインシデントの要約
   - 解決メモ生成
3. スキルのコピーを作成し、入力フィールドをカスタマイズします。

   a. セキュリティインシデント機能カードで、[詳細を表示] を選択します。

   b. [アクティブなスキル (Active skills)] セクションで、コピーするスキルを見つけ、その他のアクションアイコン ( ) を選択します。

   c. [コピーを作成] を選択します。

   d. モーダルで選択内容を確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ガイド付きセットアップが表示されます。

e. [一般的な詳細] で、スキルの一意の名前と説明を入力します。

f. [保存して続行] を選択して、次の手順に進みます。

g. [入力を選択 **(Choose input)]** を選択します。

[入力を選択 **(Choose input)]** を選択した場合、スキルの入力テンプレート [対応中]、[レビュー] および [クローズ済み] がリストされます。[対応中] テンプレートが選択されています。

テンプレートの一部のベース入力テーブルフィールド、条件、および関連リストを構成できます。入力データのリストでサポートされている関連テーブルからのみ選択してください。

ベース入力テーブル [sn_si_incident] を変更したり、セキュリティインシデント要約スキルのコピーの新しいデータソースを追加したりすることはできません。

h. 条件ビルダーとフィルタリング条件を使用して、[対応中] テンプレートの編集可能なフィールドの変更を続行します。

i. [保存して続行] を選択して、[対応中] テンプレートのガイド付きセットアップの次の手順に進みます。

- プロンプトをカスタマイズ：事前定義されたセクションを並べ替えたり削除したりして、プロンプトを編集します。各入力テンプレート構成のセキュリティインシデントレコードでプロンプトを確認してテストできます。
- 可用性を定義：

オプション	説明
スキルはいつでも利用可能	スキルはいつでもユーザーが利用できます。
スキルの利用可否をカスタマイズする	スキルは、条件が満たされた場合にのみ使用できます (デフォルト)。 条件ビルダーを使用して条件を設定します。

- 表示を選択：

オプション	説明
製品内	すべてのセキュリティ製品のセキュリティインシデントの要約を表示します。Now Assist スキルはフォームとワークスペースに表示されます。
ユーザーロール	[

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
Now Assist パネル	Now Assist スキルは Now Assist パネルで使用できます。 **注:** このオプションが表示されない場合は、Now Assist パネルをアクティブ化する必要があります。詳細については、「Turn on the Now Assist panel」を参照してください。

j. [テンプレートの保存 **(Save template)]** を選択して、[対応中] テンプレートへの変更を保存します。

k. [レビュー] テンプレートを選択します。

l. 前の手順で説明したように、フィルタリング条件を使用して、[レビュー] テンプレートと [クローズ済み] テンプレートの編集可能なフィールドを引き続き変更します。

m. [保存して続行] を選択して、ガイド付きセットアップの次の手順に進みます。

n. [テンプレートの保存 **(Save template)]** を選択して、テンプレートへの変更を保存します。

o. [レビューとアクティブ化 **(Review and Activate)]** を選択してスキルをレビューし、追加の変更を行います。

4. **[Activate** (アクティブ化)] を選択します。
スキルは、[セキュリティインシデント] ページの [利用可能なすべてのセキュリティインシデントスキル] セクションに表示されます。
5. [スキルのアクティブ化 **(Activate skill)**] を選択します。

セキュリティインシデントレスポンス向け **Now Assist** の入力とトリガー

生成 AI スキルの一部の入力またはトリガーを構成できます。入力またはトリガーを使用すると、スキルをいつどのように使用するかを決定できます。

入力とトリガー

入力は、スキルに使用されるデータを識別します。入力には、セキュリティインシデントサマリーの生成に使用されるテーブルとフィールドが含まれます。トリガーによって、アクションは開始されます。たとえば、トリガーによって、システムがサマリーを生成するタイミングが決まります。

入力とトリガーは変更できますが、スキルのデータソースは変更できません。データソースには、スキルが依存するテーブルとフィールドが含まれています。

セキュリティインシデントの要約スキル

セキュリティインシデントの要約スキルの入力により、セキュリティインシデントのサマリーが生成されるときに使用されるテーブルとフィールドが特定されます。次の表は、Now Assist アドミンコンソールの [入力を選択 (Choose input)] ページからのセキュリティインシデントのサマリースキルの入力を示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

入力	説明
データソース	セキュリティインシデント [sn_si_incident] テーブル。
入力フィールド	• 簡単な説明 • Description (説明) • 状況 • 優先度 • 作業メモ • 追加コメント
関連する入力テーブル	• 影響を受ける CI - 構成アイテム • 影響を受けるユーザー - ユーザー • セキュリティインシデントレスポンスタスク - 簡単な説明 • ステータス - [キャンセル済み] 以外のステータス。 • 関連する観測可能項目 - 観測可能項目の結果は「悪意がある」または「疑わしい」です。

自動翻訳

解決メモ生成スキル

解決メモ生成スキルの入力には、セキュリティインシデントの解決メモが生成されるときに使用されるテーブルとフィールドを識別します。次の表は、Now Assist アドミンコンソールの [入力を選択 (Choose input)] ページからの解決メモ生成スキルの入力を示しています。

入力	説明
データソース	セキュリティインシデント [sn_si_incident] テーブル。
入力フィールド	• 簡単な説明 • Description (説明) • Work notes (作業メモ) • 追加コメント

セキュリティインシデント推奨アクションの生成スキル

入力	説明
データソース	セキュリティインシデント [sn_si_incident] テーブル。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インシデントの事後分析の生成スキル

入力	説明
データソース	セキュリティインシデント [sn_si_incident] テーブル。

相関インサイト生成スキル

セキュリティインシデントの相関インサイトには、次のテーブルのレコードを含めることができますが、これらのテーブルとレコードにアクセスするための権限が必要です。

入力	説明
データソース	セキュリティインシデント [sn_si_incident] テーブル。 構成アイテム [cmdb_ci] テーブル。 インシデント [incident] テーブル。 変更要求 [change_request] テーブル。 問題 [problem] テーブル。 脆弱性一致アイテム [sn_vul_vulnerable_item] テーブル。 観測事象 [sn_ti_observable] テーブルを関連付けます。

セキュリティインシデントレスポンス向け **Now Assist**を使用したセキュリティインシデントのクローズ

セキュリティアナリストは、 セキュリティインシデントレスポンス向け Now Assist でサポートされている生成 AI スキルを使用して、作業フロー内からセキュリティインシデントを迅速にクローズできます。

セキュリティインシデントレスポンス向け **Now Assist** の概要

セキュリティインシデントレスポンス向け Now Assist を使用した生成 AI スキルを使用すると、セキュリティアナリストは次のことができます。

- セキュリティインシデントの詳細を要約し、簡潔で読みやすい形式でコンテキストをすばやく確認します。
- クローズ (解決) メモを生成します。
- セキュリティインシデントの推奨アクションの生成
- インシデントの事後分析データの生成
- 相関に関するインサイトを生成して、インシデント調査を迅速化します。

セキュリティマネージャーとアナリストは、次の場所からセキュリティインシデントサマリーとクローズメモを要求できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- セキュリティインシデントレコード
- セキュリティインシデントレスポンス ワークスペース
- Now Assistパネル。

> **注:**
> セキュリティインシデントの推奨アクションとインシデントの事後分析スキルは、[Now Assist] パネルからは使用できません。

セキュリティマネージャーとアナリストは、推奨される次のステップとインシデント後の分析データを次の場所から生成できます。

- セキュリティインシデントレコード
- セキュリティインシデントレスポンス ワークスペース

セキュリティマネージャーとアナリストは、 セキュリティインシデントレスポンス ワークスペースのセキュリティインシデントからのみ、生成された推奨アクションから修復タスクを作成できます。

1. セキュリティインシデントレスポンス向け Now Assist でセキュリティインシデントを要約

   根本的な問題、インシデントの詳細、関連リストのデータ (観測事象)、既に実行された主なアクションなどを含めたセキュリティインシデントのサマリーを生成します。

2. を使用したセキュリティインシデントの推奨アクションの生成 セキュリティインシデントレスポンス向け Now Assist
3. を使用したセキュリティインシデントのインシデントの事後分析の生成 セキュリティインシデントレスポンス向け Now Assist
4. との相関インサイトの生成 セキュリティインシデントレスポンス向け Now Assist
5. セキュリティインシデントレスポンス向け Now Assist を使用したセキュリティインシデントのクローズメモの生成

   セキュリティインシデントのクローズメモを自動的に生成します。

6. セキュリティインシデントレスポンス向け Now Assist の Now Assist パネルでの生成 AI スキルの要求

   Now Assist パネルからサマリーとクローズメモを生成します。

   > **注:**
   > セキュリティインシデントの推奨アクションとインシデントの事後分析スキルは、[Now Assist] パネルからは使用できません。

7. セキュリティインシデントレスポンス向け Now Assist スキルをカスタマイズする

   環境の要件に合わせて、スキルの入力フィールドをカスタマイズします。

セキュリティインシデントレスポンス向け **Now Assist** でセキュリティインシデントを要約

セキュリティインシデントを要約する生成 AI の機能を活用して、セキュリティインシデントのコンテキストを把握します。

始める前に

セキュリティインシデントは、 従来 コア UI (UI16) および セキュリティインシデントレスポンス ワークスペース で要約できます。生成 AI を使用してインシデントを要約するには、フィールドに 50 以上の単語を入力して入力データに使用する必要があります。入力フィールドの詳細について

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

は、「セキュリティインシデントレスポンス向け Now Assist の入力とトリガー」を参照してください。

必要なロール:sn_si.analyst、sn_si.manager、または sn_si.basic

手順

1. 従来 コア UI で、次の場所に移動します: **All** (すべて) > セキュリティインシデント > インシデント をクリックし、自分に割り当てられているセキュリティインシデントを開きます。
2. または、 **All** (すべて) > セキュリティインシデント > セキュリティインシデントレスポンスワークスペース をクリックし、自分に割り当てられているセキュリティインシデントを開きます。
3. [概要] タブで、[要約] を選択します。
   - 生成されたサマリーは、従来 Core UI16 のセキュリティインシデントレコードの上部にあるバナーに表示されます。
   - 生成されたサマリーは、セキュリティインシデントレスポンスワークスペース の [概要] タブに表示されます。
4. オプション: サマリーが生成されたら、次のオプションから選択します。

   (Optional) AI で生成されたサマリーは、重要な詳細情報が欠落している可能性があります。要約の正確性と完全性を確認してからサマリーを使用することをお勧めします。

セキュリティインシデントレスポンス向け **Now Assist** を使用したセキュリティインシデントのクローズメモの生成

セキュリティインシデントをクローズすると、クローズメモのドラフトが自動的に生成されます。ドラフトは編集可能であり、セキュリティインシデントをクローズする前にレビューされ、必要に応じて使用または変更できます。クローズメモは、他のアナリスト、マネージャー、および主要なステークホルダーにセキュリティインシデントの解決に関する情報を提供します。

始める前に
必要なロール:sn_si.analyst、sn_si.manager、または sn_si.basic

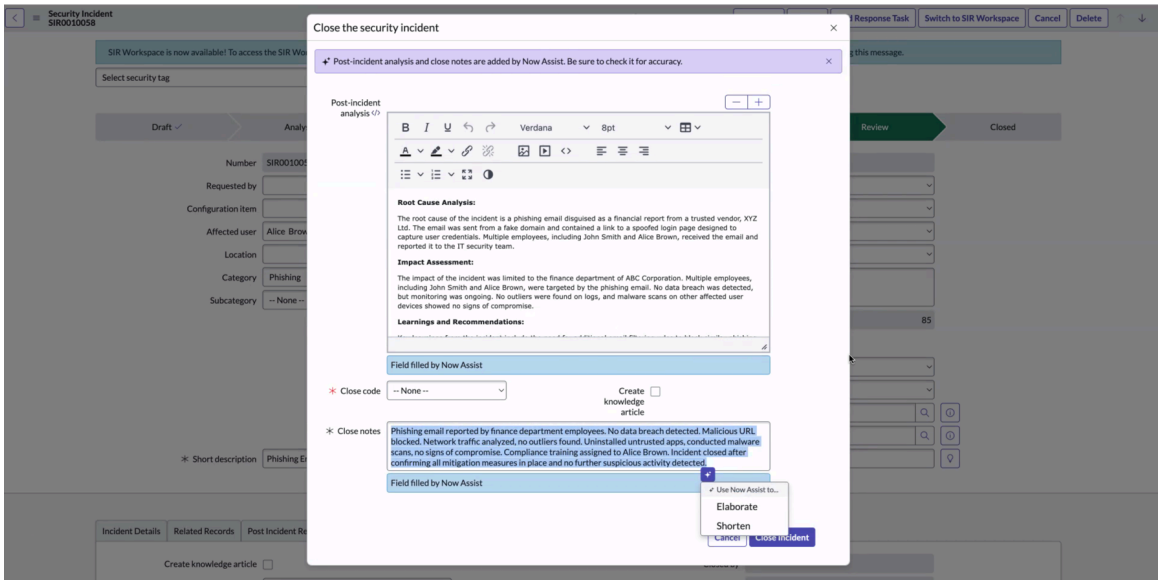
手順

1. 従来 コア UI で、次の場所に移動します: **All** (すべて) > セキュリティインシデント > インシデント をクリックし、自分に割り当てられているセキュリティインシデントを開きます。
2. または、 **All** (すべて) > セキュリティインシデント > セキュリティインシデントレスポンスワークスペース をクリックし、自分に割り当てられているセキュリティインシデントを開きます。
3. セキュリティインシデントをクローズします。

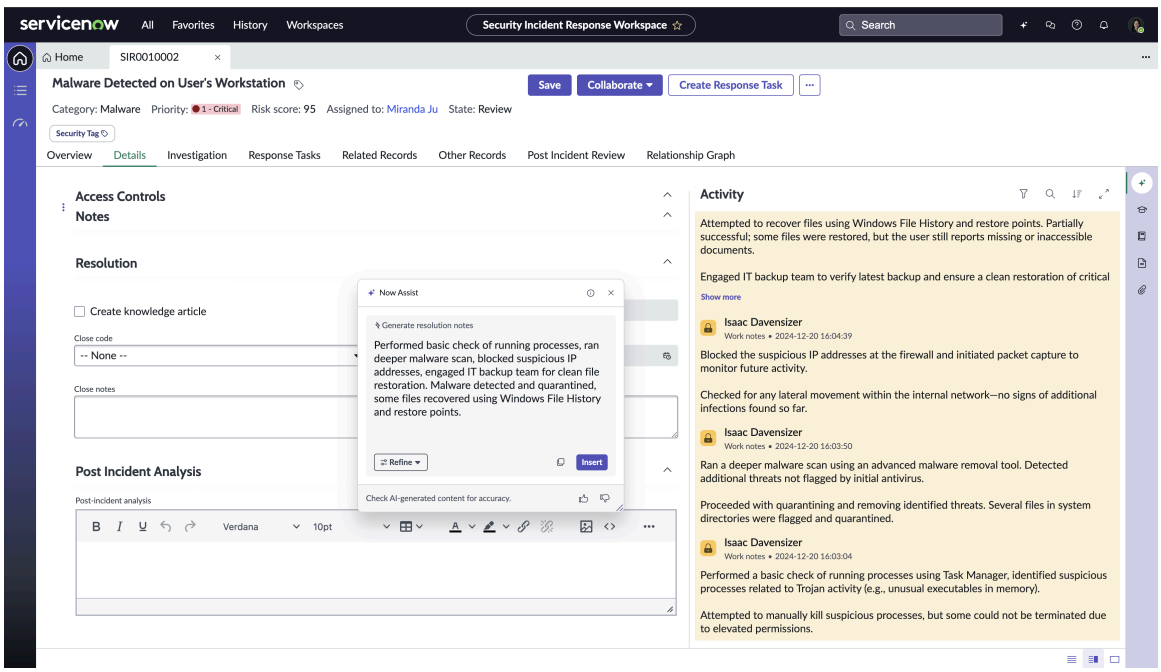
   次のスクリーンショットは、Core UI16 でセキュリティインシデントをクローズするために生成された解決メモを示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



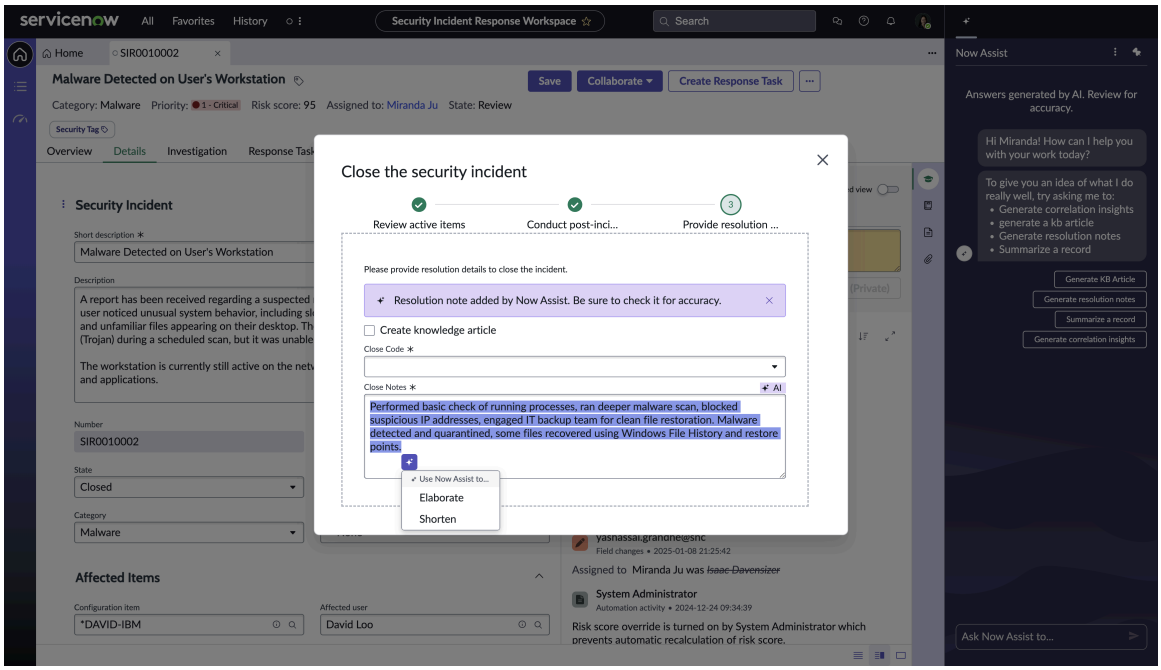
セキュリティインシデントレスポンスワークスペースから自動生成された解決メモ。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンスワークスペースの Now Assist コンテキストメニューを使用して生成された解決メモを編集します。



を使用したセキュリティインシデントの推奨アクションの生成 セキュリティインシデントレスポンス向け **Now Assist**

アナリストがセキュリティインシデントレスポンスワークスペースでセキュリティインシデントをクローズするために実行できる次のステップを自動的に生成します。推奨される手順は、既存のセキュリティインシデントとナレッジ記事に基づいています。

始める前に

推奨される次のステップは 、[クローズ済み] または [キャンセル] 以外のステータスのアクティブなセキュリティインシデントに対して機能します。

セキュリティインシデントに対して推奨アクションスキルが機能するように、AI 検索アプリケーションを有効にする必要があります。インスタンスで AI 検索が有効になっていることを確認するには、 **All** (すべて) > **AI** 検索 > **AI** 検索ステータス. ページに AI 検索が有効になっていないことが示されている場合は、サポートに連絡してください。

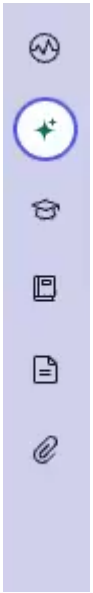
必要なロール:sn_si.analyst、sn_si.manager、または sn_si.basic

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > セキュリティインシデントレスポンスワークスペース をクリックし、自分に割り当てられているセキュリティインシデントを開きます。
2. コンテキストサイドバーで [推奨アクション] アイコン ( ) を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. [推奨事項の取得] を選択します。
4. [AI で生成されたコンテンツを確認] モーダルで、[承認する] を選択します。
   生成された推奨アクションはカードに表示されます。アクションの参照が最大 4 つ上部に表示されます。これらの参照は、ナレッジ記事 (KB) またはセキュリティインシデント (SIR#) の任意の組み合わせにすることができます。
5. カードで、いずれかを選択します。
6. オプション: [推奨アクション] パネルのリフレッシュアイコンを選択して、推奨アクションを再生成します。

   推奨アクションは 1 時間キャッシュされたままになります。次の場合は、推奨される手順を更新することを選択できます。

   - 前回アクションを生成してから、セキュリティインシデントに関連する情報が変更されたと思われる場合。
   - ページを離れ、ログアウトし、再度ログインし、1 時間以内にセキュリティインシデントに戻ります。

   1 時間後に表示するには、ステップ 3 以降のアクションを再生成する必要があります。
7. [カードで 応答タスクを作成] を選択します。
   ワークスペースに新しいタブが開きます。[簡単な説明] フィールドと [説明] フィールドは、選択した推奨アクションカードの詳細から自動的に入力されます。
8. 必要に応じてフォームを編集し、[保存] を選択して応答タスクを作成します。
   システムプロパティの値を変更するまで、生成する推奨アクションの 2 つのオプションは [詳細を表示] と [対応タスクを作成] のままになります。
9. オプション: 推奨アクションから応答タスクを作成します。
   デフォルトでは、ワークフローには、カードから作業メモに推奨アクションを保存するオプションがあります。アクションカードを作業メモに保存する代わりにアクションカードから作成するオプションが必要な場合は、 **SecOps** 推奨アクション [sn_sec_ra.card_action_config] システムプロパティの [値] フィールドを変更する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. セキュリティインシデントマネージャーロール [sn_si.manager] を持つユーザーとして、[sys_properties] に移動します。リスト。

b. SecOps 推奨アクション [sn_sec_ra.card_action_config] システムプロパティを見つけて、レコードを開きます。

c. [Value] を [share_to_work_notes] から [create_task] に変更します。

d. レコードを保存します

e. セキュリティインシデントレコードに戻り、ページを更新します。
アクションカードには、[詳細を表示] と [応答タスクを作成] のオプションがあります。

を使用したセキュリティインシデントのインシデントの事後分析の生成 セキュリティインシデントレスポンス向け **Now Assist**

根本原因分析、影響度アセスメント、学習と推奨事項の情報を含む、セキュリティインシデントのインシデントの事後分析を自動的に生成します。

始める前に

インシデントの事後分析を セキュリティインシデントレスポンス向け Now Assist で自動的に生成する場合は、インシデントの事後分析スキルを有効にする必要があります。

セキュリティインシデントをクローズする前にクローズメモが既に手動で入力されている場合、アナリストが [ステータス] フィールドを [クローズ済み] に設定しても、このコンテンツはセキュリティインシデントレスポンス向け Now Assistによって上書きされません。

必要なロール:sn_si.analyst、sn_si.manager、または sn_si.basic

手順

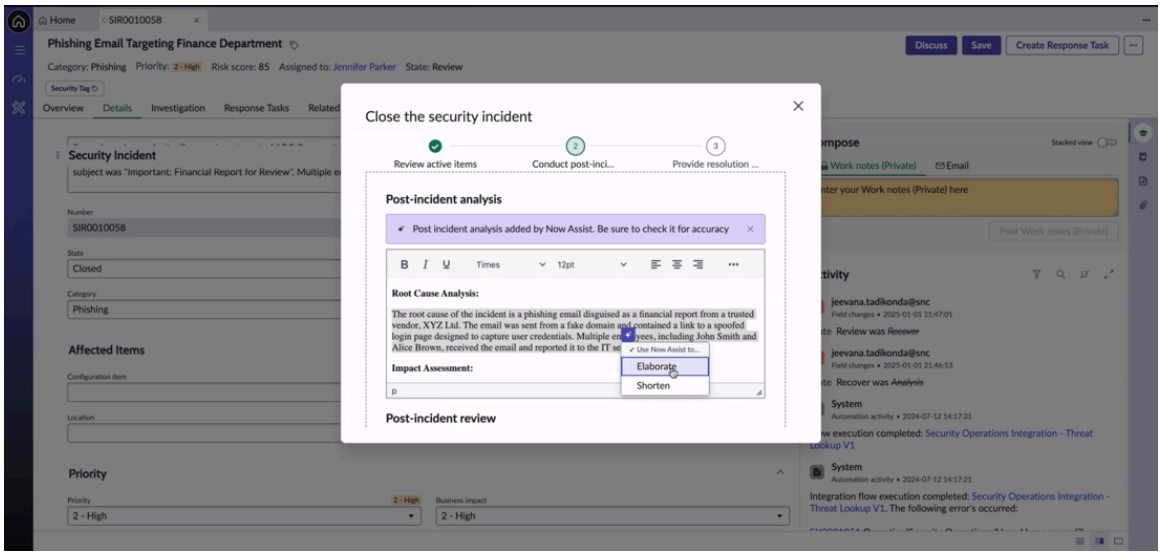
1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > セキュリティインシデントレスポンスワークスペース をクリックし、自分に割り当てられているセキュリティインシデントを開きます。
2. [詳細] タブで、[ステータス] フィールドで [クローズ済み] を選択して、セキュリティインシデントをクローズします。
[セキュリティインシデントをクローズ] モーダルが開きます。
3. オプション: [アクティブなタスクをレビュー] を選択して、このインシデントに関連付けられているアクティブな修復タスクをレビューします。
新しいタブが開き、レビュー用のレコードが表示されます。このアクションにより、関連するワークフローとアクティビティがキャンセルされ、関連する修復タスクでインシデントがクローズされるため、セキュリティインシデントをクローズする準備ができていることを確認するためにこのオプションを使用します。
4. インシデントの事後分析を生成するには、[次へ] を選択します。
インシデントの事後分析は、3 つのセクションを含むモーダルに表示されます。Now Assist アイコン (✦) は、コンテンツが セキュリティインシデントレスポンス向け Now Assist によって生成されたことを示します。
   - 根本原因分析
   - インパクトアセスメント
   - 学習内容と推奨事項

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
インシデントの事後分析オプションで Now Assist コンテキストメニューを使用して、根本原因分析/影響アセスメント/学習と推奨事項を詳細にしたり短縮したりして、テキストを置き換えることができます。**Elaborate** は、既存のテキストにさらに情報を追加するのに役立ちます。[短縮] を選択すると、選択したテキストがより簡潔になります。

次のスクリーンショットは、Now Assist コンテキストメニューを使用して、目的のインシデントの事後分析テキストを詳細化または短縮して置換する方法を示しています。



5. レポートをレビューして正確性を確認し、必要な編集を行います。
6. オプション: [アセスメントの実施] を選択し、 レポートを構成/プレビュー して、インシデントの事後レビューを実行します。
   インシデントの事後レビューに加えた編集は、このページを離れてアセスメントを実施するか、別のアクションを実行する場合、1 時間保持されます。1 時間後に、インシデントの [ステータス] を再度 [クローズ 済み] に設定して、インシデントの事後分析とクローズメモを再生成する必要があります。
7. [次へ] を選択して、解決メモを生成します。
   解決メモが [クローズメモ] フィールドに表示されます。
8. [クローズコード] のリストから 1 つ選択します。
9. **[Close Incident** (インシデントのクローズ)] を選択します。
   インシデントの事後分析は、[詳細] タブの [インシデントの事後分析] フィールドと、セキュリティインシデントレスポンスワークスペースのセキュリティインシデントの [概要] タブに保存されます。

による相関インサイトの探索 セキュリティインシデントレスポンス向け **Now Assist**

セキュリティインシデントから、相関インサイトの基準を選択します。

相関インサイトの生成に関する重要な注意

- セキュリティインシデントレスポンスワークスペースまたは 従来 UI (UI16) の任意のステータスのセキュリティインシデントレコードから相関インサイトを生成できます。
- デフォルトでは、相関インサイトは過去 30 日間の一致するレコードを検索します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- セキュリティインシデントレスポンスワークスペースの [詳細] タブ、または 従来 UI (UI16) の [構成アイテム]、[影響を受けるユーザー]、および [観測事象] の [相関インサイトの観測事象] フィルターの値を見つけて確認できます。
- 会話をリセットするまで、検索条件と結果は [Now Assist] パネルに表示されたままになります。会話をリセットするには、パネルの [Now Assist リセット] メニューアイコン ( ) を選択し、[会話をリセット] を選択します。
- 生成された相関インサイトでこれらのレコードを表示するには、次のテーブルにアクセスする必要があります。
  - 構成アイテム [cmdb_ci] テーブル。
  - インシデント [incident] テーブル。
  - 変更要求 [change_request] テーブル。
  - 問題 [problem] テーブル。
  - 脆弱性一致アイテム [sn_vul_vulnerable_item] テーブル。
  - 観測事象 [sn_ti_observable] テーブルを関連付けます。
- 相関インサイトの結果は、アクセス権を持つテーブルに基づきます。たとえば、相関インサイトの結果で脆弱性一致アイテム (VIT) を表示するには、 脆弱性対応 アプリケーションと読み取りアクセスロール (sn_vul.read_all) がインストールされている必要があります。

相関インサイトを生成する手順については、「 との相関インサイトの生成 セキュリティインシデントレスポンス向け Now Assist」を参照してください。

との相関インサイトの生成 セキュリティインシデントレスポンス向け **Now Assist**

Now Assistパネルから相関に関するインサイトを生成して、過去のイベントを作業中のセキュリティインシデントに結び付けるのに役立ちます。生成した関連情報を使用して、影響を受けるユーザー、構成アイテム、および観測事象の調査の重複を回避し、作業中のインシデントをより迅速に解決することができます。

始める前に

Now Assistパネルに [相関インサイトを生成] オプションを表示するには、相関インサイト生成スキルをアクティブ化する必要があります。

Now Assistパネルが表示されない場合は、アクティブ化する必要があります。詳細については、「Turn on the Now Assist panel 」を参照してください。

相関インサイト検索の詳細については、「 による相関インサイトの探索 セキュリティインシデントレスポンス向け Now Assist」を参照してください。

必要なロール:sn_si.analyst、sn_si.manager、または sn_si.basic

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > セキュリティインシデントレスポンスワークスペース をクリックし、自分に割り当てられているセキュリティインシデントを開きます。
2. または、 従来 UI (UI16) で、セキュリティインシデント [sn_si_incident] テーブルでセキュリティインシデントを見つけて開きます。
3. 上部のヘッダーにある Now Assist アイコン (✨) を選択して、 Now Assist パネルを開きます。
4. [相関インサイトの生成] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

相関インサイトは、次の値の 1 つ以上が一致する場合に生成されます。インサイトの基礎となる次のフィルターが [Now Assist] パネルに表示されます。他のセキュリティインシデントに一致するフィルターのみが表示されます。

> **注:**
> セキュリティインシデントレコードを開いていない場合は、[相関インサイトを生成] を選択した後、セキュリティインシデントレコードの番号を入力するように求められます。

- 構成アイテム (CI):特定のシステムの潜在的な脆弱性を特定するのに役立つ、同じ CI を持つレコード。たとえば、ユーザーのラップトップなどです。
- 影響を受けるユーザー:同じユーザーを持つ過去のインシデント。これにより、頻繁なフィッシング試行や複数の不正なアクセス試行などのパターンを確認できます。たとえば、特定のユーザーの名前などです。
- 観測事象:進行中の潜在的な攻撃や悪意のあるインフラストラクチャの繰り返しの使用を示唆する共有観測事象によってリンクされているレコード。例としては、IP アドレス、URL、ファイルハッシュなどがあります。観測事象の正確な値 (完全なファイルハッシュなど) を入力する必要があることに注意してください。

これらのフィルターのいずれにも一致するデータが存在しない場合、何も表示されません。これらの値の 1 つを作業元のセキュリティインシデントに追加して保存し、パネルで会話をリセットして再試行するように求められます。

5. 会話をリセットするには、パネルで [Now Assist リセットメニュー] アイコン ( ) を選択し、[会話をリセット] を選択します。
6. フィルターを選択します。

   一致する結果が Now Assist パネルに表示されます。

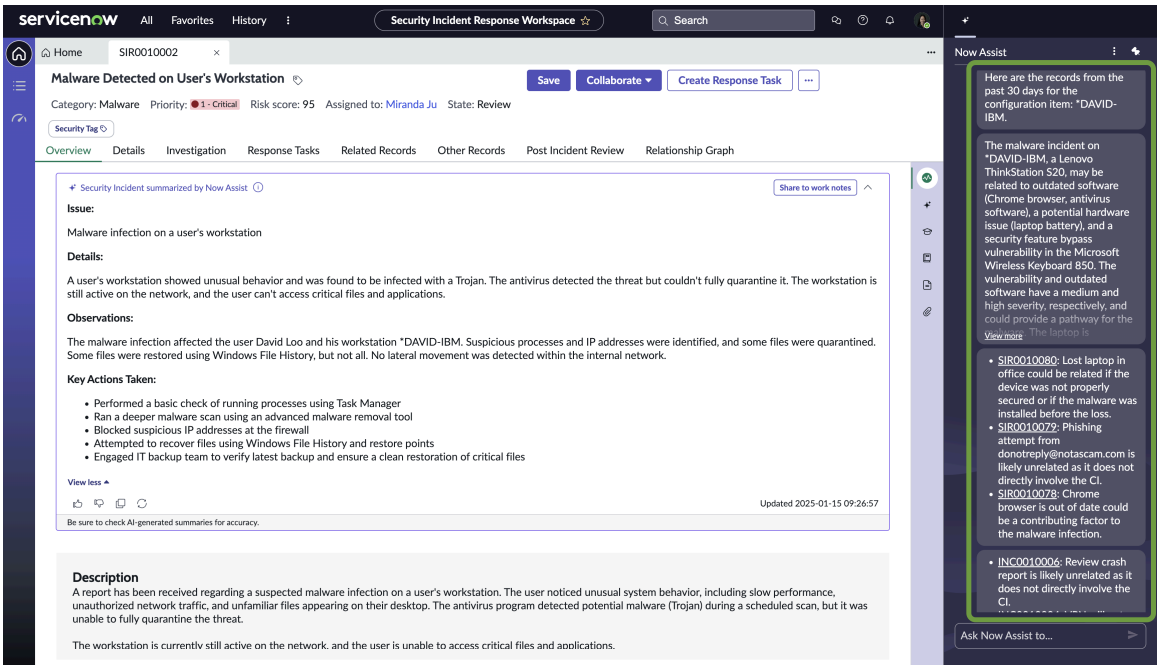
   次の例では、 構成アイテム が要求されています。検索により、高レベルのサマリーと、一致する構成アイテムがあるレコードへのリンクが返されました。

   結果は、セキュリティインシデントレコード (SIR)、インシデント (INC)、変更要求 (CHG)、問題 (PRB)、脆弱性一致アイテム (VIT) のレコードタイプ別にグループ化されます。

   - 影響を受けるユーザーフィルターは、SIR、INC、および CHG レコードを返します。
   - 構成フィルターアイテムは、SIR、INC、CHG、PRB、および VIT レコードを返します。
   - [観測事象] フィルターは SIR レコードを返します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



7. オプション: クエリの 30 日間の制限を変更するには、次の手順を実行します。
   a. セキュリティインシデントマネージャーロール [sn_si.manager] を持つユーザーとして、[sys_properties] に移動します。リスト。
   b. 相関ルックバック期間 [sn_sec_gen_ai.correlation_lookback_period] システムプロパティを見つけて、レコードを開きます。
   c. [値] フィールドに最大 360 の数値を入力します。
   d. レコードを保存します
   e. セキュリティインシデントレコードに戻り、ページを更新します。

セキュリティインシデントレスポンス向け **Now Assist** の **Now Assist** パネルでの生成 **AI** スキルの要求

Now Assist パネルからセキュリティインシデントのサマリーまたはクローズメモを要求します。

始める前に
Now Assist パネルをアクティブにする方法については、「Now Assist panel」を参照してください。

必要なロール:si_analyst、si_manager、または sn_si.basic

手順

1. セキュリティインシデントレスポンス向け Now Assist アプリケーションがインストールされているインスタンスにログインします。
2. 従来 コア UI で、次の場所に移動します: **All** (すべて) > セキュリティインシデント > インシデント をクリックし、自分に割り当てられているセキュリティインシデントを開きます。
3. または、 **All** (すべて) > セキュリティインシデント > セキュリティインシデントレスポンスワークスペース をクリックし、自分に割り当てられているセキュリティインシデントを開きます。
4. 上部のバナーにある Now Assist アイコン ( ) を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Now Assistでの AI エージェントのユースケースの使用セキュリティインシデントレスポンス

セキュリティインシデントレスポンス AI エージェントを使用して、タスクを自律的に完了します。

セキュリティインシデントレスポンスの AI エージェントの利用可能なユースケース

ユースケース名	説明	利用可能な AI エージェント
セキュリティインシデントをクローズ	このユースケースは、セキュリティアナリストが Now Assist パネルで自然言語を使用してセキュリティインシデントをクローズするのに役立ちます。	セキュリティインシデント最終作業ジェネレーター

重要:
デフォルトでは、すべてのユースケースと AI エージェントレコードは読み取り専用です。

ユースケースを変更するには、まず Duplicate an agentic workflow してから、次の手順に進む必要があります。

- ユースケースをアクティブ化します。
- ユースケース内のすべての AI エージェントをアクティブ化します。
- 必要に応じて、ユースケースを自動的に呼び出すトリガーを追加できます。

ユースケースで使用されていない AI エージェントが、 Now Assist アプリケーションとともにインストールされている場合があります。利用可能なすべてのエージェントを表示する方法については、「 AI エージェントを検索する 」を参照してください。

セキュリティインシデントレスポンス AI エージェント収集のクローズセキュリティインシデントのユースケース

セキュリティアナリストは、セキュリティインシデントのクローズのユースケースを使用して、セキュリティインシデントをクローズできます。

クローズ セキュリティインシデントのユースケース概要

セキュリティインシデントのクローズのユースケースを使用して、関連する応答タスクをキャンセルし、セキュリティインシデントのクローズ中に解決メモ、クローズメモ、クローズコード、およびインシデントの事後分析 (PIA) を生成し、 Now Assist パネルから自然言語でフィードバックを提供してコンテンツを調整します。

このユースケースを変更する場合は、 ユースケースを複製 し、特定のニーズに合わせて設定を調整し、代わりにユースケースの複製バージョンをアクティブ化できます。

セキュリティインシデントのクローズのユースケースで使用されるエージェント

セキュリティインシデントの最終作業ジェネレーターエキスパートは、「セキュリティインシデントのクローズ」ユースケースで使用されます。

セキュリティインシデントのクローズのユースケースにマッピングされたツール

次のツールは、「セキュリティインシデントのクローズ」ユースケースで使用される AI エージェントにマッピングされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントをクローズするためにマッピングされたツール

ツールタイプ	実行モード	名前	説明
スクリプト	自律型	セキュリティインシデントの詳細をフェッチ	セキュリティインシデント番号からセキュリティインシデントの詳細をフェッチするためのツール。
スクリプト	自律型	クローズコード値を取得します	セキュリティインシデントで利用可能なクローズコード値を取得するためのツール。
スクリプト	自律型	セキュリティインシデントを誤検出としてクローズします	インシデントが誤検出としてクローズされるときに使用されるツール。
スクリプト	自律型	セキュリティインシデントを更新します	セキュリティインシデントのフィールドを更新するツール。
サブフロー	自律型	クローズメモを生成	セキュリティインシデントのクローズメモを生成するツール。
サブフロー	自律型	インシデントの事後分析を生成します	セキュリティインシデントのインシデントの事後分析を生成するツール。

セキュリティインシデントのクローズユースケースのトリガー

このユースケースのトリガーはありません。必要に応じて、ユースケースを自動的に呼び出すトリガーを追加できます。

セキュリティインシデントのクローズ

Now Assistパネルで AI エージェントとチャットして、セキュリティインシデントのクローズを支援します。

始める前に
必要なロール:sn_si.analyst または sn_si.manager

手順

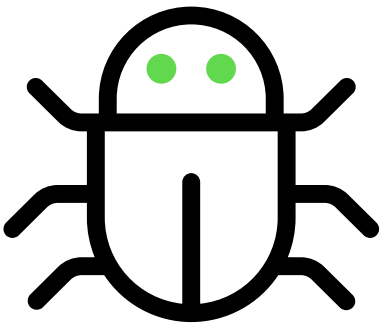
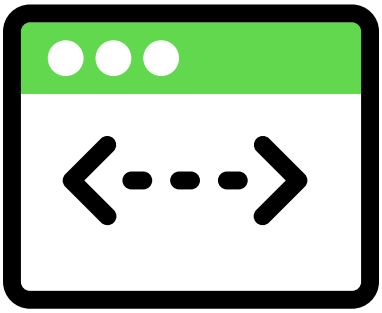
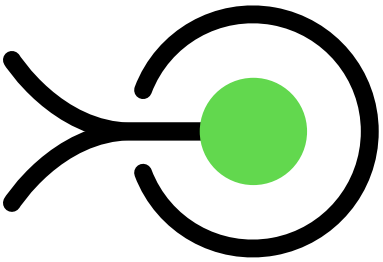
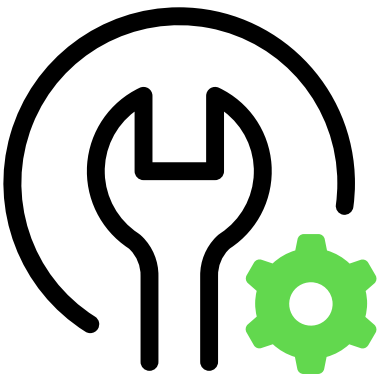
1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > セキュリティインシデントレスポンスワークスペース.
2. AI エージェントを使用して、クローズするセキュリティインシデントを開きます。
3. [Now Assist] (。
   Now Assistパネルが表示されます。
4. 次のいずれかのオプションを使用して、セキュリティインシデントをクローズします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

攻撃対象領域管理アプリケーション

攻撃対象領域管理を構成する 脆弱性対応 やその他のアプリケーションは、脆弱な資産の優先順位付けに役立ち、ビジネスクリティカルなシステムが脅威にさらされているかどうかを判断するのに役立つコンテキストを追加します。CMDB を使用すると、セキュリティチームはシステム間の依存関係を簡単に特定し、変更やダウンタイムのビジネスインパクトを迅速に評価できるようになります。

脆弱性対応 アプリケーション

脆弱性対応	アプリケーション脆弱性対応	**Container Vulnerability Response**
		
脆弱性対応アプリケーションの詳細	Application Vulnerability Response アプリケーションの詳細	Container Vulnerability Response アプリケーションの詳細
コンフィグレーションコンプライアンス	ソフトウェア部品表	
		
コンフィグレーションコンプライアンスアプリケーションについて学習する	ソフトウェア部品表アプリケーションについて学ぶ	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 ワークスペース

脆弱性マネージャー ワークスペース	**IT** 修復ワークスペース	脆弱性アセスメントのワークスペース
脆弱性マネージャー ワークスペースの詳細	IT 修復ワークスペースについて学ぶ	脆弱性アセスメントのワークスペースの詳細

トラブルシューティングとサポート

- セキュリティオペレーションリソースライブラリ
- セキュリティオペレーションコミュニティ
- 既知のエラーポータルで既知のエラー記事を検索する
- 連絡先 カスタマーサービス & サポート

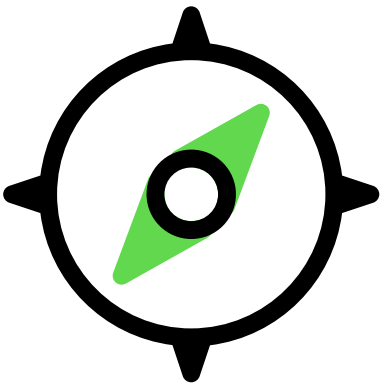
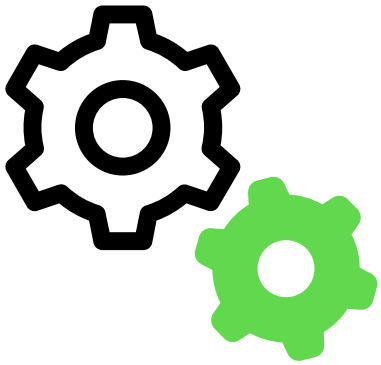
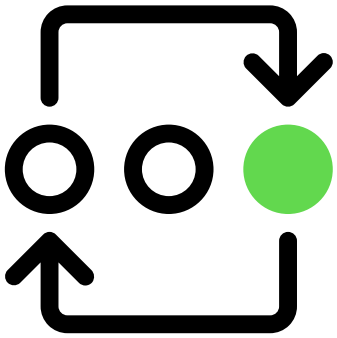
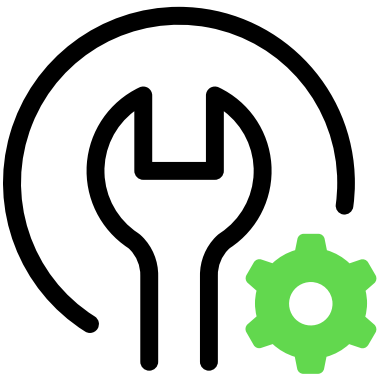
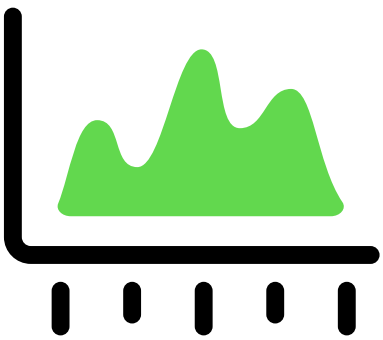
脆弱性対応

脆弱性情報データベース (NVD) およびその他のソースは、既知の脆弱性に関する情報を収集します。こうした脆弱性には、ソフトウェアの脆弱性、マルウェアが悪用できるオペレーティングシステム、その他の攻撃などがあります。ServiceNow 脆弱性対応 アプリケーションは、このような脆弱性の追跡、優先順位付け、および解決に役立ちます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

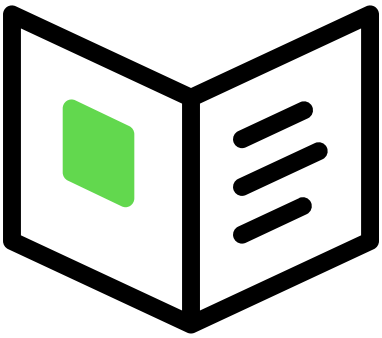
脆弱性対応

探索	セットアップと構成	統合
		
Vulnerability Response の機能について学習する	Vulnerability Response アプリケーションをインストールして設定する	他のアプリケーションと統合することで、Vulnerability Response を拡張する
脆弱性対応ワークスペースの使用	**修復**	**アナリティクスとレポート**
		
脆弱性マネージャー、IT 修復、および脆弱性アセスメントのワークスペースで VIT を監視、管理、および修正する方法について説明します。	脆弱性対応の機能を使用して脆弱性を修正し、資産を保護します	修復の進捗状況を監視

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Reference (参照)



脆弱性対応のリリースノート、コンポーネントの詳細、およびフィールド、テーブル、プロパティに関する参照情報を取得します

トラブルシューティングとサポート

- セキュリティオペレーションリソースライブラリ
- セキュリティオペレーションコミュニティ
- 既知のエラーポータルで既知のエラー記事を検索する
- 連絡先 カスタマーサービス & サポート

脆弱性対応アプリケーションの詳細

ServiceNow® 脆弱性対応 アプリケーションは、脆弱性一致アイテムをインポートし、ルールに従って自動的にグループ化します。これにより、脆弱性を迅速に修復することができます。脆弱性データは、脆弱性情報データベース (NVD) 統合やサードパーティの統合などの外部のソースから取得され、ServiceNow® により開発されたアプリケーションで処理されます。

脆弱性一致アイテム、修復タスク、およびそのライフサイクルを定義する脆弱性対応の概要をご覧ください。

企業内の一般的な脆弱性対応と ServiceNow を使用した脆弱性対応の概要、および脆弱性一致アイテム、脆弱性グループ、およびそのライフサイクルの定義。

脆弱性対応 とエンタープライズ環境

通常、組織はエンタープライズ環境内で脆弱性スキャナーとアセスメントツールを使用して、脆弱性が資産にもたらすリスクを特定して管理します。これらのツールによって特定された脆弱性は、組織の資産の維持と保護を担当するセキュリティチームと IT チームにとってはリスクとなります。一部のリスクには、次に示すタイプの特定された脆弱性が含まれます (これらに限定されなません)。

- 古いソフトウェアまたは構成ミスがあるシステムへの依存
- 保護されていないネットワークプロトコル

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 欠陥のあるサードパーティソフトウェアライブラリへの依存
- システム管理のハイジーンが不十分または一貫していない
- 強化されていないベースラインシステムイメージ

このようなの潜在的なリスクが露呈すると、セキュリティチームと IT チームは通常、スキャンツールとアセスメントツールから生成された大量の脆弱性情報の処理と取り扱いで課題に直面します。具体的には、これらのチームは特定された大量の脆弱性を管理し、組織が直面している潜在的なリスクを軽減するための実行可能な対応作業を策定する際に、その作業に圧倒されます。

次の質問に答えることで、各自のセキュリティ体制におけるこれらの課題を特定できる可能性があります。

- 特定された脆弱性のうち、最初にレビューする必要がある脆弱性はどれか？
- これらの特定された脆弱性は、組織にとってどのような意味を持つか？
- 特定されたリスクについて説明責任を負い、担当する必要がある人物は誰か？
- これらのリスクを解決/軽減するために、実際に作業を行うのは誰か？
- 特定された脆弱性を既存のリソースで効果的に軽減するにはどうすればよいか？
- 特定された脆弱性を減らすことでどのような意図しない結果が生じる可能性があるか？
- 脆弱性を修復し、実行した手順を追跡し、対策が機能したことを確認するためにどのようなプロセスに従うか？
- 全体的なリスク体制の削減が進行しているかどうかをどのように確認できるか？

脆弱性対応、 セキュリティオペレーション 、および **Now Platform®**

脆弱性対応 アプリケーションは Security Operations スイートの一部です。これらのアプリケーションを組み合わせることで、全体的なセキュリティ体制を改善して資産を保護できます。

ServiceNow 脆弱性対応 アプリケーションの 2 つの主な目標は次のとおりです。

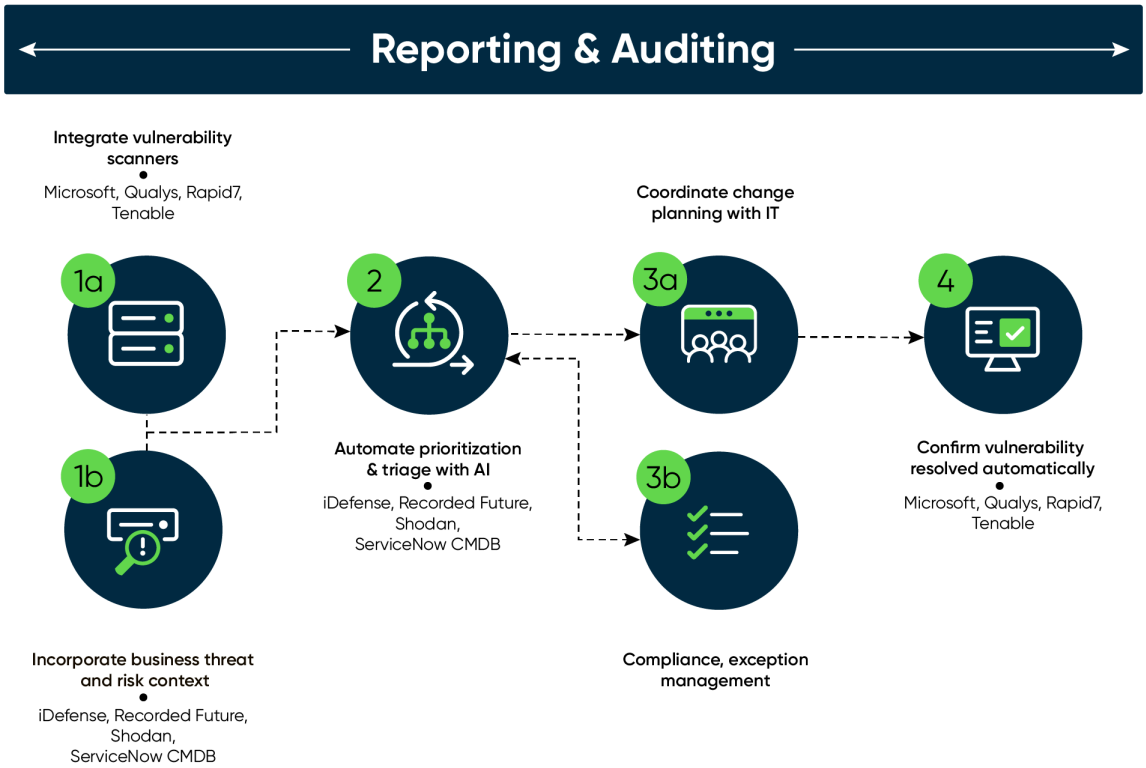
- 大量の脆弱性データの処理に直面しているセキュリティチームを支援する。
- 脆弱性の解決を担当する運用チームを支援する。

このように、脆弱性対応 アプリケーションを使用して統合から調査、解決までの情報のフローを自動化できます。

Now Platform® の脆弱性管理プロセスには、CMDB を使用したプロセス、データ、レポート、および自動化が関与することがあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



®

- サードパーティのスキャナーと ServiceNow　アプリケーションを 脆弱性対応 アプリケーションと統合して、既知の脆弱性データを取り込みます。
- エクスプロイト、脅威インテリジェンス、リスク、およびビジネスコンテキストを使用して、取り込まれた脆弱性データを拡張します。このデータは、パッチ適用と修復戦略で役立ちます。
- NVD からインポートされた脆弱性とサードパーティ製品からの検出データは、CMDB の資産と照合されます。トリアージには、複数の脆弱性一致アイテム (つまり脆弱性があると判断された資産) で構成される修復タスクの作成、カテゴリによるこれらのタスクのグループ化、優先順位付け、チームへのアサインが含まれます。
- 調整された変更および例外管理を導入して、追加の手動介入、解決のためのより多くの時間、または広範な調査が必要になる可能性がある脆弱性の解決を支援します。
- スキャナー製品からの検出によって脆弱性が自動的に解決および更新されていることを確認します。

組織で 脆弱性対応 を使用する可能性があるユーザー

脆弱性対応 ユーザーは通常、2 つのペルソナに分類されます。

脆弱性アナリスト

脆弱性アナリストは通常、セキュリティ、リスクおよびコンプライアンス、または管理分野のペルソナです。これらのユーザーは、脆弱性を監視し、修復プロセスを開始するタイミングを決定します。

> **重要:**
> 脆弱性アナリストは、主に Vulnerability Manager ワークスペース を使用して修復タスクを監視および作成します。

修復オーナー

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

修復オーナーのペルソナは通常、IT 運用、DevOps/エンジニアリングの役割を担うか、またはサービスオーナーです。これらのユーザーは、脆弱性を修正するために必要な修復タスクを行います。資産のメンテナンスまたは削除のために制御プロセスが必要な場合には、例外要求または変更要求を送信することがあります。

重要:
修復オーナーは、主に IT 修復ワークスペース 内から修復タスクに取り組みます。

アプリケーション脆弱性対応

ServiceNow® 脆弱性対応 アプリケーションの アプリケーション脆弱性対応 (AVR) 機能はアプリケーション脆弱性一致アイテム (AVIT) をインポートし、ルールに従ってアプリケーションの脆弱性を修復できます。別のサブスクリプションで利用できます。アプリケーション脆弱性対応 のドキュメントについては、「アプリケーション脆弱性対応 の詳細」を参照してください。

利用可能バージョン

脆弱性対応 にあるフォームとレコードのフィールドデータの他に、用語集とその他のリファレンス (リンク、トラブルシューティング、ナレッジ記事を含む) については、「脆弱性対応 の参照情報」を参照してください。

リリースバージョン	リリースノート
脆弱性対応 v23.0	互換性情報については、「KB0856498 脆弱性対応 互換性マトリクスおよびリリーススキーマの変更」を参照してください。

脆弱性対応 およびサポートされているアプリケーションのインストール

脆弱性対応 アプリケーションは ServiceNow Store から入手可能です。アプリケーションは、他の ServiceNow アプリケーション、および ServiceNow Store からダウンロードするサードパーティ統合もサポートしています。基本セットアップを拡張するためのオプションもあります。

基本セットアップのタスク

最初のステップとして、脆弱性対応 アプリケーションが必要です。インストールの詳細については「脆弱性対応 アプリケーションの実装チェックリスト」を参照して、脆弱性対応アプリケーションをインストールします。

- インストールが完了したら、セットアップアシスタントを使用して脆弱性対応を設定できます。

  セットアップアシスタントを使用して、アプリケーションにアクセスするためのユーザーとグループをアサインし、アサインルール、修復タスクルール、およびターゲット日の作成または編集、リスク算出のセットアップを行います。

- セットアップアシスタントから、サポートされている 1 つ以上のサードパーティ統合を選択、インストール、および設定することもできます。これらの統合は、外部システムとベンダーから脆弱性データを取得します。統合の仕組み、および 脆弱性対応 によってサポートされている統合の詳細については、「脆弱性対応 の統合」を参照してください。
- サードパーティ統合を実装する前に、脆弱性対応 の初期セットアップの一部として NVD 統合と CWE スケジュール済みジョブを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

NVD および CWE ライブラリのインストール、構成、および表示に関する詳細については、「NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理」および「CWE レコードの更新のためのスケジュール済みジョブの構成および実行」を参照してください。

- 該当する場合は、アナリティクスアプリケーションを選択します。脆弱性対応のパフォーマンスアナリティクスコンテンツパックアプリケーションには、脆弱性管理ライフサイクルのすべてのステージを対象としたレポートが含まれています。

  [オプション] 脆弱性対応のパフォーマンスアナリティクス [PA] アプリケーションのインストールと構成 アプリケーション。

- 該当する場合は、ソリューションアプリケーションを選択します。ソリューション管理は、環境内の脆弱性を、それを修復できるソリューションに関連付ける支援を行います。[オプション] 脆弱性対応のソリューション管理アプリケーションのインストール。

  注:

  - 脆弱性ソリューション管理 アプリケーションを有効にすると、Microsoft セキュリティレスポンスセンターソリューション統合 と Red Hat Solution Integration をセットアップアシスタントで編集できます。

  - 脆弱性ソリューション管理 では別のサブスクリプションが必要です。詳細については、「脆弱性ソリューション管理」を参照してください。

- [オプション] ServiceNow エージェントアプリと 脆弱性対応 のモバイルエクスペリエンス のための 脆弱性対応 モバイルアプリをインストールします。

実行可能なその他のセットアップタスク

これらの追加のセットアップタスクは、基本構成に追加され、レポート、メール通知、ネイティブ統合構成、および脆弱性一致アイテムの操作などのオプションで修復をサポートします。これらのタスクのほとんどは、セットアップアシスタントの外部で実行されます。「追加の脆弱性対応セットアップおよび構成タスク」を参照してください。

基本セットアップ以外の高度なタスク

これらのオプションの構成タスクはセットアップアシスタントの外部で実行され、コーディングまたは ServiceNow の高度な専門知識が必要であり、基本構成の一部とは見なされていません。「脆弱性対応 の高度な構成タスク」を参照してください。

脆弱性対応 のペルソナと詳細なロール

脆弱性対応 アプリケーションで脆弱性の修正を正常に完了するには、セットアップアシスタントでユーザーとグループにペルソナとロールをアサインする必要があります。

脆弱性対応 アプリケーションに必要な最初の構成手順の 1 つは、ユーザーとグループにロールをアサインすることです。ロールは、脆弱性対応、脆弱性対応のパフォーマンスアナリティクス、および脆弱性対応 とのすべてのサードパーティ統合において、ユーザーとグループが表示および実行できる内容を規定します。

セットアップアシスタントでペルソナロールを既存のユーザーとグループにアサインします。「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

アップグレードのお客様は、脆弱性対応 アプリケーションの既存のロールを引き続き使用できます。v10.3 より前に sn_vul.vulnerability_read および sn_vul.vulnerability_write 権限によりアサインされたユーザーとグループおよび修復オーナーのアクセス権は変更されていません。

ただし、脆弱性対応 アプリケーションでユーザーやグループが実行および表示できる内容をタスクレベルでより詳細に制御するために、詳細なロールを使用することをお勧めします。詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

セットアップアシスタントを使用して既にロールをアサインしており、ユーザー管理モジュールからすべてのユーザーおよびグループに対して詳細なロールのアサインを管理する場合は、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

ペルソナロールと詳細なロールの開始

主要な用語

ロール

ロールは、ユーザーとグループが 脆弱性対応 アプリケーションで表示および実行できる内容を規定します。

グループ

特定のロールと共通の目的を共有する一連のユーザー。

ペルソナロール

複数の詳細なロールで構成される、アプリケーション内の事前設定されたロール。セットアップアシスタント、脆弱性アドミン、脆弱性アナリスト、修復オーナー、構成アイテムマネージャー、および例外マネージャーのペルソナロールは、IT 組織または脆弱性修復グループのマネージャー、アナリスト、およびサービスオーナーの一般的な役職に対応するように設計されています。

継承されたロール

ユーザーが他のロールをアサインされたときに自動的に獲得するロールを説明する用語。たとえば、sn_vul.remediation_owner ペルソナロールがアサインされているユーザーまたはグループは、sn_vul.read_assigned、sn_vul.write_assigned という詳細なロールも継承します。

アクセス制御リスト (ACL)

アクセス制御リストは、ユーザーがデータを操作する前に、まず要件のセットをユーザーに要求することで、データへのアクセスを制限します。

脆弱性対応 v16.5 以降、レポートが公開されないように保護するには、すべての **report_view ACL** を *active=true* に設定します。この ACL によって、保護されたデータは許可されたユーザーのみが使用可能になります。

セットアップアシスタントでグループとユーザーをペルソナロールにアサインします。

注:
セットアップアシスタントでは、最初のセクションのタスク、ロールのアサイン、統合のインストールにシステムアドミニストレーターロール (admin) が必要です。セットアップアシスタントでペルソナロールをアサインし、統合をインストールした後、sn_vul.vulnerability_admin ロールを持つユーザーまたはグループをアサインして、セットアップアシスタントで残りのタスクを完了し、脆弱性対応 アプリケーションを管理することをお勧めします。

次の表に、アプリケーションとともにインストールされる 脆弱性対応 ペルソナロールを示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性対応 のペルソナロール	説明
sn_vul.vulnerability_admin - 脆弱性アドミンをユーザーまたはグループにアサイン。	このロールを持つユーザーは、脆弱性対応 (VR) アプリケーションとそのレコードに完全にアクセスできます。また、すべての VR アプリケーションとルールを構成したり、サードパーティ統合をインストールしたりできます。
sn_vul.vulnerability_analyst - 脆弱性アナリストをユーザーやグループにアサイン。	このロールを持つユーザーやグループは、VI 修復のすべてのレコードを表示および更新できます。
sn_vul.remediation_owner - 修復オーナーをユーザーやグループにアサイン。	このロールを持つユーザーやグループは、自分または所属するグループにアサインされた脆弱性を修正できます。このロールを持つグループまたはユーザーは、自分または所属するグループにアサインされたレコードを表示および更新します。
sn_vul.ci_manager をユーザーやグループにアサイン。	このロールを持つユーザーやグループは、構成管理データベース (CMDB) にない不一致構成アイテム (CI) の再分類を管理できます。
タスクごとにアプリケーションの特定領域への読み取りアクセス権をアサイン。	たとえば、sn_vul.read_all をアサインして、ユーザーがすべての VR レコードを表示できるようにします。修復タスクルールを表示するための読み取りアクセス権を付与するには、sn_vul.read_group_rules をアサインします。このロールを持つユーザーやグループはレコードを更新できません。

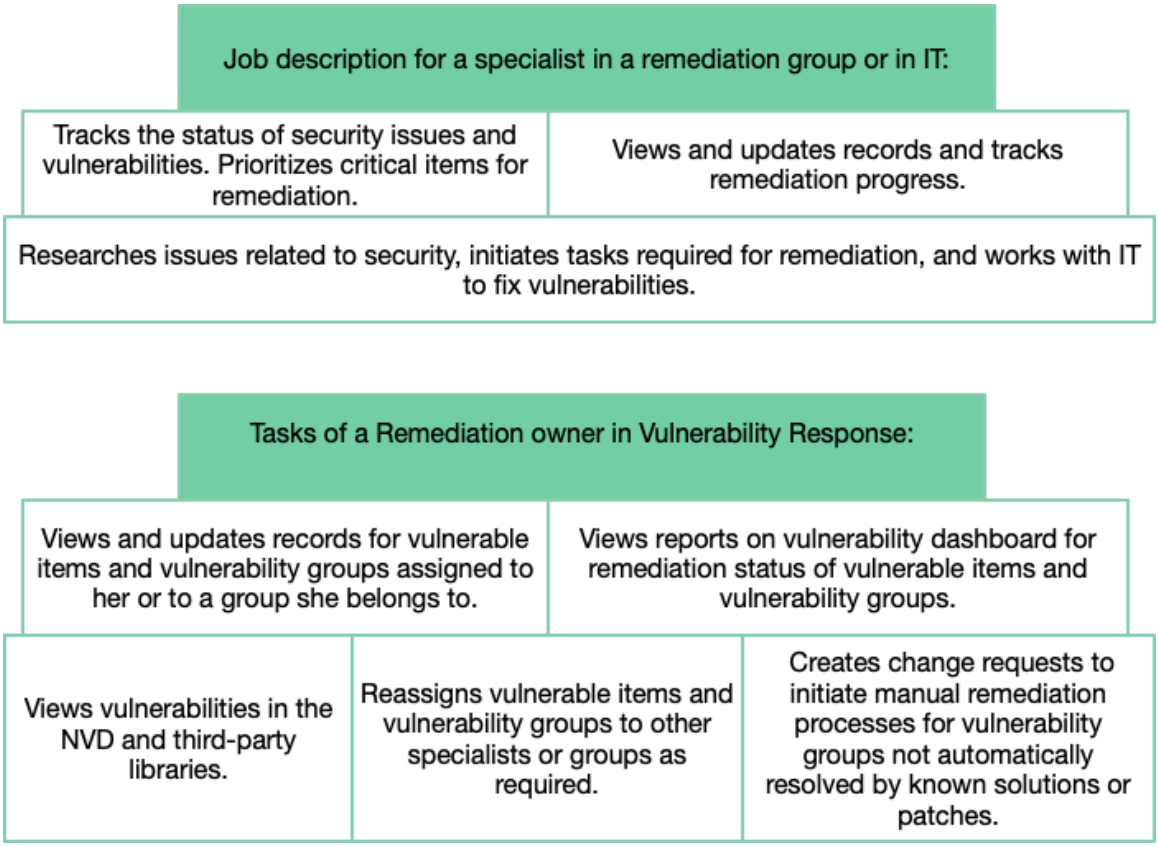
詳細なロールとペルソナロール

ペルソナロールの考え方の 1 つは、その説明が組織内のさまざまな IT または脆弱性修復の職務の説明にどのように関連するかを検討することです。次の図は、IT の修復スペシャリストの考えられる職務の説明と、この職務に関連付けられたタスクが 脆弱性対応 アプリケーションの修復オーナーペルソナロールのタスクにどのように関連しているかを示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

職務の説明とペルソナロール



職務の説明と修復オーナーのペルソナロールは、どちらも一連の修復タスクとして定義できます。前の画像では、職務の説明と緑色ブロック内のペルソナロールが、それらを説明するタスクの上にあります。この例では、修復グループのスペシャリストの一般的な職務要件の一部は、脆弱性対応 の修復オーナーペルソナを構成するタスク (レコードのレビューと更新、脆弱性の修復ステータスの追跡、修復アイテムの優先順位付け、IT による修正とパッチの適用) に直接対応しています。

ただし、組織内の職務が、脆弱性対応 アプリケーションの 5 つのペルソナロールのいずれかを構成するタスクに直接対応していない場合があります。機密データの保護や規制への準拠などのさまざまな理由から、一部のペルソナロールがユーザーやグループに提供する幅広いアクセスを制限する必要があります。または、逆に、ユーザーやグループが職務を遂行できるように、より多くのアクセス権を付与する必要があります。詳細なロールを使用すると、ロールを簡単にカスタマイズし、脆弱性対応、脆弱性対応のパフォーマンスアナリティクス、およびサードパーティの統合に対するユーザーやグループのアクセスを制御できます。

詳細なロールでタスクを定義

脆弱性対応 における詳細なロールの名前は、通常、ユーザーが 脆弱性対応 アプリケーションで実行および表示できる内容を示しています。たとえば前の画像で、修復オーナーのペルソナがアサインされているユーザーやグループには、sn_vul.read_assigned および sn_vul.write_assigned という詳細なロールが設定されています。これらの詳細なロールにより、ユーザーやグループは、アサインされた脆弱性一致アイテムと修復タスクレコードを表示および更新できます。特定の詳細なロールの説明を表示するには、システムアドミニストレーターロールを持つユーザーとして、 ユーザー管理 **(User Administration)** > ロール をクリックし、必要なロールを見つけます。ロールがアサインされたときに自動的に継承されるロールが一覧表示されます。また、ロールが他のロールのアサインに依存している場合は、必要なロールも一覧表示されます。

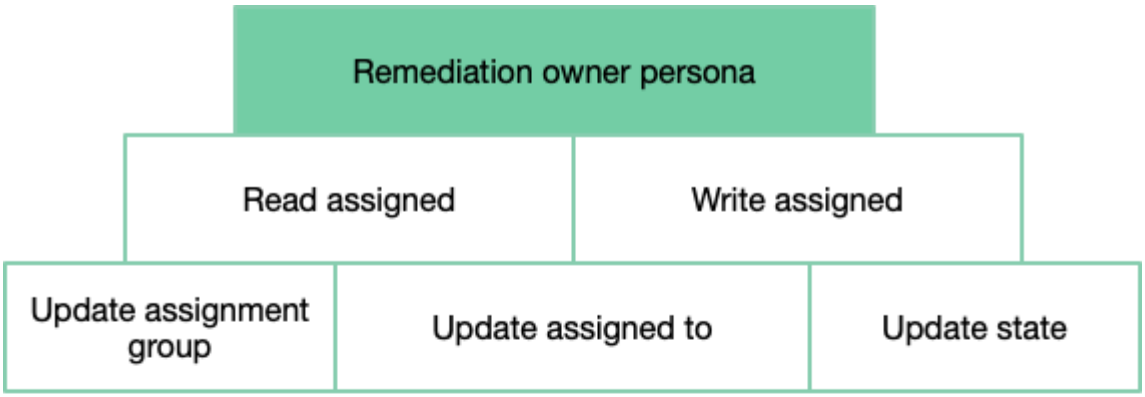
次の画像は、修復オーナーのペルソナと脆弱性アナリストのペルソナの両方について、詳細なロールを示しています。修復オーナーのペルソナには、脆弱性アナリストのペルソナの read_all 権限と write_all 権限が含まれていないことに注意してください。ユーザーやグループがすべての脆弱性一致アイテムと修復タスクレコードを読み取り、編集するには、詳細なロール read_all と write_all が

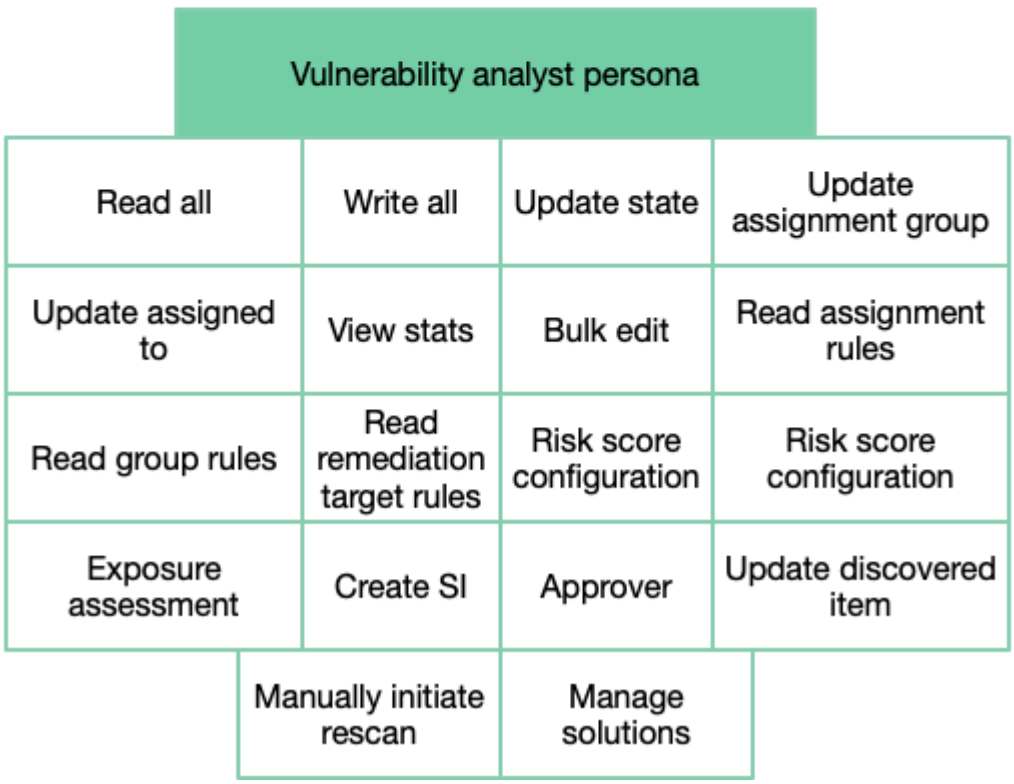
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

必要です。これらのロールをカスタマイズするには、詳細なロールを追加または削除してアクセスを拡大または制限します。

詳細なロールと修復オーナーおよび脆弱性アナリストのペルソナ





ペルソナロールで許可されている数よりも多くのアクセス権をユーザーやグループに付与する場合は、詳細なロールをさらにユーザーやグループに追加できます。逆に、タスクレベルで特定のユーザーやグループのアクセスを制限する場合は、詳細なロールを削除できます。

注:
ユーザー管理モジュールで詳細なロールをアサインして編集するには、システムアドミニストレーターロールが必要です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザー管理モジュールの詳細なロール

ユーザーまたはグループの詳細なロールを管理する方法の例については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

ペルソナロールをアサインするには、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。

脆弱性対応 アサインルールの概要

脆弱性一致アイテム (VIT) が修復のアサイン先グループに自動的にアサインされる基準を定義します。

デフォルトのアサインルール **[CI** サポートグループにアサイン] は、脆弱性一致アイテムを **CI** サポートグループにアサインするベースシステムに含まれています。[CI サポートグループにアサイン] ルールでは、VIT に関連付けられている構成アイテム (CI) に設定されているサポートグループに VIT をアサインします。

注:
アサインルールは、手動作成されたアサインは再評価しません。

アサインタイプ ([手動] または [ルール]) は、VIT フォームやリストビューから設定できます。当初ルールによりアサインされた VIT が後に手動で再アサインされた場合、元のルールが参照されます。

[アサインルール] と [アサインタイプ] 情報を使用して、アサインルールが意図した受信者に対して適切なマッチングを見つけられなかったケースを特定します。この情報を使用して、再アサインが最も多いルールを特定することもできます。

アサインルールによって設定されたアサイン先グループは、修復タスク (VUL) にオーナーをアサインするために [修復タスクルール] によって使用されます。

注:
Rapid7 InsightVM 資産タグをアサインルールの条件フィルターで使用できるようにするには、他の Rapid7 InsightVM 統合の前に Rapid7 InsightVM 資産リスト統合を実行する必要があります。

条件ビルダーに入力した検索テキストの大文字と小文字の区別は、このレコードまたはフォームではサポートされていません。

脆弱性一致アイテムの自動アサイン

[次を使用してアサイン] を使用して脆弱性一致アイテムをアサインするには、3 つの異なる方法があります。

- ユーザーグループ：このオプションを使用すると、既存の Now Platform® ユーザーグループを選択できます。
- ユーザーグループフィールド：このオプションを使用すると、cmdb_ci テーブルを使用して利用可能なアサイン先グループフィールドを選択できます。デフォルトでは、次の 3 つのグループフィールドが表示されます。
  - なし：この必須フィールドにデフォルト値がないことを示します
  - 構成アイテム：承認グループ
  - 構成アイテム：アサイン先グループ
  - 構成アイテム：サポートグループ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- スクリプト：このオプションを使用すると、スクリプトを使用して条件を定義できます。このオプションには、コーディングまたは高度な ServiceNow の専門知識が必要です。 スクリプトエディターを使用して複雑な条件を定義する方法について、詳細は KB 記事「KB0965240」を参照してください。

最優先のルール (特別な処理が必要なアイテムの場合、リスクが重大な場合、VIT を規制コンプライアンスによって処理する必要がある場合など) を最初に実行します。次に、一般的なルールを実行します。この場合、特別な処理は必要なく、誰が責任を負うべきかがわかっています。最後に、VIT をグループにアサインするデフォルトのルールを作成します。これにより、VIT が属するアサイン先グループが把握できるようになります。このグループは、決定を対象に別のルールを追加できます。このデフォルトルールは最後に実行されます。

アサインルールの評価プロセス

アサインルールは、新しい VIT がオープンになったとき (インポートされたとき、手動で作成されたとき、再度オープンになったときなど) に VIT を評価してアサインする際に使用されるものとなります。VIT やステータスの変更後にアサインルールを手動で再適用する場合を除き、VI は 1 回評価されます。

各 VIT (新規、更新、再オープン) に対して、次の処理が行われます。

- 脆弱性アサインルールごとに、VIT がアサインフィルター (最下位のアサインルールから) と比較されます。
- 条件に一致すると、VIT はアサイン先グループにアサインされます。ルックアップは停止します。
- 他のすべてのルールの中で条件が一致しない場合、デフォルトのルールが存在すれば、VIT はデフォルトのアサイン先グループにアサインされます。

  脆弱性一致アイテムがアサインされると、適切な修復タスクルールでは、脆弱性一致アイテムを修復タスクに配置するための基準の 1 つとしてアサインが使用されます。詳細については、「脆弱性対応修復タスクとタスクルールの概要」と「脆弱性対応 内のフィルタリング」を参照してください。

  注:
  デフォルトのルールは、実行順序の値が最も大きいルールです。すべての状況に対応可能な使用する最終ルールは active=true です。デフォルトのルールがない場合、修復タスクルールによってアサインされても VIT は未アサインのままになります。

アサインルールを再適用する

アサインルールを変更する場合は、[アサインルール] リストページの [変更を適用] ボタンを使用して、すべてのアクティブなオープン VI で変更されたルールを再実行します (手動でアサインされたルールを除く)。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

初めて [変更を適用] を使用する前に *Reapply all vulnerability assignment rules* のスケジュール済みジョブが実行されていない場合は、手動でアサインされた VI を除くすべてのオープン VIT に対して、すべてのアサインルールが実行されます。その後、[変更を適用] を使用すると、変更されたルールと依存ルールのみが再実行されます。あるルールを変更すると、変更されていない別のルールに VIT が一致することがあります。アサインルールを再適用しても、脆弱性一致アイテムは再グループ化されません。

スケジュール済みジョブ [*Reapply all vulnerability assignment rules*] は、デフォルトでは非アクティブです。このジョブをアクティブ化すると、手動でアサインされたものを除くすべてのオープン VIT に対して、すべてのルールが適用されます。[日次]、[週次]、[月次]、[定期的]、**[1** 回]、または [オンデマンド] で実行できます。環境内のアクティブな VI の数に応じて、最初の実行後に [実行] フィールドを適切に設定して、パフォーマンスに影響がないようにすることを忘れないでください。

アップグレードのお客様は、この機能が既存の VIT に与える影響に関する情報について、「脆弱性対応 リリースノート」を参照してください。

重要:
脆弱性アドミンおよびアナリストは、Vulnerability Manager ワークスペースで選択した脆弱性一致アイテムの最新のアサインを取得できます。この方法は、 クラシック UI ですべての脆弱性一致アイテムにアサインルールを実行する時間のかかるプロセスよりも効率的です。詳細については、「Vulnerability Manager ワークスペース でレコードの修復プロパティを再評価」を参照してください。

アサインルールのアサイン先グループが変更されると、システムプロパティ sn_vul.rerun_task_rules とビジネスルール [修復タスクへのリンク] を有効にすることで、脆弱性一致アイテムを自動的に再評価して再グループ化できます。

システムプロパティを有効にするには：

1. 次のように移動する。 **All** (すべて) > システムプロパティ > すべてのプロパティ.
2. sn_vul.rerun_task_rules システムプロパティを開きます。
3. [値] フィールドで、値を true に設定します。

システムプロパティが true に設定されている場合、アサインルールが再適用されると、条件が一致しなくなった修復タスクから脆弱性一致アイテムのリンクが解除されます。

注:
デフォルトでは、システムプロパティ sn_vul.rerun_task_rules は false に設定されています。

脆弱性一致アイテムの再グループ化を自動化するには、ビジネスルール [修復タスクへのリンク] をアクティブ化する必要があります。

ビジネスルールを有効にするには：

1. 次のように移動する。 **All** (すべて) > システム定義 > ビジネスルール.
2. [修復タスクへのリンク] ビジネスルールを開きます。
3. ビジネスルールをアクティブ化するには、[アクティブ] チェックボックスをオンにします。

ビジネスルールを有効にすると、脆弱性一致アイテムを関連するグループに移動するか、既存のグループでグループ化できない場合はグループを作成することにより、脆弱性一致アイテムが再グループ化されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

- グループが削除されることなく、脆弱性一致アイテムはグループから削除されます。
- 修復タスクルールまたは修復作業を使用して作成されたアイテムのみが削除されます。
- 再グループ化は、アサイングループが手動で変更された場合ではなく、アサインルールの一部として変更された場合にのみ自動的に行われます。

ワークスペースでの再グループ化は、修復作業から作成された修復タスクに対して実行されます。

脆弱性対応修復タスクとタスクルールの概要

修復タスク (VUL) を設定すると、アナリストと修復スペシャリストが脆弱性一致アイテム (VI) を整理して一括で分析できるようになります。修復タスクを形成する基準を設定すると、脆弱性一致アイテムを手動で修復タスクにアサインする必要がなくなります。修復タスクを使用すると、進捗状況を監視し、修復プロセスをより効率的に進めることができます。

脆弱性一致アイテムと修復タスクの保留数の追跡

脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、または修復タスクが保留された回数を追跡します。スケジュール済みジョブ [保留数の設定 **(set deferral counts)]** は毎日実行され、[保留数] 列で複数回保留されたレコード数が提示されます。レコードは、VR、AVR、および CVR の複数の保留モジュールに表示されます。

脆弱性一致アイテムの自動リフレッシュ

注:
脆弱性一致アイテムのリフレッシュの自動化は、条件フィルターまたはフィルターグループを使用して作成された修復タスクにのみ適用されます。自動化は、手動で追加された VI、または修復タスクルールを使用してグループ化された VI には適用されません。

[関連する脆弱性一致アイテムを自動更新] チェックボックスをオンにすると、修復タスクのフィルター基準に一致する新しい VI がタスクに自動的に追加されます。フィルター基準に一致しなくなった、修復タスク内の脆弱性一致アイテムはタスクから自動的に削除されます。

デフォルトでは、修復タスクが [オープン] ステータスから移行すると、このチェックボックスはオフになります。ステータスに関係なく継続的に脆弱性一致アイテムを修復タスクに追加する場合は、*`Set auto refresh vulnerable items`* ビジネスルールを無効にします。

[調査中] ステータスになると、チェックボックスを手動で再度オンにできます。修復タスクが [実装待ち] ステータスに移行しても、[関連する脆弱性一致アイテムを自動更新] は無効になりません。[実装待ち] ステータスになると、既存のタスクに新しい脆弱性一致アイテムを追加することも、既存の脆弱性一致アイテムを削除することもできません。

注:
修復タスクを手動で作成し、条件フィルターまたはフィルターグループを使用して VI を追加すると、このチェックボックスはオフになります。このボックスをオンにするかどうかは自由に選択できます。

脆弱性一致アイテムの手動リフレッシュ

フィルターグループまたは条件フィルターを使用して手動で作成された修復タスクの場合、[修復タスク] ページで関連する脆弱性一致アイテムの [リフレッシュ] 関連リンクをクリックすると、フィルター基準に一致する脆弱性一致アイテムが追加されます。基準に一致しなくなったアイテムは削除されます。このアクションにより、[関連する脆弱性一致アイテムを自動更新] チェックボックスがオンであるかどうかにかかわらず、脆弱性一致アイテムのリストを即時更新できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

条件またはフィルターグループフィルタータイプを使用して手動で作成された修復タスクは、1 時間に 1 回リフレッシュされます。

修復タスクルールについて

修復タスクルールを使用すると、脆弱性一致アイテムを自動的にグループ化してアサインする方法を定義できます。デフォルトのルール「脆弱性」は、脆弱性に基づいて脆弱性一致アイテムを収集するベースシステムに含まれています。ただし、VI からアクセス可能な列では、その他の値セットでグループ化できます。こうした値には、構成アイテム (CI) のサポートグループ、脆弱性の重大度などが含まれる場合があります。

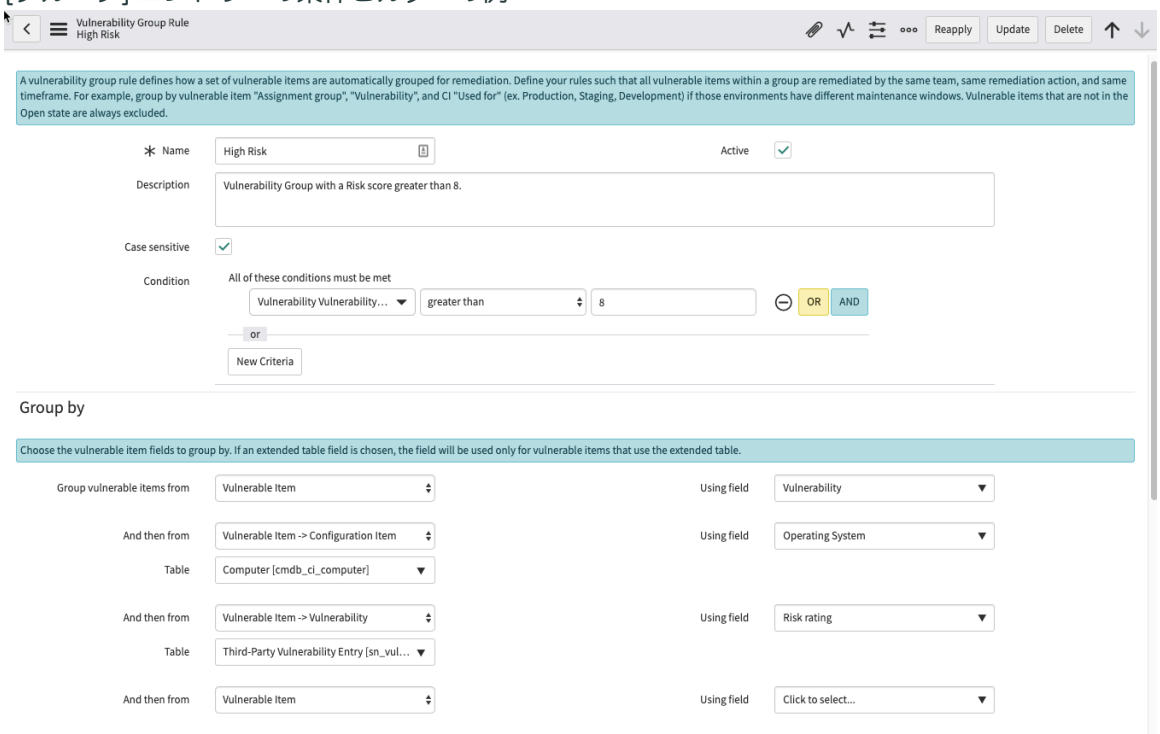
条件はいくつでも作成できます。[グループ] の選択を設定すると、別の行が表示されます。最大 6 つの [グループ分け基準] の選択を設定できます。グループのアサインを自動化することもできます。詳細については、「脆弱性対応 修復タスクルールの作成または編集」と「脆弱性対応 内のフィルタリング」を参照してください。

注:
Rapid7 InsightVM 資産タグを修復タスクルールの条件フィルターで使用できるようにするには、他の Rapid7 InsightVM 統合の前に Rapid7 InsightVM 資産リスト統合を実行する必要があります。

たとえば、脆弱な CI のコストセンター別、または脆弱性の攻撃ベクトル別に、脆弱性一致アイテムをグループ化できます。低重大度の脆弱性または低リスクの CI に対して、1 つのタスクルールを設定できます。重要なサーバーに対して、またエクスプロイトを伴う脆弱性 (会社をより多くのリスクにさらす脆弱性一致アイテム) に対しては、別のタスクルールを設定できます。

会社がより多くのリスクにさらされる脆弱性一致アイテムには、別のルールセットを使用できます。修復タスク名が修復タスクルールの [グループ分け基準] の値に追加され、新しいレコードの簡単な説明が作成されます。使用可能なフィールドの詳細については、「脆弱性対応 での修復タスクの手動作成」を参照してください。

[グループ] エントリーの条件ビルダーの例



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

新しい脆弱性一致アイテムが作成、インポート、またはクローズ後に再オープンされると、それに対して脆弱性ルールが評価されます。VI は 1 回のみ自動的に評価されます。ただし、クローズ後に再オープンする場合や、ルールを手動で再適用する場合は除きます。

新規の VI または再オープンされた VI ごとに、以下の処理が行われます。

- 修復タスクルールごとに、VI が修復タスクルールフィルターと比較されます。
- 修復タスクルール条件が一致するルールごとに、VI の [グループ] の選択に基づいてデータがルールによってプルされます。グループ名とフィールドがビルドされます。この場合は、高リスク：QID-32342：*QID-3242* のサマリー (名前：脆弱性 ID：脆弱性サマリー) となります。

  注:
  簡単な説明フィールドは 160 文字に制限されています。これより長い脆弱性サマリーは切り捨てられます。

  このルールでは、VI と同じアサイン先グループにアサインされている、一致するオープン修復タスクがあるかどうかを確認します。
  - タスクが見つかった場合、VI は [オープン] ステータスの既存のタスクに追加されます。
  - [オープン] ステータスのタスクが見つからない場合は、高リスク：**QID-32342** タスクが作成され、VI と同じアサイン先グループにアサインされて、VI が修復タスクに配置されます。

複数の修復タスクルールを定義すると、さまざまな種類の脆弱性をグループ化できます。各脆弱性は、修復タスクに配置される前に修復タスクルールの条件と比較されるため、ルールが多すぎるとパフォーマンスに影響を与えるおそれがあります。

デフォルトでは、修復タスクルールで、アイテムのグループ化の際に脆弱性一致アイテムのアサインルールによって設定されたアサイン先グループが使用され、脆弱性一致アイテムに一致するように修復タスクがアサインされます。

デフォルトのタスクルールの一部として、こうした修復タスクのアサインは [アサインルール] モジュールのルールによって制御されます。アサインルールについては、「脆弱性対応 アサインルールの概要」を参照してください。

タスクルールが削除されると、フォームまたはリストビューから、そのルールによって作成されたすべてのオープンタスクを削除できます。[オープン] ステータスでないタスクは除外されます。

修復タスクルールの再適用

修復タスクルールを変更する場合は、修復タスクルールページの [再適用] ボタンを使用して、そのルールによって作成されたすべてのアクティブなオープン修復タスクに対し、変更されたルールを再実行します。変更されたルールに基づいて、修復タスクが自動的に削除され、再作成されます。

重要:
脆弱性アドミンおよびアナリストは、Vulnerability Manager ワークスペースで選択した脆弱性一致アイテムの修復タスクルールを評価することができます。この方法は、時間のかかるクラシック UI で修復タスクルールを再適用するよりも効率的です。詳細については、「Vulnerability Manager ワークスペース でレコードの修復プロパティを再評価」を参照してください。

脆弱性対応 の修復ターゲットルール

修復ターゲットルールは、脆弱性一致アイテム (VI) を修復するための予定期間を定義します。これは SLA が脆弱性そのものの修復期間を提供するのと同様です。たとえば、資産に PCI データ (クレジットカードデータ) が含まれている場合、そのアイテムの脆弱性は PCI DSS に従って 30 日以内に修正する必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性マネージャーは、次の内容を定義して修復ターゲットルールを作成できます。

- 修復ターゲット
- リマインダーターゲット
- リマインダーおよび通知の受信者 - 脆弱性一致アイテム (VI) がリマインダーまたは修復ターゲット日を過ぎても修復されていない場合に通知する必要があるユーザー。

脆弱性アナリストと脆弱性マネージャーは、脆弱性一致アイテムが [保留]、[解決済み]、または [クローズ済み] ステータスでない限り、脆弱性一致アイテムフォームおよびリストビューで修復ターゲット日を確認できます。修復ターゲットルールはインポート時に実行され、VI が再オープンされると再実行されます。

修復ターゲット日は、VI リストビューでは次のように 色分けされた点で表示されます。

- 通知日に達していない脆弱性一致アイテムは緑色で示されます。
- 修復ターゲット日が近づいている脆弱性一致アイテムはオレンジ色で示されます。
- 修復ターゲット日を過ぎた脆弱性一致アイテムは赤色で示されます。

1 つ以上の VI について、修復ターゲット日に近づいているか、修復ターゲット日を過ぎていると、修復ターゲットルールごとに概要メールが送信されます。

修復ターゲットルールは非アクティブ化または削除が可能

ルールが非アクティブになると、ルールが適用された VI の現在の修復ターゲット日がクリアされます。VI がアクティブなルールを満たしている場合はそのルールが適用され、そうでない場合は VI にはルールもターゲット日もなく、ステータスは [ターゲットなし] になります。

ルールが削除されると、クローズ済み、保留、解決済みの VI の修復ターゲットの日付と関連フィールドは保持されます。クローズされていない VI の修復ターゲットの日付と関連フィールドはクリアされ、依存ルールが再適用されます。

修復ターゲットルールのシナリオ

複数の修復ターゲットルールが同じ脆弱性一致アイテムに適用される場合は、最も制限の厳しいルールが適用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
修復ターゲットは、[最終オープン日] の値に日数 (24 時間単位で測定) を加えて算出されます。

V17.1 以降では、修復ターゲットは [ターゲット開始 (日付)] から算出されます。デフォルト値は [最終オープン日] のままです。

たとえば、脆弱性一致アイテムが 2 つの修復ターゲットルールの条件を満たす場合：

シナリオ：脆弱性一致アイテムの最終オープン日時は 2018 年 3 月 1 日 10:00:00。

- 修復ターゲットルール 1：最終オープン日は 2018 年 3 月 7 日、修復ターゲットは最終オープンから 15 日、算出された修復ターゲット日時は 2018 年 3 月 16 日 10:00:00。
- 修復ターゲットルール 2：最終オープン日は 2018 年 3 月 10 日、修復ターゲットは最終オープンから 10 日、算出された修復ターゲット日時は 2018 年 3 月 11 日 10:00:00。

このシナリオでは、より厳しい日付制限の修復ターゲットルール 2 (10 日：脆弱性一致アイテムが 15 日より先に特定されるため) が脆弱性一致アイテムに適用されます。

注:
修復ターゲットルールが定義されると、修復ターゲット日が *Evaluate remediation targets* スケジュール済みジョブによって算出されます。

修復ターゲットのスケジュール済みジョブの評価について

Evaluate remediation targets は、毎日 4:00:00 に 1 回実行されます。

修復ターゲット日が最も早いルールから順に、有効なすべての脆弱性ルールを反復処理します。次の条件に当てはまるすべての脆弱性一致アイテムを調べます。

- [クローズ済み]、[保留]、または [解決済み] のいずれのステータスでもない。
- 修復ターゲット日がない。
- 修復ターゲットルールの日付より後の修復ターゲット日がある。

Evaluate remediation targets は、修復ターゲット日が存在しない場合は追加し、ルールの結果となる日付がレコード内の日付よりも前になる場合は、既存のターゲット日を更新します。最後に、脆弱性一致アイテムフォームの [修復ターゲット] フィールドと [修復ステータス] フィールドが更新されます。

Evaluate remediation targets が実行されると、利用可能な通知が送信されます。

Evaluate remediation targets は VI の修復フィールドをクリアし、通知の送信を停止します。

*sn_sec_cmn.evaluate_targetmissed_records*プロパティを有効にすると、*Remediation Target Rules*スケジュール済みジョブが欠落した VI を評価しなくなります。このプロパティはデフォルトで有効になっています。

修復ターゲットルールを再適用する

修復ターゲットルールを変更する場合、[修復ターゲットルール] リストページの [変更を適用] ボタンを使用して、[クローズ済み], [保留] または [解決済み] ステータスの VI を除くすべての有効なオープン VI に対して、変更されたすべてのルールを再実行します。VI の数によっては、時間がかかる場合があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

スケジュール済みジョブ *Evaluate remediation targets* が実行されている場合、再適用プロセスを開始することはできません。ただし、再適用プロセスが既に実行されていて、スケジュール済みジョブがトリガーされると、それらは並行して実行されます。

脆弱性対応 および アプリケーション脆弱性対応 の再適用プロセスは独立しており、並行して実行できます。

重要:
脆弱性アドミンおよびアナリストは、Vulnerability Manager ワークスペースで選択した脆弱性一致アイテムの最新の修復ターゲット日を取得できます。この方法は、 クラシック UI ですべての脆弱性一致アイテムに対して修復ターゲットルールを実行する時間のかかるプロセスよりも効率的です。詳細については、「Vulnerability Manager ワークスペース でレコードの修復プロパティを再評価」を参照してください。

関連情報

- 脆弱性対応 修復ターゲットルールの作成または編集
- 脆弱性対応 脆弱性一致アイテムの修復ターゲットステータスの表示
- 修復ターゲット通知の作成または編集

脆弱性の分類グループとルール

分類グループによって、グループで定義された分類ルールに基づいてテーブルの値が自動的に分類されます。各ルールの条件が順番に評価され、最初に一致したルールが使用されます。

脆弱性対応ベースシステムには、検出されたアイテムと脆弱性をそれぞれ分類する次の 2 つの分類グループが含まれています。

- 検出されたアイテムの分類
- 脆弱性エントリーの分類

脆弱性と検出されたアイテムがインポートされるたびに、それぞれのグループの脆弱性分類ルールが実行されます。ルールに設定された条件に基づいて、レコードは関連する分類グループに分類されます。こうしたルールを作成、編集、削除したり、既存の脆弱性に再適用したりできます。

注:

- 選択したテーブルに対して有効な分類グループは 1 つだけです。
- 作成したグループは削除できません。

詳細については、「分類ルールの作成と編集」、「既存の脆弱性へのルールの適用」、「分類ルールの非アクティブ化または削除」を参照してください。

脆弱性対応 の機械学習ソリューション

脆弱性アサインの推奨 は ServiceNow® 予測インテリジェンス と機械学習を使用して、脆弱性一致アイテム (VI) および修復タスク (VUL または RT) のアサイン先グループを推奨します。アサインが解除されたり、誤ってアサインされた脆弱性の結果について、所有者を特定する時間を短縮できます。また、推奨されたアサイン先グループが脆弱性の解決に適しているかどうかを評価する、システム生成による信頼スコアを表示することもできます。

予測インテリジェンス 機能は、脆弱性対応 において、既存のデータに基づいてアサイン先グループを予測できるソリューション定義モデルを作成してトレーニングすることで、より良い作業エクスペリエンスを提供するために使用されます。

詳細については、「予測インテリジェンス」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性アサインの推奨

脆弱性アサインの推奨 アプリケーション (com.snc.vulnerability.recom) では、ServiceNow 予測インテリジェンス を使用して、脆弱性対応 で推奨事項をアサインできます。このプラグインには次が必要です。

- 脆弱性対応 (com.snc.vulnerability)
- 予測インテリジェンス (com.glide.platform_ml)

詳細については、「予測インテリジェンス」を参照してください。

信頼スコア

脆弱性アサインの推奨 アプリケーションを使用して、選択した RT または VI について推奨されるアサイン先グループの信頼性レベルを報告します。信頼スコアは、推奨されるアサイン先グループが脆弱性の解決に適しているとシステムが信頼しているかどうかを評価するものです。最大 10 件の推奨アサイン先グループが表示されます。これらの推奨グループは、アサインが成功する可能性が最も高いことに基づいています。リストの最初の推奨グループは、正しいアサイン先グループであることの信頼性が最も高いことを意味します。

たとえば、0 ～ 100 のスケールで、各アサイン先グループの信頼スコアは、VI または RT がその特定のグループに属する可能性を示します。

関連情報

- 予測インテリジェンス
- 分類ソリューションの作成とトレーニング
- 類似性ソリューションの作成とトレーニング
- クラスタリングソリューションを作成してトレーニングする
- ML ソリューションの詳細設定

脆弱性対応 サードパーティ脆弱性統合の構成アイテムを識別するための **CI** ルックアップルール

サードパーティ統合からデータをインポートすると、脆弱性対応 は自動的にホストデータを使用して、構成管理データベース (CMDB) 内で一致するものを検索します。その際に **CI** ルックアップルールを使用します。これらのルールにより、構成アイテム (CI) が特定されて脆弱性一致アイテムレコードに追加されるため、修復に役立てることができます。

バージョン 19.0 以降では、次に移動します: セキュリティオペレーション > **CMDB** > ルックアップルール インスタンス内のリストを見つけます。

資産がインポートされると、最初にサードパーティ ID を使用して [検出されたアイテム] リストでルックアップが実行され、構成アイテム (CI) に一致するものが以前のインポートから検索されます。一致するホスト ID が見つかった場合は、その ID が脆弱性一致アイテムレコードの [構成アイテム] フィールドとして使用されます。

[検出されたアイテム] リストを使用して、インポートした資産が CI にどのようにマッピングされているかを確認できます。一致するものが見つからない場合、または [ホスト ID] フィールドが空の場合、ルールは他のホスト情報を使用して CI を正しく識別しようとします。それでも一致が見つからない場合は、プレースホルダー CI が作成され、[一致しない **CI**] としてマークされます。これらの CI の処理方法の詳細については、「一致しない CI」を参照してください。

CI ルックアップルールはドメインセパレーションすることができ、ソース固有です。各ソースには複数の展開を含めることができます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:
CI ルックアップルールは、脆弱性ソース統合のすべての展開で共有されます。ルールが削除または変更された場合、その削除または変更は脆弱性統合のすべての展開に影響します。

一致を試みる場合、最初のステップは、source、source_instance、およびベンダー ID 間で完全に一致するベンダー ID のルックアップです。次に、ルックアップルールが順番に実行され、ルールが一致する CI を 1 つ返すと停止します。複数の CI を返すようにルールが作成されている場合は、最初に一致したもののみが使用されます。

注:
低レベルのネットワーク要素での一致を避けるため、一致した CI が dscy_switchport、cmdb_ci_network_adapter、cmdb_ci_nic、または cmdb_ci_ip_address のいずれかである場合は、親 CI が返されます。

CI クラスを除外するためのシステムプロパティが利用可能です。このプロパティはアップグレードでは使用できません。アップグレード情報とプロパティの設定手順については、「CI クラスの無視」を参照してください。

一致する問題を見つけやすくするために、一致が見つかったときに、その問題を見つけるために使用された CI ルックアップルールが **[CI** 一致ルール] フィールドの検出されたアイテムレコードに追加されます。ルックアップルールでは、[順番 **(Order)]** 値が最も小さいものから評価されます。

CI ルックアップルールには、対応する統合プラグインが付属しています。

CI ルックアップルール Qualys 例は次のとおりです。

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

CI ルックアップルール Rapid7 例は次のとおりです。

- MacAddress
- FQDN
- HostName
- IP

CI ルックアップルールには Tenable.io 次のようなものがあります。

- FQDN
- NETBIOS
- ホスト名
- MacAddress
- DNS

注:
Tenable.io CI ルックアップルールは、検出されたアイテムの通常の FDQN、IPV4、および MacAddress 値よりも、空でないネットワークインターフェイス値 (FDQN、IPV4、および MacAddress) を優先して入力します。これらのネットワークインターフェイスの値が空の場合、通常の FDQN、IPV4、および MacAddress の値が検出されたアイテムに設定されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CI ルックアップルール Tenable.sc 例は次のとおりです。

- MacAddress
- FQDN
- NETBIOS

注:
ルールは、一度削除すると元に戻せません。新しいルールを作成する場合は、既存のルールを削除せずに非アクティブ化します。

脆弱性データのインポートはインスタンスに負荷をかける可能性があり、慎重にルールをビルドしないと、リソースのパフォーマンス問題が発生する可能性があります。 CMDB 内で反復して照合を実行するために使用されるロジックでは、処理時間が長くなる可能性があります。リソースの潜在的なデグレードやパフォーマンスの複雑化を回避するために、カスタム作成された CI ルックアップルールまたは事前定義された **CI** ルックアップルールの変更をテストします。孤立レコードの重複防止、データの削除、およびデータのクリーンアップの詳細については、「脆弱性対応 CI ルックアップルールの実行後にレコードが重複または孤立しないようにするための手順」を参照してください。

注:
CI の照合の詳細については、「KB0998706」を参照してください。

更新された **CI** ルックアップルールの再適用

CI ルックアップルールを変更する場合は、[CI ルックアップルール] リストページの [変更を適用] をクリックして、検出されたアイテムに対して次のすべてのルールを再実行します。

- 更新されたルールに一致した
- どのルールにも一致しない

ルックアップルールを再適用した後に構成アイテム (CI) が変更された場合、検出されたアイテムは新しい CI で更新されます。影響を受けた検出と脆弱性一致アイテムも更新されます。詳細については、「選択した検出されたアイテムへの CI ルックアップルールの再適用」を参照してください。

未分類のハードウェア

CI ルックアップルールによって 構成管理データベース (CMDB) で一致する資産が見つからない場合、その資産は未分類のハードウェアと呼ばれます。

データが ServiceNow のビルド済み統合からインポートされると、脆弱性対応 は自動的にホストデータを使用して CMDB で一致するものを検索します。CI ルックアップルールは、構成アイテム (CI) を識別し、それらを脆弱性一致アイテムレコードに追加して修復に役立てるために使用されます。資産が CMDB で見つからない場合、識別および調整エンジン (IRE) は、ハードウェアクラスとそのすべての子に定義された独自の識別ルールを実行し、未分類のハードウェアクラスの下に CI を作成します。ディスカバリー でこの資産が見つかると、既存の未分類のハードウェアが再分類されるのではなく、CI が作成されます。これは、識別ルールがハードウェア CI の名前に依存しているためです。

識別および調整エンジン (IRE) がアクティブ化されている場合、検出されたアイテムからの再分類オプションはサポートされません。

次に、それぞれ 脆弱性対応 および ディスカバリー を介して未分類のハードウェアで CI を作成するための IRE ペイロードの抽出を示しています。

```
"className": "cmdb_ci_unclassed_hardware",

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

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
    "fqdn": "asset01.company.com",
    "ip_address": "133.10.3.123"
  }

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

```
"className": "cmdb_ci_cmdb_ci_win_server"

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

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

この場合、既存の未分類のハードウェア CI は Windows サーバーに再分類されず、代わりに新しい CI が Windows サーバーの下に作成されます。その理由は、識別ルールがハードウェア CI の名前に依存しているためです。ペイロードに注目すると、脆弱性対応 からのペイロードにある名前は FQDN/NETBIOS のいずれかと同じですが、ディスカバリー からのペイロードのホスト名にすぎません。

関連情報

未分類のハードウェアの再分類

一致しない **CI**

構成アイテム (CI) は、インポート時に 構成管理データベース (CMDB) にある CI と自動的に照合されます。デフォルトでは、[セキュリティオペレーション > **CMDB** > 検出済みアイテム モジュールは、一致のない構成アイテムをリストします。

一致しない CI が CMDB 内の既存のクラスに属すると思われる場合は、CI ルックアップルールを確認してください。それ以外の場合は、構成アイテムの再分類を検討してください。

注:
このリストのデフォルトのフィルターは [不一致] に設定されています。フィルターを削除すると、インポートから検出されたすべてのアイテムを表示できます。

識別および調整エンジン (IRE) がアクティブ化されている場合、検出されたアイテムからの再分類オプションはサポートされません。

関連情報

一致しない構成アイテムの表示と再分類

一致しない検出されたアイテムを調整

脆弱性対応 CI ルックアップルールの実行後にレコードが重複または孤立しないようにするための手順

既存の構成アイテムの重複排除

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

識別および調整エンジンを使用して 脆弱性対応 の **CI** を作成する

識別および調整エンジン (IRE) API を使用して、構成管理データベース (CMDB) に構成アイテム (CI) を作成できます。IRE API を使用して CI を作成すると、CI が重複して作成されることを防ぎ、信頼できるデータソースにのみ CMDB への書き込みを許可することで、CI 属性を調整できます。

CI クラス (テーブル) は、インスタンスデータベース内の元のテーブル名です。CMDB には、CI に関するデータを格納する基本システムのクラスが含まれています。

CI の作成に IRE を使用する

脆弱性対応 v12.2 より前では、一致する CI が [検出されたアイテム] リストまたは CMDB で見つからない場合、CI は [一致しない CI] クラス ([sn_sec_cmn_unmatched_ci]) で作成されます。詳細については、「一致しない CI」を参照してください。

脆弱性対応 v24.0.6 以降では、IRE で CI の作成を妨げる例外が発生した場合、これらの例外の詳細が [追加情報] フィールドに記録されます。このフィールドの詳細を調べることで、根本原因を特定し、CI を正常に作成するために必要な修正を実装できます。

脆弱性対応 v12.2 から v18.0 以降では、CI ルックアップルールが適用されたときに一致するものが見つからない場合、資産情報が IRE に送信され、未分類のハードウェアクラスおよび不完全な *IP* 識別デバイスクラスのいずれかで CI が作成されます。v18.0 以降の脆弱性対応では、新しいクラスである [クラウドリソース] も含まれています。一致しないクラウドリソースの分類を優先 CI クラスに構成する方法の詳細については、「一致しないクラウド資産の CI クラスの更新」を参照してください。

CMDB CI クラス

> **注:**
> 新しいクラスを使用するには、CMDB CI Class Models プラグインをアクティブ化します。それ以外の場合は、CI が [一致しない CI] クラスに作成されます。

サードパーティのスキャナーからインポートしたホストが [検出されたアイテム] リストまたは CMDB で見つからない場合、次の新しい CMDB CI クラスのいずれかで作成されます。

CMDB CI クラス

CMDB **CI** クラス	説明
不完全な IP 識別デバイス (*cmdb_ci_incomplete_ip*)	スキャナーから受信したホスト情報で IP アドレスのみが使用可能な場合は、このテーブルに CI が作成されます。
未分類のハードウェア (*cmdb_ci_unclassed_hardware*)	スキャナーから受信したホスト情報で以下の情報が使用可能な場合は、このテーブルに CI が作成されます。 • ホスト名 • IP アドレス • DNS • NETBIOS • MAC アドレス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CMDB CI クラス (続く)

CMDB **CI** クラス	説明
	注: MAC アドレスが利用可能な場合、ネットワークアダプタエントリーが作成され、未分類のハードウェア CI に関連付けられます。IP アドレスと MAC アドレスの両方が利用可能な場合、IP アドレス CI が作成され、未分類のハードウェア CI に関連付けられます。
クラウドリソース (*cmdb_ci_cmp_resource*)	スキャナーから受信したホスト情報で *Cloud Resource ID* が使用可能な場合は、このテーブルに CI が作成されます。 注: スキャナー統合の資産タイプが [ハイブリッド] で、*sn_sec_cmn.unmatched_cloud_resource_enabled* システムプロパティが false の場合、CI は [未分類のハードウェア *(Unclassed Hardware)*] クラスに作成されますが、[クラウドリソース] クラスには作成されません。

識別および調整エンジン (IRE) がアクティブ化されている場合、検出されたアイテムからの再分類オプションはサポートされません。

次のいずれかが発生した場合、システムは自動的に [一致しない CI] クラスを使用します。

- CMDB CI Class プラグインがアクティブ化されていません。
- CI の作成時に IRE が例外を発生させます。

詳細については、「一致しない CI」を参照してください。

関連情報

CMDB CI クラスモデルストアアプリ

識別および調整エンジン (IRE)

一致しないクラウド資産の **CI** クラスの更新

脆弱性対応 v20.0 以降では、*sn_sec_cmn.unmatched_cloud_resource_enabled* システムプロパティを使用して、Qualys、Rapid7、および Tenable スキャナーの一致しないクラウド資産を [未分類のハードウェア *(Unclassed Hardware)*] に分類できます。

デフォルト値が false であるこのシステムプロパティは、ベースシステムに付属しています。一致しないクラウド資産を、インフラストラクチャとクラウド資産の両方を取り込む統合のために、[未分類のハードウェア *(Unclassed Hardware)*] (*cmdb_ci_unclassed_hardware*) または [クラウドリソース] (*cmdb_ci_cmp_resource*) クラスに分類します。

脆弱性対応 v20.0 以降、インフラストラクチャとクラウド資産の両方をサポートする統合を識別するために、サードパーティ統合 (sn_sec_int_integration) テーブルに [資産タイプ] 列が追加されています。[資産タイプ] 列には、インフラストラクチャ資産とクラウド資産の両方を取り込むスキャナー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

の値として [ハイブリッド] があります。たとえば、Qualys、Rapid7、および Tenable 統合の [資産タイプ] 列の値が [ハイブリッド] になります。

- 脆弱性対応 v20.0 以降の新規インストールの場合、一致しないすべてのクラウド資産は次のように分類されます。
  - デフォルトでは [未分類のハードウェア *(Unclassed Hardware)*] クラス。
  - *sn_sec_cmn.unmatched_cloud_resource_enabled* システムプロパティを true に変更した場合は [クラウドリソース] クラス。
- 脆弱性対応 v20.0 にアップグレードする場合：
  - [クラウドリソース] クラスに資産がある場合、*sn_sec_cmn.unmatched_cloud_resource_enabled* システムプロパティが true に設定され、一致しないクラウド資産が引き続き [クラウドリソース] (*cmdb_ci_cmp_resource*) クラスに追加されます。
  - そうでない場合は、*sn_sec_cmn.unmatched_cloud_resource_enabled* システムプロパティが false に設定され、一致しないクラウド資産は [未分類のハードウェア *(Unclassed Hardware)*] クラスに分類されます。

注:
sn_sec_cmn.unmatched_cloud_resource_enabled システムプロパティの値を変更した場合は、以前にターゲットにした CI クラスの一致しない構成アイテムを必ず削除し、ルックアップルールを再適用します。既存の CI を削除し、新しい CI が正しいクラスに作成されるように CI ルックアップルールを再適用する方法の詳細については、「KB1533376」を参照してください。

検出されたアイテム

資産は、**[CI** ルックアップルール] を使用してインポートされると、構成管理データベース (CMDB) で自動的に構成アイテム (CI) と照合されます。検出されたアイテムにより、資産の識別が CMDB の CI にどのようにマッピングされているかを把握できます。

検出されたアイテムは、[一致 **(Matched)]**、[不一致]、または [再分類] と見なされます。識別された CI は [一致 **(Matched)]** ステータス です。

潜在的な一致の問題を見つけやすくするために、CI に一致した CI ルックアップルールが **[CI** 一致ルール] フィールドに表示されます。

デフォルトでは、[セキュリティオペレーション > **CMDB** > 検出済みアイテム モジュールは一致しない構成アイテムをリストします。フィルターを削除すると、インポートから検出されたすべてのアイテムを表示できます。

[検出されたアイテム] の各フィールドの説明については、「[検出されたアイテム] フォームフィールド」を参照してください。一致しないディスカバリーアイテムの調整、および選択したディスカバリーアイテムへの CI ルックアップルールの再適用の詳細については、「一致しない検出されたアイテムを調整」および「選択した検出されたアイテムへの CI ルックアップルールの再適用」をそれぞれ参照してください。

検出されたアイテムの **CI** 変更

検出されたアイテム (DI) の構成アイテム (CI) が変更されると、影響を受ける検出と脆弱性一致アイテム (VI) が更新されます。リスクスコア、アサインルール、グループルール、修復ターゲットルールが再評価されます。

脆弱性対応 の v24.0.6 以降、[検出されたアイテム] テーブルで CI の更新を表示できます。以前の CI、更新された CI、変更を加えたユーザーなどの情報は、[監査履歴] 関連リストに文書化されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

同じ脆弱性と CI を持つ VI が存在する場合、検出は既存の VI で更新され、現在の VI はサブステート invalidCI としてクローズされます。作業メモは以下の理由で追加されます。

- ある VI から別の VI に検出が移行されたとき。
- 重複 VI がクローズされたとき。

既存の VI の CI を更新しない場合は、プロパティ sn_sec_cmn.update_on_ci_change を false に設定します。その後 CI が変更されると、新しい VI が作成され、既存の VI は invalidCI としてクローズされます。

プロパティ sn_sec_cmn.update_on_ci_change のデフォルト値は true です。

検出されたアイテムの再評価

検出されたアイテムで新しいデータを受信しても、検出されたアイテムはすぐには再評価されません。新しいデータを受信すると、*reevaluate_ci* オプションはデフォルトで *true* に設定されます。

スケジュール済みジョブ *Re-apply CI Lookup Rules on the Changed Discovered items* は、スキャナーによってソースデータが変更されている検出されたすべてのアイテムを評価します。検出されたアイテムを再処理し、ソースデータが変更された検出済みアイテムに関連する脆弱性一致アイテムを更新します。このスケジュール済みジョブの値は、デフォルトでは *On Demand* です。

注:
このスケジュール済みジョブを毎日実行することも選択できます。

脆弱性対応 修復タスクと脆弱性一致アイテム状況

脆弱性対応 アプリケーションでは、状況モデルを使用して、いつでも修復タスクのステータスを確認できます。各ステータスが互いにどのように関連し、影響を与えているかを知ることで、脆弱性一致アイテム (VI) をいつどのように修正すればよいかを判断できます。

修復タスクステータス

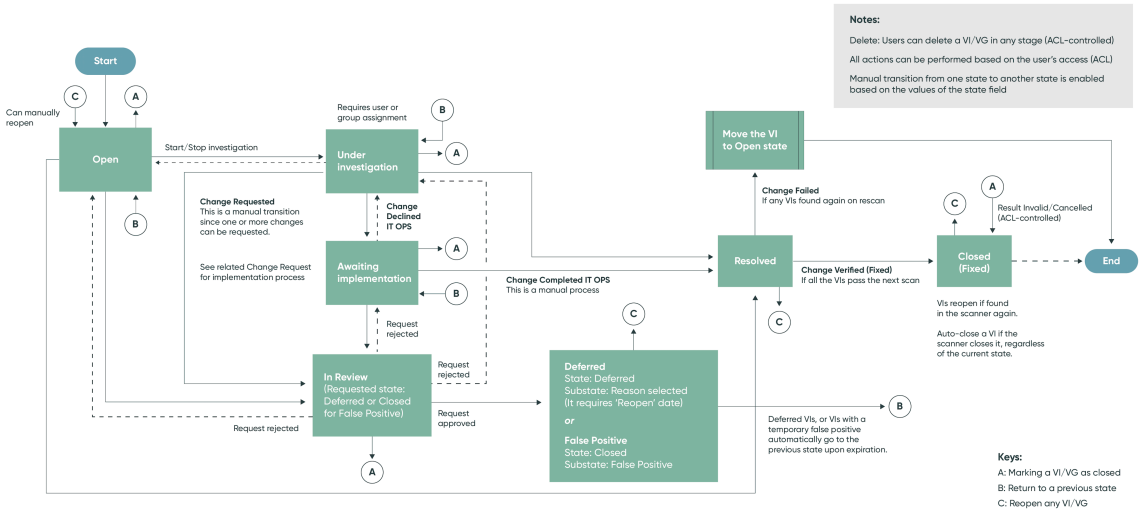
複雑なユースケースでは、脆弱性一致アイテムがその修復タスクとは異なるステータスになることがあります。状況の仕組みを理解すると、この動作を説明でき、修復タスクの作成や修復タスクルールの作成または編集に役立ちます。

注:
脆弱性対応 v23.0 以降、脆弱性一致アイテムのステータス承認ワークフローは廃止され、フローデザイナーの [脆弱性ステータス承認の変更] フローに置き換わりました。

次の図に示すように、修復タスクの想定される状況は数多くあります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応の状況フロー



注:
各タスクフォームには、ServiceNow タスクの標準である [フォロー] および [更新] ボタンが含まれています。

修復タスクのステータスと、それぞれのステータスで実行できるアクションの詳細については、「脆弱性対応 修復タスクステータス」を参照してください。

検出、修復タスク、および脆弱性一致アイテム状況の詳細については、「検出、修復タスク、および脆弱性一致アイテム状況」を参照してください。

修復タスクと VI ステータスの詳細については、「 修復タスクと脆弱性一致アイテム状況」を参照してください。

複数グループの VI に対する修復タスクステータスの詳細については、「複数グループでの脆弱性一致アイテム (VI) の修復タスクステータス」を参照してください。

脆弱性一致アイテムの経過時間の計算と表示

脆弱性一致アイテム (VI) の経過時間は、脆弱性対応 アプリケーションに詳細とともに表示されます。

脆弱性一致アイテム (VI) の経過時間は、[脆弱性一致アイテム] リストビューの [経過時間] 列、および VI (VIT) レコードの [経過時間] および [クローズ所要時間] フィールドに日/時間/分形式で表示されます。有効数字で表示される経過時間は、以下のアクティビティをより正確に実行するのに役立ちます。

- [ルールの自動削除] モジュールで、日/時間/分単位に特定の VI レコードをターゲットとして削除するようにルールを設定する。インスタンスに多数の VI レコードがある場合は特に、レコードをより正確に削除するとパフォーマンスが向上する可能性があります。
- 脆弱性対応 アプリケーションのパフォーマンスアナリティクスで、より具体的な詳細を含むレポートを表示する。
- 必要な VI のみを識別するフィルターを作成する。
- リストビューを整理して、必要な VI のみを表示する。
- より簡単にドット連結する。

スケジュール済みジョブにより経過時間が計算され、すべてのアクティブな VI が更新されました。多数の VI レコードを使用するインスタンスでは、このプロセスが遅くなり、パフォーマンスに悪影響を与える恐れがあります。VI の経過時間は、オンデマンドでより効率的に計算され、拡張され

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

た [経過時間] 列とともにより多い有効数字で表示されます。脆弱性対応 アプリケーションをインストールまたはアップグレードすると、拡張された [経過時間] 列が自動的に追加されます。

> **注:**
> アップグレードを実行し、VI の経過時間が [脆弱性一致アイテム] リストビューおよびアクティブな VI (VIT) レコードの [経過時間] および [クローズ所要時間] フィールドに日/時間/分 (9 日、18 時間、29 分) 形式で表示されない場合は、インスタンスでの [経過時間] 列が最新ではありません。アップグレード後にこの問題を解決する方法の詳細については、「KB0749231」を参照してください。

[経過時間] 列とフィールドは編集できません。sn_vul.vulnerability_read 権限を持つ脆弱性マネージャーまたは脆弱性アドミンペルソナ がこの値を表示できます。また、sn_vul.remediation_owner ロールを持つ IT 修復オーナーは、自身にアサインされたレコードでこの値を表示できます。

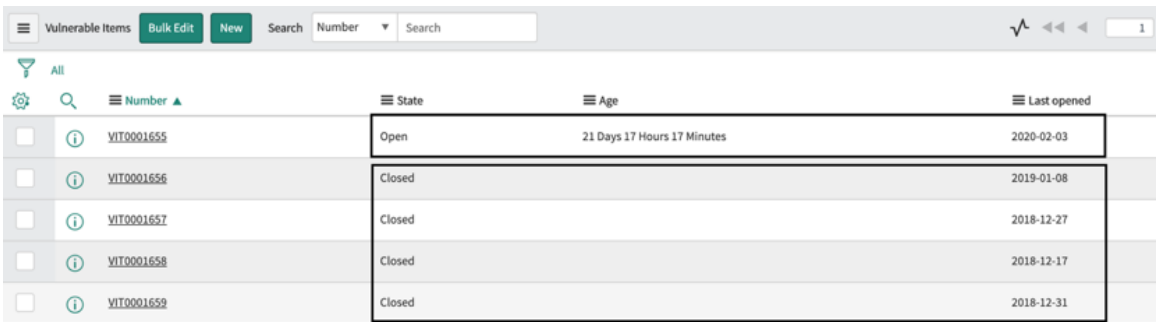
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

VI の経過時間は次の画像のように表示されます。

脆弱性一致アイテムリスト

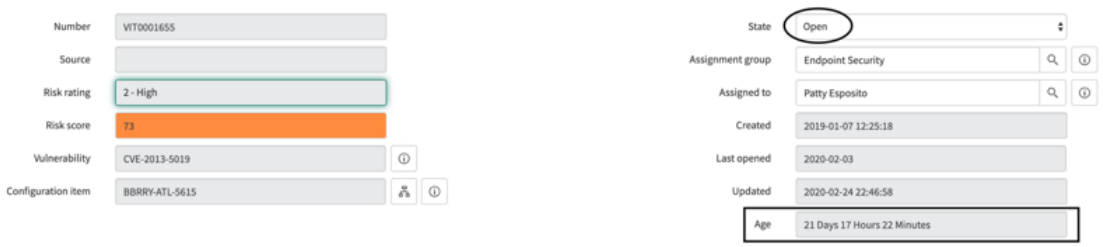
次の図に示すように、[脆弱性一致アイテム] リストビューでは、アクティブな VI についてのみ、[経過時間] 列に経過時間が日/時間/分 (21 日 17 時間 17 分) で表示されます。アクティブな VI は、[クローズ済み] 以外のステータスの VI です。この経過時間値は、VI がアクティブであった日数を表します。

[クローズ済み] ステータスの VI の経過時間は表示されません。以前に [クローズ済み] ステータスで再オープンされた VI の場合、経過時間値は VI が最後にオープンされてからアクティブであった日数を表します。



VI レコードの経過時間

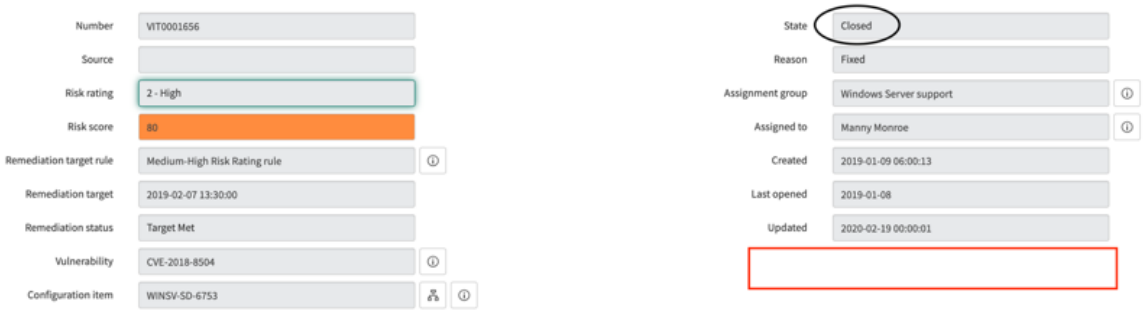
VI レコードでは、リストビューの [経過時間] 列の値が [経過時間] フィールドのアクティブな VI に対して表示されます。



[クローズ済み] ステータスの VI レコードでは [経過時間] 列の値は表示されません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

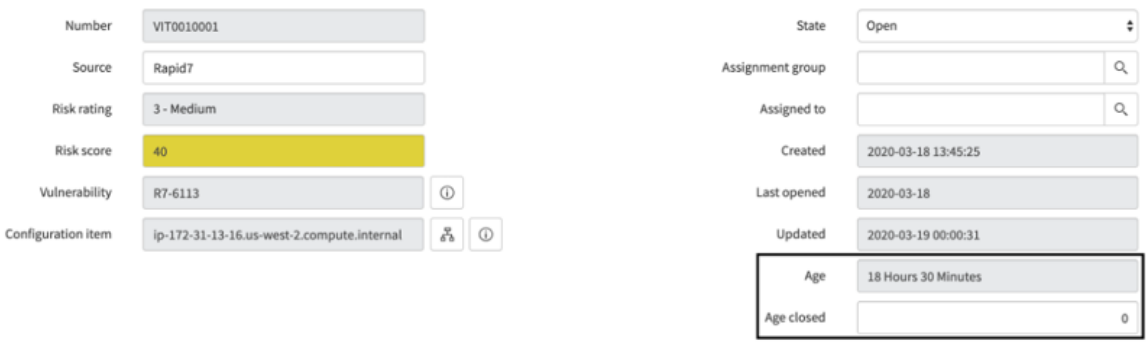
自動翻訳



VI 更新時の脆弱性一致アイテムリストおよび VI レコードの経過時間

VI が [クローズ済み] ステータスである場合、[経過時間] フィールドは表示されません。VI が [クローズ済み] に移行すると、次の図に示すように、[経過時間] 列の日数の値が [クローズ所要時間] フィールド (9) に表示されます。この値は、VI が [クローズ済み] に移行する前にアクティブだった日数を表します。たとえば、次の画像では、この VI は 9 日と 18 時間 29 分アクティブでしたが、クローズ済みレコードでは日数 (9) のみが表示されます。

この VI が再オープンされた場合、VI の状況が [オープン] に戻ると、[クローズ所要時間] フィールドは 0 にリセットされます。VI が再びアクティブになるため、経過時間 (日/時間/分) がリストビューの [経過時間] 列と VIT の [経過時間] フィールドに表示されます。



[経過時間] と [クローズ所要時間] の計算をカスタマイズする方法の詳細については、KB1703270 記事を参照してください。

脆弱性一致アイテムと修復タスクからのアサインの削除

自分または自分のグループに誤ってアサインされている可能性があると判断した脆弱性一致アイテム (VIT) および修復タスクレコードから、脆弱性一致アイテムの [アサイン先] フィールドと [アサイン先グループ] フィールドを直接クリアできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

概要

v16.5 以降、修復オーナーは 脆弱性対応 および アプリケーション脆弱性対応 アプリケーションで [アサイン解除] ボタンを使用してレコードを再アサインのために更新できます。

ユースケース

VI が修復範囲外であると判断した場合、またはレコードが自分または自分のグループに誤ってアサインされていると思われる場合、脆弱性一致アイテムレコードや修復タスクレコードの [アサイン先] および [アサイン先グループ] のフィールドから自分または自分のグループを削除できます。

モジュールのアサイン解除

[アサイン解除] ボタンは、[クローズ済み] 状況でも [解決済み] ステータスでもない以下のレコードに表示されます。

- クラシック環境と 脆弱性対応 ワークスペースの両方での修復タスク (VUL)。修復タスクがこの機能で更新されると、関連するすべての VI の [アサイン先] フィールドと [アサイン先グループ] フィールドもクリアされます。
- クラシック環境と 脆弱性対応 ワークスペースの両方での脆弱性一致アイテム (VIT)。
- アプリケーション脆弱性一致アイテム (AVI)。

UI ボタンまたは手動で更新したレコードは、該当するモジュール下の [未アサイン] モジュールに表示されます。

Unassigned UI アクションを使用してレコードを再アサインする方法については、「脆弱性一致アイテムのアサインを解除する」を参照してください。

一括編集

リスト上の複数の VI のアサインフィールドをクリアできます。VI を選択して [一括編集] を選択し、表示されるダイアログで [アサイン解除] チェックボックスをオンにします。

システムプロパティと通知

sn_vulc.vulnerability_admin ロールを持つアドミンの場合、レコードで [アサイン解除 **(Unassign)**] をクリックすると、デフォルトでは*sn_vul.unassign_vr.approval_required*、システムプロパティによって承認フローがトリガーされ、ステータス変更承認レコードがレビュー状況で作成され、承認者に対して [自分の承認] リストに表示される承認要求が発生します。

> **注:**
> 脆弱性アドミニストレーターは、*sn_vul.unassign_vr.approval_required* システムプロパティを **[false]** に設定して、承認プロセスを無効にできます。

- 承認者が要求を承認すると、*sn_vul.default_assignment_group* によって [アサイン先] フィールドと [アサイン先グループ] フィールドがクリアされ、[アサインのタイプ] フィールドに [未アサイン] が設定されます。脆弱性アドミニストレーターは、アサインフィールドがクリアされ特定のグループがアサインされるように、*sn_vul.default_assignment_group* システムプロパティの値を変更できます。たとえば、ユーザーがレコードで [アサイン解除] を選択し、それをレビューのために特定のグループにリダイレクトする場合は、選択したグループのシステム ID をシステムプロパティの値フィールドに追加できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

> **注:**
> この値を変更すると、アサインされていないすべての VI、AVIT、および CVIT の通知が、指定したグループに送信されます。

- 承認者が要求を却下した場合、却下理由が [メモ] タブに表示されます。

または、*sn_vul.default_assignment_group* が特定のグループに対して設定されていない場合、デフォルトでは、[通知のアサイン解除 (Unassign notification)] ユーザーグループに追加されたユーザーに対し、レコードがアサイン解除されたときにアラートが送信されます。*sn_vul.default_assignment_group* システムプロパティによって、このグループへの通知が決まります。

アサインタイプ [手動]、[ルール]、または [未アサイン] は、VI レコードとリストビューから使用できます。アサインタイプ [未アサイン] は、機能のシステムプロパティによって [アサイン先] および [アサイン先グループ] フィールドがクリアされた後にレコードに表示されます。

この機能のスケジュール済みジョブによるアサインルールの監視

日次スケジュール済みジョブでは、レコードのアサインタイプが [未アサイン **(Unassigned)]** に移行されるときにレコード数がカウントされます。この数を使用して、脆弱性アナリストは未アサインの VI 数が多いアサインルールに基づいて、パフォーマンスが悪いアサインルールを監視および調整できます。

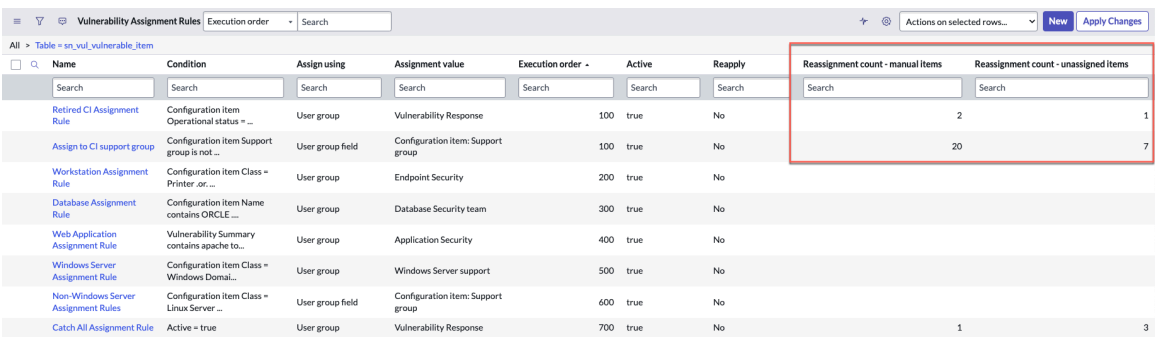
スケジュール済みジョブ *Reassignment count for assignment rules* は毎日実行され、この機能によって特定のアサインルールに対してアサインされていない VI の合計数を提示します。

このジョブによって収集されたカウントは、脆弱性対応 および アプリケーション脆弱性対応 の脆弱性一致アイテムと一意のアサインルールに適用されます。カウントは、各モジュールの各アサインルールリストにアサインルール別に表示されます。

このジョブは、手動でアサイン解除されたレコードもカウントします。手動によるカウントとこの機能によって収集されたカウントはともに、脆弱性アサインルールリストの [*Reassignment count - manual items*] と [*Reassignment count - unassigned items*] の 2 つの列に提示されます。

1. 脆弱性アドミニストレーターがこれらの数を表示するには、次に移動します: 脆弱性対応 > アドミニストレーション > アサインルール.
2. リストの右上にある歯車アイコンをクリックし、表示する [*Reassignment count - manual items*] および [*Reassignment count - unassigned items*] を選択します。
3. 最初にルールによってアサインされたが、以降に自動または手動で再アサインされた VI には、リストビューに元のルールへの参照が含まれています。

次の例は、2 つのアサインルールの再アサイン回数を示しています。



Vulnerability Assignment Rules | Execution order | Search | Actions on selected rows... | New | Apply Changes

All > Table = sn_vul_vulnerable_item

Name	Condition	Assign using	Assignment value	Execution order	Active	Reapply	Reassignment count - manual items	Reassignment count - unassigned items
Retired CI Assignment Rule	Configuration item Operational status = ...	User group	Vulnerability Response	100	true	No	2	1
Assign to CI support group	Configuration item Support group is not ...	User group field	Configuration item: Support group	100	true	No	20	7
Workstation Assignment Rule	Configuration item Class = Printer ,or, ...	User group	Endpoint Security	200	true	No		
Database Assignment Rule	Configuration item Name contains ORCLE	User group	Database Security team	300	true	No		
Web Application Assignment Rule	Vulnerability Summary contains apache to...	User group	Application Security	400	true	No		
Windows Server Assignment Rule	Configuration item Class = Windows Domai...	User group	Windows Server support	500	true	No		
Non-Windows Server Assignment Rules	Configuration item Class = Linux Server ...	User group field	Configuration item: Support group	600	true	No		
Catch All Assignment Rule	Active = true	User group	Vulnerability Response	700	true	No	1	3

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 の算出と脆弱性算出ルール

脆弱性算出では、脆弱性一致アイテムのフィールドの初期値の計算が自動化されます。各算出の条件が順番に評価され、最初に一致した算出が使用されます。

脆弱性算出

脆弱性対応 ベースシステムには、脆弱性一致アイテムのベース [リスクスコア] を設定する 2 つの脆弱性算出が含まれています。

- デフォルトのリスク計算機
- 脆弱性重大度

脆弱性算出は、条件フィルターを使用することにより、任意の条件に基づいて脆弱性一致アイテムの影響度を優先順位付けして評価するようにビルドできます。脆弱性のビジネスインパクト、構成アイテム (CI) のクラス、脆弱性一致アイテムの経過時間などの条件を問わず、追加の脆弱性算出を作成して脆弱性一致アイテムに他のフィールドを設定できます。また、既存の脆弱性算出をカスタマイズすることもできます。算出は、どのような優先順位でも反映できるように記述できます。詳細については、「脆弱性対応 算出の作成」と「脆弱性対応 内のフィルタリング」を参照してください。

さらに、構成管理データベース (CMDB) の configuration_item [cmdb_ci] の属性を使用して、脆弱性対応のリスク算出のロジックを作成できます。たとえば、組織内で外部向け CI の方が脆弱であり、即時の修復が必要であると判断した場合は、これらの CI に *`Internet Facing`* などの属性をアサインすることができます。この属性およびその他の属性は、Orlando ファミリーリリースの Common Service Data Model リリースノートに記載されています。CMDB に関する最新情報とガイダンスについては、以下のトピックを参照してください。

- Common Services Data Model 概念モデル
- CMDB スキーマモデル

各算出には、算出ルールのリストと、それを適用するタイミングを決定する条件が含まれています。算出が実行されると、各算出ルールの条件が順番に評価され、最初に一致した算出ルールが使用されます。

[脆弱性重大度] 算出では、正規化された脆弱性重大度を使用して、脆弱性一致アイテムの [リスクスコア] を計算します。

注:

- 一度にアクティブにできる算出は、ターゲットフィールド ([リスクスコア]) ごとに 1 つのみです。[脆弱性重大度] はデフォルトで無効になっています。
- 脆弱性対応 v23.0 以降、VIT でリスクスコアが更新されると、次の詳細において [メモ] セクションが更新されます。
  - 算出グループ名
  - 算出名：算出ルールがテンプレートとスクリプトのどちらに基づいているかに応じて、名前に括弧で囲まれた詳細が追加されます。算出ルールの基準を変更または表示するには、任意のルールをクリックし、[詳細表示] チェックボックスをオンにします。[値のタイプ **(Value type)**] ドロップダウンボックスから、必要なオプションを選択します。[テンプレート] を選択した場合、リスクスコアはルールで指定された条件に従って更新されます。[スクリプト] を選択した場合、既存のスクリプトを追加または更新できます。

    システムプロパティ *`sn_sec_cmn.risk_score_changes_add_worknotes`* は、作業メモセクションへの入力に役立ちます。脆弱性対応 v25.0.3 以降、このシステムプロパティはデフォルトで無効になっています。これを有効にした場合にのみ、リスクスコアに関連するすべての変更を表示できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

すべての有効な脆弱性算出では、脆弱性一致アイテムが作成される都度、関連する CI または脆弱性が変更されたとき、または脆弱性一致アイテムの [リスクスコアを計算] 関連リンクが使用されるときに、選択されたフィールドが設定されます。たとえば、インポートされた脆弱性一致アイテムで重大度の値が更新されると、脆弱性一致アイテムレコードのリスクスコアが自動的に更新されます。脆弱性インポートによって脆弱性スコアが更新されると、その脆弱性に対して再計算フラグが有効になります。その脆弱性を伴い、再計算フラグが有効 (true) になっている脆弱性一致アイテムのリスクスコアが再計算されます。

既存の脆弱性一致アイテムから [リスクスコアを計算] 関連リンクをクリックし、いずれかの算出が有効になっている場合、脆弱性一致アイテムの [リスクスコア] フィールドが更新されます。

注:

- [リスクスコアを計算] 関連リンクは、少なくとも 1 つの脆弱性算出が有効になっている場合にのみ表示されます。
- 脆弱性対応 v22.0 以降、レコードビューの [リスクスコアを計算] ボタンを選択して、Vulnerability Manager ワークスペース および IT 修復ワークスペース 内の脆弱性一致アイテムのリスクスコアを更新できます。
- 脆弱性対応 v23.0 以降、VIT のリスクスコアが変更されると、VIT の [メモ] セクションに次の詳細が記録されます。
  - 算出グループ名
  - 算出名：
  - 重み付けとリスクスコアの寄与度を含むフィールド値
  - 最終的なリスクスコア

脆弱性算出ルール

ベースシステムの [デフォルトリスク算出 **(Default Risk Calculator)]** ツールには、[デフォルトのリスクルール] というルールがあります。これは、「リスクルール」と呼ばれる特殊な脆弱性算出ルールとなります。複数の値に基づいて、[リスクスコア] が計算されます。

- 脆弱性重大度
- エクスプロイト情報
- 重要度
- 脆弱性がある CI の外部エクスポージャー
- EPSS スコア

[デフォルトのリスクルール] で使用する値と、これらの各値の重み付けを調整できます。重み付けは、ベースのリスクスコアを設定するときに各要素をどの程度考慮するかを調整するために使用されます。

デフォルトのリスクルールの基準をカスタマイズできます。詳細については、「脆弱性対応リスク算出のリスクルールのフィールドと重み付けの定義」を参照してください。

リスクルール算出機能のリスクスコアの決定方法については、「脆弱性対応 のリスクスコア算出の例」を参照してください。

重み付けパーセンテージをアサインする

フィールド値レベルで重み付けパーセンテージ (0 ～ 100) をアサインすることもできます。たとえば、重大度 ([なし] から [重大]) の各レベルに重み付けパーセンテージをアサインできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リスクルールの重大度の重み付けが 50 で、重大度レベルに次の重み付け値がアサインされている場合：

脆弱性重大度	リスクスコア
重大	100
高	50
中	20
なし	0

重大度が「重大」の場合、対応する重み付けは 50 です。重大度が「高」の場合、対応する重み付けは 25、重大度が「中」の場合、対応する重み付けは 10 です。重大度が [なし] の場合、対応する重み付けは 0 です。詳細については、「脆弱性対応 のリスクスコア算出の例」を参照してください。

脆弱性算出ルール設定

各ルールには [順序] 設定があります。しかし、条件に一致する最初のルールによって脆弱性一致アイテムの [リスクスコア] フィールドが更新されます。脆弱性算出ルール設定の詳細については、「脆弱性対応 算出の作成」を参照してください。通常、スクリプト化されていない算出ルールは、スクリプト化された算出ルールよりもパフォーマンスへの影響が少なくなります。

ベースシステムの脆弱性重大度算出には、重大度レベル (なし～重大) ごとに、重大度に基づいて [リスクスコア] の値 (0 ～ 100) をアサインする算出ルールが含まれています。[不明な重大度] には、リスクスコア 100 が自動的にアサインされます。これらの値は調整可能で、[デフォルトリスク算出 **(Default Risk Calculator)]** のように、新しい算出ルールやリスクルールを作成できます。

脆弱性のリスクスコアの重み付け

すべての脆弱性には、重大度、重要度、エクスプロイト情報などの要素に基づいてリスクスコアと評価がアサインされます。このリスク評価の算出を担当するのが、脆弱性一致アイテムのテーブルのビジネスルール *`Update Risk Rating from Risk Score`* です。リスクスコアが変更されるたびに、脆弱性一致アイテムのリスク評価が算出されて入力されます。脆弱性対応 (VR) アプリケーションのバージョン 17.1 より前では、次のリスク評価がスクリプトインクルード VulnerabilityUtils の一部として提供され、ハードコードされていました。

値 (リスク評価)	重み付け (リスクスコア)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

脆弱性対応 のバージョン 18.0 以降では、

- 出荷時のリスク評価タイプはベーステーブルで vr_risk_rating となっています。リスク評価タイプは、リスク評価が計算される各テーブルのビジネスルールの一部として渡されます。
- リスク評価の算出の対象となる [リスクスコアの重み付け] テーブルの値をクエリできるように、スクリプトが変更されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 既存のタイプにエントリーを追加するか、新しいタイプを作成します。新しいタイプを作成するときは、新しいリスク評価のラベルを追加し、関連するスクリプトとビジネスルールも変更してください。新しいリスクスコアのスタイルも新たに追加する必要があります。
- ベーステーブルのレコードをクエリするようにスクリプトを変更します。

[リスクスコアの重み付け] テーブルにアクセスするには、フィルターナビゲーターに「sn_sec_cmn_risk_score_weight」と入力します。

さらに、次のシナリオではリスクスコアが自動的に再計算されます。

- 構成アイテム (CI) が非インターネットフェーシングからインターネットフェーシングに変更されたとき。
- 脆弱性一致アイテム (VI) の関連する一般的な脆弱性とエクスポージャー (CVE) またはサードパーティエントリー (TPE) が、CVE の既知の悪用された脆弱性 (KEV) にリンクされている場合。

Tenable 脆弱性統合と Tenable リスクルール

Tenable リスクルールは Tenable 脆弱性統合 で利用できます。脆弱性優先評価 (VPR) は、脆弱性対応 の新しいデフォルトのリスク算出でインポートして使用される Tenable 製品の属性です。Tenable リスクルールは、脆弱性対応 の脆弱性算出のデフォルトのリスク算出の一部として Vulnerability Response Integration with Tenable アプリケーションとともにインストールされます。

このリスクルールデフォルトでは無効になっています。「セットアップアシスタントを使用した Tenable 脆弱性統合の構成」を参照してください。

サードパーティ統合からの 脆弱性対応 脆弱性一致アイテム検出

Now Platform® インスタンスでサードパーティのスキャンによって収集されたすべての情報を表示します。インスタンスで検出レコードと脆弱性一致アイテム (VI) レコードに対する返されたスキャン結果を表示します。これらの結果はスキャナーで表示されます。

概要

脆弱性対応 アプリケーションは、エンタープライズ環境から脆弱性一致アイテムのデータを取得するサードパーティの統合をサポートしています。検出に関する詳細データ、つまり、サードパーティ統合のスキャナーによって報告される脆弱性の単一の個別の発生は、Now Platform インスタンスの検出レコードと脆弱性一致アイテムレコードの両方にインポートされます。

サードパーティ統合によって脆弱性一致アイテム検出データが取得されます。検出は、スキャナーによって報告される脆弱性の個別の発生です。検出データは脆弱性一致アイテムとペアリングされ、検出のステータスに基づいて VI ステータスが更新されます。VI が見つからない場合は、新しい VI が作成されます。検出は、スキャナーによって直接検出されたデータによってのみオープンまたはクローズされます。

旧バージョンの 脆弱性対応 の脆弱性一致アイテム検出では、お使いの環境の CI (資産) とサードパーティのスキャナーからインポートされた脆弱性との関係により、Now Platform インスタンスに固有の脆弱性一致アイテムが作成されていました。

スキャナーによって提供される元のデータの粒度は保持されます。検出では、検出データが脆弱性一致アイテムとペアリングされます。取り込み中に脆弱性一致アイテムが見つからない場合は、新しい VI が作成されます。

脆弱性対応 v.21.1.2 以降、システムプロパティ *sn_vul.show_last_open_detection* がベースシステムで提供されます。デフォルトでは、このプロパティの値は false に設定されており、初期検出から VI に値を集計する現在の動作は変更されません。ただし、true に設定されている場合、VI は取り込み後の最後のオープン検出で自動的に更新されます。[IP アドレス]、[SSL]、[ポート]、

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[プロトコル]、[NetBIOS]、[証明] などのフィールドが VI 検出用に更新されます。必要に応じて DetectionBase スクリプトを変更すると、更新が必要な検出フィールドをカスタマイズできます。

前回のオープン検出の値を表示するには、VI フォームビューの [最後のオープン検出 **(Last Open Detection)]** タブに移動します。過去 1 年間にオープンされたすべての VI を最後のオープン検出値で更新するために、スケジュール済みジョブ *Update Last Open Detection Value To VITs* をオンデマンドで実行できます。このスケジュール済みジョブはベースシステムでも提供されます。

注:
検出されたアイテムで構成アイテム (CI) が変更されると、対応する更新も検出に反映されます。その結果、ある VI から別の VI に検出が移動される可能性があります。この変更と *sn_vul.show_last_open_detection* プロパティの値に基づいて、検出の値がソース VI とターゲット VI にロールアップされます。

脆弱性対応 のサポートされているバージョン

脆弱性対応 アプリケーションのインストールまたは更新の詳細については、「脆弱性対応 のインストール」を参照してください。

サポートされているサードパーティ統合

脆弱性一致アイテムの検出には、脆弱性対応 アプリケーションとのサードパーティ統合がサポートされている必要があります。脆弱性一致アイテムの検出のために 脆弱性対応 アプリケーションでは、以下のサードパーティ統合がサポートされています。

- Qualys ホスト検出統合
- Rapid7 データウェアハウス：
  - 脆弱性一致アイテム統合
  - 脆弱性一致アイテム解決統合
- Rapid7 脆弱性一致アイテム解決統合 (InsightVM)
  - Insight VM 統合
  - 脆弱性一致アイテム統合 - API
- Tenable 脆弱性統合
- Microsoft Defender Threat and Vulnerability Management

これらのサードパーティ統合は、個別のサブスクリプションで ServiceNow Store から入手できます。これらの統合の詳細については、「脆弱性対応 の統合」および「セキュリティオペレーションおよび ServiceNow Store」でエンタイトルメントの取得の詳細を参照してください。

サードパーティのスキャナーがインポート用に構成されていることを確認するには、「Install and configure the Rapid7 Integration for Security Operations application (Rapid7 Integration for Security Operations アプリケーションのインストールと構成)」および「Qualys 脆弱性統合 をインストールする」を参照してください。

脆弱性一致アイテムの検出に関する主要な用語

脆弱性
: 内部および外部のソースからインポートされたソフトウェア、オペレーティングシステム、資産の脆弱性に関するデータ。このデータはインポートされ、CMDB にリストされている既存の資産 (構成アイテム、CI) と比較されます。

脆弱性一致アイテム

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

インポートされた脆弱性が CMDB 内の CI と一致すると、脆弱性一致アイテムが作成または更新されます。

検出

Now Platform 環境内の脆弱性一致アイテム検出と呼ばれるスキャナーによって報告される脆弱性の単一の個別の発生。検出には、脆弱性および対応する脆弱性一致アイテムに関する拡張データが含まれます。このデータは、検出レコード (VID#) および脆弱性一致アイテムリストビューに表示され、以下の詳細を含んでいます。

- 初回検出 (データ)
- 最終検出日 (日付)
- DNS 名
- Net BIOS 名
- IP アドレス
- ポート
- プロトコル
- 実証
- SSL
- 検出回数

注:
検出テーブルにビジネスルールを追加すると、取り込みのパフォーマンスに影響します。

検出キー

検出を識別して脆弱性一致アイテムに関連付ける方法を提供する、フィールドのハッシュ化された組み合わせ。検出キーは統合ごとに固有です。

検出キー構成

スキャナー	脆弱性	ポート	プロトコル	資産 ID	実証	NIC
Qualys	はい	はい	はい	はい	いいえ	NA
Tenable	はい	はい	はい	はい	いいえ	NA
Rapid7	はい	はい	はい	はい	あり (大文字と小文字を区別しない)	はい

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

- 検出キーが指定されていない場合、または 脆弱性対応 14.0 より前のバージョンの場合、検出キーは脆弱性エントリー、ポート、プロトコル、資産 ID、および実証の組み合わせです。
- 脆弱性対応 の v19.0 以降では、新しい検出キーの NIC が Rapid7 InsightVM に追加され、デフォルトでアクティブ化されています。NIC のない既存の検出は、Rapid7 からペイロードで最初に受信する NIC で更新されます。検出キーは、NIC を含む検出で再計算され、再入力されます。NIC 値が異なる類似の検出が発生した場合は、新しい検出が作成されます。このデータは、脆弱性一致アイテムテーブルにロールアップされません。NIC 値は、sn_vul_detection_key_config および sn_vul_detection テーブルの新しい列に格納されます。

重複排除

データが特定のハードコードされた基準を満たしている場合に個々の検出を単一の VI に折りたたむ、脆弱性対応 アプリケーションによって使用されるプロセス。

VI 外部 ID

VI テーブルの [外部 ID] フィールドに格納されている値。 この値は、VI 内のキーの組み合わせで構成されるハッシュで、これによりアプリケーション内で VI が固有になります。CI と脆弱性エントリーで構成されています。

解決された脆弱性一致アイテムの再オープン

Now Platform インスタンスで [解決済み] に設定されているが後続の統合実行によって [クローズ済み]/[修正済み] に移行されていない脆弱性一致アイテムは、再スキャン中に検出された場合に再オープンされます。

サブステートが [修正済み] または [古い] であるクローズ済みの VI は、新しい検出が作成され、VI が新しい脆弱性と一致する場合に再オープンされます。

スクリプトインクルード、*DetectionBase*、メソッド *_shouldReOpenVI()* により、VIT が以前に [クローズ済み] でサブステートが [修正済み]、[古い]、または **[CI** 廃止] であった場合は再オープンされ、検出が既存の VIT にマッピングされます。

たとえば、VIT のクローズ日が検出の last_found 日より後であるとします。この VIT のレコードはクローズされたままであると想定されます。しかし、以前にクローズされた VIT が再オープンされたということは、その VIT が以前の検出によってクローズされ、脆弱性が後のスキャンで再度見つかったことを意味します。新しい検出が見つかり、それが VIT の構成アイテムと同じ脆弱性があるクローズ済み VIT と一致すると、VIT が再オープンされます。

Rapid7 検出の場合、インスタンスの [Rapid7 構成] ページで、解決済みの VI を経過時間別に再オープンするオプションが利用可能になりました。有効にすると、[解決済み] に設定されていても、後続のスキャンで [クローズ済み]/[修正済み] に移行しなかった VI は、入力した日数後に [オープン] に戻ります。

Qualys 検出で、[解決済み] に設定された VI が後続のスキャンで [クローズ済み]/[修正済み] に移行されていない場合、最終検出日が解決日より後であると、こうした VI が [オープン] に戻ります。

検出データの表示

VI レコードの脆弱性一致アイテム検出からインポートされたデータを表示します。詳細については、「脆弱性対応 脆弱性一致アイテム検出データの表示」と「統合実行 (VINTRUN) レコードの 脆弱性対応 脆弱性一致アイテム検出データの検証」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

現在の環境内の脆弱性を、それを修正できるソリューションに自動的に関連付けます。脆弱性に適用される修正アクションを識別し、脆弱性リスクが最も低減されるものから順に優先順位を付けます。

脆弱性ソリューション管理

多くの場合、セキュリティチームと IT チームは、自社環境に最も効果的な対処方法を特定するために、膨大な時間をかけて脆弱性の調査結果を追求します。大規模な組織における脆弱性の量と複雑さを考慮すると、脆弱性に関する調査結果を修復タスクに変えることは、手間がかかり、間違いを起こしやすいプロセスです。

脆弱性ソリューション管理 を使用すると、脆弱性の調査結果を修正ソリューションと自動的に関連付けることができます。組織に最も大きな影響を与えるソフトウェアパッチ、構成の更新、およびその他のコントロールを手作業によるオーバーヘッドなく特定します。

脆弱性ソリューション管理 の要件

脆弱性ソリューション管理 は 脆弱性対応 アプリケーション内で利用できる機能です。脆弱性ソリューション管理 には別のサブスクリプションが必要です。

ServiceNow Store からアプリケーションのエンタイトルメントを取得する方法の詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」を参照してください。アプリケーションをインスタンスにダウンロードした後のインストールの詳細については、「脆弱性対応のソリューション管理アプリケーションのインストール」を参照してください。

脆弱性ソリューション管理 をインストールすると、脆弱性対応 内から Microsoft セキュリティレスポンスセンター および Red Hat のソリューションデータにアクセスできます。

注:

セットアップアシスタント内から両方のソリューションアプリケーションを構成できます。「セットアップアシスタントを使用した 脆弱性ソリューション管理 のインストール済みソリューション統合の構成」を参照してください。

「Microsoft セキュリティレスポンスセンターソリューション統合 」および「Red Hat Solution Integration」を参照して、インポートされたソリューションの詳細を確認してください。

利用可能バージョン

脆弱性ソリューション管理 の最新バージョンについては、最新バージョンの 脆弱性対応 がインストールされていることを確認してください。

脆弱性ソリューション管理 のリリースバージョン	脆弱性対応 の互換バージョン	リリースノート
脆弱性ソリューション管理 v10.3	脆弱性対応 v18.0	互換性情報については、「KB0856498 脆弱性対応互換性マトリクスおよびリリーススキーマの変更」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソリューションと優先について

優先更新とは、以前のリリースから完全に置き換わるということです。たとえば、ホットフィックスの更新よりもサービスパックが優先される場合があります。ソリューションは脆弱性に関連しています。ソリューションを優先チェーン内の他のソリューションに関連付けることもできます。ソリューションは累積的であるため、先行ソリューションの脆弱性にも対応します。脆弱性ソリューション管理 は、先行ソリューションの脆弱性を優先ソリューションに自動的に関連付けます。古い脆弱性が見つかった場合は、上位の優先ソリューションで対処できますが、最も累積的である、優先度が最も高いソリューションが優先されます。

見込みのある解決策と優先ソリューション

見込みのある解決策とは、脆弱性に対処する可能性があるソリューションです。多くの場合、脆弱性には見込みのある解決策が多数あります。優先ソリューションは、脆弱性または脆弱性一致アイテム (VI) を修正するための単一のソリューションです。それによって意図が伝達され、展開メトリクスがより詳細になります。

優先ソリューション

脆弱性ソリューション管理 は、最も優先度が高いソリューションが 1 つしかない場合に、最高優先度に基づいて、検出された脆弱性に対して最も効果的なソリューション (優先ソリューション) を自動的に設定します。脆弱性に複数の最高優先度が存在する場合、値は設定されません。脆弱性対応で、優先ソリューションは、脆弱性に関連付けられたソリューションから派生した最も優先度の高い Microsoft セキュリティレスポンスセンター または Red Hat のソリューションです。

優先ソリューションの値は、脆弱性一致アイテムまたは脆弱性に設定できます。脆弱性に直接設定すると、脆弱性に関連付けられたすべての脆弱性一致アイテムがそのソリューションを継承します。一括編集機能を使用して、複数の脆弱性一致アイテムに対する優先ソリューションの値を変更します。一括編集する場合、脆弱性エントリーレベルで優先ソリューションを設定すると、以降すべての新しい VI に対して優先ソリューションが設定されるため、脆弱性一致アイテムの優先ソリューションのみが更新されます。一括編集は、現在の脆弱性一致アイテムにのみ適用されます。

> **注:**
> 脆弱性に対して最も優先度の高いソリューションが複数存在する場合、そのソリューションは影響を受ける資産に依存するため、その脆弱性レベルの優先ソリューションの値がクリアされます。脆弱性に対して最も優先度の高いソリューションが複数存在する場合は、脆弱性一致アイテムに優先ソリューションを 1 つ設定します。[脆弱性一致アイテム] フォームの [ルックアップ] リストを使用して、別のソリューションを設定できます。

ある修復タスクの脆弱性一致アイテムに対する優先ソリューションはすべて、修復タスクレコードの関連リストにあります。

すべてのソリューションをインポートすれば全データがリフレッシュされるわけではありません。優先プロセスは、以下の場合に更新されます。

- 脆弱性一致アイテムが作成されたとき。
- アクティブな VI のデータが変更されたとき。

  > **注:**
  > 脆弱性対応 v22.0 以降、上記の 2 つのケースではソリューションがキューに入れられません。

- CVE を含むサードパーティエントリーに対して新しいマッピングが作成されたとき。
- 前回のインポート以降に新しいソリューションデータがリリースされ、既存のソリューションが更新されたとき。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性対応 の v24.0.6 以降では、ベンダーのソリューションに加えてスキャナーからソリューションを取り込むことができます。Tenable、 Qualys、Microsoft TVM などのスキャナーからの修復データがソリューションの作成に利用されます。これらのスキャナーソリューションは、次の統合を使用してインポートされます。

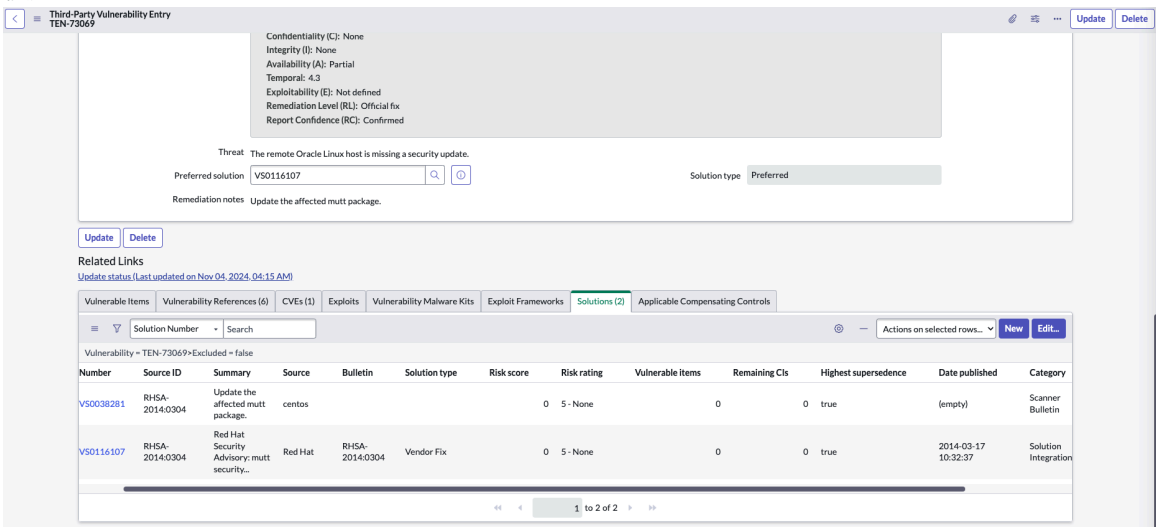
- Tenable.sc プラグイン統合
- Tenable.io プラグイン統合
- Qualys ナレッジベース (バックフィル)
- Microsoft TVM マシンの脆弱性統合 (フルインポート)
- Microsoft TVM マシンの脆弱性統合 (デルタインポート)

脆弱性統合が実行されると、サードパーティのエントリーを処理する前に修復情報のペイロードが作成されます。Tenable および Qualys の場合、修復データは脆弱性またはサードパーティのエントリーレベルで受信されます。逆に、Microsoft TVM の場合、ソリューションは検出レベルで作成されるため、追加の処理を必要とせずに、脆弱性一致アイテムに優先ソリューションを直接入力できます。これらのソリューションは、この修復情報に基づいて作成され、必要に応じて処理されます。処理時に、優先ソリューションが脆弱性に設定され、脆弱性一致アイテムにロールダウンされます。優先ソリューションは、次の順序で入力されます。

- 手動選択:ソリューションを手動で選択した場合、そのソリューションは上書きされません。
- ベンダーソリューション (Microsoft、RedHat、CVRF、および CSAF インポート):ソリューションを手動で選択しない場合は、ベンダーソリューションが自動的に選択されます。
- 最新のソリューション (有効な場合):脆弱性に対して利用可能な上位のソリューションが複数ある場合、[優先ソリューション] フィールドは空のままになります。このような場合、プロパティ *sn_vul.latest_solutions*を有効にすると、最新の上位の優先ベンダーソリューションが優先ソリューションとして設定されます。
- スキャナーセキュリティ情報 ソリューション (有効な場合):ソリューションを手動で選択しない場合、またはベンダーのソリューションが利用できない場合、単一のスキャナーソリューションがあれば、[優先ソリューション] フィールドにスキャナーソリューションが入力されます。スキャナーソリューションを入力するには、プロパティ *sn_vul.populate_scanner_solutions* を有効にする必要があります。

自動翻訳

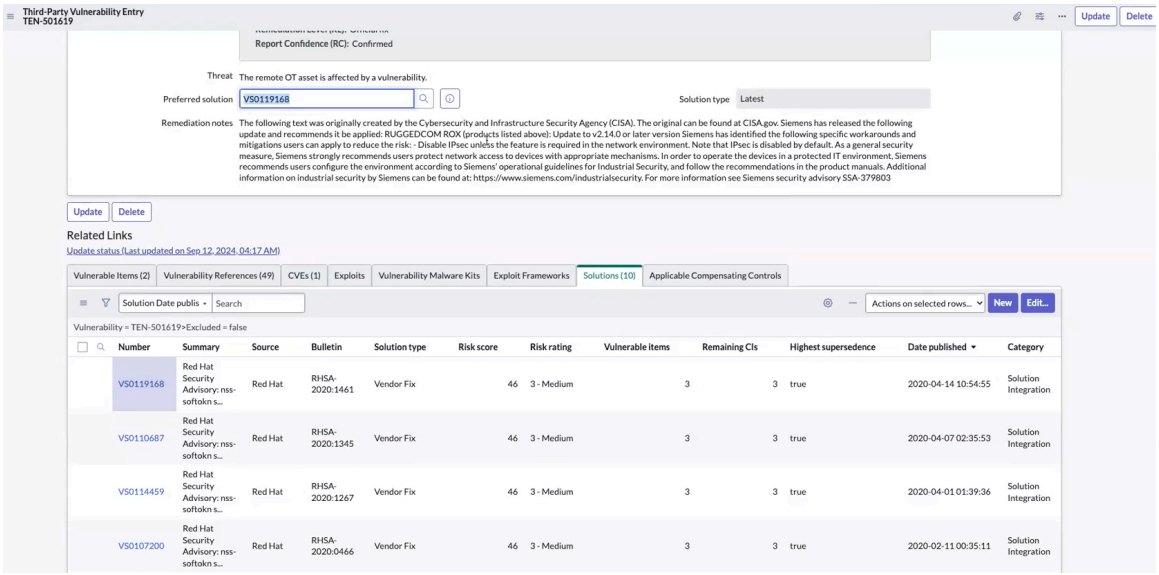
複数のソースからのソリューション



この例は、異なるソースから複数のソリューションが利用可能な場合のソリューションの選択を示しています。この場合、脆弱性にはベンダーからのソリューションとスキャナーからの 2 つのソリューションがあります。ソリューションVS0116107は優先度の高いベンダー (Redhat) から受信されるため、優先ソリューションとして選択されます。

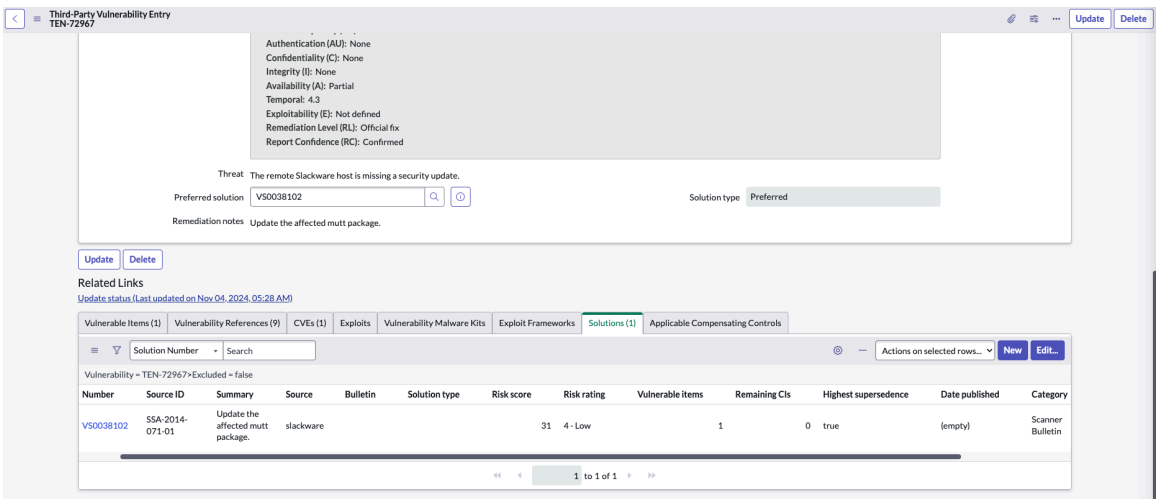
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

同じベンダーのソリューション



この例は、同じベンダー (この場合は Redhat) から複数のソリューションが入手可能な場合のソリューションの選択を示しています。*sn_vul.latest_solutions* プロパティが有効になっていて、特定の脆弱性に対して他のベンダーのソリューションを利用できない場合、これらのソリューションが処理され、脆弱性、続いて脆弱性一致アイテムの優先ソリューションが入力されます。プロパティ *sn_vul.latest_solutions* を有効にすると、最新のソリューションが優先ソリューションとして選択されます。

同じスキャナーからのソリューション



この例は、スキャナーから利用できるスキャナーソリューションが 1 つしかない場合のソリューションの選択を示しています。 *sn_vul.populate_scanner_solutions* プロパティが有効になっている場合、ソリューションが処理され、脆弱性、続いて脆弱性一致アイテムに優先ソリューションが入力されます。複数のスキャナーソリューションがある場合、あいまいさのために [優先ソリューション] フィールドは空のままになります。

ソリューション管理とパフォーマンス最適化の強化

ソリューションは、Microsoft や Redhat などのさまざまな統合から得られます。前者は毎月更新が行われます。一連の依存関係が確立され、脆弱性に対する優先ソリューションが追跡されます。ただし、他の統合においては、この更新形式が採り入れられていないため、依存関係のチェーンを確立する必要はありません。以前は、グラフを作成して優先順位を維持し、最も優先されるソリューションを特定する処理ロジックが用いられていました。これらのソリューションが、脆弱性に対する優先ソリューションとして提案されました。しかし、グラフの構築は時間がかかるため、

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

他の統合はこのプロセスから除外されています。パフォーマンスを向上させるために、脆弱性対応 v22.0 以降、*Process Vulnerability Solutions Metrics Queue* のスケジュール済みジョブで *utility.processNonGraphSolutions()* メソッドが呼び出されます。このメソッドは、Microsoft 以外の統合からのソリューションを処理します。

次に、ソリューションは、スケジュール設定済みジョブの *Process Vulnerability Solutions Metrics Queue* により、さまざまなソースからキューに入れられます。このスケジュール済みジョブでは、NVD エントリーからサードパーティエントリーへのソリューションのロールアップ、脆弱性に関する優先ソリューションの入力、およびソリューションの修復ステータスメトリクスの更新を行います。次のシナリオでは、修復ステータスメトリクスのみを更新する必要があります。

- 脆弱性の優先ソリューションが変更されたとき
- VIT が作成または削除されたとき
- VIT インポートが完了したとき

ソリューションは修復ステータスメトリクスのみを更新するためにキューに入れられますが、NVD エントリーからサードパーティエントリーにソリューションをロールアップし、優先ソリューションを入力しようとします。このプロセスを最適化するために、脆弱性ソリューションテーブルに [更新ステータス] 列が導入されています。優先ソリューションのロールアップや入力を必要とせずに、ソリューションの修復ステータスメトリクスを更新する必要がある場合、ソリューションはキューに入れられなくなります。代わりに、[更新ステータス] 列が True として直接更新されます。このアプローチにより、修復ステータスメトリクスのみを更新する必要があるケースを処理できるため、時間とリソースを節約できます。スケジュール済みジョブでは、キューに格納されたソリューションの処理が完了すると、更新ステータスが true としてマークされたソリューションが識別されます。次に、これらのソリューションを通じて反復処理され、カウントが計算され、それに応じて修復ステータスメトリクスが更新されます。このステップは、キューに入れる必要があるソリューションの数が減るため、スケジュール済みジョブのパフォーマンスを向上させる上で重要な役割を果たします。修復ステータスメトリクスを表示するには、脆弱性ソリューション [sn_vul_solution] テーブルに移動し、脆弱性ソリューションを選択します。その後、[修復ステータス] タブを選択します。このタブには、次のフィールドがあります。

修復ステータスメトリクス

フィールド	説明
優先ソリューションターゲット：優先ソリューションとなる VI の修復ステータス	
脆弱性一致アイテム	修復のためにこのソリューションが優先されるアクティブな (クローズされていない) 脆弱性一致アイテムの数。この数には、保留された脆弱性一致アイテムは含まれません。
残りの CI	修復のためにこのソリューションが優先される 1 つ以上のアクティブな脆弱性一致アイテムに関連付けられた CI の数。この数には、保留された脆弱性一致アイテムは含まれません。
合計 VI	修復のためにこのソリューションが優先されるアクティブおよびクローズ済みの脆弱性一致アイテムの数。この数には、保留された脆弱性一致アイテムは含まれません。
合計 CI	修復のためにこのソリューションが優先される 1 つ以上のアクティブおよびクローズ済みの脆弱性一致アイテムに関連付けられた CI の数。この数には、保留された脆弱性一致アイテムは含まれません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復ステータスメトリクス (続く)

フィールド	説明
修復された VI の割合	脆弱性一致アイテム (VI) の修正の完了率。このソリューションが優先される VI に適用されます。この数には、保留された脆弱性一致アイテムは含まれません。
修復された CI の割合	CI 修復の完了率。このソリューションが優先される VI に適用されます。この数には、保留された脆弱性一致アイテムは含まれません。
優先ソリューションターゲット ([保留]を含む)：優先ソリューションとなる、保留を含む VI の修復ステータス	
脆弱性一致アイテム	修復のためにこのソリューションが優先されるアクティブな (クローズされていない) 脆弱性一致アイテムの数。
残りの CI	修復のためにこのソリューションが優先される 1 つ以上のアクティブな脆弱性一致アイテムに関連付けられた CI の数。この数には、保留された脆弱性一致アイテムは含まれません。
合計 VI	修復のためにこのソリューションが優先されるアクティブおよびクローズ済みの脆弱性一致アイテムの数。
合計 CI	修復のためにこのソリューションが優先される 1 つ以上のアクティブおよびクローズ済みの脆弱性一致アイテムに関連付けられた CI の数。
修復された VI の割合	脆弱性一致アイテム (VI) の修正の完了率。このソリューションが優先される VI に適用されます。
修復された CI の割合	CI 修復の完了率。このソリューションが優先される VI に適用されます。
見込みのあるソリューションターゲット：当該のソリューションに関連する脆弱性を有するすべての VI における修復ステータス	
脆弱性一致アイテム	このソリューションが修復のソリューションとなる可能性があるアクティブな (クローズされていない) 脆弱性一致アイテムの数。この数には、保留された脆弱性一致アイテムは含まれません。
残りの CI	このソリューションが修復のソリューションとなる可能性がある 1 つ以上のアクティブな脆弱性一致アイテムに関連付けられた CI の数。この数には、保留された脆弱性一致アイテムは含まれません。
見込みのあるソリューションターゲット ([保留] を含む)：当該ソリューション関連の脆弱性を有する、保留を含むすべての VI における修復ステータス	
脆弱性一致アイテム	このソリューションが修復ソリューションとなる可能性があるアクティブな (クローズされていない) 脆弱性一致アイテムの数。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復ステータスメトリクス (続く)

フィールド	説明
残りの CI	このソリューションが修復のソリューションとなる可能性がある 1 つ以上のアクティブな脆弱性一致アイテムに関連付けられた CI の数。

3 つ目として、脆弱性を修復するために、脆弱性や VIT に対する優先ソリューションの可用性を確保する必要があります。ただし、脆弱性に対してより優先度の高いソリューションが複数存在する場合は、不明確さが生じるため優先ソリューションが設定されません。当該のシナリオに対処するために、処理ロジックを実行し、使用可能な場合は優先ソリューションを設定するアプローチが実装されます。優先度の高いソリューションが 1 つしかない場合は、それが優先ソリューションとして設定されます。複数存在する場合、[優先ソリューション] フィールドは空白のままになります。しかし、目的は、最新として公開されている最上位の優先ソリューションを優先ソリューションとして設定することです。これを実現するために、システムプロパティ *sn_vul.latest_solutions* が導入されています。デフォルトでは、このプロパティは false です。優先ソリューションが利用できないときに、最新のソリューションを優先ソリューションとして設定する機能を有効化する場合は、このプロパティを有効化することができます。有効化すると、脆弱性テーブルの [ソリューションタイプ] 列が次のオプションで更新されます。

- 優先：優先ソリューションが入力されている場合
- 最新：優先ソリューションが利用できない場合、公開日の値に基づいて、最優先のソリューションセットから最新のソリューションが選択されます。最新のソリューションとして選択されるフィールドは、*sn_vul.latest_solutions* システムプロパティを使用してカスタマイズできます。デフォルトでは値が [公開日] に設定されていますが、[最終変更日] に変更して、ソリューションの最終変更日列に基づいてソリューションを選択することもできます。
- 手動：優先ソリューションタイプを手動で更新する場合。このタイプのソリューションが最も高い優先順位になります。

特定のシナリオでは、脆弱性一致アイテム (VIT) の優先ソリューションが、対応する脆弱性の優先ソリューションと異なる場合があります。これは、優先ソリューションが脆弱性上ではなく VIT 上で手動更新されることが原因となります。このような場合、[ソリューションタイプ] フィールドは VIT で非表示になります。

脆弱性ソリューション管理 の実行内容

- Microsoft セキュリティレスポンスセンターソリューション統合 および Red Hat Solution Integration のインポート時に、新しい脆弱性一致アイテム (VITs) と修復タスクがソリューションに自動的に関連付けられます。

  MSRC ソリューションは、そのソリューションが表示される最新のセキュリティ情報に関連付けられています。

- 脆弱性レコードがソリューションに手動で関連付けられている場合、脆弱性一致アイテムと修復タスクをソリューションに自動的に関連付けます。

  注:
  別のソリューションに手動で再アサインされた脆弱性一致アイテムは、脆弱性レベルでのソリューションの変更によって自動的に更新されることはありません。

- MSRC：インポート中に、ソリューションの関連リストで表示できる優先度チェーンを作成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- ソリューションが最も優先度の高いソリューションかどうかを示します。
- 最大限にリスクを削減できるように、各ソリューションに関連付けられたソリューションリスクスコアを一覧表示します。
- 修正の進捗状況を追跡できるように、サードパーティの脆弱性エントリー、修復タスク、および脆弱性ソリューションレコードのソリューションの修復ステータスを維持します。

  これには、以下の内容が含まれています。
  - 保留ステータスの VI の有無にかかわらず、優先ソリューションのある VI に関する、修正済み割合ごとの脆弱性一致アイテムの数。
  - 保留ステータスの VI の有無にかかわらず、優先ソリューションのある VI に関する、修正済み割合ごとの構成アイテム (CI) の数。
  - 保留ステータスの VI の有無にかかわらず、見込みのある解決策がある VI に関する、修正済み割合ごとの脆弱性一致アイテムの数。
  - 保留ステータスの VI の有無にかかわらず、優先ソリューションのある VI に関する、修正済み割合ごとの構成アイテムの数。

脆弱性ソリューション管理 の機能

- 脆弱性に関連付けられたソリューションを作成、更新、表示、または削除して、サードパーティソリューションコンテンツの対象外である脆弱性ソリューションを追跡できるようにします。Rapid7 データウェアハウスとのソリューション統合はサポートされていません。
- サードパーティの脆弱性および NVD のエントリーをソリューションレコードに関連付けます。
- 脆弱性一致アイテムと修復タスクを削除して、ソリューションに再度関連付けます。
- 脆弱性フォームおよび脆弱性一致アイテムフォームで、特定の脆弱性に適用可能な優先ソリューションを表示します。
- 当該グループ内の少なくとも 1 つのアクティブな VI によって優先されているすべてのソリューションを一覧表示する修復タスクフォームで、優先ソリューション関連リストを表示します。
- 脆弱性、脆弱性一致アイテム、修復タスク、ソリューションの各フォームで、優先ソリューションの展開に関連するリスク削減を示すソリューションの修復ステータスの詳細を表示します。
- ソリューションフォームで、特定のソリューションに適用可能な脆弱性を表示します。
- MSRC：脆弱性に関する特定のソリューションの優先ソリューションを表示して、展開する最新の更新、または以前のより焦点を絞った効率的な更新を見つけます。
- さまざまな特性によりソートされたソリューションのリストを表示します。
  - すべて：公開日と番号でソートされたソリューション。
  - MSRC：最高優先度：保留されていないアクティブな脆弱性一致アイテムを含むソリューション。優先度が高い順、公開日、番号でソートされています。
  - 脆弱性一致アイテムを使用 (With Vulnerable Items)：保留されていないアクティブな脆弱性一致アイテムを含むソリューション。最高優先度、または優先、リスクスコア、番号でソートされています。展開されている場合、リストの上位のエントリーで、環境内の資産のリスクが最大限に削減されます。

ソリューションレコードのリスクスコアとリスク評価

注:
ソリューションレコードの [リスクスコア] および [リスク評価] は、脆弱性、脆弱性一致アイテム、および修復タスクに使用されるフィールドとは異なります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ソリューションレコードの [リスクスコア] は、脆弱性一致アイテムの [リスクスコア] と、このソリューションが見込みのある解決策となっているアクティブな脆弱性一致アイテムの数に基づいて重み付け計算が行われます。ソリューションの [リスクスコア] は、ソリューションが達成すると予想されているリスクの推定削減量を示します。

ソリューションレコードの [リスクスコア] は、次のように計算されます。

- 初めに、見込みのある解決策が設定されているアクティブな脆弱性一致アイテムについて、最高または最大の [リスクスコア] の 85% を取得します。
- 次に、ソリューションレコードの [リスクスコア] には、見込みのあるソリューションが設定されている脆弱性一致アイテムの合計数が集計されます。脆弱性一致アイテム数の範囲ごとにいくつかのポイントが加算され、合計が算出されます。
  - 脆弱性一致アイテムが 0 ～ 9 個の場合、追加ポイントなし
  - 脆弱性一致アイテムが 10 ～ 99 個の場合、5 ポイント追加
  - 脆弱性一致アイテムが 100 ～ 999 個の場合、10 ポイント追加
  - 脆弱性一致アイテムが 1000 個以上の場合、15 ポイント追加

  たとえば、脆弱性一致アイテムの [リスクスコア] が 80 の場合、ソリューションレコードの [リスクスコア] は 68 から始まります。その見込みのある解決策が設定されているアクティブな脆弱性一致アイテムが 200 個ある場合、最終的なソリューション [リスクスコア] は 78 になります。

ソリューションレコードの [リスク評価] には、ソリューションレコードの [リスクスコア] が [重大] から [なし] の範囲に分類されます。ソリューションの [リスク評価] で、このソリューションによって修正される脆弱性一致アイテムのリスク削減を評価します。

VR v16.1 までは、リスク評価によって結果のソリューションの [リスクスコア] が次の範囲に分類されていました。

- 1 - 重大 (90 以上のソリューションリスクスコア)
- 2 - 高 (70 ～ 89 のソリューションレコードリスクスコア)
- 3 - 中 (30 ～ 69 のソリューションレコードリスクスコア)
- 4 - 低 (1 ～ 29 のソリューションレコードリスクスコア)
- 5 - なし (0 のソリューションレコードリスクスコア)

VR v16.1 以降は、リスク評価によって結果のソリューションの [リスクスコア] が次の範囲に分類されます。

- 1 - 重大 (90 以上のソリューションリスクスコア)
- 2 - 高 (70 ～ 89 のソリューションレコードリスクスコア)
- 3 - 中 (40 ～ 69 のソリューションレコードリスクスコア)
- 4 - 低 (1 ～ 39 のソリューションレコードリスクスコア)
- 5 - なし (0 のソリューションレコードリスクスコア)

ユースケース

最も優先度が高いモジュールを使用して、現在のパッチサイクルのステータス展開の進捗状況を日付順に表示します。

脆弱性一致アイテムモジュールを使用して、最も価値の高いソリューションをリスクスコア順に表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ソリューションリストで、主要なソリューションの詳細、リスクスコア、および展開メトリクスを明らかにします。優先順位付けには、リスクスコアとアクティブな VI 数を使用します。現在のパッチサイクルのどのソリューションが進行していないかを確認します。これは、展開の前提条件を満たしていないことを示している可能性があります。

注:
脆弱性ソリューションフォームにある修正進捗状況の [リストの列をカスタマイズ] メニューから、修正された **VI** の割合 **(percent_nd_pref_vis_remediated)** を追加します。

Microsoft セキュリティレスポンスセンターソリューション統合

Microsoft セキュリティレスポンスセンターソリューション統合 によって提供される提案された修復ソリューションをレビューして実装します。

Microsoft セキュリティレスポンスセンターソリューション統合 は 脆弱性対応 の 脆弱性ソリューション管理 機能に含まれており、個別のサブスクリプションで利用できます。脆弱性対応 がソリューションを組み込む方法の詳細については、「脆弱性ソリューション管理」を参照してください。

Microsoft セキュリティレスポンスセンター は、Microsoft 製品とサービスに影響するセキュリティ脆弱性のレポートを調査し、セキュリティリスクの管理に役立つソリューションの情報を提供します。ソリューションとは、Microsoft セキュリティレスポンスセンター 製品から Microsoft セキュリティレスポンスセンターソリューション統合 にインポートされる既知の修復です。

Microsoft セキュリティレスポンスセンターソリューション統合 には、スケジュール済みジョブとして呼び出される Microsoft セキュリティレスポンスセンター 製品へのエントリーポイントが含まれています。スケジュール済みジョブでは、インスタンスを他の脆弱性管理システムと同期させることで、脆弱性修復ライフサイクルを簡素化します。スケジュール済みジョブは、指定した順序で自動的に実行されます。スケジュール済みジョブを手動で実行することもできます。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

利用可能バージョン

脆弱性ソリューション管理 および Microsoft セキュリティレスポンスセンター の最新バージョンのソリューションについては、最新バージョンの 脆弱性対応 がインストールされていることを確認してください。

脆弱性ソリューション管理およびソリューション統合のインストールと構成の詳細については、「脆弱性対応のソリューション管理アプリケーションのインストール」および「セットアップアシスタントを使用した 脆弱性ソリューション管理 のインストール済みソリューション統合の構成」を参照してください。

脆弱性対応 のリリースバージョン	脆弱性ソリューション管理 のバージョン	リリースノート
脆弱性対応 v15.0	v10.3	互換性情報については、「KB0856498 脆弱性対応互換性マトリクスおよびリリーススキーマの変更」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロール

Microsoft セキュリティレスポンスセンターソリューション統合 タスクには次のロールが含まれます。

- sn_vul.vulnerability_admin または sn_vul.admin (非推奨)：レコードの読み取り、書き込み、削除を実行できます。
- sn_vul.vulnerability_write：レコードを読み書きできます。
- sn_vul.vulnerability.read：レコードの読み取りを実行できます。
- sn_vul.remediation_owner：修復スペシャリストグループまたは個人に割り当てられたレコードの内部メモを読み書きできます。(itil ロールに含まれています。)

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

Microsoft セキュリティレスポンスセンターソリューション統合

Microsoft セキュリティレスポンスセンターソリューション統合を表示するには、次に移動します: **All** (すべて) > 脆弱性対応 > アドミニストレーション > 統合.

ベースシステムには、次の統合が含まれています。

Microsoft セキュリティレスポンスセンターソリューション統合

統合	説明
Microsoft Security Response Center ソリューション統合	ソリューションと脆弱性情報データベース (NVD) マッピングを取得して、ソリューションを脆弱性、脆弱性一致アイテム、および修復タスクに関連付けます。 **注:** Microsoft セキュリティレスポンスセンターソリューション統合は 2016 より前のソリューションは提供していません。

ソリューション

インポートされたソリューションをリストで表示するには、「ソリューションの表示」を参照してください。

Red Hat Solution Integration

脆弱性対応 アプリケーションの Red Hat Solution Integrationで提供される提案された修復ソリューションを確認して実装できます。

Red Hat Solution Integration は 脆弱性対応 の 脆弱性ソリューション管理 機能に含まれており、個別のサブスクリプションで利用できます。脆弱性対応 がソリューションを組み込む方法の詳細については、「脆弱性ソリューション管理」を参照してください。

Red Hat Solution Integrationは、Red Hat 製品とサービスに影響するセキュリティ脆弱性のレポートを調査し、セキュリティリスクの管理に役立つ解決策の情報を提供します。修復と呼ばれる解決策は、Red Hat から Red Hat Solution Integrationにインポートされます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性対応のバージョン 21.0 以降では、Red Hat はペイロードを Common Vulnerability Reporting Framework (CVRF) 形式ではなく、Common Security Advisory Framework (CSAF) 形式で送信します。XML ベースの標準である CSAF は、CVRF とは構造も形式も異なります。この変更に対応するために、新しい CSAF パーサーが開発されました。このパーサーは CSAF 形式を解釈し、必要なフィールドを抽出してそれに応じてテーブルに入力します。

注:
デフォルトでは、ペイロードは CSAF 形式で受信します。

次の抜粋は、それぞれ CSAF 形式と CVRF 形式で Red Hat から受信したペイロードを解析するための統合スクリプトを示しています。

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

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

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

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

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

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

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

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

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

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

Red Hat Solution Integrationには、Red Hat 製品へのエントリーポイントが含まれ、スケジュール済みジョブとして呼び出されます。スケジュール済みジョブでは、インスタンスを他の脆弱性管理システムと同期させることで、脆弱性修復ライフサイクルを簡素化します。自動的に実行されます。スケジュール済みジョブを手動で実行することもできます。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

利用可能バージョン

脆弱性ソリューション管理 および Red Hat の最新バージョンのソリューションについては、最新バージョンの 脆弱性対応 がインストールされていることを確認してください。

脆弱性ソリューション管理およびソリューション統合のインストールと構成の詳細については、「脆弱性対応のソリューション管理アプリケーションのインストール」および「セットアップアシスタントを使用した 脆弱性ソリューション管理 のインストール済みソリューション統合の構成」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 のリリースバージョン	脆弱性ソリューション管理 のバージョン	リリースノート
脆弱性対応 v15.0	v10.3	互換性情報については、「KB0856498 脆弱性対応互換性マトリクスおよびリリーススキーマの変更」を参照してください。

ロール

Red Hat Solution Integrationタスクには、sn_vul.configure_rhsa_integration ロールが関与します。

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

Red Hat Solution Integration

Red Hat Solution Integrationを表示するには、次に移動します: 脆弱性対応 > アドミニストレーション > 統合.

ベースシステムには、次の統合が含まれています。

Red Hat 統合

統合	説明
Red Hat Solution Integration	ソリューションと脆弱性情報データベース (NVD) マッピングを取得して、ソリューションを脆弱性、脆弱性一致アイテム、および修復タスクに関連付けます。

ソリューション

インポートされたソリューションをリストで表示するには、「ソリューションの表示」を参照してください。

Rapid7 ソリューション管理

ソリューションは、Rapid7 データウェアハウスまたは Rapid7 InsightVM から Rapid7 脆弱性統合にインポートされる既知の修復です。 Rapid7 データウェアハウスは、ソリューションと優先ソリューションの両方をインポートします。 Rapid7 InsightVM を使用すると、Rapid7 脆弱性一致アイテム統合 - API の一部としてソリューションを取得できます。

脆弱性対応 のバージョン 21.0 以降、Rapid7 InsightVM によるソリューションの作成方法が変更されています。Rapid7 InsightVM は、 **solution_summary**、 **solution_fix**、または **solution_type** フィールドに依存する代わりに、スキャナーによって提供される solution_id を使用してソリューションを作成するようになりました。これは、これらのフィールドが空の場合でも、ソリューション ID が利用可能な限り、ソリューションが作成されることを意味します。

インポートされたソリューションをリストとして表示するには、 **Rapid7** > ソリューション.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性ソリューション管理 プラグインが有効になっている場合、最新バージョンの Rapid7 脆弱性統合では、ソリューションに関する次の主要な機能が利用できます。

- Rapid7 ソリューション管理は脆弱性ソリューション管理に移動しました。
- データウェアハウスの新しい統合 Rapid7 前提条件ソリューション管理が導入されました。統合は、Rapid7 データウェアハウスから前提条件のソリューションをフェッチします。
- サードパーティエントリー (TPE) の Rapid7 (ソリューション) の関連リストは非表示になっています。
- 以前にインポートされたデータは、新しいデータモデルで表示できます。Rapid7 ソリューション、ソリューション優先度、および脆弱性ソリューションマップが再インポートされ、[次以降にインポート] フィールドが空に設定されます。ソリューション管理でフィールドが入力されます。
- 検出が更新され、ソリューションフィールドに入力されます。検出は、Vulnerability Solution Management の一部であるため、ソリューションを示します。
- Rapid7 は、Rapid7 データウェアハウスに対して TPE で優先ソリューションを設定する際に、他のソリューションよりも優先度が高くなります。
- ソリューションは、Rapid7 InsightVM の検出から脆弱性一致アイテム (VI) にロールアップされます。

> **注:**
> 脆弱性ソリューション管理 プラグインをアクティブ化していない場合、アプリケーションはそのまま機能します。

Vulnerability Solution Management

脆弱性ソリューション管理 プラグインをアクティブにすると、Rapid7 データウェアハウスと Rapid7 InsightVM の両方の Rapid7 ソリューションが脆弱性ソリューション [sn_vul_solution] テーブルに入力されます。ただし、脆弱性ソリューション管理 プラグインをアクティブ化していない場合、Rapid7 脆弱性統合はそのまま機能し、カスタム [sn_vul_r7_solution] テーブルのソリューションをインポートします。

脆弱性ソリューションテーブルを表示するには、次に移動します: **All** (すべて) > 脆弱性対応 > 脆弱性ソリューション ここでは、さまざまなベンダーのソリューションを表示して比較できます。インポートされたソリューションをカスタムテーブルで表示するには、 **All** (すべて) > **Rapid7 Vulnerability Integration** > ソリューション.

> **注:**
> ソース別にグループ化して、ベンダーに基づいてソリューションを表示します。

Rapid7 前提条件ソリューション管理統合

脆弱性ソリューション管理 プラグインをアクティブにすると、修正スクリプトが実行され、統合の順序が変更されます。Rapid7 データウェアハウスの新しい Rapid7 前提条件ソリューション統合は、前提条件ソリューションとソリューションをマッピングします。統合は次の順序で実行されます。

1. Rapid7 ソリューション統合
2. Rapid7 前提条件ソリューション
3. Rapid7 優先ソリューション統合
4. Rapid7 脆弱性ソリューションマップ統合
5. Rapid7 VI ソリューション統合 (脆弱性対応 19.0 以降)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
統合を手動で実行する場合は、Rapid7 ソリューション統合から開始します。Rapid7 統合内の [次の統合] チェーンは変更しないでください。順序は [次の統合] 列で定義されます。

TPE の Rapid7 (ソリューション) 関連リスト

脆弱性ソリューション管理 プラグインをアクティブにすると、次のことができます。

- TPE を表示するには、次に移動します。 **All** (すべて) > 脆弱性対応 > サードパーティ.
- 以前のリリースで使用できた [ソリューション (Rapid7)] 関連リストは表示されません。
- [ソリューション] 関連リストで、RedHat、Microsoft (MSRC) などの他のソースからのソリューションとともに、Rapid7 関連のソリューションを確認できます。

脆弱性ソリューション管理 プラグインをアクティブ化しないと、次のようになります。

- 関連リストの機能は同じままです。
- [ソリューション (Rapid7)] 関連リストが表示されます。
- [ソリューション] 関連リストは非表示になります。

TPE および VI の優先ソリューション

Rapid7 は、サードパーティエントリー (TPE) レベルでデータウェアハウスからソリューションを取得します。Rapid7 InsightVM の場合は検出レベルで取得します。

Rapid7 データウェアハウスの場合、ソリューションは次の方法で管理されます。

- 優先ソリューションは、脆弱性とソリューションのマッピングに基づいて TPE に設定されます。
- Rapid7 の脆弱性に Rapid7 の最も優先度が高いソリューションがある場合、その脆弱性に関連付けられているベンダーの他のソリューションに関係なく、優先ソリューションとして設定されます。
- 他のすべてのケースでは、優先ソリューションのフローは同じままです。優先ソリューションのデフォルトの動作の詳細については、「脆弱性ソリューション管理」を参照してください。

Rapid7 InsightVM の場合、ソリューションは次の方法で管理されます。

- 優先ソリューションは、検出から VI にロールアップされます。
- 単一の検出と Rapid7 のソリューションがある場合、ソリューションは VI にロールアップされます。
- 複数の検出があり、すべて Rapid7 の同じソリューションがある場合、ソリューションは VI にロールアップされます。
- 複数の検出に Rapid7 の複数のソリューションがある場合、最新のソリューションが VI にロールアップされます。

v19.0 以降の 脆弱性対応 では、Rapid7 データウェアハウスによって生成された推奨ソリューションは、Rapid7 によって脆弱性一致アイテムに直接入力され、脆弱性ソリューション管理 を必要としません。この変更により、これらの脆弱性一致アイテムのソリューションに関する不確実性が排除されます。

Rapid7 を使用してこの直接入力を実現するには、次の手順を実行します。

- 新しい統合である Rapid7 VI ソリューション統合が確立され、既存の Rapid7 脆弱性統合ワークフローに統合されます。
- 新しいテーブル [sn_vul_r7_rapid7_vi_solution_import] が作成されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 新しい変換マップ Rapid7 VI ソリューション変換が作成されます。
- スクリプトインクルード Rapid7AssetsImportProcessor は、脆弱性ソリューション管理 内の Rapid7 によって生成されたソリューションの処理を除外するように変更されました。

Rapid7 VI ソリューション統合を実行すると、Rapid7 から取得された未処理データは新しく作成されたテーブルに保存されます。続いて、Rapid7 VI ソリューション変換がトリガーされ、このデータが処理され、優先ソリューションが脆弱性一致アイテムテーブルに直接入力されます。

注:
Rapid7 VI ソリューション統合は、脆弱性ソリューション管理 プラグインがインストールされている場合にのみ優先ソリューションを入力します。

脆弱性対応 の v22.0 以降では、Rapid7 のソリューションは、スケジュール済みジョブ *Process Vulnerability Solutions Metrics Queue* の実行時にキューに入れなくなりました。このスケジュール済みジョブでは、NVD エントリからサードパーティエントリへのソリューションのロールアップ、脆弱性に関する優先ソリューションの入力、およびソリューションの修復ステータスメトリクスの更新を行います。次のシナリオでは、修復ステータスメトリクスのみを更新する必要があります。

- 脆弱性の優先ソリューションが変更されたとき
- VIT が作成または削除されたとき
- VIT インポートが完了したとき

ソリューションは修復ステータスメトリクスのみを更新するためにキューに入れられますが、NVD エントリーからサードパーティエントリーにソリューションをロールアップし、優先ソリューションを入力しようとします。このプロセスを最適化するために、脆弱性ソリューションテーブルに [更新ステータス] 列が導入されています。NVD エントリからサードパーティエントリへのソリューションのロールアップや優先ソリューションの入力を必要とせずに、ソリューションの修復ステータスメトリクスを更新する必要がある場合、ソリューションはキューに入れられなくなります。代わりに、[更新ステータス] 列が True として直接更新されます。このアプローチにより、修復ステータスメトリクスのみを更新する必要があるケースを処理できるため、時間とリソースを節約できます。スケジュール済みジョブでは、キューに格納されたソリューションの処理が完了すると、更新ステータスが true としてマークされたソリューションが識別されます。次に、これらのソリューションを通じて反復処理され、カウントが計算され、それに応じて修復ステータスメトリクスが更新されます。このステップは、キューに入れる必要があるソリューションの数が減るため、スケジュール済みジョブのパフォーマンスを向上させる上で重要な役割を果たします。

脆弱性用に **Rapid7** データウェアハウスからインポートされたソリューション優先度チェーン

ソリューションの優先ソリューションを表示するには、脆弱性ソリューションを選択し、[優先ソリューション] 関連リストを選択します。先行するソリューションを表示するには、[先行するソリューション] 関連リストを選択します。ソリューションを TPE に添付すると、そのソリューションの優先ソリューションがその TPE に添付されます。

システムプロパティによるグラフ内のソリューション優先度チェーンの最大深度の変更

Rapid7 データモデルで受信したソリューション優先度チェーンが長すぎて、優先ソリューションの入力中にグラフを作成できません。このため、チェーンの深度を制限するために、値が 500 の *sn_vul.max_recursion_depth* という名前のシステムプロパティが作成されます。チェーンの深度が 500 を超えると、残りのチェーンは無視されます。チェーンの最大深度を変更するには、[sys_properties] テーブルに移動し、プロパティの値を変更します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Rapid7 アプリケーションのアップグレード

Rapid7 脆弱性統合 プラグインをアップグレードし、脆弱性ソリューション管理 プラグインをアクティブ化していない場合、アプリケーションはそのまま機能します。

Rapid7 アプリケーションをアップグレードする前または後に 脆弱性ソリューション管理 プラグインをアクティブにすると、次の統合では [次以降にインポート] フィールドは空のままになります。

- Rapid7 優先ソリューション統合
- Rapid7 脆弱性ソリューションマップ統合
- Rapid7 ソリューション統合

> **注:**
> 次の統合実行から、データが脆弱性ソリューションテーブルに入力されます。

Rapid7 InsightVM の場合、データは検出レベルで受信されます。Rapid7 InsightVM 統合が実行されると、ソリューションが脆弱性ソリューションテーブルにインポートされます。

ソリューションベンダーからデータを取り込むための汎用フレームワーク

ソリューションインテリジェンス統合用の汎用フレームワークを使用して、ソリューションベンダーからさまざまなファイル形式でデータの取り込みをサポートできます。これらの形式は、情報交換と処理を高速化し、標準化されたレポート形式で重要なセキュリティ関連情報の共有を促進します。

サポートされているファイル形式は、次のとおりです。

Common Vulnerability Reporting Framework (CVRF)

: Common Vulnerability Reporting Framework (CVRF) は XML ベースの言語です。Oracle、Red Hat、Cisco、Microsoft などの主要ベンダーは CVRF 形式をサポートしています。

Common Security Advisory Framework (CSAF)

: Common Security Advisory Framework (CSAF) は、JSON ベースの構造化された機械可読セキュリティアドバイザリーを提供するオープンソース標準です。Siemens、Red Hat、Hitachi、Schneider などの主要ベンダーは CSAF 形式をサポートしています。

CVRF または CSAF でサポートされているソリューション管理には、次の主要な機能が含まれています。

- セットアップアシスタントによる構成
- ファイルインポートによる CVRF または CSAF データのインポートのサポート
- CVRF または CSAF の URL による CVRF または CSAF のデータのインポートのサポート
- アドバイザリーによる CVRF または CSAF のデータのインポートのサポート
- 関連する脆弱性を含むソリューションのマッピング

脆弱性対応プラグインは、作成されたソリューションのメトリクスステータスを更新します。

ソリューションプロバイダーの構成方法の詳細については、「脆弱性ソリューションプロバイダーの構成」を参照してください。

脆弱性対応 を使用したパッチオーケストレーション

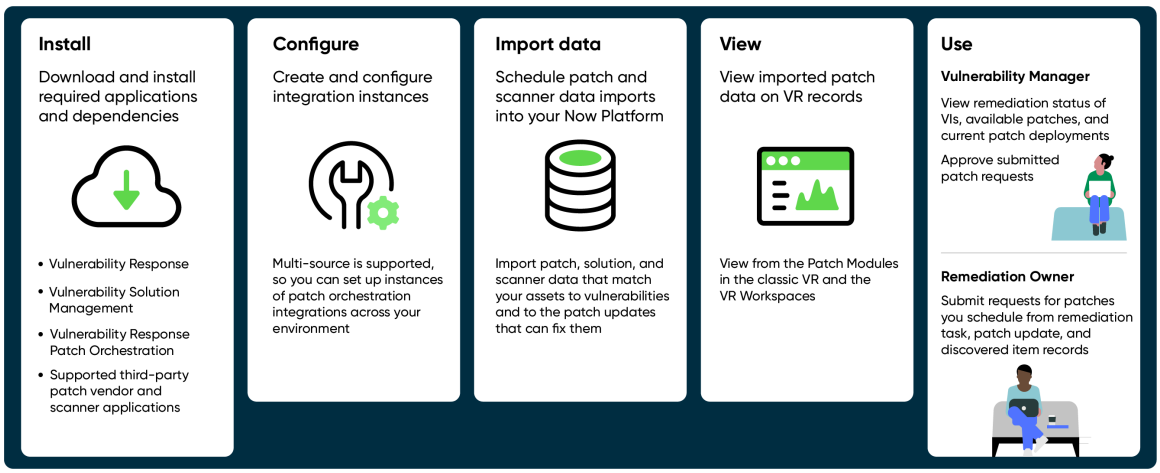
脆弱性対応 を使用したパッチオーケストレーションによって、大規模な資産グループの重大な脆弱性に対するパッチとパッチ展開を管理できます。脆弱性対応 パッチオーケストレーションとパッチオーケストレーションの統合は ServiceNow Store で入手可能です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性対応 を使用したパッチオーケストレーションについて

脆弱性対応 を使用したパッチオーケストレーションでは、サードパーティのソリューション統合、パッチベンダー、および脆弱性スキャナーからのスケジュール済みインポートのデータが使用されます。このデータは 脆弱性対応 アプリケーションで関連付けられます。このデータ編成により、脆弱性修復サイクルのステップを完了することができます。Now Platform インスタンス内からサードパーティのすべてのスキャナーデータを使用して、まず脆弱性を特定し、次にパッチと更新を適用し、最後に脆弱性一致アイテムをクローズします。



脆弱性対応 を使用したパッチオーケストレーションは、クラシック環境と 脆弱性対応 ワークスペースの両方でサポートされています。

ワークスペースでのパッチオーケストレーションの詳細については、「脆弱性対応 ワークスペースを使用したパッチオーケストレーション」を参照してください。

脆弱性マネージャー、アナリスト、IT 修復スペシャリストは、脆弱性対応 のパッチオーケストレーションを使用して、以下の修復タスクを実行できます。

- ソリューション (パッチ) を構成するパッチやベンダーのタイプに関する詳細なコンテキストと情報を確認します。
- 脆弱性対応 ワークスペースまたはクラシック環境にあるレコードから、脆弱性とソリューションのデータ、および脆弱性修復の進捗状況を表示および監視します。
- Windows、CentOS、macOS、Oracle、およびその他の資産に対して、定期的なスケジュールされた間隔で、サードパーティのソリューションベンダーによってサポートされているパッチを展開します。作業中のパッチとの競合を避けるために、営業時間外にパッチをスケジュールすることができます。
- サードパーティのスキャナーによって提供されたインポート済みの検出データを使用して、脆弱性があるがパッチ未適用の資産、またはスケジュール設定済みパッチによって正常に更新されなかった資産を特定します。
- 脆弱性対応 アプリケーションのパッチ更新、修復タスク、および検出されたアイテムレコードからの更新が必要な資産に対し、利用可能なパッチを開始およびスケジュールします。
- 修復スペシャリストによって送信されたパッチ適用要求に対するオプションの承認プロセスを使用して、パッチ展開を監視します。

主要な用語

構成アイテム (CI)

CI とは、構成管理データベース (CMDB) にリストされている既存の資産です。

脆弱性一致アイテム (VI)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

CMDB 内の既存の資産と一致するインポートされた脆弱性。脆弱性一致アイテム (VIT) は、VI の修復アクションを指定する特定の基準に従って、修復タスクまたはリストにグループ化されます。

インスタンス

ソリューションベンダーアプリケーションの個別のアカウントを指します。たとえば、各ユーザーアカウントは、HCL BigFix アプリケーションの 1 つのインスタンスである場合があります。この用語は、Now Platform® インスタンスの一意の安全な Web アドレスを意味します。

ソリューション

この統合のコンテキストには、潜在的と優先の 2 つのタイプのソリューションがあります。潜在的なソリューションは、脆弱性に対処する可能性があるソリューションです。脆弱性には多くの潜在的なソリューションがあります。優先ソリューションは、検出された特定の脆弱性に対して最も効果的なソリューションと一致します。

パッチ

脆弱性を修正するソフトウェア更新。パッチベンダーは、独自の名前をパッチに使用します。たとえば、HCL BigFix アプリケーションでは、パッチは Fixlet と呼ばれます。

優先パッチ

優先パッチは、特定の脆弱性を修正することを目的としたソフトウェア更新です。パッチが展開されると、特定の脆弱性に関連する脆弱性一致アイテムにマッピングされ、それらを修正します。

展開

この統合における展開とは、マシンにパッチを適用、開始、またはスケジュールする場合を指します。

Now Platform での展開は、マルチソースをサポートする統合を指す場合もあります。単一の統合の存在は、統合の展開と呼ばれます。展開とは、環境全体の統合と製品のことです。たとえば、お使いの環境にサードパーティのスキャナーやソリューションベンダー統合が複数展開されている場合があります。

パッチオーケストレーション統合に必要なアプリケーションと依存関係の利用可能なバージョン

- 脆弱性対応 アプリケーションと依存関係プラグイン、セキュリティサポート共通およびセキュリティサポートオーケストレーション。
- 脆弱性ソリューション管理®。
- ServiceNow® Store で入手可能な 脆弱性対応 パッチオーケストレーションアプリケーション。
- Vulnerability Response Patch Orchestration Integration with HCL BigFix、Vulnerability Response Patch Orchestration with Microsoft SCCM など、サポートされているサードパーティのパッチベンダーアプリケーション。
- サポートされている、脆弱性対応とのサードパーティスキャナー統合

必要なロール

ユーザーには、脆弱性対応 アプリケーションからデータを表示したり、パッチをスケジュールしたりするために使用している、パッチオーケストレーション統合に固有のロールが必要です。詳細については、以下に示す、使用しているサポート対象の統合に関する構成情報を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 脆弱性対応 との HCL BigFix パッチオーケストレーション統合の概要 および「The Vulnerability Response patch orchestration integration with Microsoft SCCM (Microsoft SCCM との脆弱性対応パッチオーケストレーションの統合)」。
- 脆弱性対応 ワークスペースとクラシック環境では、ユーザーにデータの表示を許可するがデータの編集は許可しない sn_vul_patch_orch.read_patch ロールが sn_vul.remediation_owner および sn_vuln.vulnerability_analyst ロールとともに継承されます。

  パッチベンダーへの接続を構成し、パッチをスケジュールするためにアサインする必要があるロールは、統合によって異なります。詳細については、「脆弱性対応 Patch Orchestration Integration with HCL BigFix の構成」および「Configure the Vulnerability Response Patch Orchestration with MS SCCM (MS SCCM との脆弱性対応パッチオーケストレーションの構成)」を参照してください。

パッチ要求の送信および承認のプロセスがアプリケーションに含まれています。デフォルトでは、Now Platform インスタンスの脆弱性対応パッチオーケストレーションアプリケーションでシステムプロパティ [**sn_vul_patch_orch.patch_approval_required**] がアクティブ化されています。

このシステムプロパティはアクティブ化されているため、パッチの展開がスケジュールされると、レビューおよび承認のために、レベル 1 - パッチ更新承認グループにアサインされたユーザーに送信されます。sn_vul_patch_orch.configure_patch ロールを持つユーザーに承認なしでパッチをスケジュールするように設定する場合は、 [**sn_vul_patch_orch.patch_approval_required**] プロパティを無効にできます。スケジュールされたパッチが通常の作業時間と競合しないように、承認をアクティブ化しておくことをお勧めします。承認システムプロパティを無効にすると、sn_vul_patch_orch.configure_patch ロールを持つすべてのユーザーが、レビューおよび承認なしでパッチをスケジュールおよび展開できます。

詳細、およびこのシステムプロパティを非アクティブ化する方法については、サポートされている統合の構成トピックを参照してください。

- 脆弱性対応 Patch Orchestration Integration with HCL BigFix の構成。
- Vulnerability Response Patch Orchestration with Microsoft SCCM 統合の構成。

脆弱性対応 レコードからのパッチ適用のスケジュール

修復スペシャリストは、脆弱性対応 アプリケーションのレコードから、脆弱性一致アイテムを解決するためのパッチ更新をスケジュールし、修復の進行状況を監視することができます。

次のレコードからパッチをスケジュールできます。

- パッチ更新
- 修復タスク
- 検出されたアイテム

脆弱性対応 のアクティブな **VI** 数をロールアップするレコード

すべての脆弱性に対してすべてのパッチをロールアップすることでパフォーマンスの潜在的な問題が発生しないように、変更を取得するスケジュール済みジョブでは、アクティブな VI 数のみを変更します。こうしたカウント変更と関連データは、脆弱性対応 アプリケーション内の以下のレコードにロールアップされます。

- VIT (脆弱性一致アイテム)
- RT (修復タスク)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 脆弱性ソリューション
- パッチ更新

パッチデータの表示とレコードへのパッチデータのロールアップ、およびソリューションなしのパッチの表示の詳細については、以下のトピックを参照してください。

- 脆弱性対応 のパッチオーケストレーションでのパッチデータとステータスのロールアップ。
- 脆弱性対応 でのパッチデータの表示とパッチ適用のスケジューリング。
- 脆弱性対応 でのソリューションのないパッチの表示。

パッチによる脆弱性一致アイテムの一括編集

パッチが用意されているクラシック環境の脆弱性一致アイテムを一括で編集できます。一括編集の動作の詳細については、「脆弱性対応 での脆弱性一致アイテムの一括編集」を参照してください。一括編集用に選択されたすべての VI に対する優先パッチ。この編集オプションは、選択したすべての VI に優先パッチがマッピングされている場合にのみ機能します。

例外管理の概要

公開されている脆弱性管理やセキュリティポリシー、標準、指針に組織が準拠できない場合は、例外を要求できます。例外管理では、ポリシーに従って修復できない脆弱性一致アイテム (VI) または修復タスク (RT) に対する例外を要求、レビュー、承認、または却下します。

一部の脆弱性には、既存のパッチ、修正、またはソリューションがない可能性があります。例外が承認されるということは、脆弱性を修復しなかった場合の結果を認識し、同意していることになるため、リスクを受け入れているということでもあるのです。

例外のライフサイクル

例外の定義

例外は、VI または RT の修復を指定した期間保留することを要求するものです。たとえば、修復オーナーは、マシンにパッチが適用できない場合に例外を要求できます。

例外の要求

修復オーナーは、例外管理プロセスを使用して、VI または RT の免除を要求できます。例外承認者がこの要求を承認すると、VI または RT は [保留] ステータスに移行します。

例外要求を承認する

すぐに修正できない VI または RT は、脆弱性アナリストによってレビューされ、リスクが評価され、修正できるまでの保留が承認されます。例外要求の承認は 2 レベルワークフローにすることができます。第 1 レベルの承認者のみが存在する場合、例外を要求して承認できます。ただし、第 1 レベルの承認者がいない場合は、例外を要求できません。詳細については、「例外承認者の追加」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

- 脆弱性対応 v15.0 以降では、VR アプリケーションを初めて展開する場合は、例外管理のフローデザイナーがデフォルトで有効になります。既にワークフローを使用している場合は、フローデザイナーに更新できます。どちらの場合も、ワークフローに戻すことはできません。例外管理と誤検出の承認ルールを設定するには、「例外管理の承認ルールの構成」を参照してください。

  VI または RT の例外要求が承認されると、以下のアクションを実行できます。

  - 再オープン
  - 削除
  - [アサイン先] または [アサイン先グループ] フィールドの更新
- 脆弱性対応 v23.0 以降、[例外ルールステータス承認] ワークフローは廃止され、フローデザイナーの [例外ルールの承認] フローに置き換わりました。

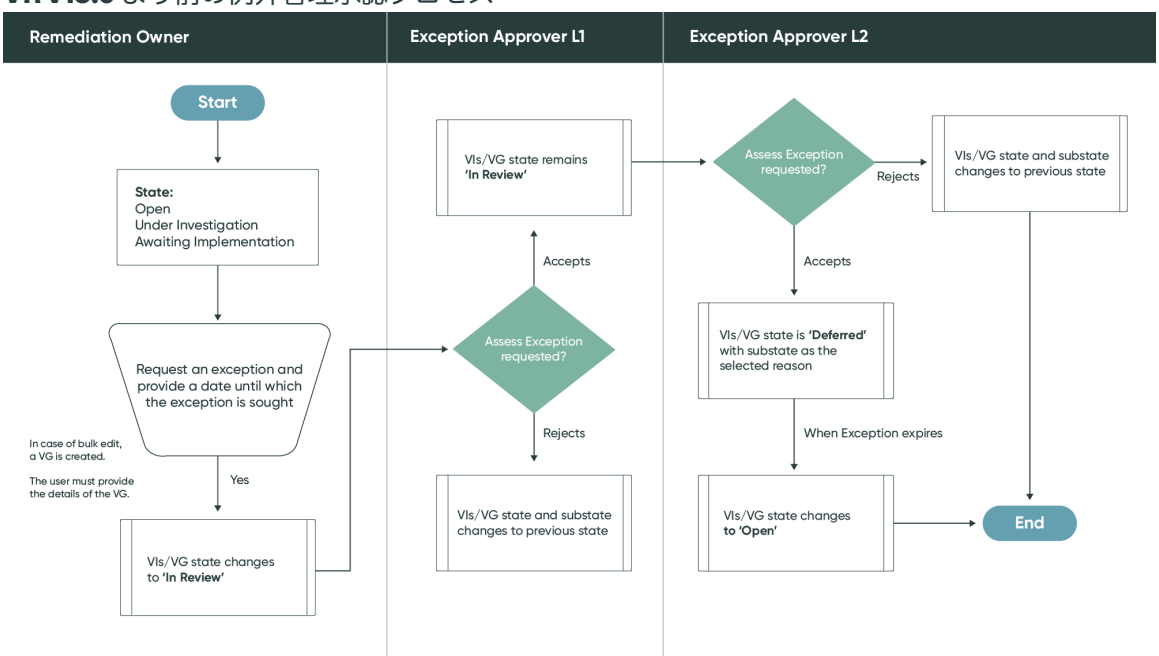
例外要求の追跡

例外を申請した後、VI または RT の [ステータス変更承認] タブを使用してそのステータスを追跡できます。RT に対してアクションが実行された場合、その RT の個々の VI のステータスを追跡することはできません。

例外要求の有効期限

特定の VI または RT に対する例外要求が期限切れになると、影響を受ける VI または RT は [オープン] ステータスに戻ります。

VR v15.0 より前の例外管理承認プロセス



単一の VI または RT 内のすべての VI が次のスキャンで合格すると、VI と、該当する場合は RT の [ステータス] フィールドが [クローズ済み] に変更され、サブステートは [修正済み] になります。

複数の保留

レコードまたは修復タスクが保留された回数が追跡されます。スケジュール済みジョブである *set deferral counts* は毎日実行され、VR の複数の保留モジュールの [保留数] 列で複数回保留されたレコードのカウントが提示されます。修復タスクが複数回保留された場合、修復タスクに関連付けられているレコードのすべてのカウントが収集され、提示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

関連情報

で修復タスクとレコードの例外を要求する Vulnerability Manager ワークスペース

IT 修復ワークスペースで例外を要求する

IT 修復ワークスペースで GRC: ポリシーとコンプライアンス管理 を使用して例外を要求する

例外ルールの概要

脆弱性対応 の例外ルールによって、脆弱性一致アイテム (VI) の保留プロセスを自動化できます。影響を受ける脆弱性、構成アイテム (CI)、または脆弱性一致アイテム (VI) を特定して、すぐに修正も保留もできない VI に対して例外を要求します。VI 保留プロセスを自動化することで、一致する VI が識別されたときにルールに基づいて VI を保留します。

組織での例外ルールの使用

例外ルールを使用すると、承認済みルールの条件に一致する場合に、新規および既存の VI を特定の期間自動的に保留できます。自動化により、手動操作がなくなるため、サービスレベルアグリーメントの欠落リスクが最小限に抑えられ、複数のアイテムの管理が容易になります。

保留ルールは順序付けに対応しているため、優先度が最も高いルールが最初に実行されます。優先度の高いルールが VI に適用されると、条件が VI と一致していても、後続のルールは再度適用されません。

注:

- 例外管理の構成で 脆弱性対応 を選択した場合にのみ、ルールを作成できます。詳細については、「脆弱性対応 の例外管理の設定」を参照してください。
- VI が例外ルールによって保留されると、作成された保留修復タスク (RT) にコピーされます。VI は、引き続き以前に属していた RT の一部です。

例外ルールのライフサイクルは次のとおりです。

- 例外ルールの作成
- 例外ルール要求の承認
- 例外ルールのアクティブ化
- 例外ルールの保留
- 例外ルールの有効期限

例外ルールの作成

例外ルールを作成して、定義された条件に一致する VI を、指定された期間自動的に保留できます。例外ルールを作成したら、承認のために送信します。

例外ルール要求の承認

例外ルール要求の承認は、2 レベルのプロセスで行われます。第 1 レベルの承認者のみが存在する場合、例外ルールは単一の承認により評価し、承認できます。しかし、第 1 レベルの承認者がいない場合は、例外ルールを承認できません。ルールが承認されると、修復タスク (RT) が作成されます。詳細については、「例外ルール要求を承認する」を参照してください。

注:

脆弱性対応 v15.0 以降では、VR アプリケーションを初めて展開する場合は、例外管理のフローデザイナーがデフォルトで有効になります。既にワークフローを使用している場合は、フローデザイナーに更新できます。どちらの場合も、ワークフローに戻すことはできません。例外管理と誤検出の承認ルールを設定するには、「例外管理の承認ルールの構成」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

例外ルールの要求が承認されると、次のアクションを実行できます。

- キャンセル
- 削除

例外ルールのアクティブ化

例外ルールが承認されると、デフォルトでは修復タスクが「保留」状態で作成されます。「有効期間開始日」以降、作成されたすべての VI と、ステータスが「クローズ済み」から「オープン」に移行した VI に対して、例外ルールが実行されます。

注:
[既存のデータで実行] オプションを有効にすると、スケジュール済みジョブは「有効期間開始日」に既存のデータに対して 1 回実行されます。

例外ルールの保留

この例外ルールで定義された条件に一致する VI は、ルールに定義された「保留期限」の日付まで保留できます。この日付になると、例外ルールに対して作成した修復タスクがクローズされ、このグループ内のすべての VI が「オープン」ステータスに戻ります。それらの VI にグループルールが再度適用され、必要な RT に割り当てられます。

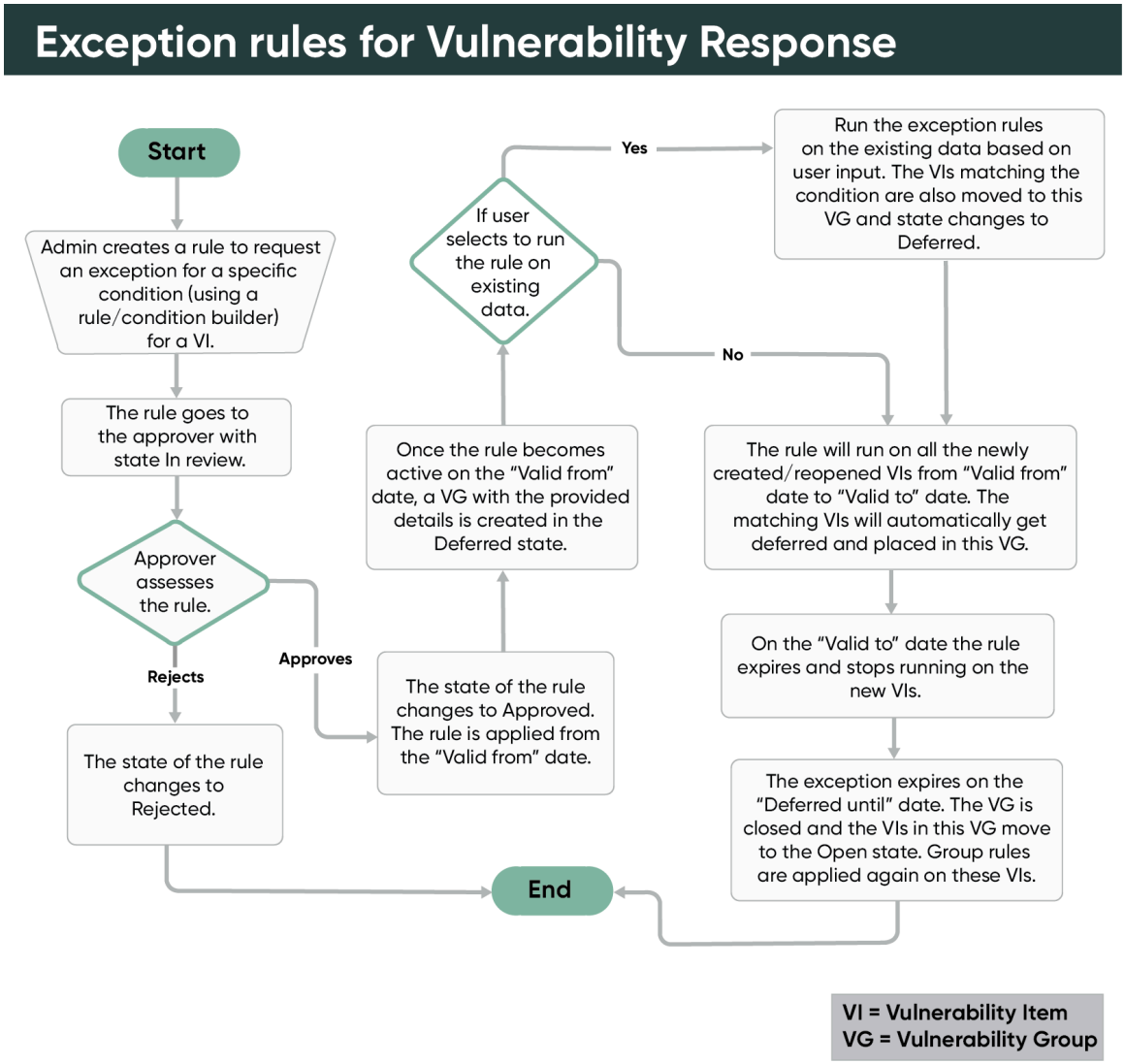
例外ルールの有効期限

例外ルールは、期限切れになると、新規または再オープンされた VI では実行されなくなります。関連付けられた RT は、「保留期限」の日付まで「保留」ステータスのままになります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

v15.0 より前の例外ルールのワークフロー



自動翻訳

除外ルールの概要

除外ルールは、脆弱性対応 での取り込みプロセス中に、脆弱性一致アイテム (VIT) に変換されないように検出をフィルタリングまたは除外する方法を提供します。

これらのルールは、次のようなさまざまなシナリオを処理するように設定できます。

- すぐに修正する必要のない、重大度またはリスクが低い脆弱性を除外します。
- アクションに対して最も重要な VIT に優先順位を付けることで、修復プロセスを改善します。
- VIT 変換から検出の割合を除外することで、データインポート中の処理時間を短縮します。

データを取り込むプロセスでは、新規検出と既存検出を処理するための異なるアプローチがあります。

- 新しい検出の場合：
  - 新しい検出が除外ルールの条件を満たさない場合、VIT を使用して検出が作成されます。
  - 新しい検出が除外ルールの条件を満たす場合、ルールは検出に関連付けられますが、VIT は作成されません。検出レコードの一致する除外ルールの参照を入力します。[除外ルール] 列には、それに応じて検出レコードの除外ルール参照が入力されます。
- 既存の検出の場合：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 検出が除外ルールの条件を満たさない場合は、通常のワークフローに進みます。
- 既存の検出が除外ルールの条件に一致する場合、その検出に関連付けられた VIT は現在のステータスのままですが、ルールは検出に関連付けられます。VIT のステータスは、*sn_vul.close_vit_with_excluded_detections* プロパティで定義された値によって制御されます。デフォルトでは、このプロパティの値は False に設定されています。値が False に設定されている場合、VIT の検出は除外され、VIT のステータスは現在のステータスのままになります。ただし、値が True に設定されている場合は、次のシナリオが発生する可能性があります。
  - VIT のすべての検出が除外されると、VIT のステータスは [クローズ済み (除外済み) (Closed Excluded)] に更新されます。

    注:
    脆弱性対応 の v22.1.2 以降では、[除外済み] という新しいサブステートが追加されています。

  - 1 つの検出が [クローズ済み] としてマークされ、残りの検出が除外されている場合、VIT は [クローズ済み (除外済み) (Closed Excluded)] として指定されます。
  - VIT にオープン検出がある場合、VIT はオープンのままになります。

関連情報

除外ルールを作成する

誤検出の概要

誤検出とは、スキャナーがシステムに脆弱性が存在することを報告したけれども、実際には脆弱性が存在しないという状況のことです。分類が間違っている、スキャナーのロジックまたはアルゴリズムが不適切であるなど、複数の理由が考えられます。修復オーナーは、脆弱性一致アイテム (VI) または修復タスク (RT) を誤検出としてマークできます。

重要:
Vulnerability Manager ワークスペース では、ホスト脆弱性一致アイテムを一括で誤検出としてマークすることができます。ホスト脆弱性一致アイテムを誤検出として一括でマークする方法の詳細については、「脆弱性マネージャーワークスペースで誤検出を一括編集」を参照してください。

誤検出のライフサイクル

誤検出の意味

実際には脆弱性がない場合でも、スキャナーが警告を表示することがあります。たとえば、構成アイテムが廃止されてもスキャナーでそのアイテムに関連する問題がまだ発生している場合は、誤検出としてマークします。

誤検出としてマーク

VI または RT を誤検出としてマークすることの詳細については、「誤検出としてマーク」を参照してください。

誤検出の処理

VI または RT が誤検出としてマークされると、ステータスは「クローズ済み」に更新され、サブステートは「誤検出」に変更されます。以下のアクションを実行できます。

- 再オープン
- 削除
- [期限] フィールドの日付の更新。この日付は、誤検出の有効期限として使用されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
承認されない場合、VI または RT は前のステータスに戻ります。

誤検出の承認

承認者は、承認ワークフローから誤検出を承認できます。

注:

脆弱性対応 v15.0 以降では、VR アプリケーションを初めて展開する場合は、例外管理のフローデザイナーがデフォルトで有効になります。既にワークフローを使用している場合は、フローデザイナーに更新できます。どちらの場合も、ワークフローに戻すことはできません。例外管理と誤検出の承認ルールを設定するには、「例外管理の承認ルールの構成」を参照してください。

誤検出の再オープン

誤検出サブステートの VI または RT はいつでも再オープンできます。

誤検出の追跡

[ステータス変更承認] セクションを使用して、誤検出のステータスを追跡します。承認されると、VI または RT のステータスが [クローズ済み] に更新され、その理由が [誤検出] になります。

誤検出の有効期限

誤検出の承認者のみが、VI または RT が期限切れになる、誤検出の期限日を設定できます。また、承認者が期限日を指定した誤検出のみが期限切れになります。この日付は、誤検出が承認された後に指定できます。

期限日のない誤検出は、永続的に誤検出となります。誤検出が期限切れになると、VI または VR のステータスが「オープン」に戻ります。

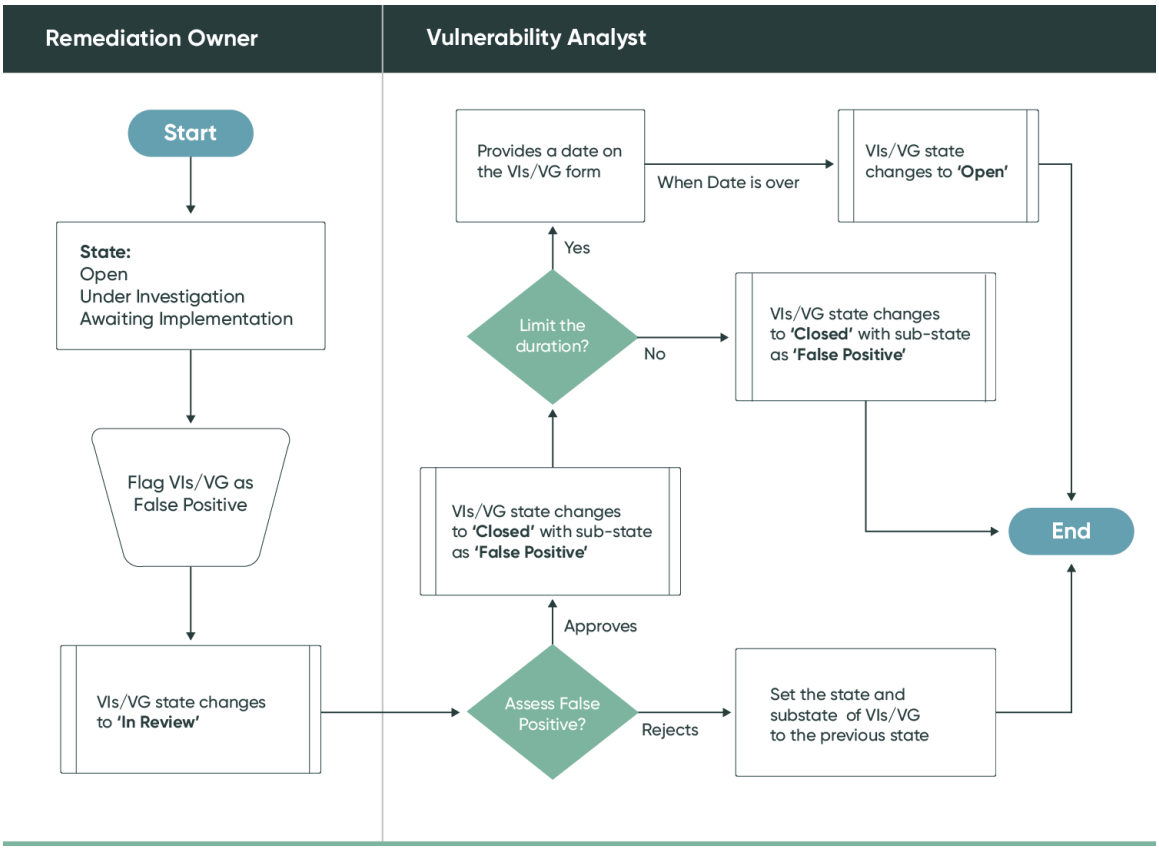
注:

脆弱性対応 の v21.0 以降では、誤検出と例外を承認する期間を設定できます。また、設定した日数経過後の承認者と要求者の両方に対するメール通知も可能です。要求が発生すると、脆弱性一致アイテムが [レビュー中] ステータスに変わり、ステータス変更レコードが作成されます。設定された期間内に承認者が応答しない場合、脆弱性一致アイテムまたは修復タスクは [オープン] ステータスに戻ります。以前のステータスは **[backup_state]** フィールドに保存されます。詳細については、「例外管理の承認ルールの構成」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

v15.0 より前の誤検出承認プロセス



すべての VI が次のスキャンに合格すると、承認プロセスは自動的に行われます。現在のステータスに関係なく、VI は自動的にクローズされます。VI または (該当する場合) RT の [ステータス] フィールドが [クローズ済み] に変わり、サブステートが [修正済み] になります。

詳細については、「誤検出のマークと承認」を参照してください。

関連情報

脆弱性一致アイテムまたは修復タスクの誤検出を要求する

脆弱性対応 の **WatchDog**

WatchDog は、指定した条件に基づいてテーブルを追跡するために使用されます。たとえば、脆弱性対応 での統合実行の失敗に関する詳細をログに記録するために使用できます。

以下のエラーに関する通知を受け取るように選択できます。この通知に基づいて、修正を計画できます。デフォルトの WatchDog は次のとおりです。

- 統合実行に失敗：統合実行の [ステータス] が [完了] に設定され、[サブステート] が [失敗] に設定されている場合、条件で 0 より大きいカウントが返される場合、つまり統合実行が失敗した場合に、ユーザーおよびユーザーグループに通知されます。
- 統合の長時間実行：統合実行が設定時間を超えているかどうかを確認するスクリプト。この WatchDog は、データ連携の実行の完了が遅れるたびに先回りしてアラートを送信します。
- 重複する定期的な実行:今後の発生時に引き続き実行される定期的な統合実行を確認するスクリプト。これらの統合実行のリストを含むリンクが生成されます。

ウォッチログ

WatchDog には、条件が満たされた回数を示すウォッチログが付属しています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

概要ダッシュボード

概要ダッシュボードを使用して、過去 30 日間の WatchDog を監視します。複数のウィジェットを作成すると、監視している他の WatchDog トピックを追跡できます。

脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で使用可能です。

> **注:**
> Tokyo を使用している場合は、Next Experience UI でダッシュボードを表示できますが、一部の機能が失われます。

レポート

名前	説明
過去 30 日間の WatchDog エラー	過去 30 日間に満たされたすべての条件。

詳細については、「WatchDog の構成」と「検出のエラー処理」を参照してください。

脆弱性対応 の変更管理

IT 修復オーナーは、脆弱性対応 アプリケーションの修復タスク (RT) から直接変更要求 (CHG) を作成および管理できます。変更要求は、修復タスクとそれに対応する脆弱性一致アイテムを修復できるように、資産に対する変更アクティビティを開始および追跡するのに役立ちます。

変更要求および脆弱性ワークフロー

脆弱性対応アプリケーションに精通していない場合、詳細については、「脆弱性対応アプリケーションの詳細」を参照してください。

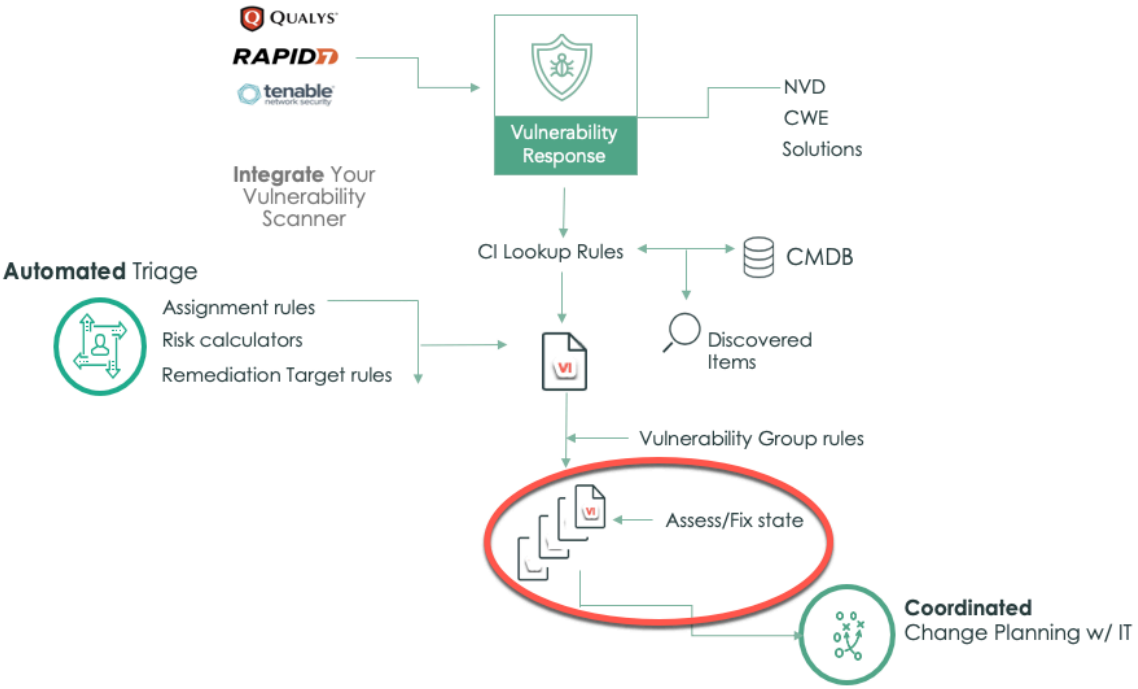
次の画像は、統合 (スキャナー) の設定から自動トリアージ、および調査に至るまでの 脆弱性対応 の情報フローを示しています。

変更要求と変更管理は、次の図に示す 脆弱性対応 のワークフローでの修復プロセス (評価/修正ステータス) に含まれています。このフェーズでは、変更要求を使用して脆弱性の修復を開始し、追跡できます。変更要求を修復タスクから直接作成および管理し、CMDB 内の構成アイテム (CI) の、影響を受ける資産のソリューションを含む、調査タスクおよび修復タスクを一覧表示できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応での変更要求



脆弱性対応での変更要求の使用タイミング

IT 修復オーナーは、CMDB 内のサポートされている構成アイテム (CI) を変更または削除するために何らかの手動制御のプロセスが必要な場合、修復タスクから変更要求を作成できます。修復タスクレコードから直接変更要求を作成して管理すると、脆弱性を迅速に調査して解決できます。解決済みの修復タスクの VI は、Now Platform での次回のスケジュール設定済みスキャン中にスキャンおよび検証され、脆弱性対応 ワークフローの自動トリアージに返されます。変更要求が必要になる可能性がある手動操作の例には、以下のようなものがあります。

- RT 解決前に脆弱性一致アイテムに対して必要なソフトウェアパッチ、修正、または IT によるその他のタスク。
- 修復タスクでの脆弱性一致アイテムのサブセットに、さらなる調査または別の部門への再アサインが必要であると判断した場合。
- 大量の脆弱性一致アイテムを含む、RT 内の脆弱性一致アイテムのサブセットを、新しい修復タスクに移動できると判断した場合。
- 修復タスクの重複を避けるために、修復タスクを既存の変更要求に関連付けることができる場合。

RT の変更要求のタイプ

脆弱性対応 アプリケーションは、Now Platform® インスタンスの ITSM 変更管理 製品によってサポートされている 3 つのタイプのサービス変更 (標準、緊急、および通常) を利用します。選択した変更のタイプにより、呼び出される状況モデルと、従う必要がある変更プロセスが決まります。変更要求では、変更の理由、優先度、リスク、変更のタイプ、変更カテゴリなど、変更に関する詳細情報が記録されます。「変更タイプ」を参照してください。

脆弱性対応 IT 修復オーナーは、通常、標準、および緊急の変更要求を修復タスクから直接作成するために、以下のオプションを使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 修復タスクからの事前設定された情報を含む変更要求を作成して、プロセスを簡素化し、時間を節約できます。
- 修復タスクを既存の変更要求に関連付けて、類似の情報や脆弱性一致アイテムを共有する重複した変更要求が作成されないようにすることができます。
- 一連の条件を使用して、脆弱性一致アイテムのサブセットを除外し、修復タスクを分割できます。選択したアイテムは自動的に新しい RT に移動されます。

修復タスクの任意のフィールドの値を使用して脆弱性一致アイテムをフィルタリングし、フィルター基準に一致するアイテムにのみ変更要求を適用できます。

関連情報

修復タスクからの変更要求の作成

既存の変更要求への修復タスクの関連付け

修復タスクの分割

変更要求と修復タスク間のステータスの同期

ソフトウェア資産管理 (SAM の基盤) を使用したソフトウェアエクスポージャーアセスメント

ServiceNow® 脆弱性エクスポージャーアセスメントアプリケーションを使用して、資産における特定のソフトウェアパッケージのインストール済みソフトウェアの合計数を判定します。ServiceNow ソフトウェア資産管理 (SAM) 基盤アプリケーションと併用すると、エクスポージャーを評価し、脆弱性一致アイテムを作成して、検出した脆弱なソフトウェアの修復を管理できます。

重要:
共通脆弱性識別子 (CVE) とソフトウェアによるエクスポージャーアセスメントを実行して、脆弱性アセスメントワークスペースの追加機能を活用できます。詳細については、「脆弱性アセスメントのワークスペースの詳細」を参照してください。

共通脆弱性識別子 (CVE) データベースを使用せずに、脆弱なソフトウェア情報 (公開者、製品、エディション、およびバージョン) を提供することで、脆弱なソフトウェアへのエクスポージャーを特定します。以下のケースについて、ソフトウェアに対するゼロデイ (当日) の脆弱性のケースを評価します。

- 製品に CVE データがまだない場合。
- 脆弱性が公知となってから NVD で脆弱性を含む CVE データが更新されるまでに遅延がある場合。
- 脆弱性スキャナーのスケジュール設定済みスキャン間の脆弱性について知りたい場合。

脆弱性エクスポージャーアセスメントアプリケーションでは、脆弱なソフトウェアの公開者と製品がわかっている場合、SAM の基盤 アプリケーションによって作成されたネットワーク内のインストール済みソフトウェアがリストされたレコードを使用して、悪意のある可能性があるソフトウェアパッケージへのエクスポージャーをオンデマンドで評価できます。

このタイプの脆弱性へのエクスポージャーの規模を知ることで、赤のアラートを実装してソフトウェアをアンインストールしたり、セキュリティオペレーションセンター (SOC) に特定のパッチを探すように通知したりして、積極的に対応できます。脆弱性一致アイテムを作成し、修復スペシャリストにタスクをアサインして、さらに調査修復を行うことができます。修復タスク (VUL) リストを表示して、必要な脆弱性一致アイテムが作成されて VUL に正しく関連付けられていることを確認します。

関連情報

脆弱性エクスポージャーアセスメントの構成

脆弱なソフトウェアへのエクスポージャーの評価

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性危機管理

脆弱性危機管理 (VCM) ワークフローで重大な脆弱性イベントを作成および追跡します。脆弱性アセスメントレコードを作成し、脆弱性のキーの属性を記録してリスクを計算し、アセスメントを実行してエクスポージャーレベルを特定し、脆弱性への調整された迅速な対応のためにステークホルダーを関与させます。

脆弱性危機イベントの管理

脆弱性危機管理は、脆弱性危機イベントを処理するための完全なワークフローであり、次の機能を備えています。

- 重大な脆弱性を、ソフトウェア資産管理 および ソフトウェア部品表 (SBOM) インベントリからのソフトウェアインストールインベントリ、スキャナーで報告された脆弱性、および 構成管理データベース (CMDB) と関連付けることで、脆弱な構成アイテムを効率的に特定します。
- アセスメント結果を修復のために脆弱性一致アイテムに変換します。
- 重大なセキュリティインシデントを開始して、脅威に迅速かつ協調的に対応します。
- 組織全体のチームと協力して取り組み、脆弱性への統一された対応を促進します。
- 部門横断型のステークホルダーや関係するチームに定期的なステータスレポートを提供し、危機全体にわたって透明性とコミュニケーションを維持します。

脆弱性アセスメントのワークスペースを使用した脆弱性危機管理

注:
脆弱性危機管理 v1.0.1 以降のアプリケーションはストアで個別のサブスクリプションとして入手できます。[脆弱性アセスメント] ワークスペースから脆弱性危機管理にアクセスできるのは、詳細なエンタイトルメントがある場合、またはストアからアプリケーションをインストールしている場合のみです。以前は、脆弱性危機管理は脆弱性緊急対応プラグインに含まれていました。v3.2.2 以降、「脆弱性緊急対応プラグイン」は「脆弱性エクスポージャーアセスメント」に名前が変更されました。

脆弱性イベントマネージャーは、関心対象となる脆弱性を特定すると、脅威インテリジェンスソース、脆弱性の特性、および影響を受ける製品に関する情報が含まれる脆弱性アセスメントレコードを作成します。この情報は、さらなる影響とエクスポージャーの分析に使用されます。

関心対象となる脆弱性のレコードが作成されると、リスクアセスメントが実行されます。このアセスメントは、構造化されたリスクスコアリング、レコードのレビュー、およびタスクを実行するアナリストの観察で構成されます。関心対象となる脆弱性の初期リスクスコアは、イベントの作成時に使用可能な属性を使用して計算されます。追加のインテリジェンスが使用可能になると、アセスメントのリスクスコアは変更される場合があります。リスクスコアを使用して、エクスプロイトの潜在的な影響を判断し、対応の優先順位を確立します。

関心対象となる脆弱性のアセスメントが作成され、組織のインフラストラクチャにリスクをもたらすと判断されたら、ソフトウェア資産管理、ソフトウェア部品表 (SBOM) インベントリ、スキャナーで報告された脆弱性、構成管理データベース (CMDB) などのソフトウェアインストールインベントリを使用した詳細なエクスポージャーアセスメントでリスクアセスメントを更新することで、脅威をさらに分析できます。影響を受ける構成アイテムとアプリケーションは、アセスメントによって自動的に特定されます。影響を受ける追加のアイテムは手動で追加できます。

アセスメントが完了すると、関連付けられた脆弱性一致アイテムがまだないエクスポージャー結果に対して、脆弱性一致アイテムまたはアプリケーション脆弱性一致アイテムを作成できます。脆弱性一致アイテムのリスクスコア算出を利用/構成して、脆弱性アセスメントレコードにリンクされた脆弱性一致アイテムのリスクスコアを調整できます。脆弱性アセスメントレコードには、エクスポージャーレベルとイベントの優先度を割り当てることができます。イベントの優先度に基づいて、脆弱性イベントマネージャーは、脆弱性アセスメントを提案、昇格、または重大なセキュリティインシデントにリンクすることを選択できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重大セキュリティインシデント管理 を使用して、修復アクティビティの追跡と管理、進行中のセキュリティインシデントのリンク、アドホックタスクの作成、影響を受けるチームの関与、ステータスレポートの送信、および 重大セキュリティインシデント管理 で利用可能なコラボレーション統合を使用したコラボレーションを行います。

ServiceNow® ソフトウェア資産管理 および ソフトウェア部品表 (SBOM) アセスメント - 処理ロジック

ソフトウェア資産管理 データを使用して、CVE の NVD からの CPE と、文字列一致ロジックを使用してディスカバリーモデルがフェッチされます。ディスカバリーモデルをフェッチした後、関連するインストールのスキャンが実行され、関連する構成アイテムがフェッチされ、[影響を受ける構成アイテム] テーブルに値が入力されます。公開者、製品、バージョン、エディションなどの詳細をさらに入力できます。これらに基づいて、レコードの一致するすべてのディスカバリーモデルとソフトウェアインストールがフェッチされます。その後、関連する構成アイテムがフェッチされ、[影響を受ける構成アイテム] テーブルに再度入力されます。

SBOM の場合、関連 (m2m) テーブル (CVE とソフトウェアの間) から、CVE に関連付けられているソフトウェアがフェッチされます。ソフトウェアの詳細を取得した後、SBOM コンポーネントの製品とバージョンを、識別されたソフトウェアの製品とバージョンと照合することによって、関連する SBOM コンポーネントが特定されます。

関連するコンポーネントが見つかると、コンポーネントに関連するエンティティがフェッチされます。エンティティからの製品モデルと、関連する CI (見つかった場合) がフェッチされ、構成アイテムが [影響を受ける構成アイテム] テーブルに保存されます。構成アイテムに脆弱性一致アイテムがない場合は、それを使用して脆弱性一致アイテムを作成できます。構成アイテムが見つからない場合、製品モデルは [影響を受けるソフトウェアモデル] テーブルに保存され、アプリケーション脆弱性一致アイテムを作成するために使用できます。

脆弱性危機管理ワークフローの使用の詳細については、「脆弱性アセスメントのワークスペースの使用」を参照してください。

関連情報

- 脆弱性アセスメントの詳細
- 脆弱性アセスメントのワークスペースの詳細
- [アセスメント] タブ

ドメインセパレーションと 脆弱性対応

ドメインセパレーションは 脆弱性対応 でサポートされています。 ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル：標準

- ベーシックレベルのサポートのすべての側面が含まれています。
- アプリケーションプロパティは、必要に応じてドメイン対応です。
- ビジネスロジック：サービスプロバイダー (SP) によって顧客ごとにプロセスを作成または変更できます。ユースケースには、単一のインスタンスでの複数のサービスプロバイダー顧客によるアプリケーションの正しい使用が反映されています。
- インスタンスのオーナーは、特定のアプリケーションに期待される通りに、テナントごとに MVP ビジネスロジックとデータパラメーターを設定できる必要があります。

サンプルユースケース：アドミンは、レコードを他のテナントに対してはクローズしないが、1 つのテナントに対してクローズする場合、コメントを必須にすることができる必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サポートレベルの詳細については、「アプリケーションでのドメインセパレーションのサポート」を参照してください。

脆弱性対応 におけるドメインセパレーションの仕組み

ドメインセパレーションによって、顧客ベース全体で VR (脆弱性対応) 手順を標準化し、運用コストの削減とサービス品質の向上を実現できます。

顧客データは、ワークフロー、ダッシュボード、レポートなどに別個の顧客ワークスペースを使用することで分離され、他のクライアントに公開されることはありません。

バージョンリリースごとの **Vulnerability Response** でのドメインセパレーションのサポート

リリース	サポートレベル	メモ
Orland	標準	
Paris	標準	
Quebec-	標準	
Rome	標準	
サンディエゴ	標準	
東京	標準	
ユタ	標準	
Vancouver	標準	
Washingtondc	標準	

脆弱性対応 アプリケーションのドメインセパレーションは、次の製品機能をカバーしています。

- サードパーティのスキャナー (Qualys、Rapid 7、Tenable など) から、正しいドメインで脆弱性一致アイテムをに取り込みます。データは、統合に使用される認証情報を持つ統合ユーザーと同じドメインに取り込まれます。
- 要求元のドメインの 脆弱性対応 から特定の資産を再スキャンします。
- CMDB CI ルックアッププロセスを使用して、スキャナーからの CI 情報が統合ユーザーのドメインの CMDB の CI と一致することを確認します。
- 統合ユーザーと同じドメインで定義されたリスクスコア算出に従って、脆弱性一致アイテムレベルでリスクスコアを計算します。
- 修復ターゲットルールは、統合ユーザーと同じドメインで定義された修復ターゲットルールに従って、脆弱性一致アイテムに対して実行されます。
- 修復タスクルールは、統合ユーザーと同じドメインで定義および維持することができます。
- 修復タスクルールを使用して作成された修復タスクは、グループルールが作成されたのと同じドメインに留まります。
- 保留ワークフローは、保留が要求された同じドメイン内の承認プロセスを通過します。
- レポートとダッシュボードには、脆弱性一致アイテムの経過時間、CI 別のオープンな脆弱性一致アイテム、影響度別の脆弱性、およびそれが属するドメインの修復ターゲット日状況など、脆弱性一致アイテムの各状況が表示されます。
- サードパーティのスキャナーや脆弱性情報データベース (NVD) データベースからのナレッジは、グローバルドメインに取り込み、複数のクライアント間でデータを共有できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
上記のすべてのケースでは、NOW Platform における分離されたドメインでの可視化の包括的な原則が適用されます。

ドメインセパレーションインポートを作成およびサポートする方法の詳細については、「統合のためのドメインセパレーションインポートの作成」および「バックグラウンドジョブフレームワークで複数のドメインを作成してサポートする」を参照してください。

ユースケース

脆弱性対応 アプリケーションは、脆弱性一致アイテムのライフサイクルをエンドツーエンドで管理します。次のユースケースはドメインセパレーションに対応しています。

- サードパーティ統合からの脆弱性一致アイテム (資産の脆弱性) の [取り込み]
  - 複数のインスタンスからデータを取り込む
  - 脆弱性一致アイテムの重複排除
  - CMDB CI と照合する
- リスクスコアと修復ターゲット日を使用した脆弱性一致アイテムの [拡張]
  - 資産の拡張 (CMDB)
  - リスクスコアと修復ターゲット日の拡張
- 脆弱性一致アイテムを [グループ化 **(Group)]** して、修復タスクにアサインする
  - 脆弱性一致アイテムを自動でグループ化する
  - 修復タスクを自動的にアサインする
- 修復
  - 修復タスク
  - 包括的な修復ライフサイクル
  - 保留ワークフロー
- 組織のセキュリティ体制と脆弱性管理プログラムの [測定 **(Measure)]**
  - 脆弱性の傾向、最も脆弱な資産、経過時間別の脆弱性
  - 修復ターゲット日別の修復ステータス

セットアップ

脆弱性対応 のドメインセパレーションを設定するには、追加の手順は必要ありません。インスタンスがドメインセパレーションされた後、すべての 脆弱性対応 テーブルで [ドメイン] 列が取得されます。脆弱性の統合インポートデータを特定のドメインに送信できます。詳細については、「統合のためのドメインセパレーションインポートの作成」を参照してください。

ドメインセパレーションデータ

データはドメインセパレーションできます。これは、次のことを意味します。

- サードパーティのスキャナーから取り込まれた脆弱性一致アイテムは統合ユーザーのドメインと同じドメインに留まり、他のドメインからはアクセスできません。
- あるドメイン内の脆弱性、脆弱性一致アイテム (インスタンス)、または資産を他のドメインから表示することはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- リスクスコアアルゴリズム、修復タスクルール、および修復ターゲットルールは、ドメイン外のユーザーは閲覧できません。
- NVD からの脆弱性情報はグローバルドメインに存在し、すべての顧客と共有できます。
- あるドメイン内の修復タスクは別のドメインから閲覧できません。
- あるドメインで作成された保留ワークフローを別のドメインで見ることはできません。
- すべてのメール通知は、属しているドメイン内に含まれます。

注:

インスタンスで利用可能なスケジュール済みインポートテンプレートは、デフォルトで [ドメイン:グローバル] に設定されています。したがって、インスタンスに複数のドメインがある場合の競合を回避するには、次の方法を調整します。

- 統合に含まれるドメイン数全体に、インスタンスで利用可能なインポートテンプレートを配布します。
- インポートテンプレートレコードのドメインをターゲットドメインのsys_idに更新します。
- 必要に応じて、各ドメインのインポートテンプレートを作成します。
- 各ドメインに 2 つのインポートテンプレートがあることを確認します。
- sn_vul_sched_import_pool:ドメインセパレーションがインスタンスに存在する場合、このテーブルレコードはドメインセパレーションする必要があります

脆弱性アナリストが自社のアプリケーションデータを管理する方法

- アナリストは、自分でアプリケーションインストール、マルチソースアプリケーション管理、および CI ルックアップルールを作成します。
- アナリストは、ドメイン内で使用するために特定の統合を構成できます。
- アナリストは、独自の保留および変更管理ワークフローを作成できます。
- アナリストは、独自の修復タスクルール、正確な脆弱性の優先順位付けを行うリスクスコアロジック、修復タスクの自動アサイン、正しいアサイン先グループへのアサインを作成できます。
- ドメインユーザーは、手動で脆弱性一致アイテムを作成した後、アイテムをクローズします。

インスタンスオーナーがドメインセパレーションできるビジネスロジックとプロセス

- 脆弱性対応 ユーザーとグループ
- 脆弱性対応 の統合
- 完全なセットアップ構成 (ユーザーとグループの管理、アプリケーションのインストール、マルチソースアプリケーション管理、CI ルックアップルール、修復タスクルール、リスク算出、修復ターゲットルールなど)
- 保留を含む完全な修復ライフサイクル
- スケジュールジョブ

関連情報

サービスプロバイダーのドメインセパレーション

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応でのサービスマッピング

サービスマッピングは、組織が IT インフラストラクチャとさまざまなコンポーネント間の関係を包括的に理解するのに役立ちます。これにより、サービス、アプリケーション、インフラストラクチャコンポーネントの自動検出とマッピングが可能になり、依存関係と関係が視覚的に表現されます。

脆弱性対応では、スケジュール済みジョブ *Set related CI services* によって、影響を受けるビジネスサービスと、脆弱性一致アイテム (VIT) に関連付けられた構成アイテム (CI) との間の接続を確立します。リンクプロセスは、統合インポートが完了した後、指定された時刻に実行されます。このスケジュール済みジョブのパフォーマンスを向上させるために、脆弱性対応の v21.1.2 以降でいくつかの変更が実装されています。それらは次のとおりです。

- リスクスコアの計算：リスクスコアの計算プロセスには、*Set related CI services* スケジュール済みジョブの使用が含まれます。CI が処理されると、このジョブは必要なデータを関連サービス [sn_vul_m2m_ci_services] テーブルに保存します。以前のコンフィグレーションコンプライアンスでは、リスク計算には、構成管理データベース (CMDB) アプリケーションプログラミングインターフェイス (API) *CIUtils* に直接アクセスして、インポート中に各テスト結果のサービスを取得する必要がありました。ただし、現在のプロセスでは、関連サービス [sn_vul_m2m_ci_services] テーブルからのスケジュール済みジョブの出力に依存して、コンフィグレーションコンプライアンスでリスクスコアを計算します。また、ベースシステムの算出は、関連サービス [sn_vul_m2m_ci_services] テーブルを利用するように変更されています。
- サービスのサイズ：*Set related CI services* スケジュール済みジョブに関連するシステムプロパティ *sn_sec_cmn.services_affected_by_CI_max_size* のサービス値が 1,000 から 500 に減少しました。
- サービスの深度：*Set related CI services* スケジュール済みジョブに関連するシステムプロパティ *sn_sec_cmn.services_affected_by_CI_max_depth* の深度が 10 から 5 に減少します。サービス値も 1,000 から 500 に減少します。
- CMDB クラスの除外：サービス計算をスキップする必要がある CMDB クラスを設定できるように、システムプロパティ *sn_sec_cmn.ignoreCIClassForService* が導入されました。ベースシステムでは、このプロパティは *cmdb_ci_unclassed_hardware*、*cmdb_ci_incomplete_ip*、*sn_sec_cmn_unmatched_ci* に設定されます。これらのクラスは脆弱性対応によって作成され、サービスマッピングがない場合があるためです。以前は、サービス計算は VIT に基づいて行われていました。ただし、代わりに検出されたアイテムを使用するようにロジックが変更されています。検出されたアイテムは、サービスの計算に使用され、同じテーブル内の CI に関連付けられます。
- サービスの完全な更新のためのスケジュール済みジョブ：サービスの完全な更新を実行するために、オンデマンドのスケジュール済みジョブ *Full refresh-related CI services for VI* が導入されました。脆弱性対応の v21.0 にアップグレードすると、ベーステーブルが脆弱性一致アイテムではなく検出されたアイテムを使用するため、*Set related CI services* ジョブの実行時間が最初は長くなります。そのため、ジョブは過去 90 日以内にスキャンされたすべての検出アイテムを処理する必要があります。さらに、より頻繁なサービス更新が必要な場合は、毎週の定期的な更新をスケジュールするか、完全な更新を実行することで対応できます。アクティビティを実行した結果、CI に関連付けられたサービスが変更され、脆弱性対応にこれらの変更を反映させる場合は、オンデマンドのスケジュール済みジョブ *Full refresh related CI services for VI* を実行できます。このジョブは、過去 90 日間に記録されたすべての検出アイテムを取得し、それに応じて関連サービスを更新します。

関連情報

Service Mapping

CIUtils - Global

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

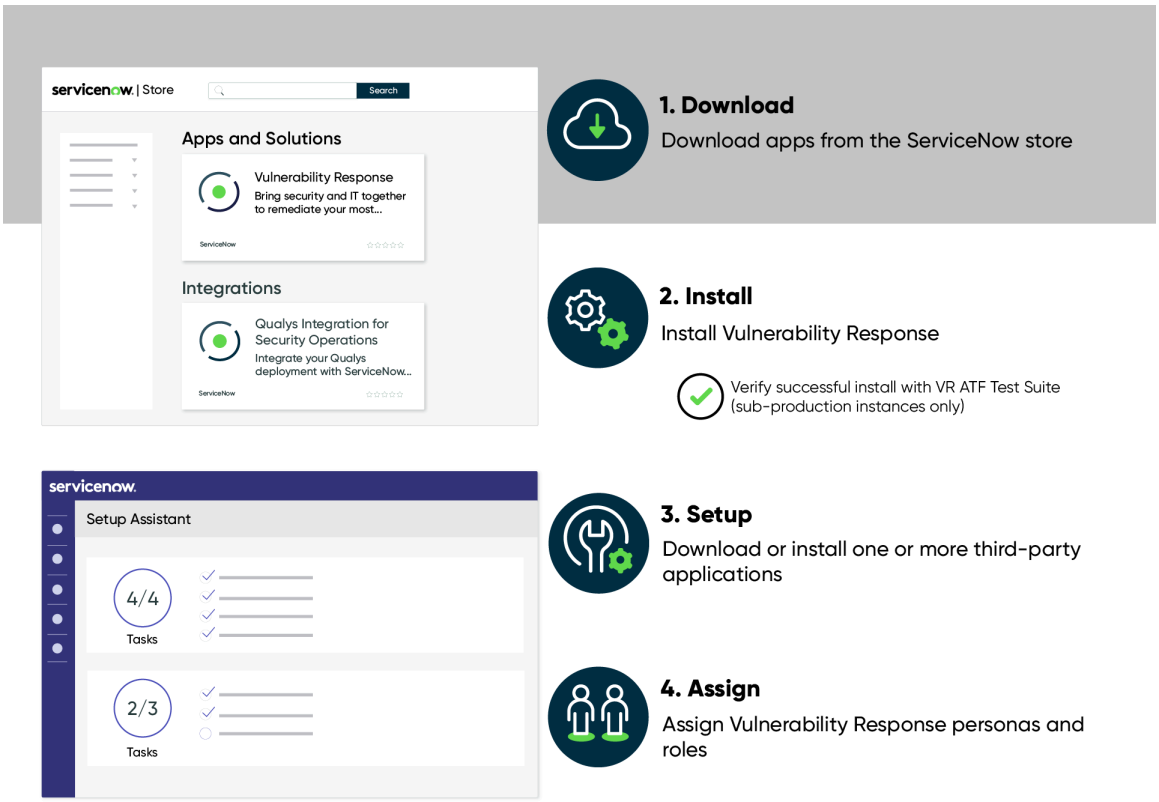
脆弱性対応 の実装

次の画像に示す手順に従って、脆弱性対応 アプリケーションを ServiceNow Store からダウンロードし、Now Platform インスタンスにインストールし、セットアップアシスタントを使用して構成します。

ベースシステム、脆弱性対応 アプリケーションとサードパーティのスキャナーアプリケーション、Qualys アプリケーションをインストールするためのインストールと構成の例を、この後の画像に示します。必要なロールと必須タスク、およびオプションの手順も一覧表示されています。

- 画像に示されている各ステップの詳細と、サポートドキュメントへのリンクを含むチェックリストについては、「脆弱性対応 アプリケーションの実装チェックリスト」を参照してください。
- この例で示されている概念と手順は、脆弱性対応 でサポートされている他のアプリケーションのインストールと構成に拡張できます。サポートアプリケーションのリストについては、「脆弱性対応 およびサポートされているアプリケーションのインストール」を参照してください。
- この例で使用する 脆弱性対応 アプリケーションと Qualys 脆弱性アプリケーションをダウンロードしてインストールするには、admin ロールが必要です。
- また、admin ロールは、脆弱性アドミン [sn_vul.vulnerability_admin] ペルソナおよびその他の脆弱性対応 ペルソナロールをユーザーとグループにアサインします。

アドミンタスク



sn_vul.vulnerability_admin ロールは、セットアップアシスタントで 脆弱性対応 および Qualys アプリケーションを構成し、予想される結果を検証します。

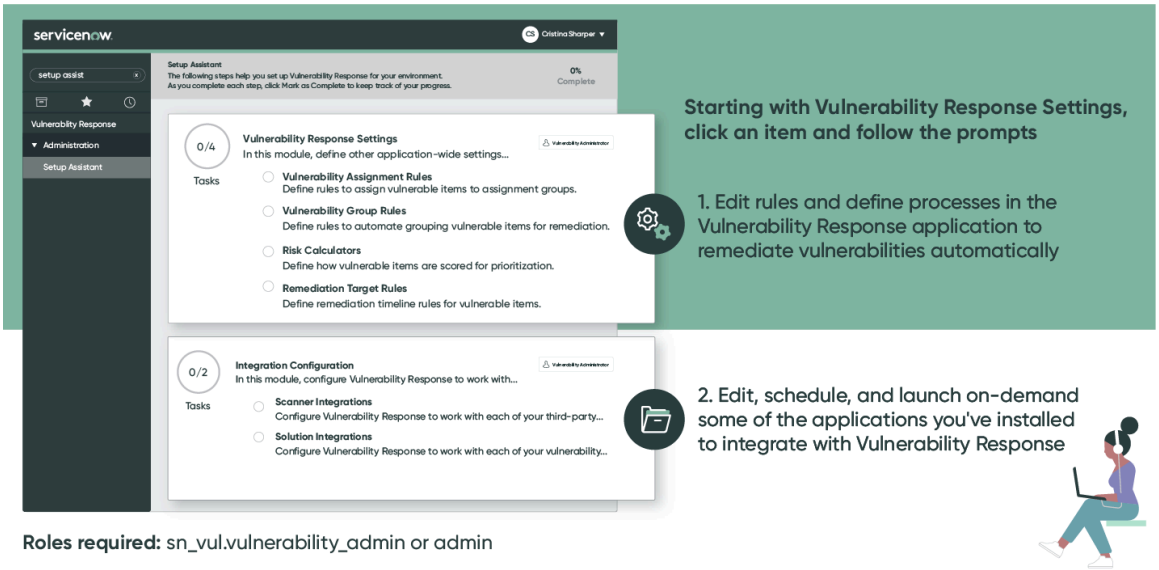
セットアップアシスタントの [脆弱性対応設定] セクション以降の手順とプロンプトに従って、インストールと構成を続行します。これらの設定を確認すると、環境のセットアップを続行する際に 脆弱性対応 のプロセスを理解および検証するのに役立ちます。

必要なロール：sn_vul.vulnerability_admin、または admin。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性アドミンのタスク



Roles required: sn_vul.vulnerability_admin or admin

以下のセクションで、 説明、デフォルト設定、およびアプリケーションとともにインストールしたデモデータを確認します。

- 脆弱性アサインルール - 脆弱性一致アイテム (VI) が適切なアサイン先グループに自動的にアサインされます。
- 修復タスクルール - 特定の条件に基づいてインポートされると、脆弱性一致アイテム (VI) が自動的にグループ化されます。
- リスク算出 - デフォルトのリスク算出が有効です。
- 修復ターゲットルール - VI および修復タスク (RT) の修復タイムラインを定義します。
- インストールしたサードパーティアプリケーションとインストール済みソリューションの設定を確認および編集し、データインポートの条件を定義します。サードパーティのアカウント情報を入力し、インポート設定、スケジュール、構成アイテム (CI) ルックアップルール、およびその他の設定を構成します。

詳細については、「脆弱性対応 アプリケーションの実装チェックリスト」を参照してください。

脆弱性対応 アプリケーションをカスタマイズまたは実装する際の詳細については、「KB1000704」を参照してください。

脆弱性対応 のインストール

Now Platform インスタンスで 脆弱性対応 アプリケーションを実行する前に、エンタイトルメントを取得して、ServiceNow Store からアプリケーションをダウンロードして Now Platform インスタンスにインストールし、セットアップアシスタントでいくつかのインストール手順を完了する必要があります。

始める前に

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

- インスタンスに必要な ServiceNow ロールがアサインされていることを確認します。
- インストールとロールの割り当てには、admin ロールが必要です。

自動翻訳

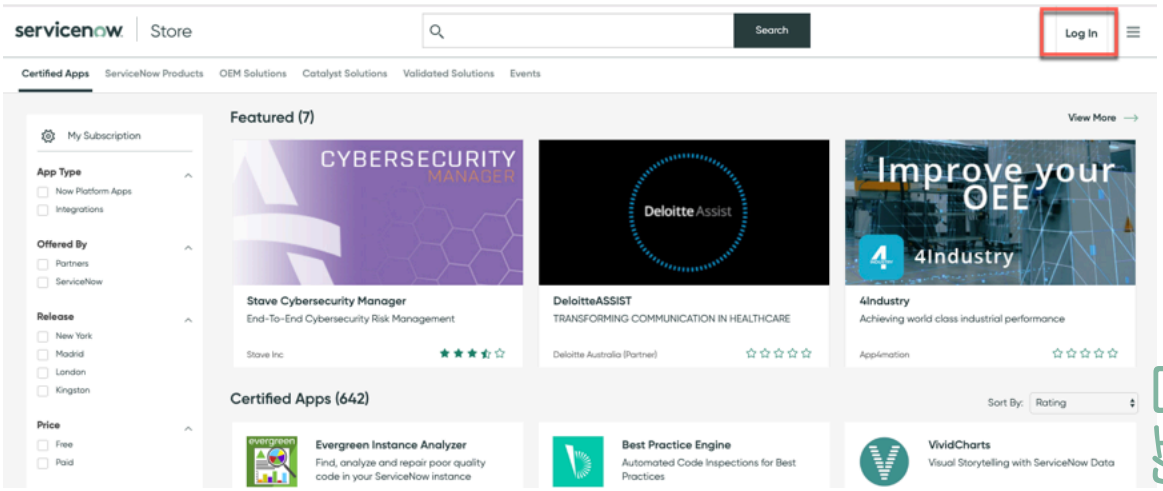
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

必要なロール：admin

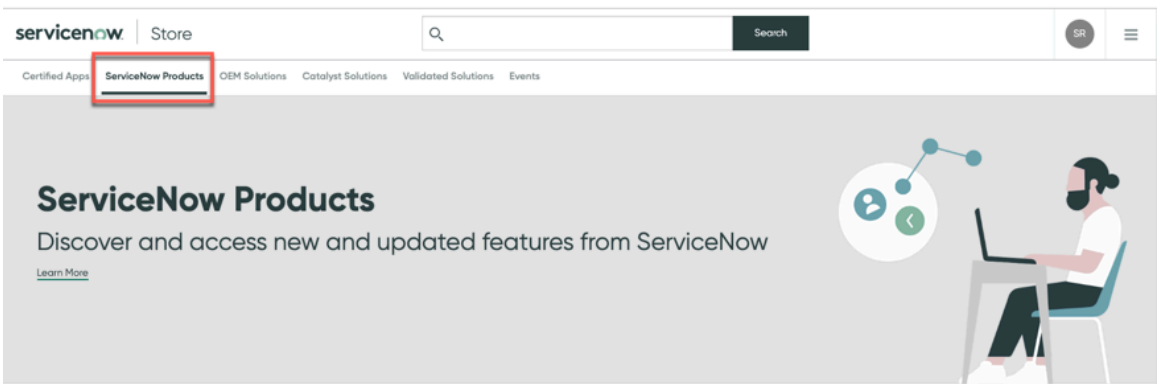
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

手順

1. エンタイトルメントを取得して 脆弱性対応 コアアプリケーションをダウンロードするには、ServiceNow Store に移動します。
2. ページ右上にある [ログイン] をクリックします。

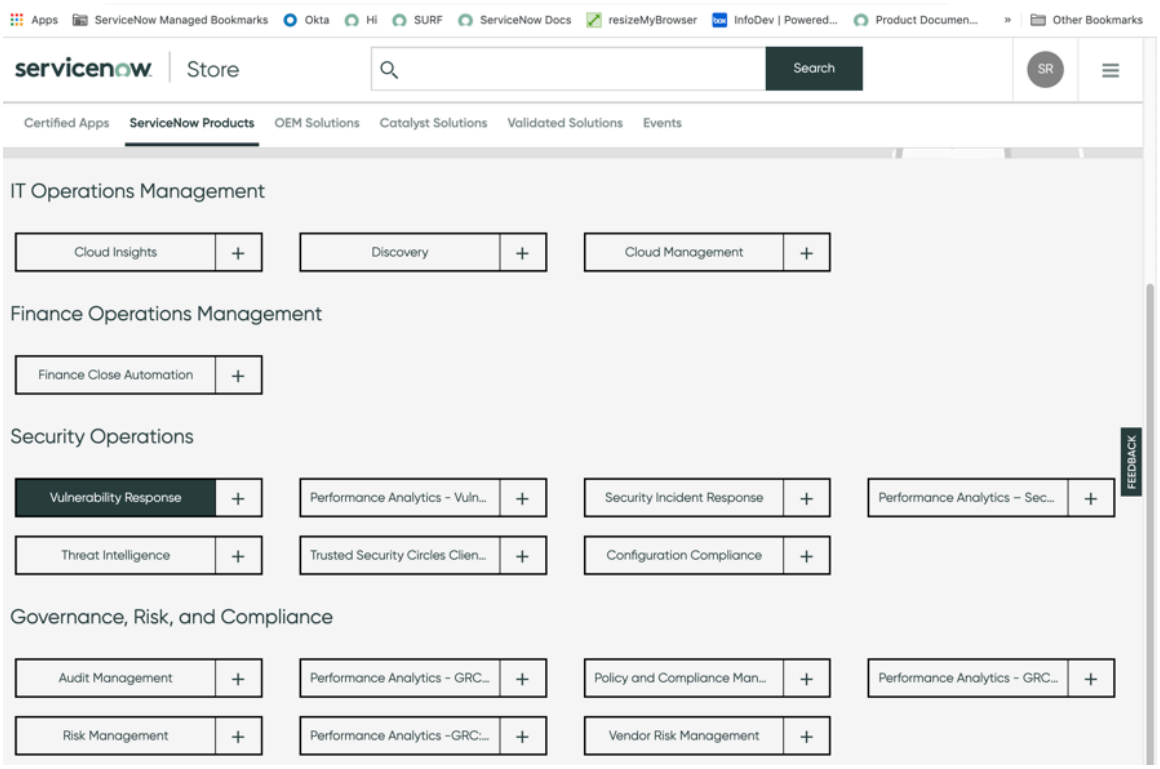


3. 表示されるダイアログで、HI 認証情報を入力し、[ログイン] をクリックします。
4. 表示されるページで選択されていない場合は、**[ServiceNow** 製品] タブをクリックします。

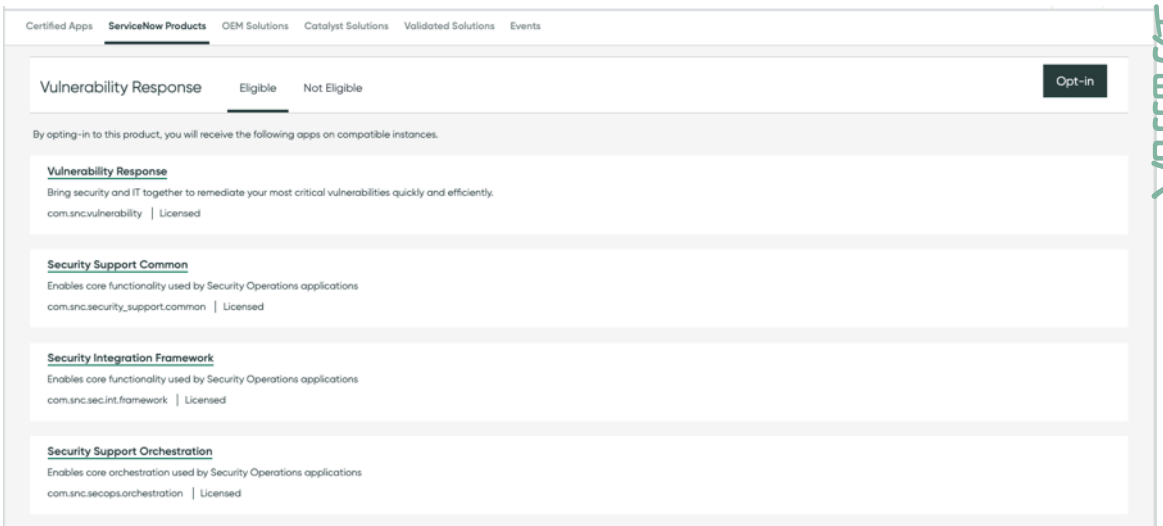


5. 脆弱性対応 アプリケーションの対象となる関連アプリケーションを表示するには、製品リストページで [脆弱性対応] 製品をクリックします。

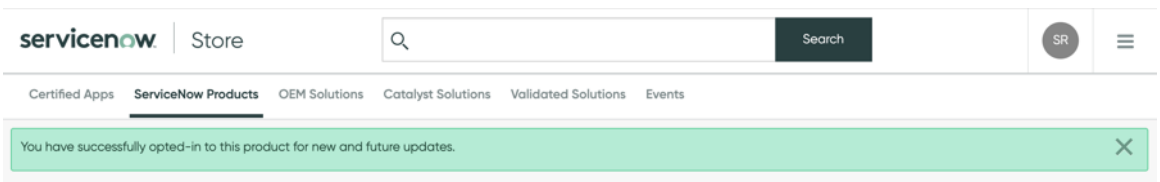
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[適格] タブには、オプトインした場合に利用できるすべてのアプリケーションが一覧表示されます。アプリケーションの詳細については、リンクをクリックしてください。



6. 脆弱性対応 コアアプリケーションを取得するには、[オプトイン] をクリックします。
7. 契約条件に同意するには、チェックボックスをオンにして [同意する] をクリックします。
   アプリケーションに正常にオプトインしたことを示すメッセージが表示されます。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

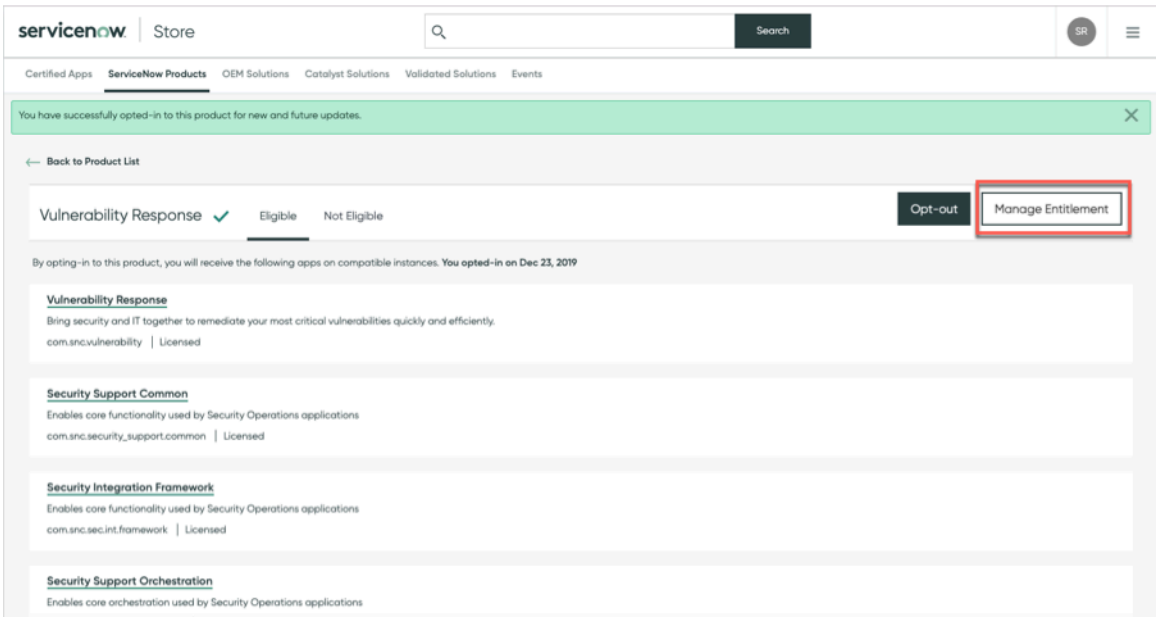
製品リストで [ServiceNow 製品] タブを選択して表示すると、次の図に示すように、脆弱性対応アプリケーションの右側のプラス記号が緑色のチェックマークに変わります。

製品リストページで、**[ServiceNow** 製品] タブのいずれかのアプリケーションの契約条件に同意し、エンタイトルメントを管理した後、プラス記号 (+) をクリックして、このページにある他のアプリケーションのエンタイトルメントとオプトインを 1 クリックで取得できます。

8. ステップ 10 に進んで、Now Platform インスタンスにアプリケーションをインストールします。
9. オプション: または、他の Now Platform インスタンスで 脆弱性対応 アプリケーションのエンタイトルメントを管理するには、次の手順に従います。

   a. [エンタイトルメントの管理 (Manage Entitlements)] ボタンが表示されていない場合は、製品リストの 脆弱性対応 アプリケーションをクリックして表示します。

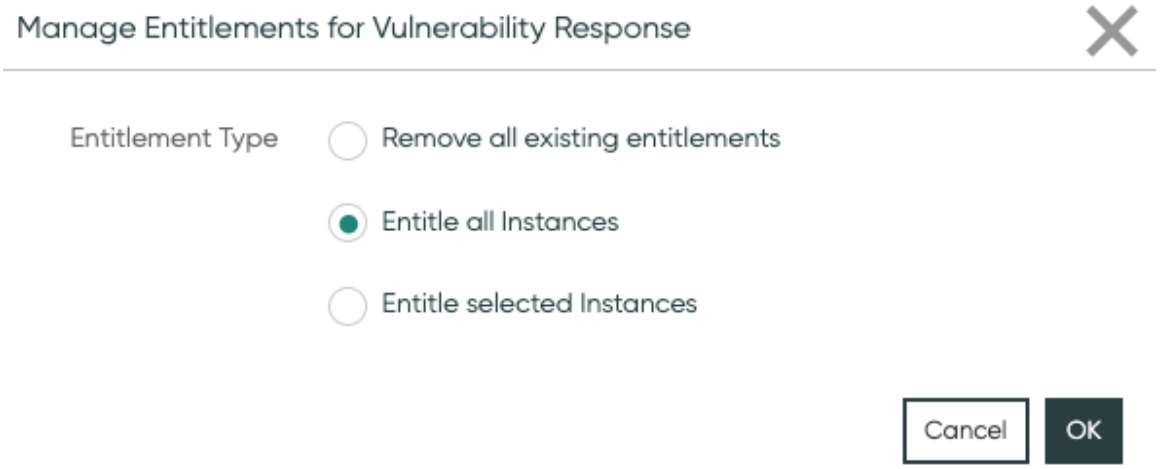
   b. [適格] タブを選択した状態で、[エンタイトルメントの管理 **(Manage Entitlements)]** をクリックします。



   c. 表示される [脆弱性対応のエンタイトルメントの管理 (Manage Entitlements for Vulnerability Response)] ダイアログで、次のいずれかを選択します。

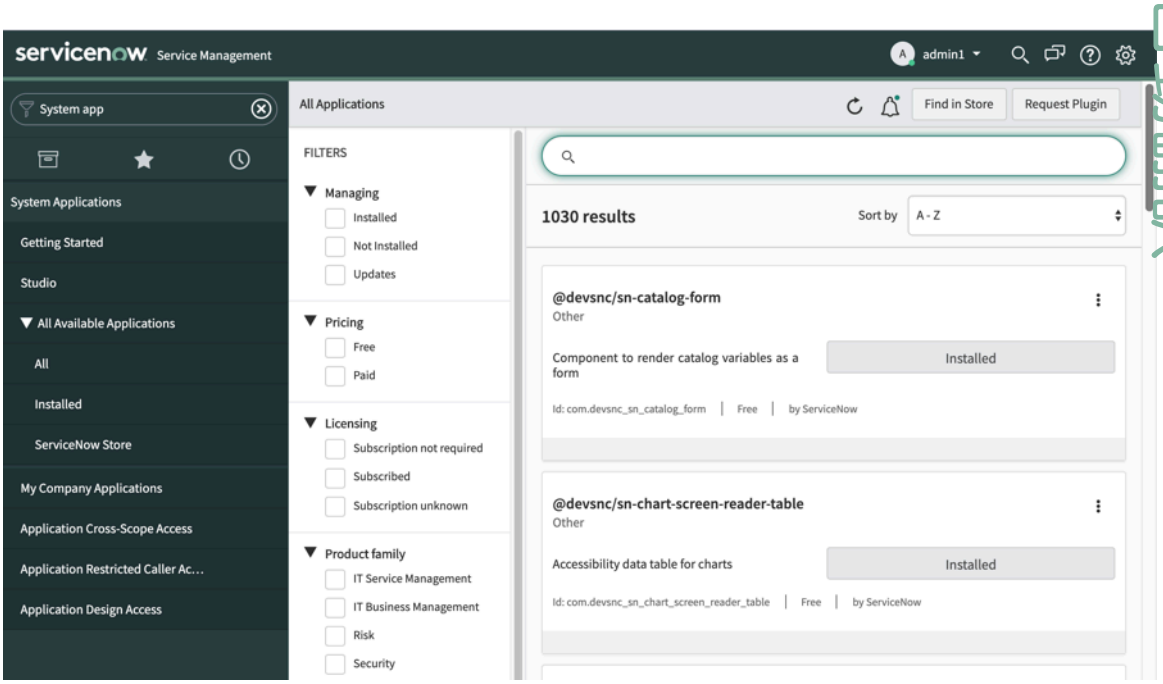
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



d. **[OK]** または [キャンセル] をクリックして続行します。
プラグインをアクティブ化して Now Platform インスタンスにアプリケーションをインストールする準備ができました。

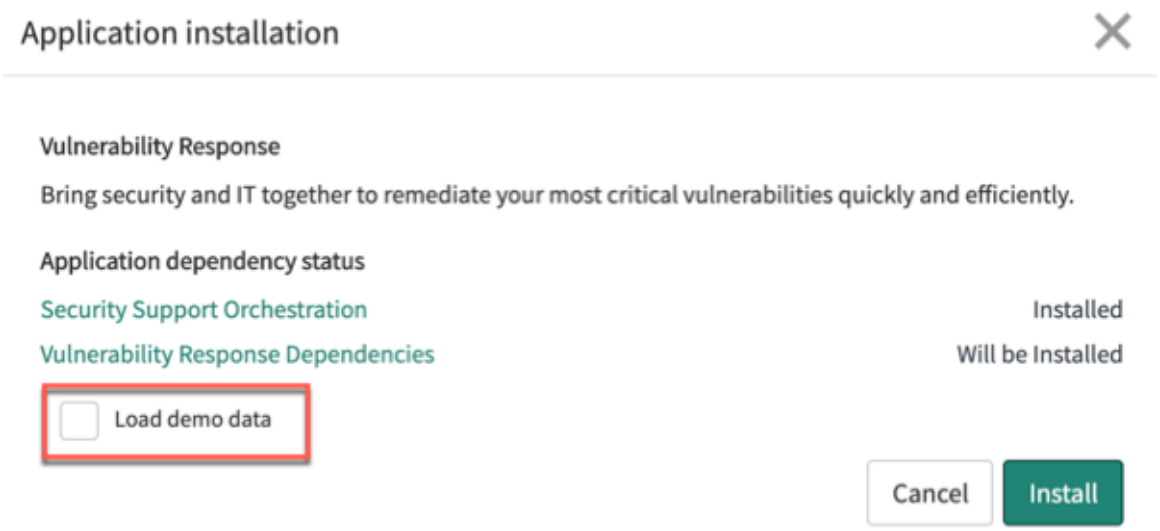
10. 脆弱性対応 アプリケーションをインストールする Now Platform インスタンスにログインします
11. 次のように移動する。 **All** (すべて) > システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて).



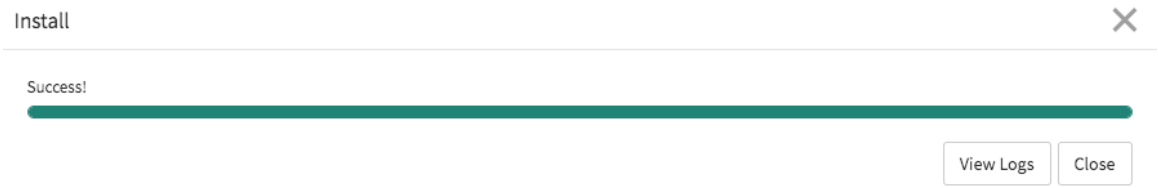
12. リストされたアプリケーションから脆弱性対応アプリケーション (sn_vul) を見つけ、選択リストからバージョンを選択して、[インストール] をクリックします。
[アプリケーションのインストール] ダイアログが表示されます。インストールされる依存関係が表示されます。
13. オプション: デモデータが必要な場合、[デモデータのロード] チェックボックスをオンにして、[インストール] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[デモデータのロード] チェックボックスをオンにしないと、後でアプリケーションマネージャーからデモデータをインストールできません。初期インストール後にデモデータをインストールまたは再インストールする方法については、Now Support ナレッジベースで「アプリケーションが既にインストールされている場合にデモデータをインストールする方法 [KB0722909] 」記事を参照してください。



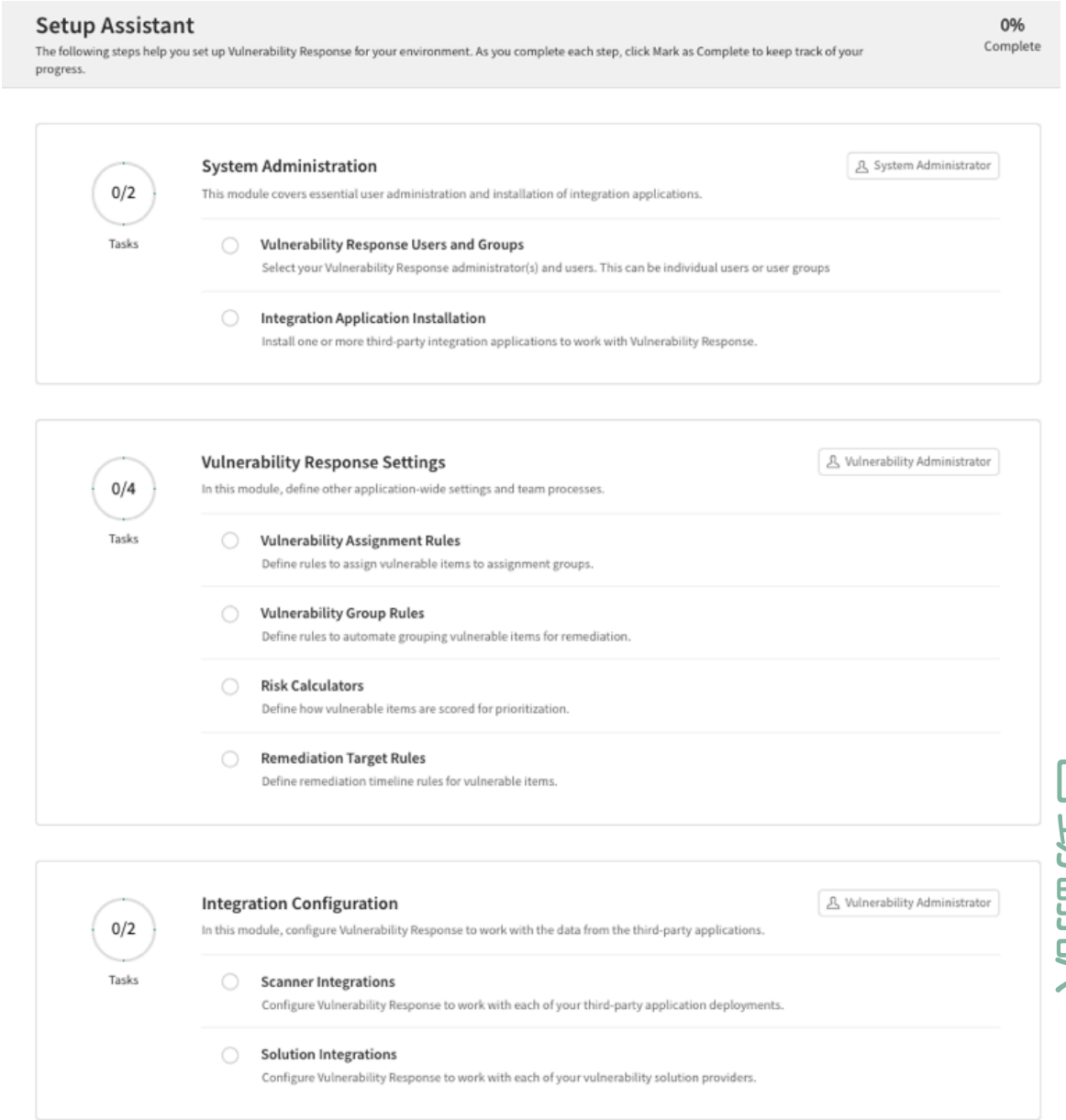
このインストールには時間がかかる場合があります。アプリケーションが正常にインストールされると、インストールダイアログにメッセージが表示されます。



14. **[Close** (終了)] をクリックします。
15. インストールが正常に完了したら、次に移動します: **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



16. 各セクションのフォームの指示に従います。

次のタスク
脆弱性対応 設定、アプリケーションのインストール、構成、統合、グループルール、リスク算出、および修復ターゲットルールの詳細については、「セットアップアシスタントを使用した 脆弱性対応 の構成」を参照してください。

脆弱性対応 とともにインストールされるコンポーネント

脆弱性対応 アプリケーションが有効になると、いくつかのタイプのコンポーネント (テーブル、ユーザーロール、スケジュール済みジョブなど) がインストールされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーションとともにインストールされるコンポーネントのフィルター済みリストの表示

脆弱性対応 の v24.0.6 以降、最も頻繁に使用されるシステムプロパティに 脆弱性対応 アプリケーション内でアクセスできるようになりました。これらのシステムプロパティを表示するには、次に移動します: **All** (すべて)脆弱性対応プロパティ.

アプリケーションファイルテーブルをフィルタリングして、アプリケーションとともにインストールされたロール、スケジュール済みジョブ、およびテーブルのみを表示します。これらのコンポーネントを表示するアプリケーションは、そのファイルがインスタンスとメタデータテーブルにロードされるようにインストールする必要があります。アプリケーションファイルテーブルからフィルター済みリストを表示するには、次の手順に従います。

1. フィルターナビゲーターで、「**sys_metadata.list**」と入力してメタデータテーブルに移動します。
2. 条件ビルダー (フィルターアイコン) を選択し、次を選択します。 アプリケーション > 次の値に等しい その後にアプリケーションの名前が続きます。たとえば アプリケーション > 次の値に等しい > 脆弱性対応.
3. 条件ビルダーで 2 番目のフィルターを追加するには、[**AND**] を選択してから次を選択します。 クラス > は をクリックし、リストから [ロール]、[スケジュール済みジョブ]、または [テーブル] のいずれかのクラスを選択します。
4. **[Run** (実行)] を選択します。

選択したクラスの結果がフィルター済みリストに表示されます。

インストールされるロール

注:
アプリケーション脆弱性対応 のロール、スケジュール済みジョブ、およびテーブルについては、「アプリケーション脆弱性対応 とともにインストールされるコンポーネント」を参照してください。

自動翻訳

ロールタイトル [名前]	説明	含まれるロール
sn_vul_prisma.configure_prisma_integration	sn_vul_prisma_hosts_importテーブルの CRUD + report_view 操作とsn_vul_prisma_host_attrbテーブルの report_view 操作を保護します。	
sn_vul.view_manager_workspace	ビュー Vulnerability Manager ワークスペース。	
sn_vul.delete	ソースレコード および脆弱性一致アイテムを削除します。v23.0 より前では、admin ロールにソースレコードを削除する権限がありました。	• sn_vul_cmn.delete • sn_vul.delete_vulnerab
sn_vul_cmn.delete	ソースレコードを削除	
sn_vulc.bulk_edit	テスト結果に対して一括編集操作を実行します。	
sn_vul.app_bulk_edit	アプリケーション脆弱性一致アイテム (AVIT) に対して一括編集操作を実行します。	sn_vul.app_write_all

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロールタイトル [名前]	説明	含まれるロール
sn_vul_container.container_bulk_edit	コンテナ脆弱性一致アイテム (CVIT) に対して一括編集操作を実行します。	sn_vul_container.write_a
sn_vul_cisa.configure_intelligence_integration	インテリジェンス統合を設定します。	
脆弱性マネージャーとシニアアナリスト [sn_vul.vulnerability_admin または sn_vul.admin (非推奨)]	プロパティと脆弱性統合を更新します。sn_vul.vulnerability_admin または sn_vul.admin (非推奨) ロールは、脆弱性統合、修復タスクルール、算出、および修復ターゲットルールに加え、タスク、レポート、およびサードパーティ統合構成を含む 脆弱性対応 管理に必要です。	• sn_vul.vulnerability_wr • sn_vul.ciso_write • sn_sec_cmn.admin • sn_vul_qualys.admin (C Vulnerability Integratio ルされている場合) • sn_vul_r7.admin (Rapi インストールされている • sn_vul_shodan.admin (Integration がインスト 場合) • sn_vul.configure_nvd_i (NVD 統合がインストー 合) • treemap_admin (パフォ ティクスアプリケーショ ルされている場合)
パッチオーケストレーション	サポートされているサードパーティのパッチベンダー統合を構成します。パッチデータとパッチレコードを表示して適用します。	• sn_vul_patch_orch.con パッチを構成して適用し • sn_vul_patch_orch.rea パッチレコードとデータ す。 • sn_vul_bigfix.configure BigFix パッチオーケスト ン統合アプリケーション す。このロールには、Bi ソールへのユーザーの接 る sn_vul_bigfix.read_i connection_admin 詳細 ています。 • sn_vul_sccm.configure このロールには、SCCM ルへのユーザーの接続を sn_vul_sccm.read_inte connection_admin 詳細 ています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロールタイトル [名前]	説明	含まれるロール
		• sn_vul_bigfix.read_inte このロールを持つユーザ は、Vulnerability Respo パッチオーケストレーシ ケーションのレコードお ケストレーションデータ り専用) できます。 • sn_vul_sccm.read_inte このロールを持つユーザ は、Vulnerability Respo Microsoft SCCM パッチ レーション統合アプリケ コードおよびパッチオー ンデータを表示 (読み取 す。
脆弱性アナリスト [sn_vul.vulnerability_write]	修復タスクと脆弱性一致アイテムを管理し、修正の進捗状況を監視するには、sn_vul.vulnerability_write ロールが必要です。	• sn_vul.read_all • sn_sc_cmn.write • sn_vul_qualys.user (Qu Vulnerability Integratio ルされている場合) • sn_vul_shodan.write (S Integration がインスト 場合)
V19.0：脆弱性イベントマネージャー [sn_vul_analyst.vul_event_manager]	sn_vul_analyst.vul_event_manager ロールは、新しい脆弱性またはソフトウェアの影響を評価する場合、または影響を受ける資産を特定して脆弱性一致アイテム (VI) を作成するためにゼロデイ脆弱性を追加する場合に使用されます。	• sn_sec_cmn.read • canvas_user • sn_vul_analyst.emerge • sn_vul.manage_exposu
その他 [sn_vul.read_all] sn_vul.vulnerability_read ロールは廃止されました。	脆弱性管理の可視化が必要なユーザーには、sn_vul.read_all ロールが必要です。たとえば、IT およびセキュリティ担当役員や、概要レベルのダッシュボードからダッシュボードのビジュアルを構成するアイテムにドリルダウンするユーザーなどです。 **重要:** 脆弱性対応 の v24.0.6 以降、sn_vul.read_all ロールにはVulnerability Manager ワークスペースにアクセスする権限があります。	• sn_sec_cmn.read • sn_vul_qualys.read (Qu Vulnerability Integratio ルされている場合) • sn_vul_shodan.read (S Integration がインスト 場合) • pa_viewer (パフォーマン クスアプリケーションが れている場合)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロールタイトル [名前]	説明	含まれるロール
		• sn_vul_tenable.read_in (Tenable 脆弱性統合がイれている場合) • sn_vul.view_manager_
sn_vul.read_assigned	自分または自分のアサイン先グループにアサインされた脆弱性一致アイテムを、クラシック UI と IT 修復ワークスペースの両方で表示します。 **重要:** 脆弱性対応 の v24.0.6 以降、sn_vul.read_assigned ロールにはIT 修復ワークスペースにアクセスする権限があります。	sn_vul.view_rem_worksp
VR システムインポートアドミン [sn_vul.vr_import_admin]	システム実行ユーザー。スケジュール済みジョブを実行します。 **注:** このユーザーは、各統合レコードのデフォルトの実行ユーザーです。変更することはできません。	• import_admin • sn_vul.vulnerability_wr
修復オーナー [sn_vul.remediation_owner]	自分または自分のグループにアサインされた脆弱性一致アイテム、修復タスクに対する権限を表示および更新します。すべての脆弱性とソリューションを表示できます。ソリューションレコードの内部メモフィールドへの書き込みアクセス権があります。	itil ロールに含まれていま
CISO および脆弱性担当役員 [sn_vul.vulnerability_ciso]	脆弱性対応のパフォーマンスアナリティクスの CISO ダッシュボードを表示します。	• sn_vul.ciso_read • sn_vul.read_all
誤検出承認者 [sn_vul.false_positive_approver]	誤検出要求を承認/却下します。	sn_vul.view_manager_wo
例外承認者 [sn_vul.exception_approver]	例外要求を承認/却下します。	sn_vul.view_manager_wo

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インストールされるスケジュール済みジョブ

スケジュール済みジョブ	説明
ホストおよびアプリモジュールの OOTB の保存済みフィルターを入力	ホストおよびアプリモジュールに関連するモジュールを移行します。
CC モジュールの OOTB の保存済みフィルターを入力	CC モジュールに関連するモジュールを移行します。
コンテナモジュールの OOTB の保存済みフィルターを入力	コンテナモジュールに関連するモジュールを移行します。
ホスト関連の保存済みフィルターをリフレッシュ	ホストモジュールの保存済みフィルターに関連するすべてのアグリゲートデータをリフレッシュします。
CC 関連の保存済みフィルターをリフレッシュ	CC モジュールの保存済みフィルターに関連するすべてのアグリゲートデータをリフレッシュします。
コンテナ関連の保存済みフィルターをリフレッシュ	コンテナモジュールの保存済みフィルターに関連するすべてのアグリゲートデータをリフレッシュします。
アプリ関連の保存済みフィルターをリフレッシュ	アプリモジュールの保存済みフィルターに関連するすべてのアグリゲートデータをリフレッシュします。
保存したフィルターに対して集計の作成と実行をトリガー	保存したフィルターに関連する集計を作成、更新、実行、およびリフレッシュします。
脆弱性対応 のバージョン 19.0 と Veracode 脆弱性統合の v4.0	Veracode CWE 統合は、脅威情報と修復の推奨のために Veracode 固有の共通脆弱性タイプ一覧 (CWE) データを取得します。 Veracode SBOM 統合は、ソフトウェアプロジェクト内のコンポーネントに関する Veracode で作成されたリリース、バージョン、および脆弱性の情報を取り込みます。この統合により、SBOM が CycloneDx JSON 形式で生成され、インスタンスにアップロードされます。 Veracode カテゴリ統合は、Veracode から拡張カテゴリデータを取得します。 Veracode DevOps 統合により、DevOps ユーザーは、SecOps ライセンスがなくてもサードパーティの脆弱性スキャンのサマリー詳細を表示できます。 Veracode 統合 (アプリケーション脆弱性一致アイテム、スキャンサマリー、アプリケーションリスト) のための JSON ベースの API。これらの統合の XML ベースの API バージョンは廃止されました。
既存の VI を自動例外ルールに関連付ける (Associate existing VIs with Auto Exception Rule)	自動例外ルールを既存の VI に自動的に関連付けます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みジョブ	説明
脆弱性検出を自動クローズ (Auto-Close Vulnerable Detections)	テーブル「sn_vul_auto_close_config」で定義された構成に基づいて、古い脆弱性検出を自動的にクローズします。
バージョン 16.1： HCL BigFix Collection、Fixlet、およびアクションの統合 (HCL BigFix Collection, Fixlet, and Actions Integrations)	HCL BigFix 製品のパッチを使用して、脆弱性に対するパッチとパッチ展開を管理します。
すべてのソリューションの関連数を計算 (Calculate Related Counts for All Solutions)	デフォルトでは非アクティブです。ソリューションデータを継続的に処理するのではなく、夜間に 1 回処理します。 v22.0 以降では、このジョブはオンデマンドでのみ実行できます。このスケジュール済みジョブはすべてのソリューションを処理するため、パフォーマンスに影響を与える可能性があります。そのため、ソリューションデータが破損している場合は、このジョブを一度だけ実行することをお勧めします。
脆弱性と修復タスクの関連 VI 数を計算 (Calculate Related VI Counts for Vulnerability and Remediation Task)	当日の手動および VI インポートによる変更をキャプチャします。脆弱性とソリューションの関係を調整し、合計を再計算します。 ソリューションデータは、[脆弱性ソリューションメトリクスキューの処理 **(Process Vulnerability Solution Metrics Queue)]** スケジュール済みジョブによって個別にキューに入れられて処理されます。
MID サーバータイムアウトの確認 (Check Mid-Server Timeout)	MID サーバーに ping を送信し、30 秒後にエラーで終了します。
V19.0：潜在的な脆弱性エクスポージャーのチェック (Check potential vulnerability exposure)	デルタ CVE、ソフトウェア、およびインストールを処理して、エクスポージャーを取得します。
実行状況 WaitComplete を確認 (Check Run State WaitComplete)	完全に完了したと確認された統合実行を完了としてマークします。
脆弱性一致アイテムとグループの保留の有効期限を確認 (Check Vulnerable Item and Groups Deferment Expiration)	脆弱性一致アイテムまたは脆弱性が期限切れになった場合 (および 1 週間以内に期限切れになる場合) に通知を送信します。 保留された VI に例外ルールが適用されるかどうかを確認し、例外ルールに従って [理由] フィールドと [期限 **(Until)]** フィールドを更新します。VI のステータスは、最新の有効期限まで [保留] のままです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みジョブ	説明
CI が関連付けられていないキャンセル VIT をクローズ (Close cancel VITs that do not have a CI associated)	構成アイテム (CI) が関連付けられておらず、3 日間更新されていない脆弱性一致アイテムを自動的にクローズします。ステータスは [クローズ済み]/[キャンセル] に設定されます。
期限切れレコード削除時に VI をクローズ (Close VI on exp record delete)	期限切れレコードが削除されると VI をクローズします。
コンプライアンス結果統合	テスト結果とともに、ポリシー、構成テスト (コントロール)、信頼できるソースの引用を、コンフィグレーションコンプライアンスアプリケーションで処理するためにインポートします。
コンプライアンス結果バックフィル統合	Tenable.io 資産統合とともに実行されるチェーン統合の一部では、検出された (資産統合によってインポートされた) 無視された資産の構成アセスメントデータをインポートします。
CR 状況の同期 (CR State Synchronization)	スクリプトで既存のすべての修復タスクと CHG の関係を改善して、同期されるようにします。今後の同期を有効にします。
バージョン 15.0 スキャン認証情報統合 (Version 15.0 Scan Credential Integration)	オンデマンドの再スキャンに備えてスキャナーへのアクセスに使用される Tenable.io 認証情報をインポートして一時的に安全に保存します。
CWE Comprehensive 2000 統合 (CWE Comprehensive 2000 Integration)	MITRE Corporation によってキュレーションされた、共通脆弱性タイプ一覧 (CWE) データセットから脆弱性情報を取得する脆弱性統合。
V18.0：古い分割アクションレコードの削除 (V18.0: Delete Stale Split Action Records)	分割タスク中間テーブルの古いレコードをクリーンアップする日次ジョブ。
ソリューションアプリケーションがアクティブでない場合は VR ソリューションを無効にする (Disable VR solutions when solutions application not active)	脆弱性対応のソリューション管理アプリケーションがインストールされていない場合は、脆弱性ソリューション管理 機能を無効にして非表示にします。
修復ターゲットを評価 (Evaluate remediation targets)	すべての脆弱性一致アイテムの修復ターゲット日を設定または更新します。ルールに対する修復ターゲット日のステータスを決定します。
• Rapid7 の更新されたキーの検出の修正 (Fixing the detections for updated key for Rapid7) • Qualys の更新されたキーの検出の修正 (Fixing the detections for updated key for Qualys) • Tenable の更新されたキーの検出の修正 (Fixing the detections for updated key for Tenable)	脆弱性対応 へのアップグレード後にトリガーされる統合固有のスケジュール済みジョブによって、検出データを自動的にクリーンアップします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みジョブ	説明
バージョン 16.1：修正ダイジェストを生成 (Version 16.1: Generate remediation digest)	このジョブは、修復オーナーユーザーグループ内のユーザーに対してメールダイジェストを自動的に生成します。ジョブは、デフォルトでアクティブ化されます。
V19.0：CISA で悪用された CVE をエクスポージャー構成に挿入 (Insert CISA exploited CVE to exposure config)	エクスポージャー構成 (Exposure Configuration) テーブルに CISA CVE を挿入してエクスポージャーを計算します。
V18.0：統一された修復タスクにクラシック修復タスクを挿入 (V18.0: Insert Classic Remediation Tasks Into Unified Remediation Task)	クラシック UI で作成されたすべての修復タスクを統一された修復タスク (sn_vul_remediation_task) に挿入するための 1 回限りのスケジュール済みジョブ。
Microsoft Security Response Center ソリューション統合 (Microsoft Security Response Center Solution integration)	Microsoft セキュリティレスポンスセンター からソリューションを取得する 脆弱性ソリューション管理 統合。
バージョン 16.1：Microsoft SCCM コレクション、パッチ更新、および展開の統合 (Version 16.1: Microsoft SCCM Collection, Patch Update, and Deployments Integrations)	Microsoft SCCM パッチを使用して、脆弱性に対するパッチとパッチ展開を管理します。
スロットル済み統合プロセスを取得 (Pick up throttled integration process)	Shodan Exploit Integration の統合プロセスを作成します。
影響を受ける製品のテキストを入力 (Populate affected products text)	アップグレード後、既存のソリューションを処理して影響を受ける製品のテキストを入力します。このジョブは 1 回のみ実行されます。
新しい CR カウント列を入力 (Populate new CR Count Column)	修復タスク [sn_vul_vulnerability] テーブルの既存のデータを使用して、お客様の新しい CR カウント列を自動的に入力します。
脆弱性ソリューションメトリクスキューを処理 (Process Vulnerability Solution Metrics Queue)	キューに格納されたソリューションデータを次の方法で処理します。 • NVD エントリーからサードパーティエントリーへのソリューションのロールアップ • 脆弱性に対する優先ソリューションの入力 • ソリューションの修復ステータスメトリクスの更新 さらに、更新ステータスとしてマークされたソリューションも処理します。 **注:** Rapid7 のみを使用している場合は、このスケジュール済みジョブを無効にしてパフォーマンスを向上させることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みジョブ	説明
脆弱性ベンダーマッピングテーブルにレコードを入力 (Populate records in vulnerability vendor mapping table) Rapid7 脆弱性に対する脆弱性ベンダーマッピングテーブルにレコードを入力 (Populate records in vulnerability vendor mapping table for Rapid7 vulnerabilities)	既存の脆弱性に対する脆弱性の脆弱性ベンダーマッピングテーブルにレコードを挿入します。
保留された脆弱性グループを再オープン (Re-open deferred vulnerability groups)	保留期限日が過ぎたときに保留された修復タスクを再オープンします。
すべての脆弱性アサインルールを再適用 (Reapply all vulnerability assignment rules)	すべてのオープン VI に対してアサインルールを再評価します。
バージョン 16.5：アサインルールの再アサイン回数 (Version 16.5: Reassignment count for assignment rules)	毎日実行され、この機能によって特定のアサインルールに対してアサインされていない VI と修復タスクの合計数を提示します。
Red Hat Solution Integration	Red Hat Security Advisory からソリューションを取得する 脆弱性ソリューション管理 統合。
V17.1：修復タスクの重複 VIT をリフレッシュして解決 (V17.1: Refresh and resolve duplicate VITs on remediation task)	「重複 VI を自動的にリフレッシュ」がアクティブな修復タスクのアイテムについて、重複する脆弱性一致アイテムを特定します。
非修復タスクルールベースの修復タスクの関連する脆弱性一致アイテムをリフレッシュ (Refresh associated vulnerable items for non-remediation task rule-based remediation task)	脆弱性一致アイテムがフィルターグループと条件グループの基準に一致する修復タスクを更新します。
前回オープンおよびクローズされた誤った脆弱性一致アイテムを修正 (Repair erroneous Vulnerable Items Last Opened and Closed)	以前に修正された欠陥によって破損した既存の UI データを修復します。
算出を再実行 (Rerun calculators)	変更によって影響を受けるすべての脆弱性一致アイテムに対し、算出を再適用します。これにより、修復タスクの累積リスクスコアの再計算がトリガーされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みジョブ	説明
	注: 環境によっては、算出の再実行に時間がかかる場合があります。
キャンセルされた統合インポートセットを再試行 (Retry Cancelled Integration Import Sets)	キャンセルされた統合インポートセットを再試行します。5 回再試行した後、エラーを返します。
統合プロセスを再試行 (Retry Integration Processes)	統合プロセスを再試行します。5 回再試行した後、エラーを返します。
脆弱性一致アイテムの値を脆弱性とグループにロールアップ (Rollup vulnerable item values to vulnerability and group)	ロールアップ算出を使用して、修復タスクのリスクスコア、脆弱性一致アイテムの数、および修復ターゲットステータスを計算します。 **注:** 脆弱性対応 の v23.0 以降では、スケジュール済みジョブが拡張され、マルチスレッド機能を備えたバックグラウンドジョブが作成されます。このアップグレードでは、ジョブをいくつかの小さな子ジョブに分割し、並列または同時に実行します。この変更により、複数のレコードを同時に処理できるようになり、タスク全体の速度が大幅に向上します。
脆弱性エントリーの昇格後に重大度算出を実行 (Run severity calculator after vuln entry promotion)	以前に欠落していた脆弱性が、Qualys クラウドプラットフォーム、Rapid7 Nexpose などのサードパーティプロバイダーからのスコアおよびその他のデータで更新された後に、重大度算出を実行します。 **注:** 脆弱性対応 v25.0.3 以降、スケジュール済みジョブが拡張され、マルチスレッド機能を備えたバックグラウンドジョブを作成できます。このアップグレードでは、ジョブをいくつかの小さな子ジョブに分割し、並列または同時に実行します。この変更により、複数のレコードを同時に処理できるようになり、タスク全体の速度が大幅に向上します。
V19.0：構成済み CVE のエクスポージャーアセスメントの実行 (Run exposure assessment for configured CVEs)	エクスポージャー構成 (Exposure Configuration) テーブル内のすべての CVE レコードのエクスポージャーを計算します。
V19.0：ソフトウェアエクスポージャーの実行 (Run software exposure)	エクスポージャー構成 (Exposure Configuration) テーブル内のすべてのソフトウェアレコードのエクスポージャーを計算します。
スケジュール設定済みの脆弱性データソースプロセッサー (Scheduled Vulnerability Data Source Processor)	インポートキューで処理対象のエントリーを確認し、利用可能なリソースに基づいてスケジュール済みインポートジョブをアサインします。
スケジュール設定済みの脆弱性統合プロセスの添付ファイル	統合 XML 添付ファイルを 14 日経過した後に削除します。この保持時間は設定できません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みジョブ	説明
のクリーンアップ (Scheduled Vulnerability integration process attachment cleanup)	
スケジュール設定済みの脆弱性統合タイムアウトチェッカー (Scheduled Vulnerability Integration timeout checker)	完了までに 60 分以上かかる統合実行をキャンセルします。
VI の関連 CI サービスを設定 (Set related CI services for VI)	統合インポートが完了すると、指定された時刻に、影響を受けるビジネスサービスを脆弱性一致アイテムに関連付けられている CI にリンクします。詳細については、「脆弱性対応でのサービスマッピング」を参照してください。
保留数の設定 (Set deferral counts)	脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、または修復タスクが保留された回数を集計します。
次の統合をトリガー (Trigger next integration)	チェーンされた統合実行における次の統合をトリガーします。
テンプレート統合 (Template Integration)	再スキャン中に単一のテンプレートレコードが Tenable.io に送信されます。
グループ解除済み脆弱性一致アイテムを更新 (Update Ungrouped Vulnerable Items)	脆弱性一致アイテムが修復タスクにあるかどうかを判断し、[グループ解除済み脆弱性一致アイテム] リストに追加するか、リストから削除します。 **注:** このジョブはアップグレード後に実行され、データ セットによっては完了までに時間がかかる場合があります。
VG の脆弱性を更新 (Update Vulnerability on VG)	アップグレード後に修復タスク (sn_vul_vulnerabilty) テーブルの [脆弱性] フィールドを更新します。このジョブは 1 回トリガーされ、その後は非アクティブになります。
脆弱性インポートテンプレート (Vulnerability Import Template)	インポートキューを処理するエンジン。10 個のうちのいずれか。
脆弱性対応のクローズ所要時間の更新 (Vulnerability Response Age Closed Update)	VI テーブルの [クローズ所要時間] 列を更新します。
脆弱性対応の CI 数 (Vulnerability Response CI count)	過去 30 日間にサードパーティのスキャナーによってスキャンされた CI の数を計算します。
脆弱性対応のリスクおよび修復ステータスのアップグレード (Vulnerability Response Risk and Remediation Status Upgrade)	アップグレード時にデータのリスク評価を更新します。
v20.0：リスク軽減の有効期限を確認する	脆弱性一致アイテムと修復タスクの補完コントロールが期限切れになっているかどうかを確認します。期限切れになると、リスクスコアが元のリスクスコアに戻され、補完コントロール

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みジョブ	説明
	が期限切れになったことを示すメール通知が送信されます。また、補完コントロールが 7 日以内に期限切れになるように設定されている場合にも、メール通知が送信されます。

インストールされるテーブル

テーブル	説明
v24.0.6 Prisma ホストのインポート [sn_vul_prisma_hosts_import]	ホストのインポートセットテーブル。
v24.0.6 Prisma ホスト属性 [sn_vul_prisma_host_attrb]	ホスト統合の資産属性テーブル。
v22.0 sn_vul_cmn_auto_close_rule	フィルター条件に基づいて、古い検出を自動的にクローズします。
sn_vul_cmn_ws_saved_filter	保存したフィルターのデータを保存します。
sn_vul_licensing_usage	重複資産、不完全な IP 資産、スキャナー資産の合計数、および最終使用率が含まれます。
sn_vul_m2m_entry_compensating_control	脆弱性エントリと補完コントロールの間の関連性を表します。
v21.0 Rapid7 スキャンエンジン [sn_vul_r7_scan_engine]	スキャン中の資産の検出と脆弱性のチェックを行うスキャンエンジンデータがインポートされたレコードを保存します。
v21.0 Rapid7 スキャンエンジンのインポート [sn_vul_r7_scan_engine_import]	処理前にインポートデータをステージングするために Rapid7 スキャンエンジンの統合で使用されます。
バージョン 19.0： [sn_vul_veracode_cwe_import]	CWE 修復推奨事項の Veracode カテゴリテーブルを拡張します。
バージョン 19.0： [sn_vul_veracode_category_import]	インポートされたカテゴリデータを格納します。
バージョン 19.0： [sn_vul_veracode_sbom_import]	インポートされた Veracode からの SBOM データを格納します。
V17.1：VI キーに証明を追加 [sn_vul_proof_key_vulnerability]	VI キーに証明を含める必要がある Rapid7 脆弱性。 脆弱性対応 の v24.0.6 以降、[Tenable VIT を分割するための正規表現] 列が追加されています。ペイロードから証明を解析するために使用

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
	される、ユーザーが入力した正規表現が保存されます。
評価される脆弱性一致アイテム [sn_vul_m2m_exp_sw_vi]	修復タスクの作成時に修復タスクをアサイン先グループにアサインします。
アサインルール [sn_vul_vgr_assignment_rule]	修復タスクの作成時に修復タスクをアサイン先グループにアサインします。 v15.0 より前：修復タスクの作成時に修復タスク をアサイン先グループにアサインします。
変更要求の関連付け [sn_vul_action_associate_cr]	新しい修復タスクと CHG の関連付けを処理するために使用されるステージングテーブル。 バージョン 15.0 より前：新しい VG と CHG の関連付けを処理するために使用されるステージングテーブル。
非同期の脆弱性一致アイテムジョブ [sn_vul_async_vi_job]	脆弱性一致アイテムを処理するバックグラウンドジョブが含まれています。1 つのジョブタイプのみがサポートされており、脆弱性を一括で編集するために使用されます。
非同期の脆弱性一致アイテムジョブタイプ [sn_vul_async_vi_job_type]	バックグラウンドジョブのタイプが含まれており、関連するスクリプトを参照します。プロセッサーは **VulnerabilityBulkEditProcessor** の 1 つのみ。
古い検出を自動クローズ [sn_vul_auto_close_config]	古い検出を自動的にクローズする方法の構成が保存されます。
脆弱性一致アイテムの粒度の構成 [sn_vul_action_vi_granularity_config]	[VI の粒度の構成] モジュールの構成ページから [ポートを含める] を有効または無効にするために使用する UI フォームを保存します。
変更要求の作成 [sn_vul_action_create_cr]	修復タスクから変更要求を作成するために使用されます。
脆弱性一致アイテムを作成 [sn_vul_action_create_vi]	情報のプレースホルダーとして使用されるステージングテーブル。このテーブルにはレコードが格納されません。
コレクション [sn_vul_patch_orch_collection]	個別のインスタンスからのコレクションデータを格納します。
CWE [sn_vul_cwe]	共通脆弱性タイプ一覧 (CWE) ソフトウェア脆弱性のカタログ。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
CWE アプリケーションプラットフォーム [sn_vul_cwe_m2m_cwe_platform]	インポートされた CWE アプリケーションプラットフォームデータが含まれています。
CWE カテゴリ [sn_vul_cwe_category]	インポートされた CWE カテゴリデータが含まれます。
CWE の一般的な結果 [sn_vul_cwe_consquence]	インポートされた CWE 共通結果データが含まれています。
CWE 外部参照 [sn_vul_cwe_reference]	インポートされた CWE 外部参照データが含まれています。
CWE で観測された例 [sn_vul_m2m_cwe_cve]	インポートされた CWE CVE データが含まれています。
CWE プラットフォーム [sn_vul_cwe_platform]	インポートされた CWE プラットフォームデータが含まれています。
CWE 外部参照 [sn_vul_cwe_reference]	インポートされた CWE 関連外部参照データが含まれています。
CWE の関係性 [sn_vul_m2m_cwe_relation]	インポートされた CWE 関係データが含まれています。
CWE ビュー [sn_vul_cwe_view]	インポートされた CWE ビューデータが含まれています。
CWE 脆弱性 [sn_vul_cwe_weakness]	インポートされた CWE 脆弱性データが含まれています。
バージョン 16.1：デバイスコレクション [sn_vul_patch_orch_m2m_src_ci_collection]	検出されたアイテムに関するコレクションデータを格納します。
バージョン 16.1：デバイス更新 [sn_vul_patch_orch_m2m_src_ci_update]	検出されたアイテムレコードに表示されている、展開されたパッチに関するデータを展開ステータスとともに保存します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
Discovery Model Vulnerable Software Match [sn_vul_discovery_model_software_match]	脆弱なソフトウェアのディスカバリーモデルとの照合を補足します。
例外管理構成 [sn_vul_exception_config]	例外管理機能の構成設定を保存します。
例外ルール [sn_vul_auto_exception_rule]	例外管理に対して評価される一連のルールが含まれています。
エクスプロイト [sn_vul_exploit]	エクスプロイトの定義 (脆弱性を利用する公開されているコード) が含まれています。
エクスプロイトフレームワーク sn_vul_exploit_framework	エクスプロイトフレームワーク (多くのエクスプロイトを実行できる完全なソフトウェアパッケージ) の名前が含まれています。
公開済みディスカバリーモデル [sn_vul_m2m_exp_sw_model]	ディスカバリーモデルと脆弱性 エクスポージャーアセスメントの間のマッピングを保存します。
エクスポージャーアセスメント [sn_vul_exp_by_sw]	エクスポージャーアセスメントのレコードを保存します。
V19.0：エクスポージャーマニフェスト (Exposure Manifest) sn_vul_analyst_exposure_manifest	デルタ処理用のマニフェストテーブル。
エクスポージャー脆弱性エントリー [sn_vul_m2m_entry_exp]	脆弱性 (sn_vul_entry) とエクスポージャーアセスメントの間のマッピングを保存します。
マルウェアキット [sn_vul_malware_kit]	マルウェアキットの詳細が含まれています。この事前作成ツールにより、追加のコーディングや構成作業を行うことなく、エクスプロイトまたは関連する一連のエクスプロイトを簡単に実行できます。
不足している資産テーブル [sn_vul_missing_asset]	一致しない資産を含む無視されたコンフィグレーションコンプライアンスアセスメントデータに対応する一時資産 ID が含まれています。
Microsoft 応答センターソリューションの更新 [sn_vul_msrc_update]	Microsoft によってソリューションデータが最後に更新された時間が含まれています。夜間インポートと比較して、ダウンロードするデルタデータを決定するために使用されます。
Microsoft セキュリティレスポンスセンター ソリューションのインポート [sn_vul_msrc_solution_import]	処理前にインポートデータをステージングするために、Microsoft Security Response Center ソリューション統合によって使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
Microsoft セキュリティレスポンスセンターソリューション統合 [sn_vul_msrc_integration]	Microsoft セキュリティレスポンスセンターソリューション統合 の脆弱性統合 [sn_vul_integration] テーブルを拡張します。
National Vulnerability Databaseエントリー [sn_vul_nvd_entry]	NIST National Vulnerability Database にある、文書化された脆弱性。
NVD CVSS インポート [sn_vul_nvd_cvss_import]	NVD インポート時に 脆弱性対応 スキーマに変換されていないステージングデータが含まれています。
バージョン 16.1 [sn_vul_patch_orch.patch_approval_required]	パッチの展開がパッチ統合からスケジュールされると、要求がレビューおよび承認のために、「レベル 1：パッチ更新の承認」グループにアサインされたユーザーに送信されます。このプロパティは、デフォルトでアクティブ化されています。
バージョン 16.1：パッチ展開 [sn_vul_patch_orch_deployment]	コレクションと CI に関する展開済みパッチに関する情報を保存します。
バージョン 16.1：パッチ更新 [sn_vul_patch_orch_update]	個別のインスタンスで利用可能なパッチに関する情報を保存します。
バージョン 16.1：潜在的なパッチ [sn_vul_patch_orch_m2m_vuln_patch]	脆弱性の解決に使用される可能性があるパッチを特定するパッチおよび脆弱性に関するデータを保存します。
V19.0：潜在的な脆弱性エクスポージャー (Potential Vulnerability Exposure) sn_vul_analyst_m2m_pot_exp_sw_model	CVE のエクスポージャーアセスメントテーブル。
製品カテゴリ [sn_vul_product_category]	インポートされた製品カテゴリデータが含まれています。
Red Hat Security Advisory [sn_vul_rhsa_update]	Red Hat ソリューションを夜間ジョブと比較して、インポートするデルタデータを決定します。
Red Hat ソリューションのインポート [sn_vul_rh_solution_import]	処理前にインポートデータをステージングするために Red Hat Solution Integration で使用されます。
Red Hat Solution Integration [sn_vul_rh_integration]	Red Hat Solution Integration の脆弱性統合 [sn_vul_integration] テーブルを拡張します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
関連ビジネスサービス [sn_vul_m2m_ci_services]	影響を受けるサービスを検索するために CI をビジネスサービスにリンクします。サービスマッピングによって追加されたかどうかを示すフラグが含まれています。
V18.0：修復作業数 [sn_vul_daily_count_re]	1 日の修復作業数。このテーブルは毎日更新されます。
V18.0：修復作業レコード [sn_vul_remediation_effort_record]	修復作業 (RE) の修正進捗状況を追跡します。RE への参照が含まれています。
修復ターゲットルール [sn_vul_ttr_rule]	脆弱性一致アイテムの修正予定期間を定義します。アプリケーションファイルを拡張します。
V18.0：修復タスク [sn_vul_remediation_task]	VR、AVR、CVR、およびテスト結果グループのすべての修復タスクを保存します。 [sn_vul_vulnerability] テーブルレコードに関連する情報で構成されます。[sn_vul_vulnerability] テーブルリストビューでレコードを表示できないユーザーは、[sn_vul_remediation_task] テーブルリストビューでレコード情報を表示できます。 このテーブルには、脆弱性マネージャーワークスペースまたは IT 修復ワークスペースのユーザーがアクセスできます
REST 統合 [sn_vul_rest_integration]	REST ベース統合の脆弱性統合 [sn_vul_integration] テーブルを拡張します。
SAM NVD 脆弱性検出 [sn_vul_sam_config]	SAM NVD で監視される CI と脆弱性はどれか、および SAM NVD 脆弱性検出が有効であるかどうかが含まれています。
スケジュール済みインポートプール [sn_vul_sched_import_pool]	データソースを同時にインポートしやすくするために使用されるスケジュール済みインポートセットレコードのコレクション。
選択した脆弱性一致アイテム [sn_vul_action_select_vi]	分割した VG の処理、CHG の作成、および CHG の関連付けに使用されるベースステージングテーブル
セットアップステータス [sn_vul_setup_status]	内部専用：セットアップアシスタントによって使用されます。セットアップアシスタントを開くたびに、ステップのステータス [完了] が表示され、右上隅のパーセンテージがこのテーブルから取得されます。
重大度マップ	ソース重大度から正規化された重大度へのマッピングが含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
[sn_vul_severity_map]	
ソリューションスキャナーマッピング [sn_vul_solution_scanner_mapping]	ベンダー、スキャナー、および除外または包含のキーワードをマッピングします。
分割 修復タスク [sn_vul_action_split_vg]	修復タスクを分割するために使用されるステージングテーブル。
サードパーティ脆弱性エントリ [sn_vul_third_party_entry]	サードパーティソースにある、文書化された脆弱性。
[sn_vul_tenable_io_template]	テンプレートレコードは Tenable.io に送信され、Tenable.io をソースとするアイテムの再スキャン中にインポートされます。
マニフェストを更新 [sn_vul_update_manifest]	更新済みでロールアップ算出による再計算が必要な修復タスクのリスト。
V17.1：CI クラスによる使用 [sn_vul_licensing_usage_by_ci_classes]	CI クラスによって集計された使用回数が含まれています。
VR 構成アイテム数 [sn_vul_vr_configuration_item_count]	サードパーティ統合からインポートされた構成アイテムの 90 日間の移動累積平均が含まれています。
脆弱性アサインルール [sn_vul_assignment_rule]	VI にアサイン先グループを設定するために評価される一連のルールが含まれています。
脆弱性算出 [sn_vul_calculator_group]	脆弱性算出ルールが含まれています。算出の順序によって最初に評価される算出が決まり、各算出で最大 1 つの算出ルールが使用されます。
脆弱性算出ルール [sn_vul_calculator]	すべての算出のルールが含まれています。算出ごとに、算出ルールが順番に確認されます。条件に一致する最初の算出では、そのルール内の値が使用されます。
脆弱性 CVE [sn_vul_m2m_entry_cve]	NVD 共通脆弱性識別子 (CVE) データを脆弱なエントリーにリンクします。
脆弱性データソースインポートキューエントリー [sn_vul_ds_import_q_entry]	データソースによって処理される前の添付ファイルのキュー。脆弱性統合によって利用されます。
脆弱性エントリー [sn_vul_entry]	文書化された脆弱性。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
脆弱性エントリースキャン [sn_vul_entry_scan]	スキャンと脆弱性エントリーの関係を保存します。
脆弱性エクスプロイトフレームワーク [sn_vul_m2m_framework_vul]	エクスプロイトフレームワークと脆弱性の関係が含まれています。
V19.0：脆弱性エクスポージャーアセスメント (Vulnerability Exposure Assessment) sn_vul_analyst_sam_config	CVE のエクスポージャーアセスメント構成テーブル。
脆弱性の粒度の構成 [sn_vul_granularity_config]	[VI の粒度の構成 (Configure VI granularity)] モジュールのポートの包含またはポートの除外のステータスを保存および管理します。
修復タスク [sn_vul_vulnerability]	修正のために整理された脆弱性一致アイテムのコレクション。
修復タスク変更要求 [sn_vul_m2m_vg_change_request]	修復タスクと CHG 要求の関連付けを格納します。
修復タスクアイテム [sn_vul_m2m_vul_group_item]	修復タスクと脆弱性一致アイテムの関連付け。
修復タスクルール [sn_vul_grouping_rule]	一連の脆弱性一致アイテムに対してグループを自動的に作成する基準を定義するルールが含まれています。
脆弱性統合 [sn_vul_integration]	外部ソースから脆弱性データをインポートするスケジュール可能なレコード。[スケジュール済みスクリプト実行] を拡張します。
脆弱性統合データソース [sn_vul_int_data_src]	脆弱性統合で使用するデータソース。
脆弱性統合ログ [sn_vul_integration_log]	脆弱性統合の実行によって出力されるログ情報を記録します。
脆弱性統合プロセス [sn_vul_integration_process]	脆弱性統合の単発のプロセス。
脆弱性統合キュー [sn_vul_integration_queue]	すべてのデータソースが使用されている場合に統合実行のインポート要求をキューに入れます。
脆弱性統合実行	脆弱性統合の発動。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
[sn_vul_integration_run]	**注:** 統合実行が進行中の場合、バックログで準備完了ステータスにすることができるのは、 1 つの統合のみです。
脆弱性統合の実行統計 [sn_vul_integration_stats]	各ステップのブレークダウン (統合実行の REST API 時間、VI 作成時間など) を保存します。
脆弱性アイテムタスク [sn_vul_m2m_item_task]	問題、変更、およびセキュリティインシデントに関連する脆弱性一致アイテム。
脆弱性マルウェアキット [sn_vul_m2m_malware_kit_vul]	脆弱性とマルウェアキットの関係が含まれています。
脆弱性前提条件ソリューション [sn_vul_m2m_solution_prerequisite]	利用可能な場合にソリューションを適用するためのソース固有の前提条件が含まれています。
脆弱性レート制限 [sn_vul_rate_limit]	スキャナーで使用するレート制限を定義します。
脆弱性参照 [sn_vul_reference]	既知の脆弱性の外部参照。
脆弱性修復ステータス [sn_vul_m2m_ttr_status]	直近で適用された修復ターゲットルールに対する脆弱性一致アイテムのステータス。
脆弱性リスクルール [sn_vul_calc_risk]	リスクスコア算出で使用される特殊な算出ルール。リスクスコアの計算に使用する、VI に関連付けられた値を示す重み付けを取得します。
脆弱性ロールアップ算出 [sn_vul_rollup]	脆弱性ロールアップ算出のリスト。
脆弱性スキャン [sn_vul_scan]	脆弱性スキャン。スキャン対象、使用するスキャナー、およびスキャン結果のサマリーが含まれています。
脆弱性スキャン構成アイテム [sn_vul_m2m_scan_configuration_item]	スキャンするためにキューに入れられた CMDB CI を関連付けます。
脆弱性スキャンキューエントリー [sn_vul_scan_q_entry]	スキャンまたは処理のためにキューに入れられたスキャンレコード。指定されたレート制限内で要求を容易にします。
脆弱性スキャンソース	ソースをスキャンレコードに関連付け、スキャンするためにキューに入れられているすべてのレコードを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
[sn_vul_m2m_scan_source]	
脆弱性スキャンタスク [sn_vul_m2m_scan_vulnerability]	スキャンレコードのソースに関する脆弱性タスクを関連付けます。
脆弱性スキャナー [sn_vul_scanner]	スキャンで使用するサードパーティのスキャナーを定義します。
脆弱性スキャナーレート制限 [sn_cmn_scanner_rate_limit]	スキャナーをレート制限に関連付けます。
脆弱性ソフトウェア [sn_vul_m2m_entry_software]	脆弱性と脆弱なソフトウェアの関連性が含まれています。
脆弱性ソリューション [sn_vul_solution]	脆弱性とその考えられる解決策との関係性データが含まれています。 脆弱性対応 の v24.0.6 以降、「スキャナーセキュリティ情報」というタイトルの新しい列がこのテーブルに追加されています。
脆弱性ソリューション [sn_vul_m2m_vulnerability_solution]	脆弱性エントリー (sn_vul_entry) テーブルを脆弱性ソリューション (sn_vul_solution) テーブルにリンクします。
脆弱性ステータス変更承認 [sn_vul_change_approval]	脆弱性の承認プロセスを追跡します。
脆弱性優先ソリューション [sn_vul_m2m_solution_supersedence]	ソリューション間のソース固有の関係が含まれています。
脆弱性更新マニフェスト [sn_vul_vuln_update]	脆弱性一致アイテムが更新またはクローズされた後、またはリスクスコアが変更された後にロールアップデータを更新する必要がある脆弱性のリストが含まれています。
脆弱性ベンダーマッピング [sun_vul_vulnerability_vendor_mapping]	脆弱性とそのベンダーのリストが含まれています。
脆弱性一致アイテム [sn_vul_vulnerable_item]	構成アイテムの脆弱性の発生が含まれています。
脆弱性一致アイテムの検出 [sn_vul_detection]	サードパーティ統合からの脆弱性一致アイテム検出が含まれています。

自動翻訳

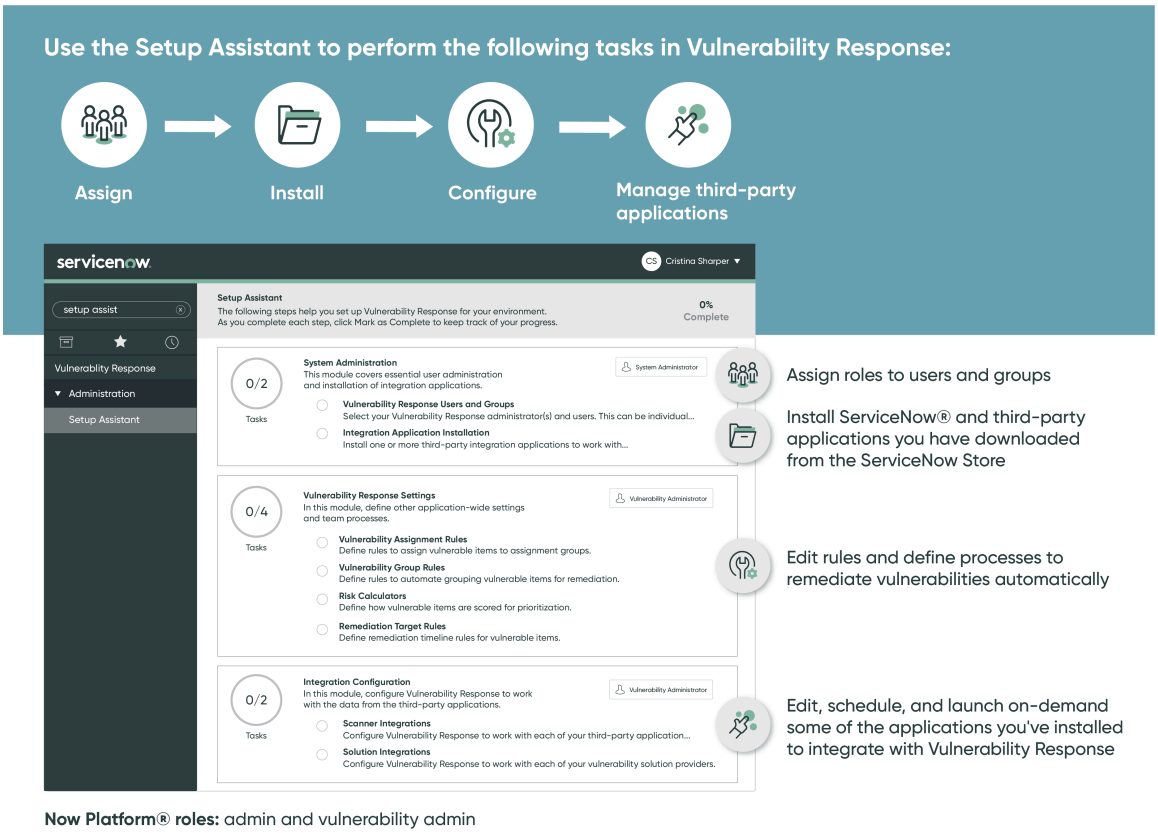
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
脆弱なソフトウェア [sn_vul_software]	特定の脆弱性があることがわかっているソフトウェア。

セットアップアシスタントを使用した 脆弱性対応 の構成

セットアップアシスタントでは、自分の環境に 脆弱性対応 および特定のサードパーティ統合をセットアップする手順を説明します。セットアップアシスタントは、脆弱性対応 を使用できるように、環境のインストールと設定に必要なほぼすべての機能を提供しています。

セットアップアシスタントの機能



Now Platform® roles: admin and vulnerability admin

セットアップアシスタントを使用するには、admin と vulnerability admin という 2 つの異なる Now Platform® ロールが必要です。

セットアップアシスタントで提供される指示とプロンプトを補足する次のセクションを参照してください。

システム管理 - ユーザーとグループをアサインして、統合アプリケーションをインストールする

必要なロール：admin

これらのタスクを開始する前に、ユーザーと統合のリストを脆弱性マネージャーから取得する必要があります。

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント.
2. 最初のセクションである [システム管理] では、アドミニストレーターがユーザーとグループにロールをアサインし、サポートされている統合をインストールします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性対応 のペルソナとロールを、セットアップアシスタントでユーザーとグループにアサインします。

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

3. セットアップアシスタントでロールをアサインします。
   - ユーザーまたはグループに sn_vul.admin のロールをアサインします。
   - 脆弱性統合、修復タスクルール、算出、および修復時間のルールを含む、脆弱性対応の管理および設定のための sn_vul.admin ロールをアサインします。
   - 修復タスクおよび脆弱性一致アイテムの作成および更新のための sn_vul_vulnerability_write ロールをアサインします。

     注:
     その他のすべてのユーザーは、自分にアサインされた修復タスクのみに対する書き込みアクセス権を自動的に受け取ります。

   - 修復タスク、脆弱性一致アイテム、およびその他の脆弱性情報を確認するための sn_vul_vulnerability_read ロールをアサインします。

     注:
     itil ロールを持つユーザーには自動的に sn_vul.remediation_owner ロールが付与され、自分のインスタンスの 脆弱性対応 アプリケーションおよび モバイルエージェント アプリケーションで、自分にアサインされた修復タスクと脆弱性一致アイテム、脆弱性エントリー、およびソリューションを表示できます。追加のアサインは必要ありません。

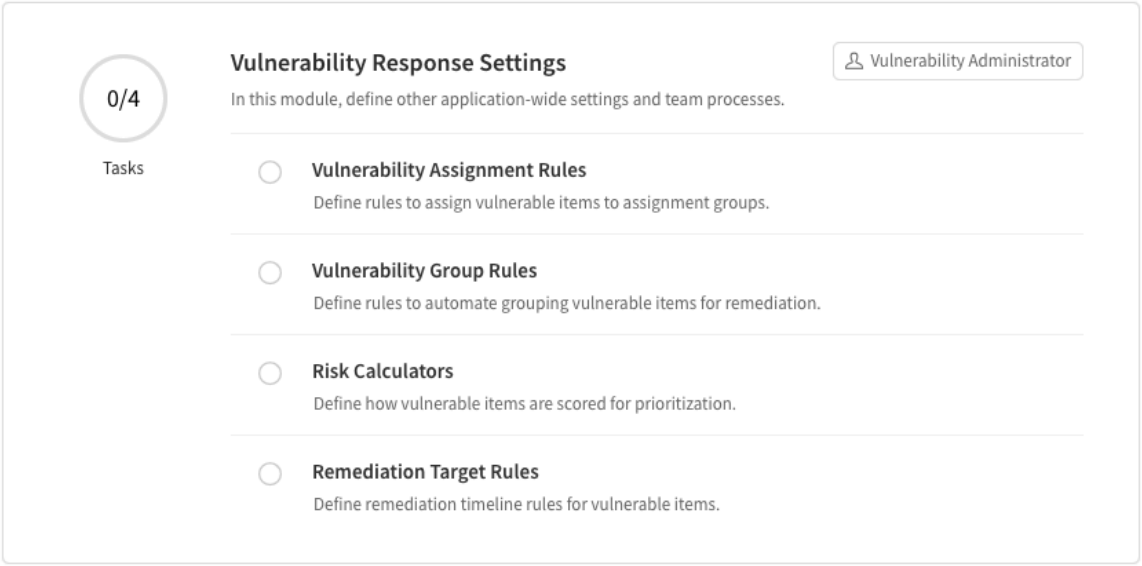
4. サードパーティ統合アプリケーションのインストール
   - 脆弱性対応 でサポートされているアプリケーションの詳細については、「脆弱性対応 およびサポートされているアプリケーションのインストール」および「脆弱性対応 の統合」を参照してください。
   - セットアップアシスタントを使用したサポートされているアプリケーションのインストールの詳細については、「セットアップアシスタントを使用した 脆弱性対応 サードパーティアプリケーションのインストール」を参照してください。

脆弱性対応 設定

必要なロール：sn_vul.vulnerability_admin、sn_vul.admin (非推奨)、または admin。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



脆弱性対応設定で、脆弱性アドミニストレーターはアプリケーション全体の設定を定義し、脆弱性対応 のルールを定義します。または、アドミニストレーターは次のタスクを実行できます。

1. 脆弱性アサインルールを作成します。

解決に向けて、修復タスクの自動アサインを定義するルールを作成します。少なくとも 1 つのルールがベースシステムに付属しています。詳細については、「脆弱性対応 アサインルールの概要」を参照してください。

> **注:**
>
> 再適用機能には、ルールのベースラインアプリケーションが必要です。ルールを作成したら、都合に応じて *Reapply all vulnerability assignment rules* のスケジュール済みジョブをアクティブ化して実行します。それ以外の場合は、ルールを変更する前に、すべてのオープン VI にすべてのルールを再適用する必要があります。
>
> ジョブが完了したら、スケジュール済みジョブの [実行] フィールドを環境に合わせて設定します。アクティブな VI の数によっては、それらを毎日評価して更新すると、パフォーマンスに重大な影響を与える可能性があります。規模が大きい環境では、週に 1 回または月に 1 回の更新を検討してください。
>
> アサインルールを再適用しても、脆弱性一致アイテムは再グループ化されません。

2. 修復タスクルールの作成

解決に向けて、修復タスクの自動作成を定義するルールを作成します。少なくとも 1 つのルール [脆弱性] がベースシステムに付属しています。フォームまたはリストビューからルールを再適用できます。

- グループルールが削除されると、フォームまたはリストビューから、そのルールによって作成されたすべてオープングループを削除できます。[オープン] ステータスでないグループは除外されます。
- 環境に対するルールの作成の詳細については、「脆弱性対応 サードパーティ脆弱性統合の構成アイテムを識別するための CI ルックアップルール」を参照してください。
- 脆弱性対応 を使用した脆弱性修復の詳細については、「脆弱性対応アプリケーションの詳細」を参照してください。

3. リスク算出を作成して有効にします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

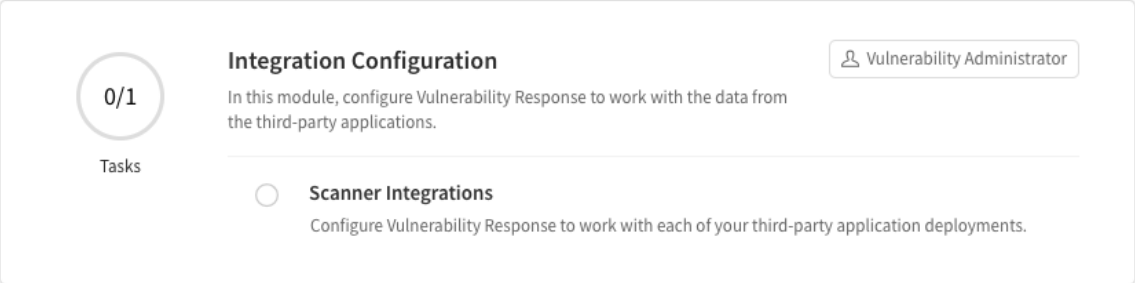
優先順位付けのために脆弱性一致アイテムのスコアを付ける方法を定義するリスク算出を有効にします。いくつかのリスク算出がベースシステムに付属しています。環境に対するリスク算出の作成または編集については、「脆弱性対応 の算出と脆弱性算出ルール」を参照してください。

4. 修復ターゲットルールを作成します。

   修復のカテゴリに対する修復ターゲットルールを作成します。少なくとも 1 つのルールがベースシステムに付属しています。環境に対するルールの作成の詳細については、「脆弱性対応 の修復ターゲットルール」を参照してください。

統合設定

必要なロール：sn_vul.vulnerability_admin、sn_vul.admin (非推奨)、または admin。



[統合構成] セクションでは、次のサードパーティ脆弱性スキャナー統合 (および 脆弱性対応のソリューション管理 アプリケーションがインストールされている場合はソリューションプロバイダー) の構成、スケジュール設定、編集、およびオンデマンドでの起動を行います。

- Qualys 脆弱性統合 の構成の詳細については、「セットアップアシスタントを使用した Qualys 脆弱性統合の構成」を参照してください。
- Vulnerability Response Integration with Tenable アプリケーションの構成がサポートされています。「セットアップアシスタントを使用した Tenable 脆弱性統合の構成」を参照してください。
- 脆弱性ソリューション管理 アプリケーションをインストールすると、[ソリューション統合] オプションが [スキャナー統合] の下に表示されます。[ソリューション統合] をクリックして、セットアップアシスタントのこのセクションから、インストールされている脆弱性ソリューションプロバイダーを設定します。Red Hat Solution Integration と Microsoft セキュリティレスポンスセンターソリューション統合 がサポートされています。

  インストールされているソリューションの詳細については、「脆弱性ソリューション管理」を参照してください。インストール後の詳細については、「脆弱性対応のソリューション管理アプリケーションのインストール」を参照してください。

  インストールされているソリューションの構成の詳細については、「セットアップアシスタントを使用した 脆弱性ソリューション管理 のインストール済みソリューション統合の構成」を参照してください。

- マルチソース統合の場合、同じサードパーティ統合に複数の展開を含めることができます。
- 元のサードパーティ統合の設定は、新しい各統合の設定のテンプレートとして使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> 元の脆弱性統合を削除する場合、テンプレートとして使用する別の統合を選択する必要があります。統合を削除する代わりに無効にすることを検討してください。無効になったテンプレートから作成された統合は、デフォルトで無効になっています。

各サードパーティ統合からのデータは一意に識別され、脆弱性対応 の単一のインスタンスで使用できます。

> **注:**
> Rapid7 InsightVM の複数の脆弱性統合はセットアップアシスタント内では使用できません。複数の Rapid7 InsightVM 統合の構成および作成については、「統合のためのドメインセパレーションインポートの作成」を参照してください。

追加タスク

セットアップアシスタントに含まれていないセットアップタスクの詳細については、「追加の脆弱性対応セットアップおよび構成タスク」を参照してください。

セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン

セットアップアシスタントで 脆弱性対応 ペルソナロールをグループまたはユーザーにアサインします。

始める前に
セットアップアシスタントを使用してアサインされた 脆弱性対応 のペルソナと詳細ロールの管理 ペルソナロールが既にあり、ユーザー管理モジュールでの詳細ロールとロールのアサインの編集および管理に関する詳しい情報が必要な場合は、「脆弱性対応」を参照してください。

アップグレードのお客様は、脆弱性対応アプリケーションの既存のロールを引き続き使用できます。脆弱性対応 の以前のバージョンで使用できる sn_vul.vulnerability_read と sn_vul.vulnerability_write の権限でアサインされたユーザーとグループおよび修復オーナーロールのアクセス権は変更されていません。

ただし、脆弱性対応 アプリケーションでユーザーとグループが実行して確認できる内容をタスクレベルでより細かく制御する場合は、ペルソナロールと詳細ロールを使用することをお勧めします。

セットアップアシスタントを使用して sn_vul.vulnerability_admin ペルソナロールをまだアサインしていない場合は、以下の手順に従ってアサインしてください。脆弱性アドミニストレーターは、このペルソナロールがアサインされると、最初のセクションの後にセットアップアシスタントタスクを完了して 脆弱性対応 アプリケーションでルールとサードパーティ統合を管理する権限を持つことになります。

ペルソナロールと詳細ロールの概要については、「脆弱性対応 のペルソナと詳細なロール」を参照してください。

アップグレードのお客様は、次の表を参考にしてください。

v10.3 より前	**v10.3** 以降
sn_vul.admin をアサインした場合	sn_vul.vulnerability_admin - 脆弱性アドミンをユーザーまたはグループにアサインすることをお勧めします。 このロールを持つユーザーは、脆弱性対応 (VR) アプリケーションとそのレコードに完全にアクセスできます。また、すべての VR アプリケー

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

v10.3 より前	v10.3 以降
	ションとルールを構成したり、サードパーティ統合をインストールしたりできます。
ユーザーとグループに sn_vulnerability_write をアサインした場合。	sn_vul.vulnerability_analyst - 脆弱性アナリストをユーザーとグループにアサインすることをお勧めします。 このロールを持つユーザーやグループは、VI 修復のすべてのレコードを表示および更新できます。
sn_vul.remediation_owner をアサインした場合	sn_vul.remediation_owner - 修復オーナーをユーザーとグループにアサインすることをお勧めします。 このロールを持つユーザーやグループは、自分または所属するグループにアサインされた脆弱性を修正できます。このロールを持つグループまたはユーザーは、自分または所属するグループにアサインされたレコードを表示および更新します。
一致しない構成アイテム (CI) の管理に sn_vul.admin をアサインした場合	sn_vul.ci - CI マネージャーをユーザーとグループにアサインすることをお勧めします。 このロールを持つユーザーやグループは、構成管理データベース (CMDB) にない不一致構成アイテム (CI) を管理できます。また、検出されたアイテムを更新できます。
保留および例外の承認のために sn_vul.admin をアサインした場合。	ユーザーとグループに、sn_vul.exception_approver - 例外承認者をアサインすることをお勧めします。 このロールを持つユーザーとグループは、修復タスクと脆弱性一致アイテムの例外、保留、およびクローズを承認できます。 v20.0 以降、このロールの詳細ロール sn_vul.read_all が削除され、すべての脆弱性一致アイテムと修復タスクではなく、自分と自分のグループに割り当てられた脆弱性一致アイテムと修復タスクにアクセスできるようになりました。
sn_vul.vulnerability_read をアサインして脆弱性管理を可視化した場合。	タスクごとにアプリケーションの特定領域への読み取りアクセス権をアサインすることをお勧めします。 たとえば、sn_vul.read_all をアサインして、ユーザーがすべての VR レコードを表示できるようにします。修復タスクルールを表示するための読み取りアクセス権を付与するには、sn_vul.read_group_rules をアサインします。このロールを持つユーザーやグループはレコードを更新できません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ペルソナロールを持つユーザーまたはグループがデフォルトで継承する詳細なロールを表示するには、次に移動します: **All** (すべて) > ユーザー管理 **(User Administration)** > ロール. 目的のロールを見つけてクリックし、レコードを開きます。[含まれるロール] タブには、ペルソナロールのすべての詳細ロールと継承されたロールが一覧表示されます。

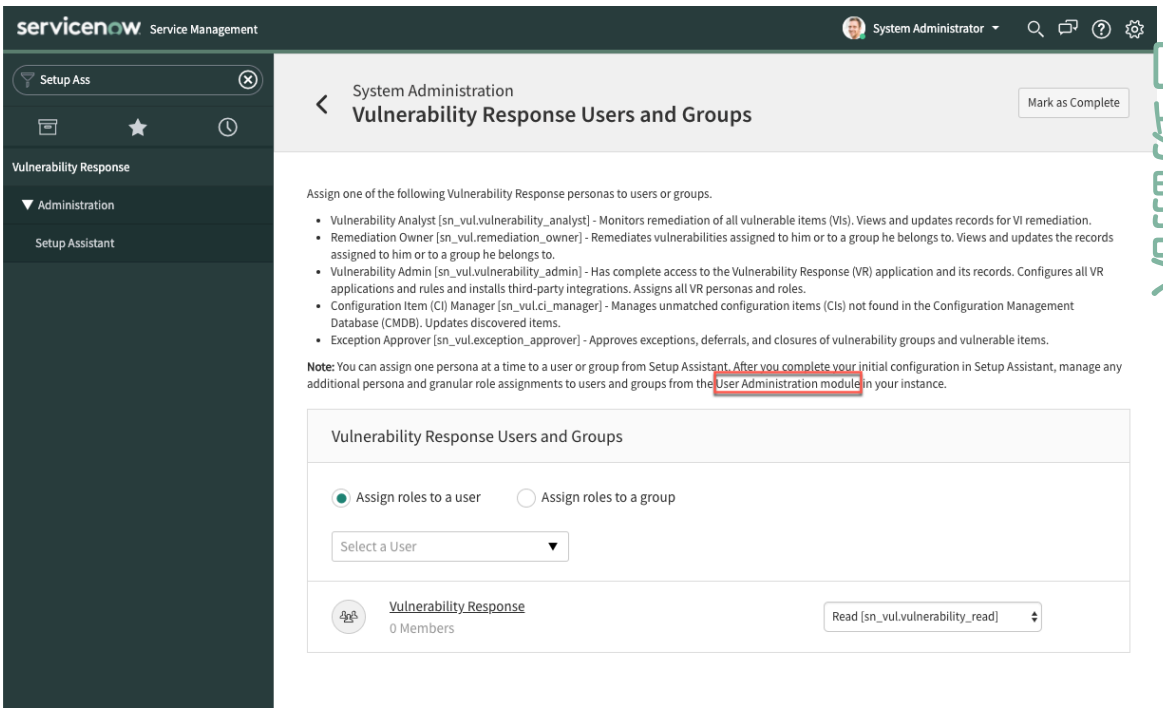
セットアップアシスタントでロールをアサインする前に、必要なすべてのユーザーとグループが作成されていることを確認するようお勧めします。または、セットアップアシスタント内から新しいユーザーとグループを追加するには、次の図に示すフォームの [ユーザー管理モジュール] リンクをクリックします。

次の例では、脆弱性対応 アプリケーションへのアクセスを制限するために、脆弱性アドミンペルソナをユーザーにアサインする方法を示しています。通常は、sn_vul.vulnerability_admin 以外のペルソナロールをグループにアサインすることをお勧めします。

必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション セットアップアシスタント。
   [セットアップアシスタント] ページが表示されます。
2. [脆弱性対応ユーザーおよびグループ] をクリックします。
   [システム管理脆弱性対応ユーザーおよびグループ] ページが表示されます。



3. [ユーザーへのロールのアサイン] を選択した状態で、リストから既存のユーザーを選択します。

   ユーザーまたはグループに 1 つのペルソナロールのみをアサインできます。

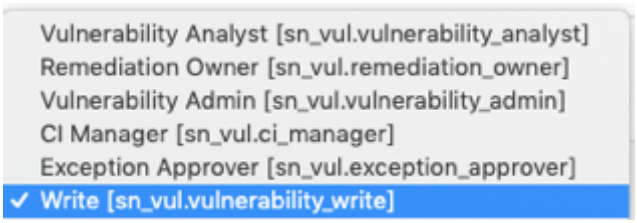
   フォームの右側でユーザーまたはグループを選択すると、デフォルトのペルソナである修復オーナー [sn_vul.remediation_owner] がデフォルトでアサインされ、変更するまでリストに表示されたままになります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
脆弱性対応 の新しいバージョンにアップグレードし、アップグレード前に sn_vul.vulnerability_read または sn_vul.vulnerability_write ロールをユーザーやグループに事前にアサインしていた場合は、次の図に示すように、そのロールが新しいペルソナロールとともに表示されます。

アップグレードのお客様は、脆弱性対応アプリケーションの既存のロールを使用し続けることができます。v10.3 より前に sn_vul.vulnerability_read および sn_vul.vulnerability_write 権限によりアサインされたユーザーとグループおよび修復オーナーのアクセス権は変更されていません。

sn_vul.vulnerability_read または sn_vul.vulnerability_write ロールが現在アサインされている既存のユーザーまたはグループの場合、これらのロールはペルソナロールとともにリストに表示されます。ペルソナロールをアサインすると、以前のロールは使用できなくなります。たとえば、次の図に示す書き込み [sn_vul.vulnerability_write] ロールは、ペルソナロールのいずれかをアサインすると、そのユーザーまたはグループにはオプションとして表示されなくなります。

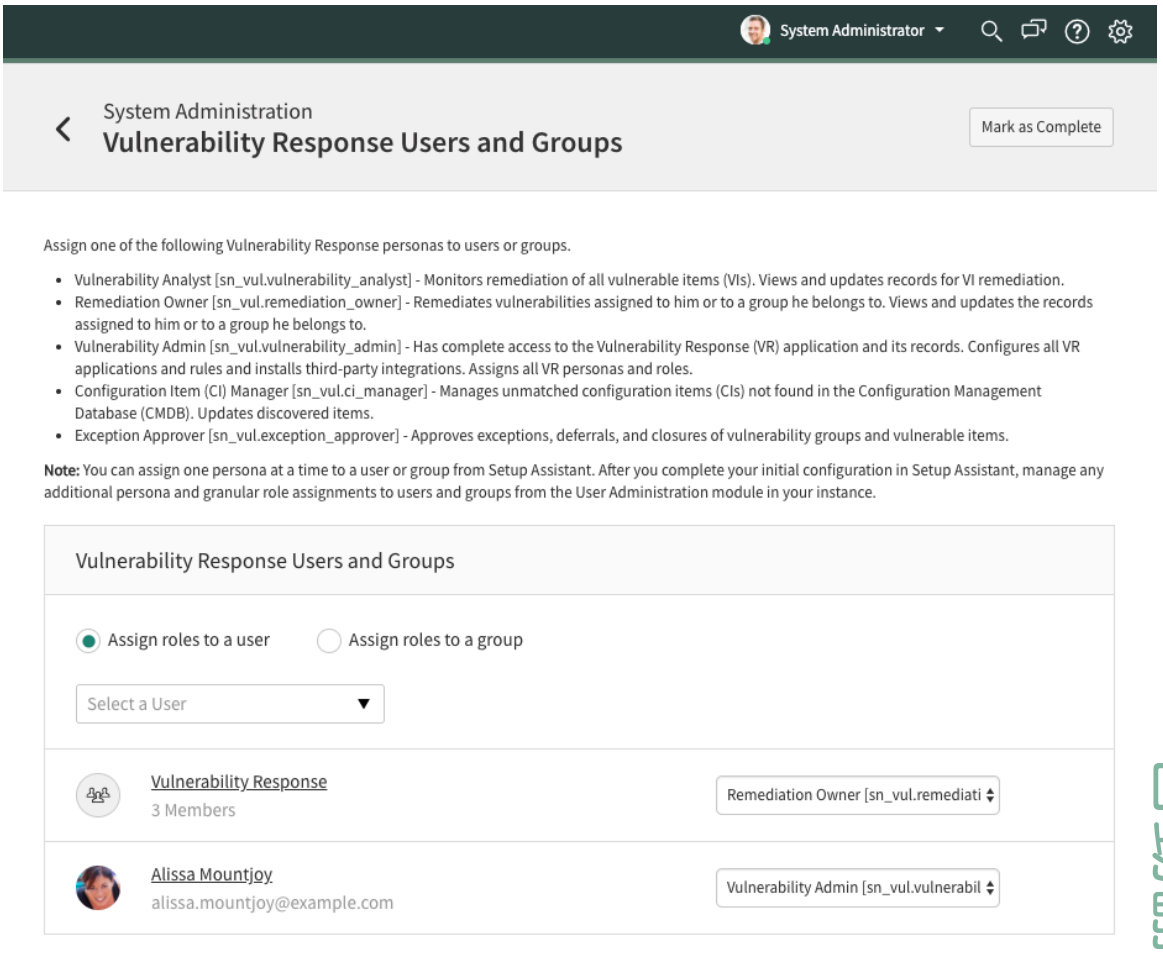


4. フォームの右側のリストから、[脆弱性アドミン **[sn_vul.vulnerability_admin]]** を選択します。ユーザーまたはグループにペルソナが正常にアサインされたことを示すメッセージが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

グループにアサインされた修復オーナーペルソナと、ユーザーにアサインされた脆弱性アドミンペルソナ



5. 続いて上記のペルソナロールの説明を参考にして、ユーザーとグループを残りのペルソナロール (修復オーナー、脆弱性アナリスト、CI マネージャー、例外承認者) にアサインします。
セットアップアシスタントを使用したユーザーとグループへのペルソナロールのアサインが正常に完了しました。
6. オプション: セットアップアシスタントからグループ内のユーザーを編集するには、次の手順を実行します。

   a. フォームにグループを表示した状態で、編集するグループの名前をクリックします。
   グループレコードが表示されます。

   b. [グループメンバー] タブを選択した状態で、[編集] をクリックします。
   [メンバーの編集] フォームが表示されます。

   c. スラッシュバケットを使用して、ユーザーを選択または削除します。

   d. [保存] をクリックして変更を保存し、グループレコードに戻ります。

   e. [更新] をクリックしてセットアップアシスタントに戻ります。

   f. セットアップアシスタントページで、[脆弱性対応ユーザーおよびグループ] をクリックして、セットアップアシスタントの構成を続行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のタスク
システムアドミニストレーターとして、セットアップアシスタントで 脆弱性対応 の構成を続行します。最初のセクションが完了したら、脆弱性アドミンペルソナロールがアサインされたユーザーに、セットアップアシスタントでタスクを実行させることができます。詳細ロール管理の詳細と例については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

脆弱性対応 のペルソナと詳細ロールの管理

セットアップアシスタントを使用してペルソナロールの初期アサインを完了したら、インスタンスのユーザー管理モジュールからユーザーまたはグループへの追加の詳細ロールのアサインを管理します。

始める前に
セットアップアシスタントを使用した 脆弱性対応 の初期設定と構成をまだ完了していない場合、またはユーザーとグループにペルソナロールをアサインしていない場合は、次に移動します: 脆弱性対応 > アドミニストレーション > セットアップアシスタント. 「セットアップアシスタントを使用した脆弱性対応 ペルソナロールのアサイン」を参照してください。

ペルソナロールの重要な用語と概要については、「脆弱性対応 のペルソナと詳細なロール」を参照してください。

ペルソナロールは、複数の詳細ロールで構成される、アプリケーション内の事前設定されたロールです。セットアップアシスタント、脆弱性アドミン、脆弱性アナリスト、修復オーナー、構成アイテムマネージャー、および例外マネージャーのペルソナロールは、IT 組織または脆弱性修復グループのマネージャー、アナリスト、およびサービスオーナーの一般的な役職に対応するように設計されています。

いずれかのロールで許可されている数よりも多くのアクセス権をユーザーとグループに付与する場合は、詳細ロールをさらにユーザーとグループに追加できます。逆に、タスクレベルで特定のユーザーやグループのアクセスを制限する場合は、詳細なロールを削除できます。また、ニーズに合わせてカスタムロールをビルドすることもできます。

必要なロール：admin

手順

1. ユーザーとグループの詳細ロールを管理するには、いずれかを選択して続行します。

   脆弱性対応 における詳細ロールの名前は、通常、ユーザーが実行して確認できる内容を示しています。特定の詳細なロールの説明を表示するには、次に移動します: **All** (すべて) > ユーザー管理 **(User Administration)** > ロール をクリックし、必要なロールを見つけます。ロールの説明、ロールがアサインされたときに自動的に継承されるロール、および他のロールに依存するロールも一覧表示されます。

2. ユーザーまたはグループの詳細ロールをアサインまたは削除するには、次の手順を実行します。
   たとえば、IT マネージャーに、レコードの表示は許可するけれども、更新や編集は許可しないロールをアサインするとします。脆弱性対応、脆弱性対応のパフォーマンスアナリティクス、およびすべてのサードパーティ統合のレコードを表示するには、このユーザーに sn_vul.read_all の詳細ロールをアサインします。

   a. 次のように移動する。 **All** (すべて) > ユーザー管理 **(User Administration)** > ユーザー.

   b. ユーザーを見つけ、 [名前] 列でレコードをクリックして開きます。
      ユーザーのレコードが表示されます。

   c. [ロール] タブが選択されていない場合は、それを選択します。
      ユーザーに現在アサインされているロールが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

d. [編集] をクリックします。
[メンバーの編集] フォームが表示されます。

e. スラッシュバケットの [コレクション] フィールドに、わかる場合はロールの名前を入力します。または、「*sn_vul」と入力して、脆弱性対応で利用可能な詳細ロールのみを表示します。

f. 「sn_vul.read_all」を見つけて [ロールリスト (Roles List)] に移動させます。

> **注:**
> 同じプロセスで、ロールを [ロールリスト (Roles List)] から [コレクション] リストに移動させ、スラッシュバケット内のユーザーから特定の詳細ロールを削除します。

g. [保存] をクリックします。
ユーザーレコードが新しい詳細ロールで表示されます。

h. [更新] をクリックして変更を保存し、[ユーザー] リストに戻ります。
脆弱性対応、脆弱性対応のパフォーマンスアナリティクス、およびサードパーティ統合のレコードを読み取れるけれども更新できない権限をユーザーに提供しました。

3. 特定のメンバーのみがより詳細なロールでアクセスを拡大できるようにグループを編集するには、次の手順を実行します。
たとえば、修復オーナー (sn_vul.remediation_owner) グループの特定のユーザーに脆弱性一致アイテムの手動作成を許可したいけれども、その権限をグループ内のすべてのユーザーにまで広げて付与したくはないとします。脆弱性一致アイテムを手動で作成する権限は、sn_vul.create_vulnerable_items 詳細ロールによって付与されます。このグループの特定ユーザーにのみこの権限を付与するには、次の手順を実行します。

a. 次のように移動する。 **All** (すべて) > ユーザー管理 **(User Administration)** > グループ.

b. 修復オーナーグループを見つけ、 [名前] 列でグループをクリックして、レコードを開きます。
グループレコードが表示されます。

c. [グループメンバー] タブが選択されていない場合は、それを選択します。
グループの現在のメンバーが表示されます。

d. リストから、詳細ロールをアサインする名前をクリックし、レコードを開きます。

e. レコードで、[ロール] タブまでスクロールして選択します。
ユーザーにアサインされているロールが表示されます。

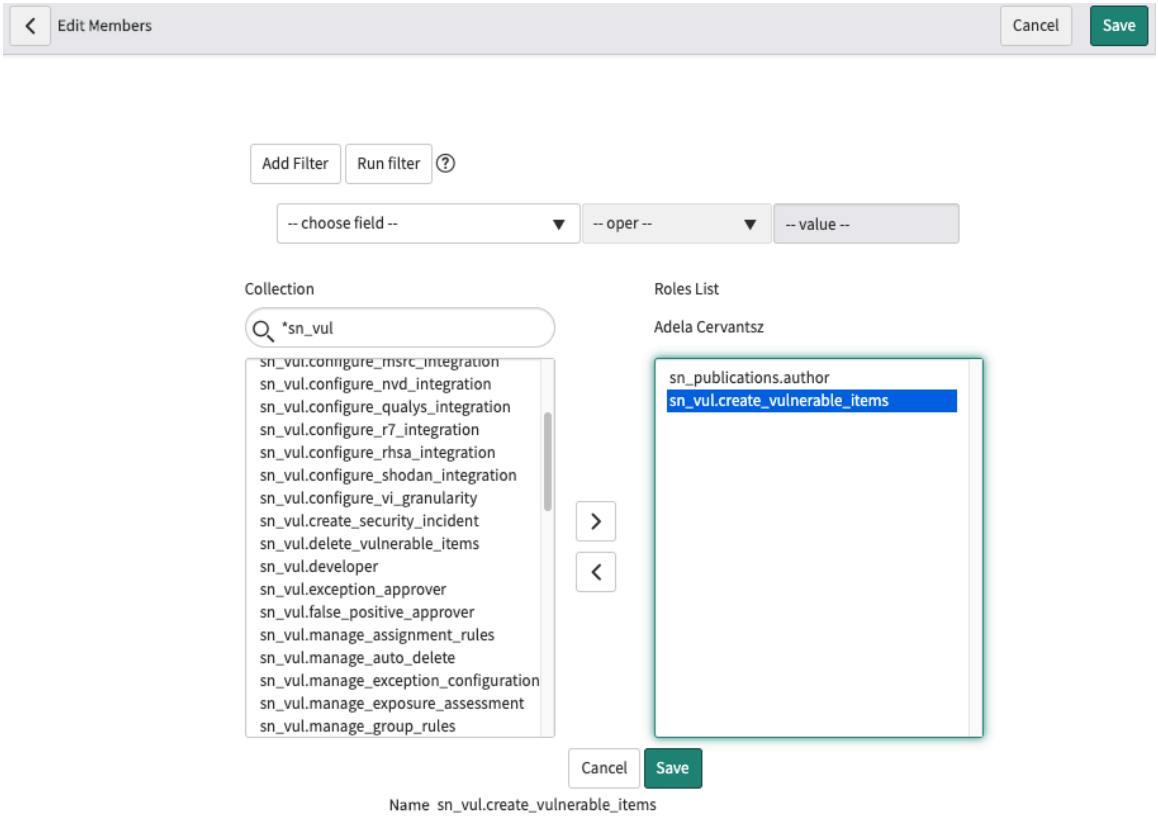
f. [編集] をクリックします。
[メンバーの編集] フォームが表示されます。

g. [コレクション] フィールドに、わかる場合はロールの名前を入力します。または、「*sn_vul」と入力して、脆弱性対応で利用可能なすべての詳細ロールを表示します。

h. 「sn_vul.create_vulnerable_items」を見つけて [ロールリスト (Roles List)] に移動させます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



i. [保存] をクリックします。
ユーザーレコードが新しい詳細ロールで表示されます。

j. 戻る矢印をクリックして、修復オーナーグループのレコード内のユーザーを表示します。

k. リストから、この詳細ロールをアサインする名前をクリックし、レコードを開き、スラッシュバケットを使用してロールをアサインします。

l. 編集を完了したら、[更新] をクリックして変更を保存し、グループリストに戻ります。
これで修復オーナー (sn_vul.remediation_owner) グループの一部のユーザーに、脆弱性一致アイテムを手動で作成する権限が付与されました。

4. 選択した詳細ロールのみを使用して新しいロールを作成するには、次の手順を実行します。
この例では、コンプライアンス監査人のロールを作成するとします。このロールはガバナンス、リスク、コンプライアンス (GRC) と緊密に連携し、そのジョブには 脆弱性対応 内の以下の権限とタスクが必要になります。

- 脆弱性一致アイテムと脆弱性グループの修正期限を管理する。
- 期限の延長または修正の保留の例外要求を承認する。
- 自動削除を使用して古い脆弱性一致アイテムのクリーンアップを管理する。
- リスクスコアを定義する。
- 脆弱性対応 内のすべてのレコードを読み取る (ただし、編集は許可されない)。

a. 次のように移動する。 **All** (すべて) > ユーザー管理 **(User Administration)** > ロール.

b. ロールリストで、[新規] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

c. ロールレコードのフィールドに入力します。

名前を作成し、このレコードを含むアプリケーションを選択して、新しいロールの簡単な説明を入力します。フォーム上のその他のフィールドの詳細については、「ロールを作成する」を参照してください。

> **注:**
> 新しいロールの名前を作成するときは、ロールリスト内で簡単に認識でき、ロールの機能を説明する名前を使用することをお勧めします。この例では、「コンプライアンス監査人 - GRC-VR」などの役職を名前にできます。

d. [Submit] をクリックします。
ロールリストが表示されます。

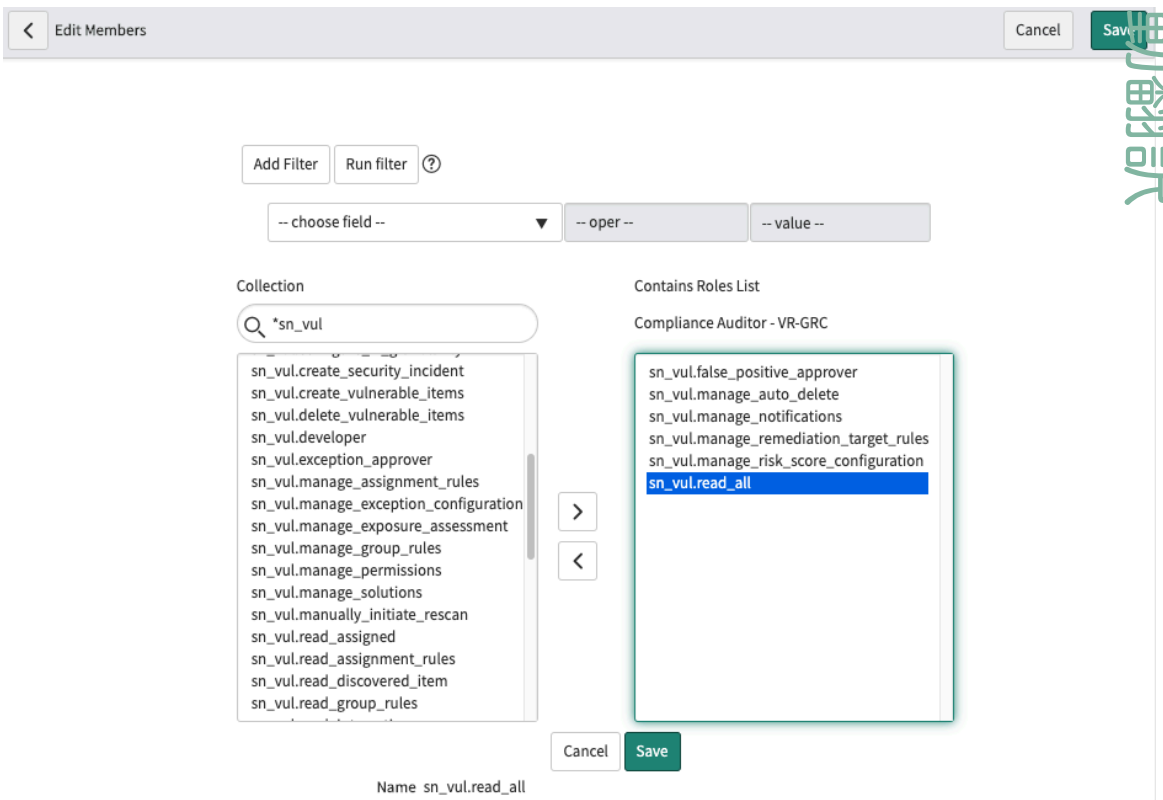
e. 新しいロールを見つけてクリックし、レコードを開きます。

f. [編集] をクリックします。
[メンバーの編集] フォームが表示されます。

g. スラッシュバケットを使用して、新しいロールに詳細ロールを追加します。

この例では、この新しいロールに必要なロールが次の図の右側の列に表示されています。

脆弱性対応の詳細ロールのみを表示するには、 [コレクション] フィールドに「*sn_vul」と入力します。



h. [保存] をクリックします。
新しいロールのレコードが表示されます。[含まれるロール] タブから始めて、必要に応じてロールの編集を続行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

i. [更新] をクリックして変更を保存します。
新しいロールがロールリストに表示されます。

セットアップアシスタントを使用した 脆弱性対応 サードパーティアプリケーションのインストール

セットアップアシスタントを使用して、エンタイトルメントがあるサードパーティ統合アプリケーションを 脆弱性対応 にインストールします。

始める前に
セットアップアシスタントは、ほとんどのサードパーティ統合アプリケーションを 脆弱性対応 とともにインストールできますが、インストールする一部のアプリケーションの構成については、インスタンスの構成モジュールから続行します。脆弱性対応 でサポートされているアプリケーションのリストについては、「脆弱性対応 の統合」を参照してください。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

- 脆弱性対応 の 脆弱性ソリューション管理 機能をインストールすると、セットアップアシスタントで Microsoft セキュリティレスポンスセンターソリューション統合 と Red Hat Solution Integration にアクセスできるようになります。
- 脆弱性ソリューション管理 は別のサブスクリプションで利用できます。脆弱性対応 がソリューションを組み込む方法の詳細については、「脆弱性ソリューション管理」を参照してください。

セットアップアシスタントからサードパーティアプリケーションをインストールしてアクティブ化する前に、以下のタスクを実行してインストールをスムーズに進めます。

セットアップタスク	説明
インストールする統合アプリケーションに対して有効な ServiceNow エンタイトルメントがあることを確認します。	次のように移動する。 サブスクリプション管理 > サブスクリプション エンタイトルメントを確認します。リストには、組織で購入したサブスクリプションが表示されます。 ServiceNow Store から セキュリティオペレーション アプリケーションのエンタイトルメントを取得する方法の詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」を参照してください。
(オプション) まだインストールしてアクティブ化していない場合は、サードパーティアプリケーションをインストールする前に 脆弱性対応 アプリケーションをインストールすることもできます。	脆弱性対応 アプリケーションのインストールとアクティブ化の詳細については、「Install and configure Vulnerability Response (脆弱性対応 のインストールと構成)」を参照してください。
まだインストールとアクティブ化を行っていない場合は、サードパーティのスキャナーアプリケーションを実行してデータをインポートする前に、NVD 統合と CWE スケジュール済みジョ	NVD および CWE 統合は、脆弱性対応 の初期設定の一部として、サードパーティのスキャナー製品を使用してインスタンスに脆弱性データをインポートする前に実行します。詳細につ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

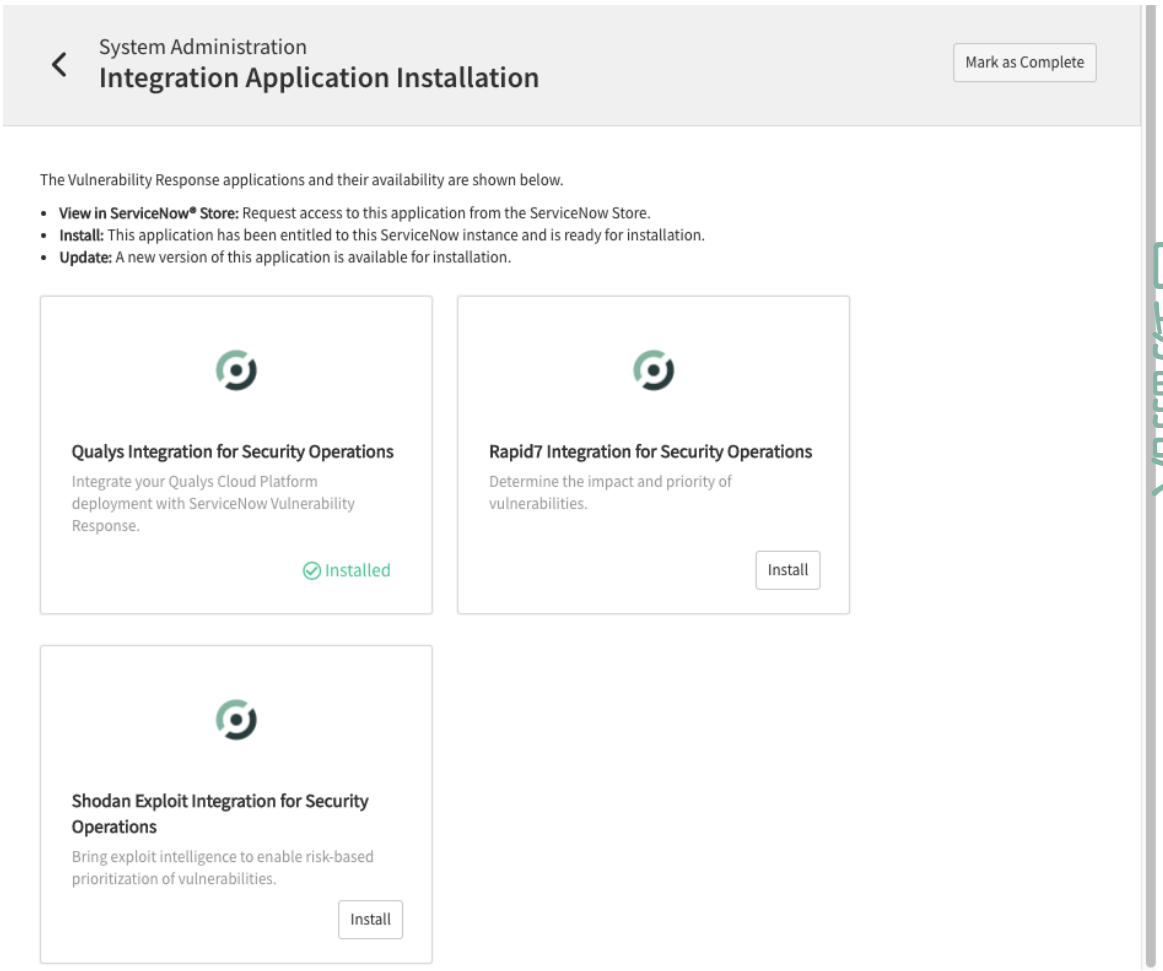
セットアップタスク	説明
ブを使用して脆弱性データをアクティブ化してインポートする必要があります。	いては、「NVD 統合の概要」を参照してください。
脆弱性対応 のサードパーティ統合に必要なセットアップタスクが完了していることを確認します。	脆弱性対応 の統合 でインストールする各統合に必要なセットアップタスクを確認します。

必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント > システム管理 > 統合アプリケーションのインストール.

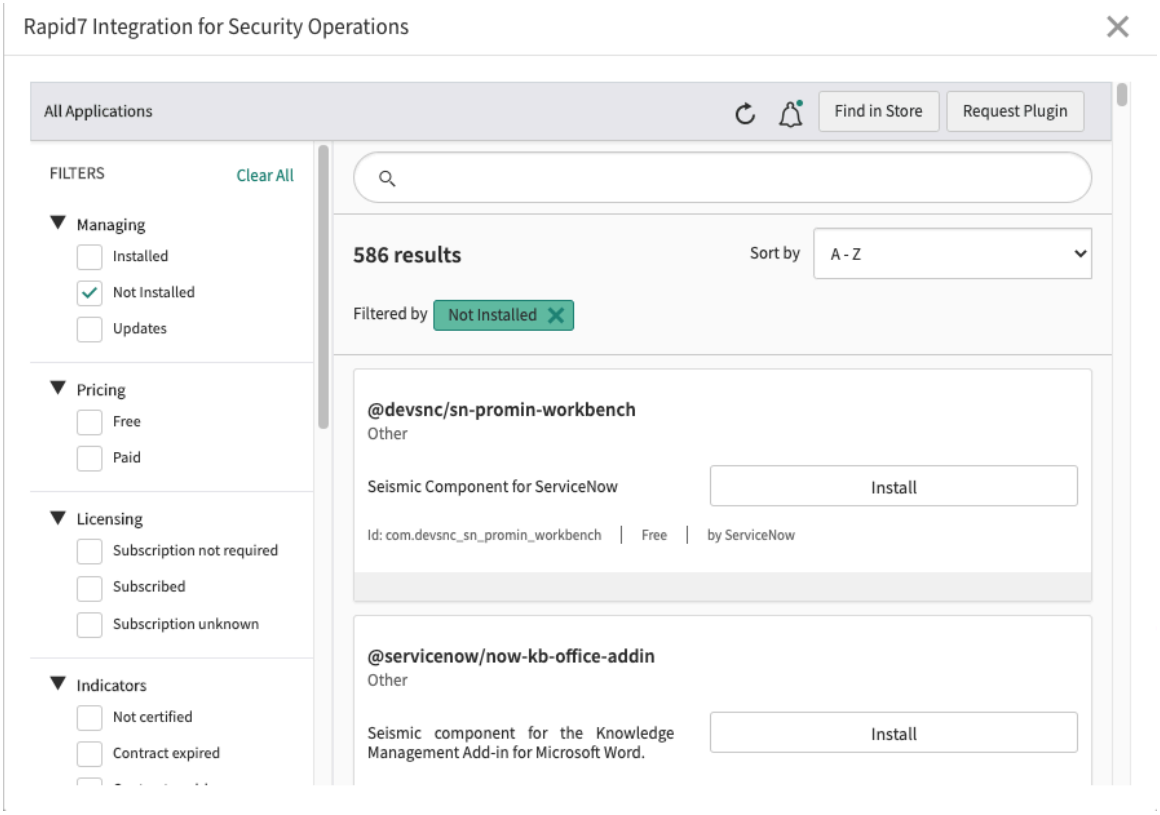
   しばらくすると、エンタイトルメントがあり、インスタンスにインストールできるアプリケーションが表示されます。



2. インストールするアプリケーションを見つけて、アプリケーションタイルで [インストール] をクリックします。
   次の図に示すように、[すべてのアプリケーション] ダイアログに、クリックしたアプリケーションタイルの名前 (Rapid7 Integration for Security Operations など) が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

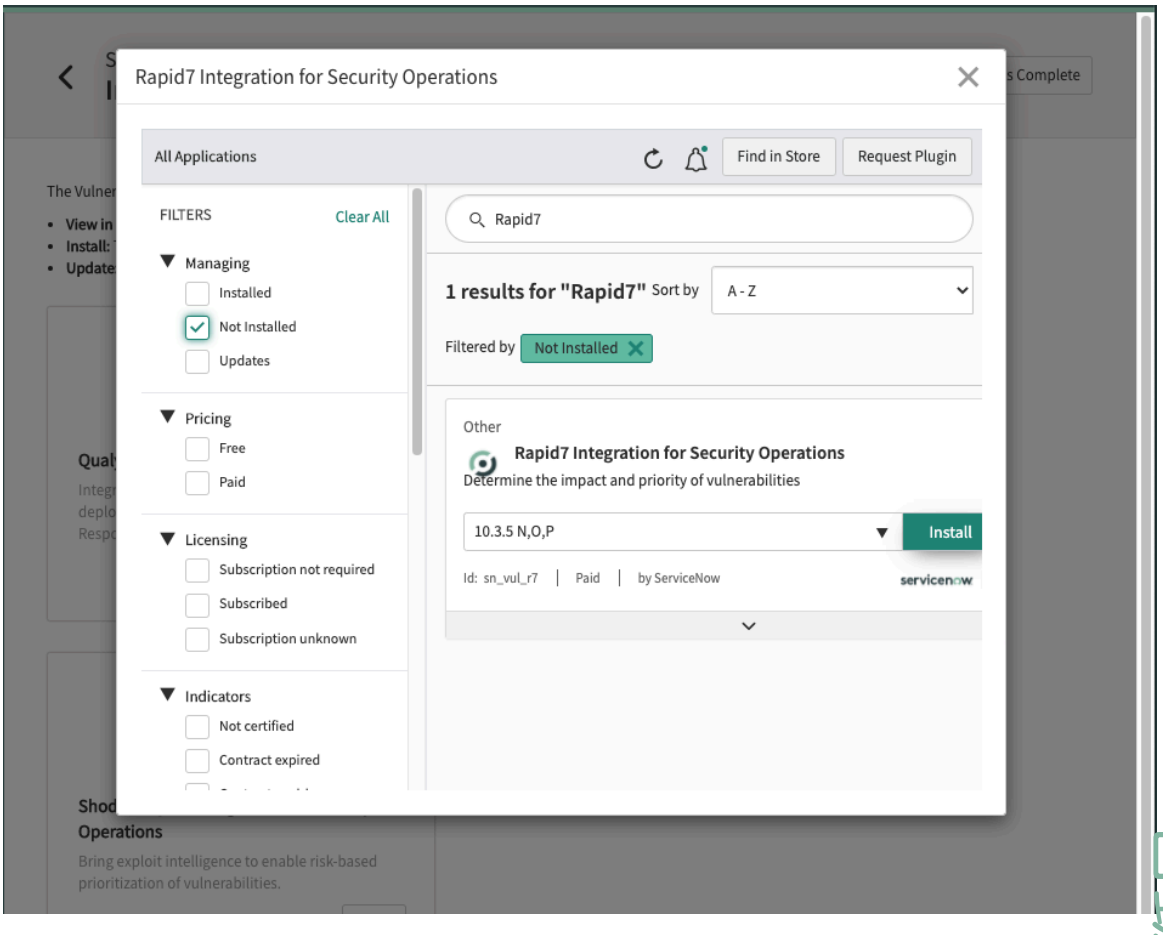


3. アプリケーションを見つけ、選択リストからバージョンを選択して、[インストール] をクリックします。

   アプリケーションの更新が利用できる場合は、[更新] ボタンが表示されます。

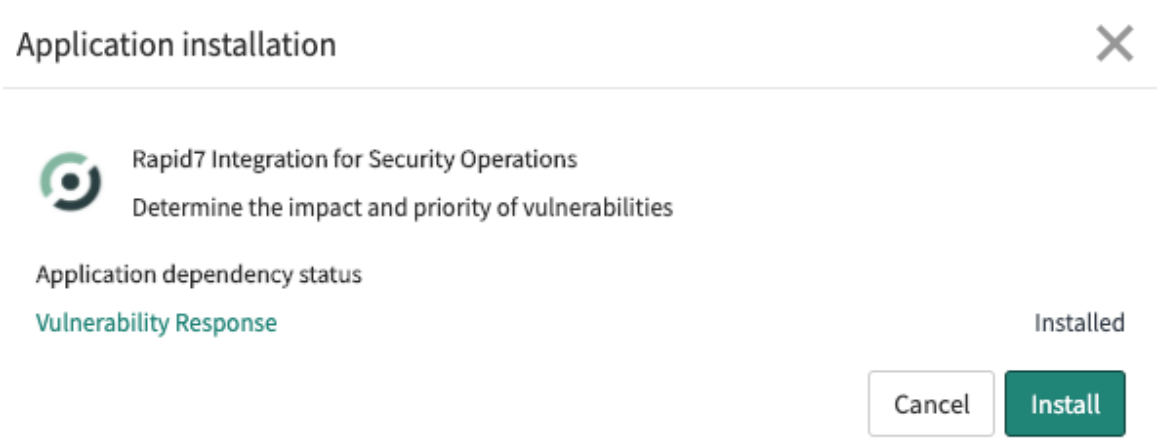
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[アプリケーションのインストール] ダイアログに、アプリケーション依存関係ステータスが表示されます。まだインストールされていない必要な依存関係は、アプリケーションとともに自動的にインストールされます。

4. [アプリケーションのインストール] ダイアログで [インストール] をクリックします。



インストールが正常に完了すると、[インストール] ダイアログに示されます。

5. ダイアログを閉じます。
アプリケーションが正常にインストールされたことを示す [すべてのアプリケーション] ページが表示されます。

自動翻訳

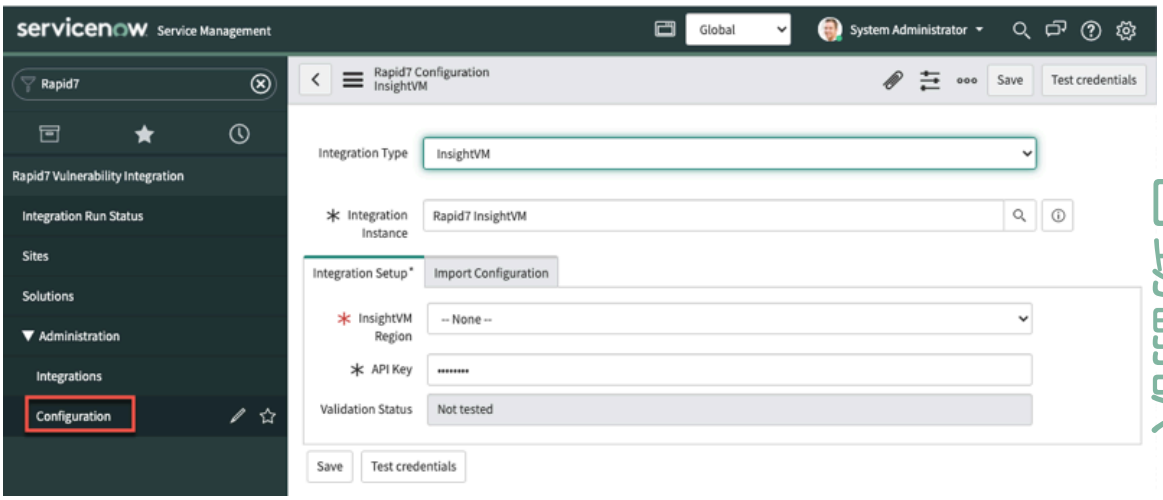
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インストールしてアクティブ化した後に、セットアップアシスタント の [統合構成] セクションから、以下のアプリケーションとインストール済みソリューションを直接構成、スケジュール設定、および起動できます。

- - Qualys 脆弱性統合
- Vulnerability Response Integration with Tenable。
- - Microsoft セキュリティレスポンスセンターソリューション統合
- - Red Hat Solution Integration
- Microsoft セキュリティレスポンスセンターソリューション統合
- Microsoft Defender Threat and Vulnerability Management 統合

上記に記載されていない他のアプリケーションの場合は、アプリケーションの構成モジュールに直接移動して構成を続行し、必要なサードパーティの認証情報を入力します。たとえば、次の画像は、Rapid7 アプリケーションの構成モジュールの場所を示しています。

特定のアプリケーションの構成の詳細については、各アプリケーションの製品名に従って、インストールおよび構成に関する製品ドキュメントを参照してください。



自動翻訳

次のタスク
アプリケーションがサポートされている場合は、セットアップアシスタントでアプリケーションの構成を続行します。

アプリケーションがセットアップアシスタントでの構成に対応していない場合は、アプリケーションの構成モジュールに直接移動して、構成を続行します。セットアップアシスタントでサポートされているアプリケーションを表示するには、「脆弱性対応 およびサポートされているアプリケーションのインストール」を参照してください。

NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理

まだインストールされていない場合は、サードパーティのスキャナー製品でインスタンスに脆弱性データをインポートする前に、NVD 統合をダウンロードして実行し、脆弱性対応の初期セットアップの一部として CWE スケジュール済みジョブを実行します。NVD の脆弱性対応統合は ServiceNow Store から入手可能です。

CWE および NVD データの取り込み

NVD と CWE の統合からインポートされたデータは、インスタンスの脆弱性データを拡張し、脆弱性、脆弱性一致アイテム、または修復タスクに対する修復をエスカレートさせるかどうかを決定するために使用されます。初回インポート後、ライブラリレコードをオンデマンドで更新したり、定期

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

的にレコードを更新するスケジュール済みジョブを設定できます。脆弱性対応 はそれらを [ライブラリ]に格納します。

NVD やサードパーティのエントリーに含まれる共通の脆弱性採点システム (CVSS) は、脆弱性の主な特徴をキャプチャします。脆弱性対応 は、CVSS データを使用して、脆弱性の重大度を反映する正規化値を生成します。重大度が計算されると、この脆弱性が組織にもたらすリスクをより深く理解できます。重大度は、脆弱性修復の評価と優先順位付けに役立ちます。

脆弱性対応 の初回インストールする時、またはサードパーティのスキャナー製品を使用して初めてデータを取り込む前：

1. CWE Comprehensive 2000 統合を使用して、CWE データの初期インポートを実行します。

   詳細については、「CWE レコードの更新のためのスケジュール済みジョブの構成および実行」を参照してください。デフォルトでは、統合レコードから [オンデマンド] で CWE 更新を実行します。スケジュール済みジョブとして実行する場合は設定する必要があります。

   > **注:**
   > NVD データベースの更新の前に実行するように CWE の更新をスケジュールします。NVD 更新のデフォルト日は [毎週] [月曜日] です。

2. 脆弱性対応 Integration with NVD アプリケーションがインストールされ、NIST National Vulnerability Database Integration - API (CVE のみ) または NIST National Vulnerability Database Integration - API (CVE および CPE) のデータが正常にインポートされたことを確認します。

   本番インスタンスでこのプラグインをアクティブ化するには、別のライセンスが必要になる場合があります。インストールされると、NIST National Vulnerability Database Integration - API (CVE のみ) がデフォルトでアクティブ化されます。これは、毎日実行されます。詳細については、「 NVD 統合の概要 」と「脆弱性対応 Integration with the NIST National Vulnerability Database のインストール」を参照してください。

3. サードパーティのライブラリはスケジュール済みジョブとして更新されます。サードパーティとの統合の詳細については、脆弱性対応 の統合 の統合ドキュメントを参照してください。

インポートされた脆弱性データと脆弱性一致アイテムを表示する

次のライブラリが利用可能です。

ライブラリ	説明
NVD	NVD によって検出された脆弱性のリストで、セキュリティチェックリスト、セキュリティ関連のソフトウェアの欠陥、不適切な構成、製品名、およびエクスプロイトを含む影響度メトリクスが含まれています。
CWE	コミュニティで開発されたソフトウェアの脆弱性タイプのリスト。 各 CWE レコードには、脆弱性を説明する関連するナレッジ記事も含まれています。[共通脆弱性タイプ一覧] 画面から脆弱性をエスカレートすることはできません。これは参照用です。
サードパーティ	インスタンスにインポートされたサードパーティ脆弱性のリスト。関連する参照、脆弱性一致アイテム、エクスプロイト、および CVE のリストが含まれています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

関連情報

脆弱性対応 脆弱性ライブラリの表示

脆弱性対応のソリューション管理アプリケーションのインストール

脆弱性対応 の 脆弱性対応のソリューション管理 機能をインスタンスで使用する前に、脆弱性ソリューション管理 アプリケーションのインストールを完了する必要があります。このアプリケーションは ServiceNow Store の別のサブスクリプションとして利用できます。

始める前に
インストールの前に、次のセットアップチェックリストを完了します。スムーズにインストールするために、これらのセットアップタスクを実行します。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

Microsoft セキュリティレスポンスセンターソリューション統合 および Red Hat Solution Integration は、脆弱性ソリューション管理 をインストールした後に 脆弱性対応のソリューション管理 で利用可能なソリューションアプリケーションです。

セットアップタスク	説明
脆弱性対応 アプリケーションがインストールされ、アクティブ化されていることを確認します。	脆弱性対応のソリューション管理 には、脆弱性対応 アプリケーションが必要です。 脆弱性ソリューション管理 の最新バージョンについては、最新バージョンの 脆弱性対応 がインストールされていることを確認してください。「KB0856498 脆弱性対応互換性マトリクスおよびリリーススキーマの変更」を参照してください。 アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応 のインストール」を参照してください。
アプリケーションのエンタイトルメントがあることを確認します。	脆弱性ソリューション管理アプリケーションのエンタイトルメントがあることを確認するには、次の場所に移動します サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 脆弱性ソリューション管理 アプリケーションのエンタイトルメントを ServiceNow Store から取得して Now Platform インスタンスにダウンロードするには、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」を参照してください。
NVD レコードが過去 10 年間の最新情報になっていることを確認します。	「NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
サードパーティ脆弱性が最新であることを確認します。	サードパーティ脆弱性統合の詳細については、「脆弱性対応 の統合」を参照してください。
インスタンスに必要な Now Platform ロールがアサインされていることを確認します。	インストールおよび予想される結果の検証には、次のロールが必要です。 脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。 • システムアドミニストレーター [admin] がアプリケーションをインストールします。まだアサインされていない場合は、アドミニストレーターが脆弱性アドミン [sn_vul.vulnerability_admin or sn_vul.admin (非推奨)] ロールをアサインします。 • 脆弱性アドミニストレーターは、構成を監視して予想される結果を確認します。

必要なロール：脆弱性ソリューション管理 アプリケーションをインストールするためのアドミン (admin) と、それを構成するための脆弱性アドミン (vulnerability admin)。

手順

1. ServiceNow Store に移動します。
2. [ログイン] をクリックし、HI 認証情報を入力します。
3. **[ServiceNow** 製品] タブをクリックして、利用可能な ServiceNow 製品を表示します。
4. **[Vulnerability Solution Management]** の横にあるプラス (**+**) 記号をクリックして、対象となるすべての関連アプリケーションを表示します。
5. [オプトイン] をクリックして、脆弱性ソリューション管理 アプリケーションのエンタイトルメントがあることを確認します。
6. 既にエンタイトルメントがある場合は、ステップ 10 にスキップして、Now Platform インスタンスにアプリケーションをインストールします。
7. プロンプトで契約条件に同意するには、チェックボックスをオンにして [承認] をクリックします。
   アプリケーションに正常にオプトインしたことを示すメッセージが表示されます。
8. オプション: 他の Now Platform インスタンスで 脆弱性ソリューション管理 のエンタイトルメントを管理する場合は、[エンタイトルメントの管理 (Manage Entitlement)] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[エンタイトルメントの管理 **(Manage Entitlement)]** ボタンが表示されていない場合は、製品リストの **[Vulnerability Solution Management]** アプリケーションをクリックして表示します。

a. オプションを選択

b. [OK] または [キャンセル] をクリックして続行します。
プラグインをアクティブ化して、インスタンスにアプリケーションをインストールする準備ができました。

9. 脆弱性ソリューション管理 アプリケーションをインストールする Now Platform インスタンスにログインします

10. 次のように移動する。 **All** (すべて) > システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて).

11. 脆弱性ソリューション管理 アプリケーション (sn_vul_solution) を見つけて、[インストール] をクリックします。
[アプリケーションのインストール] ダイアログに、アプリケーション依存関係プラグインステータスが表示されます。まだインストールされていない必要な依存関係は、アプリケーションとともに自動的にインストールされます。

12. [インストール] をクリックします。
このインストールには時間がかかる場合があります。アプリケーションとその依存関係が正常にインストールされると、インストールダイアログボックスにメッセージが表示されます。

脆弱性アドミニストレーターがセットアップアシスタント内からアプリケーションを構成できるようになりました。

13. [クローズ] をクリックします。

Microsoft セキュリティレスポンスセンターソリューション統合 および Red Hat Solution Integration は、脆弱性ソリューション管理 をインストールした後に 脆弱性対応のソリューション管理 で利用可能なソリューションアプリケーションです。

脆弱性ソリューションを表示するには、次の場所に移動します。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合設定 > ソリューション統合. 詳細については、「セットアップアシスタントを使用した 脆弱性ソリューション管理 のインストール済みソリューション統合の構成」を参照してください。

次のタスク
アプリケーションと利用可能なソリューションを構成した後、脆弱性ソリューション [sn_vul_m2m_vulnerability_solution] テーブルを使用して、CVE とソリューションが一致していることを確認します。

脆弱性対応のパフォーマンスアナリティクス **[PA]** アプリケーションのインストールと構成

脆弱性対応のパフォーマンスアナリティクス アプリケーションを使用する前に、エンタイトルメントを取得し、ServiceNow Store からアプリケーションをダウンロードして Now Platform インスタンスにインストールし、インストールと構成のいくつかの手順を完了する必要があります。PA アプリケーションは 脆弱性対応 アプリケーションの一部としてインストールされません。別のサブスクリプションで利用できます。

始める前に
インスタンスに既にアプリケーションがあり、新しいバージョンのアプリケーションに更新する場合は、次の手順 8 に進み、更新と構成を続行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

新規インストールの場合は、インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

プラグインとアプリケーションがインストールされ、アクティブ化されていることを確認するには、**All** (すべて) > サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

セットアップタスク	説明
脆弱性対応依存関係プラグイン (com.snc.vul_dep) がインストール済みでアクティブ化されていることを確認します。	脆弱性対応依存関係 このプラグインには、アプリケーションをサポートするために必要なすべての依存関係プラグインが含まれます。 プラグインがインストールされてアクティブ化されていることを確認するには、アプリケーションを希望するインスタンスで、 システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて). 他の依存関係プラグインを更新するように求められた場合は、ダイアログのリンクをクリックし、プロンプトに従って続行します。
ServiceNow 脆弱性対応 アプリケーション (sn_vul) がインストールされ、アクティブ化されていることを確認します。	脆弱性対応 プラグインがインストールされてアクティブ化されていることを確認するには、アプリケーションを希望するインスタンスで、 システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて). 他の依存関係プラグインを更新するように求められた場合は、ダイアログのリンクをクリックし、プロンプトに従って続行します。 本番インスタンスでこのプラグインをアクティブ化するには、別のライセンスが必要になる場合があります。詳細については、ServiceNow にお問い合わせください。
インスタンスに必要な ServiceNow ロールがあることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

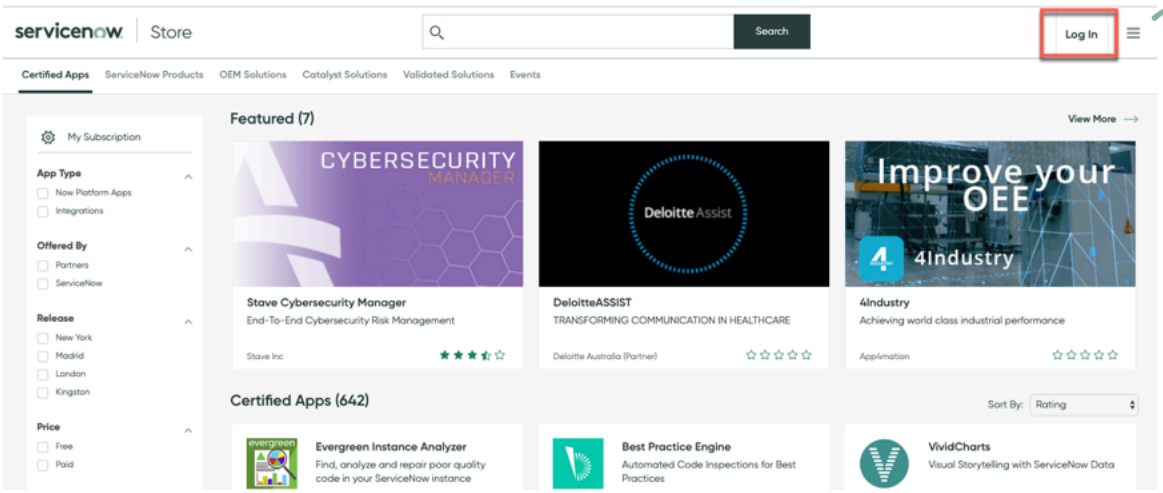
自動翻訳

セットアップタスク	説明
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。	• パフォーマンスアナリティクスアドミン [pa_admin] またはシステムアドミニストレーター [admin] がアプリケーションをインストールし、予想される結果を検証します。 • 脆弱性アドミン [sn_vul.vulnerability_admin または sn_vul.admin (非推奨)] が PA ダッシュボードを使用して構成を監視し、予想される結果を検証します。 • 修復オーナー [sn_vulc.remediation_owner] は、変更管理タスクを監督し、アサインされたレコードの読み取りと更新を行います。sn_vul.remediation_owner ロールは、ユーザーに itil ロールをアサインすると自動的にアサインされます。
パフォーマンスアナリティクスと 脆弱性対応 アプリケーションに互換性があることを確認します。	互換性情報については、「KB0856498 脆弱性対応互換性マトリクスおよびリリーススキーマの変更」を参照してください。

必要なロール：admin または pa_admin

手順

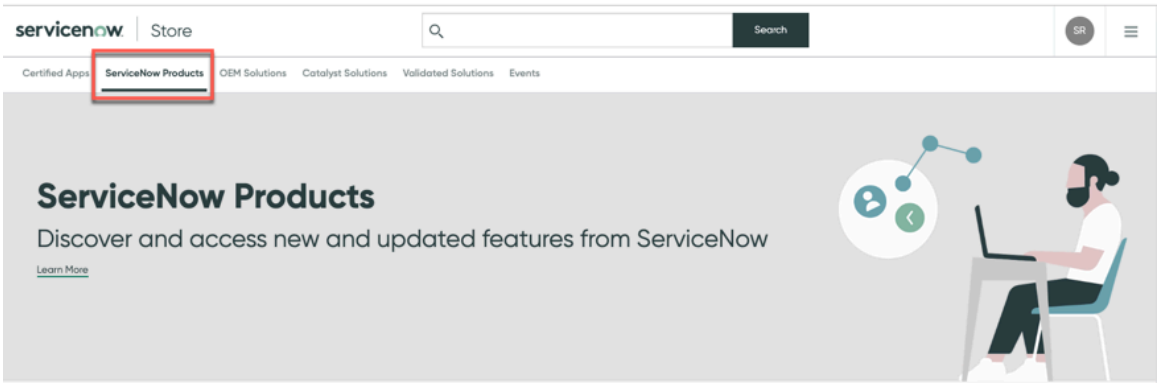
1. エンタイトルメントを取得して Now Platform インスタンスにアプリケーションをダウンロードするには、ServiceNow Store に移動します。
2. ページ右上にある [ログイン] をクリックします。



3. 表示されるダイアログで、HI 認証情報を入力し、[ログイン] をクリックします。
4. 表示されるページで選択されていない場合は、**[ServiceNow 製品]** タブをクリックします。

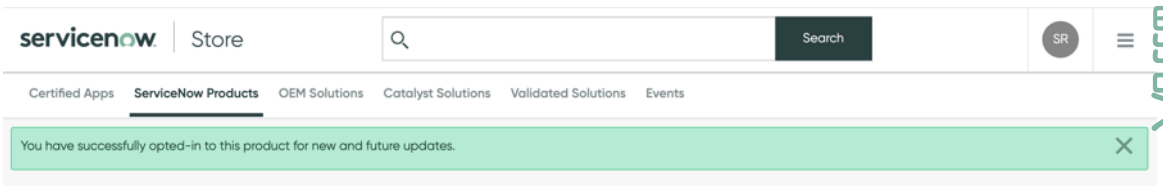
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. 製品リストページで、[パフォーマンスアナリティクス - 脆弱性対応] をクリックします。

6. [インスタンス名] と [インスタンスの理由] を入力し、[インスタンスを検証] をクリックします。[オプトイン] ボタンのあるページが表示されます。
7. 脆弱性対応のパフォーマンスアナリティクス アプリケーションを取得するには、[オプトイン] をクリックします。
8. 契約条件に同意するには、チェックボックスをオンにして [同意する] をクリックします。



9. オプション: または、他の Now Platform インスタンスでアプリケーションのエンタイトルメントを管理するには、次の手順に従います。

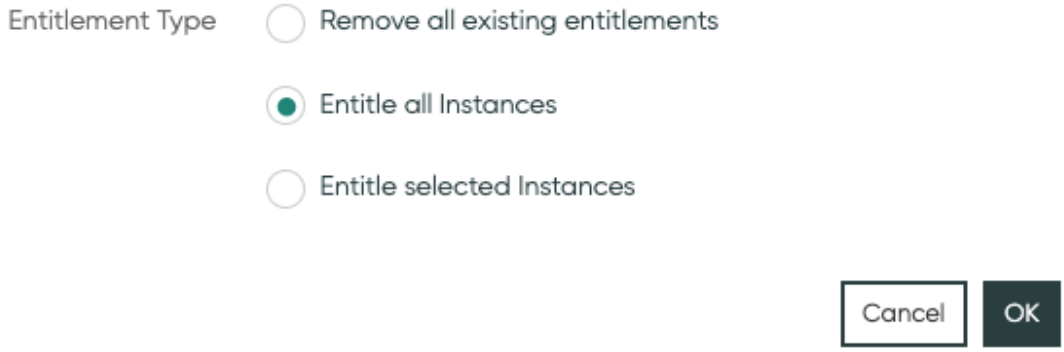
   a. [エンタイトルメントの管理 (Manage Entitlements)] ボタンが表示されていない場合は、製品リストの 脆弱性対応のパフォーマンスアナリティクス アプリケーションをクリックして表示します。

   b. [適格] タブを選択した状態で、[エンタイトルメントの管理 **(Manage Entitlements)]** をクリックします。

   c. 表示される [Vulnerability Response のエンタイトルメントの管理 (Manage Entitlements for Vulnerability Response)] ダイアログで、次のいずれかを選択します。

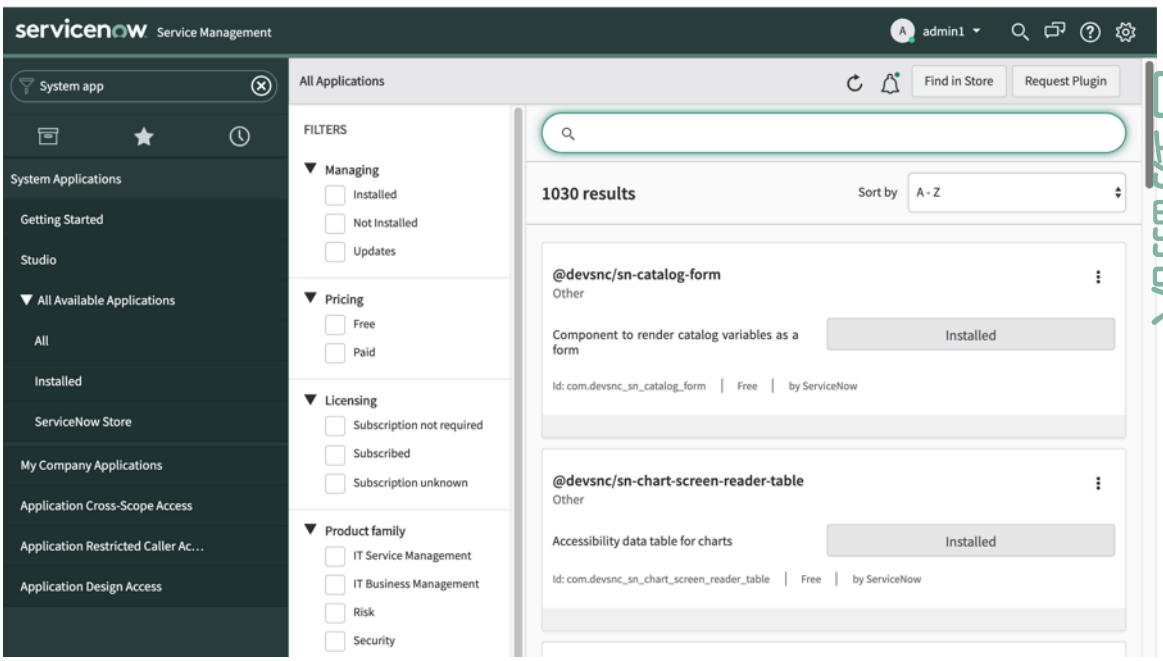
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



d. **[OK]** または [キャンセル] をクリックして続行します。
プラグインをアクティブ化して Now Platform インスタンスにアプリケーションをインストールする準備ができました。

10. 脆弱性対応 アプリケーションをインストールする Now Platform インスタンスにログインします
11. 次のように移動する。 **All** (すべて) > システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて).



12. リストされたアプリケーションから、 パフォーマンスアナリティクス - コンテンツパック - 脆弱性対応 (sn_vul_analytics) アプリケーションを見つけて、[インストール] をクリックします。

> **注:**
> 新しいバージョンに更新する場合は、選択リストから必要なバージョンを選択します。

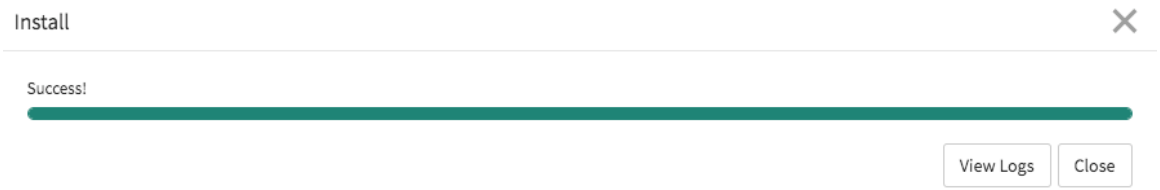
次に、[更新] をクリックします。
[アプリケーションのインストール] ダイアログが表示されます。アプリケーションとともに自動的にインストールされる依存関係も表示されます。

13. オプション: デモデータが必要な場合、[デモデータのロード] チェックボックスをオンにして、[インストール] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[デモデータのロード] チェックボックスをオンにしないと、後でアプリケーションマネージャーからデモデータをインストールできません。初期インストール後にデモデータをインストールまたは再インストールする方法については、Now Support ナレッジベースで「アプリケーションが既にインストールされている場合にデモデータをインストールする方法 [KB0722909] 」記事を参照してください。

このインストールには時間がかかる場合があります。アプリケーションが正常にインストールされると、インストールダイアログにメッセージが表示されます。

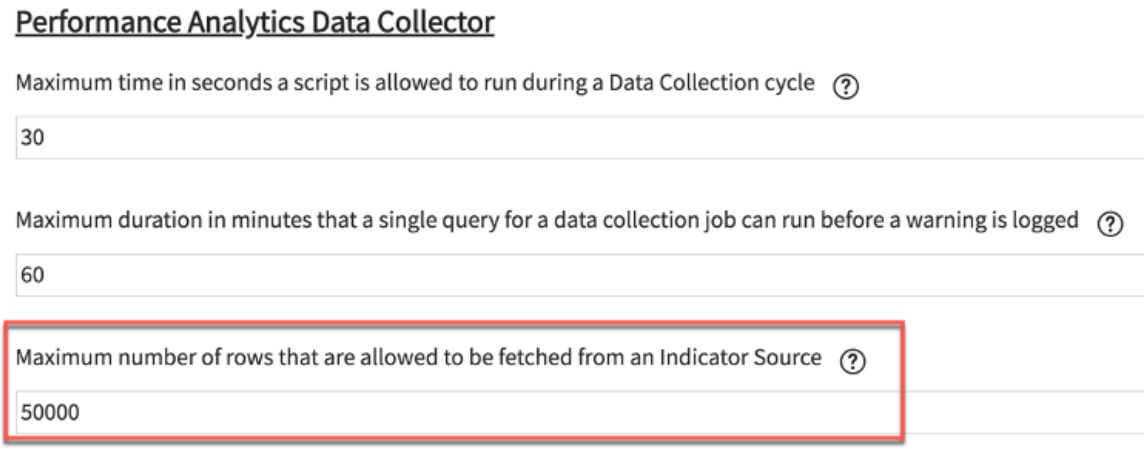


14. [クローズ] をクリックします。
15. オプション: 環境内に多数のアクティブな脆弱性一致アイテムがあることが予想される場合は、収集するレコードの最大数のデフォルト設定を変更し、スケジュール済みジョブを有効にして、営業時間外に収集することをお勧めします。
インストール後にアプリケーションのこれらの設定やその他の設定を変更するには、次の手順を実行します。

    a. 次のように移動する。 **All** (すべて) > パフォーマンスアナリティクス > 管理コンソール.

    b. [詳細構成] タイルで、[パフォーマンスアナリティクス プロパティ] リンクをクリックします。

    c. 管理コンソールの [パフォーマンスアナリティクス] ページで、[パフォーマンスアナリティクスデータコレクター (パフォーマンスアナリティクス Data Collector)] セクションまでスクロールします。
    デフォルト設定 (50,000 レコード) が、[インジケーターソースから取得することができる最大行数] に表示されます。



    d. この数は、現在の環境で予想されるアクティブな脆弱性一致アイテム (VI) の合計数よりも約 20% 多い値にまで増やすことをお勧めします。

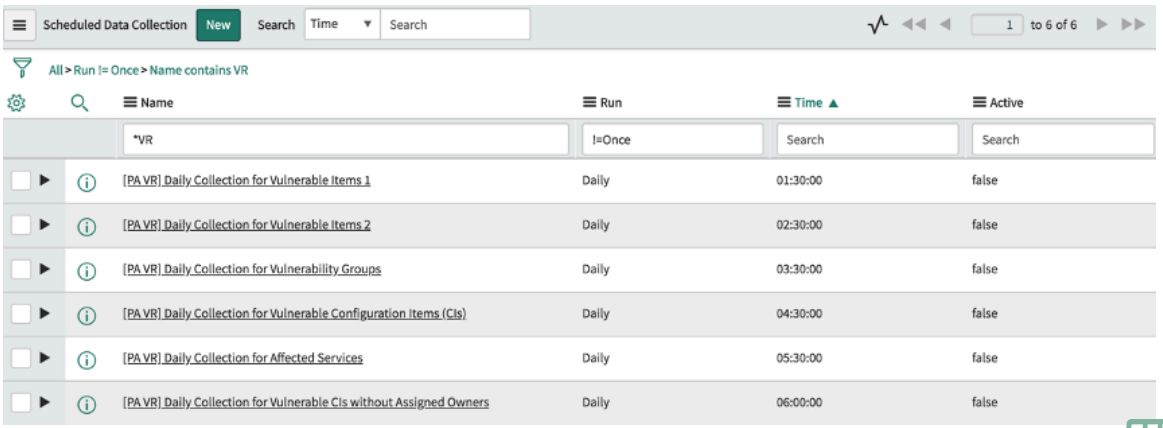
    e. **[Save** (保存)] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

f. スケジュール済みジョブを有効にするには、次に移動します: パフォーマンスアナリティクス > データコレクター > ジョブ.
[スケジュール設定済みデータ収集] リストが表示されます。[アクティブ] 列では、 パフォーマンスアナリティクス - コンテンツパック - 脆弱性対応の [アプリケーション] 列にリストされているスケジュール済みジョブは、デフォルトで無効 (false) になっています。

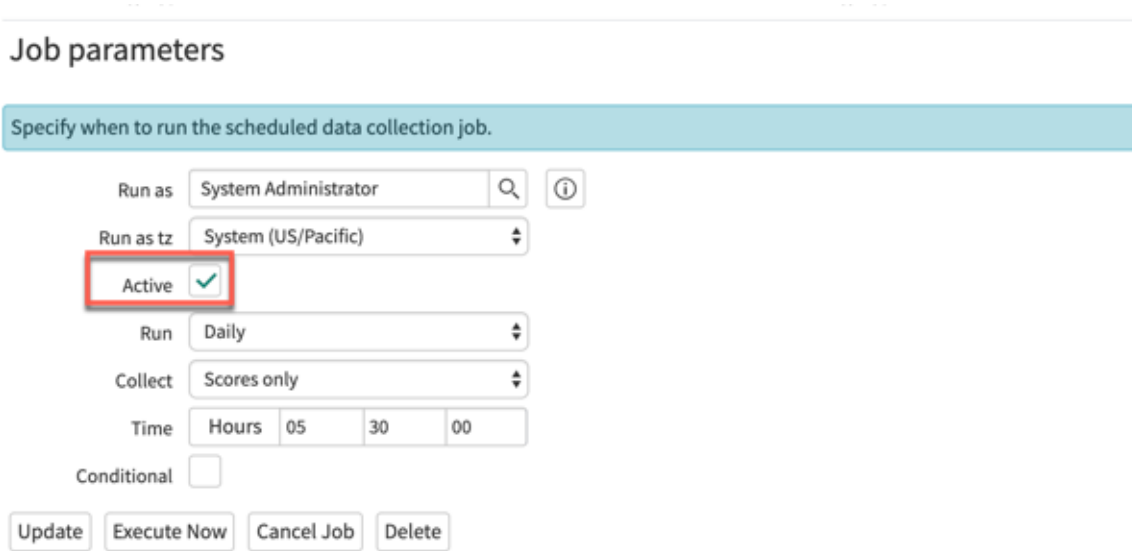
> **注:**
> 履歴データ収集のスケジュール済みジョブは、ジョブのリストに表示されません。大規模なデータセットの場合は、脆弱性対応 のパフォーマンスアナリティクスアプリケーションを設定するときに日次ジョブを有効にして、時間ごとのデータと傾向の収集を開始することをお勧めします。



g. [名前] 列で、リンクをクリックして PA_VR ジョブレコードを開きます。

h. フィールドが編集可能でない場合は、[ここ] リンクをクリックして編集します。

i. [ジョブパラメーター] セクションで、[アクティブ] チェックボックスをクリックしてジョブをスケジュールします。
時間フィールドが表示されます。



j. ジョブの開始時間を入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

大量であることが予想される場合は、営業時間外に収集時間を設定することをお勧めします。環境内で 1,000 万以上のアクティブな VI が予想される場合は、データ収集環境の設定の詳細について、ServiceNow の実装パートナーにお問い合わせください。

データ収集に使用されるインジケーターの詳細については、「脆弱性対応 の パフォーマンスアナリティクス [PA] インジケーターの表示」を参照してください。

k. 必要なすべてのジョブを有効にしたら、[更新] をクリックします。
[スケジュール設定済みデータ収集] リストが表示されます。詳細については、「パフォーマンスアナリティクスのプロパティ」を参照してください

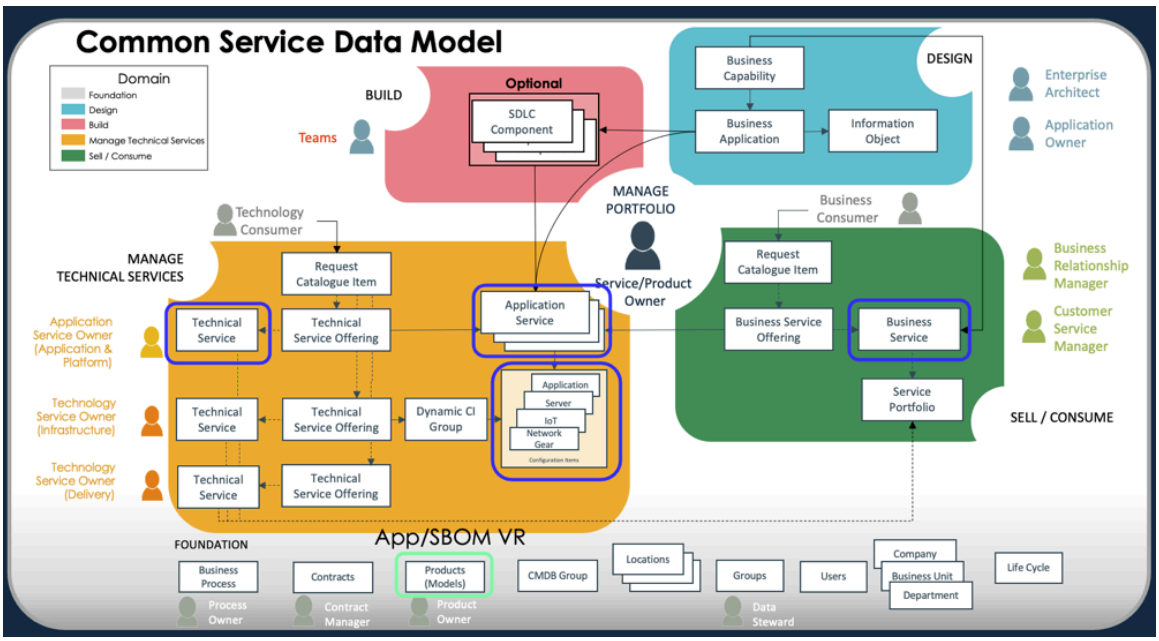
次のタスク

次のように移動する。 脆弱性対応 > 概要 をクリックしてダッシュボードを表示します。

脆弱性対応 アプリケーション と **CSDM** テーブル

テーブル 脆弱性対応、 アプリケーション脆弱性対応、サードパーティの脆弱性統合、および ソフトウェア部品表 アプリケーションは、 CSDM テーブルを管理 (データ提供) します。これらのアプリケーションは、他のアプリケーションが生成する CSDM テーブルのデータも使用します。したがって、いくつかの ServiceNow 製品は、これらの セキュリティオペレーション アプリケーションの恩恵を受け、価値を付加します。

CSDM Data Framework と 脆弱性対応 アプリケーション



CSDM脆弱性対応、アプリケーション脆弱性対応、サードパーティの脆弱性統合、およびソフトウェア部品表アプリケーションによって参照されるテーブル

資産はサードパーティの脆弱性スキャナー (統合) からインポートされると、 脆弱性対応 に取り込まれて特定のテーブルに表示されます。

- ホスト 脆弱性対応 検出済みアイテム。
- クラウドおよび コンテナ脆弱性対応 検出イメージ
- アプリケーション脆弱性対応 検出されたアプリケーション (製品モデル)

セキュリティオペレーション CMDB 構成アイテム (CI) ルックアップの一部として、インポートされたデータの (CI) レコードを CMDB 内の既存のレコードと照合する検索が実行されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

特定の各 CI レコードには、脆弱性一致アイテムのアサインルールの入力として使用できる CI に入力される、サポートグループや分類などの検出不可能な属性が含まれている場合があります。これらの属性は、アップストリームのテクニカルサービスオファリングに基づく共通サービスデータモデル (CSDM) の同期から入力される場合があります。

脆弱性対応、アプリケーション脆弱性対応、サードパーティの脆弱性統合、およびソフトウェア部品表アプリケーションに関連する CSDM オブジェクトを利用する場合は、スクリプト化されたルールを使用する必要があります。

たとえば、脆弱性一致アイテムのアサインルールを使用して修正のために脆弱性一致アイテムを自動的にアサインするには、インポートされた脆弱性エントリーで更新される構成アイテム分類の値を活用するルールを作成できます。この場合、関連する CSDM オブジェクトから必要なターゲット値をクエリするためのスクリプト化されたルールが必要です。

以下は、CI に Java があり、脆弱性エントリーに関連付けられているかどうかを確認するために使用できるスクリプト化されたクエリの例です。

Scripted (query)

脆弱性対応、 アプリケーション脆弱性対応、サードパーティの脆弱性統合、および ソフトウェア部品表 アプリケーションは、次のテーブルを参照します。詳細については、 CSDM データフレームワークと 脆弱性対応 アプリケーションの画像を参照してください。

- 製品モデル [cmdb_model] テーブル (アプリケーション脆弱性対応 と ソフトウェア部品表 で参照)。
- アプリケーションモデル [cmdb_application_product_model] テーブル (アプリケーション脆弱性対応 と ソフトウェア部品表 によって参照されます)。
- 構成アイテム [cmdb_ci] テーブル。
- ビジネスサービス [cmdb_ci_service_business] テーブル。
- サービス [cmdb_ci_service] テーブル。
- CMDB グループ [cmdb_group] テーブル。
- ダイナミック CI グループ [cmdb_ci_query_based_service] テーブル。

CSDM脆弱性対応、アプリケーション脆弱性対応、サードパーティの脆弱性統合、およびソフトウェア部品表アプリケーションによって使用されるテーブル

1. 製品モデル [cmdb_model] テーブル (アプリケーション脆弱性対応 と ソフトウェア部品表 で使用)。
2. アプリケーションモデル [cmdb_application_product_model] テーブル (アプリケーション脆弱性対応 と ソフトウェア部品表 で使用)。
3. 構成アイテム [cmdb_ci] テーブル。
4. ビジネスアプリケーション [cmdb_ci_business_app] (アプリケーション脆弱性対応 および ソフトウェア部品表 で使用)
5. ビジネスサービス [cmdb_ci_service_business]。
6. テクニカルサービス [cmdb_ci_service_technical]。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

ソフトウェア部品表ファイルをアップロードすると、SBOM アプリケーションは、アップロードした製品モデルとビジネスアプリケーションを、CMDB に既に存在するものと照合しようとします。アプリケーションサービスまたはビジネスアプリケーションを製品モデルにリンクできます。

脆弱性対応、アプリケーション脆弱性対応、サードパーティの脆弱性統合およびソフトウェア部品表アプリケーションに付加価値を提供する製品

次のServiceNow製品で脆弱性対応アプリケーションを使用すると、組織にメリットがあります。

サードパーティの脆弱性スキャナーと統合

脆弱性情報データベース (NVD) からインポートされた脆弱性とサードパーティスキャナーからの検出データは、CMDB の資産で調整されます。インポートされた脆弱性が既存の資産と一致する場合、脆弱性一致アイテムが作成されます。脆弱性一致アイテムは、修復のためのタスクに自動的にグループ化され、ビジネスコンテキストでリスクスコアが付けられ、優先順位が付けられ、修復のために適切なチームにアサインされます。統合の詳細とリストについては、「 脆弱性対応 の統合」を参照してください。

CWE Comprehensive 2000 と NVD の統合

NIST 脆弱性情報データベース (NVD) と共通脆弱性タイプ一覧 (CWE) の統合からインポートされたデータは、インスタンスの脆弱性データを拡張して、脆弱性、脆弱性一致アイテム、または修復タスクの修復をエスカレートするかどうかを決定するために使用されます。詳細については、「NVD 統合の概要」と「CWE レコードの更新のためのスケジュール済みジョブの構成および実行」を参照してください。

との統合によりメリットが得られる製品 ソフトウェア部品表

セキュリティポスチャコントロール

セキュリティポスチャコントロール により、サイバーセキュリティチームはエンタープライズ資産インベントリ全体を可視化し、全体的なセキュリティポスチャを判断できるようになります。SPC のポリシーは、脆弱性対応アプリケーションでインポートする脆弱性のある資産を検出して、セキュリティツールの範囲のギャップを見つけるのに役立ちます。

ガバナンス、リスク、コンプライアンス

統合されたリスクプログラムでセキュリティと IT をつなぎ、継続的な監視、優先順位付け、および自動化を行います。

DevOps

GitHub 環境から開始する GitHub Actions を使用して、ソフトウェア開発サイクル中に潜在的に有害なコンポーネントから環境を保護します。GitHub リポジトリから SBOM ファイルを Now Platform にアップロードします。

脆弱性対応 アサインルールの作成または編集

セットアップアシスタントを使用してアサインルールの初期アセスメントを完了したら、フィルター条件に基づいて脆弱性一致アイテムを自動的にアサインするルールを作成できます。こうしたルールは、インポート時または手動作成時に脆弱性一致アイテムをアサインします。

始める前に

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

イン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

このタスクについて

ベースシステムには、**[CI** サポートグループにアサイン] という 1 つの脆弱性アサインルールが付属しています。このルールは、CI サポートグループと同じアサイン先グループに脆弱性一致アイテムをアサインします。フィルター条件を使用してこのルールを変更するか、新しいルールを作成できます。アサインルールでは、アサインの条件と実行順序を定義します。VI がルール条件に一致すると、アサインルックアップは停止します。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > アサインルール.
2. **[CI** サポートグループに割り当て] ルールを開くか、[新規] をクリックします。
3. [新規] の場合、必要に応じて、フォームのフィールドに入力します。

脆弱性アサインルール

フィールド	説明
名前	グループルールの名前。
有効	アサインルールがアクティブかどうかを示します。
実行順序	このルールが評価される順番。 最優先のルール (特別な処理が必要なアイテム、リスクが重大な場合、または VI を規制コンプライアンスによって処理する必要がある場合) が最初に実行されます。次に、一般的なルールを実行します。この場合、特別な処理は必要なく、誰が責任を負うべきかがわかっています。最後に、VI をグループにアサインするデフォルトのルールを作成します。これにより、どのアサイン先グループに属すべきかが決定されます。このグループは、決定を対象に別のルールを追加できます。このデフォルトルールは最後に実行されます。
説明	アサインルールの説明。
条件	
プレビュー	このクエリが返す結果の数を表示します。
条件フィールド	満たす必要がある条件。 **注:** Rapid7 InsightVM 資産タグをアサインルールの条件フィルターで使用できるようにするには、他の Rapid7 InsightVM 統合の前に Rapid7 InsightVM 資産リスト統合を実行する必要があります。 条件ビルダーに入力した検索テキストの大文字と小文字の区別は、このレコードまたはフォームではサポートされていません。
新しい基準	選択する条件フィルターフィールドを追加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
次を使用してアサイン	このルールに基づいて作成されたグループのアサインを自動化するには、利用可能なオプションの 1 つを選択します。 ○ ユーザーグループ：ルックアップテーブルからユーザーグループを選択します。 ○ ユーザーグループフィールド：ドロップダウンメニューからユーザーグループフィールドを選択します。 ○ スクリプト：スクリプトを作成または編集します。 **注:** スクリプトの作成または編集には ServiceNow の専門知識が必要です。

4. **[Submit]** をクリックします。
次のインポートで新しいルールまたは更新されたルールが評価されます。

注:

再適用機能には、ルールのベースラインアプリケーションが必要です。ルールを作成したら、まだ実行していない場合は、都合に応じて *Reapply all vulnerability assignment rules* スケジュール済みジョブをアクティブ化して実行します。手動でアサインされたものを除くすべてのオープン VI に対して、すべてのルールが適用されます。環境内のアクティブな VI の数に応じて、最初の実行後に [実行] フィールドを適切に設定して、パフォーマンスに影響がないようにすることを忘れないでください。

このスケジュール済みジョブを実行していない場合は、[アサインルール] フォームで [変更を適用] ボタンを使用しようとするときに実行する必要があります。アサインルールを再適用しても、脆弱性一致アイテムは再グループ化されません。

ML を使用した 脆弱性対応 アサインルールの作成

次のスクリプトを使用して、予測インテリジェンスからの ML 推奨事項を使用して修復にそれらの推奨事項を自動的にアサインする、脆弱性一致アイテムの予備連絡先アサインルールを作成します。

始める前に

脆弱性対応 アプリケーションに対する脆弱性アサインの推奨をインストールしてアクティブ化する必要があります。このアプリケーションは ServiceNow Store から入手できます。

分類ソリューションを定義し、アクティブ化し、トレーニングする必要があります。このモデルを使用すると、アサインルールで意図した受信者との正しい一致が検出されなかった場合に、脆弱性一致アイテム (VI) の適切なアサイン先グループを予測できます。

このルールは、他のアサインルールが既に完了した後で未アサインの VI の数を減らすのに役立ちます。

詳細については、「脆弱性対応対応 脆弱性アサインの推奨 のインストール」と「脆弱性対応 のソリューション定義の作成とトレーニング」を参照してください。

必要なロール：sn_vul.vulnerability_admin

このタスクについて

高度なコーディング経験がある場合、または Now Platform とその予測インテリジェンスの機能、およびアサインルールの仕組みに関する詳細な知識がある場合にのみ、このタスクを実行することをお勧めします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > アサインルール.
2. **[New** (新規)] を選択します。
3. 必要に応じて、フォームのフィールドに入力します。
   これらのフィールドの詳細については、「脆弱性対応 アサインルールの作成または編集」を参照してください。
4. [次を使用してアサイン (Assign using)] 選択リストから [スクリプト] を選択します。
5. エディターで、次のスクリプトをコピーして貼り付けます。

```
   /*
   * Catch-all assignment rule using ML recommendation
   * NOTE: Requires Vulnerability Assignment Recommendations for Vulnerability Response
   * Classification Solution must be active and trained
   */
var vitID = current.sys_id;
getMLAssignmentRecommendation(vitID);

function getMLAssignmentRecommendation(vulnerableItemSysId) {
   var ARU = new sn_vul.AssignmentRecommendationUtils();
   ARU.initialize();

   var viPredictionObj = ARU.getPredictionsForVI(vulnerableItemSysId);
   /*
   *returns object containing array of predictions
   *payload structure:
   *
   {
      "predictions": [
         {
            "sys_id": "b6ed54f3db7b23005daef4eabf9619f3",
            "name": "Windows Server support ",
            "confidence_score": "57.54"
         },
         ...
      ],
      "exception": ""
   }
   */
   var viPredictionArray = viPredictionObj['predictions'];
   var topPredictionObj = viPredictionArray.shift();

   return topPredictionObj['sys_id'];
}
```

6. [送信] を選択します。

次のタスク

アサインルールと *Reapply all vulnerability assignment rules* スケジュール済みジョブに関する一般的な情報については、「脆弱性対応 アサインルールの概要」を確認してください。

サービスサポートの 脆弱性対応 アサインルールの作成

次のスクリプトを使用して、影響を受けるビジネスサービスに基づいて、修復のために脆弱性一致アイテムをアサインするルールを作成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：sn_vul.vulnerability_admin

このタスクについて
高度なコーディング経験がある場合、または Now Platform とアサインルールの仕組みに関する詳細な知識がある場合にのみ、このタスクを実行することをお勧めします。

このルールを使用すると、CMDB にリストされているビジネスサービスと VI の一致度に応じて VI がアサインされます。関連するサービス、部門、またはサポートグループが一致しない場合、VI は脆弱性アナリストグループにアサインされます。

このルールは、他のアサインルールが既に完了した後で誤ってアサインされている VI の数を減らすのに役立ちます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > アサインルール.
2. **[New** (新規)] を選択します。
3. 必要に応じて、フォームのフィールドに入力します。
   これらのフィールドの詳細については、「脆弱性対応 アサインルールの作成または編集」を参照してください。
4. [次を使用してアサイン (Assign using)] 選択リストから [スクリプト] を選択します。
5. エディターで、次のスクリプトをコピーして貼り付けます。

```
/*
Assigns Vulnerable Item based on related Business Service
Assigns to default Vulnerability Analyst group if no related Business Service
*/
assignToServiceSupport(current);

function assignToServiceSupport(vitGR) {
   var ci = vitGR.getValue('cmdb_ci');
   var defaultAssignmentGroup = 'Vulnerability Analyst';
   var defaultGR = new GlideRecord('sys_user_group');
   defaultGR.get('name', defaultAssignmentGroup);
   var defaultAssignmentGroupID = defaultGR.sys_id;

   var maxSizeValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_size", 1000);
   var maxDepthValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_depth", 10);
   var customValues = {
      "maxDepth": maxDepthValue,
      "maxSize": maxSizeValue
   };
   var ciu = new global.CIUtils();
   var services = ciu.servicesAffectedByCI(ci, customValues);
   var svc = new GlideRecord("cmdb_ci_service");
   var hasSvc = false;
   if (services && services.length > 0) {
      svc.addQuery("sys_id", "IN", services.join(",")); // returns the service with highest
business criticality. Implement alternate logic here.
      svc.addNotNullQuery("busines_criticality"); // typo intended
      svc.orderBy("busines_criticality");
      svc.setLimit(1);
      svc.query();
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
        hasSvc = svc.next();
    }
    if (!hasSvc) {
        // If there are no services it should be assigned to a default assignent group
        return defaultAssignmentGroupID;
    } else {
        var serviceAssignmentGroup = hasSvc.getValue('support_group'); //Also consider
managed_by_group, assignment_group, change_control
        return !gs.nil(serviceAssignmentGroup) ? serviceAssignmentGroup :
defaultAssignmentGroupID; //Return the Service assignment group if it is not empty, return
the default assignment group otherwise.
    }
}
```

6. [送信] を選択します。

次のタスク

アサインルールと *Reapply all vulnerability assignment rules* スケジュール済みジョブに関する一般的な情報については、「脆弱性対応 アサインルールの概要」を確認してください。

脆弱性対応 修復タスクルールの作成または編集

セットアップアシスタントを使用して修復タスクルールの初期アセスメントを完了したら、フィルター条件に基づいて脆弱性一致アイテムを自動的にグループ化するルールを作成できます。こうしたルールは、インポート時または手動作成時に脆弱性一致アイテムを自動的にグループ化します。フィルターを使用して、エクスプロイトを含むすべての脆弱性一致アイテムを選択するなど、このルールによってグループ化された脆弱性一致アイテムを制限します。

始める前に

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

このタスクについて

ベースシステムには、脆弱性とアサイン先グループ (アサインルールからのもの) によって脆弱性一致アイテムをグループ化する、1 つの修復タスクルール [脆弱性] が付属しています。フォームまたはリストビューからルールを再適用できます。一部のサンプルエントリーについては、「脆弱性対応 修復タスクルールの例」を参照してください。

このルールは次のように変更できます。

フィルター条件と [グループ] の選択肢を使用する。

デフォルトでは、修復タスクはアサインルールをフィルター基準の一部として使用します (利用可能な場合)。

> **注:**
> アサインルールが存在しない場合は、[ユーザーグループ] フィールドを使用してグループを選択できます。

脆弱性対応 のバージョン 18.0 以降、新しい実装の 脆弱性対応 で [脆弱性] 修復タスクルールが非アクティブ化されています。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 修復タスクルール.

2. ルールを開くか、[新規] をクリックします。

3. [新規] の場合、必要に応じて、フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクルール

フィールド	説明
名前	タスクルールの名前。
有効	タスクがアクティブかどうかを示します。
説明	ルールの説明。
大文字と小文字を区別	条件が大文字と小文字を区別するかどうかを決定します。 **注:** デフォルト値は、大文字と小文字の区別なしです。
条件	ルールのオプションのフィルター条件。 **注:** Rapid7 InsightVM 資産タグを修復タスクルールの条件フィルターで使用できるようにするには、他の Rapid7 InsightVM 統合の前に Rapid7 InsightVM 資産リスト統合を実行する必要があります。 デフォルト ([大文字と小文字を区別] チェックボックスが無効) では、タスクルールのレコードとフォームで条件ビルダーに入力する検索テキストは、大文字と小文字が区別されません。選択によって、タスクのレコードとフォームで大文字と小文字を区別する検索を有効にできます。
グループ (最大 **6** つの条件セットが利用可能)	
脆弱性一致アイテムのグループ化元	ルールが VI をグループ化するために使用するテーブル。最大 6 つのフィルターを設定できます。 選択肢は次のとおりです。 ○ 脆弱性一致アイテム [sn_vul_vulnerable_item] ○ 脆弱性一致アイテム → 構成アイテム [cmdb_ci] ○ 脆弱性一致アイテム → 脆弱性 [sn_vul_third_party_entry] **注:** 拡張テーブルを選択した場合、[使用フィールド] はその拡張テーブルを使用する脆弱性一致アイテムにのみ適用されます。
使用フィールド	ルールが VI をグループ化するために使用するテーブルのフィールド。
アサイン	
修復タスクをアサインする基準	修復タスクを自動的にアサインする場合、[グループ] の選択肢に加えて [アサイン] の選択肢が、脆弱性一致アイテムをグループ化するために使用されます。必要に応じて新しいタスクが作成され、一致するアサイン先グループが設定されたタスクに各脆弱性一致アイテムが配置されるようにします。 このルールに基づいて作成されたタスクのアサインを自動化するには、利用可能なオプションのいずれかを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ [グループ分け基準] フィールド：[グループ分け基準] セクションの [使用フィールド **(Using field)**] からユーザーグループフィールドを選択すると、そのフィールドがドロップダウンメニューに表示されます。 ○ ユーザーグループ：ルックアップリストを使用して、静的ユーザーグループを選択します。

注:
[グループ] 設定をやり直す場合は、[グループフィールドをクリア] 関連リンクでフォームの [グループ] フィールドをリセットします。

グループルールが削除されると、フォームまたはリストビューから、そのルールによって作成されたすべてオープングループを削除できます。[オープン] ステータスでないグループは除外されます。

一部のサンプルエントリーについては、「脆弱性対応 修復タスクルールの例」を参照してください。

脆弱性対応リスク算出のリスクルールのフィールドと重み付けの定義

組織に固有の脆弱性や資産データを利用したリスクスコアを生成できるように、リスクルールのパラメーターと重み付けをカスタマイズします。リスクルールに含まれるフィールドを選択することで、効果的なリスクスコアリングフレームワークを定義できます。

始める前に

さらに、構成管理データベース (CMDB) の configuration_item [cmdb_ci] の属性を使用して、脆弱性対応のリスク算出のロジックを作成できます。たとえば、組織内で外部向け CI の方が脆弱であり、即時の修復が必要であると判断した場合は、これらの CI に *Internet Facing* などの属性をアサインすることができます。この属性およびその他の属性は、Orlando ファミリーリリースの Common Service Data Model リリースノートに記載されています。CMDB に関する最新情報とガイダンスについては、以下のトピックを参照してください。

- Common Services Data Model 概念モデル
- CMDB スキーマモデル

必要なロール：sn_vul.manage_risk_score_configuration

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 脆弱性の算出.
2. [脆弱性算出] ページで、[デフォルトリスク算出 **(Default Risk Calculator)**] を選択します。
3. 次のように移動する。 [脆弱性算出] ページ > [脆弱性算出ルール] タブ > デフォルトのリスクルール.
4. オプション: [脆弱性リスクルール] ページの [リスク算出基準] セクションで、全体的なリスクスコアの計算における重要性に従って、各基準の重み付けを設定します。
5. ルールを非アクティブ化するには、[アクティブ] チェックボックスをオフにします。
6. リスク算出基準にリスクルールフィールドを追加するには、[基準を追加] を選択します。
7. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リスクルールのフィールドフォーム

フィールド	説明
参照テーブルを選択	リスクスコアの重み付けの定義に使用するテーブル。次のオプションのいずれかを選択できます。 ○ [脆弱性一致アイテム]：脆弱性一致アイテム (VI) から直接ドット連結可能なフィールドを追加します。☒ ○ [脆弱性一致アイテム] **-** [構成アイテム]：ハードウェアテーブルなど、ベーステーブルの拡張の一部であるドット連結可能なフィールドを追加します。これらのフィールドはベーステーブル (cmdb_ci) に含まれていません。 ○ [脆弱性一致アイテム] **-** [脆弱性]：サードパーティエントリーなど、ベーステーブルを拡張するテーブルに含まれるドット連結可能なフィールドを追加します。これらのフィールドは、脆弱性エントリーベーステーブルの一部ではありません。 ○ [脆弱性一致アイテム参照テーブル]：関連テーブル (m2m) に含まれるフィールド、または脆弱性一致アイテムへの参照を持つテーブルを追加します。これらのフィールドは、VI から直接ドット連結することはできません。 ○ [構成アイテム参照テーブル]：関連テーブル (m2m) に含まれるフィールド、または cmdb_ci への参照を持つテーブルを追加します。これらのフィールドは、VI から直接ドット連結することはできません。 ○ [脆弱性参照テーブル]：関連テーブル (m2m) に含まれるフィールド、または sn_vul_entry への参照を持つテーブルを追加します。これらのフィールドは、VI から直接ドット連結することはできません。 ○ [カスタム条件]：条件を評価することでルールに重み付けをアサインするには、このオプションを使用します。たとえば、インターネット向けフィルターは、構成アイテム (CI) が外部か内部かを判断します。
テーブル	[参照テーブルを選択] から次のいずれかのオプションが選択されている場合にのみ表示されるフィールド。 ○ [脆弱性一致アイテム] **->** [構成アイテム] ○ [脆弱性一致アイテム] **->** [脆弱性] ○ 脆弱性一致アイテム参照テーブル

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ 構成アイテム参照テーブル ○ 脆弱性参照テーブル
フィールド	このルールのリスクスコア算出に使用するフィールド。
集計	[参照テーブルを選択] から参照テーブルが選択されている場合にのみ表示されるフィールド。関連テーブル (m2m) から [フィールド] が選択されている場合に、算出で考慮する最小値または最大値を選択します。
重み付け	リスクルール内でのこのフィールドの重み付け。値は 0 ～ 100 の整数である必要があります。
値の重み付けを定義	各フィールド値に重み付けをアサインするコンポーネント。数値フィールドの場合、フィールド値は範囲 (1 ～ 5 など) として定義できます。重み付けは 0 ～ 100 の整数でなければなりません。 **注:** [カスタム条件] オプションが [参照テーブルを選択] で選択されている場合、このフィールドは表示されません。
条件テーブル	[参照テーブルを選択] からカスタム条件が選択されている場合にのみ表示されるフィールド。条件をリストから選択します。
フィールド名	[参照テーブルを選択] からカスタム条件が選択されている場合にのみ表示されるフィールド。リスク基準の名前を入力します。
条件	[参照テーブルを選択] からカスタム条件が選択されている場合にのみ表示されるフィールド。定義された条件に一致するこのテーブルのアイテムをプレビューします。

8. [送信] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

9. [ルール] ページで、ルールをアクティブ化して再適用し、アクティブな脆弱性一致アイテムのリスクスコアを再評価します。

   注:
   脆弱性対応 v23.0 以降の場合：

   - [デフォルトのリスク算出ツール] ルール：脆弱性一致アイテム (VIT) のリスクスコアが変更されると、VIT の [メモ] セクションに次の詳細が記録されます。
     - 算出グループ名
     - 算出名：
     - 1 より大きい重み付けを持つフィールド値とそのリスクスコアの寄与度。
     - 最終的なリスクスコア
   - [脆弱性重大度] リスクルール：VIT のリスクスコアが更新されると、次の詳細において [メモ] セクションが更新されます。
     - 算出グループ名
     - 算出名：算出ルールがテンプレートとスクリプトのどちらに基づいているかに応じて、名前に括弧で囲まれた詳細が追加されます。算出ルールの基準を変更または表示するには、任意のルールを選択し、[詳細表示] チェックボックスをオンにします。[値のタイプ **(Value type)]** ドロップダウンボックスから、必要なオプションを選択します。[テンプレート] を選択した場合、リスクスコアはルールで指定された条件に従って更新されます。[スクリプト] を選択した場合、既存のスクリプトを追加または更新できます。

Example:
例 1：ソース重大度をリスクルールの基準として追加する。

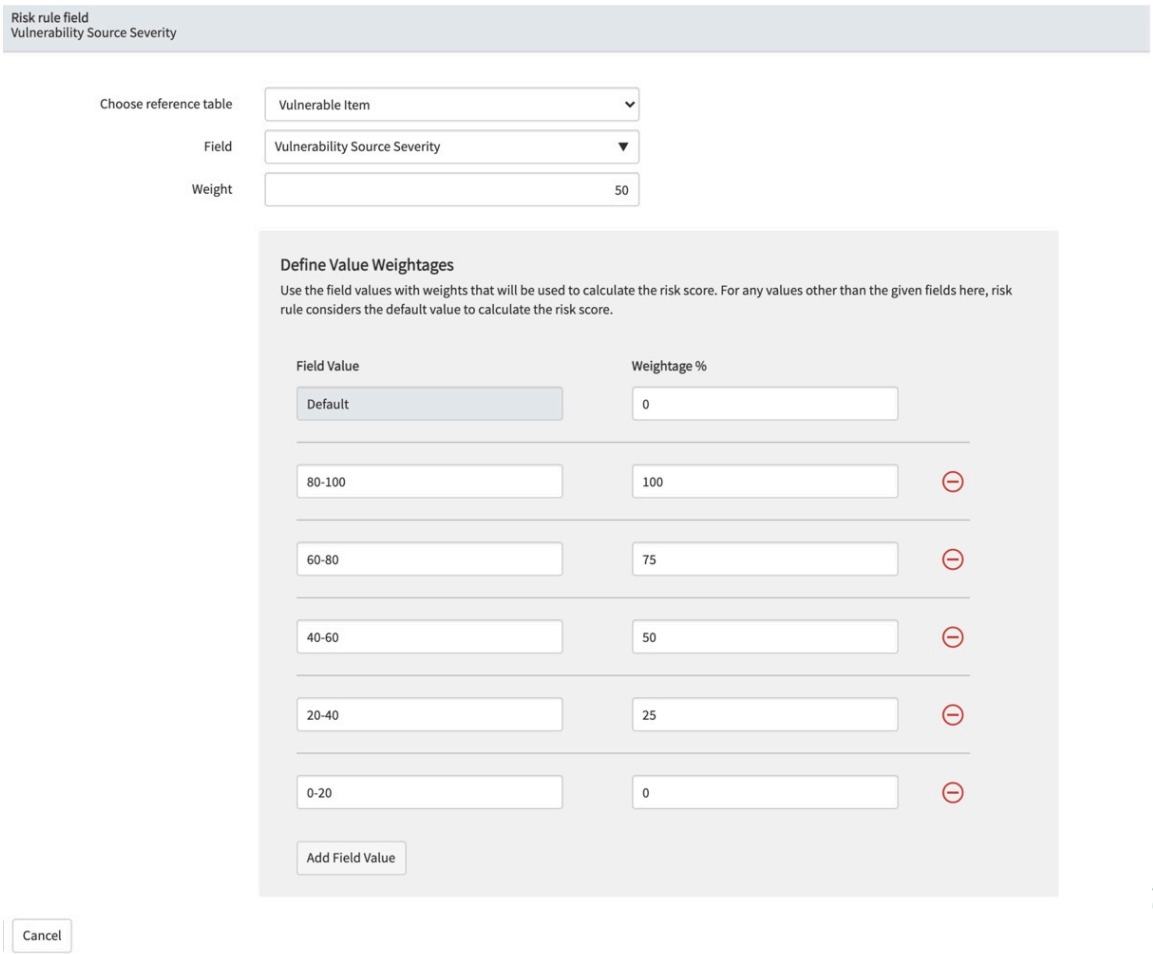
ユースケース：Qualys や Tenable などのサードパーティベンダーが独自のスコアを提供します。これらのスコアは、sn_vul_entry テーブルの [ソース重大度] フィールドに入力されます。このフィールドはリスクスコアの算出に使用します。このスコアを使用してリスクスコアを算出するには、次の操作を行います。

1. [リスクルール] ページに移動します。
2. ルールを非アクティブ化するには、[アクティブ] チェックボックスをオフにします。
3. リスク算出基準にリスクルールフィールドを追加するには、[基準を追加] を選択します。
4. [参照テーブルを選択] リストから、[脆弱性一致アイテム] を選択します。
5. [フィールド] リストから、[脆弱性ソースの重大度 **(Vulnerability.Source Severity)]** を選択します。
6. [重み付け] フィールドで、リスクルール内でのこのフィールドの相対的な重要度を入力します。値は 0 ～ 100 の整数である必要があります。
7. [値の重み付けを定義] セクションで、フィールド値を追加し、重み付けをアサインします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性一致アイテムテーブル



8. [送信] を選択します。

例 2：リスクルールの基準としてビジネス上の重要度を追加する。

ユースケース：組織に多くのビジネスサービスがあるとします。構成アイテム (CI) LINUX-SF-6381 が、以下のサービスで使用されています。

ビジネスサービスの重要度

ビジネスサービス	重要度
Cloud Management	1：最重要
e-コマース	2：ある程度重要
クライアントサービス	3：やや重要
出張費と経費	4：重要ではない

CI とサービス間のマッピングは、関連サービス [sn_vul_m2m_ci_services] テーブルに格納されます。資産 LINUX-SF-6381 で脆弱性が見つかると、脆弱性一致アイテム (VI) が作成されます。影響を受けるサービスのビジネス上の重要度の値を使用して、この VI のリスクスコアを計算できます。これらのサービスの重要度の値を使用してリスクスコアを計算するには、次の手順を実行します。

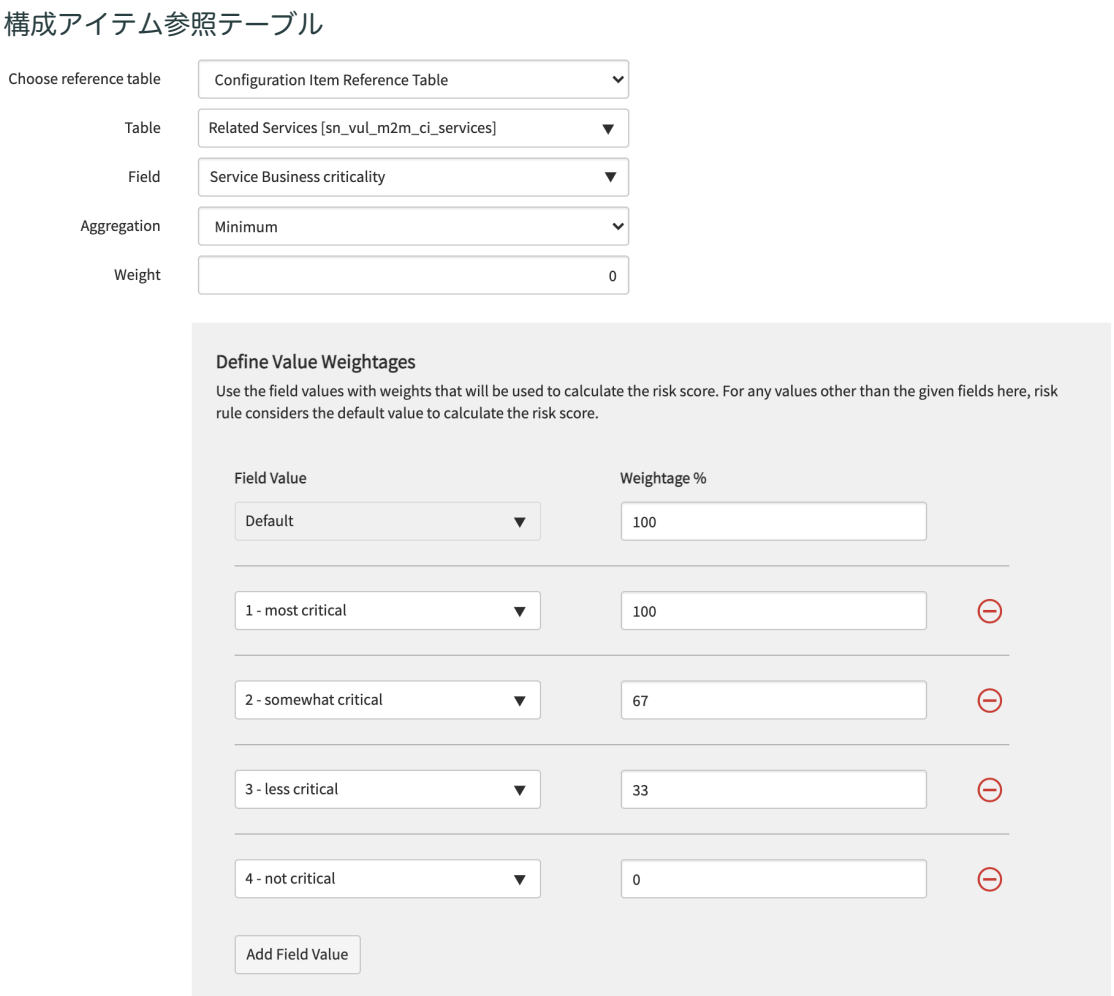
1. [リスクルール] ページに移動します。

2. ルールを非アクティブ化するには、[アクティブ] チェックボックスをオフにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. リスク算出基準にリスクルールフィールドを追加するには、[基準を追加] を選択します。
4. [参照テーブルを選択] リストから、[構成アイテム参照テーブル] を選択します。
5. [テーブル] リストから、[関連サービス **[sn_vul_m2m_ci_services]]** を選択します。
6. [フィールド] リストから、[サービスの業務上の重要度 **(Service Business criticality)]** を選択します。
7. [集計] フィールドで、[最小] を選択してこのユースケースの最も重要度の高いサービスを検索するか (**1 -** 最重要の値)、[最大] を選択してこのユースケースの最も重要度の低いサービスを検索します (**4 -** 重要ではない値)。
8. [重み付け] フィールドで、リスクルール内でのこのフィールドの相対的な重要度を入力します。値は 0 ～ 100 の整数である必要があります。
9. [値の重み付けを定義] セクションで、フィールド値を追加し、重み付けをアサインします。



10. [送信] を選択します。

例 3：リスク算出に条件付き基準を追加する。

組織に複数の構成アイテム (CI) があり、外部ユーザーはそのうちのいくつかにのみアクセスできると仮定します。ユーザーは、これらの外部向き CI に対してリスクスコアの重み付けを追加できます。

注:
これらの CI は名前で識別できます。名前は「外部 (external)」で始まります。

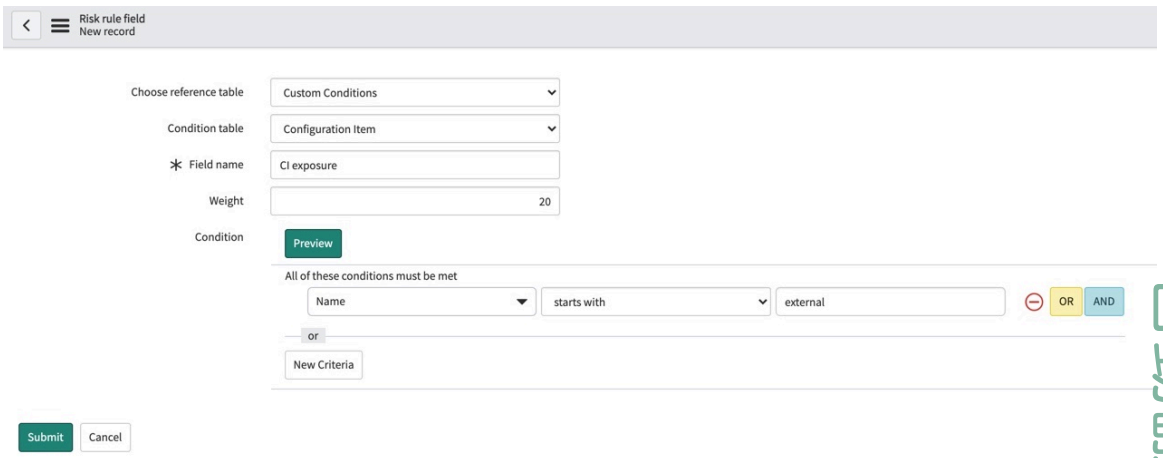
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

リスクルールに条件付き基準を追加するには、次の手順を実行します。

1. [リスクルール] ページに移動します。
2. ルールを非アクティブ化するには、[アクティブ] チェックボックスをオフにします。
3. リスク算出基準にリスクルールフィールドを追加するには、[基準を追加] を選択します。
4. [参照テーブルを選択] リストから、[カスタム条件] を選択します。
5. [条件テーブル] リストから、[構成アイテム] を選択します。
6. [フィールド名] フィールドに、「**CI** エクスポージャー」という名前を入力します。
7. [重み付け] フィールドで、リスクルール内でのこのフィールドの相対的な重要度を入力します。値は 0 ～ 100 の整数である必要があります。
8. [条件] フィールドで、 名前 > 次の値で始まる をクリックし、値 「外部」を入力します。

新しいリスクルールのカスタム条件



9. [送信] を選択します。

> **注:**
> リスクルールに条件付き基準を追加すると、パフォーマンスが低下する場合があります。

関連情報

Vulnerability Response 算出および脆弱性算出ルール

脆弱性対応算出の作成

Vulnerability Response 内でのフィルタリング

脆弱性対応 ロールアップ算出

セットアップアシスタントでリスク算出の初期アセスメントを行った後、脆弱性ロールアップ算出を使用して、修復タスクおよびインポートされた脆弱性の累積リスクスコアの計算方法を設定します。

脆弱性ロールアップ算出を使用して、修復タスクおよびインポートされた脆弱性の累積リスクスコアの計算方法を設定します。次のロールアップ算出がベースシステムに付属しています。

- *Remediation Task Rollup*：修復タスクのすべての脆弱性一致アイテムのリスクスコアをロールアップし、脆弱性一致アイテムのグループ全体の総リスクスコアを提供します。
- *Patch Update Rollup*：同じパッチ更新を含むすべての脆弱性なアイテムのリスクスコアをロールアップし、パッチ更新のリスクスコア全体を提供します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- *Organization Risk Score Rollup*：組織内のすべてのホスト脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテムと構成の問題でリスクスコアをロールアップし、統一ダッシュボードで組織の全体的なリスクスコアを提供します。

  注:
  脆弱性対応 v22.0 以降、組織スコアにおいてロールアップの重み付けを構成することができます。また、個々のロールアップ算出は削除されました。

- *Vulnerable Item Rollup*：組織内のすべてのホスト脆弱性一致アイテムでリスクスコアをロールアップし、統一ダッシュボードで組織の全体的なリスクスコアに貢献します。
- *Vulnerability Entry Rollup*：同じ脆弱性エントリーを含むすべての脆弱性一致アイテムのリスクスコアをロールアップし、脆弱性エントリーの総リスクスコアを提供します。
- *Rollup EPSS Scores from NVD to TPEs*：NVD テーブルにリストされているすべての脆弱性一致アイテム/CVE の EPSS スコアを既存の TPE にロールアップし、脆弱性が悪用される全体的な可能性を示します。
- *Remediation Effort Rollup*：修復作業のすべてのレコードのリスクスコアをロールアップし、修復作業の総リスクスコアを提供します。

次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 脆弱性ロールアップ算出.

累積リスクスコアを設定する際に、これらの計算値のそれぞれにどの程度の重み付けをするかを指定するように、ロールアップ算出を構成します。重み付けが大きいほど、ロールアップされたリスクスコアを決定するために脆弱性または修復タスクで使用される値が大きくなります。

注:
[保留を含める] を選択すると、保留されたすべての脆弱性一致アイテムが修復タスクのロールアップ計算に含まれます。必ず合計計算への影響を理解してから、このオプションを選択してください。

ロールアップ算出では、スケジュール済みジョブ *Rollup vulnerable item values to vulnerability and groups* を 15 分ごとに実行して変更を取得し、修復タスクと脆弱性の詳細とリスクスコアをロールアップします。このスケジュール済みジョブでは、VI の数、最大リスクスコア、修復ターゲット日、および修復タスクのステータスの累積値も計算されます。

注:
脆弱性エントリーの計算値には、修復ターゲットデータは含まれません。

リスクスコアは、以下の場合に計算されます。

- 脆弱性一致アイテムのリスクスコア、修復ターゲット、修復ステータス、または脆弱性が変更されたとき。
- 脆弱性一致アイテムのステータスが [オープン]、[保留]、[クローズ済み] に変わったか、[クローズ済み] または [保留] から変わったとき。
- 脆弱性一致アイテムが削除されたとき。
- 脆弱性一致アイテムが修復タスクに追加されたか、修復タスクから削除されたとき。

脆弱性ロールアップ算出の例：修復タスク VUL324567 に次の脆弱性一致アイテムがあるとします。

- リスクスコアが 30 の VIT1001
- リスクスコアが 40 の VIT1002
- リスクスコアが 50 の VIT1003

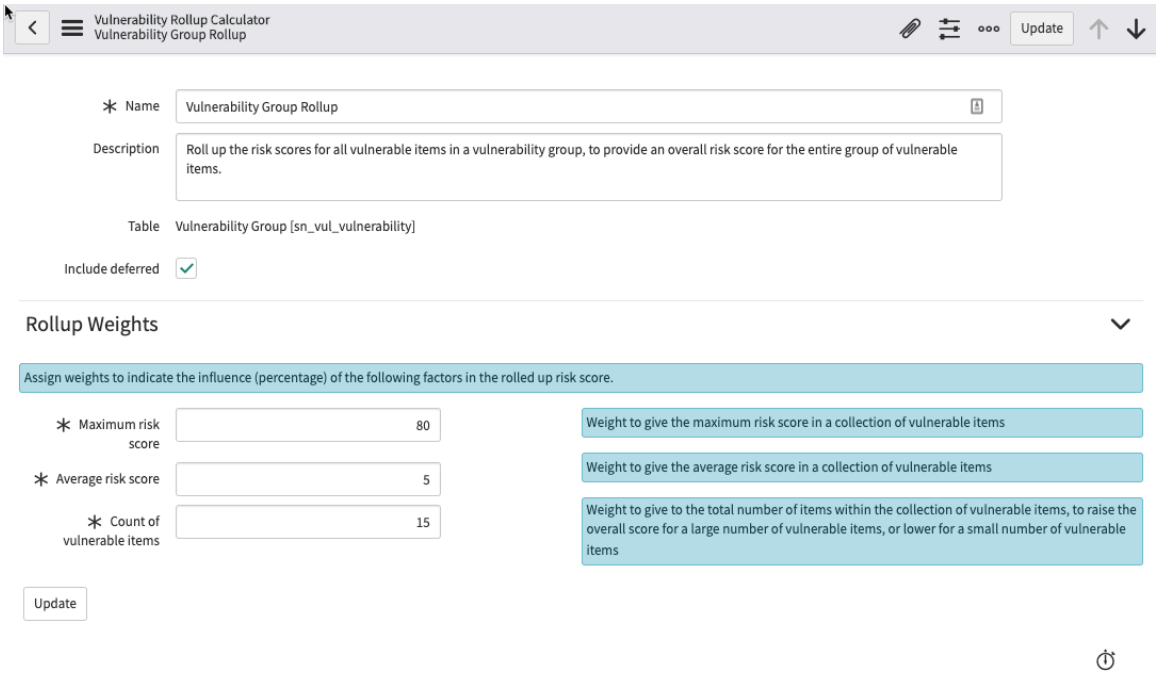
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

また、脆弱性ロールアップ算出の重み付けが次のとおりであるとします。

- 最大リスクスコア：80
- 平均リスクスコア：5
- 脆弱性一致アイテムの数：15

脆弱性ロールアップ算出の例



脆弱性ロールアップ算出の例では、修復タスクのリスクスコアを決定するための式は、次のとおりです。

(最大リスクスコア/100) * 80 + (平均リスクスコア/100) * 5 + (係数 * 15)

係数は次のように決定されます。

VI 数	係数
<10	0.2
10-100	0.4
101-1000	0.6
1001-10000	0.8
>10000	1

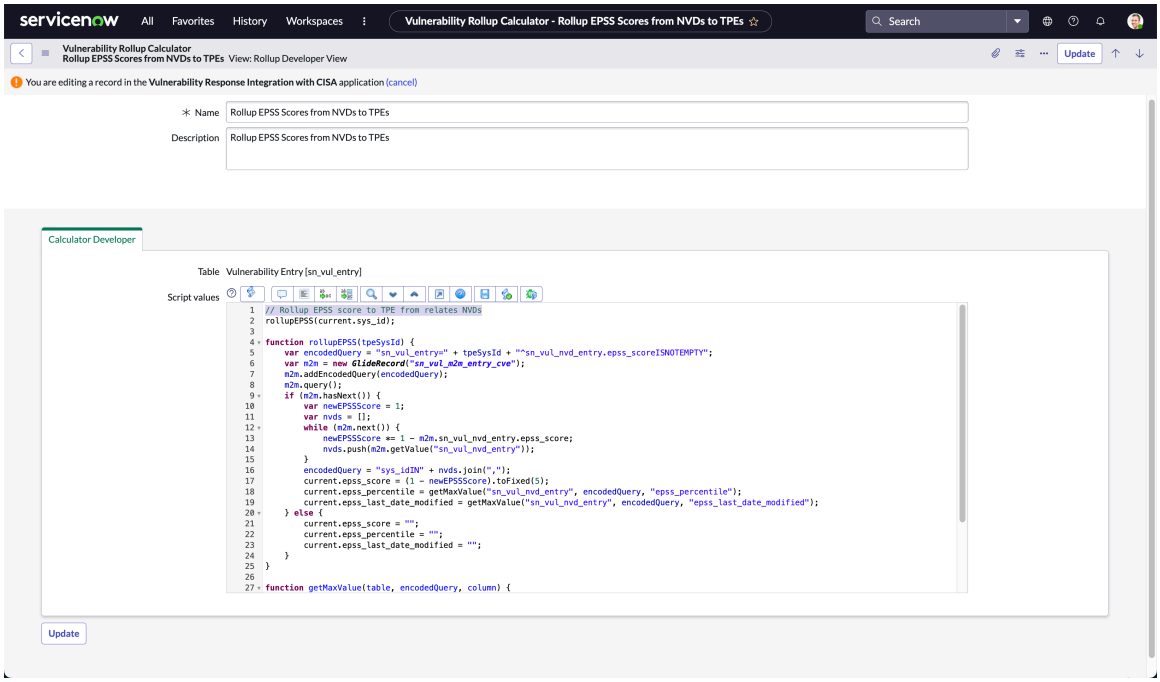
したがって、修復タスク VUL324567 の場合：

- 平均リスクスコアは 40
- 最大リスクスコアは 50
- 50 (最大リスクスコア)
- 係数は 0.2

リスクスコアは 45 [(50/100) * 80 + (40/100) * 5 + 0.2 * 15 = 40 + 2 + 3 = 45]

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

NVD から TPE に EPSS スコアをロールアップする



EPSS ロールアップ算出 - 例

たとえば、組織に 100 個の脆弱性があり、それぞれが悪用される可能性が 5% であるとします。ネットワーク防御者が強い関心を向ける質問は、これらの脆弱性の少なくとも 1 つが悪用される確率はどれくらいか、つまり全体的な脅威はどのようなものかということかもしれません。少なくとも 1 つのイベントが発生する確率は、単純に言えばイベントが発生しないことの補数 (反対) です。

```
P(at least one exploited vulnerability) = 1 - P(no vulnerabilities are exploited)
```

ここで、脆弱性がない確率というのは、悪用されていないそれぞれの脆弱性の総乗です。この例では、各脆弱性が悪用される可能性は 5% であるため、それぞれの脆弱性が悪用されない可能性は 95% です。そして、それらが 100 個あるので、これを次のように書き表すことができます。

```
P(at least one vuln exploited) = 1 - P(no vulns are exploited) = 1 - P(one vuln not
 exploited)^100 = 1 - 0.95^100 = 0.994
```

これは少なくとも 1 つの脆弱性が悪用される確率が 99.4% であることを示しています。

重要:
Rollup EPSS Scores from NVD to TPEs を変更するには、フォームのコンテキストメニューのビューを [デフォルトビュー] から [ロールアップ開発者ビュー] に切り替える必要があります。

[store-future: BEGIN review]

組織のリスクスコアにおけるロールアップ計算

組織のリスクスコアにおけるロールアップ機能では、統一ダッシュボードで組織の全体的なリスクスコアを計算します。ホスト脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、構成の問題におけるリスクスコアがロールアップされます。これまで最大リスクスコアは、VIT、AVIT、テスト結果、CVIT のスコアを平均して算出していました。しかし、脆弱性対応 v22 以降、4 つのスコアのうち最も高いスコアを最大リスクスコアとするようになりました。

最大リスクスコアを算出するには、VIT、AVIT、テスト結果、CVIT の中から最も高いスコアが選ばれることになります。たとえば、VIT のスコアが最も高い場合、そのスコアが最大リスクスコアとなります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

VIT、AVIT、CVIT、テスト結果の計数が得られたら、これらを合算してカウントメソッドで正規化します。結果のリスクスコアが、構成で指定された計数の重み付けで乗算されます。

平均リスクスコアの計算においてもプロセスは同じです。AVIT、構成の問題、テスト結果、他のスコアのリスクスコアを合算し、合計数で除算してて平均リスクスコアを算出します。最後に、すべてのリスクスコアを合算して、組織のリスクスコアを算出します。

[End]

脆弱性対応 修復ターゲットルールの作成または編集

セットアップアシスタントで修復ターゲットルールの初期アセスメントを行った後、脆弱性マネージャーは、リスクの高い脆弱性の修正を適宜行えるように、脆弱性一致アイテムレベルで修復ターゲットルールを設定できます。脆弱性一致アイテムの修正日が近づくと、ルールで指定されたユーザーまたはグループに通知が送信されます。

始める前に

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 修復ターゲットルール.
2. **[New]** をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
名前	ルールの名前。
ターゲット (日数)	脆弱性一致アイテムを最後に開いてから修正するまでの期限日数を指定します。
V17.1：ターゲット開始日 (日付)	ターゲット SLA が算出される日付。日付タイプまたは日付と時刻タイプのフィールドのみを指定できます。デフォルト値は [最終オープン日] です。このフィールドの値をカスタマイズするには、「KB1642413」を参照してください。
アクティブ	デフォルトでは、[アクティブ] チェックボックスがオンになっています。これは、修復ターゲットルールがアクティブであることを意味します。このチェックボックスをクリアすると、システムに作成された新しい脆弱性一致アイテムにこのルールは適用されません。
通知 (期限前の日数)	送信する通知のターゲット修正時間までの日数。この値を使用して計算された通知日は、修復ステータスを表示するために使用され、色分けされています。日付が通知日より前の場合、修復ステータスは「実行中」になります。通知日を過ぎており、修復ターゲット日より前の場合、ステータスはターゲット間近として表示されます。 **注:** このフィールドが 0 に設定されている場合、[ターゲット経過] 通知のみが送信されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
説明	修復ターゲットルールを説明するテキスト。
条件	条件フィルターを使用して、ルールを脆弱性一致アイテムに適用するための基準を選択します。パフォーマンスへの影響を防ぐには、完全な本番環境で条件をテストしてください。テストにより、構成管理データベース (CMDB) の条件とサイズを指定して、[修復ターゲットの評価]ジョブの実行にかかる時間を判断できます。 条件ビルダーに入力した検索テキストの大文字と小文字の区別は、このレコードまたはフォームではサポートされていません。
通知 **注:** 通知メールに表示される数には、[保留]、 [解決済み]、または [クローズ済み] ステータスの脆弱性一致アイテムは含まれません。	
ユーザー	選択した脆弱性一致アイテムがターゲットの修復ターゲット時間に近づいた、または過ぎたときに通知するユーザー。
グループ	選択した脆弱性一致アイテムがターゲットの修復ターゲット時間に近づいた、または過ぎたときに通知するグループ。
更新履歴	
	ルールの初期作成には使用されません。その後、システム作業メモがここに記録されます。

4. **[Submit]** をクリックします。
   このルールは、スケジュール済みジョブ *Evaluate remediation targets* の次回実行時、または [修復ターゲットルール] リストビューの [変更を適用] ボタンの使用時に有効になります。既存のルールが更新された場合も同様です。スケジュール済みジョブと [変更を適用 **(Apply Changes)]** の詳細については、「脆弱性対応 の修復ターゲットルール」を参照してください。

セットアップアシスタントを使用したインストール済みサードパーティ統合の構成

それぞれのインストール済みサードパーティアプリケーション展開と連動するように脆弱性対応を構成します。

始める前に

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > セットアップアシスタント > 統合設定.
2. [スキャナー統合] を選択して、インストール済みサードパーティアプリケーションの展開を構成します。
3. 脆弱性対応のソリューション管理 がインストールされている場合は、[ソリューション統合] を選択して脆弱性ソリューションプロバイダーを構成できます。

セットアップアシスタントを使用した 脆弱性ソリューション管理 のインストール済みソリューション統合の構成

Vulnerability Solution Management アプリケーションをインストールした後、セットアップアシスタントを使用して脆弱性ソリューションプロバイダーを構成できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_vul.vulnerability_admin、sn_vul.admin (非推奨)、または admin
脆弱性対応のソリューション管理 のインストール済みソリューション統合について、セットアップアシスタントで提供される指示とプロンプトを補足するには、以下のセクションを参照してください。

- 開始する前に、必要な 脆弱性ソリューション管理 とソリューション統合が既にインストールされていることを確認します。詳細については、「セットアップアシスタントを使用した 脆弱性対応サードパーティアプリケーションのインストール」を参照してください。
- サードパーティアカウントの認証情報を使用できることを確認します。一部のソリューション統合では、認証情報を編集する必要があります。
- 詳細については、インストール済みのソリューションを構成する前に「脆弱性対応のソリューション管理アプリケーションのインストール」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合設定 > ソリューション統合.

   Microsoft セキュリティレスポンスセンターソリューション統合を構成するには、Microsoft セキュリティレスポンスセンター からの API キーと URL が必要です。

   > **注:**
   > MSRC の API キーの入力はオプションです。MSRC キーを取得するには、live.com、outlook.com、または Microsoft.com のメールアカウントからの Microsoft ID、Microsoft に登録されている電話番号、または Skype ログインが必要です。

2. URL を入力します。
   MSRC 用のセットアップアシスタントの URL は、`https://api.msrc.microsoft.com` です。
3. [完了] をクリックします。
4. オプション: 認証情報の入力後に構成ページで [今すぐ実行] をクリックすると、インポートをオンデマンドで実行できます。
5. Red Hat Solution Integrationも使用できます。
   API キーは必要ありません。
6. セットアップアシスタントで、Red Hat Solution Integration の右側にある [編集] をクリックします。
7. RHSI 用のセットアップアシスタントの URL が `https://access.redhat.com/hydra/rest` であることを確認します。
8. オプション: 構成ページで [今すぐ実行] をクリックすると、インポートをオンデマンドで実行できます。
9. [完了] をクリックし、次に [完了としてマーク] をクリックして構成を完了します。
   構成が完了すると、ソリューション統合のセットアップアシスタントにチェックマークが表示されます。

セットアップアシスタントを使用した **MS TVM** 脆弱性統合の構成

セットアップアシスタントを使用してインストールした後、脆弱性対応 Integration with Microsoft Threat and Vulnerability Management (MS TVM) アプリケーションを設定します。

始める前に
脆弱性対応 Integration with Microsoft Threat and Vulnerability Management 統合のためにセットアップアシスタントで提供される指示とプロンプトに加えて、次のアクションを実行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 開始する前に、アプリケーションが既にインストールされていることを確認します。詳細については、「セットアップアシスタントを使用した 脆弱性対応 サードパーティアプリケーションのインストール」を参照してください。
- Microsoft Threat and Vulnerability Management integration for 脆弱性対応 を設定する前に、詳細について「Microsoft Threat and Vulnerability Management 脆弱性統合の準備」を参照してください。
- MS TVM アカウントの認証情報があることを確認します。これらの認証情報を取得するには、「MS TVM 統合用の Microsoft Azure の設定」を参照してください。

必要なロール：システムアドミニストレーター (admin) (インストール用)、脆弱性アドミン (sn_vul.vulnerability_admin) または sn_vul.admin (使用廃止)、統合の構成 (sn_vul_msft_tvm.configure_integration) (構成用)

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合設定 > スキャナー統合.

   [Microsoft Threat & Vulnerability Management] タイルが表示されます。

   MS TVM はマルチソース統合です。つまり、同じサードパーティ統合を複数展開できます。元のサードパーティ統合の設定は、新しい各統合の設定のテンプレートとして使用されます。

   > **注:**
   > 元の脆弱性統合を削除する場合、テンプレートとして使用する別の統合を選択する必要があります。統合を削除する代わりに無効にすることを検討してください。無効になったテンプレートから作成された統合は、デフォルトで無効になっています。

   各サードパーティ統合からのデータは一意に識別され、脆弱性対応 の単一のインスタンスで使用できます。

2. Microsoft Threat and Vulnerability Management 統合を設定するには、[編集] をクリックします。
3. フォームのフィールドに入力します。

アカウント認証情報フォーム

フィールド	説明
名前	インスタンスの名前。
TVM 地域	サーバーの場所に近い地域。API の最適なパフォーマンスを得るには、自分の場所に最も近いサーバーを使用します。
認証タイプ	ID を確認する方法。ユーザー認証は、特定のユーザーに対して、特定の資産の可視化を制御します。MS TVM は、このユーザーにエンタイトルメントされたデバイスグループをエクスポートします。デフォルト値は [アプリケーション] です。
テナント ID	組織のテナント ID。
クライアント ID	Microsoft Azure で MS TVM を登録した後に生成されるクライアント ID。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ユーザー名	完全なデバイスグループにアクセスできるユーザー。このフィールドは、[ユーザー] が [認証] タイプから選択されている場合にのみ表示されます。
パスワード	完全なデバイスグループにアクセスできるユーザー名のパスワード。このフィールドは、[ユーザー] が [認証] タイプから選択されている場合にのみ表示されます。
クライアントシークレット	MS TVM アプリケーションの登録後に生成されるクライアントシークレット。このフィールドは、[アプリケーション] が [認証] タイプから選択されている場合にのみ表示されます。

4. 変更を保存して最初の統合フォームに進むには、[次へ] をクリックします。
[脆弱性インポート構成] フォームが表示されます。
5. 脆弱性インポートを有効または無効にし、インポートする脆弱性の最初の開始日を決定し、MS TVM 脆弱性インポートを実行するタイミングをスケジュールします。
すべての脆弱性をインポートする場合は、最初の開始日を空白のままにします。
   a. オンデマンドでデータをインポートするには、[今すぐ脆弱性をインポート] をクリックします。
   b. 統合レコードを表示するには、[詳細設定] をクリックします。
6. 変更を保存して最初の統合フォームに進むには、[次へ] をクリックします。
[推奨事項インポート構成] フォームが表示されます。
7. 推奨事項のインポートを有効または無効にし、MS TVM 脆弱性インポートを実行するスケジュールを決定します。
   a. オンデマンドでデータをインポートするには、[今すぐ推奨事項をインポート] をクリックします。
   b. 統合レコードを表示するには、[詳細設定] をクリックします。
8. 変更を保存して最初の統合フォームに進むには、[次へ] をクリックします。
[マシンインポート構成] フォームが表示されます。
9. マシンインポートを有効または無効にし、インポートするマシンの最初の開始日を決定し、MS TVM マシンインポートを実行するタイミングをスケジュールします。
すべてのマシンをインポートする場合は、最初の開始日を空白のままにします。

   注:
   マシンタグはデフォルトでインポートされ、MS TVM 環境にリストされているマシンを整理および追跡するために使用されます。

   a. デフォルトの構成アイテム (CI) ルックアップルールを表示するには、**[CI** ルックアップルール] をクリックします。CI ルックアップルールでは、Now Platform CMDB の構成アイテム (CI) を特定するためにサードパーティソースのマシンデータを使用する方法を定義します。このページには、ルックアップルールを追加するか、デフォルトの CI ルックアップルールを変更するオプションがあります。詳細については、「脆弱性対応 サードパーティ脆弱性統合の構成アイテムを識別するための CI ルックアップルール」を参照してください。
   b. オンデマンドでデータをインポートするには、[今すぐマシンをインポート] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> MS TVM でステータスが「オンボーディング済み」になっているマシンは、ServiceNow アプリケーションで取得されます。

c. 統合レコードを表示するには、[詳細設定] をクリックします。

10. 変更を保存して最初の統合フォームに進むには、[次へ] をクリックします。
[マシン脆弱性インポート構成] フォームが表示されます。
11. 次の統合を有効にし、インポートする脆弱性の最初の開始日を決定します。

マシン脆弱性インポート構成フォーム

統合	説明
Microsoft TVM マシンの脆弱性デルタインポート	新規、修正済み、および更新済み脆弱性を含む、完全な脆弱性インポート中に更新された脆弱性を取得します。過去 14 日間のデルタデータのみをインポートできます。
Microsoft TVM マシンの脆弱性フルインポート	すべてのオープンな脆弱性を取得します。大量のデータがインポートされるため、毎週実行するようにスケジュールできます。

> **注:**
> マシン脆弱性統合の前にマシンのインポートを実行します。それ以外の場合、見つからないマシンの VI は作成されません。

12. セットアップアシスタントで変更を保存して設定を完了するには、[完了] をクリックします。

次のタスク

クラシック環境で脆弱性一致アイテムのグループ化をアクティブ化する場合は、次に移動します: > 脆弱性対応 > アドミニストレーション > 修復タスクルール > **Microsoft TVM** の推奨事項.

表示されるフォームで、[アクティブ] オプションを選択してアクティブ化します。または、[新規] を選択して新しいルールを作成することもできます。

詳細については、「脆弱性対応修復タスクとタスクルールの概要」を参照してください。

セットアップアシスタントを使用した **Qualys** 脆弱性統合の構成

Qualys アプリケーションをインストールした後、セットアップアシスタントを使用して構成します。

始める前に

Qualys 脆弱性統合の構成について、セットアップアシスタントで提供される指示とプロンプトを補足するには、次のセクションを使用します。

- 開始する前に、アプリケーションが既にインストールされていることを確認します。詳細については、「セットアップアシスタントを使用した 脆弱性対応 サードパーティアプリケーションのインストール」を参照してください。
- Qualys 脆弱性統合を構成する前に、「Qualys 脆弱性統合 の準備」で詳細を参照してください。
- サードパーティアカウントの認証情報を使用できることを確認します。一部のサードパーティアプリケーションを編集する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

必要なロール：システムアドミニストレーター (admin) (インストール用)、脆弱性アドミン (sn_vul.vulnerability_admin) または sn_vul.admin (非推奨) (構成用)

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合設定 > スキャナー統合.
   インストールされた統合が表示されます。
2. 構成する Qualys 脆弱性統合の右側にある [編集] をクリックします。
3. [アカウント認証情報] フォームで、Qualys クラウドプラットフォーム 認証情報を入力します。構成するには認証情報が必要です。
4. 構成を続行するときは、次のメモを参考にしてください。
   - [詳細設定] リンクで Qualys 統合レコードを指定します。スケジュール設定済みクエリに Qualys 製品でサポートされているパラメーターを追加して、インポートする脆弱性データをフィルタリングできます。詳細については、「Qualys インポートの追加のフィルターパラメーターの設定」を参照してください。
   - 以前のバージョンの 脆弱性対応 から既に構成した Qualys 脆弱性統合のバージョンにアップグレードした場合、そのバージョンは構成設定を保持して引き続き使用できます。

     Qualys 脆弱性統合のホスト検出構成のインポート設定には、修正された Qualys 脆弱性検出レコードを表示するオプションがあります。有効にすると、修正済みステータス (状態 = [修正済み]) の検出レコードから脆弱性一致アイテムを作成できます。脆弱性一致アイテム検出の詳細については、「サードパーティ統合からの 脆弱性対応 脆弱性一致アイテム検出」を参照してください。

     [ホスト検出設定] ページの [ネットワークパーティションによるルックアップ] チェックボックスをアクティブ化して、IP アドレスルックアップにネットワークパーティション識別子を含めることができます。詳細については、「Qualys 脆弱性統合 のネットワークパーティション識別子で構成アイテムを更新する」を参照してください。

     すべてのホストタグは Qualys ホストリスト統合の一部としてインポートされます。ホストタグは、主に 脆弱性対応 アサインおよび修復タスクルールでのフィルタリングに使用されます。これらは [検出されたアイテム] フォームに表示されます。

     > **注:**
     > Qualys ホストリスト統合は、脆弱性一致アイテムがインポートされてグループ化される前にすべてのタグがルール内に存在できるように、脆弱性対応 でのアサインルールまたは修復タスクルールを作成する前に実行する必要があります。

     Qualys [資産タグ] は、Qualys 脆弱性統合の下のホストタグモジュールに格納されます。
   - Qualys 脆弱性統合はマルチソースをサポートしています。同じサードパーティ統合に複数の展開を含めることができます。別の統合を追加するには、[スキャナー統合] ページで [統合を追加] をクリックします。

     元のサードパーティ統合の設定は、新しい各統合の設定のテンプレートとして使用されます。

     > **注:**
     > 元の脆弱性統合を削除する場合、テンプレートとして使用する別の統合を選択する必要があります。統合を削除する代わりに無効にすることを検討してください。無効になったテンプレートから作成された統合は、デフォルトで無効になっています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

各サードパーティ統合からのデータは一意に識別され、脆弱性対応 の単一のインスタンスで使用できます。

- 構成ページで [今すぐ実行] をクリックすると、インポートをオンデマンドで実行できます。

5. [完了] をクリックして、セットアップアシスタントでの構成を完了します。

セットアップアシスタントを使用した **Tenable** 脆弱性統合の構成

Vulnerability Response Integration with Tenable アプリケーションをインストールした後、セットアップアシスタントを使用して構成します。

始める前に

Vulnerability Response Integration with Tenable 統合について、セットアップアシスタントで提供される指示とプロンプトを補足するには、次のセクションを使用します。

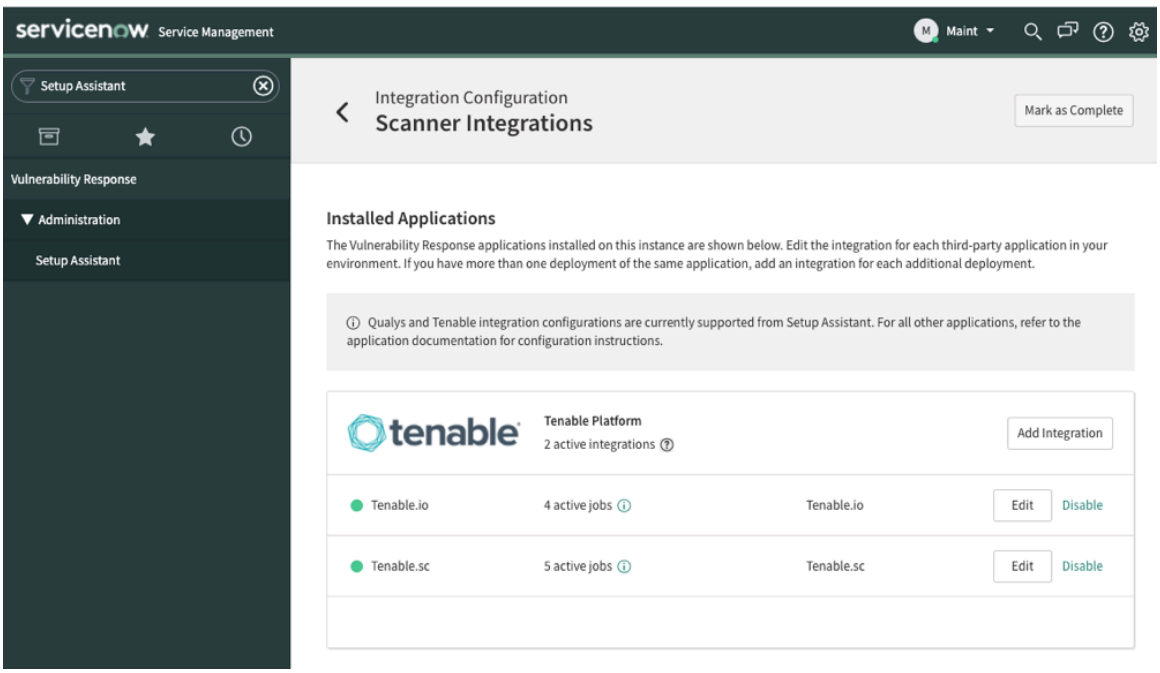
- 開始する前に、アプリケーションが既にインストールされていることを確認します。詳細については、「セットアップアシスタントを使用した 脆弱性対応 サードパーティアプリケーションのインストール」を参照してください。
- 脆弱性対応の Tenableを構成する前に、「Tenable 脆弱性統合の準備」で詳細を参照してください。
- サードパーティアカウントの認証情報を使用できることを確認します。一部のサードパーティアプリケーションを編集する必要があります。

必要なロール：システムアドミニストレーター (admin) (インストール用)、脆弱性アドミン (sn_vul.vulnerability_admin) または sn_vul.admin (非推奨)、統合の構成 (sn_vul_tenable.configure_integrations) (構成用)

手順

1. 表示されていない場合は、次に移動します: **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合設定 > スキャナー統合.

   Tenable.io および Tenable.sc 統合が表示されます。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable はマルチソース統合であり、同じサードパーティ統合に複数の展開を含めることができます。元のサードパーティ統合の設定は、新しい各統合の設定のテンプレートとして使用されます。

> **注:**
> 元の脆弱性統合を削除する場合、テンプレートとして使用する別の統合を選択する必要があります。統合を削除する代わりに無効にすることを検討してください。無効になったテンプレートから作成された統合は、デフォルトで無効になっています。

各サードパーティ統合からのデータは一意に識別され、脆弱性対応 の単一のインスタンスで使用できます。

2. 構成する Tenable 統合の右側にある [編集] をクリックします。
3. [アカウント認証情報] フォームで、フィールドに入力します。

   - Tenable.io には 64 以上の権限属性を持つアドミンアクセスが必要です。

     > **注:**
     > Tenable と脆弱性対応の統合の v3.8 以降、Tenable.io へのアクセスにアドミニストレーター権限は必要なくなりました。権限属性が 16 に等しい基本ユーザーも製品にアクセスできます。

   - Tenable.sc にはセキュリティアナリストまたはマネージャーアクセスが必要です。

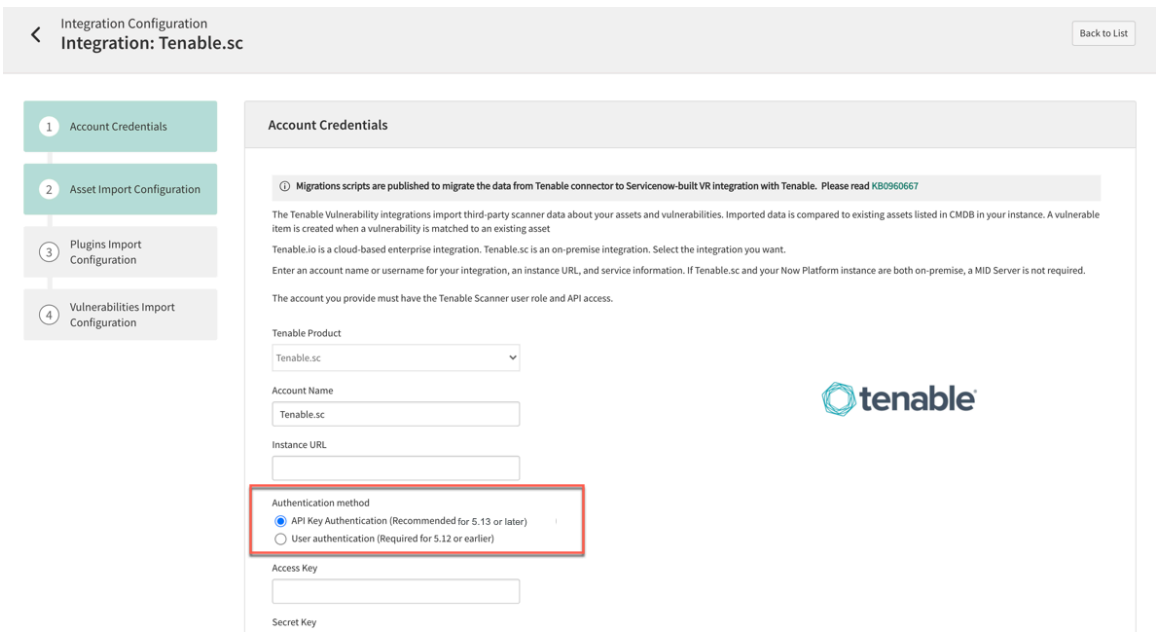
   a. Tenable 製品を選択します。

   b. Tenable アカウント名を入力します。

   c. [インスタンス URL] フィールドに、Tenable プラットフォームの URL を入力します。

   d. 認証方法を選択します。

      Tenable.sc のバージョンに基づいて、次の 2 つの認証オプションがあります。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

i. Tenable.sc の v5.13 以降では、**[API** キー認証] を選択します。Tenable アクセスキーと秘密キーを入力します。

ii. v5.13 より前では、ユーザー認証は Now Platform® インスタンスでサポートされており、必須です。Now Platform のユーザー名とパスワードを入力します。

Tenable.sc では API キー認証のみがサポートされています。Tenable アクセスキーと秘密キーを入力します。

e. オプション: MID サーバーを選択します。

(Optional) Now Platform インスタンスと Tenable.sc アプリケーションが同じ場所にない場合は、構成済みの MID サーバーを選択リストから選択します。詳細については「MID サーバー」を参照してください。

- v15.0 の 脆弱性対応 および v3.0 の Tenable 脆弱性統合 以降、「Tenable 脆弱性統合のデータ検索設定」で説明されている *Async_request* パラメーターを有効にするオプションがあります。同期呼び出しを実行する場合は、Tenable での構成が必要です。Tenable 製品のヘルプを参照してください。このパラメーターをアクティブにすると、Tenable.sc のすべての統合に適用され、タイムアウトが 30 秒になります。修正スクリプトを表示するには、次に移動します: システム定義 > 修正スクリプト.

- (Optional) 既存の顧客の場合、非同期呼び出しを使用している場合は修正スクリプトを使用できます。

Now Platform インスタンスと Tenable.sc アプリケーションの両方がオンプレミスである場合、必須ではありませんが、構成された MID サーバーを選択リストから選択することもできます。

> **注:**
> MID サーバーを使用するかどうかにかかわらず、統合は 5 分後にタイムアウトし、サーバーからの応答がない場合はメッセージが表示されます。
>
> (Optional) タイムアウトエラーが発生した場合は、セットアップアシスタントで正しい認証情報と URL を入力していることを確認してください。

4. [次へ] をクリックして、変更内容を保存し、最初の統合フォームに進みます。
[資産インポート構成] フォームが表示されます。

5. このフォームで、資産インポート統合をアクティブまたは非アクティブ化して、インポートする資産の最初の開始日を決定し、Tenable 資産インポートを実行するタイミングをスケジュールします。

Tenable.io の場合

- 資産統合を Tenable.io コンプライアンス結果およびコンプライアンス結果バックフィル統合とともに使用して、資産に関する安全な構成アセスメントデータを コンフィグレーションコンプライアンス アプリケーションにインポートできます。
- この安全な構成アセスメントデータをインポートして表示するには、バージョン 12.2 の コンフィグレーションコンプライアンス アプリケーションがインスタンスに必要です。

これらの統合でインポートされるデータとその投稿先の詳細については、「コンフィグレーションコンプライアンス インポートデータ」を参照してください。

- Tenable.io コンプライアンス結果統合およびコンプライアンス結果バックフィル統合は、デフォルトではアクティブになっていません。それらをアクティブにする場合は、提供されるデ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フォルトのスケジュール設定を使用することをお勧めします。Tenable 脆弱性統合の統合を見つけてアクティブにする方法については、以下の手順を参照してください。

- インスタンスから Tenable.io 製品の脆弱性一致アイテムの再スキャンをオンデマンドで開始できます。再スキャンを開始する前に、Tenable.io テンプレート統合と Tenable.io スキャン認証情報統合をアクティブにする必要があります。

これらの統合はデフォルトで非アクティブになっています。Tenable.io の認証情報を入力すると、すべての Tenable.io 統合が自動的にアクティブになります。これらの統合を手動でアクティブまたは非アクティブにするには、次の手順を実行します。

a. 次のように移動する。 **Tenable** 脆弱性統合 > アドミニストレーション > 統合.

b. 表示されるリストで、必要な Tenable.io 統合レコードを見つけます。

c. 各レコードを開き、[アクティブ] チェックボックスをオンにして統合をアクティブ化します。

d. [更新] をクリックして変更を保存します。

e. セットアップアシスタントに戻り、脆弱性対応 で Tenable 脆弱性統合の構成を続行します。

- Tenable.io 統合の場合、資産タグのインポートをアクティブまたは非アクティブにするオプションもあります。資産タグはデフォルトでインポートされ、Tenable.io 環境の CMDB にリストされている資産の整理と追跡に使用されます。
- Tenable.io と Tenable.sc の両方の製品について、[ネットワークパーティションによるルックアップ] の [ネットワークパーティションによるルックアップを有効化] を選択すると、同じ IP アドレスを持つ資産に識別および調整エンジン (IRE) を使用して個々の CI を作成できます。詳細については、「Tenable 脆弱性統合 のネットワークパーティション識別子で構成アイテムを更新する」と「識別および調整エンジンを使用して 脆弱性対応 の CI を作成する」を参照してください。
- 画面上部の [資産インポート] リンクの横にある **[CI** ルックアップルール] リンクをクリックして、デフォルトの構成アイテム (CI) ルックアップルールを表示します。CI ルックアップルールでは、Now Platform CMDB の構成アイテム (CI) を特定するためにサードパーティソースの資産データを使用する方法を定義します。このページには、ルックアップルールを追加するか、デフォルトの CI ルックアップルールを変更するオプションがあります。詳細については、「脆弱性対応 サードパーティ脆弱性統合の構成アイテムを識別するための CI ルックアップルール」を参照してください。
- [今すぐ資産をインポート] をクリックして、データをオンデマンドでインポートします。
- [詳細設定] リンクで資産統合レコードを指定します。v3.3 以降、スケジュール設定済みクエリに Tenable.io 製品でサポートされているパラメーターを追加して、Tenable.io の資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合でインポートする脆弱性データをフィルタリングできます。詳細については、「Tenable.io インポートの追加のフィルターパラメーターの設定」を参照してください。

6. [次へ] をクリックして、変更内容を保存し、次のフォームに進みます。
[プラグインインポート構成] フォームが表示されます。

7. このフォームで、プラグイン (サードパーティ脆弱性エントリー) インポートを有効または無効にします。インポートするプラグインの最初の開始日を決定し、Tenable プラグインのインポートを実行するタイミングをスケジュールします。

すべてのプラグイン、脆弱性および資産をインポートする場合は、最初の開始日を空白のままにします。

- [今すぐプラグインをインポート] をクリックして、データをオンデマンドでインポートします。
- [詳細設定] リンクでプラグイン統合レコードを指定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 脆弱性インポートでは、取り込む脆弱性の Tenable.io の重大度レベルをスケジュールして設定できます。特定の日付以降に作成または更新された脆弱性のみがインポートされるように日付を決定します。
- Tenable.sc 統合では、特定の日付以降に作成または更新された脆弱性のみがインポートされるように、クエリフィルターと日付を決定できます。

8. [次へ] をクリックして、変更内容を保存し、次のフォームに進みます。
[脆弱性インポート構成] フォームが表示されます。統合を有効または無効にし、インポートする脆弱性の最初の開始日を決定します。

   Tenable.io 製品の場合：

   - 重大度フィルターで選択した条件に一致する脆弱性と関連 VI のみをインポートします。
   - Tenable.io 資産統合では、脆弱性がある資産に対してのみ *Last Scan Time* がインポートされて更新されます。
   - [修正された脆弱性] オプションを有効にして、修正済みの検出レコードの VI を表示します。セットアップアシスタントでこのフラグを有効にすると、インスタンスにまだ存在しない [修正済み] ステータスの検出に対して新しい VI が作成されます。この機能を有効にすると、取り込みパフォーマンスに悪影響を与える可能性があります。
   - [フィルターのインポート] の横にある [詳細設定] リンクで脆弱性統合レコードを指定します。
   - 上部の [スケジュールをインポート] リンクをクリックして、脆弱性を取り込む間隔を構成して、統合を有効にします。

   Tenable.sc 製品の場合：

   - Tenable プラットフォームの Tenable クエリによって設定された条件フィルターに一致する脆弱性と関連 VI のみをインポートします。Tenable クエリの詳細については、Tenable のドキュメントを参照してください。

     セットアップアシスタントで選択した Tenable クエリフィルターは、Tenable.sc 資産統合にも適用されます。クエリフィルターの条件に一致する脆弱性がある資産のみがインポートされます。

   - [修正された脆弱性] オプションを有効にして、修正済みの検出レコードの VI を表示します。セットアップアシスタントでこのフラグをアクティブにすると、インスタンスにまだ存在しない [修正済み] ステータスの検出に対して新しい VI が作成されます。この機能をアクティブにすると、取り込みパフォーマンスに悪影響を与える可能性があります。
   - IP アドレスルックアップにネットワークパーティション識別子を含めるには、 ネットワークパーティションによるルックアップを有効化 のチェックボックス ネットワークパーティションによるルックアップ 節。詳細については、「Tenable 脆弱性統合 のネットワークパーティション識別子で構成アイテムを更新する」を参照してください。
   - 上部の [スケジュールをインポート] をクリックして、脆弱性を取り込む間隔を構成して、統合を有効にします。
   - [フィルターのインポート] の横にある [詳細設定] リンクで脆弱性統合レコードを指定します。
   - Tenable.sc 脆弱性統合 (Tenable.sc のオープンな脆弱性統合および修正された脆弱性統合) を構成すると、インスタンスのセットアップアシスタント内から ServiceNow Tenable.sc スキャン認証情報統合が自動的に有効 ([アクティブ]) になります。

     この統合により、インスタンスの Tenable.sc 製品からスキャナー認証情報がインポートされて更新されます。この統合は毎週実行され、Tenable 認証情報データをインポートして安全に保存します。次のように移動する。 **Tenable** 脆弱性統合 > 統合 > **Tenable.sc** スキャン認証情報統合 をクリックして、スキャン認証情報統合に関する詳細情報を表示します。

9. [完了] をクリックして、変更内容を保存し、セットアップアシスタントでの構成を完了します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

次のタスク
(オプション)移動先 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 脆弱性の算出 > デフォルトのリスク計算機 > **Tenable** リスクルール Tenable リスクルールを有効にします。

表示される [脆弱性産出ルール] フォームで、[アクティブ] チェックボックスをオンにして有効にします。

Tenable リスクルールは、脆弱性対応 の脆弱性算出のデフォルトのリスク算出の一部として Vulnerability Response Integration with Tenable アプリケーションとともにインストールされます。脆弱性優先評価 (VPR) は、新しいデフォルトのリスク算出でインポートして使用される Tenable 製品の属性です。このリスクルールはデフォルトで非アクティブになっています。Tenable リスク算出ルールを有効にすると、インポートされた VPR 値が脆弱性一致アイテムのリスクスコアの計算に使用されます。このリスク算出のデフォルトの重み付け分布：VPR = 70%、資産 = 15%、ビジネス上の重要度 = 15%。この Tenable リスク算出ルールを有効にすると、データ取り込みのパフォーマンスが影響を受ける可能性があります。

「脆弱性対応 の算出と脆弱性算出ルール」を参照してください。

脆弱性ソリューションプロバイダーの設定

チェックリストに従って脆弱性ソリューションプロバイダーを設定し、セットアップアシスタントでプロバイダーを構成します。

ソリューション統合チェックリストの準備

セットアップアシスタントを使用して、Common Vulnerability Reporting Framework (CVRF) または Common Security Advisory Framework (CSAF) のデータ形式をサポートするすべてのベンダー向けにソリューションインテリジェンス統合の実装の準備を行います。

Common Vulnerability Reporting Framework (CVRF) ソリューション統合の準備

セットアップアシスタントを使用して、Common Vulnerability Reporting Framework (CVRF) データ形式をサポートするすべてのベンダー向けにソリューションインテリジェンス統合の実装の準備を行います。

事前準備

ソリューションを提供するベンダーと統合するには、次のチェックリストのタスクを実行してください。アプリケーションをインストールする前に、チェックリストを印刷して、リストされているアイテムが完了していることを確認してください。

統合準備チェックリスト

タスク	説明
依存アプリケーション ☐	以下のアプリケーションが ServiceNow Store からインストールされていることを確認します。 • Vulnerability Solution Management：脆弱性ソリューション管理 のインストールの詳細については、「セットアップアシスタントを使用した 脆弱性対応 サードパーティアプリケーションのインストール」および「脆弱性対応のソリューション管理アプリケーションのインストール」を参照してください。 • 脆弱性対応：脆弱性対応 アプリケーションのインストールおよびアクティブ化の詳細については、「脆弱性対応 のインストール」を参照してください。この統合には、脆弱性対応 のバージョン 16.1 以降が必要です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統合準備チェックリスト (続く)

タスク	説明
サードパーティアカウント認証情報 ☐	サードパーティアカウントの認証情報を使用できることを確認します。一部のソリューション統合では、認証情報を編集する必要があります。
ベンダー認証 ☐	API を使用してソリューションをインポートするためにベンダーを認証していることを確認します。ベンダーの認証方法の詳細については、「接続および資格情報エイリアスの構成」を参照してください。 API ベースのベンダーを設定しない場合は、この手順をスキップできます。
フローとフローアクションのカスタマイズ ☐	Cisco 以外の API ベースのベンダーを設定する場合は、アドバイザリーの応答から一意のキーと CVRF URL を抽出するためのフローとフローアクションをカスタマイズする必要があります。 **注:** CVRF URL の公開は、全ベンダーの標準ではありません。 Cisco 以外のベンダー向けにフローをカスタマイズするには、「Cisco 以外の Common Vulnerability Reporting Framework ベンダーの構成」を参照してください。 Cisco 以外のベンダーを設定しない場合は、この手順をスキップできます。デフォルトでは、Cisco 向けのフローはアプリケーションに付属しています。
ロール ☐	統合を管理できるアドミングループまたはユーザーが存在することを確認します。アサインされていない場合、アドミニストレーターは脆弱性アドミン (sn_vul.vulnerability_admin) およびその他のロールをアサインします。

Common Security Advisory Framework (CSAF) ソリューション統合の準備

セットアップアシスタントを使用して、Common Security Advisory Framework (CSAF) データ形式をサポートするすべてのベンダー向けにソリューションインテリジェンス統合を実装する準備を行います。

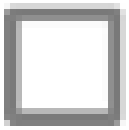
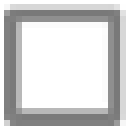
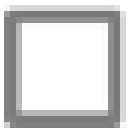
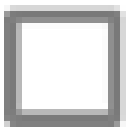
事前準備

ソリューションを提供するベンダーと統合するには、次のチェックリストのタスクを実行してください。アプリケーションをインストールする前に、チェックリストを印刷して、リストされているアイテムが完了していることを確認してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

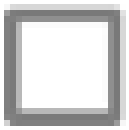
統合準備チェックリスト

タスク	説明
依存アプリケーション 	以下のアプリケーションが ServiceNow Store からインストールされていることを確認します。 • Vulnerability Solution Management：脆弱性ソリューション管理 のインストールの詳細については、「セットアップアシスタントを使用した 脆弱性対応 サードパーティアプリケーションのインストール」および「脆弱性対応のソリューション管理アプリケーションのインストール」を参照してください。 • 脆弱性対応：脆弱性対応 アプリケーションのインストールおよびアクティブ化の詳細については、「脆弱性対応 のインストール」を参照してください。この統合には、脆弱性対応 のバージョン 16.1 以降が必要です。
サードパーティアカウント認証情報 	サードパーティアカウントの認証情報を使用できることを確認します。一部のソリューション統合では、認証情報を編集する必要があります。
ベンダー認証 	API を使用してソリューションをインポートするためにベンダーを認証していることを確認します。ベンダーの認証方法の詳細については、「Common Security Advisory Framework (CSAF) の接続および資格情報エイリアスを構成する」を参照してください。 API ベースのベンダーを設定しない場合は、この手順をスキップできます。
フローとフローアクションのカスタマイズ 	Red Hat 以外の API ベースのベンダーを設定する場合は、アドバイザリーの応答から一意のキーと CSAF URL を抽出するためのフローとフローアクションをカスタマイズする必要があります。 **注:** CSAF URL の公開は、全ベンダーの標準ではありません。 Red Hat 以外のベンダー向けにフローをカスタマイズするには、「Red Hat 以外の Common Security Advisory Framework ベンダーを構成する」を参照してください。 Red Hat 以外のベンダーを設定しない場合は、この手順をスキップできます。デフォルトでは、Red Hat 向けのフローはアプリケーションに付属しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統合準備チェックリスト (続く)

タスク	説明
ロール 	統合を管理できるアドミングループまたはユーザーが存在することを確認します。アサインされていない場合、アドミニストレーターは脆弱性アドミン (sn_vul.vulnerability_admin) およびその他のロールをアサインします。

脆弱性ソリューションプロバイダーの構成

Vulnerability Solution Management アプリケーションをインストールした後、セットアップアシスタントを使用して脆弱性ソリューションプロバイダーを構成します。

始める前に

必要なロール：sn_vul.vulnerability_admin、sn_vul.admin (非推奨)、または admin。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合設定.
2. [ソリューション統合] をクリックします。
3. [インストール済みソリューション] セクションで、URL、API、またはインポートを使用してデータをフェッチします。
   - URL または API を使用してデータをフェッチするには、[統合を追加] をクリックします。
   - Common Vulnerability Response Framework (CVRF) ファイルまたは Common Security Advisory Framework (CSAF) ファイルをアップロードしてデータをフェッチするには、[ファイルをインポート] をクリックします。

次のタスク

データをインポートする形式に応じて、次のいずれかのタスクを実行できます。

- CVRF の場合：
  - CVRF ファイルをインポートする場合は、「ファイルインポートによる Common Vulnerability Reporting Framework データのインポート」を参照してください。
  - API を使用して CVRF データをインポートする場合は、「CVRF URL による Common Vulnerability Reporting Framework (CVRF) データのインポート」を参照してください。
  - アドバイザリーを介して CVRF データをインポートする場合は、「アドバイザリーからの Common Vulnerability Reporting Framework データのインポート」を参照してください。
- CSAF の場合：
  - CSAF ファイルをインポートする場合は、「 ファイルインポートによる Common Security Advisory Framework データのインポート」を参照してください。
  - API を使用して CSAF データをインポートする場合は、「 CSAF URL による Common Security Advisory Framework (CSAF) データのインポート」を参照してください。
  - アドバイザリーを介して CSAF データをインポートする場合は、「 アドバイザリーからの Common Security Advisory Framework データのインポート」を参照してください。
-

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Common Vulnerability Reporting Framework (CVRF)

Common Vulnerability Reporting Framework (CVRF) は、脆弱性レポートドキュメントを作成するための標準化されたフレームワークを提供します。これは XML ベースの言語であり、複数の組織の多様なステークホルダー間で重要なセキュリティ関連情報を簡単に共有できます。CVRF フォーマットを利用することで、情報の交換と処理を迅速化できます。

ファイルインポートによる **Common Vulnerability Reporting Framework** データのインポート

CVRF ファイルをインポートして CVRF 形式でデータを表示します。インポートは 1 回限りのアクティビティです。

始める前に
必要なロール：sn_vul.vulnerability_admin、sn_vul.admin (非推奨)、または admin。

このタスクについて
インポートされると、キューエントリーが添付ファイルとともに作成され、エントリーの処理時に解析されます。データはそれぞれのテーブルに入力されます。CVRF データを解析する前に、構成に基づいてスキャナーマッピングレコードが作成されます。次に、スキャナーマッピングデータがベンダーマッピングデータに変換されます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合設定 > ソリューション統合 > 共通脆弱性対応フレームワーク **(Common Vulnerability Response Framework)**.
2. [ファイルをインポート] をクリックします。

   注:
   一度にアップロードできるのは 1 つの XML ファイルのみで、最大ファイルサイズは 1 GB です。

3. [名前] フィールドに、統合の一意の名前を入力します。
   スケジューラーはこの名前で作成されます。
4. [ベンダー] フィールドに、ベンダーの名前を入力します。
   ソリューションの [ソース] フィールドにベンダー名が入力されます。
5. [完了] をクリックします。

タスクの結果
インポートキューが作成されます。情報バーのリンクをクリックすると、ベンダーのキューエントリーと関連リストが表示されます。ジョブのステータスを表示することもできます。

データが CVRF 形式にインポートされた後、データは次のように処理されます。

1. キューが処理されると、ファイルは専用のデータソースで解析されます。
2. 処理が完了すると、アプリケーションログが更新されます。
3. CVRF XML ファイルが解析されると、ServiceNow® 脆弱性対応 アプリケーションの以下のテーブルに入力されます。
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution
   - sn_vul_nvd_entry
   - sn_vul_software
   - sn_vul_product_category

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

エラーまたは例外に関連する詳細情報は、アプリケーションログで確認できます。

接続および資格情報エイリアスの構成

ベンダーを認証するために、接続および資格情報エイリアスを構成します。アドバイザリー解析では、サードパーティベンダーが認証されます。

始める前に

必要なロール：sn_vul.vulnerability_admin、sn_vul.admin (非推奨)、または admin

手順

1. OAuth 認証を作成します。
   「Create an endpoint for clients to access the instance (インスタンスにアクセスするクライアント用のエンドポイントを作成する)」を参照してください。
2. 接続および資格情報エイリアスを作成します。
   「Create a Connection and Credential alias (接続および資格情報エイリアスを作成する)」を参照してください。
3. 接続を作成します。
   a. 新しく作成された接続および資格情報エイリアスの名前をクリックします。
   b. [接続] タブで、[新規] をクリックします。
   c. 認証タイプが OAuth の場合は、ステップ 1 で **OAuth** エンティティプロファイルとして作成されたアプリケーションレジストリプロファイルを選択します。
   d. [接続] でレコードの関連リストからレコードを作成します。
   e. [認証情報] フィールドで、ステップ 3d で作成された認証情報レコードを選択します。
   f. [接続 **URL**] フィールドに、ベンダーの URL を入力します。
   g. **[Submit]** をクリックします。

Cisco 以外の **Common Vulnerability Reporting Framework** ベンダーの構成

Cisco 以外の Common Vulnerability Reporting Framework ベンダーを API サポートとともに構成します。

始める前に

必要なロール：sn_vul.vulnerability_admin、sn_vul.admin (非推奨)、または admin。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 接続と認証情報 > 接続 **&** 資格情報エイリアス.
2. ベンダーがサポートする認証タイプでレコードを作成します。
   ベンダーの認証方法の詳細については、「接続および資格情報エイリアスの構成」を参照してください。
3. 次のように移動する。 **All** (すべて) > 脆弱性対応 > **Flow Designer**.
4. 「アドバイザリー解析」というフローを複製します。

   注:
   - アクションを変更する必要がある場合は、アクションをコピーして新しいフローで使用してください。
   - ベンダーに従ってページネーション関連のロジックを更新してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. 日付範囲パラメーターのロジックが Cisco と同じでない場合は、[ページネーションパラメーターの更新] アクションをコピーし、ベンダーの要求に応じて変更します。
6. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 拡張データマッピング.
7. ベンダーに従って [プロパティキー] の値を変更して、Cisco 向けのレコードを作成します。このロジックは、必要なフィールドをアドバイザリーペイロードから ServiceNow テーブルにマッピングするためのものです。
8. API ペイロードから以下の API タグをマッピングします。これらのタグを詳細情報にマッピングして、拡張データマッピングテーブルに入力する必要があります。デフォルトでは、Cisco 固有のマッピングが付属しています。

   注:
   アドバイザリーを公開する複数のベンダーを構成する必要がある場合は、レコードを作成する必要があります。

アドバイザリーペイロードタグ	テーブル **sn_vul_cvrf_solution_integration** の列	説明
CVRF URL	cvrf_url	CVRF URL を含むタグ名。
アドバイザリー ID (応答の一意のキー)	ID	一意の識別子を含むタグ名。
最終変更日	last_modified_date	レコードが最後に更新された日付を含むタグ名。
securityAdvisoryIntegrationSyncS	統合	脆弱性ソリューションレコードを作成する統合スケジュール済みジョブ sysId を参照します。

9. 応答形式に基づいて、アドバイザリー解析フローから [リストを取得] アクションをコピーして解析のロジックを変更します。

アドバイザリーからの **Common Vulnerability Reporting Framework** データのインポート

インポートタイプを API としてベンダー URL を設定して、アドバイザリーから CVRF データをインポートします。

始める前に
必要なロール：sn_vul.vulnerability_admin、sn_vul.admin (非推奨)、または admin

このタスクについて
統合が実行されると、アドバイザリーがフェッチされます。CVRF URL とアドバイザリー ID がペイロードから抽出されます。CVRF URL ごとに REST API 呼び出しが行われ、データが解析されて sn_vul_solution テーブルに格納されます。

手順
1. 次のように移動する。 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合設定 > ソリューション統合 > 共通脆弱性対応フレームワーク **(Common Vulnerability Response Framework)**.
2. [統合を追加] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. フォームのフィールドに入力します。

ソリューションアドバイザリーフォームのインポート

フィールド	説明
インポートタイプ	インポートタイプを選択するオプション。[**API**] を選択します。
名前	統合の一意の名前。
ベンダー	ベンダーの名前。 **注:** ソリューションの [ソース] フィールドにベンダー名が入力されます。
接続エイリアス	認証された認証情報を選択するオプション。 **注:** sys_alias テーブルには、認証情報とアドバイザリーのベース URL が格納されます。
スケジュール	データを更新する頻度。
曜日	データを更新する曜日。
時刻	データを更新する曜日の時間。
API 構成	
フロー	フローを選択するオプション。 スケジューラーが実行されると、フローがトリガーされます。フローは、アドバイザリーを解析し、CVRF URL を抽出して、それらの詳細を更新テーブルに保存します。既存のフローをコピーし、必要に応じて編集できます。たとえば、ページネーションに関連する変更を行うことができます。
フローアクション	フローアクションを選択するオプション。 フローアクションは、スライディングウィンドウ機能を処理します。フローアクションを更新し、クエリパラメーターをドラッグしてアクションに直接追加できます。
マッピングテーブル	マッピングテーブルを選択するオプション。 拡張データマッピングテーブルのレコードは、アドバイザリーのペイロードから CVRF URL とアドバイザリー ID を抽出するために使用されます。
応答からの勧告	アドバイザリーのリストの抽出元になるアドバイザリーのペイロードからタグ名を入力するオプション。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
フィルター基準	
時間範囲パラメーター	要求の時間範囲と API 呼び出しの日付形式を選択するオプション。 開始日/終了日要求パラメーターは、API 呼び出し中に開始日と終了日に使用されるパラメーター名です。例：StartDate、start_date、endDate、end_date。
日付形式	日付形式を入力するオプション (mm/dd/yyyy など)。 日付形式は、API がフィルタリングのために必要とする形式です。GlideDate でサポートされていない形式は機能しません。
初期範囲 (日数)	スケジューラーの初回実行時にデータをフェッチする必要がある日数を入力します。 後続の実行では、スライディングウィンドウメカニズムに従います。 **注:** 時間範囲を選択しない場合は、[パラメーターなし] を選択します。
スキャナーマッピング	
スキャナーソース	サードパーティエントリー (TPE) のソースを選択するオプション。
脆弱性列	キーワードを選択するオプション。
キーワード	選択した脆弱性列を検索するためのキーワードを入力するオプション。

4. [完了] をクリックします。

CVRF URL による Common Vulnerability Reporting Framework (CVRF) データのインポート

セットアップアシスタントでベンダー URL を設定して、CVRF データをインポートします。

始める前に

必要なロール：sn_vul.vulnerability_admin、sn_vul.admin (非推奨)、または admin

このタスクについて

統合が実行されると、解析される URL からデータがフェッチされます。データは、ベンダー名をソースとした sn_vul_solution テーブルに格納されます。

注:
Oracle は、ソリューションを提供するために CVRF URL を直接公開します。したがって、Oracle データをインポートするための統合を構成する場合は、Oracle の CVRF URL があることを確認し、次の手順に従います。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合設定 > ソリューション統合 > 共通脆弱性対応フレームワーク **(Common Vulnerability Response Framework)**.
2. [統合を追加] をクリックします。
3. フォームのフィールドに入力します。

CVRF フォームのインポート

フィールド	説明
インポートタイプ	インポートのタイプ。**[URL]** を選択します。
名前	統合の一意の名前。
ベンダー	ベンダーの名前。 **注:** ソリューションの [ソース] フィールドにベンダー名が入力されます。
URL	CVRF 形式のソリューションデータのフェッチ元 URL。
スケジュール	データを更新する頻度。 **注:** CVRF のステータスタグに「FINAL」が表示されている場合、不要な実行を防ぐためにフィールドは自動的に [オンデマンド] に設定されます。
曜日	データを更新する曜日。
時刻	データを更新する曜日の時間。

4. [完了] をクリックします。

Common Vulnerability Reporting Framework データインポートのトラブルシューティング

トラブルシューティングのアクションは、脆弱性対応アプリケーションで CVRF データをインポートする際の一般的な問題の解決に役立ちます。

問題	アクション
統合実行時間が長い	統合が予想よりも長期間実行される場合は、次の手順を実行します。 1. sn_vul_ds_import_q_entry テーブルに移動します。 2. [ステータス] フィールドでグループ化します。[完了]、[処理中]、または [キューに格納 (In queued)] 状況のエントリーを確認できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

問題	アクション
API ベースのインポートで統合が失敗した	API ベースのインポートで統合が失敗した場合は、次の手順を実行します。 **1.** [フローデザイナー] に移動します。 **2.** 構成で選択されたフローを開きます。 **注:** Cisco の場合は、アドバイザリー解析フローを開きます。 **3.** [実行] をクリックします。 **4.** 最新の実行またはデバッグする必要がある実行を開きます。 **5.** 各ステージのフローを確認します。
API ベースのインポートでタイムアウトエラーにより統合が失敗した	アドバイザリー解析フローのタイムアウトが原因で API ベースのインポートにおいて統合が失敗した場合は、次の手順を実行します。 **1.** sys_properties.LIST を開いてタイムアウト値を増やします。 **2.** [名前] 列で、sn_vul.CVRFFlowTimeout (inMiliSeconds) を検索します。 **注:** 時間はミリ秒単位です。 **3.** レコードを開き、大きい数値に更新します。 **4.** レコードを保存し、統合を再実行します。
「ベンダーマッピングデータ変換へのスキャナーマッピングが進行中です (Scanner mapping to vendor-mapping data transformation is in progress)」というエラーで統合が失敗した	統合が URL または API ベースのインポート中に「ベンダーマッピングデータ変換へのスキャナーマッピングが進行中です (Scanner mapping to vendor-mapping data transformation is in progress)」というエラーで失敗したかどうかを確認します。データは、変換が完了した後にのみ入力されます。しばらくしてから実行してください。 このエラーが発生した場合は、しばらく待ってから統合を再度実行してください。
ファイルのインポート中にインポートキューが作成されない	ファイルのインポート中に、インポートキューが作成されないことがあります。このエラーは、スキャナーマッピングデータをベンダーマッピングデータにマッピングする変換が進行中であることを意味します。プロセスが完了すると、キューエントリーが作成されます。

Common Security Advisory Framework (CSAF)

Common Security Advisory Framework (CSAF) を 脆弱性ソリューション管理 と併用すると、機械可読な JSON 形式による自動セキュリティ通知が可能になります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

CSAF では、ソリューション管理フレームワークを使用して任意のソリューションインテリジェンスベンダーと統合し、インテリジェンスデータをインポートできます。CSAF セキュリティ通知は、次のいずれかのタイプになります。

- セキュリティアドバイザリー
- Vulnerability Exploitability Exchange (VEX)
- セキュリティインシデントレスポンス
- 情報アドバイザリー

CSAF は、ベンダーからのセキュリティアドバイザリーのファイルインポート、URL インポート、および API インポートのみをサポートします。

ファイルインポートによる **Common Security Advisory Framework** データのインポート

CSAF ファイルをインポートして CSAF 形式でデータを表示します。インポートは 1 回限りのアクティビティです。

始める前に

必要なロール：sn_vul.vulnerability_admin、sn_vul.admin (非推奨)、または admin。

このタスクについて

インポートされると、キューエントリーが添付ファイルとともに作成され、エントリーの処理時に解析されます。データはそれぞれのテーブルに入力されます。CSAF データを解析する前に、構成に基づいてスキャナーマッピングレコードが作成されます。次に、スキャナーマッピングデータがベンダーマッピングデータに変換されます。

スキャナーマッピングは、脆弱性情報データベース (NVD) ベースの脆弱性には適用されません。NVD ベースの脆弱性は、NVD データベースに Common Vulnerability Entry (CVE) を含む脆弱性です。

最も優先度が高いソリューションが 1 つしかなく、それが脆弱性一致アイテムにロールダウンされる場合は、優先ソリューションが設定されます。1 つの NVD エントリーに複数のベンダーソリューションが含まれている場合、最上位の優先ソリューションが複数あるため、優先ソリューションは入力されません。この場合、ソリューションを手動で選択する必要があります。サードパーティの脆弱性の場合、優先ソリューションは、対応するスキャナーマッピングを追加した場合にのみ入力されます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合設定 > ソリューション統合 > 共通セキュリティアドバイザリーフレームワーク.
2. [ファイルをインポート] を選択します。

   注:
   一度にアップロードできるのは 1 つの JSON ファイルのみで、最大ファイルサイズは 15 MB です。

3. [名前] フィールドに、統合の一意の名前を入力します。
   スケジューラーはこの名前で作成されます。
4. [ベンダー] フィールドに、ベンダーの名前を入力します。
   ソリューションの [ソース] フィールドにベンダー名が入力されます。
5. [完了] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスクの結果
インポートキューが作成されます。情報バーのリンクを選択すると、ベンダーのキューエントリーと関連リストが表示されます。ジョブのステータスを表示することもできます。

データが CSAF 形式にインポートされた後、データは次のように処理されます。

1. キューが処理されると、ファイルは専用のデータソースで解析されます。
2. 処理が完了すると、アプリケーションログが更新されます。
3. CSAF JSON ファイルが解析されると、ServiceNow® 脆弱性対応アプリケーションの以下のテーブルに入力されます。
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution
   - sn_vul_nvd_entry
   - sn_vul_software
   - sn_vul_product_category

エラーまたは例外に関連する詳細情報は、アプリケーションログで確認できます。

Common Security Advisory Framework (CSAF) の接続および資格情報エイリアスを構成する

ベンダーを認証するために、接続および資格情報エイリアスを構成します。アドバイザリー解析では、サードパーティベンダーが認証されます。

始める前に
必要なロール：sn_vul.vulnerability_admin、sn_vul.admin (非推奨)、または admin

手順

1. OAuth 認証を作成します。
   「Create an endpoint for clients to access the instance (インスタンスにアクセスするクライアント用のエンドポイントを作成する)」を参照してください。
2. 接続および資格情報エイリアスを作成します。
   「Create a Connection and Credential alias (接続および資格情報エイリアスを作成する)」を参照してください。
3. 接続を作成します。
   a. 新しく作成された接続および資格情報エイリアスの名前を選択します。
   b. [接続] タブで、[新規] を選択します。
   c. 認証タイプが OAuth の場合は、ステップ 1 で **OAuth** エンティティプロファイルとして作成されたアプリケーションレジストリプロファイルを選択します。
   d. [接続] でレコードの関連リストからレコードを作成します。
   e. [認証情報] フィールドで、ステップ 3d で作成された認証情報レコードを選択します。
   f. [接続 **URL**] フィールドに、ベンダーの URL を入力します。
   g. [送信] を選択します。

Red Hat 以外の Common Security Advisory Framework ベンダーを構成する

API サポートを使用して、Red Hat 以外の Common Security Advisory Framework (CSAF) ベンダーを構成します。

始める前に
必要なロール：sn_vul.vulnerability_admin、sn_vul.admin (非推奨)、または admin。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 接続と認証情報 > 接続 **&** 資格情報エイリアス.
2. ベンダーがサポートする認証タイプでレコードを作成します。
   ベンダーの認証方法の詳細については、「Common Security Advisory Framework (CSAF) の接続および資格情報エイリアスを構成する」を参照してください。
3. 次のように移動する。 **All** (すべて) > 脆弱性対応 > **Flow Designer**.
4. 「アドバイザリー解析」というフローを複製します。

   注:
   - アクションを変更する必要がある場合は、アクションをコピーして新しいフローで使用してください。
   - ベンダー API に従って、page_index_key パラメーターと page_size_key パラメーターを確認します。
   - ベンダーに従ってページネーション関連のロジックを更新してください。

5. 日付範囲パラメーターのロジックが Red Hat と同じでない場合は、[ページネーションパラメーターの更新] アクションをコピーし、ベンダーの要求に応じて変更します。
6. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 拡張データマッピング.
7. ベンダーに従って [プロパティキー] の値を変更して、Red Hat 向けのレコードを作成します。
   このロジックは、必要なフィールドをアドバイザリーペイロードから ServiceNow テーブルにマッピングするためのものです。
8. API ペイロードから以下の API タグをマッピングします。
   これらのタグを詳細情報にマッピングして、拡張データマッピングテーブルに入力する必要があります。デフォルトでは、Red Hat 固有のマッピングが付属しています。

   注:
   アドバイザリーを公開する複数のベンダーを構成する必要がある場合は、レコードを作成する必要があります。

アドバイザリーペイロードタグ	テーブル **sn_vul_cvrf_solution_integration** の列	説明
CSAF URL (CSAF ペイロードを指すリソース URL)	cvrf_url	CSAF URL を含むタグ名。
アドバイザリー ID (応答の一意のキー)	ID	一意の識別子を含むタグ名。
最終変更日	last_modified_date	レコードが最後に更新された日付を含むタグ名。
csaf (静的値)	advisory_format	CSAF ペイロードのアドバイザリーフォーマットの値。これは、すべての CSAF 統合に適用される静的値であることに注意してください。
securityAdvisoryIntegrationSyncS	統合	脆弱性ソリューションレコードを作成する統合スケジュール

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

アドバイザリーペイロードタグ	テーブル **sn_vul_cvrf_solution_integration** の列	説明
		済みジョブ sysId を参照します。

9. 応答形式に基づいて、アドバイザリー解析フローから [リストを取得] アクションをコピーして解析のロジックを変更します。

アドバイザリーからの **Common Security Advisory Framework** データのインポート

インポートタイプを API としてベンダー URL を設定して、アドバイザリーから CSAF データをインポートします。

始める前に
必要なロール：sn_vul.vulnerability_admin、sn_vul.admin (非推奨)、または admin

このタスクについて
統合が実行されると、アドバイザリーがフェッチされます。CSAF URL とアドバイザリー ID がペイロードから抽出されます。CSAF URL ごとに REST API 呼び出しが行われ、データが解析されて sn_vul_solution テーブルに格納されます。

スキャナーマッピングは、脆弱性情報データベース (NVD) ベースの脆弱性には適用されません。NVD ベースの脆弱性は、NVD データベースに Common Vulnerability Entry (CVE) を含む脆弱性です。

最も優先度が高いソリューションが 1 つしかなく、それが脆弱性一致アイテムにロールダウンされる場合は、優先ソリューションが設定されます。1 つの NVD エントリーに複数のベンダーソリューションが含まれている場合、最上位の優先ソリューションが複数あるため、優先ソリューションは入力されません。この場合、ソリューションを手動で選択する必要があります。サードパーティの脆弱性の場合、優先ソリューションは、対応するスキャナーマッピングを追加した場合にのみ入力されます。

手順
1. 次のように移動する。 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合設定 > ソリューション統合 > 共通セキュリティアドバイザリーフレームワーク.
2. [統合を追加] を選択します。
3. フォームのフィールドに入力します。

ソリューションアドバイザリーフォームのインポート

フィールド	説明
インポートタイプ	インポートタイプを選択するオプション。[**API**] を選択します。
名前	統合の一意の名前。
ベンダー	ベンダーの名前。 **注:** ソリューションの [ソース] フィールドにベンダー名が入力されます。
接続エイリアス	認証された認証情報を選択するオプション。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: sys_alias テーブルには、認証情報とアドバイザリーのベース URL が格納されます。
スケジュール	データを更新する頻度。
曜日	データを更新する曜日。
時刻	データを更新する曜日の時間。
API 構成	
フロー	フローを選択するオプション。 スケジューラーが実行されると、フローがトリガーされます。フローは、アドバイザリーを解析し、CSAF URL を抽出して、それらの詳細を更新テーブルに保存します。既存のフローをコピーし、必要に応じて編集できます。たとえば、ページネーションに関連する変更を行うことができます。
フローアクション	フローアクションを選択するオプション。 フローアクションは、スライディングウィンドウ機能を処理します。フローアクションを更新し、クエリパラメーターをドラッグしてアクションに直接追加できます。
マッピングテーブル	マッピングテーブルを選択するオプション。 拡張データマッピングテーブルのレコードは、アドバイザリーのペイロードから CSAF URL とアドバイザリー ID を抽出するために使用されます。
応答からの勧告	アドバイザリーのリストの抽出元になるアドバイザリーのペイロードからタグ名を入力するオプション。
フィルター基準	
時間範囲パラメーター	要求の時間範囲と API 呼び出しの日付形式を選択するオプション。 開始日/終了日要求パラメーターは、API 呼び出し中に開始日と終了日に使用されるパラメーター名です。例：StartDate、start_date、endDate、end_date。
日付形式	日付形式を入力するオプション (`mm/dd/yyyy` など)。 日付形式は、API がフィルタリングのために必要とする形式です。GlideDate でサポートされていない形式は機能しません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
初期範囲 (日数)	スケジューラーの初回実行時にデータをフェッチする必要がある日数を入力します。 後続の実行では、スライディングウィンドウメカニズムに従います。 **注:** 時間範囲を選択しない場合は、[パラメーターなし] を選択します。
スキャナーマッピング	
スキャナーソース	サードパーティエントリー (TPE) のソースを選択するオプション。
脆弱性列	キーワードを選択するオプション。
キーワード	選択した脆弱性列を検索するためのキーワードを入力するオプション。

4. [完了] を選択します。

CSAF URL による Common Security Advisory Framework (CSAF) データのインポート

セットアップアシスタントでベンダー URL を設定して、CSAF データをインポートします。

始める前に
必要なロール：sn_vul.vulnerability_admin、sn_vul.admin (非推奨)、または admin

このタスクについて
統合が実行されると、解析される URL からデータがフェッチされます。データは、ベンダー名をソースとした sn_vul_solution テーブルに格納されます。

注:
URL は、アドバイザリーの詳細を含む直接 CSAF ペイロード、または Resource-Oriented Lightweight Information Exchange (ROLIE) フィード URL のいずれかです。いずれの場合も、ペイロードは適切に解析され、ソリューションレコードが作成されます。CSAF URL をインポートするには、次の手順を実行します。

ROLIE フィードをサポートする URL インポートを使用して、CSAF 集積者または信頼できるプロバイダーから脆弱性ソリューションをインポートすることもできます。これらの脆弱性ソリューションは、共通脆弱性識別子 (CVE) に基づいて、正しいベンダーおよび脆弱性一致アイテム (VIT) に自動的にマッピングされます。

スキャナーマッピングは、脆弱性情報データベース (NVD) ベースの脆弱性には適用されません。NVD ベースの脆弱性は、NVD データベースに Common Vulnerability Entry (CVE) を含む脆弱性です。

最も優先度が高いソリューションが 1 つしかなく、それが脆弱性一致アイテムにロールダウンされる場合は、優先ソリューションが設定されます。1 つの NVD エントリーに複数のベンダーソリューションが含まれている場合、最上位の優先ソリューションが複数あるため、優先ソリューションは入力されません。この場合、ソリューションを手動で選択する必要があります。サードパーティの脆弱性の場合、優先ソリューションは、対応するスキャナーマッピングを追加した場合にのみ入力されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合設定 > ソリューション統合 > 共通セキュリティアドバイザリーフレームワーク.
2. [統合を追加] を選択します。
3. フォームのフィールドに入力します。

CSAF フォームのインポート

フィールド	説明
インポートタイプ	インポートのタイプ。**[URL]** を選択します。
名前	統合の一意の名前。
単一ベンダー	1 つのベンダーから CSAF をインポートする場合は、このオプションを選択します。
ベンダー	ベンダーの名前。このフィールドは、[単一ベンダー] を選択した場合にのみ使用できます。 注: ソリューションの [ソース] フィールドにベンダー名が入力されます。
マルチベンダー	複数のベンダーから CSAF をインポートする場合は、このオプションを選択します。
集計関数	ソリューションをインポート可能な信頼できるプロバイダー。
URL	CSAF 形式のソリューションデータのフェッチ元 URL。
スケジュール	データを更新する頻度。 注: CSAF のステータスタグに「最終」が表示されている場合、不要な実行を防ぐためにフィールドは自動的に [オンデマンド] に設定されます。
日	データを更新する曜日。
時刻	データを更新する曜日の時間。
スキャナーマッピング 注: [スキャナーマッピング] セクションは、CSAF ではオプションです。	
スキャナーソース	サードパーティエントリー (TPE) のソースを選択するオプション。
脆弱性列	キーワードを選択するオプション。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
キーワード	選択した脆弱性列を検索するためのキーワードを入力するオプション。

4. [完了] を選択します。

Common Security Advisory Framework データインポートのトラブルシューティング

トラブルシューティングのアクションは、脆弱性対応アプリケーションで CSAF データをインポートする際の一般的な問題の解決に役立ちます。

問題	アクション
統合実行時間が長い	統合が予想よりも長期間実行される場合は、次の手順を実行します。 1. sn_vul_ds_import_q_entry テーブルに移動します。 2. [ステータス] フィールドでグループ化します。[完了]、[処理中]、または [キューに格納 (In queued)] 状況のエントリーを確認できます。
API ベースのインポートで統合が失敗した	API ベースのインポートで統合が失敗した場合は、次の手順を実行します。 1. [フローデザイナー] に移動します。 2. 構成で選択されたフローを開きます。 注: Red Hat の場合、アドバイザリー解析フローを開きます。 3. **[Executions]** を選択します。 4. 最新の実行またはデバッグする必要がある実行を開きます。 5. 各ステージのフローを確認します。
API ベースのインポートでタイムアウトエラーにより統合が失敗した	アドバイザリー解析フローのタイムアウトが原因で API ベースのインポートにおいて統合が失敗した場合は、次の手順を実行します。 1. sys_properties.LIST を開いてタイムアウト値を増やします。 2. [名前] 列で、sn_vul.CVRFFlowTimeout (inMiliSeconds) を検索します。 注: 時間はミリ秒単位です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

問題	アクション
	3. レコードを開き、大きい数値に更新します。 **4.** レコードを保存し、統合を再実行します。
「ベンダーマッピングデータ変換へのスキャナーマッピングが進行中です (Scanner mapping to vendor-mapping data transformation is in progress)」というエラーで統合が失敗した	統合が URL または API ベースのインポート中に「ベンダーマッピングデータ変換へのスキャナーマッピングが進行中です (Scanner mapping to vendor-mapping data transformation is in progress)」というエラーで失敗したかどうかを確認します。データは、変換が完了した後にのみ入力されます。しばらくしてから実行してください。 このエラーが発生した場合は、しばらく待ってから統合を再度実行してください。
ファイルのインポート中にインポートキューが作成されない	ファイルのインポート中に、インポートキューが作成されないことがあります。このエラーは、スキャナーマッピングデータをベンダーマッピングデータにマッピングする変換が進行中であることを意味します。プロセスが完了すると、キューエントリーが作成されます。

追加の脆弱性対応セットアップおよび構成タスク

修復に役立てるために、基本セットアップ以外にこれらの追加の管理セットアップタスクを構成の一環として実行できます。これらのタスクは、セットアップアシスタントの外部で実行します。

脆弱性対応 で提供されるデフォルトのレポートを使用して、セキュリティ体制を監視できます。現在の環境に合わない場合は、こうしたレポートを編集するか、または独自のレポートを作成するためのテンプレートとして使用できます。

脆弱性対応のパフォーマンスアナリティクス アプリケーションがインストールされている場合は、レポート、レスポンシブダッシュボードなどを作成できます。詳細については、「レポートの概要」を参照してください。

メール通知により、生産性が向上し、ワークフローがスムーズになります。

ソフトウェアエクスポージャーアセスメントでは、ソフトウェア資産管理 (SAM の基盤) で公開者、製品名、およびバージョン番号を検索して、脆弱なソフトウェアへのエクスポージャーを特定します。

脆弱性ライブラリの可視化により、グループ化と修復タスクに柔軟性を持たせることができます。

例外管理を構成すると、公開されている脆弱性管理やセキュリティポリシー、標準、指針に組織が準拠できない場合に例外を要求する際に役立ちます。

追加のセットアップタスクについては、この概要の後に続くトピックを参照してください。

脆弱性対応のクイックスタートテスト

アプリケーションの開発やアップグレードの適用などの構成変更を行った後も、脆弱性対応 が変わらず正常に動作するかを検証します。自分のインスタンスに固有のデータを使用するときは、それが成功するように、これらのクイックスタートテストをコピーしてカスタマイズします。

本番システムでテストを実行できないようにするために、テスト実行プロパティはデフォルトでは無効になっています。開発、テスト、およびその他の非本番インスタンスでのみテストを実行してください。デモデータやデモアカウントが作成されている場合は、非本番環境または本番環境でインスタンスを使用する前に、すべてのデモデータを削除する必要があります。脆弱性対応 のテストスイー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

トの設定と実行の詳細については、「脆弱性対応 の自動テストフレームワーク (ATF) テストスイートの実行」を参照してください。

脆弱性対応 クイックスタートテストでは、脆弱性対応 アプリケーション (sn_vul) をアクティブ化してデモデータをロードする必要があります。

脆弱性対応 テスト

テスト	説明	リリースバージョン
VR：修正ターゲットルールの作成	修正ターゲットルールを作成します。	Madrid
VR：脆弱性グループルールの作成	脆弱性グループルールを作成します。	Madrid
VR：フォームを介した脆弱性一致アイテムの作成	ユーザーが脆弱性一致アイテムフォームから脆弱性一致アイテムを正常に作成できるかどうかを判断します。	Madrid
VR：脆弱性グループのライフサイクル	ユーザーが脆弱性グループを正常に解決できるかどうかを判断します。	Madrid
VR：脆弱性一致アイテムのライフサイクル	ユーザーがライフサイクルを通して脆弱なアイテムを正常に移動できるかどうかを判断し、クローズ済みの脆弱性一致アイテムを再度開くことができるかどうかを判断します。	Madrid
VR：ロールアップ計算機	ロールアップリスク計算機が、脆弱性グループのすべての脆弱なアイテムのスコアを使用して、脆弱なアイテムのグループ全体の全体的なリスクスコアを算出できるかどうかを判断します。	New York
VR：脆弱性対応 アサインルール	アサインルールのサンプルセットが脆弱なアイテムをアサイングループに自動アサインして修復できるかどうかを確認します。	New York
VR：脆弱性計算機	脆弱性計算機をテストします。	New York
VR：CI ルックアップ - Qualys	「field_matching」メソッドを使用して、Qualys 用の「ネットワークアダプターによるルックアップ」という名前の新しいルックアップルールを作成します。新しいルックアップルールを使用し、ネットワークアダプターおよび IP アダプターで、[検出されたアイテム] テーブルの構成アイテムに一致させることができるかどうかを確認します。	Orlando

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 テスト (続く)

テスト	説明	リリースバージョン
VR：通常および緊急の変更要求の作成	ユーザーが脆弱性グループから通常および緊急の変更要求を作成できるかどうかを確認します。	Orlando
VR：脆弱性グループの分割	ユーザーが脆弱性グループを分割できるかどうかを確認します。	Orlando
VR：CHG がキャンセルされたときに VG ステータスを更新	脆弱性グループに関連付けられている変更要求がキャンセルされたときに、脆弱性グループの [ステータス] フィールドが正常に移行するかどうかを確認します。	Orlando
VR：CHG が [レビュー] に移行したときに VG ステータスを更新	脆弱性グループに関連付けられている変更要求が [レビュー] ステータスに移行したときに、脆弱性グループの [ステータス] フィールドが正常に移行するかどうかを確認します。	Orlando
VR：CI ルックアップ - Rapid7	既存の Rapid7 脆弱性統合 ルックアップルール、 **IP** アドレスを使用して CI ルックアップをテストします。	Orlando
VR：CI ルックアップ - Qualys	Qualys 脆弱性統合 に対する新しいルックアップルールを作成して CI ルックアップをテストします。	Orlando
VR：VI の例外承認ワークフロー	例外要求を作成し、承認プロセスが機能していることを確認します。	Orlando
VR：VI の誤検出承認ワークフロー	誤検出の例外要求を作成し、承認プロセスが機能していることを確認します。	Orlando
VR: アプリケーション脆弱性対応 (AVR)	ルールと計算機が正しく機能しているかどうかを判定します。更新が機能していることを検証します。	Orlando
修復ターゲットルール：VI インポートテスト	インポート中に VR 修復ターゲットルールをテストします。	Paris
VR：分類ルール	脆弱性を自動的に分類するサンプル分類ルール	Tokyo

関連情報

クイックスタートテスト

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 の自動テストフレームワーク (ATF) テストスイートの実行

脆弱性対応 アプリケーションをインストールまたはアップグレードした後に、自動テストフレームワーク (ATF) テストスイートを実行します。

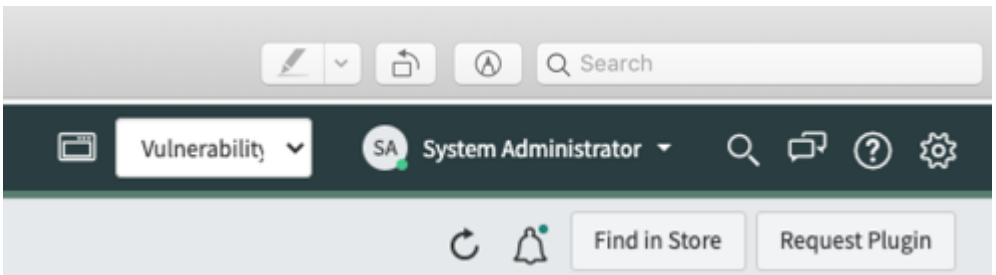
始める前に

正常にインストールされ、インスタンスが設計どおりに機能することを確認します。

本番システムでテストを実行できないようにするために、テスト実行プロパティはデフォルトでは無効になっています。開発、テスト、およびその他の非本番インスタンスでのみテストを実行してください。デモデータやデモアカウントが作成されている場合は、非本番環境または本番環境でインスタンスを使用する前に、すべてのデモデータを削除する必要があります。

- 脆弱性対応 をインストールしたときにデモデータがインストールされていることを確認します。脆弱性対応 テストスイートを実行するには、デモデータが必要です。
- テストを有効にするには、次の手順を実行します。
  1. 次のように移動する。 **All** (すべて) > 自動テストフレームワーク **(ATF)** > アドミニストレーション > プロパティ.
  2. [テスト/テストスイートの実行を有効にする] チェックボックスがオンになっていない場合は、オンにします。
  3. [保存] をクリックします。
  4. ヘッダーでスコープが [脆弱性対応] に設定されていないか、ヘッダーにスコープが表示されていない場合は、ブラウザーウィンドウの設定アイコン ( ) をクリックします。
  5. [システムの設定] ウィンドウで、[開発者] をクリックします。
  6. 選択されていない場合は、[ヘッダーにアプリケーションピッカーを表示 **(Show application picker in header)]** をクリックしてウィンドウを閉じます。
  7. [システムアドミニストレーター] の横に表示されるリストで、フィールドの [脆弱性対応] をクリックします。

     フィールドは、次の画像のように表示されます。



必要なロール：admin または atf_test_admin

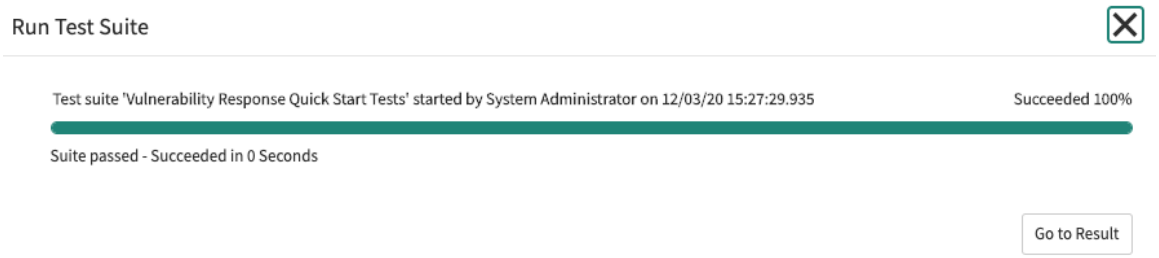
手順

1. 次のように移動する。 **All** (すべて) > 自動テストフレームワーク **(ATF)** > スイート.
2. [テストスイート] リストから、[脆弱性対応クイックスタートテスト **(Vulnerability Response Quick Start Tests)]** を見つけます。
3. それを選択してレコードを開きます。
4. 開いたレコードで、[アクティブ] チェックボックスをオンにします。
5. [更新] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [テストスイートを実行] ボタンが表示されない場合は、画面をリフレッシュしてレコードを再度開き、[テストスイートを実行] をクリックしてテストを開始します。
しばらくすると、[テストスイートを実行] ダイアログにテストの成功が表示されます。詳細については、[結果に移動] をクリックしてくださ



い。

次のタスク
おめでとうございます!脆弱性対応 の構成を続行できます。

脆弱性対応 の自動テスト、自動テスト、テストスイート、および自動テストの作成の詳細については、「自動テストフレームワーク (ATF)」を参照してください。

脆弱性対応対応 脆弱性アサインの推奨 のインストール

脆弱性アサインの推奨 をインストールにして、アサインが解除されたか間違ってアサインされた、脆弱性の検出結果の所有者を特定するために費やす時間を短縮します。このアプリケーションはServiceNow Store の別のサブスクリプションとして利用できます。

始める前に ®
Now Platform インスタンスの 脆弱性対応 の 脆弱性アサインの推奨 機能を実行する前に、脆弱性対応 アプリケーションの 脆弱性アサインの推奨 を最初にダウンロードしてインストールする必要があります。インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

> **注:**
> このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。詳細については「Activate a ServiceNow Store application (ServiceNow Store アプリケーションのアクティブ化)」を参照してください。

必要なロール：admin

セットアップタスク	アクション
脆弱性対応 アプリケーションがインストールされ、アクティブ化されていることを確認します。	次のように移動する。 **All** (すべて) > システムアプリケーション > すべてのアプリケーション > インスタンスにインストールされている. 脆弱性対応 がインストールされている場合は、このリストに表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応 のインストール」を参照してください。
予測インテリジェンス アプリケーションがインストールされ、アクティブ化されていることを確認します。	次のように移動する。 システムアプリケーション > すべてのアプリケーション > インスタンス

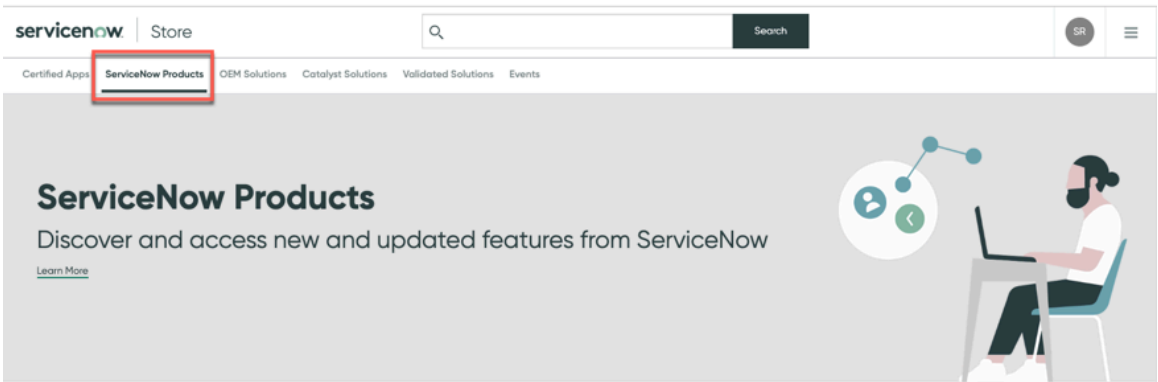
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	アクション
	にインストールされている. 予測インテリジェンス がインストールされている場合は、このリストに表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「Install Predictive Intelligence」を参照してください。
インスタンスに必要な ServiceNow ロールがあることを確認します。	インストールおよび予想される結果の検証に必要な以下のロールがあることを確認します。 • vulnerability_admin：脆弱性アサインの推奨 を有効にして構成するために必要です。また、このロールを使用して、脆弱性一致アイテムと修復タスクのアサインの推奨事項を表示および選択することもできます。 • ServiceNow admin：アプリケーションをインストールするために必要です。

手順

1. ServiceNow Store に移動します。
2. [ログイン] をクリックし、HI 認証情報を入力します。
3. 利用可能な ServiceNow 製品を表示するには、ServiceNow [製品] タブをクリックします。



4. 脆弱性アサインの推奨 のエンタイトルメントを所有しているすべての関連アプリケーションを表示するには、脆弱性対応 製品をクリックします。

   ページには、オプトインした場合に利用できるすべてのアプリケーションが一覧表示されます。アプリケーションの詳細を参照するには、アプリケーションのリンクをクリックしてください。

5. 脆弱性アサインの推奨 のエンタイトルメントがあることを確認するには、[オプトイン] をクリックします。
6. 契約条件に同意するには、チェックボックスをオンにして [同意する] をクリックします。
   アプリケーションに正常にオプトインしたことを示すメッセージが表示されます。
7. ステップ 10 に進んで、Now Platform インスタンスにアプリケーションをインストールします。
8. オプション: 他の Now Platform インスタンスで 脆弱性アサインの推奨 アプリケーションのエンタイトルメントを管理する場合は、[エンタイトルメントの管理 **(Manage Entitlement)]** をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

(Optional) [エンタイトルメントの管理 **(Manage Entitlement)]** ボタンが表示されていない場合は、製品リストの 脆弱性アサインの推奨 アプリケーションをクリックして表示します。

a. オプションを選択します。

b. [OK] または [キャンセル] をクリックして続行します。
プラグインをアクティブ化して Now Platform インスタンスにアプリケーションをインストールする準備ができました。

9. 脆弱性アサインの推奨 アプリケーションをインストールする Now Platform インスタンスにログインします

10. 次のように移動する。 **All** (すべて) > システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて).

11. リストされたアプリケーションから、脆弱性アサインの推奨 アプリケーション (sn_vul_recom) を見つけて、[インストール] をクリックします。
アプリケーションのインストールダイアログボックスが表示され、インストールされている依存関係が表示されます。

12. オプション: デモデータが必要な場合、[デモデータのロード] チェックボックスをオンにして、[インストール] をクリックします。

注:
[デモデータのロード] チェックボックスをオンにしないと、後でアプリケーションマネージャーからデモデータをインストールできません。初期インストール後にデモデータをインストールまたは再インストールする方法については、Now Support ナレッジベースで「アプリケーションが既にインストールされている場合にデモデータをインストールする方法 [KB0722909] 」記事を参照してください。

このインストールには時間がかかる場合があります。アプリケーションとその依存関係が正常にインストールされると、インストールダイアログボックスにメッセージが表示されます。

13. [クローズ] をクリックします。

14. 脆弱性アサインの推奨 を設定するには、「脆弱性対応 の脆弱性アサインの推奨の構成」を参照してください。

脆弱性対応 の脆弱性アサインの推奨の構成

脆弱性アサインの推奨 を有効にして、アサインが解除されたか間違ってアサインされた、脆弱性の検出結果の所有者を特定するために費やす時間を短縮します。

始める前に
必要なロール：sn_vul.manage_assignment_recom_config

このタスクについて
このアプリケーションはデフォルトで有効になっていません。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > アサインの推奨.

2. [アサインの推奨の有効化/無効化] を選択します。
[予測インテリジェンスソリューション定義] フィールドが表示されます。デフォルト値は [脆弱性一致アイテムのアサイン **(Vulnerable Item Assignment)]** です。

3. [保存] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性対応 のソリューション定義の作成とトレーニング

予測インテリジェンス を使用して、脆弱性対応 のソリューション定義モデルを作成してトレーニングします。このモデルを使用して、既存のデータに基づいて脆弱性一致アイテム (VI) または修復タスク (RT) のアサイン先グループを予測できます。

始める前に
必要なロール：sn_vul.vulnerability_admin

手順

1. 次のように移動する。 **All** (すべて) > 予測インテリジェンス > 分類 > ソリューション定義.
2. [分類定義] フォームで、[脆弱性一致アイテムのアサイン **(Vulnerable Item Assignment)]** をクリックします。
   これはデフォルトのソリューション定義です。

   注:
   - デフォルトのトレーニング頻度は 30 日です。つまり、構成されたフィルター条件に一致する VI データセットを使用して、30 日ごとにモデルが自動的に再トレーニングされるということです。
   - 脆弱性一致アイテムテーブルのフィールドをトレーニングに使用できます。デフォルトのソリューション定義では、**Vulnerability.Summary** と **Configuration item.Name** の 2 つの VI フィールドでトレーニングします。組織内の脆弱性の所有権を予測するために役立つフィールドに応じて、トレーニングに使用するフィールドをカスタマイズできます。

3. 分類ソリューションを作成およびトレーニングするには、「分類ソリューションの作成とトレーニング」を参照してください。

   注:
   類似性またはクラスタリングソリューションを作成してトレーニングすることもできます。詳細については、以下を参照してください。
   - 類似性ソリューションを作成してトレーニングします。
   - クラスタリングソリューションを作成してトレーニングする

4. [更新 **&** 再トレーニング] をクリックします。

   注:
   ML ソリューションの詳細設定を構成するには、「ML ソリューションの詳細設定」を参照してください。

脆弱性対応 算出の作成

脆弱性算出は、特定の基準が満たされたときにターゲットフィールドを計算するために事前定義された式です。脆弱性一致アイテムの [リスクスコア] を計算する算出には、リスクルールを含めることができます。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
スクリプトを含む脆弱性算出を実行すると、パフォーマンスの低下を感じることがあります。

最も単純なルールが最初に実行されるようにルールを並べ替え、条件とテンプレート値またはリスクルールで処理できないアイテムに対してのみ、スクリプトを実行します。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性 > アドミニストレーション > 脆弱性の算出.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

脆弱性算出フォーム

フィールド	説明
名前	脆弱性算出の名前。
テーブル	脆弱性一致アイテムテーブルの名前が自動的に入力されます。
アプリケーション	脆弱性対応 が自動入力されます。
ターゲットフィールド	計算するためのフィールド。
説明	算出のテキスト説明。
有効	算出をオンまたはオフにします。

4. ヘッダーを右クリックして、[保存] を選択します。
[脆弱性算出ルール] セクションが表示されます。
5. [新規] をクリックして、算出ルールを作成します。

注:
[新しいリスクルール] フォーム ([ターゲットフィールド] が [リスクスコア] の場合にのみ使用可能) については、ステップ 10 を参照してください。

6. 必要に応じてフィールドに入力します。

[脆弱性算出ルール] フォーム

フィールド	説明
名前	算出ルールの名前。
順序	脆弱性算出を実行する順序。順序エントリーが 100 の算出は、順序エントリーが 200 の算出の前に実行されます。
算出	算出の親が自動入力されます。
有効	デフォルトでは、[アクティブ] チェックボックスがオンになっています。これは、算出ルールがアクティブであることを意味します。このチェックボックスをオフにすると、システムに作成された新しい脆弱性一致アイテムにこのルールは適用されません。
詳細表示	選択すると、[条件タイプ] と [値タイプ] から、スクリプト化された条件とスクリプト値を選択できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. 必要に応じて、[この条件を満たしている場合] タブのフィールドに入力します。

[この条件を満たしている場合] タブ

フィールド	説明
名前	算出ルールの名前。
順序	脆弱性算出を実行する順序。順序エントリーが 100 の算出は、順序エントリーが 200 の算出の前に実行されます。
算出	算出の親が自動入力されます。
有効	デフォルトでは、[アクティブ] チェックボックスがオンになっています。これは、算出ルールがアクティブであることを意味します。このチェックボックスをオフにすると、システムに作成された脆弱性一致アイテムにこのルールは適用されません。
詳細表示	選択したら、[条件タイプ] と [値タイプ] から、スクリプト化された条件とスクリプト値を選択します。
条件タイプ	[詳細ビュー **(Advanced view)**] を選択すると使用できます。次の選択肢があります。 ○ フィルター：フィルター条件を使用します。 ○ フィルターグループ：新しいフィルターグループの作成の説明を参照して、算出基準を定義します。 ○ スクリプト：この算出を適用するタイミングを決定するために使用されるスクリプト条件。 **注:** 算出を適用するタイミングを決定するスクリプトを作成する前に、[脆弱性算出 **(Vulnerability Calculators)**] リストに戻ります。ベースシステムに付属している脆弱性算出レコードを確認します。
条件	算出を使用するかどうかを決めるための基本的なフィルター条件を定義します。 [フィルターグループ] または [スクリプト] の条件タイプのいずれかを選択すると、このフィールドは非表示になります。 条件ビルダーに入力した検索テキストの大文字と小文字の区別は、このレコードまたはフォームではサポートされていません。

8. [これらの値を設定 **(Set these values)**] タブをクリックし、必要に応じて、フォームのフィールドに入力します。

[これらのフィールドを設定 **(Set these fields tab)**] タブ

フィールド	説明
値のタイプ	[詳細ビュー **(Advanced view)**] を選択すると使用できます。次の選択肢があります。 ○ テンプレート：各フィールドに設定する値を定義します。 ○ スクリプト：各フィールドの値を設定するために使用します。
スクリプト値	[スクリプト] の値タイプを選択した場合に使用できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	計算を適用する値を定義します。
テンプレート	算出に使用するフィールドと値を選択します。 [スクリプト] 値タイプのいずれかを選択すると、このフィールドは非表示になります。

9. すべての入力が完了したら、[送信] をクリックします。

> **注:**
> 既存の算出を編集し、既存のすべてのスコアを更新する場合は、 [算出を再適用] ボタンを使用できます。有効な脆弱性一致アイテム (VI) をすべて実行し、その算出を使用して値を設定する場合は、それらの VI の値を再計算します。算出の再適用には時間がかかるため、スケジュール済みジョブで処理されます。

10. 必要に応じて、[新しいリスクルール] フォームのフィールドに入力します。

その値から取得されるべき結果の割合に従って、各重み付けを設定します。スキャナーで提供されないデータ、またはリスクスコアに含めるべきでないデータについては、重み付けをゼロに設定します。

フィールドを追加、削除、または更新できます。フィールド値の重み付けパーセンテージを設定することもできます。詳細については、「脆弱性対応リスク算出のリスクルールのフィールドと重み付けの定義」を参照してください。

重み付けを更新すると、残りの重み付けと想定される [リスクスコア] の結果がシナリオに表示されます。

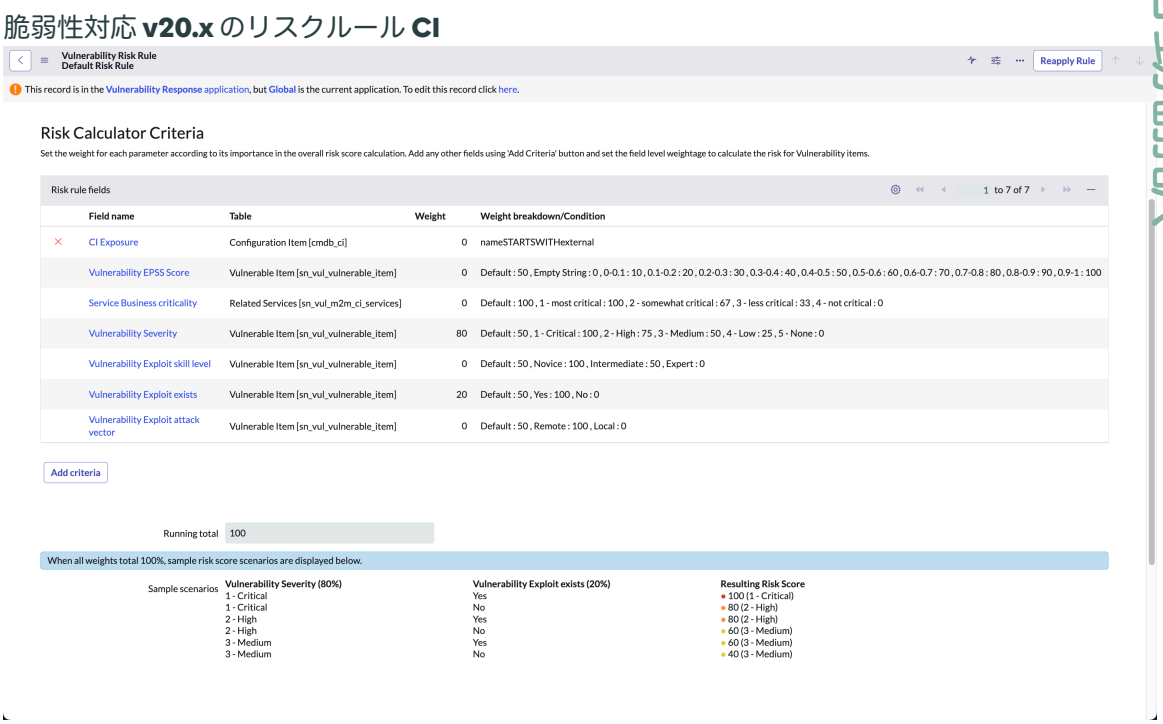
フィールド	説明
名前	算出ルールの名前。
順序	脆弱性算出を実行する順序。順序エントリーが 100 の算出は、順序エントリーが 200 の算出の前に実行されます。
算出	算出の親が自動入力されます。
有効	デフォルトでは、[アクティブ] チェックボックスがオンになっています。これは、算出ルールがアクティブであることを意味します。このチェックボックスをオフにすると、システムに作成された新しい脆弱性一致アイテムにこのルールは適用されません。
条件	算出を使用するかどうかを決めるための基本的なフィルター条件を定義します。 [フィルターグループ] または [スクリプト] の条件タイプのいずれかを選択すると、このフィールドは非表示になります。
重み付け	
脆弱性重大度	重大度に基づく結果の割合。
脆弱性 EPSS スコア	脆弱性が悪用される可能性。デフォルトでは、この条件の重み付けはゼロです。これをリスクスコアの計算に使用する場合は、この基準に対して適切な重み付けを設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
エクスプロイト有無	エクスプロイトの存在に起因する結果の割合。この情報が脆弱性に存在しない場合は、重み付けをゼロに設定します。
エクスプロイトスキルレベル	エクスプロイトに必要とされるスキルレベルに起因する結果の割合。この情報が脆弱性に存在しない場合は、重み付けをゼロに設定します。
エクスプロイト攻撃ベクトル	攻撃のターゲットに起因する結果の割合。この情報が脆弱性に存在しない場合は、重み付けをゼロに設定します。
ビジネスサービスの重要度	ビジネス上の重要度に起因する結果の割合。CI をビジネスサービスにリンクしていない場合は、重み付けを 0 に設定します。
CI エクスポージャー	CI がインターネットに接続されているかどうかに起因する結果の割合。重み付けがゼロ以外の場合、インターネットに接続する CI を定義する条件フィルターが表示されます。フィルターを設定して、インターネットに接続する構成アイテムを選択します。条件に一致するレコードをプレビューできます。
現在までの累計	自動計算された割合の合計。この値が 100 に達すると、シナリオのプレビューにさまざまなシナリオのサンプルリスクスコアが表示されます。
リスクスコアシナリオ	すべての重み付けの合計が 100% になると、リスクスコアのシナリオが表示され、考えられる一部のシナリオでリスクスコアのプレビューが示されます。

埋め込みリストを使用して、基準を追加または削除し、各基準の重み付けを調整できます。



11. [送信] をクリックします。

使用しないデフォルトの脆弱性算出の無効化

脆弱性算出を使用しない場合は、定義した他の脆弱性算出に加えて、デフォルトの算出を無効にします。脆弱性算出は、脆弱性一致アイテムレコードが作成または更新されるたびに実行され、初期インポートのパフォーマンスに影響を与える可能性があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 脆弱性の算出.
2. 関連する算出を開きます。
3. 算出を非アクティブ化するには、[アクティブ] チェックボックスをオフにします。
4. [更新] をクリックします。

脆弱性対応 自動削除ルールの作成、有効化、または変更

脆弱性一致アイテム (VI) および修復タスク (RT) の削除ルールを作成、有効化、または変更することができます。自動削除を使用して、VI および RT テーブルから古いレコードを削除します。

始める前に
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

必要なロール：

- admin：自動削除ルールの変更
- sn_vul.vulnerability_admin または sn_vul.admin (非推奨)：自動削除モジュールの表示

このタスクについて
時間の経過により、大量のクローズ済みレコードがインスタンスの VI テーブルや VUL テーブルに蓄積されることがあります。これらのレコードの多くは、クローズされて 365 日以上経過している可能性がありますが、削除されていません。これらの古いクローズ済みレコードの多くを削除するために、自動削除ルールを使用します。これらのレコードを削除すると、VI テーブルや VUL テーブルのレコード数が大幅に減少するだけでなく、高いパフォーマンスの維持にも役立ちます。

自動削除はデフォルトではクローズされて 365 日が経過しているレコードを対象としますが、最初の実行では単一のトランザクションで非常に多くのレコードが消去される可能性があります。環境の規模に応じて、削除プロセスを調整してクエリの範囲を制限することをお勧めします。たとえば、最初の実行は 450 日以上経過したクローズ済みレコードに対して開始できます。その実行の完了後に、日数を徐々に少なくしながら (425、400、375)、365 日以上経過した古いレコードの数を減らすことができます。

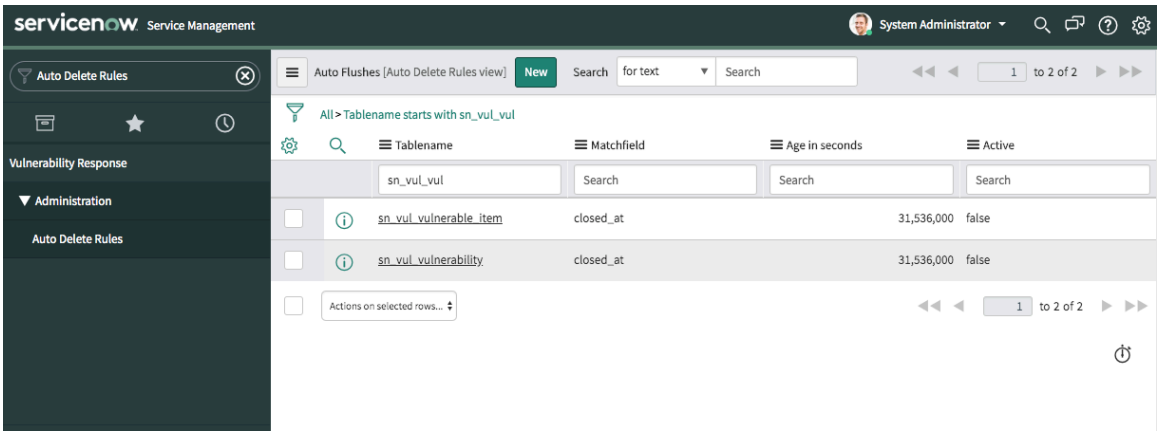
Now Platform® には、指定された条件を満たすクローズ済みレコードと、それらを参照するレコードを自動的に削除する、2 つのルールが付属しています。一方のルールは脆弱性一致アイテムを削除し、もう一方のルールは修復タスクを削除します。デフォルトでは、これらの自動削除ルールは無効になっているため、レコードを削除する前に手動でアクティブ化する必要があります。インスタンスに用意されている 2 つの事前設定ルールを選択するか、独自に作成することができます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > ルールの自動削除.
   リストビューが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



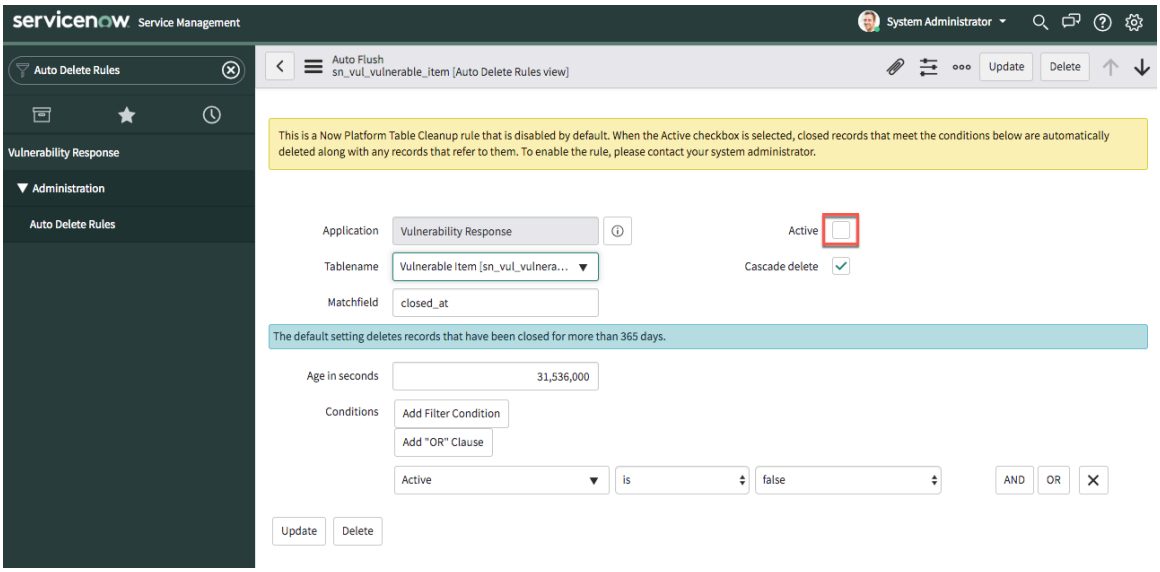
2. 編集するには、脆弱性一致アイテムの削除ルール (sn_vul_vulnerable_item) または修復タスクの削除ルール (sn_vul_vulnerability) を選択します。
3. 新しいルールを作成するには、[新規] をクリックします。
4. 必要に応じて、フォームのフィールドに入力するか、フィールドの内容を編集します。

フィールド	説明
アプリケーション	レコードが削除されるアプリケーションの名前。デフォルト値は Vulnerability Response です。
テーブル名	ルールが適用されるテーブルの名前。
一致フィールド	システムが期間を監視するフィールド。
有効	ルールをアクティブ化するためのオプション。アクティブ化すると、レコードを削除できます。
カスケード削除	一致するすべてのレコードと、それを参照するすべてのレコードを削除するオプション。このオプションが選択されていない場合、一致するレコードのみが削除されますが、それを参照するレコードは削除されません。
経過時間 (秒)	削除する脆弱性レコードの経過時間。VI ルールと RT ルールのどちらも経過時間は 365 日です。この経過時間は秒単位で表示されます。
条件	ルールが適用される VI テーブルや RT (VUL) テーブルのレコードを定義するフィルター条件。

5. ルールをアクティブ化するには、[アクティブ] チェックボックスをオンにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



ルールがアクティブ化されると、1 時間ごとのプラットフォーム機能である自動フラッシュによって、ルールがアクティブ化されているテーブルからレコードが削除されます。

削除基準に一致するレコードが数百万、数千万とある場合は、段階的なプロセスでレコードを削除できるように、自動削除ルールを有効にする前にServiceNow カスタマーサポートに問い合わせることをお勧めします。

脆弱性対応ホームページに脆弱性重要度チャートを追加する

概要には、脆弱性重要度を定義するチャートやその他の可視化を追加できます。

始める前に

- 脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。
- 脆弱性アナリティクスプラグインをアクティブ化する必要があります。

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 概要.
   一部のレポートは、デフォルトでダッシュボードに追加されています。これらのレポートの詳細については、「デフォルトの 脆弱性対応 ダッシュボードを使用する」を参照してください。
2. ダッシュボードヘッダーの近くで、カードビューアイコン + [コンテンツを追加] をクリックして、ウィジェットを追加するダイアログボックスを開きます。
3. [ウィジェットを追加] ダイアログボックスのリストから、[レポート] を選択してその他の 脆弱性対応 レポートを表示します。
4. ゲージに追加する画面上の場所をクリックします。
5. [コンテンツを追加] ボックスを閉じます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 メール通知を定義する

メール通知を設定して、誤検出要求の承認や却下など、重要な更新やアクティビティに関する有用な情報を共有します。メール通知を作成するときに、送信時期、受信者、内容を指定できます。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > メールテンプレート.
2. **[New** (新規)] を選択します。

   メール通知を作成する手順について、詳細は「Create an email notification」を参照してください。

タスクの結果
受信者がメール通知のリンクをクリックすると、ロールに基づいてリンクが Vulnerability Manager ワークスペース または IT 修復ワークスペース で開きます。

- ユーザーのロールが sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin の場合、Vulnerability Manager ワークスペース でリンクが開きます。
- ユーザーのロールが sn_vul.remediation_owner の場合、IT 修復ワークスペースでリンクが開きます。

受信者に前述のいずれのロールもない場合は、メール通知のリンクがクラシック UI で開きます。

脆弱性対応 のメールテンプレートを削除

メール通知を作成するときに、送信時期、受信者、内容を指定できます。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性 > アドミニストレーション > メールテンプレート.
2. **[New** (新規)] を選択します。

   メールテンプレートを作成するための詳細な手順については、「Construct an email message with a template」を参照してください。

修復ターゲット通知の作成または編集

脆弱性アドミニストレーターは、修復ターゲット通知を編集するか、新しい通知を追加して、通知の送信タイミング、通知の受信者、通知の内容を指定できます。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 通知.
2. 修復ターゲットの通知レコードを選択するか、[新規] を選択します。
3. 必要に応じて、フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フォームフィールドの詳細については、「Create an email notification」を参照してください。

4. [通知をプレビュー] を選択してメッセージを表示します。

タスクの結果

脆弱性対応 の v21.0 以降の場合、受信者がメール通知のリンクをクリックすると、そのロールに応じてレコードは Vulnerability Manager ワークスペース または IT 修復ワークスペース で開きます。

- ユーザーのロールが sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin の場合、Vulnerability Manager ワークスペース でリンクが開きます。
- ユーザーのロールが sn_vul.remediation_owner の場合、IT 修復ワークスペース でリンクが開きます。

受信者に前述のいずれのロールもない場合は、メール通知のリンクがクラシック UI で開きます。

脆弱性エクスポージャーアセスメントの構成

脆弱性エクスポージャーアセスメントアプリケーションを使用して、脆弱なソフトウェアに対する資産のゼロデイ (当日) エクスポージャーを評価します。

重要:
共通脆弱性識別子 (CVE) とソフトウェアによるエクスポージャーアセスメントを実行して、脆弱性アセスメントワークスペースの追加機能を活用できます。詳細については、「脆弱性アセスメントのワークスペースの詳細」を参照してください。

必要なロール：admin

互換性とシステム要件

脆弱性対応 アプリケーションは ServiceNow Store から入手可能です。ソフトウェア資産管理 (SAM) 基盤アプリケーション [com.snc.asset_management] が、脆弱性対応アプリケーションの一部としてインストールされます。SAM の基盤アプリケーションがインスタンスにインストールされていることを確認するには、 システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて) com.snc.asset_managementを検索します。アプリケーションがインストールされていない場合は、[インストール] を選択します。SAM の基盤の詳細については、「Software Asset Management Foundation plugin」を参照してください。

脆弱性エクスポージャーアセスメントアプリケーションは Now Platform® インスタンスの資産データにアクセスする必要があるため、資産管理アプリケーションには参照するデータが必要です。ソフトウェアディスカバリーモデルテーブル [cmdb_sam_sw_discovery_model] とソフトウェアインストール [cmdb_sam_sw_install] にはデータが必要です。

脆弱性エクスポージャーアセスメントアプリケーションは、SAM の基盤 または SAM Pro Now Platform® アプリケーションとも連携します。SAM Pro アプリケーションは ServiceNow Store のコア 脆弱性対応 製品には含まれておらず、別途サブスクリプションが必要です。

注:
SAM Pro アプリケーションは、より良い結果が得られるコンテンツライブラリにのみ必要です。

脆弱性対応 v23.0 以降、Pro または Enterprise サブスクリプションを利用している場合、[すべて **(All)**] メニューの [エクスポージャーアセスメント] リンクをクリックすると、ロールに応じてワークスペースの [エクスポージャーアセスメント] ページにリダイレクトされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ワークスペースの [エクスポージャーアセスメント] ページへのアクセス

ロール	ワークスペース
脆弱性マネージャー	脆弱性マネージャーのワークスペース
イベントマネージャー [sn_vul_analyst.vul_event_manager] または緊急対応 [sn_vul_analyst.emergency_response]	脆弱性アセスメントのワークスペース

ワークスペースにリダイレクトされて [クラシック版エクスポージャーアセスメント (Classic Exposure Assessment)] ページに留まるようにするには、[モジュール - エクスポージャーアセスメント (Module - Exposure Assessment)] ページの [リンクタイプ] タブで [リンクタイプ] を [レコードリスト] に設定します。[モジュール - エクスポージャーアセスメント (Module - Exposure Assessment)] ページにアクセスするには、[すべて] メニューの [エクスポージャーアセスメント **(Exposure Assessment)]** リンクの横にある [モジュールの編集] アイコンを選択します。

脆弱性書き込みロール [sn_vulnerability_write] を持っている場合、脆弱性対応 アプリケーションでインスタンス内の脆弱なソフトウェアのエクスポージャーアセスメントレコードをオンデマンドで作成および編集できます。

関連情報

脆弱なソフトウェアへのエクスポージャーの評価

脆弱性対応 の例外管理の設定

公開されている脆弱性管理やセキュリティポリシー、標準、指針に組織が準拠できない場合は、例外を要求できます。例外管理では、ポリシーに従って修復できない脆弱性一致アイテム (VI) または修復タスク (RT) に対する例外を要求、レビュー、承認、または却下します。

始める前に

脆弱性対応 モジュールを使用して、要求された例外の期間を制限し、例外要求または誤検出要求にアンケートを追加します。デフォルトでは、 ServiceNow 脆弱性対応 モジュールを使用して例外が要求されます。GRC: ポリシーとコンプライアンス管理 の統合を使用して例外を要求することもできます。

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

必要なロール：sn_vul.manage_exception_configuration

このタスクについて

脆弱性対応 が有効であれば、例外を要求できる期間を制限できます。同様に、GRC: ポリシーとコンプライアンス管理 モジュールがインストールされていれば、構成画面で GRC: ポリシーとコンプライアンス管理 を選択できます。このオプションを有効にすると、GRC からポリシーおよびコントロール目標を指定する例外を要求できます。

アンケートを追加すると、例外要求または誤検出要求を出しているユーザーにアンケートが送信されます。デフォルトのアンケートを使用することも、要件に基づいて作成することも可能です。

アンケートは、例外が要求されている理由を例外承認者が理解する際に役立ちます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 例外管理.
2. [例外管理構成] フォームで、[例外の管理に使用] リストからオプションを選択して、例外を管理する方法を選択します。
   脆弱性対応 または GRC: ポリシーとコンプライアンス管理のいずれかを選択できます。GRC: ポリシーとコンプライアンス管理 を使用して例外を要求するには、GRC プラグインをアクティブ化する必要があります。構成を変更しても、既存のデータには影響しません。
3. 脆弱性対応 オプションを選択した場合は、次の情報を入力します。

VR 例外管理フォームの設定

フィールド	説明
期間	例外を要求できる期間。
単位	指定された期間の時間単位。
例外を要求するアンケートを有効化	上がっている例外要求にアンケートを追加するオプション。
例外を要求するアンケート	例外を要求するために自分が選択したアンケートを表示します。デフォルトでは、[例外のアンケート] が表示されます。 **注:** このフィールドは、[例外を要求するアンケートを有効化] チェックボックスがオンの場合にのみ表示されます。
補完コントロールのためのアンケート	リスク削減要求について修復オーナーが回答する必要があるアンケートを表示します。脆弱性対応の v20.0 以降では、リスク削減要求のアンケートを設定できるようになりました。デフォルトでは、[補完コントロールのためのアンケート] が選択されています。 **注:** このフィールドは、[例外を要求するアンケートを有効化] チェックボックスがオンの場合にのみ表示されます。
誤検出をマークするアンケートを有効化	上がっている誤検出要求にアンケートを追加するオプション。
誤検出をマークするアンケート	誤検出としてマークするために自分が選択したアンケートを表示します。デフォルトでは、誤検出要求のアンケートが表示されます。 **注:** このフィールドは、[誤検出をマークするアンケートを有効化] チェックボックスがオンの場合にのみ表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

既存のアンケートをカスタマイズして v20.0 にアップグレードした場合、このカスタマイズされたアンケートは、デフォルトの [補完コントロールのアンケート **(Compensating Control Questionnaire)]** の代わりにリスク削減要求に表示されます。

4. GRC: ポリシーとコンプライアンス管理 オプションを選択した場合は、次の情報を入力します。

VR 例外管理フォームの設定

フィールド	説明
誤検出をマークするアンケートを有効化	上がっている誤検出要求にアンケートを追加するオプション。
誤検出をマークするアンケート	誤検出としてマークするために自分が選択したアンケートを表示します。デフォルトでは、誤検出要求のアンケートが表示されます。

5. 例外と誤検出要求の条件に基づいてアンケートを構成するには：

   a. [VR アンケート構成] セクションで、[新規] を選択します。

   b. [アンケートの構成 - 新規レコード (Questionnaire Configuration - New Record)] フォームで、フィールドに入力し、[送信] を選択します。
   [アンケート構成] フォームのフィールドの詳細については、「[アンケート構成] フォームのフィールド」を参照してください。
   作成されたアンケートは、[VR 例外管理フォームの設定 (Settings for VR Exception Management)] フォームの [VR アンケート構成] セクションに表示されます。

   たとえば、重大な脆弱性一致アイテムの誤検出要求のアンケートを構成する場合は、[脆弱性一致アイテムの誤検出] 承認ルールを選択し、条件を [リスク評価が 1 - 重大 (Risk rating is 1 - Critical)] と指定し、[アンケート構成] フォームで目的のアンケートを選択します。

6. [保存] を選択します。

例外承認者の追加

例外を要求できるように、ユーザーを承認者グループに追加します。

始める前に

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

必要なロール：sn_vul.exception_approver

このタスクについて

脆弱性対応v14.0 までは、脆弱性一致アイテムまたは修復タスクの例外要求は、デフォルトの 2 レベルの承認フローを使用して承認されます。要求は、2 つのレベルの承認者によって承認される必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
脆弱性対応 v14.0 までは、第 1 レベルの承認者がいない場合は、例外を要求できません。ただし、脆弱性対応 v15.0 以降では、VR アプリケーションを初めて展開する場合は、例外管理のフローデザイナーがデフォルトで有効になります。既にワークフローを使用している場合は、フローデザイナーに更新できます。どちらの場合も、ワークフローに戻すことはできません。例外管理と誤検出の承認ルールを設定するには、「例外管理の承認ルールの構成」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > ユーザー管理 **(User Administration)** > グループ.
2. [名前] 列で「例外」を検索し、[例外承認者 **-** レベル **1]** をクリックします。

注:
脆弱性対応 の v12.8.1 以降では、システムプロパティ [sys_properties] テーブルのワークフローで、ベースシステムのシステムプロパティを使用して例外承認を行うことができます。このため、ワークフローで例外または誤検出要求が作成されると、この要求はシステムプロパティで定義されているグループ ID に承認のために送信されます。次のように移動する。 **All** (すべて) > システムプロパティ をクリックし、[*sn_vul.exception_approver_L1*]、[*sn_vul.exception_approver_L2*]、または [*sn_vul.false_positive_approver_group*] を選択して、プロパティ値を変更します。

3. [グループ例外承認者 - レベル 1 (Group Exception Approver - Level 1)] フォームで、[グループメンバー] 関連リストをクリックします。
4. [新規] をクリックして、リストを作成します。
5. フォームのフィールドに入力します。

ユーザーフォーム

フィールド	説明
ユーザー ID	ユーザーの一意の識別子。
名	ユーザーの名。
姓	ユーザーの姓。
タイトル	ユーザーの役職。タイトルまたはジョブの説明を入力するか、リストから選択します。
部門	ユーザーの部門。
パスワード	ユーザーにアサインされたパスワード。このパスワードは、永続的または一時的なものにすることができます。
パスワードのリセットを強制	セキュリティを確保するためにユーザーがパスワードをリセットできるようにするオプション。
ロックアウト	ユーザーをインスタンスからロックアウトし、ユーザーのすべてのアクティブなセッションを終了するオプション。admin ロールを持つユーザーはロックアウトできません。
有効	このユーザーをアクティブにするオプション。次の領域では、自分だけが非アクティブなユーザーを見ることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ ユーザーのリスト ○ 参照フィールドの選択リスト (虫眼鏡アイコン) ○ 参照フィールドに入力すると表示されるオートコンプリートリスト
Web サービスへのアクセスのみ	このユーザーを非インタラクティブユーザーとして指定するオプション。
内部統合ユーザー	このユーザーを内部統合ユーザーとして指定するオプション。
メール	ユーザーのメールアドレス。
言語	ユーザーの優先言語。
カレンダー同期	ワークスケジュールの管理に使用されるカレンダー。たとえば、 Outlook です。
タイムゾーン	このユーザーがいる場所のタイムゾーン。
日付形式	ユーザーの優先日付形式。
電話 (勤務先)	ユーザーの勤務先電話。
携帯電話	ユーザーの携帯電話。
写真	[クリックして追加...] をクリックしてアップロードできる写真。

6. **[Submit]** をクリックします。
7. ステップ 1 ～ 5 を繰り返して、「例外承認者 - レベル 2」を作成します。
   承認者は、[脆弱性対応] > [自分の承認] に移動し、要求を承認する必要があります。

> **注:**
> GRC: ポリシーとコンプライアンス管理 の例外を承認するには、「ポリシーとコンプライアンス管理オプションのセットアップ」を参照してください。

例外管理の承認ルールの構成

脆弱性対応 v15.0 以降では、フローデザイナーを使用して、例外管理、例外ルール、および誤検出管理の例外要求を承認します。脆弱性対応 (VR) を初めて展開した場合、フローデザイナーはデフォルトで有効になっています。

始める前に
必要なロール：sn_vul.vulnerability_admin

このタスクについて
既存の VR ユーザーの場合、デフォルトのオプションはワークフローです。
脆弱性対応 v15.0 以降を展開した場合、システムプロパティ *sn_vul.flow_designer_activation* の値は true に設定されます。つまり、フローデザイナーはデフォルトで有効になっています。

v15.0 より前の 脆弱性対応 を既に使用している場合、このシステムプロパティの値は false に設定されます。値を true に変更すると、フローデザイナーをアクティブ化できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

> **注:**
> フローデザイナーをアクティブ化した後、 ワークフローの使用に戻すことはできません。ワークフローとフローデザイナーの詳細な比較については、「例外管理ワークフローとフローデザイナー」を参照してください。

フローデザイナーを使用するには、 承認ルールモジュールを使用してルールを作成します。このモジュールを使用すると、以下の各例外管理ワークフローの承認ルールを構成できます。

- 修復タスクの要求例外
- 脆弱性一致アイテムの例外要求
- 例外ルール
- 修復タスクの誤検出
- 脆弱性一致アイテムの誤検出

> **注:**
> ルール内に複数の承認レベルを含む条件を定義することもできます。フローデザイナーは、このモジュールで作成されたルールを自動的に継承し、一致する承認ワークフローを処理します。承認レベルの構成の詳細については、「例外管理の承認レベルの作成」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 承認ルール.
2. [承認ルール] ページで、承認ルールを設定するグループを選択します。
3. フォームのフィールドに入力します。

承認ルールフォーム

フィールド	説明
名前	承認構成名。
テーブル	ルールが適用されるテーブル。
アプリケーション	デフォルト値は脆弱性対応です。
ルールタイプ	ルールタイプを指定します。たとえば、例外管理、誤検出、例外ルールなどです。
有効	デフォルトで有効になっており、承認ルールが使用中であることを示します。
説明	承認ルールの簡単な説明。
承認の有効期限 (日数) 脆弱性対応 の v21.0 以降	承認者が要求を承認できる期限。
承認者に通知 (日数) 脆弱性対応 の v21.0 以降	承認者にアクションを実行するよう通知される日付。

4. [更新] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[承認構成] タブには、デフォルトで 2 つのレベルの承認者が設定されています。ルールを選択して、ルール内のさまざまなユースケースに基づいて条件を定義できます。詳細については、「承認ルールの構成の作成」を参照してください。

> **注:**
> 各構成ページで、複数の承認レベルを作成できます。詳細については、「例外管理の承認レベルの作成」を参照してください。

Example:
さまざまなユースケースに基づいて、異なる構成アイテムで見つかった同じ脆弱性に対して、異なる承認プロセスを定義できます。

承認ルールの構成の作成

一致する脆弱性一致アイテム、修復タスク、または承認レベルの例外ルールを除外するための条件を定義します。

始める前に
必要なロール：sn_vul.vulnerability_admin

このタスクについて
承認構成モジュールでは、さまざまな構成に対して複数のレベルの承認を構成できます。条件ベースのルールを定義します。各ルールには複数の承認レベルが含まれています。

> **注:**
> 承認ルールモジュールを使用して、例外管理ワークフローの承認ルールを構成します。承認ルールの構成の詳細については、「例外管理の承認ルールの構成」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 承認ルール.
2. 承認ルールを選択し、[承認構成] タブに移動します。
3. 構成を選択します。
4. フォームのフィールドに入力します。

[承認構成] フォーム

フィールド	説明
名前	承認構成名。
承認ルール	承認ルールのテーブルとタイプの詳細が含まれています。
順序	ルール内のさまざまな構成の実行順序。たとえば、順序エントリーが 100 の構成は、順序エントリーが 200 の構成よりも前に実行されます。
有効	デフォルトで有効になっており、承認構成が使用中であることを示します。
説明	承認構成レベルの簡単な説明。

5. 次のいずれかの方法で、脆弱性一致アイテムまたは修復タスクの条件を設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
条件	一致する脆弱性一致アイテムまたは修復タスクを識別します。
詳細条件	脆弱性一致アイテムまたは修復タスクの条件を定義するスクリプト。 **注:** このフィールドは、[詳細] チェックボックスをオンにした場合に表示されます。

6. [更新] を選択します。
ルール内に複数の承認レベルを含む条件を定義できます。フローデザイナーは、このモジュールで作成されたルールを自動的に継承し、一致する承認ワークフローを処理します。承認レベルの構成の詳細については、「例外管理の承認レベルの作成」を参照してください。

Example:
以下に対してさまざまな承認パスを定義できます。

- 例 1：さまざまなタイプの脆弱性または構成アイテム (インターネット向けまたは内部向け)。
- 例 2：修復オーナーがホスト脆弱性一致アイテム (VIT) または修復タスク (VUL) に対してこれらの要求を同時に発生させた場合の保留要求とリスク低減要求。

  [変更承認] 列には、保留ステータスの変更承認レコードが保持されます。条件ビルダーを使用して [変更承認] 列に条件を設定すると、保留承認レコードは考慮されますが、リスク低減承認レコードは考慮されません。したがって、リスク削減ステータスの変更承認レコードに条件を設定するには、[詳細条件] フィールドを使用します。

  [脆弱性一致アイテムの例外要求] 承認ルールの場合、[中から低のリスク評価の要求 **(Request for risk rating from Medium to Low)]** 承認構成がベースシステムに付属しています。この構成はデフォルトで False に設定されています。この構成を使用して、リスク削減要求の承認パスを [中] から [低] に設定できます。リスク削減要求のさまざまなリスク評価の変更に適用できるように、この構成でスクリプトを更新することもできます。

  [中から低のリスク評価の要求 (Request for risk rating from Medium to Low)] 構成：

```
function evaluate() {
    var gr = new GlideRecord("sn_vul_change_approval");
    gr.addQuery("sys_id", approval);
    gr.addQuery("current_value", "3 - Medium");
    gr.addQuery("desired_value", "4 - Low");
    gr.query();
    if (gr.next()) {
        return true;
    }
    return false;
}
evaluate();
```

  上記の構成を最小順序で True に設定し、[デフォルト構成 **- VI** の例外要求 **(Default configuration - Exception request for VI)]** 構成を True に設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

結果：修復オーナーが IT 修復ワークスペースから保留要求とリスク削減要求を同時に発生させると、保留承認要求は [デフォルト構成 **- VI** の例外要求 **(Default configuration - Exception request for VI)]** で定義された承認者にリダイレクトされ、リスク削減承認要求は [中から低のリスク評価の要求 **(Request for risk rating from Medium to Low)]** 構成で定義された承認者にリダイレクトされます。

例外管理の承認レベルの作成

例外要求を承認するユーザーとユーザーグループのレベルを定義します。

始める前に
必要なロール：sn_vul.vulnerability_admin

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 承認ルール.
2. 承認ルールを選択し、[承認構成] タブに移動します。
3. 構成を選択します。
4. [承認者レベル] セクションで、承認者レベルを選択します。
5. フォームのフィールドに入力します。

[承認者レベル] フォーム

フィールド	説明
名前	承認レベル名。
承認が必要	選択したレベルに必要な承認数を選択します。 ○ 1 人の承認者が必要 ○ すべてのユーザーの承認が必要
有効	デフォルトで有効になっており、承認レベルが使用中であることを示します。
順序	ルール内のさまざまな構成の実行順序。たとえば、順序エントリーが 100 の構成は、順序エントリーが 200 の構成よりも前に実行されます。
承認ルール	承認ルールのテーブルとタイプの詳細が含まれています。
承認構成	承認構成が含まれています。
次を使用してアサイン	以下のいずれかのオプションを選択します。 ○ ユーザーおよびユーザーグループ ○ 承認テーブルフィールド ○ スクリプト
グループ	複数のユーザーで構成される承認者レベルグループ。ユーザーには、次のいずれかのロールが必要です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ sn_vul.exception_approver：例外管理および例外ルール用 ○ sn_vul.false_positive_approver：誤検出用
ユーザー	グループにリストされているユーザーを編集します。

6. 変更を保存するには、[更新] を選択します。

注:
v15.0 より前では、例外レベル 1 にのみユーザーがいる場合、ワークフロープロセスは機能します。ただし、v15.0 以降は、各レベルに少なくとも 1 人のユーザーが必要です。

v15.0 より前では、ワークフローで第 2 レベルにユーザーが存在しない場合、脆弱性一致アイテムまたは脆弱性グループは保留されていました。しかし、v15.0 以降では、第 2 レベルにユーザーが存在しない場合、承認要求は自動的に却下されます。

Example:
Linux サーバーと Windows サーバーには、脆弱性のさまざまな承認レベルが存在する場合があります。

例外管理ワークフローとフローデザイナー

脆弱性対応 v15.0 以降では、脆弱性対応 (VR) を初めて展開する場合は、例外管理で例外要求を承認するためのフローデザイナーがデフォルトで有効になります。既存の VR ユーザーの場合、デフォルトのオプションはワークフローです。

注:
脆弱性対応 v19.0 以降、新しい顧客に対してフローデザイナーのみがサポートされています。既存のユーザーが脆弱性対応 v19.0 にアップグレードすると、フローデザイナーと例外管理ワークフローの両方がサポートされます。

ワークフローとフローデザイナー

考慮事項	Workflow	フローデザイナー
バージョン	脆弱性対応 の v15.0 より前。	脆弱性対応 の v15.0 以降。
デフォルトオプション	既存の VR ユーザーのデフォルトのオプション。	v15.0 以降の新しい VR ユーザーのデフォルトのオプションです。
承認プロセスの設定	例外管理には、例外ルールとともに例外と誤検出の要求が含まれます。	さまざまなユースケースに対する各種のレベルの定義、各種の承認者の追加などがあります。ワークフローより簡単に実装できます。例外管理には、例外ルールとともに例外と誤検出の要求が含まれます。
フローデザイナーへのアップグレード	ワークフローからフローデザイナーにアップグレードできます。ただし、既存の要求は、ワークフローを使用してのみ承認できます。	フローデザイナーはデフォルトで有効になっています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ワークフローとフローデザイナー (続く)

考慮事項	Workflow	フローデザイナー
システムプロパティ *sn_vul.flow_designer_action*	v15.0 より前の例外管理にワークフローを使用している場合、システムプロパティは false に設定されます。フローデザイナーをアクティブ化するには、このプロパティを true に設定します。 **注:** フローデザイナーをアクティブ化した後、 ワークフローの使用に戻すことはできません。	v15.0 以降で VR を初めて使用する場合、システムプロパティ値はデフォルトで true に設定されています。
承認ルールモジュール	システムプロパティを true に設定すると、「承認ルールモジュールを有効化」スケジュール済みジョブが 24 時間以内に実行されます。このスケジュール済みジョブにより、承認ルールモジュールが有効になります。このモジュールをすぐにアクティブ化するには、このジョブを手動で実行します。	VR v15.0 以降、初めて VR を展開した場合、このモジュールはデフォルトで利用可能です。
承認レベル	2 つのレベルの承認者のみを設定するオプションを提供します。	任意の数の構成、承認者レベルの設定、各ルールの承認者の動的な追加など、複数のオプションを提供します。

誤検出承認者の追加

誤検出承認者グループに追加されたユーザーのみが、脆弱性一致アイテム (VI) および修復タスク (VUL) の誤検出を承認できます。誤検出の許可は単一レベルの承認プロセスです。

始める前に

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

注:

脆弱性対応 v15.0 以降では、VR アプリケーションを初めて展開する場合は、例外管理のフローデザイナーがデフォルトで有効になります。既にワークフローを使用している場合は、フローデザイナーに更新できます。どちらの場合も、ワークフローに戻すことはできません。例外管理と誤検出の承認ルールを設定するには、「例外管理の承認ルールの構成」を参照してください。

必要なロール：sn_vul.vulnerability_admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > > ユーザー管理 **(User Administration)** > グループ.
2. [名前] 列で、[誤検出] を検索し、オプションをクリックします。
3. [グループ] フォームで、[グループメンバー] > [新規] (または [編集]) に移動します。
4. [ユーザー] フォームで、ユーザーの詳細を入力してレコードを作成し、[送信] をクリックします。すべてのロールがユーザーに付与されます。選択したユーザーが [グループメンバー] リストに追加されます。こうしたメンバーは、VI または修復タスクを誤検出としてマークする要求を承認できます。承認されると、レコードのステータスが [クローズ済み] に更新され、指定された日付にのみ再オープンされます。

リスク削減のアンケートを構成する

脆弱性対応 v20.0 以降では、一連のフィルタリングされた脆弱性一致アイテムまたは修復タスクのリスク削減要求のアンケートをカスタマイズできます。

始める前に
必要なロール：admin

このタスクについて
[脆弱性一致アイテムの補完コントロール用アンケート **(Questionnaire for compensating controls for vulnerable items)]** および [脆弱性グループの補完コントロール用アンケート **(Questionnaire for compensating controls for vulnerable group)]** 承認ルールがベースシステムに付属しています。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 例外管理.
2. [VR 例外管理の設定 (Settings for VR Exception Management)] フォームで、[例外を要求するアンケートを有効化] チェックボックスをオンにします。
3. リスク削減要求の条件に基づいてアンケートを構成するには：
   a. [VR アンケート構成] セクションで、[新規] を選択します。
   b. [アンケート構成 - 新規レコード (Questionnaire Configuration - New Record)] フォームで、[脆弱性グループの補完コントロール用アンケート **(Questionnaire for compensating controls for vulnerable group)]** または [脆弱性一致アイテムの補完コントロール用アンケート **(Questionnaire for compensating controls for vulnerable items)]** 承認ルールを選択して、条件を指定します。
   c. 目的のアンケートを選択し、[送信] を選択します。
   [アンケート構成] フォームのフィールドの詳細については、「[アンケート構成] フォームのフィールド」を参照してください。
   作成されたアンケートは、[VR 例外管理フォームの設定 (Settings for VR Exception Management)] フォームの [VR アンケート構成] セクションに表示されます。
4. [VR 例外管理の設定 (Settings for VR Exception Management)] で [保存] を選択します。

修復タスクの脆弱性対応 **SLA** の表示

脆弱性一致アイテムが正しく処理されるようにするために、脆弱性対応 修復タスクのサービスレベルアグリーメント (SLA) を定義できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

このタスクについて
このリストの SLA 定義は、脆弱性対応に固有のプラットフォーム SLA リストのサブセットです。

詳細な手順については、「Create an SLA definition」を参照してください。

VI の修復にかかる時間を追跡する場合は、脆弱性対応 の修復ターゲットルール の使用を優先できます。修復ターゲットルールは、脆弱性対応のコンテキスト内で指定した脆弱性一致アイテム (VI) を修復するための予定期間を定義します。一方、SLA は脆弱性そのものの修復期間を指定している場合があります。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > **SLA** 定義.
2. 定義をクリックします。
   タスク **SLA** は、修復タスクの関連リストに表示されます。

WatchDog の構成

WatchDog 構成ページを使用して新しい WatchDog を作成するか、または指定の条件で既存の WatchDog を更新します。各 WatchDog の通知を有効にし、条件が満たされたときに通知を受け取ることができます。

始める前に
必要なロール：sn_sec_cmn.admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > **WatchDog** > 構成.
2. 実装する WatchDog を選択します。
3. フォームのフィールドに入力します。

WatchDog 統合フォーム

フィールド	説明
名前	WatchDog の名前。
有効	チェックボックスを *true* に設定すると、WatchDog が有効になります。
条件タイプ	[フィルター] または [スクリプト] から選択します。
詳細条件	このフィールドは、[条件タイプ] で [スクリプト] が選択されている場合にのみ表示されます。
テーブル	WatchDog 条件を実行するテーブルを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
条件	WatchDog を評価する条件。
通知	WatchDog 条件が満たされた場合にグループまたはユーザーに通知することを選択するためのチェックボックス。
ユーザー	WatchDog 条件が満たされた場合に通知を受け取るユーザーのリスト。
グループ	WatchDog 条件が満たされた場合に通知を受け取るグループ。
ウォッチログ	
WatchDog	WatchDog テーブルへの参照。
カウント	WatchDog 基準を満たすレコードの数。
メモ	WatchDog ログの追加メモ。

4. [更新] を選択します。

脆弱性対応 の高度な構成タスク

以下のセットアップタスクは、コーディングまたは ServiceNow の高度な専門知識が必要であり、基本構成の一部とは見なされていません。

高度なコーディング経験がある場合、または Now Platform の専門知識がある場合にのみ、これらのタスクを実行することをお勧めします。

統合のためのドメインセパレーションインポートの作成

インポートされたデータを特定のドメインに配置する必要がある場合は、統合を実行するようにアサインされたユーザーがそのドメインに属している必要があります。

始める前に

必要なロール：
import_admin および特定の統合用の統合の構成ロール (sn_vul.configure_r7_integration や sn_vul_tenable.configure_integration など)。

このタスクについて

この一連のタスクには、コーディングまたは高度な ServiceNow の専門知識が必要です。

インポートキューには、スケジュール済みジョブ (統合) が処理するデータ添付ファイルが含まれています。ドメインセパレーションされた環境では、スケジュール済みジョブを正しいインポートキューと一致させる必要があります。

手順

1. ドメインを作成します。
2. 作成するドメインごとに、ユーザーを作成してそのドメインにアサインします。

   このユーザーは、脆弱性統合におけるドメインの **run_as** プレースホルダーと考えてください。グローバルドメイン内の **VR.System** ユーザーに相当します。このユーザーには、データソース、変換マップおよび脆弱性データへのアクセスが必要です。

   注:
   このユーザーを他の目的に使用しないでください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

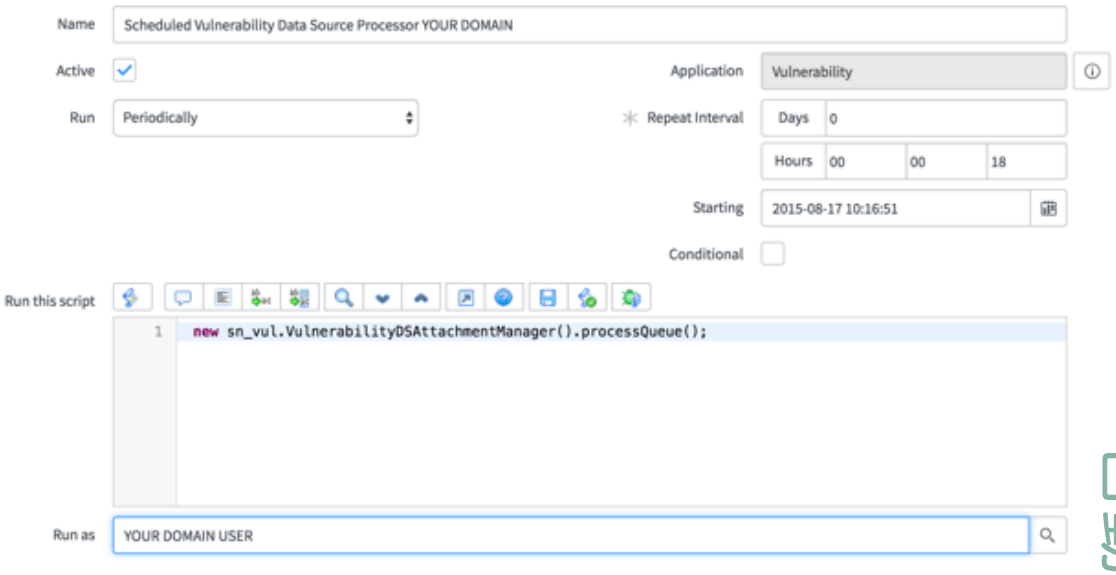
自動翻訳

3. 各ドメインで、スケジュール済みジョブを作成します。
その他の注意事項と設定の詳細については、「ドメインセパレーションの追加の設定」を参照してください。

   a. 次のように移動する。 **All** (すべて) > システム定義 > スケジュール済みジョブ.

   b. スケジュール設定済みの脆弱性データソースプロセッサーをドメインにコピーします。

   c. スケジュール済みジョブを識別するには、名前にドメインを追加します。



   d. [実行方法] フィールドで、**run_as** ユーザーをステップ 2 で作成したユーザーに変更します。

   脆弱性対応の v20.1 以降、次のスクリプトの変更がベースシステムに付属しています。

4. 注:
次の UI アクションを編集して、統合が **run_as** ユーザードメインで実行されるようにします。

   [Qualys ホスト検出統合 **(Qualys Host Detection Integration)]** 統合ジョブの [今すぐ実行] UI アクションを編集して、このコードブロックをファイルの先頭に追加します。

   Example

```
//sys id below is of host detection integration
if(current.sys_id == "5d9cf0daff540300c68c9f783894fa4d"){
current.run_as = gs.getUserID
();
}
```

5. 注:
次のスクリプトインクルードを編集して、統合が **run_as** ユーザードメインで実行されるようにします。

   VulnerabilityIntegrationUtils スクリプトインクルードのメソッド **addIntegrationRun** を編集して、ハイライト表示されたコードを追加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

6. **VulnerabilityIntegrationUtils** スクリプトインクルードのメソッド **addProcessRun** を編集して、以下の画像のハイライト表示されたコードを追加します。
   addProcessRun のコード

```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

7. **VulnerabilityIntegrationUtils** スクリプトインクルードのメソッド **copyProcess** を編集して、以下の画像のハイライト表示されたコードを追加します。
   copyProcess のコード

Script

```
_copyProcess: function(intProcGr, isProcessErrored) {
    var copy = new GlideRecord('sn_vul_integration_process');
    copy.initialize();
    copy.setValue('integration_run', intProcGr.getValue('integration_run'));
    copy.setValue('parameters', intProcGr.getValue('parameters'));
    copy.setValue('state', 'new');
    copy.setValue('notes', '');
    copy.setValue('sys_domain', intProcGr.getValue('sys_domain'));
    if (isProcessErrored) {
        copy.setValue('errored_retries', parseInt(intProcGr.getValue('errored_retries')) + 1);
        var nextRetryDueOn;
        if (intProcGr.getValue('next_retry_due_on') != '')
            nextRetryDueOn = new GlideDateTime(intProcGr.getValue('next_retry_due_on'));
        else
            nextRetryDueOn = new GlideDateTime();

        var intgInstance = new sn_vul.VulnerabilityIntegrationHelper().getIntScriptInstance(intProcGr);
        var nextRetryDelay = intgInstance.getNextRetry(intProcGr.errored_retries);
        nextRetryDueOn.addSeconds(nextRetryDelay * 60);
        if (parseInt(intProcGr.getValue('errored_retries')) + 1 < intgInstance.getMaxRetry())
            copy.setValue('next_retry_due_on', nextRetryDueOn.getValue());
    } else
        copy.setValue('retries', intProcGr.retries + 1);

    copy.insert();
    return copy;
},
```

8. **DataSourceVulnReportRefreshProcessor** スクリプトインクルードのメソッド **_processFromDataSourceGroups** を編集して、この元のコードを変更します。
   元の _processFromDataSourcesGroups のコード

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

```
23
24      _processFromDataSourceGroups: function(payload, fileName) {
25          var gr = new GlideRecord("sn_vul_int_data_src");
26          gr.addQuery("sn_vul_integration", this.integrationGr.sys_id + "");
27          gr.orderBy("ds_group_number");
28          gr.orderBy("last_used");
29          gr.query();
30          var lastGroup;
31          if (gr.getRowCount() == 0) {
32              throw new Error("There are no data sources to provide data to.");
33          }
34          while (gr.next()) {
35              var thisGroup = gr.getValue("ds_group_number");
36              if (lastGroup == thisGroup && lastGroup !== undefined) {
37                  continue;
38              } else {
39                  var ds = new GlideRecord("sys_data_source");
40                  if (!ds.get(gr.sys_data_source + ""))
41                      continue;
42
43                  var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                  mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue());
45                  gr.setValue("last_used", new GlideDateTime().getValue());
46                  gr.update();
47                  lastGroup = thisGroup;
48              }
```

To：

編集後の _processFromDataSourcesGroups のコード

```
43                  var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                  mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue(),this.integrationProcessGr.getValue("sys_domain"));
45                  gr.setValue("last_used", new GlideDateTime().getValue());
46                  gr.update();
47                  lastGroup = thisGroup;
```

9. **VulnerabilityDSAttachmentManager** スクリプトインクルードのメソッド **queueItem** を編集して、ハイライト表示された次のコードブロックを追加します。
queueItem

```
44      queueItem: function(dataSource, attachmentName, reportData, optIntegrationProcess,optDomain) {
45          var gr = new GlideRecord(this._QUEUE_TABLE);
46          gr.initialize();
47          gr.setValue("status", "NEW");
48          gr.setValue("data_source", dataSource);
49          if (optIntegrationProcess)
50              gr.setValue("integration_process", optIntegrationProcess);
51          if(optDomain){
52                  gr.setValue("sys_domain", optDomain);
53          }
54          var sysId = gr.insert();
```

_getNext

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
156     _getNext: function() {
157         // First go through the retries, if any
158         var gUser = new GlideRecord("sys_user");
159         gUser.get(gs.getUserID());
160         var sysDomainUser = gUser.getValue("sys_domain");
161         var gr = new GlideRecord(this._QUEUE_TABLE);
162         gr.addQuery("status", "RETRY");
163         gr.addQuery("sys_domain", sysDomainUser);
164         gr.orderBy("queued_on");
165         gr.query();
166         if (gr.next()) {
167             return gr;
168         }
169
170         // Then handle the regular queued items
171         gr = new GlideRecord(this._QUEUE_TABLE);
172         gr.addQuery("status", "QUEUED");
173         gr.orderBy("queued_on");
174         gr.addQuery("sys_domain", sysDomainUser);
175         gr.query();
176         if (gr.next()) {
177             return gr;
178         }
179
```

_processQueueEntry 関数

```
182     _processQueueEntry: function(entry) {
183         var schedGrId = this._getScheduledImportSet(entry.data_source);
184         if (gs.nil(schedGrId)) {
185             return;
186         }
187
188         var dataSourceGr = new GlideRecord("sys_data_source");
189         if (!dataSourceGr.get(entry.data_source)) {
190             gs.warn("Non existent data source - marking as complete");
191             entry.setValue("status", "COMPLETE");
192             entry.setValue("processing_notes", "Data source does not exist, could not process.");
193             entry.update();
194             return;
195         }
196
197         try {
198             this._deleteDataSourceAttachments(entry.data_source);
199             if (!this._verifyDataSourceAttachmentsDeleted(entry.data_source)) {
200                 gs.error("VulnerabilityDSAttachmentManager._processQueueEntry: Attachments not deleted for queue
entry " + entry.sys_id);
201                 throw "Attachments not deleted";
202             }
203             var attachmentApi = new GlideSysAttachment();
204             attachmentApi.copy(this._QUEUE_TABLE, entry.sys_id + "", this._DATA_SOURCE, dataSourceGr.sys_id + "");
205             var schedGr = new GlideRecord("scheduled_import_set");
206             schedGr.get(schedGrId);
207             schedGr.setValue("data_source", entry.data_source);
208             schedGr.setValue("run_as", gs.getUserID());
209             schedGr.update();
```

この時点で、ドメインセパレーションインポートの準備ができました。

> **注:**
> 脆弱性対応 または アプリケーション脆弱性対応 の統合が複数展開されている場合は、展開ごとにこのプロセスを繰り返します。

バックグラウンドジョブフレームワークで複数のドメインを作成してサポートする

脆弱性対応製品のバックグラウンドジョブは、レコードに対して複数のプロセスを実行するために長時間実行されるように設計されています。バックグラウンドジョブプロセッサーは、システムユーザーを介して実行され、グローバルドメインにレコードを作成するベースシステムに付属しています。

始める前に

必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > ドメイン管理 > ドメイン.
2. ドメインを作成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドメインの作成方法の詳細については、「Create a domain」を参照してください。

作成したドメインごとに、ユーザーを作成してそのドメインにアサインします。このユーザーは、ドメインの run_as プレースホルダーと考えてください。グローバルドメインの VR.System ユーザーに相当します。このユーザーには、脆弱性データへのアクセスが必要です。

3. スケジュール済みジョブ *Scheduled Background Job Manager*、および *Close the parent background job* の run_as を変更します。

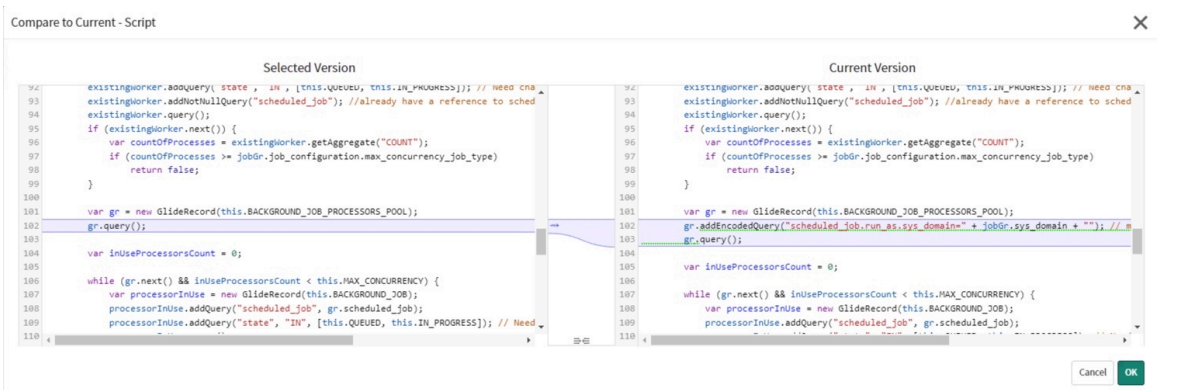
   複数のドメインを作成している場合は、このジョブを複製してそれに応じて実行ユーザーを変更します。非アクティブモードでは、グローバルドメインの実行ユーザーで、上記のジョブの 1 つのコピーを保持することもできます。

   10 個のプロセッサージョブ (たとえば、*Background job processor 10*) がベースシステムに付属しています。これらのジョブの実行ユーザーをドメインセパレーションユーザーに変更します。複数のドメインが存在する場合は、ドメインごとに 2 つのジョブで十分ですが、必要に応じてこれらのジョブを複製することもできます。2 つのプロセッサージョブを run_as ユーザーとともにグローバルドメインに保持します。

   脆弱性対応 の v20.0 以降、次のスクリプトの変更がベースシステムに付属しています。

4. スクリプトインクルード *BackgroundJobManager* を変更し、下のイメージに示すように以下の行を追加します。

```
gr.addEncodedQuery("scheduled_job.run_as.sys_domain=" + jobGr.sys_domain + "");
```



> **注:**
> 正しいドメインからルールのオンデマンド再適用をトリガーします。

脆弱性対応 CI ルックアップルールの作成

[CI ルックアップルール] モジュールには、サードパーティの脆弱性統合のインポート中に受信したホスト情報に一致するレコードを検索するために使用されるルールが含まれています。ホスト情報は、検出されたアイテム、一致しない構成アイテムクラス、および 構成管理データベース (CMDB) と照合されます。

始める前に

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

必要なロール：sn_vul.vulnerability_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタスクについて
CI ルックアップルールを作成するには、ServiceNow および 脆弱性対応 の高度な専門知識が必要です。既存のルックアップルールのいずれかを修正するのではなく、それをコピーしてコピーを修正することを検討してください。新しいルールで問題がなければ、元のルールを非アクティブ化します。

注:
ルールは、一度削除すると元に戻せません。新しいルールを作成する場合は、既存のルールを削除せずに非アクティブ化します。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > **CMDB** > **CI** ルックアップルール.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

CI ルックアップルールフォーム

フィールド	説明
名前	ルールの名前。
ルックアップメソッド	照合に使用される方法。選択肢は次のとおりです。 ○ [スクリプト]：ビルド済み (IP アドレス、DNS 名など) またはカスタムスクリプト。 ○ [一致するフィールド **(Field matching)**]：CMDB 内のテーブルまたはフィールドを検索します。
タイプ	スクリプト [ルックアップメソッド] で使用するタイプ。
順序	ルールの優先順位。順序が最も低いルールが最初に評価されます。
有効	ルールがアクティブか無効かを示すチェックボックス。
ソース	このルールへの入力として使用されるソース。
ソースフィールド	このルールへの入力として使用されるソースフィールド。任意のフィールドを選択しますが、文字列値として扱われます。
条件	CI ルックアップルールが適用される条件。この条件は、サードパーティスキャナーの属性に依存します。 **注:** 資産属性はペイロードの一部です。サードパーティのスキャナーから受信されます。ペイロードの例については、[検出されたアイテム] テーブルを参照してください。
スクリプト	[タイプ] に基づく編集可能なサンプルスクリプトが表示されます。デフォルト関数のテンプレートに含まれるコメントに従って、カスタムスクリプトを実装します。 **注:** process 関数には、*rule*、*sourceValue*、および *sourcePayload* の 3 つのパラメーターがあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
検索するテーブル	CMDB 内を検索するテーブル。[ルックアップ方法] に一致するフィールドとともに使用されます。
検索対象フィールド	CI を見つけるために使用できる情報を含むフィールド。[ルックアップ方法] に一致するフィールドとともに使用されます。このフィールドは、CI レコード、またはネットワークアダプタなどの関連レコードにあります。

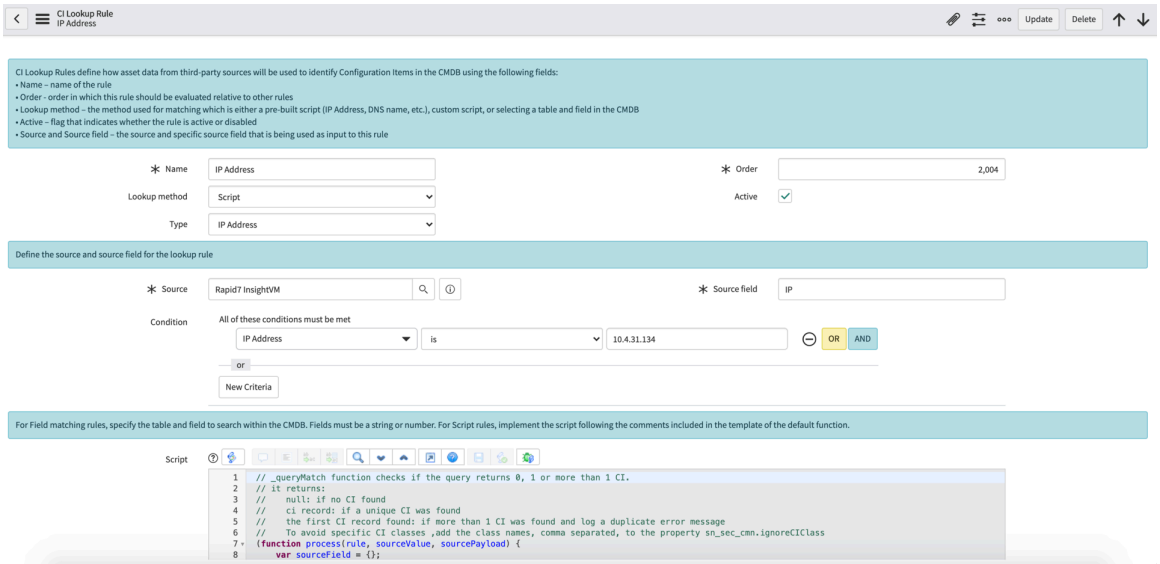
4. **[Submit]** をクリックします。

CI ルックアップルールの実装情報の詳細については、「脆弱性対応 CI ルックアップルールの実行後にレコードが重複または孤立しないようにするための手順」を参照してください。

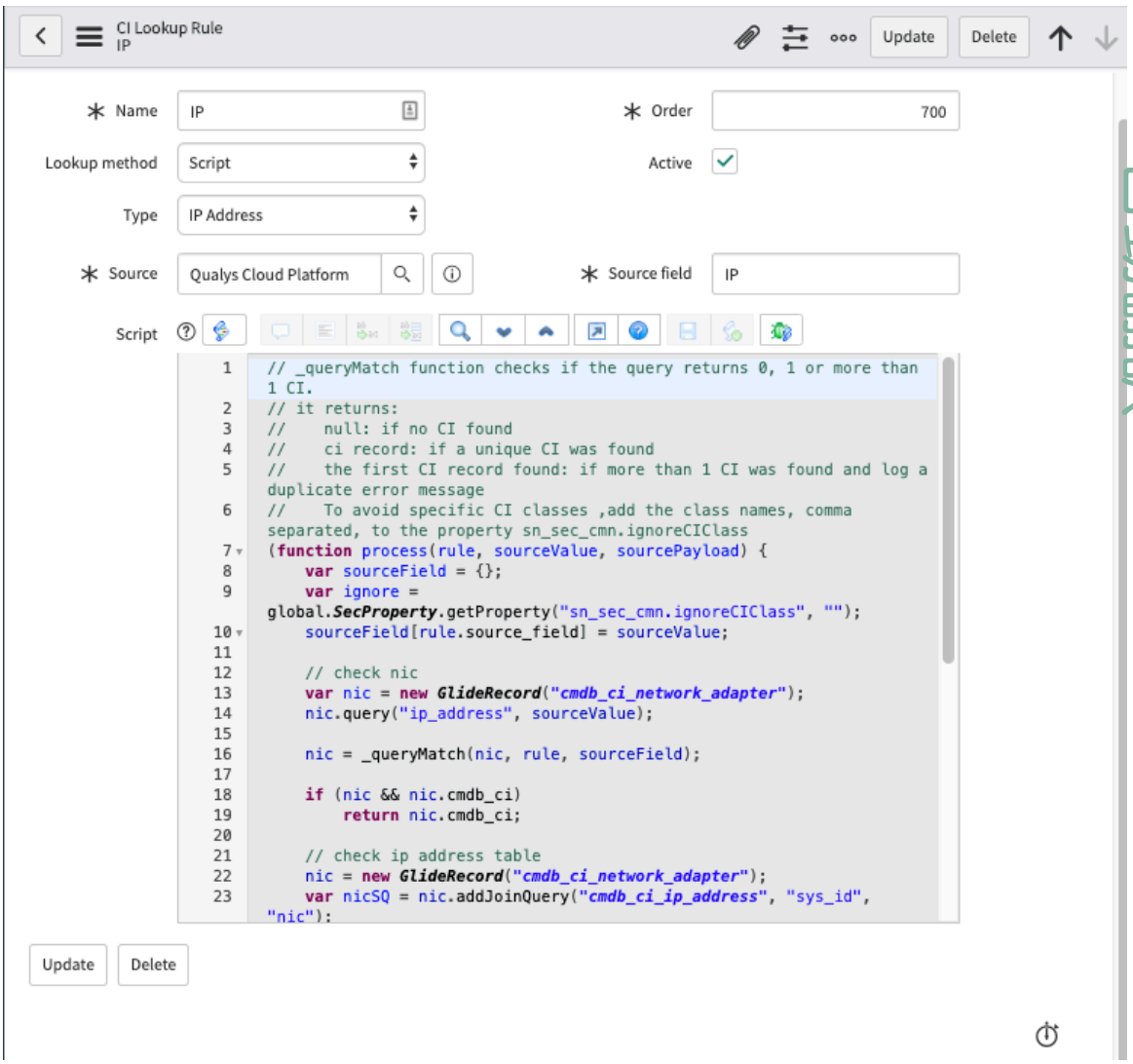
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

V12.0 の条件ビルダーを使用した CI ルックアップルールの例



V12.0 より前のスクリプトを使用した CI ルックアップルールの例



自動翻訳

関連情報

脆弱性対応 脆弱性一致アイテムフォームフィールド

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CI クラスの無視

ロードバランサー [cmdb_ci_lb] などの一部の構成アイテム (CI) クラスを無視するには、CI ルックアップルールを実行する際に、**ignoreCIClass** [*sn_sec_cmn.ignoreCIClass*] システムプロパティを設定します。

始める前に
必要なロール：admin

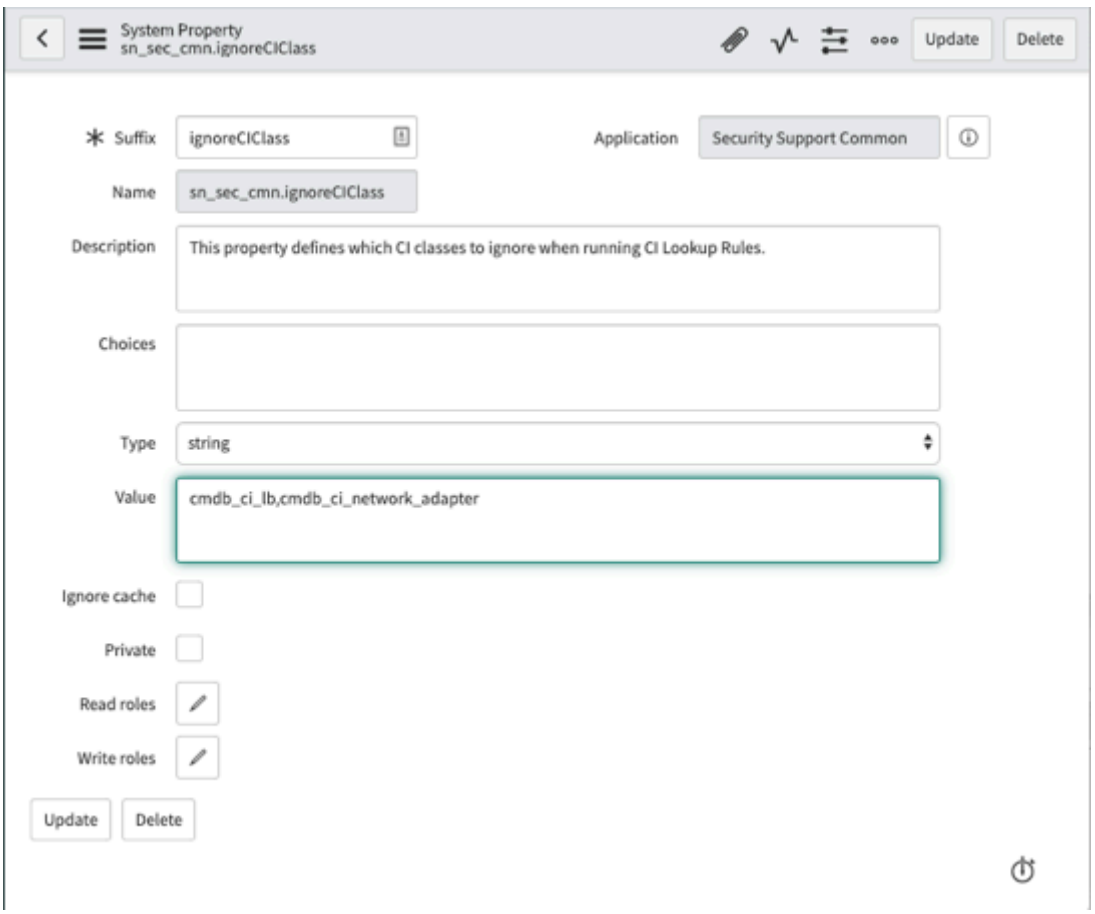
注:

脆弱性対応 v9.0 以降では、**ignoreCIClass** システムプロパティを使用できますが、以前のバージョンからアップグレードすると、このプロパティの機能は使用できません。

バージョン 9.0 より前の セキュリティオペレーション アプリケーションからアップグレードした場合は、この機能を有効にする方法について KB0788209 を参照してください。

手順

1. 左側のナビゲーションバーで「sys_properties.list」と入力します。
2. [入力] をクリックします。
3. [検索] メニューで、[名前] に「sn_sec_cmn.ignoreCIClass」と入力します。
4. [値] テキストボックスに、除外する CI クラスをカンマ区切りリストで入力します。



5. [更新] をクリックします。
   このリストは、次回のインポート時に CI ルックアップルールで使用されます。インポート中に作成された脆弱性一致アイテムは、sn_sec_cmn.ignoreCIClass システムプロパティの [値] フィールドにリストされているいずれのタイプの CI にも関連付けられていません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

廃止された CI のフィルタリング

CI ルックアップルールの実行中に廃止された構成アイテム (CI) をフィルタリングします。Security Operations CMDB CI ルックアップルールの実行時に廃止された CI をフィルタリングするには、**filterOutDecommissionedCI**[**sn_sec_cmn.filterOutDecommissionedCI**] システムプロパティを true に設定します。

始める前に
必要なロール：admin

このタスクについて
このシステムプロパティのデフォルト値は true です。このプロパティは 脆弱性対応 の CI ルックアップルールにのみ適用され、IRE のルックアップロジックには影響しません。

手順

1. 左側のナビゲーションバーで「sys_properties.list」と入力します。
2. [入力] を選択します。
3. [検索] メニューの [名前] に「sn_sec_cmn.filterOutDecommissionedCI」と入力して、廃止された CI をフィルタリングします。
4. [値] テキストボックスに値「true」または「false」と入力します。
   デフォルト値は true です。
5. [更新] を選択します。
   この値は、次回のインポート時に CI ルックアップルールで使用されます。sn_sec_cmn.filterOutDecommissionedCI システムプロパティは、ルックアップルールの実行中に、以下に示す条件を満たす CI を除外します。

```
_isCIDecommissioned: function(gr, filterDecommissionCi) {
        var install_status = false;
        var life_cycle_stage_status = false;
        // check for property
        if (filterDecommissionCi == "true") {
           if (gr.isValidField("install_status"))
              install_status = gr.install_status == 7;
           if (gr.isValidField("life_cycle_stage_status"))
              life_cycle_stage_status = gr.life_cycle_stage_status == "Retired";
        }
        return install_status || life_cycle_stage_status;
```

CI の自動昇格

autoPromoteFields [**sn_sec_cmn.autoPromoteFields**] システムプロパティで JSON 文字列を編集し、構成アイテム (CI) ルックアップルールにより、すべての Security Operations CMDB CI が [cmdb_ci] テーブルの一致するエントリに自動昇格されるようにします。

始める前に
必要なロール：sn_vul.vulnerability_admin

このタスクについて
システムプロパティタイプは「文字列」で、JSON 文字列を入力する必要があります。このプロパティはデフォルトで有効になっており、CI ルックアップルールの実行中に一致する CI を昇格させます。

カスタム作成されたルックアップスクリプトは、スクリプトから子テーブルレコードを返す場合があります。このプロパティの場合、*CIIdentify Script Include* の *_autoPromoteCI* 関数は

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ルックアップスクリプトによって返された CI を取得し、関係を自動的にトラバースして *cmdb_ci* エントリーに到達したらそれを返します。

自動昇格ロジックを上書きする、つまり、新しい CI クラスを追加または更新するには、[**sn_sec_cmn.autoPromoteFields**] システムプロパティの値フィールドに JSON オブジェクトを追加します。

手順

1. 左側のナビゲーションバーで「sys_properties.list」と入力します。
2. [入力] を選択します。
3. [**sn_sec_cmn.autoPromoteFields**] システムプロパティを見つけて、レコードを選択して開きます。

   デフォルト文字列：

```
{
 "dscy_switchport":"cmdb_ci",
 "cmdb_ci_network_adapter":"cmdb_ci",
 "cmdb_ci_nic":"cmdb_ci",
 "cmdb_ci_ip_address":"nic"
}
```

4. [値] テキストボックスで、デフォルトのペアリング形式を使用して文字列を編集します。
5. [更新] を選択します。
   この値は、次回のインポート時に CI ルックアップルールで使用されます。

脆弱性一致アイテムキーの構成

脆弱性対応 アプリケーションの脆弱性一致アイテム (VI) キーの粒度を構成して、組織内の脆弱性一致アイテム (VI) の構成要素を定義します。

始める前に
必要なロール：admin
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

主要な用語：

構成アイテム (CI)
: CMDB にリストされている既存の資産。

脆弱性
: 米国国立標準技術研究所 (NIST)、脆弱性情報データベース (NVD)、共通脆弱性識別子 (CWE)、または 脆弱性対応 とのサードパーティ統合からインポートされた既知の脆弱性のレコード。

脆弱性一致アイテム
: インポートされた脆弱性が CMDB 内の構成アイテムと一致すると、脆弱性一致アイテムが作成されます。

検出

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サードパーティ統合のスキャナーによってレポートされる脆弱性の単一で個別の発生。検出は、インスタンスにおける検出と脆弱性一致アイテムレコードの両方でインポートおよび表示されます。脆弱性一致アイテム検出とも呼ばれます。

デフォルトでは、脆弱性一致アイテムは、構成アイテム (CI)、脆弱性、および統合インスタンスの固有の組み合わせです。脆弱性一致アイテムをより詳細に作成するには、脆弱性一致アイテム検出から一意のポートを追加し、組織にとって最も効果的と思われるレベルで脆弱性の修正を管理します。

脆弱性一致アイテムをより詳細に作成する場合は、ポートを含むように脆弱性一致アイテムキーを構成します。[ポートを含める] を有効にすると、脆弱性一致アイテム検出からの一意のポートによって脆弱性一致アイテムが作成されます。

脆弱性対応 V17.1 以降では、VI キーとして証明を追加することで、Rapid7 脆弱性を識別して修正できます。詳細については、「Rapid7 脆弱性一致アイテムのキーに実証を追加する」を参照してください。

[ポートを含める] オプションを有効にするには、次の表からオプションを選択します。

VI キーに対して [ポートを含める] オプションを初めて有効にする場合の **3** つのシナリオ

次の場合	説明
次の条件の 1 つ以上が満たされている場合： • 脆弱性一致アイテムの検出をサポートしていなかった v10.0 より前のバージョンの 脆弱性対応 からアップグレードしようとしている。 • 新規利用者であり、Now Platform® インスタンスに脆弱性対応データ (脆弱性一致アイテムまたは脆弱性一致アイテム検出) がない。 • 既にインスタンス内のすべての脆弱性一致アイテムレコードと関連データが削除済みであり、新規インポート以降は一意のポートで識別される VI を含めるように、すべての脆弱性対応データをビルドする準備ができている。	[ポートを含める] を有効にします。 [ポートを含める] を有効にすると、インポートされた検出では、次回のインポート以降は一意のポートで識別される VI を含む脆弱性一致アイテムが作成されます。
両方の条件が満たされている場合： • v10.0 以降の 脆弱性対応 があり、インスタンスに保持しておきたい既存の脆弱性対応データ (脆弱性一致アイテムまたは脆弱性一致アイテム検出) がある。 • 一意のポートで識別される VI を含めるために、新しい脆弱性一致アイテムの作成を開始することを望んでいる。	[ポートを含める] を有効にします。既存の検出とそれに関連する脆弱性一致アイテムは保持されます。 [ポートを含める] を有効にすると、新しい検出では、次回のインポート以降は一意のポートで識別される VI を含む新しい脆弱性一致アイテムが作成されます。
両方の条件が満たされている場合： • v10.0 以降の 脆弱性対応 がある。 • 既存の脆弱性対応データ (脆弱性一致アイテムまたは脆弱性一致アイテム検出) があるが、新規インポート以降は脆弱性データをビルドして一意のポートで識別される VI を含めたいため、既存のデータを保持することは望んでいない。	**1.** インスタンスからすべての脆弱性一致アイテムレコードと関連データを削除します。 **2.** [ポートを含める] を有効にします。 [ポートを含める] を有効にすると、新しい検出では、次回のインポート以降は一意のポートで識別される VI を含む新しい脆弱性一致アイテムが作成されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

[ポートを含める] オプションが有効になっている場合、1 つの構成アイテムに対して複数の脆弱性一致アイテムが作成されることがあります。たとえば、構成アイテムの 2 つのポート (ポート 80 と 443) に脆弱性が存在する場合、次回のインポートからは各ポートに 1 つずつ、2 つの一意の VI が作成されます。

注:

VI を作成する場合は、この機能を有効にする前に、一意のポートで VI を含めるようにしてください。ポートを含む VI キーを有効にしたら、[ポートを含める] を無効にしてデフォルトの VI キーの粒度 (ポートに対して VI が作成されても一意のポートで識別されない粒度) を使用した脆弱性データのインポートに戻る前に、まず脆弱性対応データを削除する必要があります。脆弱性データの削除の詳細については、「脆弱性対応 のすべての脆弱性一致アイテムレコードと関連データの削除」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > **VI** の粒度の構成.

   [最終更新日] フィールドには、VI キーが最後に構成された日付が表示されます。

2. [ポートを含める] チェックボックスをクリックして有効にします。

3. [保存] をクリックします。
   確認ダイアログが表示されます。

   インスタンスに脆弱性一致アイテム検出レコードがない場合、次回のインポート以降は、一意のポートによって脆弱性一致アイテム検出と脆弱性一致アイテムの両方が作成されます。

   インスタンスに既存の脆弱性一致アイテム検出と脆弱性一致アイテムがある場合、既存の検出および関連する脆弱性一致アイテムは保持されます。新しい検出では、次回のインポート以降、一意のポートで識別される VI を含む新しい脆弱性が作成されます。

次のタスク
脆弱性一致アイテム検出および脆弱性一致アイテムのレコードに、ポート別の脆弱性一致アイテムが表示されていることを確認します。詳細については、「脆弱性対応 脆弱性一致アイテム検出データの表示」を参照してください。

Rapid7 脆弱性一致アイテムのキーに実証を追加する

Rapid7 VI の脆弱性一致アイテム (VI) キーとして実証を追加します。特定の脆弱性に対する実証を含めることで、Rapid7 スキャナー統合では、Rapid7 から受け取った実証ごとに VI を作成できます。

VI キーは、脆弱性、構成アイテム (CI)、および統合インスタンスの組み合わせです。実証に基づいて検出を異なる VI に分割すると、複数の VI が作成されます。脆弱性は適切な修復オーナーにアサインできます。

たとえば、脆弱性と CI が同じであるが、実証が異なる 2 つの検出があり、1 つの VI が作成される場合があります。脆弱性対応 V17.1 以降では、VI キーとして実証を追加することで、脆弱性を識別して修復できます。

次の方法で、実証を VI キーとして追加できます。

次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > **VI** の粒度の構成 をクリックし、証明を含めるオプションを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[ユースケース：既存の **VI** の **VI** キーに実証を含めるか、検出の実証に基づいて既存の **VI** を分割する **(Use case: Including proof in VI key for existing VIs or splitting existing VIs based on detection proof)]**

実証に基づいて VI を作成するには、R7 log4j 脆弱性を使用できます。たとえば、R7-apache-log4j-core-cve-2021-44228、R7-amazon_linux-cve-2021-44228、または R7-amazon-linux-ami-2-cve-2021-44228 などの複数の R7 log4j 脆弱性のうちのいずれかを使用できます。

VI 内のすべての検出に同じ実証がある場合、既存の VI は「VI キー (external_id) の実証」を含むように更新されます。実証が異なる複数の検出がある場合、既存の VI はクローズされます。検出は、「VI キー (external_id) の実証」を使用して新しい VI に分割されます。

注:

脆弱性 ID を指定すると、既存の VI が実証に基づいて分割されます。この脆弱性 ID の新しい脆弱性も、VI キーの 1 つとして実証を持っています。

脆弱性対応 のすべての脆弱性一致アイテムレコードと関連データの削除

Now Platform® インスタンスの 脆弱性対応 アプリケーションから、すべての Vulnerability Response データ (脆弱性一致アイテムまたは脆弱性一致アイテム検出) および関連データとレコードを完全に削除します。

始める前に

脆弱性対応 アプリケーションの脆弱性一致アイテム検出レコード、脆弱性一致アイテム、脆弱性グループ、および関連レコードをインスタンスから削除します。このプロセスを使用して、サードパーティ統合から心機一転してデータをインポートするために、または脆弱性一致アイテム (VI) のキー構成をデフォルト設定に戻すための前提条件として、インスタンスを一掃します。VI キーの構成の詳細については、「脆弱性一致アイテムキーの構成」を参照してください。

注:

このアクションを実行すると、すべての脆弱性一致アイテムレコードと関連データがインスタンスから削除されます。このデータは、一度削除すると取得できなくなります。また、データのインポートを一時停止し、脆弱性対応 とのアクティブなサードパーティ統合を無効にする必要があります。

VI キー構成を変更する前に、このプロセスで脆弱性一致アイテムデータを削除する必要があります。すべてのデータを削除すると、次回のインポート以降は、すべての脆弱性一致アイテムと脆弱性一致アイテム検出がマッピングされ、最新のデータで更新されます。

データを削除する前に、以下の条件が当てはまることを確認してください。

- v10.0 以降の 脆弱性対応 がインストールされている。詳細については、「サードパーティ統合からの 脆弱性対応 脆弱性一致アイテム検出」を参照してください。
- [ポートを含める] を無効にして、VI キー構成をデフォルト設定に戻したい。
- 既存の脆弱性一致アイテムと脆弱性一致アイテム検出があっても、それらが不要であるか、または更新して保持する必要がない。
- 既存のすべての脆弱性対応データと関連レコードを削除してインスタンスをクリーンアップする必要があると判断した。

必要なロール：sn_vul.vulnerability_admin

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性統合.
2. 表示されているすべてのアクティブな統合を記録します。

   スケジュール済みジョブとともにリストされているすべてのアクティブな統合は、すべての脆弱性一致アイテムと関連データを削除する前に無効になるため、データ削除中に新しいデータはインポートされません。このリストを記録すると、削除の完了後に統合をアクティブ化できるようになります。

3. HI ナレッジベースで「How to delete existing Vulnerability Response Data for reimport (再インポートのために既存の脆弱性対応データを削除する方法)」記事を確認します。
4. [アクティブ] 列に書き込むことができないという警告メッセージが表示された場合は、アクティブな統合を無効にするために、次の手順を実行します。

   a. [名前] 列で、アイテムをクリックしてレコードを開きます。

   b. [アクティブ] チェックボックスを編集できない場合は、ここのリンクをクリックしてレコードを編集します。

   c. [アクティブ] チェックボックスをクリックして統合を無効にし、次回のスケジュール済みジョブをキャンセルします。

   d. [更新] をクリックして変更を保存し、リストに戻ります。

   e. [統合] リストからアクティブな統合を無効にしたことを確認します。
   統合を無効にすると、アクティブな統合リストに表示されなくなります。非アクティブな統合のリストを表示し、すべての脆弱性データを削除した後に無効にしたすべての統合を見つけるには、上部の [アクティブ] 列に「=false」と入力します。

5. 既存の脆弱性データの削除に関する KB 記事の手順を進めます。
6. すべてのデータが正常に削除されたことを確認したら、 脆弱性対応 > アドミニストレーション > **VI** の粒度の構成.
7. フォームで次のようにします。
   - 新規インポートからのポートを含めるように脆弱性データをビルドするという理由でデータを削除した場合は、[ポートを含める] を有効にして [保存] をクリックします。
   - VI キーをデフォルト設定に戻すためにデータを削除した場合は、[ポートを含める] を無効にして [保存] をクリックします。

   詳細については、「脆弱性一致アイテムキーの構成」を参照してください。

脆弱性対応 内のフィルタリング

修復タスクルール、算出、アサインルールでは、条件ビルダーを使用して作成されたインポート時の条件が使用されます。各レコードはこうしたフィルターを使用して評価されるため、基準を変更するとパフォーマンスに影響する場合があります。

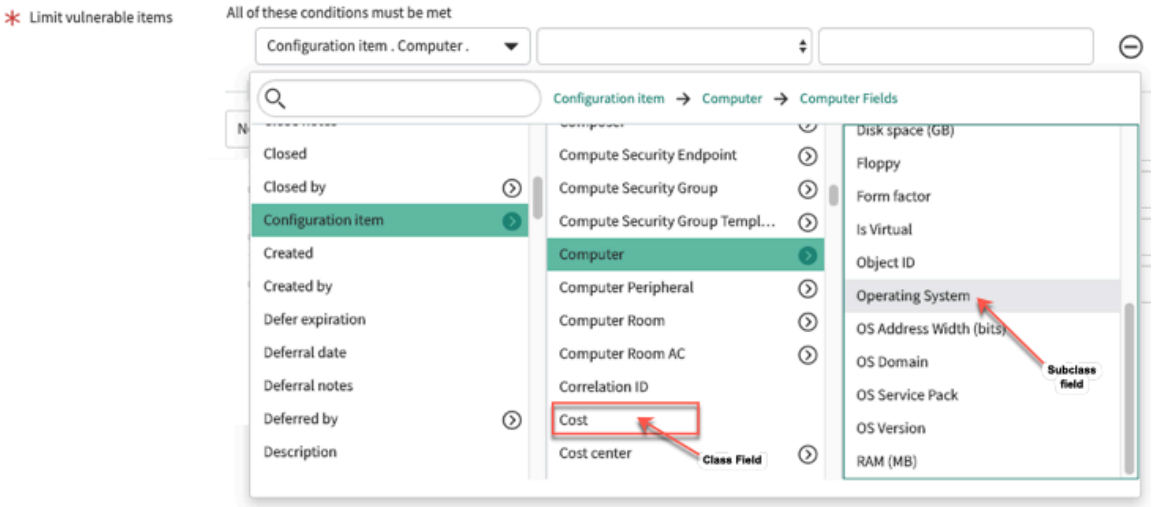
ベースシステムに含まれるルールと算出は、パフォーマンスが最適化されています。ルールや算出の編集または作成には注意が必要であり、ServiceNow と 脆弱性対応 の両方の専門知識が必要になる場合があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サブクラスフィールドに基づくフィルタリングの回避

一部のテーブルは拡張をサポートしています。CMDB CI [cmdb_ci] テーブルはその一部です。cmdb_ci_hardware や cmdb_ci_computer などのテーブルは、このテーブルを拡張します。親テーブルにないフィールドに基づいてフィルタリングを行う場合、そのフィルターのビルドと評価に費用を要する場合があります。



たとえば、 構成アイテム > コスト コストは構成アイテムのクラスフィールドであり、サブクラスフィールドではないため、パフォーマンスに悪影響を与えることはありません。

構成アイテム > コンピューターただし、別のフィールド (この場合は **Operating System**) へのドット連結を必要とするサブクラスです。このプロセスには何ミリ秒もかかる場合があり、何百万ものの脆弱性一致アイテムをインポートすると、すぐに累積してしまい、パフォーマンスに影響します。

注:
[contains] 条件の使用はワイルドカード検索に似ており、パフォーマンスに影響を与える可能性があります。可能な場合は [次の値に等しい] を使用する方が効率的です。

脆弱性対応の重大度マッピング

脆弱性対応には、標準 ServiceNow の重大度マッピングに対する脆弱性情報データベース (NVD) が備わっています。ServiceNow のサードパーティ統合では、インストール時に重大度マッピングを提供します。これらのマップは、既存のマップのフィールドを変更することで調整できます。

Rapid7 脆弱性統合セキュリティマッピング

Normalised_Severity

sn_vul_nvd_entry テーブルからの重大度を使用して、サードパーティエントリーの normalised_severity を計算します。これは、**sn_vul_entry** テーブルのルックアップ正規化重大度におけるビジネスルールで設定されています。

Source_severity

「Rapid7 脆弱性統合 - API」の実行中に、**severity_score** テーブルのデータが **source_severity** テーブルにマッピングされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

優先度

このフィールドは空白です。

Qualys 脆弱性統合セキュリティマッピング

Normalised_Severity

sn_vul_nvd_entry テーブルからの重大度を使用して、サードパーティエントリーの normalised_severity を計算します。これは、**sn_vul_entry** テーブルのルックアップ正規化重大度におけるビジネスルールで設定されています。

Source_severity

「Qualys ナレッジベース統合」の実行中に、**SEVERITY_LEVEL** のデータが **source_severity** テーブルにマッピングされます。

優先度

Qualys データにマッピングされたビジネスルールで「Qualys ホスト検出統合」が実行されているときに、[優先度] フィールドのデータが [重大度] テーブルから取得され、[優先度]テーブルにマッピングされます。

注:
ビジネスルールはバックグラウンドで実行され、Qualys の優先度をチェックし、適切に優先度をマッピングします。このことから、Qualys データのマッピングにおいてはビジネスルールが重要と言えます。

Tenable.io 脆弱性統合の重大度マッピング

Normalised_Severity

sn_vul_nvd_entry テーブルからの重大度を使用して、サードパーティエントリーの normalised_severity を計算します。これは、**sn_vul_entry** テーブルのルックアップ正規化重大度におけるビジネスルールで設定されています。

Source_severity

「Tenable.io プラグイン統合」の実行中に、**risk_factor** テーブルのデータが **source_severity** テーブルにマッピングされます。

優先度

「Tenable.io オープン脆弱性統合」の実行中に、**severity_id** のデータが **source_severity** にマッピングされます。

VPR

「Tenable.io プラグイン統合」の実行中に、スコアからのデータが **Source_risk_score** にマッピングされます。

「Tenable.io プラグイン統合」の実行中に、「スコアから算出」データが **Source_risk_score** にマッピングされます。

Tenable.sc 脆弱性統合重大度マッピング

Normalised_Severity

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

sn_vul_nvd_entry テーブルからの重大度を使用して、サードパーティエントリーの **normalised_severity** を計算します。これは、**sn_vul_entry** テーブルのルックアップ正規化重大度におけるビジネスルールで設定されています。

Source_severity

「Tenable.io プラグイン統合」の実行中に、**riskFactor** テーブルのデータが **source_severity** テーブルにマッピングされます。

優先度

「Tenable.io オープン脆弱性統合」の実行中に、**"severity": { "id": "0", "name": "Info", "description": "Informative" }** として受信した重大度のデータが **source_severity** にマッピングされます。

VPR

「Tenable.io プラグイン統合」の実行中に、**vprScore** からのデータが **Source_risk_score** にマッピングされます。

「Tenable.io プラグイン統合」の実行中に、「vprScore から算出」のデータが **Source_risk_score** にマッピングされます。

TVM 重大度マッピング

Normalised_Severity

sn_vul_nvd_entry テーブルからの重大度を使用して、サードパーティエントリーの normalised_severity を計算します。これは、**sn_vul_entry** テーブルのルックアップ正規化重大度におけるビジネスルールで設定されています。

Source_severity

「Microsoft **TVM** 脆弱性 **(CVE)** 統合」の実行中に、[重大度] テーブル のデータが **source_severity** にマッピングされます。

優先度

このフィールドは空白です。

脆弱性対応 重大度マップの作成

脆弱性対応 重大度マッピングは、サードパーティソースの重大度フィールドを 脆弱性対応 内で認識可能なフィールドに変換します。

始める前に

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

このタスクについて

脆弱性対応 には、脆弱性情報データベース (NVD) から、正規化された ServiceNow 重大度へのマッピングが付属しています。Qualys 脆弱性統合などの ServiceNow サードパーティ統合では、インストール時に重大度マッピングが提供されます。これらのマップは、既存のマップのフィールドを変更することで調整できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重大度マップの作成または編集は、自分の環境におけるカスタマイズされたまたは非標準のサードパーティマッピングのみを対象としています。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 正規化された重大度マッピング.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

フィールドマッピング

フィールド	説明
ソース	重大度マッピングのソースの名前。
ソース値	ソース重大度の値。
ターゲット値	ターゲットの重大度の値。選択肢は次のとおりです。 ○ 1- 重大 ○ 2 - 高 ○ 3：中 ○ 4：低 ○ 5：なし

4. ソース重大度レベルごとにステップ 3 を繰り返します。
5. **[Submit]** をクリックします。

脆弱性対応 レポートおよび関連リストのサービス分類の定義

サービス分類を定義することで、脆弱性対応 のレポートと関連リストに焦点を当てます。さらに、要求されたサービス分類の数を減らすことで、脆弱性対応 データ収集のパフォーマンスを向上させることができます。

始める前に
必要なロール：admin

注:

システムプロパティの編集には、ServiceNow と 脆弱性対応 の両方の専門知識が必要です。

手順

1. 左側のナビゲーションバーで「sys_properties_list.do」と入力します。
2. [入力] をクリックします。
3. [検索] メニューで、[名前] に「sn_vul.service_classifications」と入力します。
4. *sn_vul.service_classifications* システムプロパティを開きます。
5. [値] テキストボックスに、必要なサービス分類のカンマ区切りリストを入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
この設定が空の場合、すべてのサービスが一覧表示されます。

例：

ビジネスサービス、テクニカルサービス、およびアプリケーションサービスを表示し、サービスオファリング、シェアードサービス、および未分類のサービスを除外するには、値を「ビジネスサービス,テクニカルサービス,アプリケーションサービス」に設定します。

アプリケーションサービスを表示するには、値を「アプリケーションサービス」に設定します。

6. [更新] をクリックします。
   各レポートおよび脆弱性一致アイテム関連リストのデータは、夜間パフォーマンスアナリティクスジョブの次回実行時にサービス分類によってフィルタリングされます。

脆弱性一致アイテムテーブルの選択されたフィールドの監査

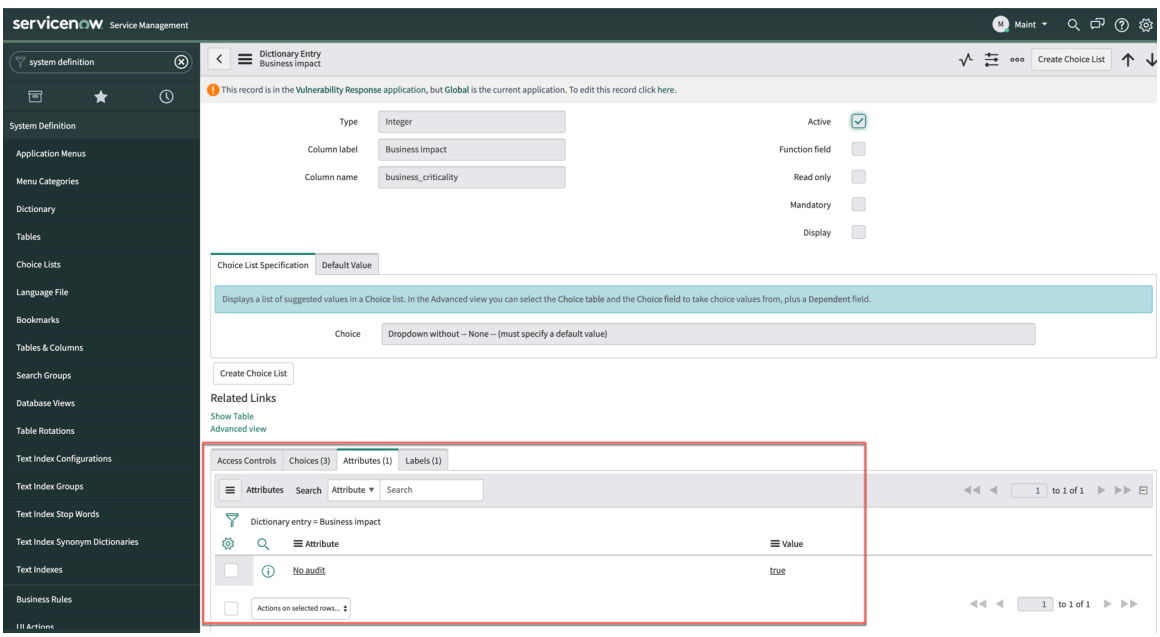
脆弱性一致アイテム [sn_vul_vulnerable_item] テーブルで指定したフィールドの監査を有効にします。この監査方法は、デフォルトで監査できないフィールドを監査する場合に便利です。

始める前に
必要なロール：admin

このタスクについて
sn_vul_vulnerable_item テーブルはデフォルトで監査可能です。no_audit 属性が true に設定されているフィールドは監査不可です。テーブルの監査の詳細については、「テーブルの監査を有効にする」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > システム定義 > テーブル をクリックし、sn_vul_vulnerable_itemテーブルを検索します。
   テーブルの辞書エントリーのリストが表示されます。
2. フィールドの監査を有効にするには、エントリーの名前をクリックします。
   そのエントリーの [辞書エントリー] ページが表示されます。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 次のように移動する。 属性 > 監査なし.
   [辞書の属性] ページが表示されます。
4. no audit=true 属性を削除するには、[削除] をクリックします。
   このフィールドの監査が有効になっています。

脆弱性対応 バックグラウンドジョブフレームワーク構成

Now Platform® インスタンスでバックグラウンドジョブフレームワークを定義します。この構成変更は、バックグラウンドジョブの実行に使用されるシステムリソースの量を減らすことで、パフォーマンスを向上させるのに役立ちます。

バックグラウンドジョブフレームワークで編集できる内容

バックグラウンドジョブ構成モジュールでは、 フレームワークに以下の設定オプションがあります。

- 脆弱性対応 プロセスに対して同時に実行されるバックグラウンドジョブの数を定義できます。
- バックグラウンドで実行され、大量のデータを処理する長いジョブの場合は、パーティションを作成して小さなチャンクでデータを処理できます。
- ジョブはキャンセルできます。

バックグラウンドジョブフレームワークを構成する理由

Now Platform® のバックグラウンドジョブは、脆弱性対応 のレコードに対して複数のプロセスを実行するために長時間実行されるように設計されています。こうしたジョブは、以前は非同期で実行されるビジネスルールに基づいていました。こうしたジョブによって影響を受ける大量のレコードを処理できるように、インスタンスのバックグラウンドで実行できるジョブの数は制限されていません。完了までに時間がかかる複数のジョブをバックグラウンドで同時に実行すると、スケジュール済みジョブの実行に使用されるシステムリソースが影響を受け、パフォーマンスが低下する恐れがあります。

バックグラウンドジョブフレームワークを構成すると、バックグラウンドジョブの実行に使用されるシステムリソースの量を減らすことで、パフォーマンスを向上させるのに役立ちます。

主要な用語

ジョブ機能
: 特定のジョブを表します。たとえば、特定のジョブに以下の機能が含まれている場合があります。
  - ジョブを同じタイプの別のジョブと並列に実行できる。
  - ジョブをパーティション化できる。
  - ジョブを実行中にキャンセルできる。

同時実行
: 並列に実行されるジョブまたはジョブの一部を表します。

パーティション
: パーティションは、並列処理してパフォーマンスを向上させるために分割できるジョブの一部です。通常は、実行時間の長いジョブが該当します。

ジョブ構成
: 特定のスケジュール済みジョブの設定を指します。

スケジュール済みジョブ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

スケジュール済みジョブは、特定の時間または繰り返しスケジュールで実行できる自動化された作業です。

システムリソース

環境内の指定された数のバックグラウンドジョブとスケジュール済みジョブをサポートする必要があるシステムリソースの量を表します。

システム プロパティ

システムプロパティには、ほとんどまたはまったく変更されない構成情報が保存されます。システムプロパティを変更または追加するたびに、キャッシュがフラッシュされ、クラスター内のすべてのノードが同期されます。このキャッシュのフラッシュはパフォーマンスに影響します。

ビジネスルール

ビジネスルールとは、レコードが表示、挿入、更新、または削除されるとき、またはテーブルに対してクエリが実行されるときに実行する、サーバー側スクリプトです。ビジネスルールを使用すると、特定の条件が満たされたときにフォームフィールドの値を自動的に変更するタスクや、メール通知やスクリプトアクション用のイベントを自動的に作成するタスクなどを実現できます。

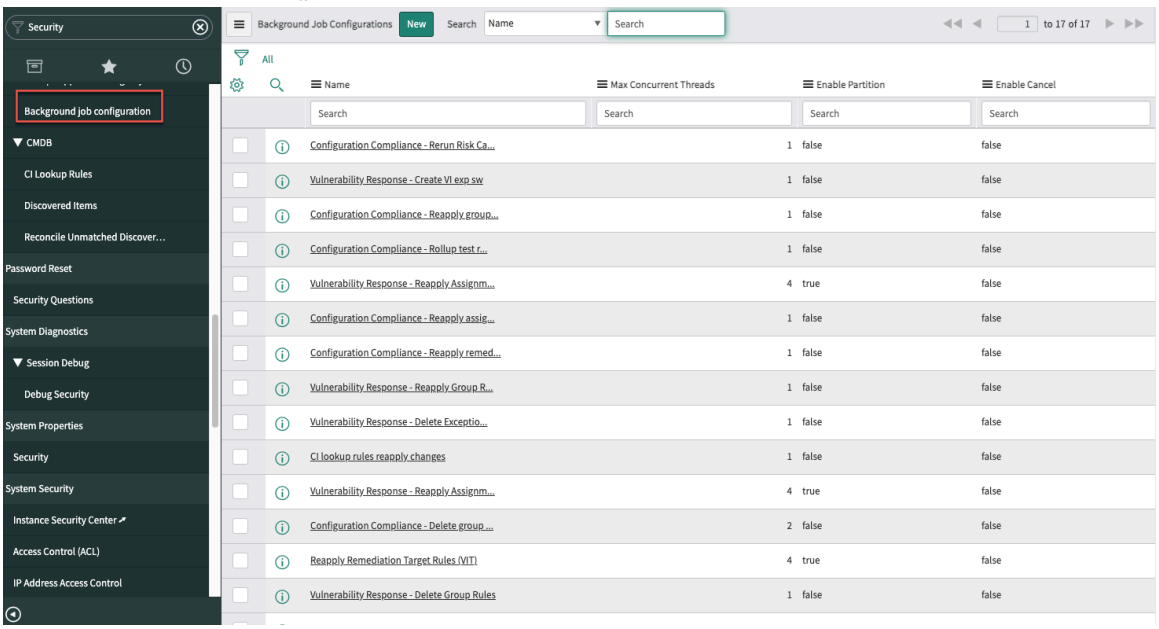
バックグラウンドジョブフレームワークを定義するユースケース

たとえば、脆弱性一致アイテム (VIT) レコードおよ アリケーション脆弱性対 脆弱性一致アイテム (AVIT) レコードの修復ターゲットルールを適用するバックグラウンドジョブは、複数のタスクで大量のレコードを同時に処理します。

インポートのサイズや環境内のレコードの数によっては、このジョブは利用可能なシステムリソースを大量に使用し、正常に完了するまでに時間がかかる場合があります。そのため、システムメンテナンスジョブまたはその他のスケジュール済みジョブの実行が遅くなることがあります。

バックグラウンドジョブ構成モジュールでは、ジョブが名前と一意の構成 ID 別に一覧表示されます。こうしたレコードで、特定のバックグラウンドジョブに対して同時に実行するタスクの数を定義できます。また、データのパーティションを処理するようにジョブを設定すると、タスクがより迅速かつ簡単に完了し、使用するシステムリソースが少なくなります。実行時間が長すぎると判断した場合は、ジョブをキャンセルすることもできます。

バックグラウンドジョブ構成モジュール



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

バックグラウンドジョブ構成を定義するために必要な手順の詳細については、「脆弱性対応 のバックグラウンドジョブ構成の定義」を参照してください。

脆弱性対応 のバックグラウンドジョブ構成の定義

特定のバックグラウンドジョブに対して同時に実行するタスクの数を定義します。また、データのパーティションをインポートするようにジョブを設定すると、タスクがより迅速かつ簡単に完了し、使用するシステムリソースが少なくなります。実行時間が長すぎると判断した場合は、ジョブをキャンセルすることもできます。

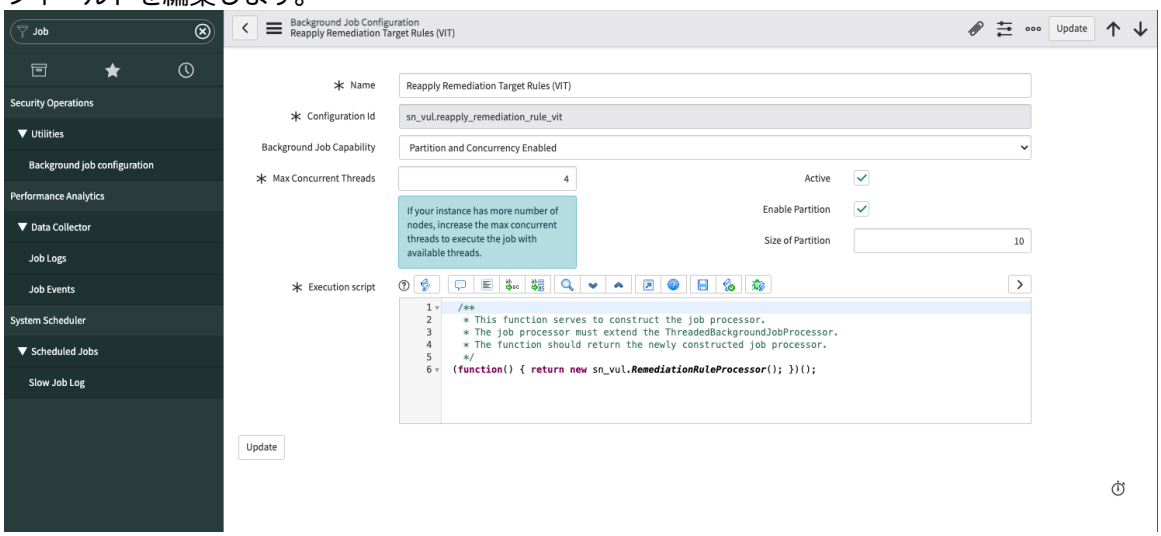
始める前に

必要なロール：sn_vul.vulnerability_admin、または sn_sec_cmn.manage_background_job の詳細ロールを持つ脆弱性マネージャー

例については、下記セクションの手順を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > バックグラウンドジョブ構成.
2. [名前] 列で、レコードをクリックして開きます。
3. フィールドを編集します。



4. [更新] をクリックして変更を保存します。
   構成変更の結果を検証する方法については、次の例を参照してください。

   アプリケーションに含まれている修復ターゲットルールジョブ構成には、脆弱性一致アイテム用とアプリケーション脆弱性一致アイテム用の 2 つがあります。

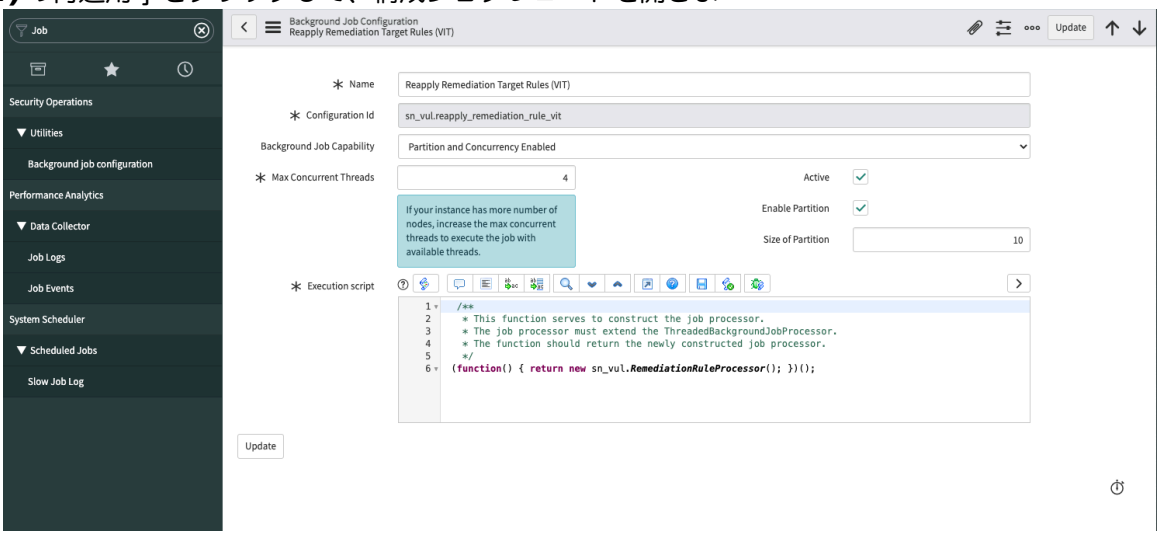
   - 修復ターゲットルール (VIT) の再適用
   - 修復ターゲットルール (AVIT) の再適用

   修復ターゲットルールを変更し、利用可能なシステム処理リソースをほとんど使用せずにルールを再適用するとします。処理リソースを制限するために、バックグラウンドジョブ構成モジュールで、実行するバックグラウンドジョブの数とジョブごとに処理するアイテムの数を調整できます。
5. これらの設定を定義するには、 セキュリティオペレーション > バックグラウンドジョブ構成 をクリックし、[修復ターゲットルール

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

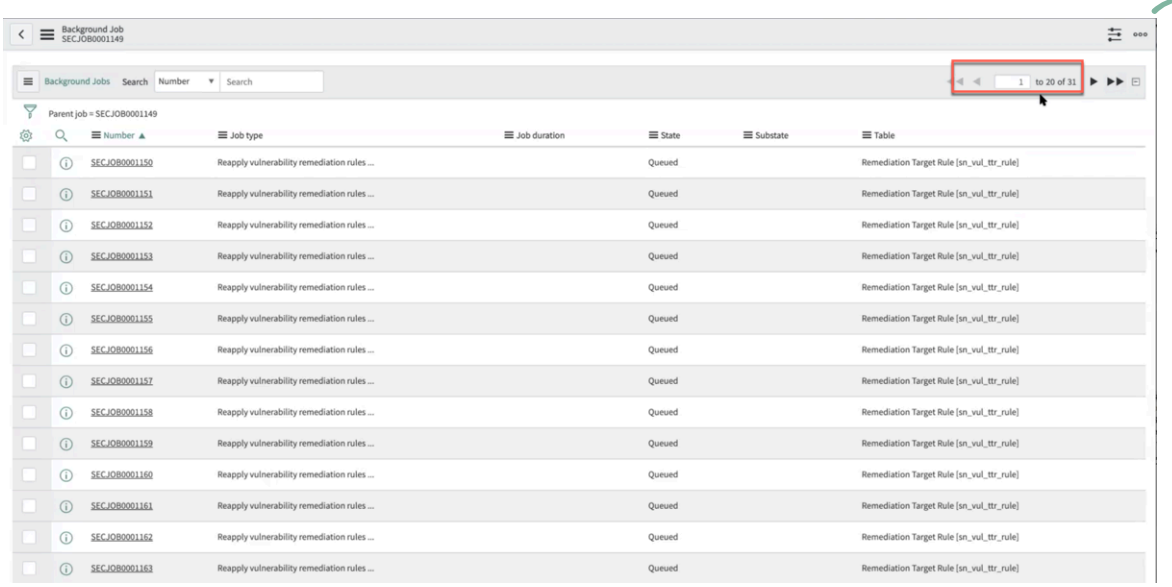
(VIT) の再適用] をクリックして、構成ジョブレコードを開きま



す。

例として、300 個を超える VI があるとします。

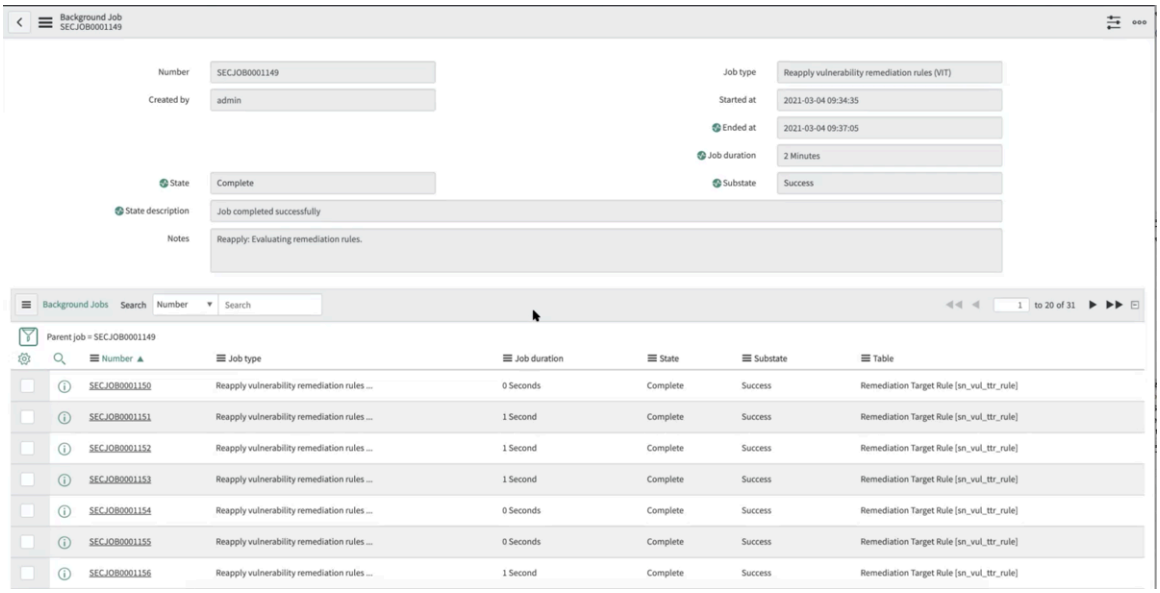
6. 開いている構成ジョブレコードで、[パーティションサイズ] の値を **4** から **10** に変更します。
7. 次のように移動する。 脆弱性対応 > 修復ターゲットルールで、変更した脆弱性修復ルールを再適用し、リストからレコードを選択して [変更を適用] をクリックし、既存の VI のターゲットルールを再評価します。
[脆弱性修正ルール (VIT) の再適用 (Reapply vulnerability remediation rules (VIT))] ジョブがキューに入れられます。
8. [ステータスを表示] リンクをクリックしてバックグラウンドジョブレコードを表示し、次の画像に示すように、ジョブがキューに入れられていることを確認します。
この例では、307 個の VI (ジョブあたり最大 10 アイテム) のターゲットルールを処理するために 31 個のジョブが作成されます。これらのジョブは、プライマリバックグラウンドジョブの子ジョブです。子ジョブはレコードを順番に処理します。



すべてのジョブが正常に完了すると、バックグラウンドジョブレコードのフィールドが更新されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



9. 脆弱性一致アイテムに移動し、新しいルールの変更が反映されていることを確認します。

脆弱性対応 のバックグラウンドジョブの高度な並列処理

この高度な設定では、ジョブタイプに関係なく、並列処理されるバックグラウンドジョブの総数を制御します。

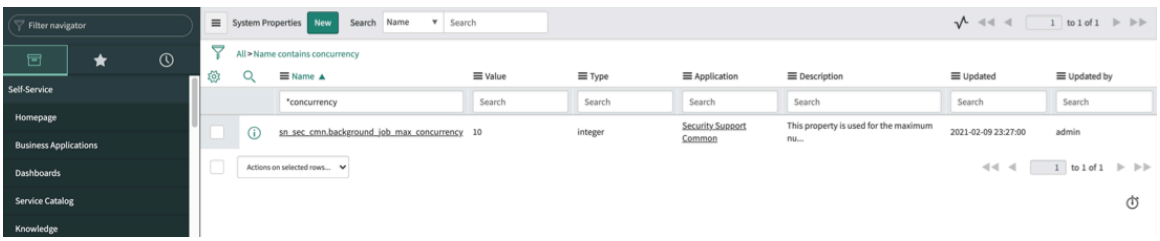
始める前に

必要なロール：sn_vul.vulnerability_admin、または sn_sec_cmn.manage_background_job の詳細ロールを持つ脆弱性マネージャー

> **注:**
> この手順には、高度なプログラミング知識が必要です。

手順

1. フィルターナビゲーターで、「**sys_properties.list**」と入力し、*sn_sec_cmn.background_job_max_concurrency* システムプロパティを見つけます。



2. 該当するレコードをクリックして開きます。

デフォルトでは、*sn_sec_cmn.background_job_max_concurrency* システムプロパティで最大 10 個のバックグラウンドジョブを並列実行できます。

インスタンスのノード数が少ない場合は、 システムプロパティでこの値を減らすことができます。たとえば、グループルールリストに 7 つのアサインルールがあるとします。[アサインルールを再適用] ジョブ設定レコードで、 [最大同時実行スレッド数] に 3 つのジョブが設定されています。フレームワークの同時実行値は 10 ですが、システムは単一ノードインスタンスであるため、[アサインルールを再適用] ジョブから 2 つのパーティション化されたジョブを同時実行で処理で

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

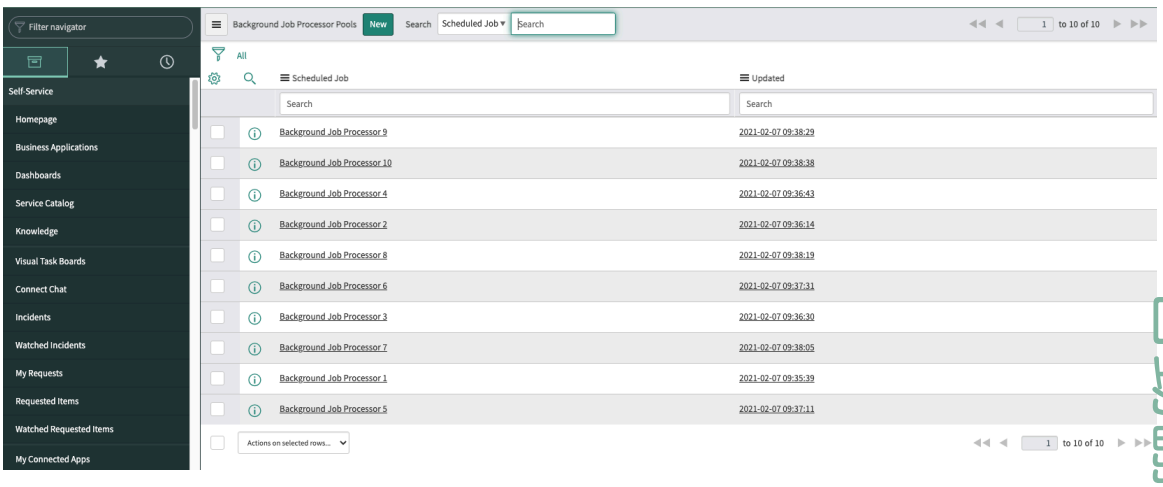
きます。[最大同時実行スレッド数] を 1 つのアサインルールジョブレコードに設定すると、すべての [アサインルールを再適用] ジョブタイプが順番に処理されます。

逆に、インスタンスのノード数が多い場合はこの値を増やすことができますが、その変更を行うには、スケジュール済みジョブもさらに追加する必要があります。

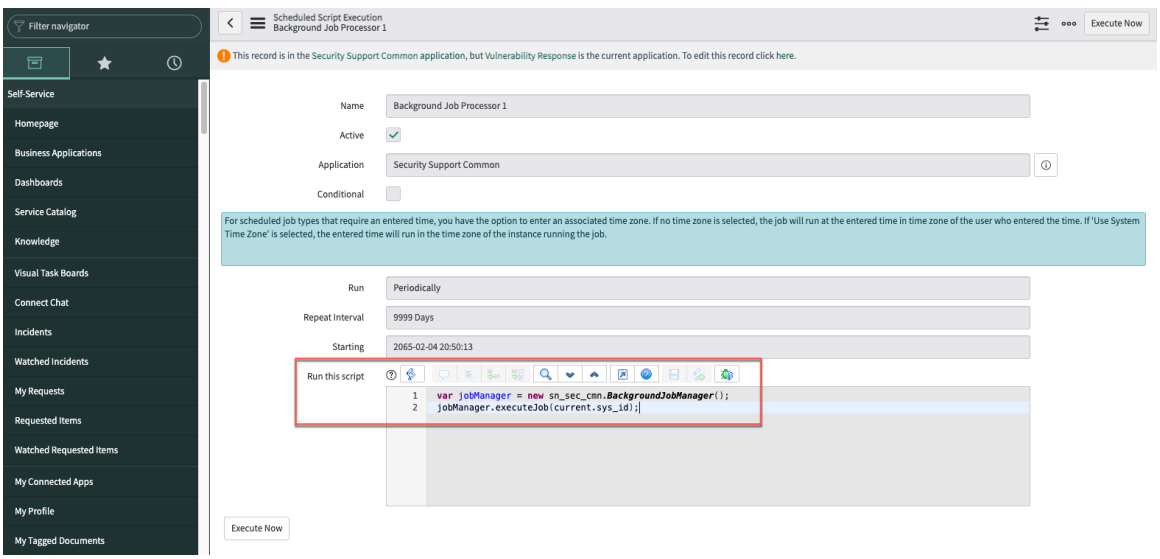
スケジュール済みジョブの数を増やすには、システムプロパティの増分値と一致するまで何度でもスケジュール済みジョブを複製します。たとえば、デフォルトで 10 個のスケジュール済みジョブがあるとします。その場合、20 個のジョブが必要な場合は、ジョブを 10 回複製する必要があります。

Now Platform® に付属している処理用の 10 個のスケジュール済みジョブが sn_sec_cmn_background_job_processor_pool テーブルに表示されます。

3. フィルターナビゲーターで、「**sn_sec_cmn_background_job_processor_pool.list**」と入力します。



4. コピーするジョブをクリックし、ジョブの数がシステムプロパティの増分値と一致するまで必要なだけ複製します。



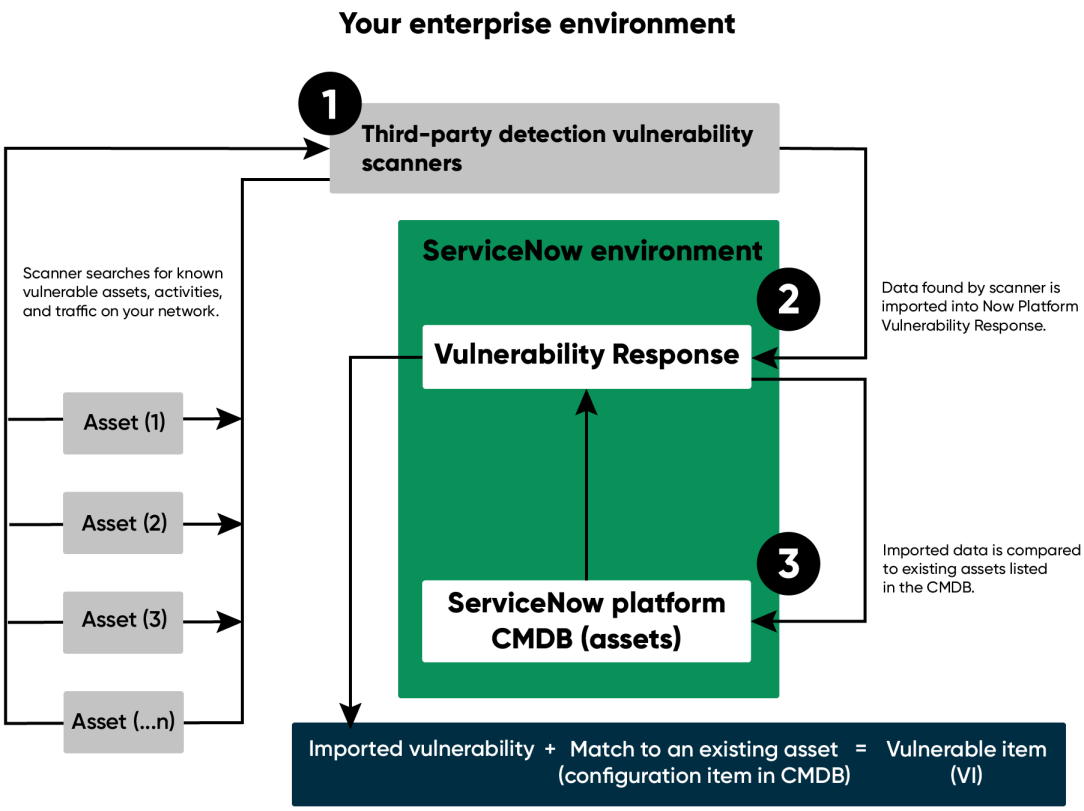
5. スケジュール済みジョブを定義したら、コピーしたジョブの「sn_sec_cmn_background_job_processor_pool」リストで [新規] をクリックして参照を追加します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 の統合

脆弱性対応 には、サードパーティ統合のサポートが含まれています。このセクションには、独自の統合を開発するための基本的なガイドラインが用意されています。

サードパーティ統合



脆弱性情報データベース (NVD) からインポートされた脆弱性とサードパーティスキャナーからの検出データは、CMDB の資産で調整されます。インポートされた脆弱性が既存の資産と一致する場合、脆弱性一致アイテムが作成されます。脆弱性一致アイテムは、修復のためのタスクに自動的にグループ化され、ビジネスコンテキストでリスクスコアが付けられ、優先順位が付けられ、修復のために適切なチームにアサインされます。

注:

サードパーティ統合は個別に扱われます。現在の環境で複数のサードパーティ統合アプリケーションが使用されている場合、統合全体での脆弱性一致アイテム (VI) の重複排除は行われません。たとえば、Rapid7 と Qualys の間では VI の重複排除はできません。

ただし、IP やポートなどの間で重複排除を行うため、サードパーティのスキャナー (Qualys など) と ServiceNow インスタンス内の VI の間では検出数の不一致が想定されます。

アプリケーション脆弱性対応 によりサポートされているサードパーティ統合については、「他のアプリケーションとの アプリケーション脆弱性対応 の統合」を参照してください。

- CISA Known Exploit Vulnerability (KEV) Integration
- Microsoft Threat and Vulnerability Management 脆弱性統合の概要
- 脆弱性対応 との HCL BigFix パッチオーケストレーション統合の概要
- 脆弱性対応 Patch Orchestration Integration with Microsoft SCCM の概要

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- NVD 統合の概要
- Qualys Vulnerability Integration
- Rapid7 脆弱性統合の概要
- Shodan Exploit Integration
- Tenable 脆弱性統合の概要
- Microsoft Security Response Center ソリューション統合

  Microsoft セキュリティレスポンスセンターソリューション統合 は 脆弱性ソリューション管理 で使用できます。Microsoft セキュリティレスポンスセンターソリューション統合 と Red Hat Solution Integration のインストールと構成については、「脆弱性対応のソリューション管理アプリケーションのインストール」を参照してください。セットアップアシスタント内から、Microsoft セキュリティレスポンスセンターソリューション統合 および Red Hat Solution Integration をオンデマンドで構成、編集、スケジュール設定、および起動できます。

統合に関するその他の注意事項

統合に対する複数の展開がサポートされている場合は、「統合のためのドメインセパレーションインポートの作成」を参照してください。

- セットアップアシスタント内から、多くの統合アプリケーションをオンデマンドでインストール、構成、スケジュール設定、および起動できます。
- セットアップアシスタントから Rapid7 脆弱性統合 アプリケーションをインストールできますが、セットアップアシスタント内からこの統合を構成することはできません。詳細については、「Rapid7 脆弱性統合 をインストールする」を参照してください。
- Tenable の 脆弱性対応の Tenable アプリケーションは、Tenable によって作成され、管理されます。次の場所にあるドキュメントを参照してください。 脆弱性対応の Tenable.

統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、 脆弱性対応のバージョン 18.2.4 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

VR v17.1 以降、以下の統合プロセスステータス名が更新されています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

V17.1 より前のステータス名	V17.1 以降のステータス名
処理中	取得中
WaitComplete	待機中/処理中

注:
ダウンロードされて処理された添付ファイルを表示できます。統合実行のステータスが [waitcomplete] の場合は、完了した統合の割合が表示されます。

[store-future: BEGIN review]脆弱性対応 v22.1.2 以降、除外ルールで脆弱性を取り込みから除外することができます。さらに、Rapid7、Qualys、脆弱性対応の Tenable、Microsoft Defender Threat and Vulnerability Management 統合を実行したときや、脆弱性を手動で取り込んだときに、除外された検出数を表示することもできます。この情報は、統合実行の画面の [検出] タブからアクセスできます。詳細については、「除外ルールの概要」と「除外ルールを作成する」を参照してください。[End]

手動で作成された統合

必要に応じて、ServiceNow Store アプリケーションとして利用できない他の統合を追加できます。詳細については、「脆弱性統合を手動で作成する」を参照してください。

NVD 統合の概要

NVD 統合では、National Institute of Standards and Technology (NIST) 脆弱性情報データベース (NVD) 製品からインポートしたデータを使用して、コードの欠陥の影響と優先度を判断できます。この統合は、脆弱性対応 の初期設定の一部として、サードパーティのスキャナー製品を使用してインスタンスに脆弱性データをインポートする前に実行します。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

NIST NVD は、共通脆弱性識別子 (CVE) と共通プラットフォーム一覧 (CPE) の両方のデータを収集し、そのデータを Now Platform で利用できるようにします。脆弱性対応 と簡単に統合し、CVE と CPE の脆弱性をマッピングして、インスタンスでデータを拡張します。

重要:
統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

インストール後、NIST National Vulnerability Database Integration-API (CVE のみ) 統合がスケジュール済みジョブとして自動的に呼び出され、毎日実行されます。スケジュール済みジョブを手動で実行することもできます。スケジュール済みジョブでは、インスタンスを他の脆弱性管理システムと同期させることで、脆弱性修復ライフサイクルを簡素化します。

ヒント:
本番インスタンスでこのプラグインをアクティブ化するには、別のライセンスが必要になる場合があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

利用可能バージョン

リリースバージョン	リリースノート
脆弱性対応 Integration with NVD v1.2	

NVD と CWE の統合による脆弱性データの初期インポート

1. CWE Comprehensive 2000 統合を使用して、CWE データの初期インポートを実行します。

   「CWE レコードの更新のためのスケジュール済みジョブの構成および実行」を参照してください。デフォルトでは、統合レコードから [オンデマンド] で CWE 更新を実行します。これを構成する必要があります。

   注:
   NVD データベースの更新の前に実行するように CWE の更新をスケジュールします。NVD 更新のデフォルト日は [毎週] [月曜日] です。

2. 脆弱性対応 Integration with NVD アプリケーションがインストールされ、NIST National Vulnerability Database Integration - API (CVE のみ) または NIST National Vulnerability Database Integration - API (CVE および CPE) のいずれかから、初期データが正常にインポートされたことを確認します。

   CPE の場合、NIST National Vulnerability Database Integration - API (CPE のみ) からの初回データインポートが正常に完了していることを確認します。

   本番インスタンスでこのプラグインをアクティブ化するには、別のライセンスが必要になる場合があります。プラグインをインストールすると、NIST National Vulnerability Database Integration - API (CVE のみ) がデフォルトで有効になります。これは、毎日実行されます。詳細については、「脆弱性対応 Integration with the NIST National Vulnerability Database のインストール」を参照してください。

3. サードパーティのライブラリはスケジュール済みジョブとして更新されます。サードパーティとの統合の詳細については、脆弱性対応 の統合 の統合ドキュメントを参照してください。

インポートされた脆弱性データと脆弱性一致アイテムの概要

Now Platform インスタンスでは、インポートされた各脆弱性は、Qualys などのサードパーティスキャナー製品のソースライブラリの脆弱性エントリーで示されます。インスタンスでインポートおよび更新される脆弱性一致アイテム (VI) は、Qualys ライブラリなどのサードパーティライブラリを参照します。サードパーティライブラリも NVD を参照できます。

たとえば、Qualys などの製品からサードパーティの脆弱性データを取り込むと、QID (Qualys 識別子) を参照する VI が取り込まれます。Qualys の場合、その QID は NVD ライブラリの CVE を参照します。脆弱性対応 アプリケーションの修復タスクまたは脆弱性一致アイテムレコードでその QID をクリックし、NVD と CWE の統合を実行してデータを取り込むと、現在の拡張された脆弱性データが表示され、VI と CVE、CWE、および CPE 間の関係を確認できます。

独自のライブラリを持つ Qualys などのサードパーティスキャナー製品を実行する前に、少なくとも NIST National Vulnerability Database Integration - API (CVE のみ) 統合 (CISA 関連の詳細も含む) と CWE 統合をインストールして実行し、脆弱性データを取り込む必要があります。これらの NVD および CWE データインポートは、データをインポートする前にサードパーティ製品を使用して 脆弱性対応 または アプリケーション脆弱性対応 データを拡張します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

NVD、CWE、およびサードパーティライブラリの管理と表示に関する詳細については、「NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理」および「脆弱性対応 脆弱性ライブラリの表示」を参照してください。

NVD が正常にインポートされたことを確認したら、脆弱性データ CWE レコードの更新のためのスケジュール済みジョブの構成および実行 をさらに拡張します。

サードパーティ製品を使用して脆弱性データをインポートする前に、NVD と CWE のインポートを実行します。サードパーティのライブラリはスケジュール済みジョブとして更新されます。サードパーティとの統合の詳細については、脆弱性対応 の統合 の統合ドキュメントを参照してください。

NVD 統合の表示

NVD 統合を表示するには、次に移動します: 脆弱性対応またはアプリケーション脆弱性対応 > アドミニストレーション > 統合.

ベースシステムには、次の統合が含まれています。

> **注:**
> NIST National Vulnerability Database Integration - API (CVE のみ) 統合のみがデフォルトで有効化されています。

NVD 統合

統合	説明
NIST National Vulnerability Database Integration - API (CVE のみ)	NIST NVD 脆弱性データ (CVE) のみを取得します。デフォルトでは、この統合は毎日実行されるように自動的に設定されます。
NIST National Vulnerability Database Integration-API (CPE のみ)	NIST NVD から CPE データを取得します。この統合は、デフォルトでは非アクティブです。 正式名の形式、システムで名前を確認する方法、およびテキストとテストを名前にバインドするための説明形式を含む CPE データをキャプチャする場合は、この統合をアクティブ化します。この情報は [脆弱なソフトウェア (Vulnerable Software)] に保存されます。 この統合は毎日実行するように設定され、デフォルトでは非アクティブになっています。この統合をアクティブ化するには、「NIST National Vulnerability Database-API (CPE のみ) のアクティブ化」を参照してください。
NIST National Vulnerability Database Integration-API (マッピングされていない CPE)	NIST NVD からフェッチされた CVE に関連付けられている CPE データを取得します。この統合は、デフォルトでは非アクティブです。 正式名の形式、システムで名前を確認する方法、およびテキストとテストを名前にバインドするための説明形式を含む CPE データをキャプチャする場合は、この統合をアクティブ化します。この情報は、NVD 脆弱性エントリーレコード関連リストに格納されます。この統合はオンデマンドで実行するように設定され、デフォルトでは非アクティブになっています。この統合をアクティブ化するには、「NIST National Vulnerability Database-API (マップされていない CPE) のアクティブ化」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重要:
「NIST National Vulnerability Database Integration-API (CVE および CPE)」統合は非推奨になりました。

統合実行状況については、「(National Vulnerability Database) NVD Integration インポート実行状況の表示」を参照してください。

NVD 統合の準備

統合を成功させるには、統合前のタスクを計画して慎重に実行する必要があります。これらのタスクを実行して、統合の準備をします。NVD 統合は、NIST 脆弱性情報データベース (NVD) に精通していることを前提としています。

始める前に
必要なロール：admin

このタスクについて

注:
NVD 統合を実行する前に、要件に基づいて必要な構成変更を行います。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

CWE レコードの更新のためのスケジュール済みジョブの構成および実行

CWE からのデータのインポートにより、インスタンスの脆弱性データがさらに強化されます。脆弱性をエスカレートする必要があるかどうかを決定するときは、共通脆弱性タイプ一覧 (CWE) データベースからダウンロードした CWE レコードを参照用に使用します。この統合は、脆弱性対応 の初期設定の一部として、サードパーティのスキャナー製品を使用してインスタンスに脆弱性データをインポートする前に実行します。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

注:
NVD データベースの更新の前に実行するように CWE の更新をスケジュールします。NVD 更新のデフォルト日は [毎週] [月曜日] です。

定期的に共通脆弱性タイプ一覧データベースから共通の脆弱性レコードを更新します。必要に応じて、デフォルトのスクリプトを更新するか、独自のスクリプトを作成することもできます。

各 CWE レコードには、脆弱性を説明する関連するナレッジ記事も含まれています。共通脆弱性タイプ一覧のページから脆弱性をエスカレートすることはできません。

- admin ロールを持っている場合は、スケジュール済みジョブにリポジトリを追加できます。
- sn_vul.vulnerability_read がある場合は、スケジュール済みジョブを実行できます。
- sn_vul.vulnerability_write がある場合は、スケジュール済みジョブの詳細を編集できます。

このタスクについて
統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、 脆弱性対応のバージョン 18.2.4 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 統合.
2. **[CWE Comprehensive 2000** 統合 **(CWE Comprehensive 2000 Integration)]** スケジュール済みジョブを選択します。
3. 必要に応じてフィールドを変更します。

脆弱性統合フォーム

フィールド	説明
名前	スケジュール済みジョブの名前。
有効	スケジュール済みジョブがアクティブかどうかを示します。ジョブを特定の期間実行しない場合は、使用するパラメーターを設定してジョブを非アクティブ化することができます。
実行	ジョブを実行する頻度。このフィールドの設定に基づいて後続のフィールドが表示または非表示になります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: CWE の更新は、デフォルトでは [オンデマンド] です。NVD 更新前のスケジュールされた期間に設定します。 次の選択肢があります。 ○ 日次：時刻を選択します。 ○ 週次：(最も一般的な選択肢) 日付と時刻を選択します。 ○ 月次：日付と時刻を選択します。 ○ 定期的：繰り返し間隔と開始日時を選択します。 ○ 1 回：開始日時を選択します。
曜日	スケジュール済みジョブを実行する日付。 [実行] フィールドで [週次 **(Weekly)]** を選択した場合、このフィールドには曜日が表示されます。[実行] フィールドで [月次 **(Monthly)]** を選択した場合、このフィールドには月日が表示されます。 注: NVD データベースの更新の前に実行するように CWE の更新をスケジュールします。NVD 更新のデフォルト日は [毎週] [月曜日] です。
時刻	スケジュール済みジョブを開始する時刻。 注: NVD データベースの更新の前に実行するように CWE の更新をスケジュールします。NVD 更新のデフォルト時刻は 01:00:00 です。
統合スクリプト	[データソース] 関連リストで指定されたデータソースからデータを取得するためのスクリプト。
ソース統合	[読み取り専用]
ソースインスタンス	[読み取り専用]
アプリケーション	[読み取り専用] スケジュール済みジョブを実行するアプリケーションの名前。
繰り返し間隔	スケジュール済みジョブが再度実行されるまでの日数と時間。このフィールドは、[実行] リストから [定期的] が選択されている場合に表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
開始中	定期的な更新を開始する日時。このフィールドは、[実行] リストから [定期的] が選択されている場合に表示されます。
条件付き	条件付きパラメーターを追加するチェックボックス。
条件	スケジュール済みジョブを実行する条件。このフィールドは、[条件付き **(Conditional)**] チェックボックスがオンになっている場合に表示されます。
プロセッサ戦略をレポート	データを取得してスケジュール済みジョブを処理するための戦略。 ○ [統合スクリプト] フィールドのスクリプトを使用して [データソース] 関連リストのデータソースからデータを取得するには、[データソース添付ファイル] を選択します。 ○ [レポートプロセッサスクリプト **(Report Processor script)**] フィールドでカスタムプロセッサを選択するには、[カスタムレポートプロセッサ] を選択します。
プロセッサをレポート	スケジュール済みジョブの実行時に実行されるスクリプト。このフィールドは、[プロセッサ戦略をレポート] リストで [カスタムレポートプロセッサ] が選択されている場合に表示されます。
プロセッサ生成スクリプト	レポートプロセッサをビルドするスクリプト。このフィールドは、[プロセッサ戦略をレポート] リストで [カスタムレポートプロセッサ] が選択されている場合に表示されます。

4. ヘッダーを右クリックして、変更を保存します。
5. スケジュール済みジョブを直ちに実行するには、[今すぐ実行] をクリックします。
脆弱性統合ビューに戻ります。
6. インポートの進行状況を監視するには、**[CWE Comprehensive 2000** 統合 **(CWE Comprehensive 2000 Integration)]** スケジュール済みジョブを再度選択し、[脆弱性統合実行] タブを選択します。

「脆弱性対応 脆弱性ライブラリの表示」を参照して、インポートされたエントリーを確認します。

脆弱性対応 **Integration with the NIST National Vulnerability Database** のインストール

インスタンスで統合を実行する前に、インストールと構成のステップを完了して、脆弱性対応 が NIST 脆弱性情報データベース (NVD) 製品と適切に統合されるようにします。このアプリケーションは別のサブスクリプションとして利用できます。

始める前に

インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

セットアップタスク	説明
脆弱性対応 アプリケーションがインストールされ、アクティブ化されていることを確認します。	このアプリケーションがアクティブ化されていることを確認するには、次の場所に移動します サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応 のインストール」を参照してください。
インスタンスに必要な ServiceNow ロールがあることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。 • まだアサインされていない場合、システムアドミニストレーター [admin] はアプリケーションをインストールし、ユーザーを 脆弱性対応 の脆弱性マネージャーまたは アプリケーション脆弱性対応 のアプリケーションセキュリティマネージャーグループにアサインします。脆弱性対応 のグループロールの詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。アプリケーション脆弱性対応 のグループロールの詳細については、「アプリケーション脆弱性対応 のユーザーロールおよびロール」を参照してください。 • 脆弱性マネージャーまたはアプリケーション セキュリティマネージャーは構成を監督し、期待される結果を検証します。

必要なロール：admin

注:
NVD 統合を実行する前に、要件に基づいて必要な構成変更を行います。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

手順

1. NVD 統合をインストールするインスタンスにログインします。
2. ServiceNow Store に移動します。
3. ServiceNow Store で、NVD の脆弱性対応統合アプリケーションを検索します。
4. アプリケーションタイルを選択します。
   インストールしているアプリケーションに関する詳細情報が表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

> **注:**
> 該当する場合は、[他の要件] および [依存関係] セクションを読むことを検討してください。

5. [アプリを要求] を選択して、Now Support ログイン認証情報を入力します。
6. [取得] を選択します。
7. [インスタンス名] と [インスタンスの理由] を入力し、[インスタンスを検証] を選択します。
8. [要求] を選択します。
   詳細なインストール手順が記載されたメールが届きます。
9. 次のように移動する。 **All** (すべて) > システムアプリケーション > アプリケーション > **All** (すべて).
10. アプリケーションを見つけて選択し、[インストール] を選択します。
    アプリケーションはインスタンスに自動でインストールされます。

次のタスク
初期インストール後の変更については、「オプションの NVD 統合の変更とアクティビティ」を参照してください。

NIST National Vulnerability Database-API (マップされていない **CPE)** のアクティブ化

フェッチされた共通脆弱性識別子 (CVE) データの共通プラットフォーム一覧 (CPE) データを取り込む場合は、オンデマンドスケジュール済みジョブで完全なデータインポートを実行できます。

始める前に
National Institute of Standards and Technology (NIST) National Vulnerability Database Integration (NVD)–API (マップされていない CPE) 統合では、正式名の形式、システムで名前を確認する方法、およびテキストとテストを名前にバインドするための説明形式を含むデータをキャプチャします。この情報は、NVD 脆弱性エントリーレコード関連リストに格納されます。

必要なロール：sn_vul.vulnerability_admin またはアプリケーションセキュリティマネージャー

手順
1. 次のように移動する。 **All** (すべて) > 脆弱性対応またはアプリケーション脆弱性対応 > **NVD** > 統合.
2. NIST National Vulnerability Database Integration - API (マップされていない CPE) 統合を選択します。
3. [アクティブ] チェックボックスをオンにします。

> **注:**
> この統合は、オンデマンドで実行するように事前設定されています。この統合をアクティブにすると、NIST NVD Integration-API (CVE のみ) 統合の後に自動的に実行されます。他の統合パラメーターを変更するには、ServiceNow と 脆弱性対応 の両方の専門知識が必要であり、不完全なデータになる可能性があります。

   a. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 統合.
   b. NIST National Vulnerability Database Integration - API (マップされていない CPE) 統合を選択します。
   c. [**Integration Details**] を選択します。
   [次以降にインポート] フィールドの値に関係なく、取得されたすべての CVE の CPE が取得されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [今すぐ実行] を選択して、最初の完全なサポート統合を実行します。
最初のインポートが完了すると、スケジュールされたデルタデータのインポートが再開されます。
統合実行状況については、「(National Vulnerability Database) NVD Integration インポート実行状況の表示」を参照してください。

NIST National Vulnerability Database-API (CPE のみ) のアクティブ化

共通プラットフォーム一覧 (CPE) データを取り込む場合は、日次スケジュール済みジョブで完全なデータインポートを実行できます。

始める前に
National Institute of Standards and Technology (NIST) National Vulnerability Database Integration (NVD)–API (CPE のみ) 統合では、正式名の形式、システムで名前を確認する方法、およびテキストとテストを名前にバインドするための説明形式を含む (CPE) データをキャプチャします。この情報は [脆弱なソフトウェア] テーブルに保存されます。

必要なロール：sn_vul.vulnerability_admin またはアプリケーションセキュリティマネージャー

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応またはアプリケーション脆弱性対応 > **NVD** > 統合.
2. NIST National Vulnerability Database Integration - API (CPE のみ) 統合を選択します。
3. [アクティブ] チェックボックスをオンにします。
   - この統合は、毎日実行するように事前設定されています。他の統合パラメーターを変更するには、ServiceNow の専門知識が必要であり、不完全なデータになる可能性があります。
   - この統合を有効にすると、NIST National Vulnerability Database Integration - API (CVE のみ) 統合および NIST National Vulnerability Database Integration - API (マッピングされていない CPE) 統合が自動的にアクティブになり、その実行フィールドがオンデマンドに設定されます。
   - さらに、NIST National Vulnerability Database Integration- API (CPE のみ) の統合実行が正常に完了すると、NIST National Vulnerability Database Integration-API (CVE のみ) が自動的にトリガーされます。NIST National Vulnerability Database Integration- API (CVE のみ) が正常に完了すると、NIST National Vulnerability Database Integration-API (マッピングされていない CPE) が自動的にトリガーされます。

   注:
   NIST National Vulnerability Database Integration - API (CPE のみ) 統合の [次以降にインポート] 日付フィールドは、デフォルトでは空です。過去 357 日間のデータをフェッチするには、空のままにします。

   NVD スキャンからの初回インポート中に履歴データを取得するには、NIST National Vulnerability Database Integration - API (CPE のみ) 統合レコードで開始日を設定します。

   a. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 統合.
   b. NIST National Vulnerability Database Integration - API (CPE のみ) 統合を選択します。
   c. [**Integration Details**] を選択します。
   d. [次以降にインポート] フィールドの値として、取得する最も早い日付を設定します。
   インポートが成功するたびに、この日付は選択された日の日時にリセットされます。
4. [今すぐ実行] を選択して、最初の完全なサポート統合を実行します。
最初のインポートが完了すると、スケジュールされたデルタデータのインポートが再開されます。
統合実行状況については、「(National Vulnerability Database) NVD Integration インポート実行状況の表示」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

オプションの **NVD** 統合の変更とアクティビティ

NVD 統合専用のオプションの変更を構成します。

> **注:**
> ここに記載されている以外のその他の NVD 統合構成を変更するには、ServiceNow および 脆弱性対応 の高度な専門知識が必要であり、製品ドキュメントの範囲を超えています。

NVD 統合インポートの手動実行

最初のインポートに失敗した場合、またはスケジュールされた最初のインポートを待ちたくない場合は、日次または週次スケジュール済みジョブから独立して完全なデータインポートを実行できます。

始める前に

> **注:**
> NIST National Vulnerability Database Integration-API (CPE のみ) 統合と NIST National Vulnerability Database Integration-API (マッピングされていない CPE) 統合はデフォルトで無効にされています。詳細については、「NIST National Vulnerability Database-API (CPE のみ) のアクティブ化」と「NIST National Vulnerability Database-API (マップされていない CPE) のアクティブ化」を参照してください。

必要なロール：sn_vul.vulnerability_admin

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応またはアプリケーション脆弱性対応 > アドミニストレーション > 統合.
2. 統合を選択します (NIST National Vulnerability Database Integration - API (CVE のみ) など)。
3. [今すぐ実行] を選択します。

   > **注:**
   > NIST National Vulnerability Database Integration-API (マップされていない CPE) 統合がアクティブ化されている場合、CPE データは NVD 脆弱性エントリの [脆弱なソフトウェア] 関連リストに保存されます。「脆弱性対応脆弱性フォームフィールド」を参照してください。

4. 統合実行状況については、「(National Vulnerability Database) NVD Integration インポート実行状況の表示」を参照してください。

(National Vulnerability Database) NVD Integration インポート実行状況の表示

[脆弱性統合実行] 関連リストを使用して、統合実行の成功を確認し、問題を特定して、修復の決定を通知します。

始める前に

NVD 統合インポート実行状況を表示するには次のステップを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 脆弱性対応 および NVD の脆弱性対応統合アプリケーションをインストールして設定する必要があります。
- NVD 統合インポートが実行されている必要があります。NIST National Vulnerability Database Integration-API (CVE のみ) 統合がデフォルトで実行されます。

> **注:**
> NIST National Vulnerability Database Integration-API (CPE のみ) 統合と NIST National Vulnerability Database Integration-API (マッピングされていない CPE) 統合はデフォルトで無効にされています。詳細については、「NIST National Vulnerability Database-API (CPE のみ) のアクティブ化」と「NIST National Vulnerability Database-API (マップされていない CPE) のアクティブ化」を参照してください。

必要なロール：sn_vul.vulnerability_admin またはアプリケーションセキュリティマネージャー

このタスクについて

統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。

この通信ミスを回避するために、 脆弱性対応のバージョン 18.2.4 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは [最後の処理済みレコード **(Last Record Processed)]** フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。最後の処理済みレコードが 1 時間以上前のものである場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

> **注:**
> [最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。
>
> - *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
> - *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

手順

1. NVD 統合実行状況チャートを使用していない場合は、 次のように移動 **All** (すべて) > 脆弱性対応 またはアプリケーション脆弱性対応 > アドミニストレーション > 統合.
2. 統合のリンクを選択します。
3. [脆弱性統合実行 **(Vulnerability Integration Runs)]** 関連リストを選択します。
4. すべてのインポートが成功したことを確認します。

Trouble?

実行が失敗した場合の一般的な原因は次のとおりです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- ネットワークの中断。
- データ転送の問題による、変換中のデータ破損。

これらの条件のいずれかが発生した場合は、[今すぐ実行 **(Execute Noe)]** を選択して統合を再実行します。

関連情報

脆弱性対応脆弱性フォームフィールド

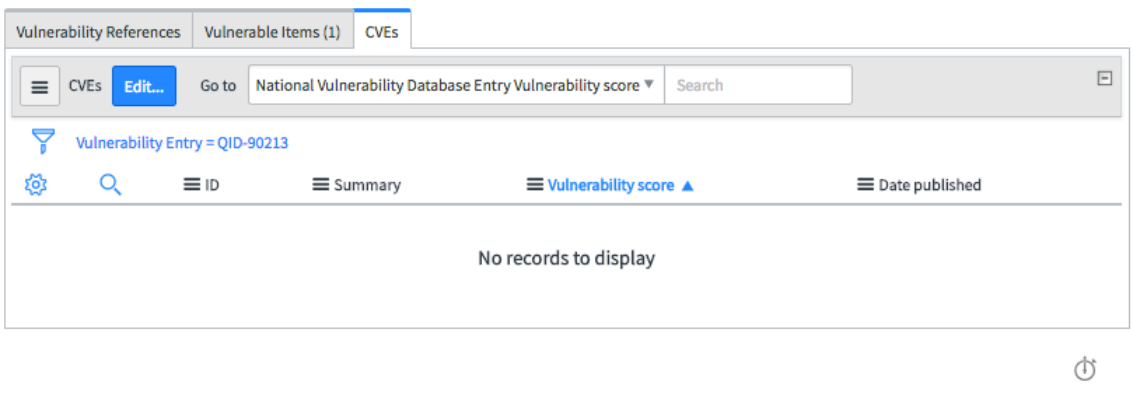
CVE をサードパーティエントリーに追加

共通脆弱性識別子 (CVE) 情報を単一のサードパーティ脆弱性に関連付けることができます。通常はサードパーティ統合インポート中に追加されますが、複数の CVE (脆弱性) を手動で追加できます。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > ライブラリー > サードパーティ.
2. レコードを開きます。
3. **[CVE]** 関連リストタブをクリックします。



4. [編集] をクリックします。
5. 追加する CVE を選択します。

> **注:**
> 条件フィルターを使用して、CVE コレクションを絞り込むことができます。

6. [保存] をクリックします。

関連情報

脆弱性対応脆弱性フォームフィールド

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 脆弱性ライブラリの表示

脆弱性情報データベース (NVD)、共通脆弱性タイプ一覧 (CWE)、またはサードパーティからインポートされた脆弱性データを表示して、修復タスクをエスカレートするかどうかを決定できます。

始める前に

必要なロール： sn_vul.remediation_owner

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > ライブラリー.

   特定のフィールドの詳細については、「脆弱性対応脆弱性フォームフィールド」を参照してください。

   次のライブラリが利用可能です。

ライブラリ	説明
NVD	NVD によって検出された脆弱性のリストで、セキュリティチェックリスト、セキュリティ関連のソフトウェアの欠陥、不適切な構成、製品名、およびエクスプロイトを含む影響度メトリクスが含まれています。
CWE	コミュニティで開発されたソフトウェアの脆弱性タイプのリスト。 各 CWE レコードには、脆弱性を説明する関連するナレッジ記事も含まれています。[共通脆弱性タイプ一覧] 画面から脆弱性をエスカレートすることはできません。これは参照用です。
サードパーティ	インスタンスにインポートされたサードパーティ脆弱性のリスト。関連する参照、脆弱性一致アイテム、エクスプロイト、および CVE のリストが含まれています。

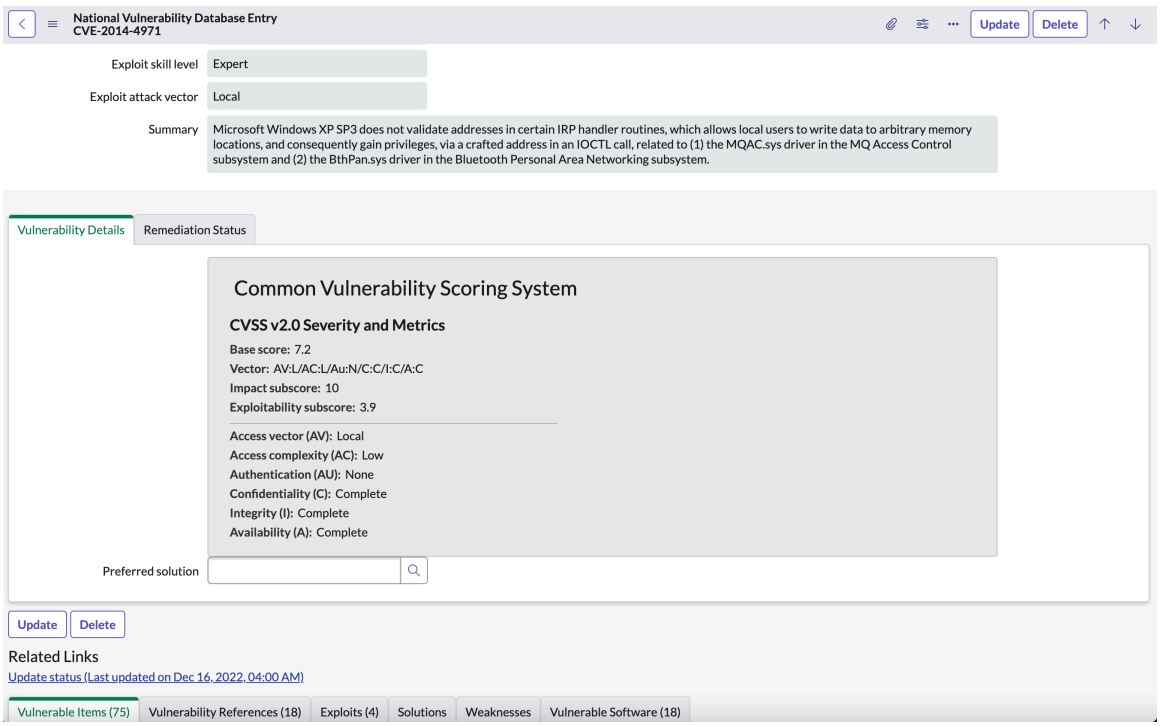
2. ライブラリを選択して、脆弱性を表示します。
3. リスト内のリンクをクリックしてレコードを開きます。

   National Vulnerability Database エントリーライブラリの CVE レコード。詳細については、[関連リンク] を参照してください。データをインポートした後、脆弱性を選択し、脆弱性一致アイテムとの関係、エクスプロイト、考えられるソリューション、潜在的なパッチ、および HI ナレッジベースの KB 記事への参照を調べることができます。脆弱性ソリューション管理 がインストー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ルされている場合、NVD レコードの優先ソリューションが使用可能であれば、それを表示できます。



CISA Known Exploit Vulnerability (KEV) Integration

脆弱性対応 と CISA Known Exploit Vulnerability (KEV) カタログの統合は、これらの脆弱性を効果的に優先順位付けして修正するのに役立ちます。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

CISA は、政府機関や企業に対して頻繁に悪用される脆弱性を緊急に優先的に修復します。

CISA について

Cybersecurity & Infrastructure Security Agency (CISA) は、最も悪用されている脆弱性に関するレポートを公開するアメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁です。脆弱性対応と簡単に統合して、一般的な脆弱性とエクスポージャー (CVE) の脆弱性をマッピングして、インスタンスのデータを拡張します。この情報は、[サードパーティ脆弱性エントリー] テーブルにロールアップされます。最も早い期日が脆弱性一致アイテムへのロールアップに考慮されます。

> **注:**
> CISA によって取得された CVE の **[CISA が存在します (CISA Exists)]** チェックボックス。

CISA 統合から取得される値：

- CVE ID
- 期日
- 追加された日付
- ベンダー/プロジェクト

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 製品
- 既知のランサムウェア (脆弱性対応の v21.0 以降では、 [ランサムウェアキャンペーンで使用されることがわかっている **(Known To Be Used in Ransomware Campaigns)]** 新しいフィールドが、CISA Known Exploited Vulnerabilities (KEV) カタログから取り込まれます。これは、National Vulnerability Entry データベーステーブルの [既知のランサムウェア] フィールドのフラグによって示されます。このフラグは、共通脆弱性識別子 (CVE) レベルで設定され、サードパーティエントリ (TPE) にロールアップされます。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

スケジュール済みジョブ

CISA 統合は、日次スケジュール済みジョブとして自動的に呼び出されます。スケジュール済みジョブを手動で実行することもできます。スケジュール済みジョブでは、インスタンスを他の脆弱性管理システムと同期させることで、脆弱性修復ライフサイクルを簡素化します。

利用可能バージョン

リリースバージョン	リリースノート
脆弱性対応 v16.5、v18.0 CISA v1.0、v1.2 との 脆弱性対応 統合	

CISA 統合の表示

CISA 統合を表示するには、次に移動します: 脆弱性対応 > アドミニストレーション > 統合 > **CISA Known Exploit Vulnerability Integration**.

ベースシステムには、次の統合が含まれています。

注:
デフォルトでは、CISA 統合のみが有効にされています。

CISA 統合

統合	説明
Cybersecurity & Infrastructure Security Agency (CISA) との統合	CISA 脆弱性データ (CVE) を取得し、既存の脆弱性データを拡張します。この統合は、毎日実行するように自動的に設定されます。

サードパーティの脆弱性データを表示する方法については、「脆弱性対応 脆弱性ライブラリの表示」を参照してください。

CISA 統合の準備

統合を成功させるには、統合前のタスクを計画して慎重に実行する必要があります。これらのタスクを実行して、統合の準備をします。CISA Known Exploit Vulnerability Integrationでは、アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁 (CISA) に精通していることを前提としています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_vul.vulnerability_admin

このタスクについて

注:
CISA 統合を実行する前に、要件に基づいて必要な構成変更を行います。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、 脆弱性対応のバージョン 18.2.4 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

ServiceNow® Vulnerability Response Integration with CSA アプリケーションのインストール

インスタンスで統合を実行する前に、インストールと構成のステップを完了して、Cybersecurity & Infrastructure Security Agency (CISA) Known Exploited Vulnerability アドバイザーと 脆弱性対応 を統合する必要があります。このアプリケーションは別のサブスクリプションとして利用できます。

始める前に
インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

セットアップタスク	説明
脆弱性対応 アプリケーションがインストールされ、アクティブ化されていることを確認します。	このアプリケーションがアクティブ化されていることを確認するには、次の場所に移動します サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

セットアップタスク	説明
	アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応 のインストール」を参照してください。
脆弱性対応 Integration with NVD アプリケーションがインストールされ、アクティブ化されていることを確認します。	このアプリケーションがアクティブ化されていることを確認するには、次の場所に移動しますサブスクリプション管理 > サブスクリプションインスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応 Integration with the NIST National Vulnerability Database のインストール」を参照してください。
インスタンスに必要な ServiceNow ロールがあることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。 • まだアサインされていない場合、システムアドミニストレーター [admin] はアプリケーションをインストールし、ユーザーを 脆弱性対応の脆弱性マネージャーにアサインします。脆弱性対応 のグループロールの詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。 • 脆弱性マネージャーは構成を監督し、期待される結果を検証します。

必要なロール：admin

手順

1. Vulnerability Response Integration with CISA をインストールするインスタンスにログインします。
2. ServiceNow Store に移動します。
3. ServiceNow Storeで、Vulnerability Response Integration with CISA アプリケーションを検索します。
4. アプリケーションタイルを選択します。
   インストールしているアプリケーションに関する詳細情報が表示されます。

   注:
   該当する場合は、[他の要件] および [依存関係] セクションを読むことを検討してください。

5. [アプリを要求] を選択して、Now Support ログイン認証情報を入力します。
6. [取得] を選択します。
7. [インスタンス名] と [インスタンスの理由] を入力し、[インスタンスを検証] を選択します。
8. [要求] を選択します。
   詳細なインストール手順が記載されたメールが届きます。
9. 次のように移動する。 システムアプリケーション > アプリケーション.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

10. アプリケーションを見つけて選択し、[インストール] を選択します。
アプリケーションはインスタンスに自動でインストールされます。

次のタスク

注:
CISA 統合の場合、設定は必要ありません。

Exploit Prediction Scoring System (EPSS) 統合について

脆弱性対応 と EPSS の統合の概要です。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

概要

Exploit Prediction Scoring System (EPSS) 統合は、First.org から一般的な脆弱性とエクスポージャー (CVE) に関連する EPSS データをインポートし、脆弱性に優先順位を付けて修復します。詳細については、「https://www.first.org」を参照してください。Exploit Prediction Scoring System (EPSS) は、ソフトウェアの脆弱性が実際に悪用される可能性 (確率) を推定するためのデータ主導型の取り組みです。EPSS モデルは、0 ～ 1 (0 ～ 100%) の確率スコアを生成します。スコアが高いほど、脆弱性が悪用される確率が高くなります。

EPSS 統合からのデータのインポートにより、インスタンスの NVD データがさらに強化されます。NVD レコードが存在しない場合は、CVE テーブルにプレースホルダーが作成され、同じテーブルに EPSS の詳細が追加されます。この統合は、脆弱性対応 の初期設定の一部として、サードパーティのスキャナー製品を使用してインスタンスに脆弱性データをインポートする前に実行します。

重要:
統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は VR.System です。この値は変更しないでください。

EPSS 統合を使用したデータの初期インポート

1. First.org EPSS 統合を使用して EPSS データの初期インポートを実行します。詳細については、「CVE レコードを EPSS データで更新するためスケジュール済みジョブを構成して実行する」を参照してください。

   重要:
   デフォルトでは、統合レコードから [日次] で EPSS 更新を実行します。スケジュール済みジョブとして実行する場合は設定する必要があります。

2. サードパーティのライブラリはスケジュール済みジョブとして更新されます。詳細については、「NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理」を参照してください。

   重要:
   EPSS の前に、NIST National Vulnerability Database Integration - API (CVE のみ) 統合を実行することが推奨されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サードパーティ製品を使用して脆弱性データをインポートする前に、EPSS のインポートを実行します。サードパーティのライブラリはスケジュール済みジョブとして更新されます。サードパーティとの統合の詳細については、Vulnerability Response 統合の統合ドキュメントを参照してください。

> **重要:**
> ベースシステムには、次の統合が含まれています。統合はデフォルトでアクティブになっています。

最初の実行後、ベースシステムのスケジュール済みジョブが順番に自動的に統合を実行します。スケジュール済みジョブを手動で実行することもできます。スケジュール済みジョブでは、インスタンスを他の脆弱性管理システムと同期させることで、脆弱性修復ライフサイクルを簡素化します。

EPSS 統合を有効にすると、[EPSS スコア (EPSS Score)]、[EPSS パーセンタイル (EPSS Percentile)]、および [EPSS 最終変更日 (EPSS Last Modified)] フィールドが脆弱性エントリテーブルに追加されます。既存の CVE の場合、これらのフィールドは、最初のインポートジョブが正常に完了すると自動更新されます。EPSS スケジュール済みジョブの完了後に脆弱性エントリテーブルに追加された新しい CVE がある場合、新しく追加された CVE はそのソースを EPSS として示します。スコアは、ベースシステム *Rollup EPSS score from NVD to TPEs calculator* を使用して、NVD テーブルの CVE から既存の TPE にロールアップされます。電卓を変更することもできます。詳細については、「脆弱性対応 ロールアップ算出」を参照してください。

関連情報

脆弱性対応 算出の作成

CVE レコードを **EPSS** データで更新するためスケジュール済みジョブを構成して実行する

ベースシステムのスケジュール済みジョブをカスタマイズして、CVE レコードを EPSS データで更新します。

始める前に

> **重要:**
> EPSS 統合を有効にするには、Vulnerability Response Integration with CISA (com.snc.vulnerability.cisa) プラグインをダウンロードしてアクティブ化する必要があります。

EPSS データを保存するために NVD テーブルに追加された新しいフィールドのリストを以下に示します。

- EPSS スコア (EPSS Score)
- EPSS パーセンタイル (EPSS Percentile)
- EPSS 最終変更 (EPSS Last Modified)

> **注:**
> 新しく追加されたフィールドを表示するには、要件に従ってリストビューまたはフォームビューを構成します。

必要なロール：admin

このタスクについて
EPSS 統合からのデータのインポートにより、インスタンスの NVD データがさらに強化されます。NVD レコードが存在しない場合は、CVE テーブルにプレースホルダーが作成され、同じテーブルに EPSS の詳細が追加されます。この統合は、脆弱性対応の初期設定の一部として、インスタンスに脆弱性データをインポートした後に実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
デフォルトでは、First.org EPSS 統合はアクティブステータスです。ベースシステムのスケジュール済みジョブは、デフォルトで毎日実行するように設定されています。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 統合.
2. First.org EPSS 統合を見つけて選択します。
3. 必要に応じてフィールドを変更します。
4. ヘッダーを右クリックして [保存] を選択し、変更を保存します。
5. スケジュール済みジョブをすぐに実行するには、[今すぐ実行] を選択します。
   脆弱性統合ビューに戻ります。
6. 選択 **First.org EPSS** > [脆弱性統合実行] タブ をクリックして、インポートの進行状況を表示します。
   スケジュール済みジョブが正常に完了すると、CVE で EPSS スコア、パーセンタイル、および最終変更 EPSS スコアのタイムスタンプが更新されます。

次のタスク

- 「リスク算出ビジネスルールへの EPSS スコア条件の追加」を参照してください。
- 「脆弱性対応 脆弱性ライブラリの表示」を参照して、インポートされたエントリーを確認します。

リスク算出ビジネスルールへの **EPSS** スコア条件の追加

ビジネス ルールを変更して、リスク算出に EPSS スコア条件を追加します。

始める前に

注:
脆弱性に関する EPSS 更新を脆弱性一致アイテムにロールダウンするには、次の手順が必要です。

必要なロール：sn_vul.manage_risk_score_configuration

手順

1. 次のように移動する。 **All** (すべて) > システム定義 > ビジネスルール.
2. [再計算フラグを設定 **(Set recalculate flag)**] を見つけます。

   注:
   2 つの *Set recalculate flag* ビジネスルールがあります。どちらでも使用できます。

3. [実行タイミング **(When to run)**] タブに移動します。
4. [「OR」項目を追加] を選択してから、[フィールドを選択] で [EPSS Score] を選択し、[演算子を選択] フィールドで [change] を選択します。
5. [更新] を選択します。

Microsoft Threat and Vulnerability Management 脆弱性統合の概要

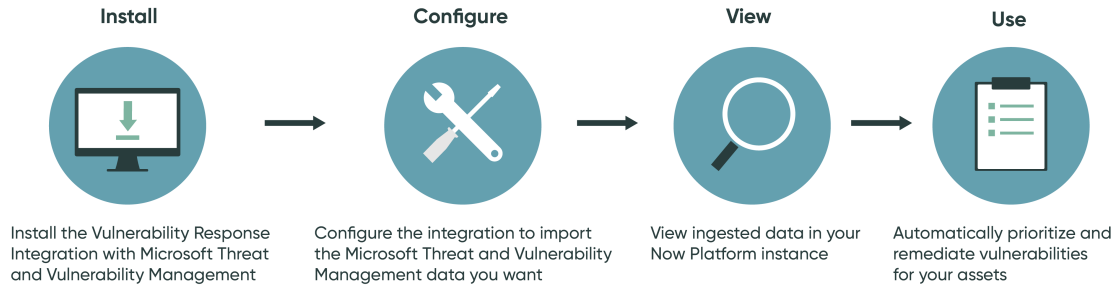
脆弱性対応 Integration with Microsoft Threat and Vulnerability Management (MS TVM) アプリケーションでは、MS TVM からインポートされたデータを使用して、資産の脆弱性の優先順位付

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

けと修正を行います。アプリケーションは ServiceNow Store の個別のサブスクリプションで利用できます。

MS TVM 脆弱性統合を使用して、資産と脆弱性に関するサードパーティのスキャナーデータをインポートできます。脆弱性対応 ダッシュボードで脆弱性と脆弱性一致アイテムに関するレポートを表示できます。



利用可能バージョン

リリースバージョン	リリースノート
脆弱性対応 Integration with MS TVM v2.2	脆弱性対応アプリケーションのリリース済バージョン、互換性、スキーマ変更について詳しくは、HI ナレッジベース記事「Vulnerability Response Compatibility Matrix and Release Schema Changes (脆弱性対応互換性マトリクスおよびリリーススキーマの変更点) [KB0856498]」 を参照してください。

ドメインセパレーションと **MS TVM**

統合を実行するドメインにユーザーをアサインして、指定されたドメインに脆弱性統合データをインポートします。MS TVM 脆弱性統合用のドメインセパレーションインポートを作成する場合は、「統合のためのドメインセパレーションインポートの作成」を参照してください。

統合に関する用語と主な機能

脆弱性一致アイテムと脆弱性

次の場合に Now Platform インスタンスに脆弱性一致アイテムが作成されます。

- サードパーティのスキャナーからインポートした脆弱性が CMDB の既存の資産 (構成アイテム) と一致する。MS TVM 製品では、これらの一致を脆弱性と呼びます。
- サードパーティのスキャナーからインポートした脆弱性が CMDB の既存の資産と一致しない。この場合、脆弱性一致アイテムとともに一致しない構成アイテム (CI) も作成されます。

  既存の CI がホストと一致しない場合、識別および調整エンジン (IRE) を使用して CI を 2 つの新しいクラスに作成することができます。それ以外の場合は、一致しない CI が [不一致] CI クラスに作成されます。詳細については、「識別および調整エンジンを使用して 脆弱性対応 の CI を作成する」を参照してください。

サードパーティ脆弱性エントリー

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

サードパーティの脆弱性エントリーは、MS TVM などのサードパーティのスキャナーからインポートされ、Now Platform インスタンスのサードパーティ脆弱性エントリーテーブルにリストされます。また、National Vulnerability Database エントリー (CVE) は MS TVM からインポートされます。これら両方のタイプのエントリーに関連付けられているエクスプロイト情報は、MS TVM から取得されます。このエクスプロイト情報はリスク計算に使用できます。

> **注:**
> サードパーティの脆弱性は、CVE が割り当てられていない脆弱性に対してのみ取得されます。MS TVM は、脆弱性に一時的な名前を追加できます (例：TVM-XXXX-XXXX)。この名前は、CVE ID が割り当てられた後に更新されます。

構成アイテム (CI)

CI は、CMDB にリストされている既存の資産です。

検出されたアイテム

検出されたアイテムは、CMDB の既存の CI と一致する MS TVM マシンインポートから取り込まれた資産です。

一致するものが見つからない場合は、CMDB の [一致しない CI] クラスに CI が作成されます。CMDB CI クラスモデルプラグインを有効にすると、識別および調整エンジン (IRE) が新しいクラスを使用して CI を作成します。詳細については、「識別および調整エンジンを使用して 脆弱性対応 の CI を作成する」を参照してください。元の一致しない CI が再分類され、検出されたアイテムレコードを更新してステータスが反映されます。検出されたアイテムにより、資産がどのように識別され、CMDB の CI にマッピングされるかを把握できます。

CI ルックアップルール

データが MS TVM からインポートされると、脆弱性対応 は自動的にマシン (資産) データを使用して CMDB 内の一致を検索します。CI ルックアップルールは CI の識別に使用され、VI が作成されると VI レコードに追加されます。

インスタンス

インスタンスは MS TVM の複数のアカウントを指します。各アカウントは、MS TVM アプリケーションのインスタンスにすることができます。

統合

統合は、MS TVM マシンとの統合など、サードパーティのソースから情報を取得するスケジュール済みジョブです。

展開

統合でマルチソースがサポートされている場合、単一の統合の存在は、統合の展開と呼ばれます。展開とは、環境全体の統合と製品のことです。たとえば、お使いの環境に MS TVM を複数展開する場合があります。

この MS TVM 統合に含まれる主な機能は次のとおりです。

- 環境全体で資産を特定し、検出された既存のアイテム、脆弱性一致アイテム、および検出レコードで CI を更新して、脆弱性に関する詳細を提供します。
- すべての MS TVM 統合でジョブを実行するタイミングをスケジュールできます。スケジュール済みジョブをオンデマンドで実行することもできます。
- 脆弱性一致アイテムをグループ化できます。
- CI ルックアップルールを設定して、サードパーティソースからの資産データを使用して CMDB 内の CI を特定する方法を定義できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

必要な **Now Platform** ロール

統合タスクには、Now Platform インスタンスで次のロールが必要です。

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

admin

システムアドミニストレーターはセットアップアシスタントを使用して MS TVM アプリケーションをインストールします。アサインされていない場合、アドミニストレーターはセットアップアシスタントで脆弱性アドミン (sn_vul.vulnerability_admin) およびその他のロールをアサインします。

sn_vul.vulnerability_admin

アサインされると、脆弱性アドミニストレーターはセットアップアシスタントで MS TVM 統合の構成を完了します。このロールは、脆弱性対応 アプリケーションとそのレコードに完全にアクセスできます。脆弱性アドミニストレーターは、インストールされたサードパーティ統合のすべての 脆弱性対応 アプリケーションとルールを構成します。

sn_vul_msft_tvm.configure_integration

このロールには、sn_vul_msft_tvm.read_integration の詳細なロールが含まれています。このロールを持つユーザーは、 Microsoft Threat and Vulnerability Management アプリケーションとの脆弱性対応統合を設定できます。

sn_vul_msft_tvm.read_integration

このロールを持つユーザーは、Microsoft Threat and Vulnerability Management アプリケーションとの脆弱性対応統合レコードのみを表示できます。

脆弱性対応グループ

デフォルトで脆弱性対応グループはセットアップアシスタントで利用可能になっています。脆弱性対応グループにアサインされたユーザーは sn_vul.read_all および sn_vul.remediation_owner ロールを自動的に継承します。

MS TVM 統合

マルチソースは、すべての MS TVM 統合でサポートされています。脆弱性対応 のセットアップアシスタントから、次の統合の複数のインスタンスを環境全体に追加して展開できます。また、セットアップアシスタントから 脆弱性対応 Integration with the MS TVM アプリケーションをインストールして設定します。

MS TVM 統合を表示するには、次に移動します: **Microsoft TVM** 脆弱性統合 > アドミニストレーション > 統合. 脆弱性対応 は、スケジュール設定された時間間隔に従ってデータをインポートするための MS TVM エンドポイントとの統合を提供します。ベースシステムには、次の統合が含まれています。

MS TVM 統合

実行シーケンス	スケジュール	統合	説明
1	日次	Microsoft TVM 推奨事項の統合	脆弱性を修正するためのすべてのアクション可能なセキュリティ推奨事

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MS TVM 統合 (続く)

実行シーケンス	スケジュール	統合	説明
			項のリストを取得します。
2	日次	Microsoft TVM 脆弱性 (CVE) 統合	National Vulnerability Database エントリーとサードパーティ脆弱性エントリーのリスト、およびそれらのエクスプロイト情報を取得します。
3	日次	Microsoft TVM マシンの統合	マシンタグを含むすべての資産 (マシン) データを Microsoft TVM から取得して、インスタンスで処理します。
4	週次 **注:** インストール後、この統合はマシンのインポート後に自動的に実行されます。	Microsoft TVM マシンの脆弱性統合 (フルインポート)	すべての資産のすべてのオープンな脆弱性を取得します。
5	日次	Microsoft TVM マシンの脆弱性統合 (データインポート)	新規、修正済み、および更新された脆弱性を含む、組織の完全な脆弱性インポートで変更されたすべての情報を取得します。

脆弱性一致アイテムは、設定したグループルール従って修復タスクにグループ化され、アサインルールに基づいて修復にアサインされます。詳細については、「脆弱性対応修復タスクとタスクルールの概要」と「脆弱性対応 アサインルールの概要」を参照してください。

CI ルックアップルール

データが MS TVM からインポートされると、脆弱性対応 は自動的にマシン (資産) データを使用して 構成管理データベース (CMDB) 内の一致を検索します。CI ルックアップルールは、CI を識別し、VI の作成時にそれらを VI レコードに追加する際に使用されます。CI ルックアップルールの詳しい仕組みについては、「脆弱性対応 サードパーティ脆弱性統合の構成アイテムを識別するための CI ルックアップルール」を参照してください。

注:
削除したルールは元に戻せません。既存のルールを削除するのではなく、無効にする必要があります。

次の MS TVM ルックアップルールはベースシステムに付属しています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- MAC_ADDRESS
- FQDN
- IP

注:
資産の IP_ADDRESS and MAC_ADDRESS には複数の値を使用できます。CI ルックアップルールでは、すべての値を照合します。

検出されたアイテム

MS TVM マシンの統合からインポート中に検出された CI を表示できます。

注:
このリストのデフォルトのフィルターは [不一致] に設定されています。フィルターを削除すると、インポートから検出されたすべてのアイテムを表示できます。

詳細については、「検出されたアイテム」を参照してください。

マシンタグ

マシンタグ (ホストタグとも呼ばれます) は、組織の資産の整理と追跡に使用されます。マシンにタグをアサインします。

すべてのマシンタグは、MS TVM マシン統合の一部としてインポートされます。マシンタグは通常、 脆弱性対応 アサインルールと修復タスクルールでのフィルタリングに使用されます。タグは [検出されたアイテム] フォームに表示されます。

注:
脆弱性対応 アプリケーションで 脆弱性対応 アサインルールまたは修復タスクルールを作成する前に MS TVM マシンの統合を実行し、脆弱性一致アイテムをインポートしてグループ化する前にこれらのルールですべてのタグを使用できるようにします。タグに関する次の点にも注意してください。

- タグストレージでは大文字と小文字は区別されません。「Paris」タグが作成された場合、「PARIS」タグを [マシンタグ] テーブルに格納することはできません。Paris と PARIS は、システムで同じマシンタグと見なされます。最初にインポートされたタグが格納され、認識されます。
- 修復タスクルールのグループキーとしてマシンタグを使用すると、予期しない結果を生じることがあります。グループキーは修復タスクテーブルの列ですが、マシンタグは条件ビルダーでのみ使用することを目的としています。
- マシンタグは、グローバルシステムプロパティ sn_vul.import_host_tags で制御されます。このプロパティはデフォルトで [true] に設定されています。タグを無効にすると、すべての Now Platform インスタンスで無効になります。

次に行うこと

ServiceNow® Store から 脆弱性対応 integration with Microsoft Threat and Vulnerability Management をダウンロードすると、インストールと構成が 脆弱性対応 のセットアップアシスタントでサポートされます。詳細については、「セットアップアシスタントを使用して、Vulnerability Response integration with the MS TVM アプリケーションをインストールして設定します。」を参照してください。

Microsoft Threat and Vulnerability Management 脆弱性統合の準備

セットアップタスクを実行することで、ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) 脆弱性統合の準備をすることができます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

チェックリストの使用を開始する前に

脆弱性対応 Integration with the MS TVM アプリケーションのインストールと構成を行うには、アプリケーションをインストールして、脆弱性データを Now Platform インスタンスにインポートする前に、次のチェックリストを印刷し、リストされているアイテムが完了していることを確認することをお勧めします。

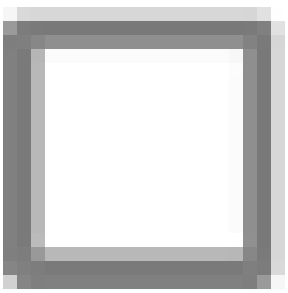
統合準備チェックリスト

タスク	説明
	次のいずれかの情報セットがあることを確認します。 • MS TVM アカウントの ClientSecret、ClientId、および TenantId • MS TVM アカウントのユーザー名、パスワード、ClientId、および TenantId。この情報を取得するには、「MS TVM 統合用の Microsoft Azure の設定」を参照してください。
	まだインストールしてアクティブ化していない場合は、サードパーティアプリケーションをインストールする前に 脆弱性対応 アプリケーションをインストールします。 脆弱性対応 アプリケーションのインストールとアクティブ化の詳細については、「脆弱性対応 のインストール」を参照してください。この統合には、脆弱性対応 のバージョン 14.0 以降が必要です。
	インスタンスにアプリケーションがまだない場合は、エンタイトルメントを取得し、脆弱性対応 Integration with MS TVM アプリケーションを Now Platform インスタンスにダウンロードします。 「」を参照してください。
	インポートする予定の脆弱性一致アイテムの数を見積もります。 インポートする予定の脆弱性一致アイテムの数をインスタンスが受け入れることができることを確認します。インスタンスが小さすぎると、ロードに時間がかかることがあります。インスタンスのサイズがわからない場合、またはサポートが必要な場合は、ServiceNow テクニカルサポートにお問い合わせください。
	統合を管理し、脆弱性一致アイテムを修正する次のグループまたはユーザーがいることを確認します。 admin セットアップアシスタントを使用して、MS TVM との脆弱性対応統合アプリケーションをインストールします。アサインされていない場合、アドミニストレーターはセットアップアシスタントで脆弱性アドミン

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

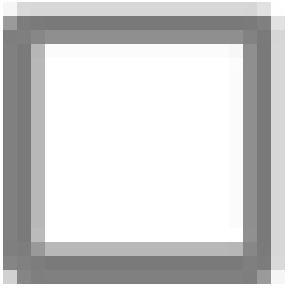
統合準備チェックリスト (続く)

タスク	説明
	(sn_vul.vulnerability_admin) およびその他のロールをアサインします。 sn_vul.vulnerability_admin MS TVM 統合の構成を完了します。このロールは、脆弱性対応 (VR) アプリケーションとそのレコードに完全にアクセスできます。このアドミニストレーターは、すべての VR アプリケーションとルールを構成し、サードパーティ統合を構成します。 sn_vul_msft_tvm.configure_integration MS TVM 脆弱性統合を構成します。このロールには、sn_vul_msft_tvm.read_integration の詳細なロールが含まれています。 sn_vul_msft_tvm.read_integration MS TVM 脆弱性統合のレコードを表示 (読み取り) できます。 脆弱性対応グループ デフォルトで脆弱性対応グループはセットアップアシスタントで利用可能になっています。脆弱性対応グループにアサインされたユーザーは sn_vul.read_all および sn_vul.remediation_owner ロールを自動的に継承します。 まだ作成されていない場合は、セットアップアシスタントを使用する前に、追加のグループを作成し、ユーザー管理モジュールでインスタンスにユーザーを追加することをお勧めします。詳細については、「ユーザーグループの作成」を参照してください。 脆弱性対応 アプリケーションでユーザーが実行および表示できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。
	脆弱性対応 Integration with NVD をインストールし、NIST National Vulnerability Database Integration - API (CVE のみ) を実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統合準備チェックリスト (続く)

タスク	説明
	最初のインポートのパフォーマンスを改善するには、インスタンスの特定の機能、ルール、またはジョブを無効にすることができます。 • 脆弱性算出を使用しない場合は無効にします。これらの算出では、定義した算出に加え、脆弱性一致アイテムレコードが作成および更新されるたびに実行されます。詳細については、「使用しないデフォルトの脆弱性算出の無効化」を参照してください。 • レコードの最初のインポート中に、特定の通知関連のビジネスルールによって大量の通知が生成され、取り込みのパフォーマンスに影響を与える可能性があります。

これで、「セットアップアシスタントを使用して、Vulnerability Response integration with the MS TVM アプリケーションをインストールして設定します。」に進む準備が整いました。

MS TVM 統合用の Microsoft Azure の設定

Microsoft Threat and Vulnerability Management (MS TVM) API にリモートでアクセスできるように、Microsoft Azure ポータルでアカウントを設定します。MS TVM テナントにアクセスして、マシン、脆弱性、およびセキュリティの推奨事項に関する情報を収集するには、このアカウントが必要です。

始める前に

必要なロール：Microsoft Azure ポータルアドミン。

このタスクについて

この統合のために ServiceNow® アプリケーションをインストールする前に、Microsoft Azure ポータルで次のセットアップタスクを完了してください。

最新のコンテンツにアクセスできることを確認するには、Microsoft ドキュメント Web サイトを参照してください。Microsoft Azure ポータルで OAuth 2.0 認証用のアプリケーション ID を作成していない場合は、次の手順のステップを実行します。

手順

1. Azure ポータルアドミンの認証情報を使用して、Microsoft Azure ポータルにログインします。
2. 左側のナビゲーションパネルで、**[Azure Active Directory]** を選択します。
3. 表示される [概要] ペインで、[アプリの登録 (プレビュー)] をクリックします。
4. [アプリの登録 (プレビュー)] ペインで、[新規登録] をクリックします。
   [アプリケーションの登録] フォームが表示されます。
5. フォームのフィールドに入力します。

アプリケーションフォームの登録

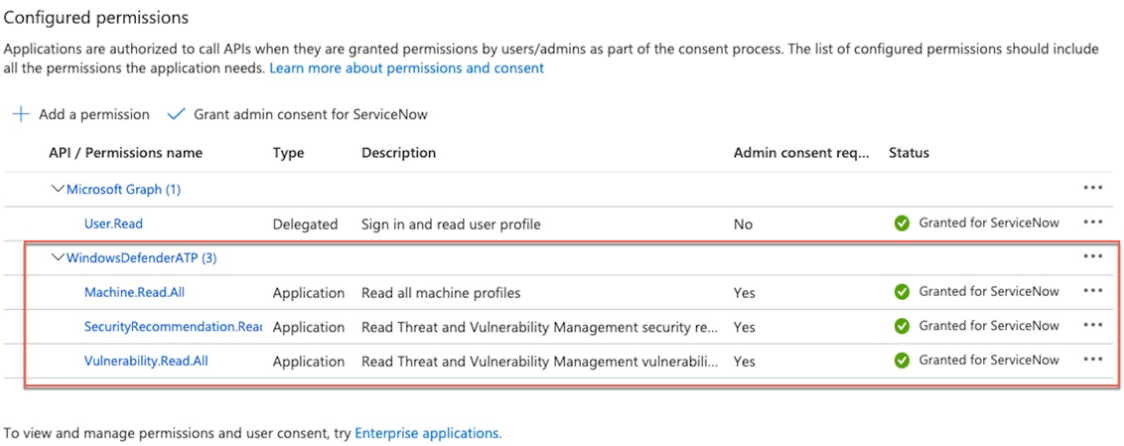
フィールド	説明
名前	アプリケーションの名前。この例では、「ServiceNow MS TVM Integration」と入力されています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
サポートされているアカウントの種類	このアカウントの場合、 [サポートされているアカウントの種類] で [この組織のディレクトリ内のアカウントのみ **(ServiceNow** のみ **-** 単一テナント**) (Accounts in this organizational directory only) (ServiceNow only - Single tenant)]** をクリックします。
リダイレクト **URL** (オプション)	このフィールドに値を入力しても、統合では使用されません。

6. [登録] をクリックします。
アプリケーション (クライアント) ID とディレクトリ (テナント) ID が作成されます。ServiceNow VR-TVM 統合セットアップアシスタントの構成ステップ中に、設定ページの [クライアント **ID]** および [テナント **ID]** フィールドにこれらの値を入力します。この手順は セットアップアシスタントを使用して、Vulnerability Response integration with the MS TVM アプリケーションをインストールして設定します。で説明されています。
7. [ServiceNow MS TVM 統合] ペインにアプリケーション (クライアント) ID が表示されている場合は、**[API** 権限の表示 **(View API Permissions)]** をクリックします。
8. 次のように移動する。 **API** 権限の要求 > 組織が使用する **API**をクリックし、[**Windows Defender ATP**] をクリックします。
9. [ServiceNow MS TVM 統合 - API 権限] ペインで、[権限を追加] をクリックします。
10. マシン、脆弱性、およびセキュリティの推奨事項への読み取りアクセス権を付与しま



す。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

11. **[<組織名> にアドミンの同意を付与する (Grant Admin Consent for <your organization name>)]** をクリックします。

    注:
    ServiceNow インスタンスからアプリケーションとして認証するには、次のアクションを実行します。

    a. 次のように移動する。 **Servicenow MS TVM** 統合 > 証明書とシークレットをクリックし、[新しいクライアント シークレット] をクリックします。

    b. フォームのフィールドに入力します。

    クライアントシークレットフォーム

フィールド	説明
説明	アプリケーションの名前。
有効期限	有効期限日。

    c. [追加] をクリックします。

    [値] フィールドに新しいクライアントシークレット (新しいパスワード) が入力されます。

    注:
    Now Platform インスタンスで統合を構成するときに、このパスワードが必要になります。詳細については、「セットアップアシスタントを使用して、Vulnerability Response integration with the MS TVM アプリケーションをインストールして設定します。」を参照してください。

    d. このパスワードを安全な場所に保存します。このページから移動すると、このパスワードは確認できません。

    これで、Microsoft Azure ポータルで認証用のアプリケーション ID を正常に作成できました。

次のタスク

次は統合用に Now Platform® インスタンスをセットアップします。

セットアップアシスタントを使用して、Vulnerability **Response integration with the MS TVM** アプリケーションをインストールして設定します。

脆弱性対応 Integration with Microsoft Threat and Vulnerability Management (MS TVM) アプリケーションをインストールして設定し、MS TVM からインポートされたデータを使用して、資産の脆弱性の優先順位付けと修正を行えるようにします。

始める前に

ServiceNow® Microsoft Threat and Vulnerability Management 脆弱性統合を実行する前に、ServiceNow Store から Vulnerability Response Integration with Microsoft Threat and Vulnerability Management アプリケーションをダウンロードし、脆弱性対応 アプリケーションのセットアップアシスタントを使用してインストールして設定する必要があります。

MS TVM アプリケーションをインストールする前に、Microsoft Threat and Vulnerability Management 脆弱性統合の準備 のチェックリストのすべてのアイテムが完了していることを確認してください。Microsoft Azure アカウントの設定方法の詳細については、「MS TVM 統合用の Microsoft Azure の設定」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

必要なロール：sn_vul.vulnerability_admin ロールを最初にアサインし、セットアップアシスタントで Microsoft Threat and Vulnerability Management アプリケーションをインストールする admin ロール。インストール後に、セットアップアシスタントでアプリケーションを構成する脆弱性アドミンロール (sn_vul.vulnerability_admin または sn_vul.admin (使用廃止))。

このタスクについて

MS TVM 統合をインストールして構成する前に、次の手順を実行します。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合アプリケーションのインストール.

   しばらくすると、インスタンスにインストールできるアプリケーションが表示されます。

2. **[Microsoft Threat and Vulnerability Management]** タイルを見つけて、[インストール] をクリックします。

   ServiceNow Store からダウンロードした 脆弱性対応 Integration with Microsoft Threat and Vulnerability Management アプリケーションがインストールされます。

3. セットアップアシスタントのプロンプトに従ってインストールを続行します。
   セットアップアシスタントを使用したアプリケーションのインストールの詳細については、「セットアップアシスタントを使用した 脆弱性対応 サードパーティアプリケーションのインストール」を参照してください。

次のタスク

セットアップアシスタントでインストールを完了したら、 統合設定 > スキャナー統合 セットアップアシスタントで構成を続行します。セットアップアシスタントで提供されているプロンプトを補足するための詳細情報については、「セットアップアシスタントを使用した MS TVM 脆弱性統合の構成」を参照してください。

Microsoft Threat and Vulnerability Management® 統合用のデータ取得設定

データ取得設定を使用すると、ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) 脆弱性統合から Now Platform インスタンスにインポートするデータのタイプとスコープを決定できます。

データ取得設定は、インポートするデータを制御するのに役立ちます。これらのフィルターの値は統合インスタンスで設定できます。統合インスタンスを表示するには、次に移動します: **Microsoft** の脅威と脆弱性の管理の脆弱性統合 > 統合インスタンス をクリックし、MS TVM 統合をクリックします。

[統合インスタンス] ページで、[統合インスタンスパラメーター] をクリックしてパラメーターのリストを表示するか、[脆弱性統合] タブをクリックして、スケジュール、REST の詳細、インテグレーションの詳細、データソース、および統合実行情報を表示します。

Now Platform インスタンスでの MS TVM 統合用のデータ取得設定とフィルター

Now Platform インスタンスでの MS TVM 統合には、次の設定を使用できます。これらの構成設定およびその他の構成設定は、Now Platform インスタンスの [統合インスタンス] ページに表示されます。最初の数回の統合実行では、これらの設定をデフォルト設定のままにすることをお勧めします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MS TVM。

vi_size_limit

MS TVM マシン脆弱性統合の結果セットに含める脆弱性一致アイテムレコードの数を定義します。この設定は int32 形式にする必要があります。デフォルト値は 2,000 です。

vulnerabilities_size_limit

MS TVM 脆弱性 (CVE) 統合の結果セットに含める脆弱性レコードの数を定義します。この設定は int32 形式にする必要があります。デフォルト値は 2,000 です。

recommendations_size_limit

MS TVM 推奨事項統合の結果セットに含める脆弱性レコードの数を定義します。この設定は int32 形式にする必要があります。デフォルト値は 2,000 です。

asset_size_limit

MS TVM マシン統合の結果セットに含める脆弱性レコードの数を定義します。この設定は int32 形式にする必要があります。デフォルト値は 2,000 です。

machine_filter

MS TVM から取得したマシンをフィルタリングします。このフィルターは MS TVM マシン統合に適用されます。デフォルト値では、onBoardingStatus が onBoarded のマシンが取り込まれます。

Microsoft Threat and Vulnerability Management 脆弱性統合用の REST メッセージ

ServiceNow Microsoft Threat and Vulnerability Management (MS TVM) 脆弱性統合に REST メッセージを使用して、MS TVM API への呼び出しを行うことができます。

MS TVM アクセストークン

また、MS TVM アクセストークンに REST メッセージを使用して MS TVM API からアクセストークンを取得し、REST API 要求を認証することもできます。REST メッセージのレコードメソッドを変更すると、MS TVM に対する認証要求に影響します。

MS TVM 統合

MS TVM 統合に REST メッセージを使用して、MS TVM から情報を取得できます。REST メッセージのレコードメソッドを変更すると、 情報を取得するための MS TVM への要求に影響します。REST メッセージには、次の REST メソッドが含まれています。

REST メソッド

REST メソッド	メソッドの説明
GET 脆弱性	MS TVM から脆弱性とエクスプロイト情報を取得します。
マシン別にソフトウェア脆弱性を取得	すべてのオープンな脆弱性を取得します。
推奨事項を取得	組織に影響するすべてのアクション可能なセキュリティ推奨事項のリストを取得します。
マシンを取得	資産のコレクションを取得します。
マシン別にソフトウェア脆弱性の変更を取得	新規、修正済み、および更新済み脆弱性を含む、組織の完全な脆弱性インポートで変更されたすべての情報を取得します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Microsoft Threat and Vulnerability Management® 脆弱性統合のデータ変換

インポートするデータを特定すると、ServiceNow Microsoft Threat and Vulnerability Management (MS TVM) アプリケーションからデータが取得され、一連のデータソースによって処理され、インスタンス内で変換されます。

インストール時に、正規化された重大度マップが [正規化された重大度マッピング (Normalized Severity Mapping)] モジュールにインストールされます。これらのマップ変換では、Microsoft サードパーティ脆弱性重大度レベルを標準の重大度レベルにインポートし、インスタンスで処理されます。重大度マッピングの作成については、「脆弱性対応 重大度マップの作成」を参照してください。

MS TVM マシンのインポート

インポートされたマシンのデータは、最初に MS TVM マシンのインポート [sn_vul_msft_tvm_machines_import] テーブルにロードされます。

MS TVM マシンの変換は、インポートされたマシン情報を変換するために使用されます。

> **注:**
> この変換マップを変更すると、MS TVM マシンのインポートからのデータの処理方法が変更されます。

この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ Microsoft **TVM Machines Transform** を検索します。

次の表に、統合別の変換マップフィールドを示します。

MS TVM マシン変換マップのフィールド

ソースフィールド	ターゲットフィールド	説明
u_id	source_id	資産の一意の ID。この ID は、検出されたアイテムレコードの source_id にマップされます。
u_ipaddresses.macAddress	mac_address	API から cmdb_ci レコードの host mac address フィールドにマッピングされる MAC アドレス。
u_ipaddresses.ipAddress	ip_address	cmdb_ci レコードの IP アドレスフィールドにマッピングされる IP アドレスフィールド。
u_lastseen	last_scan_date	検出されたアイテムレコードの last_scan_date フィールドにマッピングされるフィールド。
u_machinetags		sn_sec_cmn_host_tag に保存されているタグ。タグから資産へのマッピングは sn_sec_cmn_m2m_src_ci_tag に保存されます。
u_osplatform	os	cmdb_ci レコードの os フィールドにマップするフィールド。
u_computerdnsname	fqdn	API から cmdb_ci レコードの fqdn フィールドに dnsname

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MS TVM マシン変換マップのフィールド (続く)

ソースフィールド	ターゲットフィールド	説明
		フィールドをマッピングするフィールド。

変換プロセス中に、次の変換スクリプトが実行されます。

MS TVM マシンの変換マップスクリプトのタイミングと目的

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	統合プロセスのスコープ変数 [sn_vul_sccm] の値を初期化するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onBefore (インポートセットの変換が完了する前)。	ホストの値を更新し、ホストが存在するかどうかを確認するために使用されるスクリプト。結果に基づいて、このスクリプトはスコープ変数 (sn_vul_msft_tvm) の値を変更します。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onComplete (インポートセットが変換を完了したとき)	作成、更新、および無視される CI の数を設定するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

MicrosoftTVMMachinesProcessor スクリプトインクルードは onBefore 変換スクリプトから呼び出されます。Microsoft TVM マシンの統合からの出力を取得し、CI に変換します。このスクリプトインクルードを変更すると、CI および検出されたアイテムテーブルの Microsoft TVM マシンのデータ変換が変更される可能性があります。

MS TVM 脆弱性統合

インポートされた脆弱性データは、最初に Microsoft TVM CVE (脆弱性) インポート [sn_vul_msft_tvm_vulnerabilities_import] テーブルにロードされます。

注:
この変換マップを変更すると、MS TVM 脆弱性インポートからのデータの処理方法が変更されます。

この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ Microsoft **TVM Vulnerabilities Transform** を検索します。

次の表に、統合別の変換マップフィールドを示します。

Microsoft TVM 脆弱性変換マップのフィールド

ソースフィールド	ターゲットフィールド	説明
u_id	ID	sn_vul_entry レコードの [ID] 列にマッピングします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Microsoft TVM 脆弱性変換マップのフィールド (続く)

ソースフィールド	ターゲットフィールド	説明
u_severity	source_severity	[重大度] フィールドを重大度にマッピングします。デフォルト値は 5 です。
u_publishedon	date_published	u_publishedon フィールドを公開日にマッピングします。
u_publicexploit	public_exploit	スキャナーによって提供された u_publicexploit を脆弱性エントリーテーブルの公開 exploit 列にマッピングします。
u_cvssv3	v3_base_score	cvssv3 スコアを脆弱性エントリーレコードの v3 ベーススコアにマッピングします。
u_description	summary	説明を脆弱性エントリーレコードのサマリフィールドにマッピングします。
u_exploitinkit	malware_kit	u_exploitinkit フィールドを [エクスプロイト] テーブルのマルウェアキットにマッピングします。
u_exploittypes	type	エクスプロイトタイプを [エクスプロイト] テーブルのタイプにマッピングします。
u_exploitverified	is_exploit_verified	u_exploitverified フィールドを [エクスプロイト] テーブルの検証済みエクスプロイトにマッピングします。
u_exploituris	exploit_links	u_exploituris フィールドを [エクスプロイト] テーブルのエクスプロイトリンクにマッピングします。

変換プロセス中に、次の変換スクリプトが実行されます。

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	統合プロセスのスコープ変数 [sn_vul_sccm] の値を初期化するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onBefore (インポートセットの変換が完了する前)。	NVD またはサードパーティのエントリーテーブルの値を作成または更新するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onComplete (インポートセットが変換を完了したとき)	作成された新しいアイテムと更新されて無視されたアイテムの値を設定するために使用される

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

スクリプトが実行されるタイミング	目的
	スクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

MS TVM 推奨事項のインポート

インポートされた推奨事項データは、最初に MS TVM 推奨事項のインポート [sn_vul_msft_tvm_recom_import] テーブルにロードされます。

注:
この変換マップを変更すると、MS TVM 推奨事項のインポートからのデータの処理方法が変更されます。

この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ をクリックし、「 **MS TVM** 推奨事項の変換」を検索します。

次の表に、統合別の変換マップフィールドを示します。

MS TVM 推奨事項変換マップのフィールド

ソースフィールド	ターゲットフィールド	説明
u_recommendedvendor	recommended_vendor	u_recommendedvendor フィールドを [ベンダー] 列にマッピングします。
u_weaknesses	weaknesses	u_weaknesses フィールドを [脆弱性] 列にマッピングします。
u_exposedmachinescount	src_exposed_machines_cnt	u_exposedmachinescount フィールドを [公開済みマシン数] 列にマッピングします。
u_status	status	ステータスを推奨レコードの [ステータス] フィールドにマッピングします。
u_productname	product_name	u_productname フィールドを推奨レコードの [製品名] にマッピングします。
u_nonproductiv_impactedassets	non_prod_impacted_assets	u_nonproductiv_impactedassets フィールドを推奨レコードの [影響を受ける資産] 列にマッピングします。
u_activealert	active_alert	u_activealert フィールドを推奨事項レコードの [アクティブなアラート] 列にマッピングします。
u_recommendedversion	recommended_version	u_recommendedversion フィールドを推奨レコードの [推奨バージョン] 列にマッピングします。
u_totalmachinecount	total_machine_count	u_totalmachinecount フィールドを推奨レコードの [マシン

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MS TVM 推奨事項変換マップのフィールド (続く)

ソースフィールド	ターゲットフィールド	説明
		の合計数] 列にマッピングします。
u_exposureimpact	exposure_impact	u_exposureimpact フィールドを推奨レコードの [エクスポージャーの影響] 列にマッピングします。
u_recommendationname	recommendation_name	u_recommendationname フィールドを推奨レコードの [推奨事項の名前] 列にマッピングします。
u_subcategory	subcategory	u_subcategory フィールドを推奨レコードの [サブカテゴリ] 列にマッピングします。
u_id	source_id	推奨事項 ID を MS TVM から [ソース ID] 列にマッピングします。
u_remediationtype	remediation_type	u_remediationtype フィールドを推奨レコードの [推奨事項タイプ] 列にマッピングします。
u_relatedcomponent	related_component	u_relatedcomponent フィールドを推奨レコードの [関連コンポーネント] 列にマッピングします。
u_recommendedprogram	recommended_program	u_recommendedprogram フィールドを推奨レコードの [推奨プログラム] 列にマッピングします。
u_recommendationcategory	recommendation_category	u_recommendationcategory フィールドを推奨レコードの [推奨事項のカテゴリ] 列にマッピングします。
u_publicexploit	public_exploit	u_publicexploit フィールドを推奨レコードの [公開エクスプロイト] 列にマッピングします。
u_vendor	vendor	u_vendor フィールドを推奨レコードの [ベンダー] 列にマッピングします。
[Script]	integration_instance	推奨事項のインポート元のインスタンスの名前。
[Script]	sys_domain	このレコードがインポートされるドメイン。

変換プロセス中に、次の変換スクリプトが実行されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

MS TVM 推奨事項変換マップのスクリプト

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	統合プロセスのスコープ変数 [sn_vul_sccm] の値を初期化するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onBefore (インポートセットの変換が完了する前)。	推奨事項の値を更新し、推奨事項が存在するかどうかを確認するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onComplete (インポートセットが変換を完了したとき)	作成、更新、および無視されるアイテムの値を設定するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

MS TVM マシン脆弱性のインポート

MS TVM マシン脆弱性変換マップは、MS TVM からインポートされたオープンおよび修正済みの脆弱性情報を変換するために使用されます。

注:
この変換マップを変更すると、MS TVM マシン脆弱性インポートからのデータの処理方法が変更されます。

MS TVM のオープンおよび修正された脆弱性変換マップにアクセスするには、 システムインポートセット > 変換マップ をクリックし、 **MS TVM** マシン脆弱性変換を検索します。

次の表に、統合別の変換マップフィールドを示します。

MS TVM マシン脆弱性変換マップのフィールド

ソースフィールド	ターゲットフィールド	説明
u_id	detection_key	u_id フィールドを検出テーブルの [検出キー] 列にマッピングします。
u_diskpaths	proof	u_diskpaths フィールドを検出テーブルの [実証] 列にマッピングします。
u_registrypaths	proof	u_registrypaths フィールドを検出テーブルの [実証] 列にマッピングします。
u_recommendedsecurityupdateid	preferred_solution	sn_vul_solution テーブルに同じ ID のソリューションが存在する場合、u_recommendedsecurityupdateid フィールドを脆弱性一致アイテムテーブルの [優先ソリューション] 列にマッピングします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MS TVM マシン脆弱性変換マップのフィールド (続く)

ソースフィールド	ターゲットフィールド	説明
u_recommendationreference	recommendation	u_recommendationreference フィールドを脆弱性一致アイテムテーブルの [推奨事項] 列にマッピングします。
u_cveid	vulnerability	u_cveid フィールドを脆弱性一致アイテムテーブルの [脆弱性] 列にマッピングします。
u_status	source_status	u_status フィールドを検出テーブルの [ソースステータス] 列にマッピングします。
u_eventtimestamp	temporal_score	u_eventtimestamp フィールドを脆弱性一致アイテムテーブルの [前回検出日] 列にマッピングします。
u_lastseentimestamp	last_seen	u_lastseentimestamp フィールドを脆弱性一致アイテムテーブルの [前回確認日] 列にマッピングします。
u_firstseentimestamp	first_seen	u_firstseentimestamp フィールドを脆弱性一致アイテムテーブルの [初回確認日] 列にマッピングします。
u_recommendedsecurityupdate	solution_summary	u_recommendedsecurityupdate フィールドを脆弱性一致アイテムテーブルの [ソリューションの概要] 列にマッピングします。
u_recommendedsecurityupdateurl	solution_summary	u_recommendedsecurityupdateurl フィールドを脆弱性一致アイテムテーブルの [ソリューションの概要] 列にマッピングします。

変換プロセス中に、次の変換スクリプトが実行されます。

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	統合プロセスのスコープ変数 [sn_vul_sccm] の値を初期化するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スクリプトが実行されるタイミング	目的
onBefore (インポートセットの変換が完了する前)。	脆弱性エントリーと検出が存在するかどうかを確認するために使用されるスクリプト。そうでない場合、これらのレコードはそれぞれのテーブルに作成されます。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onComplete (インポートセットが変換を完了したとき)	MS TVM からインポートされた VI と検出の数を更新するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

Microsoft Threat and Vulnerability Management 脆弱性統合の統合実行状況チャート

Microsoft Threat and Vulnerability Management (MS TVM) 統合実行状況モジュールを使用して、MS TVM 統合実行のステータスをグラフィカルに表示できます。

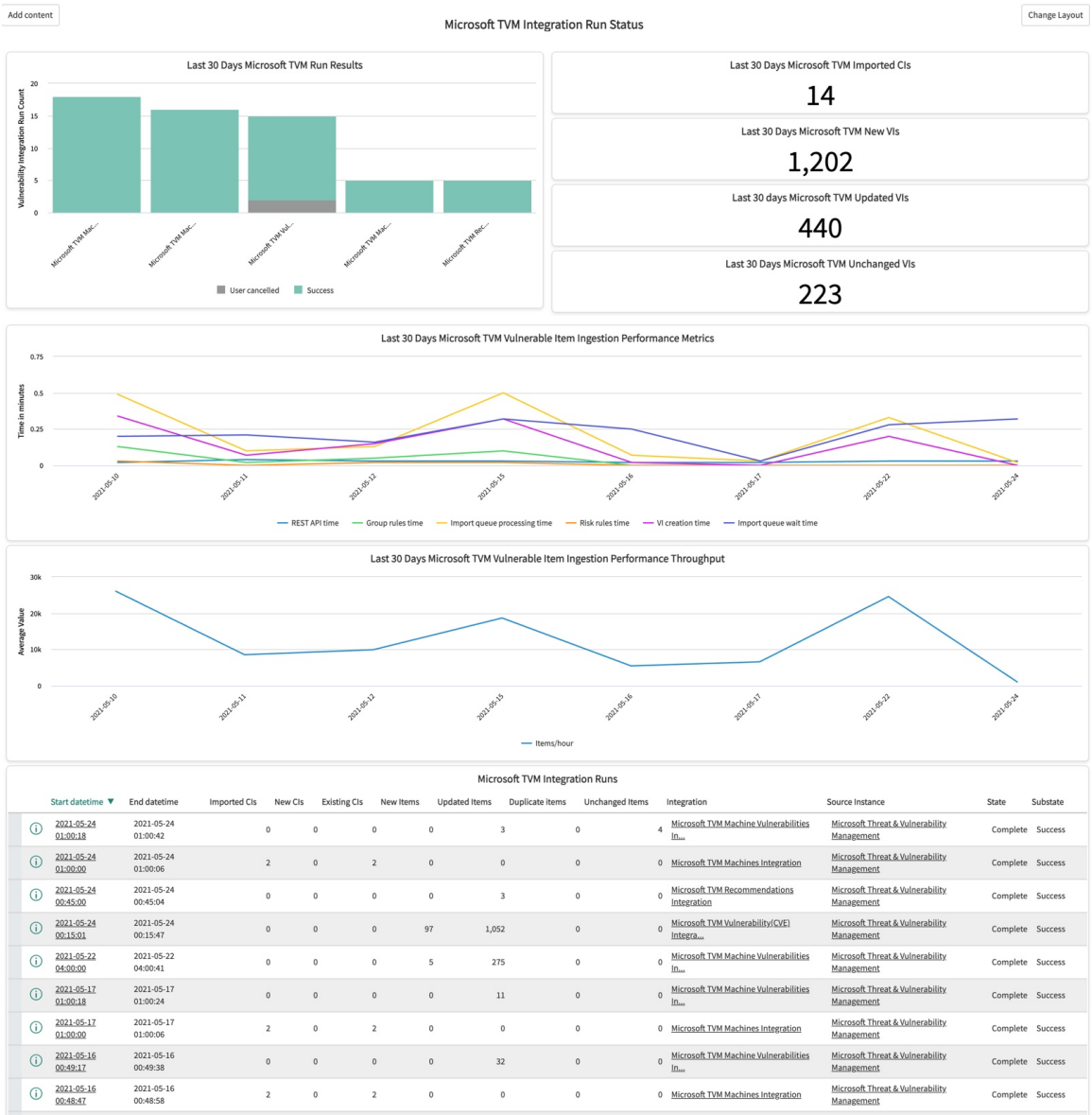
脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で使用可能です。

> **注:**
> Tokyo を使用している場合は、Next Experience UI でダッシュボードを表示できますが、一部の機能が失われます。

チャートで、グラフの任意の部分をポイントすると、その部分に固有のデータの概要が表示されます。棒グラフの任意の部分をクリックすると、より詳細な情報を提供するリストが開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



MS TVM 統合実行状況チャートレポート

名前	説明
過去 30 日間の Microsoft TVM の結果	各統合で完了した統合実行の数。このレポートには、成功した実行と失敗した実行の両方が表示されます。各実行は棒グラフで表示されます。
過去 30 日間の Microsoft TVM の新しい VI	過去 30 日間にインポートされた新しい脆弱性一致アイテムの数。
過去 30 日間の Microsoft TVM 更新済み VI	過去 30 日間にインポートされた更新済み脆弱性一致アイテムの数。
過去 30 日間の Microsoft TVM 未変更 VI	過去 30 日間にインポートされた重複脆弱性一致アイテムの数。
MS TVM 統合実行数	統合実行レコードのリスト。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	説明
	注: V16.1： この統合の検出を検証するには、検出または検出結果を *sn_vul_detection* テーブルの ServiceNow 検出データと比較します。 統合の進行中は、検出数または検出結果数が変更される可能性があります。このレポートでは、統合実行の完了後に、インスタンスの [現在までの数] 列に検出数が表示されます。
過去 30 日間の Microsoft TVM 脆弱性一致アイテムの取り込みパフォーマンスメトリクス	過去 30 日間に比較された脆弱性一致アイテムの日次パフォーマンスメトリクス。
過去 30 日間の Microsoft TVM 脆弱性一致アイテムの取り込みパフォーマンススループット	過去 30 日間に測定された Microsoft TVM ホスト検出統合の日次脆弱性一致アイテムの取り込みスループット。
過去 30 日間の Microsoft TVM インポート済み CI	過去 30 日間にインポートされた新しい構成アイテムの数。

Microsoft Threat and Vulnerability Management 統合インポートの実行状況の確認

Microsoft Threat and Vulnerability Management (MS TVM) インポートの実行状況を使用して、統合の実行が成功したことを確認し、問題を特定します。

始める前に

この手順は、以下を前提としています。

- 脆弱性対応 と MS TVM 脆弱性統合がインストールおよび設定されている。
- MS TVM 脆弱性統合のインポートがスケジュールされ、実行されている。

必要なロール：sn_vul.vulnerability_admin

このタスクについて

統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、 脆弱性対応のバージョン 18.2.4 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

手順

1. 次のように移動する。 **All** (すべて) > **Microsoft** の脅威と脆弱性の管理 > 統合.
   a. 統合を選択します。
   b. [脆弱性統合実行] 関連リストをクリックします。
2. インポートのステータスが [完了] で、サブステートが [成功] になっていることを確認します。実行が失敗した場合の一般的な原因は次のとおりです。
   - ネットワークの中断。
   - データ転送でのデータ劣化による、変換中のデータ破損。
3. オプション: 実行の失敗につながったこれらのいずれかの条件が表示された場合は、[今すぐ実行] をクリックして統合を再実行します。

脆弱性インスタンスに基づいて **Microsoft TVM** 検出を分割し、脆弱性一致アイテムを分割します

ServiceNow® 脆弱性対応では、Microsoft Threat and Vulnerability Management (MS TVM) スキャナーからの検出を分割し、検出された脆弱性インスタンスごとに一意の脆弱性一致アイテム (VIT) を作成できます。この分割により、VIT をさまざまな修復チームにアサインできるため、脆弱性の管理と追跡が強化されます。

始める前に
必要なロール：admin

このタスクについて
Microsoft Threat and Vulnerability Management (MS TVM) スキャナーのペイロードには検出データが含まれ、実証内の各パスが検出の分割に使用されます。ペイロードの diskpath タグは脆弱性の場所を識別し、特定のパスに従って脆弱性を正確に特定および管理を容易にします。

手順

1. サードパーティ統合テーブル [sn_sec_int_integration] で、Tenable.io と Tenable.sc の **[VI** キー列に証明を含める] の値を true に設定します。
2. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > **VI** の粒度の構成.
3. [ポートを含める] フォームで、[ポートを含める] チェックボックスをオンにして、[ここをクリック] リンクを選択します。
4. [VI キーに証明を追加] リストで、[新規] を選択します。
5. [VI キー新規レコードに実証を追加 (Add proof to the VI key- New record)] フォームの [脆弱性] フィールドに、実証を含める Microsoft Threat and Vulnerability Management (MS TVM) CVE を追加し、[送信] を選択します。
   選択した脆弱性が [VI キーに証明を追加] リストに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Example: Microsoft Threat and Vulnerability Management (MS TVM) スキャナーからの検出の分割

Microsoft Threat and Vulnerability Management (MS TVM) スキャナーからの次の検出は、diskpath タグに実証を示しています。

```
          "id": "329f3283
fae116€796ff1b59c8dd56fef4067elf_mozilla_firefox_126.0.1.0_CVE-2024-7528",
          "deviceId":"329f3283fae116e796ff1b59c8dd56fef4067e1f",

          "rbacGroupId":
    "rbacGroupName": "Unassigned",
     "deviceName": "ip-0a1409fd.secops.com",
      "osPlatform": "WindowsServer2019",
        "oVersion": "10.0.17763.5936",
      "osArchitecture": "x64",
       "softwareVendor": "mozilla",
      "softwareName": "firefox",
      "softwareVersion": "126.0.1.0",

          "cveId"; "CVE-2024-7528",
         #vulnerabilitySeverityLevel": "High",
       #recommendedSecurityUpdate":; "mfsa2024-33",

      "recommendedSecurityUpdateId": null,

          "recommendedSecurityUpdateUrl": null,
           "diskPaths": ['c: llprogram files\lamazonllcfn-bootstraplilibcrypto-3.dll", "C: \lprogram
files\lamazon\lcfn-bootstrap\\libsst-3.dll,

        "registryPaths":
          1 "HKEY LOCAL, MACHINE\\SOFTWAREW\WOW6432Nodel
lMicrosoft|\Windows|1CurrentVersion\|Uninstalll\Mozilla Firefox 126.0.1 (x86 en-US)"


       #lastSeenTimestamp": "2024-08-28 19:36:07",

        "firstSeenTimestamp": "2024-08-06 20:32:34",

      "end0fSupportStatus": null,
        "end0fSupportDate": null,
     "exploitabilityLevel": "NoExploit",
        "recommendationReference": "va-_-mozilla-_-firefox",

        "cvssScore": 8.8,
      "securityUpdateAvailable": true,
        "cveMitigationStatus": null
```

脆弱性対応 との **HCL BigFix** パッチオーケストレーション統合の概要

HCL BigFix 製品との 脆弱性対応 パッチオーケストレーション統合により、大規模な資産グループの重大な脆弱性に対するパッチとパッチの展開を管理できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 を使用したパッチオーケストレーション

脆弱性対応 を使用したパッチオーケストレーションでは、サードパーティのソリューション統合、パッチベンダー、および脆弱性スキャナーからのスケジュール済みインポートが使用されます。スキャナー検出データは、環境内の資産を脆弱性とそれらを修正できるパッチ更新と照合します。承認のためにパッチ要求を送信し、脆弱性一致アイテムを解決するためのパッチ更新をスケジュールし、修復の進捗状況すべてを Now Platform の 脆弱性対応 アプリケーションのレコードから監視します。

Vulnerability Response Patch Orchestration with HCL BigFix®

HCL BigFix と脆弱性対応パッチオーケストレーションとの統合アプリケーションを ServiceNow 脆弱性ソリューション管理、パッチオーケストレーション、および 脆弱性対応 アプリケーションと併用すると、脆弱性マネージャーとアナリストは次のタスクを実行できます。

- パッチのタイプとベンダーのソリューション (パッチ) に関する詳細なコンテキストと情報を表示します。
- 脆弱性対応 ワークスペースのレコードから、脆弱性とソリューションのデータ、および脆弱性の修復の進捗状況を表示および監視します。

IT スペシャリストと修復オーナーは、次のタスクを実行できます。

- Windows、CentOS、MAC、Oracle、およびその他の資産に対して、BigFix 製品でサポートされているパッチを営業時間外に定期的に展開し、作業の競合を回避します。
- 脆弱性がある未パッチ資産、またはサードパーティスキャナーからインポートされた検出データから、パッチスケジュールによって正常に更新されなかった資産を特定します。
- IT 修復ワークスペースまたはクラシック環境から、パッチ更新、修復タスク、および検出されたアイテムレコードからパッチが適用されていない脆弱な資産に対して利用可能なパッチをスケジュールします。

脆弱性対応 および **BigFix** アプリケーションで使用される主要な用語

構成アイテム (CI)

CI は、構成管理データベース (CMDB) にリストされている既存の資産です。BigFix は CI、コンピューターを呼び出します。

コンピューターグループ

資産のグループを指す BigFix 製品で使用される用語。

脆弱性一致アイテム

CMDB 内の既存の資産と一致するインポートされた脆弱性。

インスタンス

BigFix アプリケーションの個別のアカウント。各ユーザーアカウントは、BigFix アプリケーションのインスタンスにすることができます。この用語は、Now Platform インスタンスの一意の安全な Web アドレスを意味します。

統合

統合は、BigFix マシンとの統合など、サードパーティのソースから情報を取得する Now Platform のスケジュール済みジョブです。

ソリューション

この統合のコンテキストには、潜在的と優先の 2 つのタイプのソリューションがあります。潜在的なソリューションは、脆弱性に対処する可能性があるソリューションです。脆弱性には多くの潜在的なソリューションがあります。優先ソリューションは、検出された特定の脆弱性に対して最も効果的なソリューションと一致します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

パッチ

脆弱性を修正するソフトウェア更新。BigFix アプリケーションでは、パッチは Fixlet と呼ばれます。たとえば、BigFix には Windows、CentOS、MAC、Oracle、およびその他の製品用の Fixlet があります。

優先パッチ

優先パッチは、特定の脆弱性を修正することを目的としたソフトウェア更新です。パッチが展開されると、特定の脆弱性に関連する脆弱性一致アイテムにマッピングされ、それらを修正します。

修復タスク

脆弱性を修正するために必要なアクションの 脆弱性対応 アプリケーション内の脆弱性一致アイテムのリスト。

展開

この統合における展開とは、マシンにパッチを適用、開始、またはスケジュールする場合を指します。BigFix はこれらの展開、アクションを呼び出します。Now Platform で BigFix からダウンロードしたパッチに対して展開 (アクションを作成) できます。脆弱性対応 の個々のレコードから検出されたアイテム、パッチ、または修復タスクに移動します。スケジュール済みジョブを含むパッチを個々のマシンまたはコンピューターグループに展開できます。

Now Platform での展開は、マルチソースをサポートする統合を指す場合もあります。単一の統合の存在は、統合の展開と呼ばれます。展開とは、環境全体の統合と製品のことです。たとえば、お使いの環境に BigFix 脆弱性統合を複数展開する場合があります。

Vulnerability Solution Management と Vulnerability Response Patch Orchestration with HCL BigFix 統合

ソリューション管理は、脆弱性ソリューション管理 アプリケーションによって提供されます。これは、脆弱性の検出結果とそれらを修正するソリューション (パッチ) のブレークダウンを関連付ける Now Platform アプリケーションです。組織に最も大きな影響を与える製品やサービス、構成の更新、およびその他のコントロールに対するサードパーティからのソフトウェアパッチを特定します。サードパーティのスキャナー情報とともに、脆弱性対応のソリューション管理、脆弱性対応、および Vulnerability Response Patch Orchestration with HCL BigFix アプリケーションを連携して、ソリューションから脆弱性、脆弱性一致アイテムに優先パッチをロールアップして、使用している環境で脆弱性を修正してクローズすることができます。

脆弱性対応のソリューション管理、脆弱性対応、および Vulnerability Response Patch Orchestration with HCL BigFix 統合はすべて ServiceNow Store で入手可能です。

必要な Now Platform ロール

統合のインストール、構成、および修復タスクには、Now Platform インスタンスで次のロールが必要です。

admin

このロールを持つユーザーは、ServiceNow Store のアプリケーションのエンタイトルメントを取得し、Now Platform のインスタンスにダウンロードします。

sn_vul.vulnerability_admin

このロールを持つユーザーは、Now Platform インスタンスでアプリケーションをアクティブ化し、脆弱性対応 アプリケーションの構成を完了します。このロールは、脆弱性対応 (VR) アプリケーションとそのレコードに完全にアクセスできます。このアドミンユーザーは、すべての VR アプリケーション、ルール、およびサードパーティ統合を設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

sn_vul_bigfix.configure_integration

このロールを持つユーザーは、BigFix Patch Orchestration Integration アプリケーションを構成します。このロールには、sn_vul_bigfix.read_integration の詳細なロールが含まれています。

sn_vul_bigfix.read_integration

このロールを持つユーザーは、脆弱性対応 のレコードと、BigFix Patch Orchestration Integration アプリケーションおよびパッチオーケストレーションデータを表示できます。

sn_vul_patch_orch.configure_patch

このロールを持つユーザーは、パッチを設定して適用することができます。

sn_vul_patch_orch.read_patch

このロールを持つユーザーは、パッチ情報を表示できます (読み取り専用)。

承認者

展開する前に、送信されたパッチ要求を承認する場合は、承認者レベル 1 と承認者レベル 2 の承認者グループにユーザーをアサインします。

セットアップアシスタントを使用したこのロールの割り当ての詳細については、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。Now Platform の 脆弱性対応 ロールの詳細については、「脆弱性対応 のペルソナと詳細なロール」を参照してください。

CI ルックアップルール

データが BigFix アプリケーションからインポートされると、脆弱性対応 アプリケーションがマシン (資産) データを使用して 構成管理データベース (CMDB) 内の一致を自動的に検索します。CI ルックアップルールは、CI (資産) を識別し、VI の作成時にそれらを脆弱性一致アイテム (VI) レコードに追加する際に使用されます。

次の CI ルックアップルールはベースシステムに付属しており、CI (資産) を識別して 脆弱性対応 アプリケーションに追加する際に使用されます。

- MAC_ADDRESS
- IP_ADDRESS
- DNS_NAME

資産の IP_ADDRESS には複数の値を使用できます。CI ルックアップルールでは、すべての値を照合します。CI ルックアップルールとその仕組みの詳細については、「脆弱性対応 サードパーティ脆弱性統合の構成アイテムを識別するための CI ルックアップルール」を参照してください。

MID サーバー

脆弱性対応 Patch Orchestration with HCL BigFix 統合はオンプレミスの統合です。MID サーバークラスターに含まれていないスタンドアロン MID サーバーが必要です。MID サーバーは、BigFix サーバーからデータをインポートするために、インスタンスからリモートマシンでスクリプトを実行する必要があります。この統合用の API は、Now Platform インスタンスで設定した MID サーバーを使用して呼び出されます。詳細については、「脆弱性対応 Patch Orchestration integration with HCL BigFix の準備」を参照してください。

脆弱性対応 Patch Orchestration with HCL BigFix の統合および依存関係

Vulnerability Response Patch Orchestration with HCL BigFix 統合には、次の製品と依存関係アプリケーションが必要です。これらのアプリケーションは ServiceNow Storeで入手できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

パッチオーケストレーション統合に必要なアプリケーションと依存関係の利用可能なバージョン

脆弱性対応 のワークスペースでパッチオーケストレーションデータと利用可能な更新 (パッチ) を表示するには、次のアプリケーションが必要です。リストされているすべてのアプリケーションは ServiceNow Store で入手できます。一部のアプリケーションには別のサブスクリプションが必要です。

必要なアプリケーションとファミリーリリースと互換性のあるバージョンについての詳細は、HI ナレッジベース記事「Vulnerability Response Compatibility Matrix and Release Schema Changes (脆弱性対応互換性マトリクスおよびリリーススキーマの変更点) [KB0856498]」を参照してください。

アプリケーションとリリースバージョン
脆弱性対応
脆弱性ソリューション管理
脆弱性対応パッチオーケストレーションアプリケーション
脆弱性対応 Patch Orchestration with HCL BigFix アプリケーション
Security Support Common
セキュリティサポートオーケストレーション
サポートされているサードパーティの脆弱性スキャナーアプリケーション

脆弱性対応 パッチオーケストレーションアプリケーションテーブル

脆弱性対応 パッチオーケストレーションアプリケーションには次のテーブルが含まれます。

テーブル	説明
パッチの更新 [sn_vul_patch_orch_update]	個別のインスタンスで利用可能なパッチに関する情報を保存します。
デバイス更新 [sn_vul_patch_orch_m2m_src_ci_update]	検出されたアイテムレコードに表示されている、展開されたパッチに関するデータを展開ステータスとともに保存します。
コレクション [sn_vul_patch_orch_collection]	個別のインスタンスからのコレクションデータを格納します。
デバイスコレクション [sn_vul_patch_orch_m2m_src_ci_collection]	検出されたアイテムに関するコレクションデータを格納します。
パッチ展開 [sn_vul_patch_orch_deployment]	コレクションと CI に関する展開済みパッチに関する情報を保存します。
潜在的なパッチ [sn_vul_patch_orch_m2m_vuln_patch]	脆弱性の解決に使用される可能性があるパッチを特定するパッチおよび脆弱性に関するデータを保存します。

Vulnerability Response Patch Orchestration Integrations with HCL BigFix®

ServiceNow エンジニアリングによって開発された統合により、BigFix 製品とのオーケストレーションされたソリューション展開を構成します。次の統合は、ServiceNow Store からダウンロー

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ドする 脆弱性対応 Patch Orchestration Integration with HCL BigFix アプリケーションに含まれています。

Now Platform インスタンスに統合アプリケーションをインストールした後、これらの統合を表示するには、次に移動します: 統合 > **BigFix** パッチオーケストレーション統合 > 統合.脆弱性対応 アプリケーションは、BigFix エンドポイントとのこれらの統合によってインポートされたスケジュール済み時間間隔でデータを処理します。

統合	説明
BigFix コレクション統合	• この統合は毎日実行されるようにスケジュールされ、チェーンされた統合実行の最初に実行されます。 • コンピューターグループ (構成アイテム) を構成するコンピューターとコンピューターグループを BigFix アプリケーションから取得します。
BigFix Fixlet 統合	• スケジュールされている場合、この統合は BigFix コレクション統合の完了によってトリガーされます。オンデマンドで実行することもできます。 • 利用可能なすべての Fixlet (パッチ) に関する情報を BigFix サーバーから取得します。
BigFix デバイス Fixlet 統合	• スケジュールされている場合、この統合は BigFix Fixlet 統合の完了によってトリガーされます。オンデマンドで実行することもできます。 • 現在コンピューター (資産) にある Fixlet に関する情報を BigFix サーバーから取得します。
BigFix アクション統合	• スケジュールされている場合、この統合は BigFix Device Fixlet 統合の完了によってトリガーされます。オンデマンドで実行することもできます。 • IT チームによってスケジュールされた BigFix サーバーのパッチに関する情報を取得します。

脆弱性対応 **Patch Orchestration integration with HCL BigFix** の準備

次のセットアップタスクを実行して、統合の準備をします。

始める前に

必要なロール：admin。アプリケーションのインストールとロールの割り当てを行います。他のロールを次の表に示します。

このタスクについて

統合を成功させるには、統合前のタスクを計画して慎重に実行する必要があります。

これで、「脆弱性対応 Patch Orchestration with HCL BigFix アプリケーションのインストール」に進む準備が整いました。

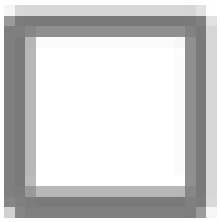
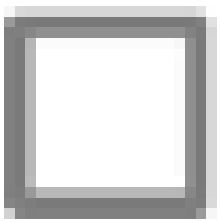
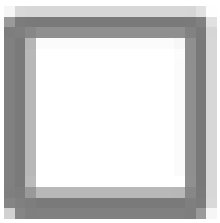
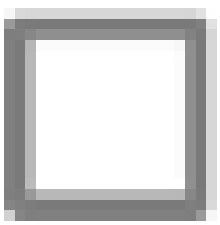
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 脆弱性対応 Patch Orchestration with HCL BigFix アプリケーションをスムーズにインストールして構成するには、提供されているチェックリストに従ってください。
2. アプリケーションをインストールする前に、次のチェックリストを印刷し、リストされているアイテムが完了していることを確認することをお勧めします。

   インストールと設定が完了したら、脆弱性とパッチ関連の情報を Now Platform® インスタンスにインポートします。

タスク	説明
	(オプション) まだインストールしてアクティブ化していない場合は、サードパーティアプリケーションをインストールする前に 脆弱性対応 アプリケーションをインストールすることもできます。 脆弱性対応 アプリケーションのインストールとアクティブ化の詳細については、「脆弱性対応 のインストール」を参照してください。この統合には、脆弱性対応 のバージョン 16.0 以降が必要です。
	まだインストールされていない場合は、エンタイトルメントを取得し、サードパーティのスキャナーアプリケーションをインストールして脆弱性データをインポートします。 脆弱性対応 でサポートされているサードパーティ製スキャナーの詳細については、「脆弱性対応 の統合」を参照してください。 「」を参照してください。
	まだインストールされていない場合は、エンタイトルメントを取得し、Vulnerability Response Patch Orchestration with HCL BigFix アプリケーションを Now Platform® インスタンスにダウンロードします。 「」を参照してください。
	BigFix 認証情報を取得します。 BigFix 製品にアクセスするために必要なアカウント名、パスワード、およびその他のサービス情報があることを確認します。
	統合を管理し、脆弱性一致アイテムを修正するグループまたはユーザーがいることを確認します。 admin システムアドミニストレーターは、エンタイトルメントを取得し、BigFix パッチオーケストレーションアプリケーションと統合に必要なその他のアプリケーションをダウンロードしてインストールします。アサインされていない場合、アドミニ

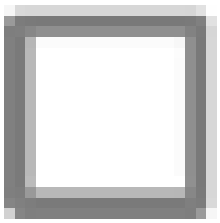
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスク	説明
	ストレーターは 脆弱性対応 のセットアップアシスタントで、または [ユーザー管理] モジュールから、脆弱性アドミン (sn_vul.vulnerability_admin) およびその他のロールをアサインします。 sn_vul.vulnerability_admin アサイン後、脆弱性アドミニストレーターは、BigFix 統合と他のサードパーティアプリケーションの構成を完了します。このロールは、脆弱性対応 (VR) アプリケーションとそのレコードに完全にアクセスできます。このロールは、すべての VR アプリケーション、ルール、サードパーティ統合、Vulnerability Response Patch Orchestration、および脆弱性ソリューション管理アプリケーションを設定します。 sn_vul_bigfix.configure_integration このロールを持つユーザーは、BigFix Patch Orchestration Integration アプリケーションを構成します。このロールには、ユーザーが BigFix コンソールに接続して Now Platform で統合インスタンスを設定できるようにする sn_vul_bigfix.read_integration と connection_admin 詳細ロールが含まれています。 sn_vul_bigfix.read_integration このロールを持つユーザーは、脆弱性対応 のレコードと、BigFix Patch Orchestration Integration アプリケーションおよびパッチオーケストレーションデータを表示できます。 sn_vul_patch_orch.configure_patch このロールを持つユーザーは、パッチを設定して適用することができます。変更管理がアクティブで、承認者がアサインされている場合、脆弱性一致アイテムまたはパッチ更新レコードからこのユーザーによって要求されたパッチは、承認のために送信されます。 sn_vul_patch_orch.read_patch このロールを持つユーザーは、レコードでパッチ情報を表示できます (読み取り専用)。このロールは、IT 修復および脆弱性マネージャーのワークスペースに必要な sn_vul.remediation_owner および sn_vuln.vulnerability_analyst ロールに継承されます。 承認者 承認者レベル 1 およびオプションで承認者レベル 2 にアサインされたユーザーと承認者グループが送信されたパッチ要求を承認します。デフォルトでは、パッチは展開前に承認のために承認者レベル 1 グループに送信されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスク	説明
	承認プロセスの詳細については、「脆弱性対応 を使用したパッチオーケストレーション」を参照してください。承認者とグループの設定の詳細については、「セットアップアシスタントを使用した脆弱性対応 ペルソナロールのアサイン」を参照してください。 システムアドミニストレーターは、統合のためにユーザーとグループにロールを最初にアサインします。デフォルトで脆弱性対応グループは利用可能になっています。まだ作成していない場合は、修復スペシャリストおよび脆弱性アナリストのロールに対して追加のグループを作成し、インスタンスのユーザー管理モジュールを使用してユーザーを追加することもできます。「ユーザーグループを作成」を参照してください。
	統合に必要なインスタンス内の機能、ルール、依存関係プラグイン、またはジョブが有効になっていることを確認します。 ○ Vulnerability Response Patch Orchestration with HCL BigFix は、スタンドアロンの MID サーバーを使用する必要があるオンプレミスの統合です。インスタンスの MID サーバーの詳細については、「MID サーバー」を参照してください。 ○ 次のように移動する。 システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて) をクリックし、プラグインを見つけます。インスタンスにインストールされていない場合は、インストールしてアクティブ化します。

次のタスク
これで、「脆弱性対応 Patch Orchestration with HCL BigFix アプリケーションのインストール」に進む準備が整いました。

脆弱性対応 **Patch Orchestration with HCL BigFix** アプリケーションのインストール

Vulnerability® Response Patch Orchestration with HCL BigFix アプリケーションを ServiceNow　Store からダウンロードします。

始める前に
必要なロール： sn_vul.vulnerability_admin ロールの初期アサインとアプリケーションのインストールを行う admin ロール。インストール後に Vulnerability Response Patch Orchestration with HCL BigFix およびその他のアプリケーションを構成する脆弱性アドミンロール (sn_vul.vulnerability_admin または sn_vul.admin (使用廃止)) 。

このタスクについて
アプリケーションをインストールする前に、脆弱性対応 Patch Orchestration integration with HCL BigFix の準備 のチェックリストのすべてのアイテムが完了していることを確認してください。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて).
2. **Vulnerability Response Patch Orchestration with HCL BigFix** アプリケーションを見つけて、[インストール] をクリックします。

   このアクションにより、ServiceNow Store からダウンロードしたアプリケーションがインストールされます。
3. または、セットアップアシスタントからアプリケーションをインストールすることもできます。セットアップアシスタントを使用したアプリケーションのインストールの詳細については、「セットアップアシスタントを使用した 脆弱性対応 サードパーティアプリケーションのインストール」を参照してください。

次のタスク
インストールが完了したら、次に移動します: **All** (すべて) > **BigFix** パッチオーケストレーション統合 > 構成 構成を続行します。

脆弱性対応 **Patch Orchestration Integration with HCL BigFix** の構成

アプリケーションをインストールしたら、BigFix アカウント情報を使用してアプリケーションを構成し、認証情報を検証します。

始める前に
必要なロール： v sn_vul.vulnerability_admin および sn_vul_bigfix.configure_integration

手順

1. 次のように移動する。 **BigFix** パッチオーケストレーション統合 > 構成.
2. フィールドに BigFix 情報と認証情報を入力します。

フィールド	説明
統合インスタンス	使用する BigFix インスタンスアカウントの名前 (例：BigFix Patch management integration)。
ホスト名	BigFix ホストの URL を入力します。
ユーザー名	BigFix アカウントのユーザー名を入力します。
パスワード	BigFix アカウントのパスワードを入力します。
MID サーバー	使用するリストからスタンドアロン MID サーバーの名前を入力します。Now Platform での MID サーバーと設定タスクの詳細については、「脆弱性対応 Patch Orchestration integration with HCL BigFix の準備」を参照してください。

3. [認証情報を保存してテスト] をクリックします。
   BigFix と Now Platform インスタンス間の接続のステータスが [検証ステータス] フィールドに表示されます。成功したテストが表示されない場合は、プロンプトに従います。
4. オプション: この統合では、ドメインセパレーションがサポートされています。
   複数の構成をインスタンスに追加できます。構成を追加するには次のステップを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. 次のように移動する。 **BigFix** パッチオーケストレーション統合 統合インスタンス。

b. アプリケーションスコープである Vulnerability Response Patch Orchestration with HCL BigFix が [アプリケーションスコープ] フィールドに表示されていることを確認します。

c. [新規] をクリックします。

d. フォームに入力します。

フィールド	説明
名前	統合インスタンスの名前。
アプリケーション	Vulnerability Response Patch Orchestration with HCL BigFix
統合	[読み取り専用] BigFix パッチ管理がデフォルトです。
アクティブ	デフォルトで有効にされています (オン)。オフにすると、インスタンスはアクティブになりません。

e. **[Submit]** をクリックします。
新しい統合インスタンスが [統合インスタンス] リストに表示されます。

f. ステップ 1 ～ 3 を繰り返して、統合インスタンスを設定し、認証情報をテストします。

5. パッチ要求の承認を設定します。
デフォルトでは、システムプロパティ [**sn_vul_patch_orch.patch_approval_required**] がアクティブ化されているため、パッチの展開がスケジュールされると、レビューおよび承認のために、レベル 1 - パッチ更新承認グループにアサインされたユーザーに送信されます。

sn_vul_patch_orch.configure_patch ロールを持つユーザーに承認なしでパッチをスケジュールするように設定する場合は、 [**sn_vul_patch_orch.patch_approval_required**] プロパティを無効にできます。スケジュールされたパッチが通常の作業時間と競合しないように、承認をアクティブ化しておくことをお勧めします。

> **注:**
> 承認システムプロパティを無効にすると、sn_vul_patch_orch.configure_patch ロールを持つすべてのユーザーが、レビューおよび承認なしでパッチをスケジュールおよび展開できます。

sn_vul.vulnerability_admin ロールを持つユーザーとして、 システムプロパティを無効にするには次の操作を実行します。

a. 次のように移動する。 **sys.properties.list**.

b. **sn_vul_patch_orch.patch_approval_required** を見つけてクリックし、レコードを開きます。

c. [値] フィールドに「false」と入力します。

d. [更新] をクリックします。

6. このプロパティを非アクティブ化しない場合は、パッチ要求の承認者をアサインする必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

sn_vul.vulnerability_admin ロールを持つユーザーは、次のステップを実行します。

a. 次のように移動する。 脆弱性対応 > アドミニストレーション > 承認ルール.

b. [パッチ更新承認承認ルールを展開] がリストに表示されない場合は、画面の左上にある緑色のフィルターアイコンの右側にある [すべて] をクリックしてリスト全体を表示します。

c. リストで [展開のパッチ更新の承認] をクリックします。

d. レコードで [承認構成] タブを選択し、[デフォルト構成：パッチ更新承認] をクリックします。

e. レコードで [レベル 1：パッチ更新の承認] をクリックします。

f. このグループにユーザーを追加します。

このグループに割り当てられたユーザーは、sn_vul_patch_orch.configure_patch ロールを持つユーザーによって送信されたパッチ要求を承認します。[自分の承認] に移動して、要求を表示および処理します。

7. [更新] をクリックして変更を保存します。

8. オプション: スケジュールされたパッチ要求を展開する前に複数の承認が必要になるように、複数レベルの承認を設定できます。

a. [デフォルト構成 - パッチ更新承認] レコードを表示した状態で、[新規] をクリックします。

b. フィールドに入力します。

フィールド	説明
名前	承認レベル名 (例：レベル **2 -** パッチ更新の承認)。
アクティブ	デフォルトで有効になっており、承認レベルが使用中であることを示します。
承認が必要	選択したレベルに必要な承認数を選択します。 ▪ 1 人の承認者が必要 ▪ すべてのユーザーの承認が必要
順序	ルール内のさまざまな構成の実行順序。たとえば、順序エントリーが 100 の構成は、順序エントリーが 200 の構成よりも前に実行されます。
ロール	リストからグループのロールを選択します。
承認ルール	承認ルールのテーブルとタイプの詳細が含まれています。
承認構成	承認構成が含まれています。
次を使用してアサイン	以下のいずれかのオプションを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	▪ ユーザーおよびユーザーグループ ▪ 承認テーブルフィールド ▪ スクリプト
グループ	複数のユーザーで構成される承認者レベルグループ。ユーザーは、指定する次のいずれかのロールを持っている必要があります。
ユーザー	グループにリストされているユーザーを編集します。

c. [送信] をクリックして編集を保存します。

脆弱性対応 **Patch Orchestration Integration with HCL BigFix** のパッチデータの表示

パッチデータ、パッチロールアップデータ、脆弱性情報、および脆弱性の修復ステータスがインスタンス内のレコードに表示されます。

脆弱性対応 ワークスペースでのパッチデータの表示

必要なロール：

- パッチを設定およびスケジュールするための sn_vul_patch_orch.configure_patch ロール
- sn_vul_patch_orch.read_patch を使用して、レコードのパッチ情報を表示します (読み取り専用)。このロールは、IT 修復および脆弱性マネージャーのワークスペースに必要な sn_vul.remediation_owner および sn_vuln.vulnerability_analyst ロールに継承されます。

IT 修復ワークスペースで次のパッチを表示できます。

- [ホーム] ビューでは、スコアカードをクリックして、VI の優先ソリューション、脆弱な CI、および VI の優先パッチを表示できます。
- [リスト] ビューでは、 [パッチ] リンクのすべてのパッチ更新レコード (VPU) と、自分に割り当てられているパッチ適用済みの脆弱性一致アイテム (VIT) を表示できます。

次のレコードからパッチをスケジュールできます。

- パッチ更新から (VPU)
- 修復タスク (RT)
- 検出されたアイテム (SDI) レコード

脆弱性マネージャーワークスペースでは、以下のようにパッチを表示できます。

- 監視トピックの [ホーム] ビューから、[脆弱性一致アイテム] タブで優先パッチと潜在的なパッチ、パッチスケジュール日、およびパッチがダウンロードされているかどうかを確認できます。
- 修復作業の [リスト] ビューでは、[脆弱性一致アイテム] タブで VI レコードのパッチデータを表示できます。

クラシック環境ビューから、 **All** (すべて) > 脆弱性対応 > パッチ.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

VR ワークスペースとクラシック環境ビューのパッチ更新レコード

パッチデータとパッチロールアップデータおよびステータスは、インスタンス内のレコードに表示されます。パッチレコードは、脆弱性対応 との統合のパッチオーケストレーション機能の一部として含まれています。IT 修復ワークスペースの [リスト] ビューから 脆弱性対応 ワークスペースのパッチ (VPU) レコードを表示します。クラシックビューと 脆弱性対応 ワークスペースの両方のパッチ更新レコードには、以下のデータが含まれています。

- Vulnerability Solution Management アプリケーションによってインポートされたパッチベンダーからの脆弱性ソリューションデータと情報。
- ソース修復ステータス。これには、パッチによって修正できる特定の脆弱性があるデバイスと、更新されていないデバイスの合計数が含まれます。
- 修復された VI の割合と、優先パッチとしてパッチがある合計 VI を含む修復ステータス。
- クラスビューのレコードの関連リンクにある関連デバイス、脆弱性一致アイテム、パッチ展開、およびパッチ要求。このデータは、脆弱性対応 ワークスペースのレコードのタブに表示されます。
- 修復オーナーが承認のために送信したパッチ要求。

脆弱性一致アイテムレコードのステータスロールアップ

レコードへのステータスロールアップの詳細については、「脆弱性対応 のパッチオーケストレーションでのパッチデータとステータスのロールアップ」を参照してください。

アクティブな VI 数をロールアップするレコード

すべての脆弱性にすべてのパッチをロールアップすることを避けるために、スケジュール済みジョブはアクティブな VI 数の変更のみを取得します。これらのカウント変更と関連データは、脆弱性対応 内の次のレコードにロールアップされます。

- VIT
- RT
- 脆弱性ソリューション
- パッチ更新

ソリューションのないパッチのデータの表示

ソリューションのないパッチを表示する方法の詳細については、「脆弱性対応 でのソリューションのないパッチの表示」を参照してください。

脆弱性対応のパッチデータ

脆弱性管理 (PA) および CISO ダッシュボードは、脆弱性対応 アプリケーションの パフォーマンスアナリティクス のサブスクリプションに含まれています。パフォーマンスアナリティクス のサブスクリプションがあっても、パッチオーケストレーション統合がインストールされていない場合、 [修復] タブは CISO ダッシュボードに表示されますが、データは入力されません。

脆弱性管理 (PA) ダッシュボードの場合は、次に移動します: **All** (すべて) > 脆弱性対応 > 概要.[修復] タブをクリックし、ページの下部までスクロールして、パッチ更新データ (スケジュールされているパッチとスケジュールされていないパッチ、ターゲットの日付がないパッチ、および週次の数) を表示します。

CISO ダッシュボードの場合は、次に移動します: **All** (すべて) > 脆弱性対応 > **CISO** ダッシュボード.[概要] タブを選択した状態で、ページの下部までスクロールして、パッチ範囲データ (重大度、スケジュールされているパッチとスケジュールされていないパッチ、およびターゲットの日付がないパッチ) を表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性対応 ダッシュボードの詳細については、「デフォルトの 脆弱性対応 ダッシュボードを使用する」、「脆弱性対応 ワークスペースを使用したパッチオーケストレーション」、「脆弱性対応 ダッシュボードでのパッチオーケストレーションデータの表示」を参照してください。

脆弱性対応 **Patch Orchestration Integration HCL BigFix** のパッチのスケージュール

Now Platform インスタンスの 脆弱性対応 アプリケーションのパッチ更新および修復タスクレコードからパッチをスケジュールします。

始める前に

バージョン 16.1 以降では、脆弱性対応 ワークスペースまたはクラシック環境からパッチをスケジュールできます。

必要なロール：

- パッチを設定およびスケジュールするための sn_vul_patch_orch.configure_patch ロール
- sn_vul_patch_orch.read_patch を使用して、レコードのパッチ情報を表示します (読み取り専用)。このロールは、IT 修復および脆弱性マネージャーのワークスペースに必要な sn_vul.remediation_owner および sn_vuln.vulnerability_analyst ロールに継承されます。

手順

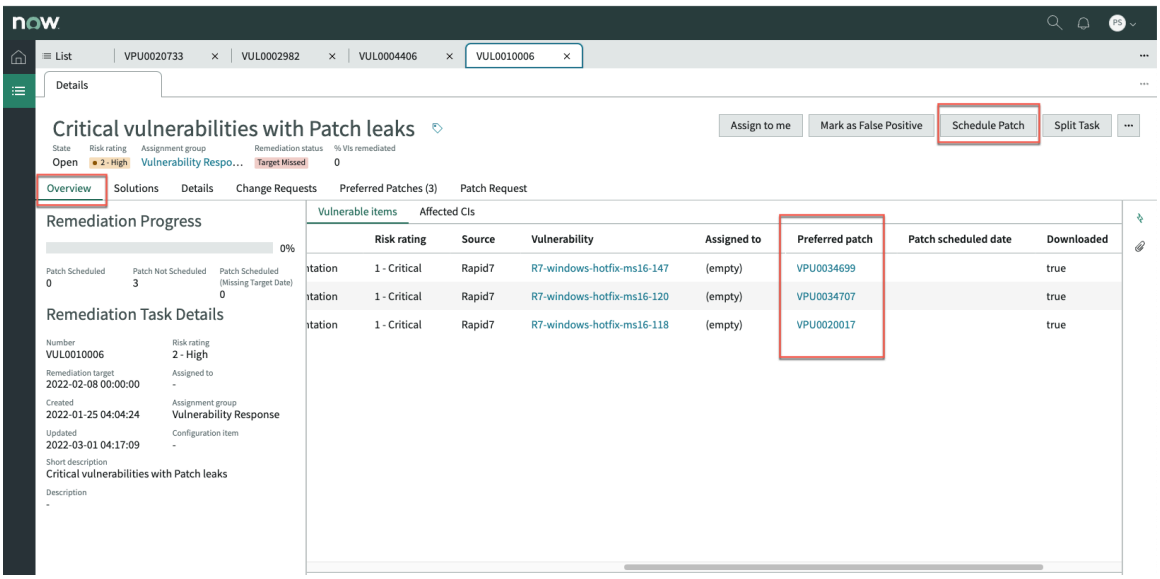
1. 脆弱性 脆弱性対応 ワークスペースで、sn_vul.remediation_owner ロールを持つユーザーとして、次の場所に移動します。 **All** (すべて) > 脆弱性対応 > **IT** 修復ワークスペース.
2. ホームページで、**[VI** の優先パッチ] をクリックします。
   割り当てられた優先パッチを含む VI のパッチ更新レコードのリストが表示されます。
3. 開くレコードを見つけてクリックします。
4. または、ワークスペースのリストビューから、 パッチ > **All** (すべて) [Patch Update] レコードを見つけます。
   [パッチ更新] レコードが表示されます。他のパッチが既にスケジュールされている可能性があるため、パッチをスケジュールする前にデータを確認することをお勧めします。
5. 表示されるデータと実行できる操作については、次のテーブルを参照してください。
6. [パッチをスケジュール] をクリックします。
7. ダイアログボックスで、フィールドに入力します。
8. [展開] をクリックします。
   パッチ要求がレビューのために送信されます。送信されたすべての要求のステータスは、以下から表示できます 例外要求 > **My requests** (自分の要求) リストビューから。
9. または、自分または自分のグループにアサインされた修復タスク (RT) からパッチをスケジュールすることもできます。

   注:
   修復タスクレコードからパッチをスケジュールするオプションは、パッチがタスク内の VI にマッピングされている (関連付けられている) 場合にのみ使用できます。これらのパッチは、[概要] タブを選択した状態で修復タスクレコードの右にスクロールすると、[優先パッチ] 列に表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

優先パッチを使用した修復タスク



10. RT レコードから [パッチをスケジュール] をクリックし、上記の手順に従ってダイアログでスケジュールします。
11. クラシック環境では、前述のステップのパッチをスケジュールできます。
これらのレコードを見つけるには、次の手順を実行します。

    a. クラシック環境で、次に移動します: 脆弱性対応 > パッチ > **All** (すべて).

    b. 表示されるリストから、[パッチ更新] レコードを見つけます。

    c. 修復タスクの場合は、次に移動します: 脆弱性対応 > 修復タスク レコードを見つけます。[修復ステータス] タブで修復ステータスを追跡します。レコードの下部の [関連リンク] にパッチデータが表示されます。

    d. [パッチをスケジュール] をクリックして、フィールドに入力します。

フィールド	説明
展開名	このパッチ展開の名前を入力します。この名前は、更新を追跡するのに役立ちます。
パッチ更新	リストの利用可能なパッチから 1 つ選択します。
資産	1 つ選択： ▪ コンピューターグループ：このパッチのコレクション (資産のグループ) を選択する場合は、このオプションを選択します。グループは、BigFix アプリケーションからインポートされた構成アイテムで構成されています。 ▪ コンピューターリスト：このパッチを適用する個々のコンピューター (資産) を選択する場合は、このオプションを選択します。表示されるダイアログで、メーカー、

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	場所、クラス、最終更新日時、メンテナンススケジュールに関するデータを確認できます。
開始時間と終了時間	期間の開始時間と終了時間を入力します。パッチの展開を開始するタイミングと、パッチをインストールできる最終日を入力します。

Vulnerability Response Patch Orchestration Integration with HCL BigFix の REST メッセージ

脆弱性対応 Patch Orchestration Integration with HCL BigFix REST メッセージは、BigFix API の呼び出しに使用されます。

BigFix ログイン

BigFix ログインの REST メッセージを使用して、REST API 要求を認証することもできます。REST メッセージの記録方法を変更すると、BigFix に対する認証要求に影響します。

パラメーター名	値	説明
sourceType	cumulative	ソース統合がどこからデータをプルするかを示します。コードで使用されます。変更は推奨されません。
sortDIR	desc	統合からプルされたデータのソート方向を示します。変更は推奨されません。
sortField	severity	データのソートの基準となるフィールドを示します。変更は推奨されません。
type	vuln	資産統合のために統合からフェッチするデータのタイプを示します。変更は推奨されません。

BigFix 統合

BigFix 統合の REST メッセージを使用して、BigFix から情報を取得できます。REST メッセージのレコードメソッドを変更すると、 情報を取得するための BigFix への要求が影響を受けます。REST メッセージには、次の REST メソッドが含まれています。

REST メソッド

REST メソッド	説明
GET フェッチデータ	指定されたクエリに基づいて、次のいずれかに関する情報を BigFix から取得します。 • コンピューター/コンピューターグループ • Fixlet

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

REST メソッド (続く)

REST メソッド	説明
	• コンピューター上の関連する Fixlet • アクション

パラメーター名	値	説明
url	ユーザーに基づく動的な値	BigFix コンソールのエンドポイントを示します

BigFix 展開パッチ

BigFix 統合の REST メッセージを使用して、Now Platform® から BigFix へのパッチをスケジュールすることができます。REST メッセージのレコードメソッドを変更すると、 情報を取得するための BigFix への要求が影響を受けます。REST メッセージには、次の REST メソッドが含まれています。

REST メソッド	説明
POST 展開パッチ	単一または複数のコンピューター上の BigFix コンソールへのパッチをスケジュールします。

パラメーター名	値	説明
url	ユーザーに基づく動的な値	BigFix コンソールのエンドポイントを示します。
title	ユーザーに基づく動的な値	展開のタイトル。
settings_tag	値を含む XML タグ名付き設定	さまざまなパラメーターを含む、パッチのスケジュール中に BigFix に送信される設定を示します。
computer_tag	値を含む XML タグ名付きコンピューター	パッチがスケジュールされるコンピューターのリストを示します。
site_name	パッチ更新の値	Fixlet が存在するサイトの名前。
fixlet_id	パッチ更新の値	Fixlet の ID。

Patch Orchestration Integration with HCL BigFix のデータ変換

データは 脆弱性対応 Patch Orchestration Integration® with HCL BigFix 統合から取得され、一連のデータソースによって処理されて、Now Platform® インスタンスで変換されます。

BigFix コレクションインポート

インポートされた資産 (コンピューターおよびコンピューターグループ) のデータは、BigFix コレクションインポート [sn_vul_bigfix_collection_import] テーブルにロードされます。BigFix

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Computer and Computer Groups Import TM (変換マップ?) を使用して、インポートされた情報を変換します。

> **注:**
> この変換マップを変更すると、BigFix コレクションインポートからのデータの処理方法が変更されます。

この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ をクリックし、BigFix Computer and Computer Groups Import TM を見つけます。次の表に、統合別の変換マップフィールドを示します。

BigFix Computer and Computer Groups インポート変換マップスクリプトのタイミング

スクリプト	説明
OnStart (インポートセットが変換を作成したとき)。	統合プロセスのスコープ変数 [sn_vul_bigfix] の値を初期化するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onBefore (インポートセットの変換が完了する前)。	CI ルックアップルールとコレクション、およびそれらの関係に基づいて CI を作成および更新するために使用されるスクリプト。結果に基づいて、このスクリプトはスコープ変数 [sn_vul_bigfix] の値を変更します。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onComplete (インポートセットが変換を完了したとき)	作成、更新、および無視される CI の数を設定するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

BigFix Fixlet インポート

インポートされた Fixlet のデータは、BigFix Fixlet インポート [sn_vul_bigfix_patch_update_import] テーブルにロードされます。

BigFix Fixlet Import TM は、インポートされた情報を変換するために使用されます。

> **注:**
> この変換マップを変更すると、BigFix Fixlet インポートからのデータの処理方法が変更されます。

この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ をクリックし、BigFix Fixlet Import TM を見つけます。

次の表に、統合別の変換マップフィールドを示します。

BigFix Fixlet インポート変換マップフィールド

ソースフィールド	ターゲットフィールド	説明
u_id	article_id	サイト内の Fixlet の一意の ID。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

BigFix Fixlet インポート変換マップフィールド (続く)

ソースフィールド	ターゲットフィールド	説明
u_id	source_id	サイト内の Fixlet の一意の ID。
U_site_name	Sn_vul_bigfix_site_name	Fixlet が依存する BigFix のサイト名。
U_display_name	タイトル	Fixlet のタイトル。
[Script]	Bulletin_id	ソリューションのソース ID。
[Script]	Sn_vul_solution	ソース ID に基づくソリューション。
U_source	bulletin_source	ソリューションのソースベンダー。
[Script]	Date_release	Fixlet のリリース日。
U_category	Update_category	Fixlet のカテゴリ。
[Script]	Is_highest_supersedence	Fixlet が最も優先度が高いかどうかを示すブール値。
[Script]	Is_downloaded	Fixlet がダウンロードされているかどうかを示すブール値。
[Script]	Integration_instance	Fixlet のインポート元のインスタンスの名前。
U_source_severity	Source_severity	Fixlet の重大度。
U_applicable_count	Num_total	Fixlet が欠落しているデバイスの合計数。
[Script]	Last_modified	Fixlet の最終変更日。

BigFix Fixlet インポート変換マップスクリプトのタイミング

スクリプト	説明
OnStart (インポートセットが変換を作成したとき)。	統合プロセスのスコープ変数 [sn_vul_bigfix] の値を初期化するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onBefore (インポートセットの変換が完了する前)。	スコープ変数 [sn_vul_bigfix] の値を更新するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onComplete (インポートセットが変換を完了したとき)	作成、更新、および無視される Fixlet の数を設定するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

BigFix Device Fixlet インポート

コンピューター上にインポートされた関連する Fixlet のデータは、BigFix Device Fixlet インポート [sn_vul_bigfix_patch_update_import] テーブルにロードされます。

BigFix Device Fixlet TM は、インポートされた情報を変換するために使用されます。

> **注:**
> この変換マップを変更すると、BigFix Device Fixlet インポートからのデータの処理方法が変更されます。

この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ をクリックし、BigFix Device Fixlet TM を見つけます。

次の表に、統合別の変換マップフィールドを示します。

BigFix Device Fixlet 変換マップスクリプトのタイミング

スクリプト	説明
OnStart (インポートセットが変換を作成したとき)。	統合プロセスのスコープ変数 [sn_vul_bigfix] の値を初期化するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onBefore (インポートセットの変換が完了する前)。	CI ルックアップルールとコレクション、およびそれらの関係に基づいて CI を作成および更新するために使用されるスクリプト。結果に基づいて、このスクリプトはスコープ変数 [sn_vul_bigfix] の値を変更します。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onComplete (インポートセットが変換を完了したとき)	作成、更新、および無視される CI の数を設定するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

BigFix アクションインポート

インポートされたアクションのデータは、BigFix アクションインポート [sn_vul_bigfix_patch_update_import] テーブルにロードされます。

BigFix Actions Import TM は、インポートされた情報を変換するために使用されます。

> **注:**
> この変換マップを変更すると、BigFix アクションインポートからのデータの処理方法が変更されます。

この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ をクリックし、BigFix Fixlet Import TM を見つけます。

次の表に、統合別の変換マップフィールドを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

BigFix アクションインポート変換マップフィールド

ソースフィールド	ターゲットフィールド	説明
u_id	source_id	アクションの一意の ID。
U_name	name	アクションの名前
[Script]	Sn_vul_bigfix_discovered_item	パッチが展開されている検出されたアイテムの参照
U_status	status	アクションのステータス
[Script]	Sn_vul_patch_orch_update	パッチの参照
U_apply_count	Count_success	アクションの成功回数。
U_retry_count	retry	アクションの再試行回数。
[Script]	Deployment_time	アクションの開始時間。
[Script]	deadline	アクションの終了時間。
[Script]	Source_created	アクションの作成時間。
[Script]	Integration_instance	アクションのインポート元のインスタンスの名前。

BigFix アクションインポート変換マップスクリプトのタイミング

スクリプト	説明
OnStart (インポートセットが変換を作成したとき)。	統合プロセスのスコープ変数 [sn_vul_bigfix] の値を初期化するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onBefore (インポートセットの変換が完了する前)。	スコープ変数 [sn_vul_bigfix] の値を更新するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onComplete (インポートセットが変換を完了したとき)	作成、更新、および無視されるアクションの数を設定するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

Vulnerability Response patch orchestration integration with HCL BigFix のワークフローの例

パッチオーケストレーションが HCL BigFix 製品でどのように機能するかを示す例を示します。

始める前に

たとえば、環境全体に 3 週間に 1 回パッチを適用するとします。最新のパッチ適用期間は 1 週間前に完了しましたが、最近判明した重大な脆弱性を修正するためのパッチを適用する必要があります。この脆弱性は重大であるため、次のスケジュールされたパッチにさらに 2 週間待つことはできません。

必要なロール：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 脆弱性マネージャーワークスペース用の sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin。
- IT 修復オーナーワークスペースを表示するための sn_vul.remediation_owner。
- パッチを設定およびスケジュールするための sn_vul_patch_orch.configure_patch ロール。
- sn_vul_patch_orch.read_patch を使用して、レコードのパッチ情報を表示します (読み取り専用)。このロールは、IT 修復および脆弱性マネージャーのワークスペースに必要な sn_vul.remediation_owner および sn_vuln.vulnerability_analyst ロールに継承されます。

このタスクについて

脆弱性マネージャーワークスペースで作業する脆弱性マネージャーまたはアナリストは、重要な脆弱性を含むインポートされた VI をキャプチャするために、監視トピックを作成するか、既存の監視トピックを編集することを検討してください。パッチオーケストレーション統合では、これらの脆弱性の修正と追跡に使用するパッチを確認することもできます。次の表は、パッチオーケストレーションの監視トピックに設定できるいくつかのサンプルを示しています。これらの例を参考にして、環境に最適な設定を判断してください。監視トピックの設定方法の詳細については、「で監視トピックを作成する Vulnerability Manager ワークスペース」を参照してください。

脆弱性マネージャーワークスペースでのパッチオーケストレーションのサンプル監視トピック

監視トピック名	説明
パッチ漏れのある重大な脆弱性	Risk rating is 1 - critical かつ Reason is Patch Not Scheduled
パッチ適用がスケジュールされた重大な脆弱性 (SLA 未適用)	Reason is Patch Scheduled (Missing Target Date)
パッチ適用がスケジュールされた重大な脆弱性	Risk rating is 1 - critical かつ Patch scheduled date is not empty かつ Reason is Patch Scheduled

- 脆弱性マネージャーまたはアナリストは、監視トピックと修復作業を作成した後、修復タスクを生成します。VI レコードと修復タスクから、[ディスカバリー] タブにドリルダウンし、BigFix 製品によってインポートされた資産とともに、追跡している脆弱性がある検出済みアイテムレコードを見つけることができます。
- 脆弱性アナリストまたはアドミンは、脆弱性に関連付けられたパッチデータを監視できます。検出されたアイテムレコードから特定の資産 (構成アイテム) にパッチを展開することもできます。

IT 修復スペシャリストには、パッチ展開を使用して脆弱性に対処するオプションがあります。

- パッチ更新レコード (VPU 番号) からパッチをスケジュールできます。
- 脆弱性一致アイテム (VI) に優先ソリューションがマッピングされていて、それらが自分または自分のグループにアサインされている場合は、これらの脆弱性一致アイテムを含む修復タスクからパッチをスケジュールできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. IT 修復スペシャリストは、IT 修復ワークスペースで [ホーム] ビューをクリックします。
2. ホームビューから、[アサインされた修復タスク] スコアカードをクリックしてレコードを表示します。

   この例では、重大な脆弱性に関連するテキストがないか、修復タスクの [簡単な説明] フィールドを確認します。たとえば、脆弱性マネージャーが、この重大な脆弱性がある VI (VIT#) を検出するために、「 パッチ漏れのある重大な脆弱性」という監視トピックを作成したとします。

   レコードを開いた状態で、VI や優先パッチをレビューし、自分または自分のグループがすでに承認のためにパッチ要求を送信しているかどうかを確認することもできます。
3. 十分な情報がある場合は、この修復タスクからパッチの要求を送信することもできます。

   注:
   レコードに関連付けられた VI にマッピングされたパッチがない場合、そのレコードでは [パッチをスケジュール] ボタンは使用できません。
4. [パッチをスケジュール] をクリックして、ダイアログのフィールドに入力します。
   パッチのスケジュール方法の詳細については、「脆弱性対応 Patch Orchestration Integration HCL BigFix のパッチのスケージュール」を参照してください。
5. または、IT 修復ワークスペースのリストビューから、修復タスク、脆弱性一致アイテム、ソリューション、およびパッチのリンクをクリックして、これらのレコードを表示することもできます。

   この例の場合、監視トピック名の代わりに、パッチの記事 ID またはセキュリティ情報 ID とタイトルがわかっている可能性があります。その場合、この脆弱性を持つ VI が自分または自分のグループに割り当てられているかどうかを確認します。パッチ更新レコードから、パッチ要求を送信できます。VI レコードから、潜在的なパッチを確認し、パッチ要求を送信する場合は関連する修復タスクを開くことができます。
6. ワークスペースにアクセスできない場合、またはクラシック環境からデータを表示してパッチをスケジュールする場合は、次の手順に従います。

   a. 次のように移動する。 **All** (すべて) > 脆弱性対応 > パッチ > **All** (すべて).

   b. 必要な [パッチ更新] レコードを見つけます。
      「Critical」リスクスコアのレコードをフィルタリングすることもできます。

   c. [修復ステータス] タブの関連する VI および修復済み VI の割合フィールドを確認します。
      VI で利用可能なパッチがある場合、[パッチをスケジュール] ボタンがレコードの右上に表示されます。

   d. 要求を送信する場合は、[パッチをスケジュール] をクリックします。
      パッチのスケジュール方法の詳細については、「脆弱性対応 Patch Orchestration Integration HCL BigFix のパッチのスケージュール」を参照してください。

   e. または、パッチ ID 情報がなく、グループにアサインされた修復タスクの [簡単な説明] フィールドで、重大な脆弱性に関連するテキストを確認することもできます。

   f. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 修復タスク > 所属グループにアサイン済み.

   g. 必要なレコードを見つけてクリックして開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

開いているレコードの [修復ステータス] タブで、VI および 修復された VI の割合を確認します。VI レコード、優先ソリューション、優先パッチ、およびパッチ要求の [関連リンク] をクリックします。

> **注:**
> レコードに関連付けられた VI にマッピングされたパッチがない場合、そのレコードでは [パッチをスケジュール] ボタンは使用できません。

h. パッチ要求を送信する場合は、レコードから [パッチをスケジュール] をクリックします。

脆弱性対応 **Patch Orchestration Integration with Microsoft SCCM** の概要

Microsoft System Center Configuration Manager (SCCM) 製品と 脆弱性対応 の統合により、資産の重大な脆弱性に対するパッチとパッチの展開を管理します。

脆弱性対応 を使用したパッチオーケストレーション

脆弱性対応 を使用したパッチオーケストレーションでは、サードパーティのソリューション統合、パッチベンダー、および脆弱性スキャナーからのスケジュール済みインポートが使用されます。スキャナー検出データは、環境内の資産を脆弱性とそれらを修正できるパッチ更新と照合します。承認のためにパッチ要求を送信し、脆弱性一致アイテムを解決するためのパッチ更新をスケジュールし、修復の進捗状況すべてを Now Platform インスタンスから監視します。

脆弱性対応 **Patch Orchestration with Microsoft SCCM**

Vulnerability® Response Patch Orchestration with the Microsoft SCCM アプリケーションを ServiceNow 脆弱性ソリューション管理、パッチオーケストレーション、および 脆弱性対応 アプリケーションと併用すると、脆弱性マネージャーとアナリストは次のタスクを実行できます。

- パッチのタイプとベンダーのソリューション (パッチ) に関する詳細なコンテキストと情報を表示します。
- 脆弱性対応 ワークスペースのレコードから、脆弱性とソリューションのデータ、および脆弱性の修復の進捗状況を表示および監視します。

IT スペシャリストと修復オーナーは、次のタスクを実行できます。

- Windows、CentOS、macOS、Oracle、およびその他の資産に対して、Microsoft SCCM 製品でサポートされているパッチを営業時間外に定期的に展開し、作業の競合を回避します。
- 脆弱性がある未パッチ資産、またはサードパーティスキャナーからインポートされた検出データから、パッチスケジュールによって正常に更新されなかった資産を特定します。
- IT 修復ワークスペースまたはクラシック UI から、パッチ更新、修復タスク、および検出されたアイテムレコードからパッチが適用されていない脆弱な資産に対して利用可能なパッチをスケジュールします。

脆弱性対応 および **Microsoft SCCM** アプリケーションで使用される主要な用語

構成アイテム (CI)

CI は、構成管理データベース (CMDB) にリストされている既存の資産です。Microsoft SCCM は CI (デバイス) を呼び出します。

コレクションとデバイスコレクション

資産のグループを指す Microsoft SCCM 製品で使用される用語。

脆弱性一致アイテム

CMDB 内の既存の資産と一致するインポートされた脆弱性。

インスタンス

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Microsoft SCCM アプリケーションの個別のアカウント。各ユーザーアカウントは、Microsoft SCCM アプリケーションのインスタンスにすることができます。この用語は、Now Platform インスタンスの一意の安全な Web アドレスを意味します。

統合

統合とは、Microsoft SCCM マシンとの統合など、サードパーティのソースから情報を取得する Now Platform のスケジュール済みジョブです。

ソリューション

この統合のコンテキストには、潜在的と優先の 2 つのタイプのソリューションがあります。潜在的なソリューションは、脆弱性に対処する可能性があるソリューションです。脆弱性には多くの潜在的なソリューションがあります。優先ソリューションは、検出された特定の脆弱性に対して最も効果的なソリューションと一致します。

パッチ

脆弱性を修正するソフトウェア更新。Microsoft SCCM アプリケーションでは、パッチはパッチと呼ばれます。たとえば、Microsoft SCCM には Windows、CentOS、MAC、Oracle、およびその他の製品用のパッチがあります。

優先パッチ

優先パッチは、特定の脆弱性を修正することを目的としたソフトウェア更新です。パッチが展開されると、特定の脆弱性に関連する脆弱性一致アイテムにマッピングされ、それらを修正します。

修復タスク、または 脆弱性対応 の v15.0 より前の脆弱性グループ

脆弱性を修正するために必要なアクションの 脆弱性対応 アプリケーション内の脆弱性一致アイテムのリスト。

展開

この統合における展開とは、マシンにパッチを適用、開始、またはスケジュールする場合を指します。Microsoft SCCM からダウンロードしたパッチを Now Platform に展開するには、脆弱性対応 の個々のレコードから検出されたアイテム、パッチ、または修復タスクに移動します。スケジュール済みジョブを含むパッチを個々のマシンまたはコンピューターグループに展開できます。

Now Platform での展開は、マルチソースをサポートする統合を指す場合もあります。単一の統合の存在は、統合の展開と呼ばれます。展開とは、環境全体の統合と製品のことです。たとえば、お使いの環境に Microsoft SCCM 脆弱性統合を複数展開する場合があります。

脆弱性ソリューション管理 および 脆弱性対応 Patch Orchestration Integration with Microsoft SCCM

脆弱性ソリューション管理 アプリケーションは、脆弱性の検出結果とそれらを修正するソリューション (パッチ) のブレークダウンを関連付ける Now Platform アプリケーションです。組織に最も大きな影響を与える製品やサービス、構成の更新、およびその他のコントロールに対するサードパーティからのソフトウェアパッチを特定します。サードパーティのスキャナー情報とともに、脆弱性対応のソリューション管理、脆弱性対応、および Vulnerability Response Patch Orchestration with Microsoft SCCM アプリケーションを連携して、ソリューションから脆弱性、脆弱性一致アイテムに優先パッチをロールアップして、使用している環境で脆弱性を修正してクローズすることができます。脆弱性対応のソリューション管理、脆弱性対応、および 脆弱性対応 Patch Orchestration Microsoft SCCM Integration アプリケーションはすべて ServiceNow Store で入手可能です。

必要な Now Platform ロール

統合のインストール、構成、および修復タスクには、Now Platform インスタンスで次のロールが必要です。

admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このロールを持つユーザーは、ServiceNow Store のアプリケーションのエンタイトルメントを取得し、Now Platform のインスタンスにダウンロードします。

sn_vul.vulnerability_admin

このロールを持つユーザーは、Now Platform インスタンスでアプリケーションをアクティブ化し、脆弱性対応 アプリケーションの構成を完了します。このロールは、脆弱性対応 (VR) アプリケーションとそのレコードに完全にアクセスできます。このアドミンユーザーは、すべての VR アプリケーション、ルール、およびサードパーティ統合を設定します。

sn_vul_sccm.configure_integration

このロールを持つユーザーは、Microsoft SCCM Patch Orchestration Integration アプリケーションを構成します。このロールには、sn_vul_sccm.read_integration の詳細なロールが含まれています。

sn_vul_sccm.read_integration

このロールを持つユーザーは、脆弱性対応 のレコードと、Microsoft SCCM Patch Orchestration Integration アプリケーションおよびパッチオーケストレーションデータを表示できます (読み取り専用)。

sn_vul_patch_orch.configure_patch

このロールを持つユーザーは、パッチを設定して適用することができます。

sn_vul_patch_orch.read_patch

このロールを持つユーザーは、パッチ情報を表示できます (読み取り専用)。

承認者

展開する前に、送信されたパッチ要求を承認する場合は、承認者レベル 1 と承認者レベル 2 の承認者グループにユーザーをアサインします。

セットアップアシスタントを使用したこのロールの割り当ての詳細については、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。

CI ルックアップルール

データが Microsoft SCCM アプリケーションからインポートされると、脆弱性対応 アプリケーションがリソース ID データを使用して 構成管理データベース (CMDB) 内の一致を自動的に検索します。CI ルックアップルールは、CI (資産) を識別し、VI の作成時にそれらを脆弱性一致アイテム (VI) レコードに追加する際に使用されます。次の CI ルックアップルールはベースシステムに付属しており、CI (資産) を識別して、検出されたアイテムに追加する際に使用されます。

このルックアップルールは、Service Graph Connector with SCCM によって取り込まれたデータに依存しています。SCCM 統合を実行する前に、CMDB 統合をインストールして実行する必要があります。SCCM サーバーが複数インストールされている場合は、[SCCM パッチオーケストレーション構成] ページでサービスグラフコネクタ 接続エイリアスを構成できます。

MID サーバー

Vulnerability Response Patch Orchestration with Microsoft SCCM はオンプレミスの統合です。MID サーバークラスターに含まれていないスタンドアロン Windows MID サーバーが必要です。MID サーバーは、SCCM サーバーからデータをインポートするために、インスタンスからリモートマシンでスクリプトを実行する必要があります。この統合用の API は、Now Platform インスタンスで設定した MID サーバーを使用して呼び出されます。脆弱性対応 Patch Orchestration Integration with Microsoft SCCM の準備。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Vulnerability Response Patch Orchestration with the Microsoft SCCM アプリケーションの統合と依存関係

Vulnerability Response Patch Orchestration with Microsoft System Center Configuration Manager (SCCM) 統合には、次の製品と依存関係アプリケーションが必要です。これらのアプリケーションは ServiceNow Store で入手できます。

パッチオーケストレーション統合に必要なアプリケーションと依存関係の利用可能なバージョン

脆弱性対応 のワークスペースとクラシック UI でパッチオーケストレーションデータと利用可能な更新 (パッチ) を表示するには、次のアプリケーションが必要です。リストされているすべてのアプリケーションは ServiceNow Store で入手できます。一部のアプリケーションには別のサブスクリプションが必要です。

必要なアプリケーションとファミリーリリースと互換性のあるバージョンについての詳細は、HI ナレッジベース記事「Vulnerability Response Compatibility Matrix and Release Schema Changes (脆弱性対応互換性マトリクスおよびリリーススキーマの変更点) [KB0856498]」を参照してください。

アプリケーションとリリースバージョン
脆弱性対応
脆弱性ソリューション管理
脆弱性対応パッチオーケストレーションアプリケーション
脆弱性対応と Microsoft SCCM のパッチオーケストレーションアプリケーション
Security Support Common
セキュリティサポートオーケストレーション
SCCM とのサービスグラフコネクタ

脆弱性対応 パッチオーケストレーションアプリケーションテーブル

脆弱性対応 パッチオーケストレーションアプリケーションには次のテーブルが含まれます。

テーブル	説明
パッチの更新 [sn_vul_patch_orch_update]	個別のインスタンスで利用可能なパッチに関する情報を保存します。
デバイス更新 [sn_vul_patch_orch_m2m_src_ci_update]	検出されたアイテムレコードに表示されている、展開されたパッチに関するデータを展開ステータスとともに保存します。
コレクション [sn_vul_patch_orch_collection]	個別のインスタンスからのコレクションデータを格納します。
デバイスコレクション [sn_vul_patch_orch_m2m_src_ci_collection]	検出されたアイテムに関するコレクションデータを格納します。
パッチ展開 [sn_vul_patch_orch_deployment]	コレクションと CI に関する展開済みパッチに関する情報を保存します。
潜在的なパッチ [sn_vul_patch_orch_m2m_vuln_patch]	脆弱性の解決に使用される可能性があるパッチを特定するパッチおよび脆弱性に関するデータを保存します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Vulnerability Response Patch Orchestration with MicrosoftSCCM 統合

ServiceNow® エンジニアリングによって開発された統合により、Microsoft SCCM®製品とのオーケストレーションされたソリューション展開を構成します。次の統合は、ServiceNow Store からダウンロードする Microsoft SCCM Patch Orchestration Integration アプリケーションに含まれています。

Now Platform インスタンスに統合アプリケーションをインストールした後、これらの統合を表示するには、次に移動します: 統合 > **SCCM** パッチオーケストレーション統合 > 統合.脆弱性対応 アプリケーションは、Microsoft SCCM エンドポイントとのこれらの統合によってインポートされた、スケジュール済み時間間隔でデータを処理します。

統合	説明
Microsoft SCCM コレクション統合	• この統合は毎日実行されるようにスケジュールされ、チェーンされた統合実行の最初に実行されます。 • SCCM コレクションからデバイスコレクションを取得します。
Microsoft SCCM デバイスコレクション統合	• スケジュールされている場合、この統合は SCCM コレクション統合の完了によってトリガーされます。オンデマンドで実行することもできます。 • この統合では、各コレクションのデバイスがフェッチされます。この統合により、検出されたアイテムテーブルと [デバイスコレクション] テーブルにレコードが作成されます。
Microsoft SCCM パッチ更新統合	• スケジュールされている場合、この統合は SCCM デバイスコレクション統合の完了によってトリガーされます。オンデマンドで実行することもできます。 • デバイス (資産) にインストールされているか欠落しているパッチに関する情報を SCCM サーバーから取得します。
Microsoft SCCM 展開統合	• スケジュールされている場合、この統合はパッチ更新統合の完了によってトリガーされます。オンデマンドで実行することもできます。 • IT チームによってスケジュールされた、SCCM サーバーにあるパッチに関する情報を取得します。

脆弱性対応 Patch Orchestration Integration with Microsoft SCCM の準備

次のセットアップタスクを実行して、統合の準備をします。

始める前に

必要なロール：admin。アプリケーションのインストールとロールの割り当てを行います。他のロールを次の表に示します。

このタスクについて

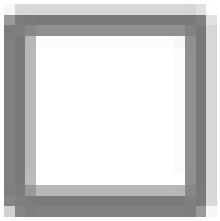
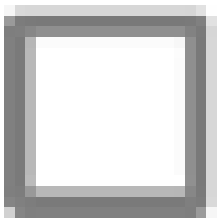
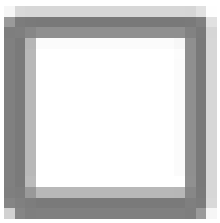
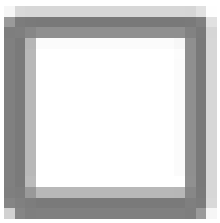
統合を成功させるには、統合前のタスクを計画して慎重に実行する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

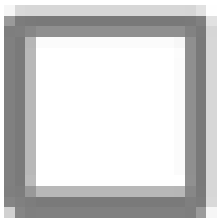
手順

1. Vulnerability Response Patch Orchestration with Microsoft SCCM アプリケーションをスムーズにインストールして構成するには、以下に提供されているチェックリストに従ってください。
2. アプリケーションをインストールして、脆弱性とパッチ関連情報を Now Platform® インスタンスにインポートする前に、次のチェックリストを印刷し、リストされているアイテムが完了していることを確認することをお勧めします。

タスク	説明
	(オプション) まだインストールしてアクティブ化していない場合は、サードパーティアプリケーションをインストールする前に 脆弱性対応 アプリケーションをインストールすることもできます。 脆弱性対応 アプリケーションのインストールとアクティブ化の詳細については、「脆弱性対応 のインストール」を参照してください。この統合には、脆弱性対応 のバージョン 16.1 以降が必要です。
	まだインストールされていない場合は、エンタイトルメントを取得し、サードパーティのスキャナーアプリケーションをインストールして脆弱性データをインポートします。 脆弱性対応 でサポートされているサードパーティ製スキャナーの詳細については、「脆弱性対応 の統合」を参照してください。 「」を参照してください。
	まだインストールされていない場合は、エンタイトルメントを取得し、Vulnerability Response Patch Orchestration® with Microsoft SCCM アプリケーションを Now Platform® インスタンスにダウンロードします。 「」を参照してください。
	Microsoft SCCM 認証情報を取得します。 Microsoft 製品にアクセスするために必要なアカウント名、パスワード、およびその他のサービス情報があることを確認します。

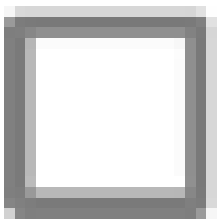
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスク	説明
	統合を管理し、脆弱性一致アイテムを修正するグループまたはユーザーがいることを確認します。 admin システムアドミニストレーターは、エンタイトルメントを取得し、Microsoft SCCM パッチオーケストレーションアプリケーションと統合に必要なその他のアプリケーションをダウンロードしてインストールします。アサインされていない場合、アドミニストレーターは 脆弱性対応 のセットアップアシスタントで、または [ユーザー管理] モジュールから、脆弱性アドミン (sn_vul.vulnerability_admin) およびその他のロールをアサインします。 sn_vul.vulnerability_admin アサイン後、脆弱性アドミニストレーターは、Microsoft SCCM 統合とその他のサードパーティアプリケーションの構成を完了します。このロールは、脆弱性対応 (VR) アプリケーションとそのレコードに完全にアクセスできます。このロールは、すべての VR アプリケーション、ルール、サードパーティ統合、脆弱性対応 パッチオーケストレーションアプリケーションおよび Vulnerability Solution Management アプリケーションを設定します。 sn_vul_sccm.configure_integration このロールを持つユーザーは、Microsoft SCCM Patch Orchestration Integration アプリケーションを構成します。このロールには、ユーザーが SCCM コンソールに接続して Now Platform で統合インスタンスを設定できるようにする sn_vul_sccm.read_integration と connection_admin granular 詳細ロールが含まれています。 sn_vul_sccm.read_integration このロールを持つユーザーは、脆弱性対応のレコードと、Microsoft SCCM Patch Orchestration Integration アプリケーションおよびパッチオーケストレーションデータを表示できます (読み取り専用)。 sn_vul_patch_orch.configure_patch このロールを持つユーザーは、パッチを設定して適用することができます。変更管理がアクティブで、承認者がアサインされている場合、脆弱性一致アイテムまたはパッチ更新レコードからこのユーザーによって要求されたパッチは、承認のために送信されます。 sn_vul_patch_orch.read_patch このロールを持つユーザーは、レコードでパッチ情報を表示できます (読み取り専用)。このロール

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスク	説明
	は、IT 修復および脆弱性マネージャーのワークスペースに必要な sn_vul.remediation_owner および sn_vuln.vulnerability_analyst ロールに継承されます。 承認者 承認者レベル 1 およびオプションで承認者レベル 2 にアサインされたユーザーと承認者グループが送信されたパッチ要求を承認します。デフォルトでは、パッチは展開前に承認のために承認者レベル 1 グループに送信されます。 承認プロセスの詳細については、「Vulnerability Response Patch Orchestration with Microsoft SCCM 統合の構成」を参照してください。承認者とグループの設定の詳細については、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。 システムアドミニストレーターは、統合のためにユーザーとグループにロールを最初にアサインします。デフォルトで 脆弱性対応 グループは利用可能になっています。まだ作成していない場合は、修復スペシャリストおよび脆弱性アナリストのロールに対して追加のグループを作成し、インスタンスのユーザー管理モジュールを使用してユーザーを追加することもできます。「ユーザーグループを作成」を参照してください。
	統合に必要なインスタンス内の機能、ルール、依存関係プラグイン、またはジョブが有効になっていることを確認します。 ○ Vulnerability Response Patch Orchestration with Microsoft SCCM は、スタンドアロン Windows MID サーバーを使用する必要があるオンプレミスの統合です。インスタンスの MID サーバーの詳細については、「MID サーバー」を参照してください。 ○ 次のように移動する。 システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて) をクリックし、プラグインを見つけます。インスタンスにインストールされていない場合は、インストールしてアクティブ化します。

脆弱性対応 **Patch Orchestration with Microsoft SCCM** アプリケーションのインストール

アプリケーションを ServiceNow Store からダウンロードします。

始める前に

アプリケーションをインストールする前に、脆弱性対応 Patch Orchestration Integration with Microsoft SCCM の準備 のチェックリストのすべてのアイテムが完了していることを確認してください。

必要なロール： sn_vul.vulnerability_admin ロールの初期アサインとアプリケーションのインストールを行う admin ロール。インストール後に 脆弱性対応 Patch Orchestration Microsoft SCCM およびその他のアプリケーションを構成する脆弱性アドミンロール (sn_vul.vulnerability_admin または sn_vul.admin (使用廃止))。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。準本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、ServiceNow Store アプリケーションのアクティブ化 に進むためにエンタイトルメントを取得する必要はありません。

手順

1. 次のように移動する。 **All** (すべて) > システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて).
2. 脆弱性対応と **Microsoft SCCM** のパッチオーケストレーションアプリケーションを見つけて、[インストール] をクリックします

   このアクションにより、ServiceNow Store からダウンロードしたアプリケーションがインストールされます。
3. または、セットアップアシスタントからアプリケーションをインストールすることもできます。セットアップアシスタントを使用したアプリケーションのインストールの詳細については、「セットアップアシスタントを使用した 脆弱性対応 サードパーティアプリケーションのインストール」を参照してください。

次のタスク
インストールが完了したら、次に移動します: **All** (すべて) > **Microsoft SCCM** パッチオーケストレーション統合 > 構成 構成を続行します。

Vulnerability Response Patch Orchestration with Microsoft SCCM 統合の構成

アプリケーションをインストールしたら、アカウント情報を使用してアプリケーションを構成し、認証情報を検証します。

始める前に
必要なロール：sn_vul.vulnerability_admin および sn_vul_sccm.configure_integration

手順

1. 次のように移動する。 **All** (すべて) > **Microsoft SCCM** パッチオーケストレーション統合 > 構成.
2. フィールドに Microsoft SCCM 情報と認証情報を入力します。

フィールド	説明
統合インスタンス	使用する Microsoft SCCM インスタンスアカウントの名前 (例：Microsoft SCCM Patch management integration)。
ホスト名	Microsoft SCCM ホストの URL を入力します。
ユーザー名	Microsoft SCCM アカウントのユーザー名を入力します。
パスワード	Microsoft SCCM アカウントのパスワードを入力します。
MID サーバー	使用するリストからスタンドアロン MID サーバーの名前を入力します。Now Platform での MID サーバーと設定タスクの詳細については、「脆弱性対応 Patch Orchestration

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	Integration with Microsoft SCCM の準備」を参照してください。

3. [認証情報を保存してテスト] をクリックします。
Microsoft SCCM と Now Platform インスタンス間の接続のステータスが [検証ステータス] フィールドに表示されます。成功したテストが表示されない場合は、プロンプトに従います。
4. オプション: この統合では、ドメインセパレーションがサポートされています。
複数の構成をインスタンスに追加できます。構成を追加するには次のステップを実行します。

   a. 次のように移動する。 **All** (すべて) > **Microsoft SCCM** パッチオーケストレーション統合 統合インスタンス。

   b. アプリケーションスコープである脆弱性対応と Microsoft SCCM のパッチオーケストレーションが [アプリケーションスコープ] フィールドに表示されていることを確認します。

   c. [新規] をクリックします。

   d. フォームに入力します。

フィールド	説明
名前	統合インスタンスの名前。
アプリケーション	Vulnerability Response Patch Orchestration with Microsoft SCCM
統合	[読み取り専用] Microsoft SCCM パッチ管理がデフォルトです。
アクティブ	デフォルトで有効にされています。オフにすると、インスタンスはアクティブになりません。

   e. **[Submit]** をクリックします。
   新しい統合インスタンスが [統合インスタンス] リストに表示されます。

   f. ステップ 1 ～ 3 を繰り返して、統合インスタンスを設定し、認証情報をテストします。

5. パッチ要求の承認を設定します。
デフォルトでは、システムプロパティ [**sn_vul_patch_orch.patch_approval_required**] がアクティブ化されているため、パッチの展開がスケジュールされると、レビューおよび承認のために、レベル 1 - パッチ更新承認グループにアサインされたユーザーに送信されます。

   sn_vul_patch_orch.configure_patch ロールを持つユーザーに承認なしでパッチをスケジュールするように設定する場合は、 [**sn_vul_patch_orch.patch_approval_required**] プロパティを無効にできます。スケジュールされたパッチが通常の作業時間と競合しないように、承認をアクティブ化しておくことをお勧めします。

   注:
   承認システムプロパティを無効にすると、sn_vul_patch_orch.configure_patch ロールを持つすべてのユーザーが、レビューおよび承認なしでパッチをスケジュールおよび展開できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

sn_vul.vulnerability_admin ロールを持つユーザーとして、 システムプロパティを無効にするには次の操作を実行します。

a. 次のように移動する。 **All** (すべて) > **sys.properties.list**.

b. **sn_vul_patch_orch.patch_approval_required** を見つけてクリックし、レコードを開きます。

c. [値] フィールドに「false」と入力します。

d. [更新] をクリックします。

6. このプロパティを非アクティブ化しない場合は、パッチ要求の承認者をアサインする必要があります。
sn_vul.vulnerability_admin ロールを持つユーザーは、次のステップを実行します。

a. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 承認ルール.

b. [パッチ更新承認承認ルールを展開] がリストに表示されない場合は、画面の左上にある緑色のフィルターアイコンの右側にある [すべて] をクリックしてリスト全体を表示します。

c. リストで [展開のパッチ更新の承認] をクリックします。

d. レコードで [承認構成] タブを選択し、[デフォルト構成：パッチ更新承認] をクリックします。

e. レコードで [レベル 1：パッチ更新の承認] をクリックします。

f. このグループにユーザーを追加します。

このグループに割り当てられたユーザーは、sn_vul_patch_orch.configure_patch ロールを持つユーザーによって送信されたパッチ要求を承認します。[自分の承認] に移動して、要求を表示および処理します。

7. [更新] をクリックして変更を保存します。

8. オプション: スケジュールされたパッチ要求を展開する前に複数の承認が必要になるように、複数レベルの承認を設定できます。

a. [デフォルト構成 - パッチ更新承認] レコードを表示した状態で、[新規] をクリックします。

b. フィールドに入力します。

フィールド	説明
名前	承認レベル名 (例：レベル **2 -** パッチ更新の承認)。
アクティブ	デフォルトで有効になっており、承認レベルが使用中であることを示します。
承認が必要	選択したレベルに必要な承認数を選択します。 ▪ 1 人の承認者が必要 ▪ すべてのユーザーの承認が必要
順序	ルール内のさまざまな構成の実行順序。たとえば、順序エントリーが 100 の構成は、順序

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	エントリーが 200 の構成よりも前に実行されます。
ロール	リストからグループのロールを選択します。
承認ルール	承認ルールのテーブルとタイプの詳細が含まれています。
承認構成	承認構成が含まれています。
次を使用してアサイン	以下のいずれかのオプションを選択します。 ▪ ユーザーおよびユーザーグループ ▪ 承認テーブルフィールド ▪ スクリプト
グループ	複数のユーザーで構成される承認者レベルグループ。ユーザーは、指定する次のいずれかのロールを持っている必要があります。
ユーザー	グループにリストされているユーザーを編集します。

c. [送信] をクリックして編集を保存します。

脆弱性対応 **Patch Orchestration Integration with Microsoft SCCM** のパッチデータとパッチデータロールアップの表示

パッチデータ、パッチロールアップデータ、脆弱性情報、および脆弱性の修復ステータスがインスタンス内のレコードに表示されます。

脆弱性対応 ワークスペースでのパッチデータの表示

必要なロール：

- パッチを設定およびスケジュールするための sn_vul_patch_orch.configure_patch ロール
- sn_vul_patch_orch.read_patch を使用して、レコードのパッチ情報を表示します (読み取り専用)。このロールは、IT 修復および脆弱性マネージャーのワークスペースに必要な sn_vul.remediation_owner および sn_vuln.vulnerability_analyst ロールに継承されます。

IT 修復ワークスペースで次のパッチを表示できます。

- [ホーム] ビューでは、スコアカードをクリックして、VI の優先ソリューション、脆弱な CI、および VI の優先パッチを表示できます。
- [リスト] ビューでは、 [パッチ] リンクのすべてのパッチ更新レコード (VPU) と、自分に割り当てられているパッチ適用済みの脆弱性一致アイテム (VIT) を表示できます。

次のレコードからパッチをスケジュールできます。

- パッチ更新から (VPU)
- 修復タスク (RT)
- 検出されたアイテム (SDI) レコード

脆弱性マネージャーワークスペースでは、以下のようにパッチを表示できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 監視トピックの [ホーム] ビューから、[脆弱性一致アイテム] タブで優先パッチと潜在的なパッチ、パッチスケジュール日、およびパッチがダウンロードされているかどうかを確認できます。
- 修復作業の [リスト] ビューでは、[脆弱性一致アイテム] タブで VI レコードのパッチデータを表示できます。

クラシック環境ビューから、 **All** (すべて) > 脆弱性対応 > パッチ.

VR ワークスペースとクラシック環境ビューのパッチ更新レコード

パッチデータとパッチロールアップデータおよびステータスは、インスタンス内のレコードに表示されます。パッチレコードは、脆弱性対応 との統合のパッチオーケストレーション機能の一部として含まれています。IT 修復ワークスペースの [リスト] ビューから 脆弱性対応 ワークスペースのパッチ (VPU) レコードを表示します。クラシック環境と 脆弱性対応 ワークスペースの両方のパッチ更新レコードには、次のデータが含まれています。

- Vulnerability Solution Management アプリケーションによってインポートされたパッチベンダーからの脆弱性ソリューションデータと情報。
- ソース修復ステータス。これには、パッチによって修正できる特定の脆弱性があるデバイスの合計数が含まれます。さらに、更新が適用されていないデバイスも含まれます。
- 修復された VI の割合と、優先パッチとしてパッチがある合計 VI を含む修復ステータス。
- クラスビューのレコードの関連リンクにある関連デバイス、脆弱性一致アイテム、パッチ展開、およびパッチ要求。このデータは、脆弱性対応 ワークスペースのレコードのタブに表示されます。
- 修復オーナーが承認のために送信したパッチ要求。

脆弱性一致アイテムレコードのステータスロールアップ

レコードへのステータスロールアップの詳細については、「脆弱性対応 のパッチオーケストレーションでのパッチデータとステータスのロールアップ」を参照してください。

アクティブな VI 数をロールアップするレコード

すべての脆弱性にすべてのパッチをロールアップすることを避けるために、スケジュール済みジョブはアクティブな VI 数の変更のみを取得します。これらのカウント変更と関連データは、脆弱性対応 内の次のレコードにロールアップされます。

- VIT
- RT
- 脆弱性ソリューション
- パッチ更新

ソリューションのないパッチのデータの表示

ソリューションのないパッチを表示する方法の詳細については、「脆弱性対応 でのソリューションのないパッチの表示」を参照してください。

脆弱性対応のパッチデータ

脆弱性管理 (PA) および CISO ダッシュボードは、脆弱性対応 アプリケーションの パフォーマンス アナリティクス のサブスクリプションに含まれています。パフォーマンスアナリティクス のサブスクリプションがあっても、パッチオーケストレーション統合がインストールされていない場合、 [修復] タブは CISO ダッシュボードに表示されますが、データは入力されません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性管理 (PA) ダッシュボードの場合は、次に移動します: **All** (すべて) > 脆弱性対応 > 概要.[修復] タブをクリックし、ページの下部までスクロールして、パッチ更新データ (スケジュールされているパッチとスケジュールされていないパッチ、ターゲットの日付がないパッチ、および週次の数) を表示します。

CISO ダッシュボードの場合は、次に移動します: **All** (すべて) > 脆弱性対応 > **CISO** ダッシュボード. [概要] タブを選択した状態で、ページの下部までスクロールして、パッチ範囲データ (重大度、スケジュールされているパッチとスケジュールされていないパッチ、およびターゲットの日付がないパッチ) を表示します。

脆弱性対応 ダッシュボードの詳細については、「デフォルトの 脆弱性対応 ダッシュボードを使用する」、「脆弱性対応 ワークスペースを使用したパッチオーケストレーション」、「脆弱性対応 ダッシュボードでのパッチオーケストレーションデータの表示」を参照してください。

Microsoft SCCM integration with 脆弱性対応 とのパッチスケージュール

Now Platform インスタンスの 脆弱性対応 アプリケーションのパッチ更新および修復タスクレコードからパッチをスケジュールします。

始める前に

バージョン 16.1 以降では、脆弱性対応 ワークスペースまたはクラシック環境からパッチをスケジュールできます。

必要なロール：

- パッチを設定およびスケジュールするための sn_vul_patch_orch.configure_patch ロール
- sn_vul_patch_orch.read_patch を使用して、レコードのパッチ情報を表示します (読み取り専用)。このロールは、IT 修復および脆弱性マネージャーのワークスペースに必要な sn_vul.remediation_owner および sn_vuln.vulnerability_analyst ロールに継承されます。

手順

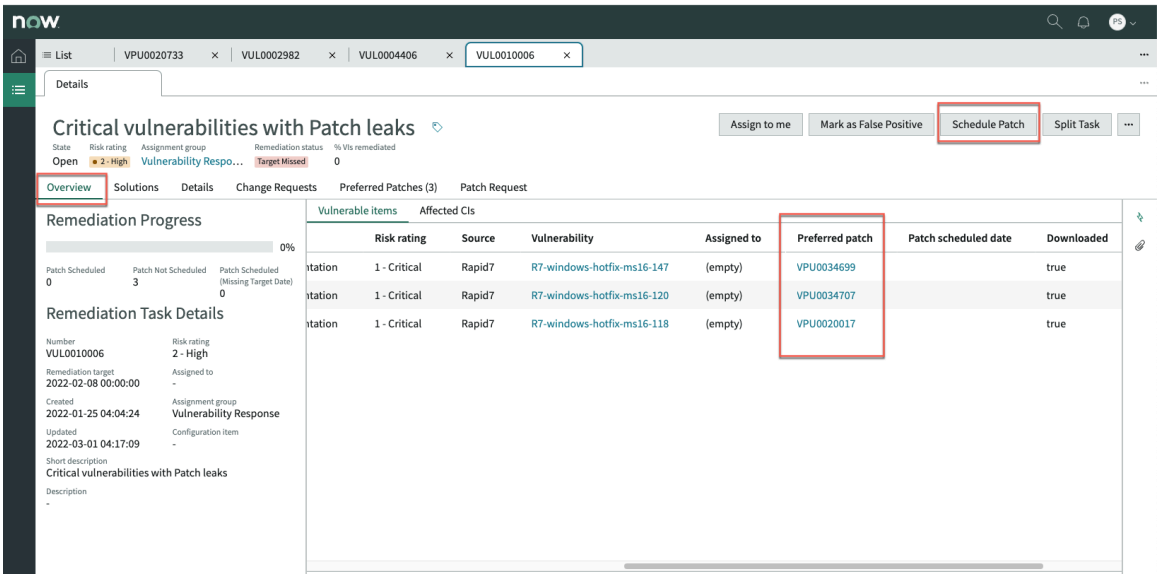
1. 脆弱性 脆弱性対応 ワークスペースで、sn_vul.remediation_owner ロールを持つユーザーとして、次の場所に移動します。 **All** (すべて) > 脆弱性対応 > **IT** 修復ワークスペース.
2. ホームページで、**[VI** の優先パッチ] をクリックします。
   割り当てられた優先パッチを含む VI のパッチ更新レコードのリストが表示されます。
3. 開くレコードを見つけてクリックします。
4. または、ワークスペースのリストビューから、 パッチ > **All** (すべて) [Patch Update] レコードを見つけます。
   [パッチ更新] レコードが表示されます。他のパッチが既にスケジュールされている可能性があるため、パッチをスケジュールする前にデータを確認することをお勧めします。
5. IT 修復ワークスペースに表示されるデータと実行できる操作については、次のテーブルを参照してください。
6. [パッチをスケジュール] をクリックします。
7. ダイアログボックスで、フィールドに入力します。
8. [展開] をクリックします。
   パッチ要求がレビューのために送信されます。送信されたすべての要求のステータスは、以下から表示できます 例外要求 > **My requests** (自分の要求) リストビューから。
9. または、自分または自分のグループにアサインされた修復タスク (RT) からパッチをスケジュールすることもできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:
修復タスクレコードからパッチをスケジュールするオプションは、パッチがタスク内の VI にマッピングされている (関連付けられている) 場合にのみ使用できます。これらのパッチは、[概要] タブを選択した状態で修復タスクレコードの右にスクロールすると、[優先パッチ] 列に表示されます。

優先パッチを使用した修復タスク



10. RT レコードから [パッチをスケジュール] をクリックし、上記の手順に従ってダイアログでスケジュールします。
11. オプション: クラシック環境では、前述のステップのパッチをスケジュールできます。これらのレコードを見つけるには、次の手順を実行します。

    a. クラシック環境で、次に移動します: **All** (すべて) > 脆弱性対応 > パッチ > **All** (すべて).

    b. 表示されるリストから、[パッチ更新] レコードを見つけます。

    c. 修復タスクの場合は、次に移動します: 脆弱性対応 > 修復タスク レコードを見つけます。[修復ステータス] タブで修復ステータスを追跡します。レコードの下部の [関連リンク] にパッチデータが表示されます。

    d. [パッチをスケジュール] をクリックして、フィールドに入力します。

フィールド	説明
展開名	このパッチ展開の名前を入力します。この名前は、更新を追跡するのに役立ちます。
説明	パッチに関するテキストを追加します。この情報は、[パッチ更新] レコードの [説明] フィールドに表示されます。
展開タイプ	リストからオプションを 1 つ選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	▪ 必須：このパッチは必須の更新です。 ▪ 利用可能：このパッチは必須ではありませんが、展開に利用可能です。
コレクション	続行するには、リストからコレクション (資産のグループ) を選択します。これらのグループは SCCM からインポートされた資産コレクションです。
展開時間の基準	展開期間の基準とするタイムゾーンをリストから選択します。
利用可能な時間	パッチが展開に最初に利用可能になる時間の値を設定します。
期限	期限を設定します。この値は、パッチをインストールできる最終日を示します。

e. [展開] をクリックします。

脆弱性対応 **Patch Orchestration with Microsoft SCCM** の **REST** メッセージ

Microsoft SCCM との脆弱性対応パッチオーケストレーションは、SCCM Windows Management Instrumentation (WMI) クラスを使用して SCCM サーバー API を呼び出します。

概要

SMS プロバイダー は、管理サービスと呼ばれる HTTPS を介した相互運用性アクセスを API に提供します。管理サービスは、Open Data (OData) v4 プロトコルに基づく REepresentational State Transfer (REST) API です。

この統合で使用する管理サービスの詳細については、「What is the administration service in Configuration Manager (Configuration Manager の管理サービスとは) 」を参照してください。

必要な認証は Windows New Technology LAN Manager NTLM プロトコルを使用するため、API の呼び出しは PowerShell スクリプトを使用して MID サーバーを介して行われます。

Microsoft SCCM 統合

Microsoft SCCM 統合の REST メッセージを使用して、Microsoft SCCM から情報を取得できます。REST メッセージのレコードメソッドを変更すると、 情報を取得するための Microsoft SCCM への要求が影響を受けます。REST メッセージには、次の REST メソッドが含まれています。

WMI クラス名：

- SMS_Collection
- SMS_DeploymentSummary

パラメーター名	値	説明
url	ユーザーに基づく動的な値	SCCM コンソールのエンドポイントを示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Microsoft SCCM 展開パッチ

Microsoft SCCM 統合の REST メッセージを使用して、Now Platform® から Microsoft SCCM へのパッチをスケジュールすることができます。REST メッセージのレコードメソッドを変更すると、 情報を取得するための SCCM への要求が影響を受けます。REST メッセージには、次の REST メソッドが含まれています。

REST メソッド	説明
POST 展開パッチ	単一または複数のコンピューター上の SCCM コンソールへのパッチをスケジュールします。

パラメーター名	値	説明
url	ユーザーに基づく動的な値	SCCM コンソールのエンドポイントを示します。
title	ユーザーに基づく動的な値	展開のタイトル。
settings_tag	値を含む XML タグ名付き設定	さまざまなパラメーターを含む、パッチのスケジュール中に SCCM に送信される設定を示します。
computer_tag	値を含む XML タグ名付きコンピューター	パッチがスケジュールされるコンピューターのリストを示します。
site_name	パッチ更新の値	パッチが存在するサイトの名前。
Patch_id	パッチ更新の値	パッチの ID。

Patch Orchestration with Microsoft SCCM Integration のデータ変換

データは Patch Orchestration with Microsoft SCCM Integration から取得され、一連のデータソースによって処理されて、Now Platform インスタンスで変換されます。

SCCM コレクションのインポート

インポートされたコレクションのデータは、SCCM コレクションインポート [sn_vul_sccm_collection_import] テーブルにロードされます。SCCM コレクション (変換マップ) は、インポートされた情報を変換するために使用されます。

注:
この変換マップを変更すると、SCCM コレクションのインポートからのデータの処理方法が変更されます。

この変換マップにアクセスするには、次に移動します: **All** (すべて) > システムインポートセット > 変換マップ をクリックし、[SCCM コレクション変換] を見つけます。次の表に、統合別の変換マップフィールドを示します。

ソースフィールド	ターゲットフィールド	説明
u_collectionid	source_id	コレクションの一意の ID。
u_name	name	コレクションの名前。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ソースフィールド	ターゲットフィールド	説明
u_membercount	device_count	このコレクション内のデバイスの数。
[script]	integration_instance	パッチのインポート元のインスタンスの名前。

SCCM コレクションのインポート変換マップスクリプトのタイミング

スクリプト	説明
OnStart (インポートセットが変換を作成したとき)。	統合プロセスのスコープ変数 [sn_vul_sccm] の値を初期化するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onBefore (インポートセットの変換が完了する前)。	スコープ変数 [sn_vul_sccm] の値を更新するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onComplete (インポートセットが変換を完了したとき)	作成、更新、および無視されるアイテムの数を設定するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

SCCM パッチ更新のインポート

インポートされたパッチのデータは、SCCM パッチ更新インポート [sn_vul_sccm_patch_update_import] テーブルにロードされます。

SCCM パッチ更新の変換は、インポートされた情報を変換するために使用されます。

注:
この変換マップを変更すると、SCCM パッチ更新のインポートからのデータの処理方法が変更されます。

この変換マップにアクセスするには、次に移動します: **All** (すべて) > システムインポートセット > 変換マップ をクリックし、SCCM パッチ更新変換を見つけます。

次の表に、統合別の変換マップフィールドを示します。

SCCM パッチ更新のインポート変換マップフィールド

ソースフィールド	ターゲットフィールド	説明
[Script]	URL	パッチの URL。
u_nummissing	num_missing	このパッチが適用されていないデバイスの数。
[Script]	date_release	パッチリリース日。
u_bulletinid	bulletin_id	パッチのセキュリティ情報 ID。
u_numtotal	num_total	デバイスの合計数。
u_localizeddescription	description	パッチの説明。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

SCCM パッチ更新のインポート変換マップフィールド (続く)

ソースフィールド	ターゲットフィールド	説明
[Script]	is_highest_supersedence	優先度が最も高いパッチです。
u_numnotapplicable	num_not_applicable	このパッチを適用できないデバイスの数。
u_iscontentprovisioned	is_downloaded	パッチが SCCM サーバーにダウンロードされているかどうか。
u_numunknown	num_unknown	不明なデバイスの合計数。
u_articleid	article_id	パッチの記事 ID。
u_localizeddisplayname	title	パッチのタイトル。
u_ci_id	source_id	SCCM のパッチの一意の ID。
u_numpresent	num_present	パッチがインストールされているデバイスの数。
[Script]	integration_instance	パッチのインポート元のインスタンスの名前。
[Script]	sn_vul_solution	ソース ID に基づくソリューション。
[Script]	last_modified	パッチの最終変更日。
u_severity	source_severity	パッチの重大度。

SCCM パッチ更新のインポート変換マップスクリプトのタイミング

スクリプト	説明
OnStart (インポートセットが変換を作成したとき)。	統合プロセスのスコープ変数 [sn_vul_sccm] の値を初期化するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onBefore (インポートセットの変換が完了する前)。	スコープ変数 [sn_vul_sccm] の値を更新するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onComplete (インポートセットが変換を完了したとき)	作成、更新、および無視されるアイテムの数を設定するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

SCCM デバイスパッチ更新のインポート

デバイスにあるインポートされた関連パッチのデータは、SCCM デバイスパッチ更新インポート [sn_vul_sccm_device_patch_import] テーブルにロードされます。

SCCM デバイスパッチ更新の変換は、インポートされた情報を変換するために使用されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:
この変換マップを変更すると、SCCM デバイスパッチ更新インポートからのデータの処理方法が変更されます。

この変換マップにアクセスするには、次に移動します: **All** (すべて) > システムインポートセット > 変換マップ をクリックし、[SCCM デバイスパッチ更新変換 (SCCM Device Patch Update Transform)] を見つけます。

次の表に、統合別の変換マップフィールドを示します。

SCCM デバイスパッチ更新の変換マップスクリプトのタイミング

スクリプト	説明
OnStart (インポートセットが変換を作成したとき)。	統合プロセスのスコープ変数 [sn_vul_sccm] の値を初期化するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onBefore (インポートセットの変換が完了する前)。	CI ルックアップルールとパッチ、およびそれらの関係に基づいて CI を作成および更新するために使用されるスクリプト。結果に基づいて、このスクリプトはスコープ変数 [sn_vul_sccm] の値を変更します。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onComplete (インポートセットが変換を完了したとき)	作成、更新、および無視されるアイテムの数を設定するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

SCCM デバイスコレクションのインポート

インポートされたデバイスコレクションのデータは、SCCM デバイスコレクションインポート [sn_vul_sccm_device_collection_import] テーブルにロードされます。

SCCM デバイスコレクションインポートの変換は、インポートされた情報を変換するために使用されます。

注:
この変換マップを変更すると、SCCM デバイスコレクションのインポートからのデータの処理方法が変更されます。

この変換マップにアクセスするには、次に移動します: **All** (すべて) > システムインポートセット > 変換マップ をクリックし、SCCM デバイスコレクション変換を見つけます。

次の表に、統合別の変換マップフィールドを示します。

デバイスコレクションインポートの変換マップスクリプトのタイミング

スクリプト	説明
OnStart (インポートセットが変換を作成したとき)。	統合プロセスのスコープ変数 [sn_vul_sccm] の値を初期化するために使用されるスクリプト。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

デバイスコレクションインポートの変換マップスクリプトのタイミング (続く)

スクリプト	説明
	このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onBefore (インポートセットの変換が完了する前)。	CI ルックアップルールとコレクション、およびそれらの関係に基づいて CI を作成および更新するために使用されるスクリプト。結果に基づいて、このスクリプトはスコープ変数 [sn_vul_sccm] の値を変更します。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onComplete (インポートセットが変換を完了したとき)	作成、更新、および無視されるアイテムの数を設定するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

SCCM デバイスコレクションインポートの変換マップフィールド

ソースフィールド	ターゲットフィールド	説明
u_id	source_id	アクションの一意の ID。
U_name	name	アクションの名前
[Script]	Sn_vul_sccm_discovered_item	パッチが展開されている検出されたアイテムの参照
U_status	status	アクションのステータス
[Script]	Sn_vul_patch_orch_update	パッチの参照
U_apply_count	Count_success	アクションの成功回数。
U_retry_count	retry	アクションの再試行回数。
[Script]	Deployment_time	アクションの開始時間。
[Script]	deadline	アクションの終了時間。
[Script]	Source_created	アクションの作成時間。
[Script]	Integration_instance	アクションのインポート元のインスタンスの名前。

SCCM 展開のインポート

インポートされた展開からのデータは、SCCM 展開インポート [sn_vul_sccm_deployment_import] テーブルにロードされます。

SCCM 展開インポートの変換は、インポートされた情報を変換するために使用されます。

注:
この変換マップを変更すると、SCCM 展開インポートからのデータの処理方法が変更されます。

この変換マップにアクセスするには、次に移動します: **All** (すべて) > システムインポートセット > 変換マップ をクリックし、SCCM 展開変換を見つけます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

SCCM 展開変換マップのフィールド

ソースフィールド	ターゲットフィールド	説明
u_id	source_id	展開の一意の ID。
u_name	name	展開の名前。
[Script]	deadline	展開の期限。
u_numberinprogress	count_progress	展開で進行中のデバイスの数。
[Script]	deployment_time	展開の開始時間。
[Script]	integration_instance	展開のインポート元のインスタンスの名前。
[Script]	source_created	展開の作成時間。
[Script]	sn_vul_patch_orch_update	パッチの参照
[Script]	sn_vul_patch_orch_collection	パッチが展開されている検出されたアイテムの参照。
u_softwarename	name	展開の名前。
u_numberother	count_other	展開のためのその他のデバイス数。
u_numberunknown	count_unknown	展開で不明ステータスのデバイスの数。
u_deploymentid	source_id	展開の一意の識別子。
u_numbersuccess	Count_success	展開で成功したデバイスの数。
u_numbererrors	count_error	展開でのデバイスのエラー数。
u_numbertargeted	count_total	展開でのデバイスの合計数。

自動翻訳

SCCM 展開インポートの変換マップスクリプトのタイミング

スクリプト	説明
OnStart (インポートセットが変換を作成したとき)。	統合プロセスのスコープ変数 [sn_vul_sccm] の値を初期化するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onBefore (インポートセットの変換が完了する前)。	スコープ変数 [sn_vul_sccm] の値を更新するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onComplete (インポートセットが変換を完了したとき)	作成、更新、および無視されるアイテムの数を設定するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

脆弱性対応 **Patch Orchestration integration with Microsoft SCCM** のワークフローの例

パッチオーケストレーションが Microsoft SCCM でどのように機能するかを示す例。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
たとえば、環境全体に 3 週間に 1 回パッチを適用するとします。最新のパッチ適用期間は 1 週間前に完了しましたが、最近判明した重大な脆弱性を修正するためのパッチを適用する必要があります。この脆弱性は重大であるため、次のスケジュールされたパッチにさらに 2 週間待つことはできません。

必要なロール：

- 脆弱性マネージャーワークスペース用の sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin。
- IT 修復オーナーワークスペースを表示するための sn_vul.remediation_owner。
- パッチを設定およびスケジュールするための sn_vul_patch_orch.configure_patch ロール。
- sn_vul_patch_orch.read_patch を使用して、レコードのパッチ情報を表示します (読み取り専用)。このロールは、IT 修復および脆弱性マネージャーのワークスペースに必要な sn_vul.remediation_owner および sn_vuln.vulnerability_analyst ロールに継承されます。

このタスクについて
脆弱性マネージャーワークスペースで作業する脆弱性マネージャーまたはアナリストは、重要な脆弱性を含むインポートされた VI をキャプチャするために、監視トピックを作成するか、既存の監視トピックを編集することを検討してください。パッチオーケストレーション統合では、これらの脆弱性の修正と追跡に使用するパッチを確認することもできます。次の表は、パッチオーケストレーションの監視トピックに設定できるいくつかのサンプルを示しています。これらの例を参考にして、環境に最適な設定を判断してください。監視トピックの設定方法の詳細については、「で監視トピックを作成する Vulnerability Manager ワークスペース」を参照してください。

脆弱性マネージャーワークスペースでのパッチオーケストレーションのサンプル監視トピック

監視トピック名	説明
パッチ漏れのある重大な脆弱性	Risk rating is 1 - critical かつ Reason is Patch Not Scheduled
パッチ適用がスケジュールされた重大な脆弱性 (SLA 未適用)	Reason is Patch Scheduled (Missing Target Date)
パッチ適用がスケジュールされた重大な脆弱性	Risk rating is 1 - critical かつ Patch scheduled date is not empty かつ Reason is Patch Scheduled

- 脆弱性マネージャーまたはアナリストは、監視トピックと修復作業を作成した後、修復タスクを生成します。VI レコードと修復タスクから、[ディスカバリー] タブにドリルダウンし、SCCM 製品によってインポートされた資産とともに、追跡している脆弱性がある検出済みアイテムレコードを見つけることができます。
- 脆弱性アナリストまたはアドミニストレーターは、脆弱性に関連付けられたパッチデータを監視できます。検出されたアイテムレコードから特定の資産 (構成アイテム) にパッチを展開することもできます。

IT 修復スペシャリストには、パッチ展開を使用して脆弱性に対処するオプションがあります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- パッチ更新レコード (VPU 番号) からパッチをスケジュールできます。
- 脆弱性一致アイテム (VI) に優先ソリューションがマッピングされていて、それらが自分または自分のグループにアサインされている場合は、これらの脆弱性一致アイテムを含む修復タスクからパッチをスケジュールできます。

手順

1. IT 修復スペシャリストは、IT 修復ワークスペースで [ホーム] ビューをクリックします。
2. ホームビューから、[アサインされた修復タスク] スコアカードをクリックしてレコードを表示します。

   この例では、重大な脆弱性に関連するテキストがないか、修復タスクの [簡単な説明] フィールドを確認します。たとえば、脆弱性マネージャーが、この重大な脆弱性がある VI (VIT#) を検出するために、「 パッチ漏れのある重大な脆弱性」という監視トピックを作成したとします。

   レコードを開いた状態で、VI や優先パッチをレビューし、自分または自分のグループがすでに承認のためにパッチ要求を送信しているかどうかを確認することもできます。
3. 十分な情報がある場合は、この修復タスクからパッチの要求を送信することもできます。

   注:
   レコードに関連付けられた VI にマッピングされたパッチがない場合、そのレコードでは [パッチをスケジュール] ボタンは使用できません。
4. [パッチをスケジュール] をクリックして、ダイアログのフィールドに入力します。
   パッチのスケジュール方法の詳細については、「Microsoft SCCM integration with 脆弱性対応 とのパッチスケージュール」を参照してください。
5. または、IT 修復ワークスペースのリストビューから、修復タスク、脆弱性一致アイテム、ソリューション、およびパッチのリンクをクリックして、これらのレコードを表示することもできます。
   この例の場合、監視トピック名の代わりに、パッチの記事 ID またはセキュリティ情報 ID とタイトルがわかっている可能性があります。その場合、この脆弱性を持つ VI が自分または自分のグループに割り当てられているかどうかを確認します。パッチ更新レコードから、パッチ要求を送信できます。VI レコードから、潜在的なパッチを確認し、パッチ要求を送信する場合は関連する修復タスクを開くことができます。
6. ワークスペースにアクセスできない場合、またはクラシック環境からデータを表示してパッチをスケジュールする場合は、次の手順に従います。

   a. 次のように移動する。 脆弱性対応 > パッチ > **All** (すべて).

   b. 必要な [パッチ更新] レコードを見つけます。
      「Critical」リスクスコアのレコードをフィルタリングすることもできます。

   c. [修復ステータス] タブの関連する VI および修復済み VI の割合フィールドを確認します。
      VI で利用可能なパッチがある場合、[パッチをスケジュール] ボタンがレコードの右上に表示されます。

   d. 要求を送信する場合は、[パッチをスケジュール] をクリックします。
      パッチのスケジュール方法の詳細については、「Microsoft SCCM integration with 脆弱性対応 とのパッチスケージュール」を参照してください。

   e. または、パッチ ID 情報がなく、グループにアサインされた修復タスクの [簡単な説明] フィールドで、重大な脆弱性に関連するテキストを確認することもできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

f. 次のように移動する。 脆弱性対応 > 修復タスク > 所属グループにアサイン済み.

g. 必要なレコードを見つけてクリックして開きます。
開いているレコードの [修復ステータス] タブで、VI および 修復された VI の割合を確認します。VI レコード、優先ソリューション、優先パッチ、およびパッチ要求の [関連リンク] をクリックします。

> **注:**
> レコードに関連付けられた VI にマッピングされたパッチがない場合、そのレコードでは [パッチをスケジュール] ボタンは使用できません。

h. パッチ要求を送信する場合は、レコードから [パッチをスケジュール] をクリックします。

Qualys 脆弱性統合の概要

Qualys 製品センサーがデータを収集して Qualys アプリケーションに自動的に送信すると、情報が継続的に分析され、関連付けられます。Qualys 脆弱性統合として 脆弱性対応 と簡単に統合して、脆弱性を CI およびビジネスサービスにマッピングし、悪意がある可能性の脅威の影響度と優先度を判別します。

を使用した Qualys 脆弱性統合 の構成 脆弱性 > アドミニストレーション > セットアップアシスタント により、データ取得の柔軟性と拡張性が向上します。

Qualys クラウドプラットフォーム アプリケーションを複数展開している場合は、展開ごとに統合を追加できます。複数のサードパーティの展開と脆弱性によって識別される資産は、CMDB と統合され、調整されます。この統合は、複数の展開間でスキャンプロセスが重複している場合でも行われます。各展開から供給されたデータは、脆弱性対応 の単一インスタンスで識別されて利用可能です。Qualys 脆弱性統合ナレッジベースレコードは展開全体で正規化され、展開全体で同じ脆弱性のインスタンスが同じ脆弱性として確実に扱われます。

> **注:**
> 元の脆弱性統合は削除できませんが、無効にすることはできます。無効になったテンプレートから作成された統合は、デフォルトで無効になっています。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

> **注:**
> Qualys 脆弱性統合はアプライアンスリスト、資産グループ、動的検索リスト、および静的検索リストの統合を作成しますが、通常の運用には必要ありません。

利用可能バージョン

Yokohama のリリースバージョン	リリースノート
Qualys 脆弱性統合 v12.7、v12.8	互換性情報については、「KB0856498 脆弱性対応 互換性マトリクスおよびリリーススキーマの変更」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インストールされるコンポーネント

統合とともにインストールされているロール、統合ジョブ、テーブルの現在のリスト、およびインスタンスに現在インストールされている内容を表示する方法のリンクについては、「Qualys 脆弱性統合 とともにインストールされるコンポーネント」を参照してください。

プライマリ統合とサポート統合

Qualys のプライマリ統合とサポート統合は、Qualys Vulnerability Integration からデータを取得することで、インスタンスの脆弱性データを拡張します。一連のスケジュール済みジョブによって、統合が自動的に呼び出されます。手動で実行することもできます。スケジュール済みジョブでは、インスタンスを他の脆弱性管理システムと同期させることで、脆弱性修復ライフサイクルを簡素化します。プライマリ統合とサポート統合は変更可能です。

Qualys 統合はスケジュール済みジョブとして実行されます。統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

> **注:**
> 有効な run-as ユーザーを設定しないと、統合が実行されるたびに、データソースレコードにデータ検索添付ファイルが重複して作成される場合があります。データソースの添付ファイルが複数になると処理時間が増加し、変換結果に一貫性がなくなります。

インポート中、CVE レコードがまだ存在しない場合は NVD レコードとして作成され、デフォルトで Qualys のサードパーティエントリーで参照されます。

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

プライマリ統合

プライマリ統合は、スケジュールに基づいて呼び出される Qualys API とやり取りする Qualys クラウドプラットフォーム へのエントリーポイントです。

に移動してプライマリ統合を表示するには **Qualys Vulnerability Integration** > アドミニストレーション > プライマリ統合.

サポート統合

サポート統合は、スケジュールに従って、またはプライマリ統合による発動なしで実行されることを意図していないプロセスです。

に移動すると、サポート統合が表示されます。 **Qualys Vulnerability Integration** > アドミニストレーション > サポート統合.

Qualys のサービスグラフコネクタ

バージョン 2.2 以降、Qualys 用のサービスグラフコネクタは ServiceNow® Store から入手できます。詳細については、「Service Graph Connector for Qualys」を参照してください。

Qualys データソースのフィールドからのデータは、グローバル資産 API と資産管理およびタグ付け API を使用してインポートされます。

グローバル資産 API：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- CSAM ライセンスが必要です。
- 資産情報には、ハードウェアカテゴリや OS カテゴリなどの詳細が含まれます。

資産管理とタグ付け API：

- CSAM ライセンスは不要です。
- 資産情報には、ハードウェアカテゴリや OS カテゴリについての詳細は含まれません。

詳細については、「Service Graph Connector for Qualys APIs」を参照してください。

。

識別および調整エンジン (IRE) を使用した CI の作成

既存の CI がサードパーティのスキャナーからインポートされたホストと一致しない場合、識別および調整エンジン (IRE) を使用して新しい CI を作成できます。新しいクラスを使用して CI を作成するには、CMDB CI クラスモデルプラグインを有効にします。これを行わない場合は、一致しない CI が [不一致] CI クラスに作成されます。詳細については、「識別および調整エンジンを使用して 脆弱性対応 の CI を作成する」を参照してください。一致しないクラウドリソースの分類を優先 CI クラスに構成する方法の詳細については、「一致しないクラウド資産の CI クラスの更新」を参照してください。

検索リスト

検索リストは、脆弱性のカスタムグループを作成するために Qualys で使用されます。それらを保存して、チケットの作成や、脆弱性スキャンとレポートのカスタマイズに使用できます。検索リストモジュールを使用すると、スケジュールに基づいて Qualys からインスタンスに検索リストデータをダウンロードできます。

検索リストは、動的検索リストインポートまたは静的検索リストインポートデータ変換マップを使用して Qualys からプルされます。これらの各変換では、インポートを実行するスケジュールを定義できます。

オプションプロファイル

オプションプロファイルは Qualys スキャン設定で使用できます。Now Platform からスキャンを開始する場合は、オプションプロファイルが必要です。

オプションプロファイルは、オプションプロファイルリスト統合によって Qualys 製品からインポートされます。検索リスト統合、Qualys 動的検索リスト、および Qualys 静的検索リスト統合からインポートした後にオプションプロファイルリスト統合を実行すると、オプションプロファイルに関連付けられている検索リストを確認できます。

資産グループ

資産グループは Qualys プラットフォームで設定されます。資産グループは、Now Platform からスキャンが開始されたときに、一致する IP アドレスのスキャンに使用されるスキャナーアプライアンスを識別します。

アプライアンスが関連付けられている資産グループは、資産グループリスト統合によって Qualys からプルされます。

資産グループをインポートした後、アプライアンスリスト統合を開始して、Now Platform の Qualys デフォルトアプリケーションレコードの [アプライアンス名] フィールドと [アプライアンスステータス] フィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ホストタグ

すべてのホストタグは Qualys ホストリスト統合の一部としてインポートされます。ホストタグは、主に 脆弱性対応 アサインおよび修復タスクルールでのフィルタリングに使用されます。これらは [検出されたアイテム] フォームに表示されます。

> **注:**
> Qualys ホストリスト統合は、脆弱性一致アイテムがインポートされてグループ化される前にすべてのタグがルール内に存在できるように、脆弱性対応 でのアサインルールまたは修復タスクルールを作成する前に実行する必要があります。

- タグストレージでは大文字と小文字は区別されません。**[San Diego]** タグが作成されると、**[SAN DIEGO]** タグを [ホストタグ] テーブルに格納できなくなります。「San Diego」と「SAN DIEGO」は同じホストタグと見なされます。最初にインポートされたタグが優先されます。
- 修復タスクルールのグループキーとしてホストタグを使用すると、予期しない結果になることがあります。ホストタグは、条件ビルダー専用です。
- ホストタグは、グローバルシステムプロパティ **sn_vul.import_host_tags** で制御されます。このプロパティはデフォルトで [true] に設定されています。タグをオフにすると、すべてのインスタンスでオフになります。

ホストタグ (資産タグとも呼ばれます) は、組織の資産の整理と追跡に使用されます。ホスト資産にはタグを割り当てることができます。これにより、スキャンを開始するときに、スキャンするホストに関連付けられたタグを選択できます。ホストタグモジュールを使用すると、スケジュールに基づいて Qualys からインスタンスにホストタグデータをダウンロードできます。

スキャンによってクローズされていない解決済みの脆弱性一致アイテムの再オープン

Now Platform インスタンスで [解決済み] に設定されていてもサードパーティの統合実行によって [クローズ済み]/[修正済み] に移行されていない脆弱性一致アイテムは、再スキャン中に検出された場合に再オープンされます。

Qualys 検出で、[解決済み] に設定された VI が後続のスキャンで [クローズ済み]/[修正済み] に移行されていない場合、最終検出日が解決日より後であると、これらの VI が [オープン] に戻ります。

データ検索の制限

デフォルトでは、Qualys からのデータの取得方法に制限はありません。多くのレコードは、顧客が脆弱性対応プロセスを使用して修正しようとしない、重大度の低い脆弱性に関連している可能性があります。対応する REST メッセージ/メソッドのパラメーターを更新すると、この動作が変更される場合があります。

この更新を処理する REST メッセージ/メソッドは、**[Qualys** ホスト検出 **-** 標準/投稿 **(Qualys Host Detection – Standard/post)]** です。値を更新するには、次の値を使用して新しい HTTP クエリパラメーターを post メソッドに追加します。

- 名前：重大度
- 値：3 ～ 5 (または必要な適切な重大度)

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

関連情報

Qualys REST メッセージ

Qualys 脆弱性統合 の準備

統合を成功させるには、統合前のタスクを計画して慎重に実行する必要があります。これらの手順を実行して、統合を準備することが重要です。Qualys 脆弱性統合は、ユーザーが Qualys Cloud Platform スキャンに精通しており、環境で実行していることを前提としています。

注:
統合を実行する前に、要件に基づいて必要な構成変更を行います。

重要な前提条件

インポートする予定の脆弱性一致アイテムの数に基づいて、インスタンスのサイジングを検証します。インスタンスが小さすぎると、ロードに時間がかかることがあります。インスタンスのサイズがわからない場合は、カスタマーサービス & サポート にお問い合わせください。

フィルタリングを使用して初期インポートのアイテム数を制限し、後続のインポートでフィルターを調整して展開を段階的に行います。

Qualys スキャナーは、脆弱性対応 アプリケーションではデフォルトで無効になっています。これらのアプリケーションをソースとする脆弱性一致アイテムまたは修復タスクから再スキャンを実行しようとすると、[再スキャン] ボタンは使用できません。

実行するアクション

- [ホスト検出リストインポート] 統合の最初の開始日を決定します。

  [開始時間] フィールドを過去数時間または数日に設定することを検討してください。理想的には、前回の Qualys スキャンの日付を選択します。開始日には、脆弱性管理ソリューションを使用する前に検出された脆弱性を含めることができます。スキャンサイクルの開始に使用する最も早い開始時間を設定します。このため、すべてのホストがスキャンされるまでに 1 週間かかる場合は、その時間の 1 週間前にこの値を設定します。

- admin、sn_vuln.admin、および sn_vul_qualys.admin のロールにユーザーを追加します。詳細については、「ユーザーへのロールのアサイン」を参照してください。

- 統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

- 脆弱性算出を使用しない場合は、定義した他の脆弱性算出に加えて、次の操作を実行します - 使用しないデフォルトの脆弱性算出の無効化。脆弱性算出は、脆弱性一致アイテムレコードが作成または更新されるたびに実行され、初期インポートのパフォーマンスに影響を与える可能性があります。
- レコードの最初のインポート中に、特定の通知関連のビジネスルールによって大量の通知が生成され、パフォーマンスが影響を受ける可能性があることを確認します。最初のインポートの前に、ビジネスルールを無効にします。
- Qualys のデフォルトとは異なるスキャナーを使用する場合は、「Set up scanner appliances (スキャナーアプライアンスの設定)」を参照してください。
- Qualys サーバーの URL と認証情報を準備します。認証情報には、Qualys サブスクリプションのナレッジ、スキャン、および検出情報を取得するための適切な権限が付与されている必要があります。
- 脆弱性対応アサインルールまたは修復タスクルールでホストタグを使用する場合は、ルールを作成する前に Qualys ホストリスト統合が実行されていることを確認してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Qualys 脆弱性統合 をインストールする

インスタンスで Qualys 脆弱性統合を実行する前に、Qualys 脆弱性統合 アプリケーションをインストールして構成する必要があります。このアプリケーションは別のサブスクリプションとして利用できます。

始める前に

インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

> **注:**
> このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

必要なロール：アプリケーションをダウンロードしてインストールするアドミン

セットアップタスク	説明
脆弱性対応 アプリケーションがインストールされ、アクティブ化されていることを確認します。	アクティブ化されていることを確認するには、サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応 のインストール」を参照してください。
Qualys 脆弱性統合 アプリケーションのエンタイトルメントを取得して、Now Platform インスタンスにダウンロードします。	アプリケーションがまだインスタンスにダウンロードされていない場合は、「」を参照してください。
統合を準備します。	「Qualys 脆弱性統合 の準備」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント.

   しばらくすると、インスタンスにインストールできるアプリケーションが表示されます。

2. Qualys 脆弱性統合タイルを見つけて、[インストール] をクリックします。
3. セットアップアシスタントのプロンプトに従います。
   セットアップアシスタントを使用したアプリケーションのインストールの詳細については、「セットアップアシスタントを使用した 脆弱性対応 サードパーティアプリケーションのインストール」を参照してください。
4. セットアップアシスタントで [統合設定] > [スキャナー統合] に移動して、構成を続行します。
   セットアップアシスタントで提供されているプロンプトを補足するための詳細情報については、「セットアップアシスタントを使用した Qualys 脆弱性統合の構成」を参照してください。

次のタスク

スキャナーは脆弱性対応アプリケーションでデフォルトで非アクティブ化されているため、スキャナーをアクティブ化します。Qualys スキャナーをアクティブ化する方法の詳細については、「Qualys スキャナーのアクティブ化」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Qualys スキャナーのアクティブ化

スキャナーは脆弱性対応アプリケーションのデフォルトで非アクティブ化されているため、Qualys 脆弱性統合 のインストール後にスキャナーをアクティブ化する必要があります。

始める前に
必要なロール：sn_vul.vulnerability_admin

このタスクについて
これらのアプリケーションをソースとする脆弱性一致アイテムまたは修復タスクから再スキャンを実行しようとすると、[再スキャン] ボタンは使用できません。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性スキャン > スキャナー.
2. アクティブ化するスキャナー製品を見つけ、レコードを選択して開きます。
3. [有効] チェックボックスをオンにします。
4. [更新] を選択します。
5. アクティブ化した製品は、次のインポート後に脆弱性一致アイテムおよび修復タスクレコードの [ソース] フィールドに表示され、[再スキャン] は UI アクションとして使用できます。

Qualys 脆弱性統合 とともにインストールされるコンポーネント

次のロール、統合ジョブ、テーブルが Qualys 脆弱性統合とともにインストールされます。

> **注:**
> アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「アプリケーションとともにインストールされているコンポーネントの検索」を参照してください。

アプリケーションとともにインストールされるコンポーネントのフィルター済みリストの表示

アプリケーションファイルテーブルをフィルタリングして、アプリケーションとともにインストールされたロール、スケジュール済みジョブ、およびテーブルのみを表示します。これらのコンポーネントを表示するアプリケーションは、そのファイルがインスタンスとメタデータテーブルにロードされるようにインストールする必要があります。アプリケーションファイルテーブルからフィルター済みリストを表示するには、次の手順に従います。

1. フィルターナビゲーターで、「**sys_metadata.list**」と入力してメタデータテーブルに移動します。
2. 条件ビルダー (フィルターアイコン) を選択し、次を選択します。 アプリケーション > 次の値に等しい その後にアプリケーションの名前が続きます。たとえば アプリケーション > 次の値に等しい > 脆弱性対応.
3. 条件ビルダーで 2 番目のフィルターを追加するには、[**AND**] を選択してから次を選択します。 クラス > は をクリックし、リストから [ロール]、[スケジュール済みジョブ]、または [テーブル] のいずれかのクラスを選択します。
4. **[Run** (実行)] を選択します。

選択したクラスの結果がフィルター済みリストに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インストールされるロール

ロール タイトル [名前]	説明	含んでいるロール
sn_vul_qualys.read	Qualys 脆弱性統合レコードの読み取りアクセス権があります。	
sn_vul_qualys.user	Qualys 脆弱性統合のユーザー。レコードの読み取りと書き込みが可能です。	sn_vul_qualys.read
sn_vul_qualys.admin	Qualys 脆弱性統合のアドミン。たとえば、統合の開始日を変更し、いくつかの詳細構成を設定できます。	• sn_vul_qualys.user • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	Qualys 脆弱性統合を構成できます。	sn_vul_qualys.admin

インストール済み統合ジョブ

統合ジョブ	説明
Qualys 静的検索リスト統合	脆弱性エントリーを見つけるために Qualys 検索リストを同期します。静的リストタイプのレコードのみを取得します。
Qualys 包括的ホスト検出統合	Qualys からホストと脆弱性データを取得し、インスタンスで処理します。 ホスト検出 API への REST メッセージ呼び出しを調整します。 この統合の出力は脆弱性一致アイテムです。この統合により、脆弱性のすべての状況 ([新規]、[修正済み]、[アクティブ]、および [再オープン]) がインポートされます。デフォルトでは、この統合は非アクティブで毎週実行されます。 **注:** この統合がアクティブになると、日次の包括的なジョブは、[新規]、[修正済み]、および [再オープン] の状況のみをインポートします。
Qualys ホストリスト統合	認証済みおよび未認証のホストスキャンデータとホストタグを Qualys から週に 1 回取得し、インスタンスの [検出されたアイテム] モジュールに保存します。最近スキャンされていない資産を特定するのに役立ちます。
Qualys ホスト検出統合	Qualys からホストと脆弱性データを取得し、インスタンスで処理します。ホストリスト検出 API への REST メッセージ呼び出しを調整します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統合ジョブ	説明
	この統合の出力は脆弱性一致アイテムです。 Qualys ホストタグはこの統合でインポートされます。
Qualys チケット統合	Qualys チケットを取得してインスタンスに追加します。チケットリスト API への REST メッセージ呼び出しを調整します。 Qualys の設定はチケットになる検出を成約する可能性があるため、多くの場合、ホスト検出よりもチケットの数が少なくなります。
Qualys オプションプロファイルリスト統合	Qualys 製品からオプションプロファイルを取得します。オプションプロファイルには、Now Platform インスタンスからスキャンを開始するときに必要なスキャン設定が含まれています。
Qualys アプライアンスリスト統合	Qualys からスキャナーアプライアンス情報を取得します。
Qualys 資産グループ統合	Qualys から資産グループ情報を取得します。資産グループは、一致する構成アイテムをスキャンするために使用するスキャナーアプライアンスを識別するために使用されます。
Qualys ナレッジベース (バックフィル)	Qualys ナレッジベースエントリーを取得します。 Qualys ホスト検出統合の後に実行するようにスケジュールされています。ホスト検出統合で参照されたもののシステムに存在しなかった QID でインスタンスを更新します。
Qualys ナレッジベース	Qualys ナレッジベースエントリーを取得します。取得されるデータは、統合が最後に実行されてから Qualys によって脆弱性が更新された日付に基づいています。 このデータは、Qualys 識別子 (QID) が最新であることを確認するだけでなく、履歴データをインスタンスに入力するのにも役立ちます。
Qualys 動的検索リスト統合	脆弱性エントリーを見つけるために Qualys 検索リストを同期し、動的リストタイプレコードを取得します。
Qualys の更新されたキーの検出の修正	検出を識別して Qualys 脆弱性一致アイテムに関連付ける方法を提供する、フィールドのハッシュ化された組み合わせ
ネットワークパーティション識別子を使用して検出された既存のアイテムの Qualys 更新	検出された既存のアイテムを更新します。既存の Qualys Vulnerability Integration データの CI は、ネットワークパーティション識別子の粒度を含むように作成または更新されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インストールされるテーブル

テーブル	説明
検索リスト脆弱性 sn_vul_qualys_m2m_search_list_vul	Qualys 検索リストと脆弱性の間のマッピングを保存します。
Qualys 脆弱性スキャナー sn_vul_qualys_scanner	Qualys 再スキャン機能のスキャナー情報を保存するために脆弱性スキャナーを拡張するテーブル
Qualys 検索リスト sn_vul_qualys_search_list	Qualys 検索リスト統合によって取得される検索リストを格納します。
Qualys アプライアンスインポート sn_vul_qualys_appliance_imp	インポートセット行を拡張するテーブル。フィールドマップ変換はスキップされ、応答添付ファイルは onComplete スクリプトで直接処理されます。
Qualys CI sn_vul_qualys_ci	テーブルは使用されなくなりました。
ホスト検出ページネーション sn_vul_qualys_host_detection_pagination	テーブルは使用されなくなりました。
Qualys 統合実行 sn_vul_qualys_integration_run	テーブルは使用されなくなりました。
Qualys の統合 sn_vul_qualys_integration	脆弱性統合を拡張し、Qualys に対応するすべての統合を格納するテーブル。
Qualys 静的検索リストインポート sn_vul_qualys_static_search_list_imp	インポートセット行を拡張するテーブル。フィールドマップは、データをターゲットテーブル、Qualys 検索リストに変換するために使用されます。
Qualys ナレッジベース sn_vul_qualys_knowledge_base	インポートセット行を拡張するテーブル。フィールドマップ変換はスキップされ、応答添付ファイルは onComplete スクリプトで直接処理されます。
Qualys チケットリスト sn_vul_qualys_ticket_list_imp	インポートセット行を拡張するテーブル。フィールドマップ変換はスキップされ、応答添付ファイルは onComplete スクリプトで直接処理されます。
Qualys オプションプロファイル sn_vul_qualys_option_profile	Qualys から取得されたオプションプロファイルを格納するテーブル。このテーブルは再スキャンで使用されます。
Qualys 動的検索リストインポート sn_vul_qualys_dynamic_search_list_imp	インポートセット行を拡張するテーブル。フィールドマップは、データをターゲットテー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
	ブル、Qualys 検索リストに変換するために使用されます。
Qualys インポートセット再実行 sn_vul_qualys_import_rerun	テーブルは使用されなくなりました。
Qualys オプションプロファイルインポート sn_vul_qualys_option_profile_import	インポートセット行を拡張するテーブル。フィールドマップ変換はスキップされ、応答添付ファイルは onComplete スクリプトで直接処理されます。

Qualys 脆弱性統合 のネットワークパーティション識別子で構成アイテムを更新する

IP アドレスを共有する環境内の資産に対して、一意の構成アイテム (CI) を作成します。環境全体で個別の資産を特定し、検出された既存のアイテム、脆弱性一致アイテム、および検出レコードで CI を自動的に更新して、脆弱性に関する詳細を提供します。

始める前に
必要なロール：admin

このタスクについて
デフォルトでは、脆弱性対応 アプリケーションで資産を識別する方法の 1 つは IP アドレスです。場合によっては、資産は IP アドレスを共有できますが、それらは 1 つの CI として CMDB に保存されます。

たとえば、次の表に示すように、環境内の複数の資産 (CI) が IP アドレスを共有できますが、ネットワークとリポジトリの ID は一意です。ただし、デフォルトでは、これらの資産は通常、IP アドレスのルックアップ中に単一の CI（CI 1）として識別され、保存されます。

デフォルトの **IP** ルックアップと **CI** の作成

ソース	**IP** アドレス	**NETWORK_ID**	構成アイテム
Qualys 脆弱性統合：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

ソース	**IP** アドレス	**REPOSITORY_ID**	構成アイテム
Qualys 脆弱性統合：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

同じ IP アドレスを持つ資産に対して個別の CI を作成して、それらを個別の資産として識別できるようにすることができます。新規のデータのインポートから開始し、スケジュール済みジョブ *`Update existing discovered items with network partition identifier`* を実行することで、ネットワークパーティション識別子 [network_partition_identifier] を含む既存の CI をより細かく更新できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このスケジュール済みジョブは、デフォルトでは非アクティブです。セットアップアシスタントで Qualys 脆弱性統合 の資産と修正済みおよびオープンな脆弱性の統合に対してこの機能をアクティブ化して、この識別子をレコードに表示します。

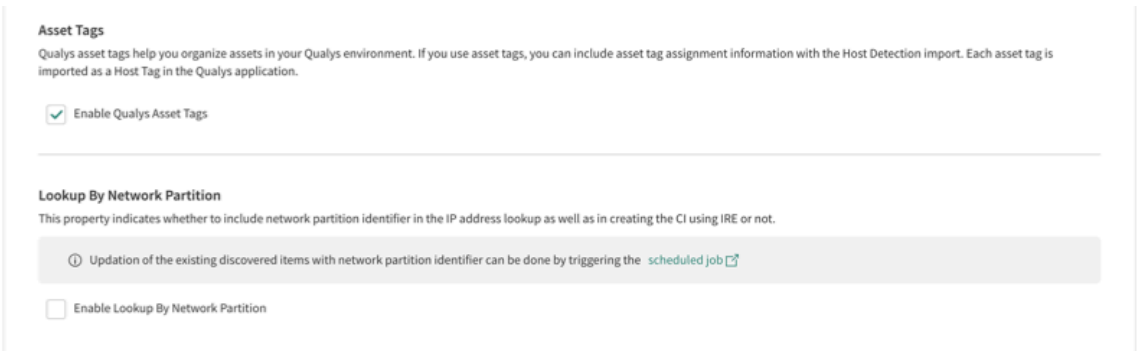
このスケジュール済みジョブを有効にすると、インポートされたデータから既存の CI レコードにネットワークパーティション識別子 [network_partition_identifier] が追加されます。IRE によって作成された既存の CI も更新されます。スケジュール済みジョブは、次のインポートから始まるネットワークパーティション識別子を含む CI も作成します。または、オンデマンドでジョブを開始して既存のデータを更新することもできます。

脆弱性対応 の v14.0 および Qualys 脆弱性統合 脆弱性統合の v12.1 以降、CMDB CI クラスモデル (1.0.21.) がサポートされています。クラスモデルでは、識別および調整 (IRE) 識別ルールにネットワークパーティション識別子 [network_partition_identifier] があります。

オプション	説明
スケジュール済みジョブをオンデマンドで実行します。	検出された既存のアイテムを更新します。既存の Qualys 脆弱性統合データの CI は、ネットワークパーティション識別子の粒度を含むように作成または更新されます。検出されたアイテム、脆弱性一致アイテム、および検出レコードはすべて新しい CI で更新されます。
次のスケジュール済みジョブとの統合からの新しいデータのインポートを待機します。	次のスケジュール済みジョブから始まるネットワークパーティション識別子を使用して、新しい資産ごとに CI を作成します。CI、脆弱性一致アイテム、および検出レコードはすべて、新しい粒度を含むように更新されます。完全一致が見つからない場合は、新しい CI が作成されます。

手順

1. 次のように移動する。 脆弱性対応 > セットアップアシスタント > 統合設定 > スキャナー統合.
2. Qualys 脆弱性統合 を選択します。
3. 必要な統合を編集します。
4. 選択 ホスト検出設定.
5. 選択 ネットワークパーティションによるルックアップを有効化 の チェックボックス ネットワークパーティションによるルックアップ



節。

6. [完了] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

IP ルックアップと **CI** の作成に含まれるネットワークパーティション識別子 **NETWORK_ID** と **REPOSITORY _ID**

ソース	**IP** アドレス	**NETWORK_ID**	ネットワークパーティション識別子のない資産の **CI**	ネットワークパーティション識別子のある **CI** 資産
Qualys 脆弱性統合：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

ソース	**IP** アドレス	**REPOSITORY_ID**	ネットワークパーティション識別子のない資産の **CI**	ネットワークパーティション識別子のある **CI** 資産
Qualys：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

Qualys 脆弱性統合 の資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合からデータをインポートできるように、IP アドレスおよび不完全な IP アドレス CI の識別ルックアップルールにネットワークパーティション識別子属性が自動的に含まれます。

スケジュール済みジョブをアクティブ化してレコードを保存した後、スケジュール済みジョブをオンデマンドで起動して、ネットワークパーティション識別子を含む CI で検出された既存のアイテムを更新することもできます。既存の検出されたアイテム、脆弱性一致アイテム、および検出レコードの CI は自動的に更新されます。

オプションの **Qualys** の変更

Qualys 統合に特化したオプションの変更を構成し、一部のデータを簡素化します。

セットアップアシスタントまたはプライマリ統合からその開始日をリセットするか、最初のインポート時にビジネスルールを変更して無効にすることができます。

最初のレコードインポートの前に通知関連のビジネスルールを無効にする

レコードの最初のインポート中に、特定の通知関連のビジネスルールによって大量の通知が生成され、パフォーマンスが影響を受ける可能性があることを確認します。これらのビジネスルールは、インポート中に無効になるように変更する必要があります。

始める前に
必要なロール：admin

手順

1. 次のように移動する。**All** (すべて) > システム定義 > ビジネスルール.
2. [影響を受ける **CI** 通知 **(Affected ci notifications)]** を検索します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. ビジネスルールを開き、条件 current.sys_class_name != "sn_vul_vulnerable_item" を挿入します。
4. [更新] をクリックします。
5. 次のビジネスルールについてこの手順を繰り返します。
   - 影響を受けるコストセンター通知
   - 影響を受けるグループ通知
   - 影響を受ける場所の通知

> **注:**
> 最初のレコードのインポートが完了した後、これらのビジネスルールを再度有効にすることができます。ただし、無効にしておくことを検討してください。大量の通知が生成され、インスタンスのパフォーマンスに影響を与える可能性があります。

最初の開始日の変更

セットアップアシスタントを使用してインストール中に、Qualys 統合の最初の開始日を設定します。その開始日は、次に示すように、セットアップアシスタントまたはプライマリ統合からリセットできます。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

このタスクについて
統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、 脆弱性対応のバージョン 18.2.4 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

> **注:**
> [最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。
>
> - *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
> - *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > アドミニストレーション > プライマリ統合.
2. **[Qualys** ホスト検出統合] をクリックします。
3. [統合の詳細] をクリックします。
4. [開始時間] フィールドを過去の値に設定すると、その時間以降にスキャンおよび検出されたすべての脆弱性が検出されます。

   セットアップアシスタントを使用して Qualys を構成した場合、[開始時間] フィールドには、最初に今日の日付の 3 か月前、その後は今日の日付が事前に入力されます。

   注:
   過去最大 1 か月前の値を設定することを検討してください。これにより、大量のデータで Qualys API レート制限を超えることがなくなり、実行タイムアウトがトリガーされなくなります。

5. [送信] または [更新] をクリックします。
6. オプション: [今すぐ実行] をクリックして、今すぐ実行します。

詳細な **Qualys** 構成と変更

Qualys統合に特化した詳細なオプションの変更を構成し、一部のデータを簡素化します。これらの変更のほとんどには、コーディングや高度な ServiceNow または Qualys クラウドプラットフォーム の専門知識が必要です。

Qualysインポートに関するその他のヒントについては、HI ナレッジベースのナレッジ記事「Qualys インポートジョブのパフォーマンスチューニングのヒント」を参照してください。

Qualys から **ServiceNow** への優先度およびステータスマッピング値の変更

要件の優先度とステータスのマッピング値を変更します。

始める前に
必要なロール：admin

このタスクについて
これは高度なカスタマイズオプションです。

手順

1. 次のように移動する。 **All** (すべて) > システム定義 > ビジネスルール.
2. **[Qualys** 値のマッピング **(Map Qualys Values)]** を検索して開きます。
3. [詳細] タブをクリックします。
4. 要件に従って変更します。
   最も一般的な変更には、新しい状況値の追加や、重要度や優先度の変更が含まれます。
5. [更新] をクリックします。

アサイン先グループに基づいてレコードへの書き込み機能を制限する

アサイン先グループのメンバーシップに基づいて、レコードの書き込み/読み取り権限を制限できます。特定の要件に基づいて条件とスクリプトを変更します。

始める前に
必要なロール：security_admin (admin から昇格したロール)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:
このアクションは脆弱性スコープで実行されます。

手順

1. 次のように移動する。 **All** (すべて) > システムセキュリティ > アクセス制御 **(ACL)**.
2. sn_vul で始まる ACL を検索します。
3. アクセス制御レコード (例：sn_vul_vulnerable_item、操作：書き込み) を選択します。
4. 必要に応じて、レコードの [詳細] ボックスをオンにして [ロール] エントリーを表示します。
5. 要件に合わせて [ロール] スクリプトを変更します。
   グループ別のアクセス権を変更するスクリプトの例

```
answer = (current.assigned_to == gs.getUserID() ||
 isMemberOfForScopedApp(current.assignment_group));
// Note: standard 'isMemberOf' does not work within Scoped App
// gs.getUser().isMemberOf(current.assignment_group);
function isMemberOfForScopedApp(groupID){
var result = false;
if (groupID != ''){
var userID = gs.getUserID();
var now_GR = new GlideRecord("sys_user_grmember");
gr.addQuery("group", groupID);
gr.addQuery("user", userID);
gr.query();
if (gr.next()){
result = true;
}
}
return result;
}
```

6. [更新] をクリックします。

スキャナーアプライアンスのセットアップ

Qualys から直接ではなく Now Platform® からスキャンを開始する場合は、IP アドレス範囲のスキャンを設定できます。

始める前に

データは、Qualys 資産グループとそれに関連するデフォルトアプライアンス (スキャナー) に基づいて Qualys 統合から取得されます。

ターゲットの IP アドレス範囲にアプライアンスが構成されていない場合は、統合インスタンスのデフォルトとして設定されているアプライアンスがスキャンに使用されます。

必要なロール：sn_vul_qualys.admin

手順

1. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > スキャナーアプライアンス.
2. 必要に応じて、フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
アプライアンス名	レコードを手動で作成すると、このフィールドに入力するように求められます。 一致する構成アイテムのスキャンの呼び出しに使用する Qualys スキャナーアプライアンスの名前を入力します。 スキャンを外部スキャナーで開始する場合は、External 値を使用します。
アプライアンス ID	一致する構成アイテムのスキャンの呼び出しに使用する Qualys スキャナーアプライアンスのアプライアンス識別子を入力します。 レコードを手動で作成すると、このフィールドに入力するように求められます。 スキャンを外部スキャナーで開始する場合は、0 値を使用します。
アプライアンスステータス	Qualys 統合によって返されたデータについて、スキャナーアプライアンスの前回のステータスを表示します。手動で作成されたレコードの場合、ステータスは有効な [アプライアンス **ID]** が指定されている場合にのみ更新されます。
資産グループ ID	このレコードを作成した Qualys 資産グループ識別子を表示します。このフィールドには、Qualys 統合によって作成されたレコードの値のみが表示されます。
資産グループ名	このレコードを作成した Qualys 資産グループ名を表示します。このフィールドには、Qualys 統合によって作成されたレコードの値のみが表示されます。
順序	スキャンの優先度を決定するために使用する値を入力します。基準が競合するアプライアンスの場合、順序値が小さいアプライアンスの優先度が高くなります。
手動作成	このレコードがユーザーによって手動で作成されたかどうかを示します。
フィルタグループを使用	一致する構成アイテムをスキャンで検索するためのフィルターグループを指定するには、このチェックボックスをオンにします。
フィルターグループ	一致する構成アイテムをスキャンで検索するために使用するフィルターグループを選択します。このフィールドは、[フィルターグループを使用] を選択した場合にのみ表示されます。
IP	スキャンを呼び出すときにこのアプライアンスで使用する IP アドレスまたは IP アドレス範囲のカンマ区切りリスト
統合インスタンス	このアプライアンスに関連付けられた Qualys 統合インスタンス
オプションプロファイル	一致する構成アイテムのスキャンに使用するオプションプロファイルを選択します。

3. [更新] をクリックします。

Qualys 脆弱性スキャナーとスキャンの設定および管理

Qualys 脆弱性スキャンを実行して、CI に影響するソフトウェアの脆弱性を見つけることができます。脆弱性一致アイテムレコードから、または構成アイテム (CI) と IP アドレスのスキャンレコードを直接作成することによって、スキャンを開始できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Qualys の脆弱性一致アイテムを [脆弱性一致アイテム] 画面から直接スキャンする場合は、複数の脆弱性一致アイテムを同時にスキャンすることもできます。

セキュリティインシデントレスポンス がアクティブ化されている場合、セキュリティインシデントカタログ、セキュリティインシデントレコード、またはセキュリティスキャン要求から、スキャンを開始することもできます。

Qualys の脆弱性一致アイテム、セキュリティインシデントカタログ、セキュリティインシデント、またはセキュリティスキャン要求から送信されたスキャンは、デフォルトの Qualys スキャナーによって実行されます。

一致する構成アイテムのスキャンに使用するオプションプロファイルを選択できます。

- オプションプロファイルには Qualys スキャン設定が含まれています。
- Now Platform® から Qualys スキャンを開始する場合は、オプションプロファイルが必要です。

ServiceNow が開始する Qualys IP スキャンの構成

ベースシステムに付属する Qualys スキャナーは、IP アドレスに基づいてスキャンを開始するためのベースライン統合を提供します。

始める前に

一致する構成アイテムのスキャンに使用するオプションプロファイルを選択できます。

- オプションプロファイルには Qualys スキャン設定が含まれています。
- Now Platform® から Qualys スキャンを開始する場合は、オプションプロファイルが必要です。

必要なロール：sn_vul_qualys.admin

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性スキャン > スキャナー.
2. Qualysレコードを開きます。
3. [アクティブ] および [デフォルト] チェックボックスをオンにします。

   Qualys スキャナーを使用して Qualys VI を自動的にスキャンするには、[アクティブ] を選択する必要があります。また、自動的に実行させるために [デフォルト] を選択する必要はありません。

   v12.0 より前では、スキャナーを使用するためには [アクティブ] であることが必要です。[デフォルト] も選択されている場合、スキャナーは、スキャン中に選択されていなくても自動的に使用されます。
4. [ソース統合] フィールドで、検索アイコンをクリックし、**Qualys** のオプション (**[Qualys** クラウドプラットフォーム] など) を選択します。
5. **[Update** (更新)] をクリックします。
6. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > アドミニストレーション > プライマリ統合.
7. **[Qualys** 資産グループリスト統合 **(Qualys Asset Group List Integration)]** を開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

a. [アクティブ] チェックボックスをオンにします。

b. [今すぐ実行] をクリックします。

8. スキャナーアプライアンスを設定するには、次の手順に従います。

> **注:**
> 検索リスト統合、Qualys 動的検索リスト、および Qualys 静的検索リスト統合からインポートした後にオプションプロファイルリスト統合を実行すると、オプションプロファイルに関連付けられている検索リストを確認できます。

a. **[Qualys** オプションプロファイルリスト統合 **(Qualys Option Profile List Integration)]** を開きます。

b. [アクティブ] チェックボックスをオンにします。

c. [今すぐ実行] をクリックします。

d. スキャナーアプライアンスのセットアップの箇所に記載されている手順に従って、スキャナーアプライアンスを構成します。
それらの手順を完了したら、ここに戻って構成を続行します。

e. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > アドミニストレーション > プライマリ統合.

f. **[Qualys** アプライアンスリスト統合 **(Qualys Appliance List Integration)]** を開きます。

g. [アクティブ] チェックボックスをオンにします。

h. [今すぐ実行] をクリックします。
Qualys スキャナーアプライアンスが正しく設定されました。

関連情報

Qualys 脆弱性統合の概要

複数の **Qualys** 脆弱性または脆弱性一致アイテムのスキャン

影響を受ける少なくとも 1 つの構成アイテム (CI) またはフォームに入力された IP アドレスを含む、複数の Qualys 脆弱性または脆弱性一致アイテムは、同時にスキャンできます。

始める前に

必要なロール：sn_vul.vulnerability_write

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

手順

1. 次のいずれかの操作を行います。
   - 次のように移動する。 **All** (すべて) > 脆弱性対応 > 修復タスク.
   - 次のように移動する。 **All** (すべて) > 脆弱性対応 > すべて.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

2. スキャンするレコードのチェックボックスをオンにします。
3. [選択した行のアクション] リストをクリックし、[脆弱性一致アイテムの再スキャン **(Re-scan for Vulnerable items)]** をクリックします。
   スキャンへのリンクを含むメッセージが表示され、作業メモが更新されます。
4. リンクをクリックすると、スキャンの進行状況または結果が表示されます。

解決済みの修復タスクの **Qualys** 自動スキャンの構成

Qualys 脆弱性一致アイテムを更新するために自動的に実行されるスキャンをスケジュールできます。

始める前に

修復タスクが [解決済み] に移行すると、関連する脆弱性一致アイテムのステータスを更新するためにスキャンが自動的に開始されます。

- スキャンはデフォルトでは無効になっています。
- 次の場所にある **Qualys** レコードの **scan_on_resolved** 統合インスタンスパラメーターを使用してスキャンを有効にします **All** (すべて) > **Qualys Vulnerability Integration** > 統合インスタンス > **Qualys**. 詳細については、次の手順を参照してください。
- このスキャンはインスタンス固有です。複数のインスタンスがあり、このスキャンを有効または無効にする場合は、変更する各インスタンスの統合インスタンスパラメーターで **scan_on_resolved** パラメーターを無効にする必要があります。
- スキャンが有効になっている場合は、オンデマンドでスキャンを開始することも、指定された期間内でのみスキャンを実行するようにスケジュールすることもできます。期間の開始時間と終了時間の設定方法については、「Qualys 再スキャンをスケジュールされた間隔内でのみ実行するように構成する」を参照してください。

必要なロール：sn_vul_qualys.admin

手順

1. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > アドミニストレーション > 統合インスタンス.
2. **[Qualys]** を選択してレコードを開きます。
   Qualys の統合インスタンスパラメーターがタブに表示されます。
3. 自動スキャンを有効にするには、*scan_on_resolved* パラメーターを探します。
4. プロパティの [値] 列に「true」と入力します。
5. [更新] をクリックします。

Qualys 再スキャンをスケジュールされた間隔内でのみ実行するように構成する

Qualys Vulnerability Integration で、必要な時間中にのみ再スキャンが実行されるように、または利用できるように、スキャンの開始時間と終了時間のパラメーターを設定します。

始める前に

この構成は、スケジュールされた再スキャンと Qualys 製品で Now Platform® インスタンスから手動で開始する再スキャンの両方に適用されます。

統合インスタンスのスキャンの開始時間と終了時間のパラメーターを設定すると、Qualys 製品の再スキャンが利用可能な期間を指定できます。たとえば、深夜 0 時から午前 10 時など、営業時間外にのみ再スキャンを指定することができます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

この設定はインスタンス固有です。複数のインスタンスがある場合は、変更する各インスタンスの統合インスタンスパラメーターで scan_start_time と scan_end_time の値を構成する必要があります。

必要なロール：sn_vul_qualys.admin

手順

1. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > 統合インスタンス > **Qualys**.
2. **[Qualys]** をクリックしてレコードを開きます。
   Qualys の統合インスタンスパラメーターが表示されます。
3. scan_start_time パラメーターの [値] 列に、再スキャンを有効にする期間の開始時刻を UTC タイムゾーンで 24 時間形式 (00:00 ～ 24:00) で入力します。
4. scan_end_time の [値] 列に、利用可能な時間帯の終了時刻を同じ形式 (00:00 ～ 24:00) で入力します。
   たとえば、scan_start_time パラメーターに開始時刻の 00:00 を入力し、scan_end_time に同じ日の朝の 10:00 AM を入力すると、深夜 0 時から午前 10 時までの時間帯以外にスケジュール設定されたスキャンまたは手動で開始されたスキャンがキューに入り、翌日の時間帯の開始時間 00:00 に起動されます。

   同じ例で、修復オーナーが午前 11:00 に再スキャンを手動で開始した場合、利用可能な構成済みスキャン時間外であるため、再スキャンはすぐには開始されません。スキャン要求は、翌日の時間帯の開始 (この例では 00:00) までキューに入ったままになります。
5. [更新] をクリックして設定を保存します。

Qualys 脆弱性スキャンレート制限

さまざまなタイプのスキャンの実行レートを定義して、外部スキャナーに送信される要求の数を制限できます。レート制限を定義したら、それを Qualys スキャナーに適用できます。

Qualys スキャンレート制限の定義

スキャンキュー内の負荷を分散するために、さまざまなタイプのスキャンの実行レートを指定できます。レート制限で指定された条件によって、キューに格納されたエントリーにレート制限が適用されるかどうかが決まります。

始める前に

必要なロール：sn_vul.admin

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性スキャン > レート制限定義.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レート制限定義

フィールド	説明
名前	キューエントリーが満たす必要がある条件を識別する、わかりやすい名前を入力します。例：「1 分あたりのスキャン数」
キュー条件	キューに格納されたスキャンエントリーがこのレート制限の対象であるかどうかを判断するために使用する条件を入力します。特定のスキャナーに固有の条件を入力してはなりません。
評価スクリプト	キューに格納されたエントリーを評価するロジックを含むスクリプトを作成します。エントリーを処理するかどうかを定義するために、スクリプトで true/false を返すことが重要です。また、評価スクリプトは、評価対象のキューに格納されたエントリーに基づいて作成します。

4. **[Submit]** をクリックします。

Qualys スキャナーへのスキャンレート制限の適用

[レート制限定義 **(Rate Limit Definitions)]** を使用してスキャンレート制限を定義すると、特定の Qualys スキャナーにレート制限を適用できます。

始める前に
必要なロール：sn.vul_admin

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性スキャン > スキャナーレート制限.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

スキャナーレート制限

フィールド	説明
スキャナー	レート制限を適用するスキャナーを選択します。
レート制限	このスキャナーに適用するレート制限を選択します。
しきい値	選択したスキャナーに適用する、選択したレート制限のしきい値を入力します。たとえば、スキャナーで毎分 4 回のスキャンが許可されており、レート制限が 1 分あたりの要求として定義されている場合、しきい値は 4 になります。

4. **[Submit]** をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Qualys 脆弱性スキャンキューの表示

Qualys 脆弱性スキャン統合に送信された脆弱性スキャン要求は、システムリソースが過負荷にならないようにキューに入れられます。必要に応じて、キューに入れられた要求のステータスを表示できます。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

このタスクについて
キューに入れられたスキャンのリストには、スキャンされた CI を識別する自動生成スキャン名が含まれています。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性スキャン > スキャンキュー.
   送信されたすべての Qualys スキャン要求がリストに表示されます。[ステータス] 列には、キューに入れられた各エントリーの現在のステータスが表示されます。[完了] のステータスは、スキャンがキューから削除されたことを示します。必ずしもスキャンの処理が完了したことを示すわけではありません。スキャンが完了した場合または失敗した場合は、[処理中] 列に適切な作業メモのテキストが表示されます。

   > **注:**
   > スキャンのためにハッシュ値が送信され、スキャナーが結果を見つけることができなかった場合、[ステータス] には [完了] が表示され、[処理中] 列の作業メモには [不明] と示されます。

2. スキャンの処理が終了したら、キューに入れられたレコードをクリックして、スキャン要求の詳細を表示します。

確認済み検出インポートのベースシステムフィルターの有効化

Qualys クラウドプラットフォーム から確認済みの検出のみをインポートするには、統合パラメーターを使用してデフォルトのフィルターを有効にします。

始める前に
必要なロール：sn_vul_qualys.admin、sn_vul.vr_import_admin

このタスクについて
ベースシステム統合インスタンスパラメーター「include_only_confirmed」は、Qualys クラウドプラットフォーム から検出のフィルター済みリストをインポートするために使用できます。デフォルトでは、このパラメーターは *FALSE* に設定され、潜在的、確認済み、または情報確認用のいずれかの検出がすべてインポートされます。

手順

1. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > アドミニストレーション > 統合インスタンス.
2. [統合インスタンス] リストから Qualys Cloud Platform 統合を開きます。
3. [統合インスタンスパラメータ] リストから [`include_only_confirmed`] パラメーターを開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

4. デフォルト値を *True* に更新します。
5. [更新] をクリックします。
   Qualys クラウドプラットフォーム 統合から確認済みの検出をインポートするフィルターが有効になりました。

タスクの結果

デフォルトでは、Qualys クラウドプラットフォーム 統合からの確認済みの検出のみが、次回の Qualys 脆弱性インポートの実行時にインポートされます。情報確認用や潜在的などの他のすべての検出は無視され、インポートされません。詳細については、「View Vulnerability Response vulnerable item detection data (Vulnerability Response 脆弱性一致アイテム検出データの表示)」を参照してください。

Qualys 脆弱性統合の再スキャンの開始

Now Platform オンデマンドから Qualys 製品の再スキャンを開始して、スケジュールされたスキャンサイクル間で脆弱性一致アイテムが修正されたことを確認します。

始める前に

脆弱性対応ワークスペースから再スキャンを開始できます。詳細については、「でのレコードと修復タスクの再スキャン Vulnerability Manager ワークスペース」と「IT 修復ワークスペースでの脆弱性一致アイテムと修復タスクの再スキャン」を参照してください。

クラシック環境での再スキャンの開始方法については、次のセクションを参照してください。

Now Platform から Qualys 製品の再スキャンを開始するために必要なセットアップ：

Now Platform® インスタンスから Qualys 製品の脆弱性一致アイテムの再スキャンをオンデマンドで開始できます。

修復オーナー、IT スペシャリスト、脆弱性アナリスト、または脆弱性マネージャーは、スケジュール設定済みのフルスキャンに関連するオーバーヘッドとボリュームを削減するために、環境内の資産 (構成アイテム) の特定の脆弱性についてターゲットの再スキャンをオンデマンドで開始できます。脆弱性一致アイテム (VI)、修復タスク (RT)、サードパーティエントリー (TPE)、または Now Platform インスタンスから検出されたアイテムレコードから Qualys 製品の再スキャンを開始できます。

再スキャンにより、修復アクティビティ、パッチ、およびその他のアクションによって構成アイテム (CI) の特定の脆弱性が正常に修正されたことを確認できます。

ユースケース：

たとえば、3 週間に 1 回環境全体をスキャンするとします。最新のフルスキャンは 1 週間前に完了しましたが、重大な脆弱性を修正するために昨日パッチを適用しました。この脆弱性の特性を考えると、この脆弱性が修正されたことを確認するのに次のスケジュール済みスキャンまで 2 週間待つことはできません。以前のスキャン中に検出された重大な脆弱性がパッチによって正常に修正されたことを確認するために、Now Platform for Qualys 脆弱性一致アイテムからターゲット再スキャンを開始できます。

クローズ済み以外のステータスで Qualys がソースの VI の再スキャンを開始できます。「でのレコードと修復タスクの再スキャン Vulnerability Manager ワークスペース」および「IT 修復ワークスペースでの脆弱性一致アイテムと修復タスクの再スキャン」を参照してください。

再スキャンに必要な次のセットアップを完了していることを確認します。詳細については、前のセクションにリストされた Qualys 脆弱性スキャナーとスキャンの構成と管理で始まる手順を参照してください。

必要なロール：sn_vul_manually_initiate_rescan

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム.
2. 再スキャンをトリガーする脆弱性一致アイテムレコードを見つけて開きます。

   注:
   ソースが Qualys の VI の再スキャンのみを開始できます。VI リストビューの [ソース] 列、または個々のレコードの [ソース] フィールドに Qualys が表示されていることを確認します。条件ビルダーを使用して、VI をソース別にグループ化できます。または、[ソース] 列が VI リストビューに表示されていない場合は、リストの左上にある [リストをカスタマイズ] アイコン (歯車アイコン) をクリックし、スラッシュバケットを使用して [ソース] を [利用可能] から [選択済み] に移動します。

3. または、 **All** (すべて) > 脆弱性対応 > 修復タスク, 脆弱性対応 > ライブラリー > サードパーティ、または再スキャンに使用する修復タスクの [検出されたアイテム **(Discovered items**)] レコード、サードパーティエントリーレコード、または検出されたアイテムレコードに対して。

   選択内容に応じて、次のレコードで [再スキャン] ボタンを使用できます。

   - 単一の VI レコードでは、VI のソースが Qualys 製品で、[クローズ済み] 以外のステータスである必要があります。複数の VI レコードの場合、すべての VI のソースが Qualys であり、[クローズ済み] 以外のステータスである必要があります。
   - RT レコードでは、修復タスクは [クローズ済み] を除くあらゆるステータスをとることが可能ですが、関連する VI はすべてソースが Qualys である必要があります。
   - サードパーティエントリー (TPE) レコードには、Qualys がソースで [クローズ済み] 以外のステータスの関連 VI レコードが少なくとも 1 つ必要です。
   - 検出されたアイテムレコードでは、Qualys がソースで [クローズ済み] 以外のステータスの VI が構成アイテムに少なくとも 1 つあります。

4. 選択したレコードの右上にある [再スキャン] をクリックします。
   表示されるダイアログで、いずれかを選択して続行します。

オプション	説明
[オプションのプロファイルを指定] チェックボックスをオンにします。	リストから、再スキャンに使用する Qualys スキャナーのオプションのプロファイルを選択します。これらは、構成してリストしたアプライアンス(スキャナー)です **Qualys Vulnerability Integration** > スキャナーアプライアンス.
[オプションのプロファイルを指定] チェックボックスをオフにします (オンの場合)。	[スキャナーアプライアンス] リストでデフォルトのスキャナーとして設定したスキャナーの Qualys オプションプロファイルがスキャンに使用されます。 Now Platform から開始するデフォルトのスキャナーの設定の詳細については、前のセクションに記載されているスキャナーアプライアンスのセットアップを参照してください。

5. [スキャンの要求 **(Request Scan)]** をクリックします。

   スキャンが処理されていることを示すメッセージが表示されます。すべての再スキャンのステータスは、再スキャンの開始に使用した VI、RT、TPE、および検出されたアイテムレコードの [スキャン] 関連リストでいつでも確認できます。メッセージで [詳細を表示] をクリックして再スキャンのステータスを表示し、指定されたレコードから開始された他の再スキャンを表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

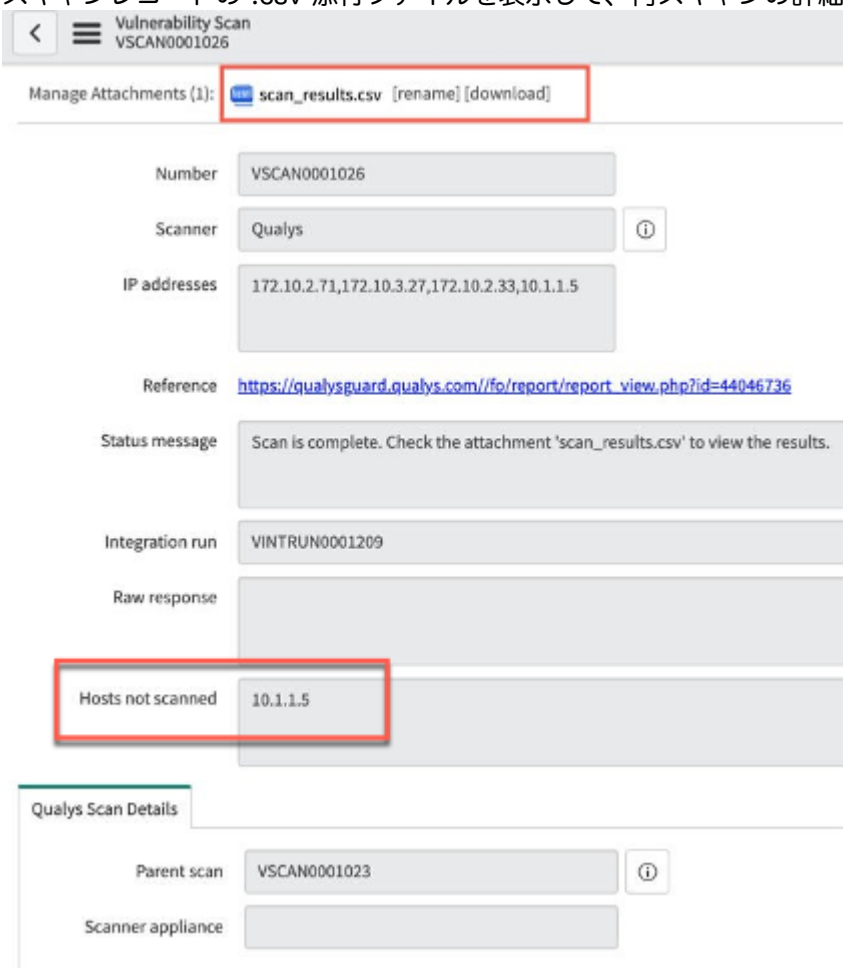
自動翻訳

インスタンスは、正常に完了するか設定された追跡期間がタイムアウトするまで、再スキャンステータスを追跡します。タイムアウトしてもスキャンは停止しません。タイムアウトは、実際の再スキャンが停止したときではなく、Now Platform が再スキャンステータスの追跡を停止したときです。

再スキャンが正常に完了すると、脆弱性一致アイテムを更新するために Qualys ホスト検出統合が自動的に開始されます。VI の数に応じて、Qualys ホスト検出統合スキャンの完了後に検出、VI、および RT が更新されます。ホスト検出統合が完了したら、これらのレコードに移動して更新を表示します。

このスキャンはインスタンス固有であり、無効にすることができます。Qualys 統合について、および統合の表示方法の詳細については、「Qualys 脆弱性統合の概要」を参照してください。

次のタスク
スキャンレコードの .csv 添付ファイルを表示して、再スキャンの詳細を確認できます。



前の画像に示すように、再スキャン中に環境内のホスト (構成アイテム) にアクセスできない場合、これらの資産に関連付けられた検出と VI は再スキャンの完了時に更新されません。これらが含まれていない理由を把握するのに役立つよう、再スキャンが完了すると、これらの CI の資産 IP アドレスが [スキャンされていないホスト (Hosts not scanned)] フィールドの脆弱性レコードに表示されます。

Qualys の脆弱性のメタデータ

Qualys ホスト検出統合が機能拡張され、Qualys のフィールドが増えました。これらのフィールドは、悪用される可能性のない Linux 脆弱性をフィルタリングするのに役立ちます。この機能拡張により、検出レベルと脆弱性一致アイテム (VI) レベルでの統合が改善されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Qualys から追加のメタデータをインポートする

脆弱性一致アイテム (VI) の追加のメタデータをインポートして、カーネルまたはサービスへの影響度に基づいて脆弱性をフィルタリングします。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント.
2. [統合設定] で、[スキャナー統合] をクリックします。
3. [インストール済みアプリケーション] で、Qualys アプリケーションの [編集] をクリックします。
4. [ホスト検出設定] をクリックします。
5. 次のように移動する。 検出用に追加のメタデータをインポート.
6. Qualys から追加のメタデータをインポートするには、次のチェックボックスを必要に応じて手動でオンにします。
   - カーネルメタデータ：実行中または実行されていない Linux カーネルで見つかった脆弱性を識別します。

     返されたメタデータの値が [いいえ] の場合は、実行されていないカーネルが原因で脆弱性が悪用される可能性がないことを意味します。取得された値の詳細については、「Qualys の脆弱性のメタデータ値」を参照してください。
   - サービスメタデータ：実行中または実行されていないポートやサービスで見つかった脆弱性を識別します。
   - 悪用可能な構成メタデータ：現在のホスト構成が原因で悪用される可能性があるかどうかを識別します。

   注:
   デフォルトでは、これらのチェックボックスは選択されていません。
7. 過去の日付の Qualys ホスト検出統合を実行します。
   開始日の設定方法の詳細については、「オプションの Qualys の変更」を参照してください。

タスクの結果
メタデータがインポートされました。

次のタスク
インポートされたメタデータを表示するには、フィルターナビゲーションに「sn_vul_detection.list」と入力します。[脆弱性一致アイテムの検出] リストが表示されます。新しく追加された列に表示される値の詳細については、「Qualys の脆弱性のメタデータ値」を参照してください。

Qualys の脆弱性のメタデータ値

カーネルメタデータ、サービスメタデータ、および構成メタデータがインポートされると、いくつかの値も取得されます。値 **[0]**、**[1]**、[利用不可] はバックエンドで処理され、それぞれ [いいえ]、[はい]、[空] に変換されます。

これらの値は、[脆弱性一致アイテムの検出および脆弱性一致アイテム (Vulnerability Item Detections and Vulnerability Items)] リストの次の列に入力されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [実行中のサービスに影響] 列
- [悪用可能な構成に影響] 列
- [実行中のカーネルに影響] 列

注:

- デフォルトでは、これらの列は表示されません。フォームレイアウトの構成方法については、「フォームレイアウトの構成」を参照してください。
- 以前の検出では、これらの列の値が空の場合があります。データを更新するには、過去の Qualys ホスト検出統合を実行します。開始日の設定方法の詳細については、「オプションの Qualys の変更」を参照してください。

次の表は、取得された値とその重大性を示しています。

取得されたフィールド値とその重大性

フィールド	値	重大性
AFFECT_RUNNING_KERNEL	0	実行されていないカーネルで脆弱性が検出されました。脆弱性が悪用される可能性はありません。
AFFECT_RUNNING_KERNEL	1	実行中のカーネルで脆弱性が検出されました。脆弱性が悪用される可能性があります。
AFFECT_RUNNING_KERNEL	利用不可	脆弱性はカーネル関連の脆弱性ではありません。
AFFECT_RUNNING_SERVICE	1	実行されていないポートまたはサービスで脆弱性が検出されました。脆弱性が悪用される可能性はありません。
AFFECT_RUNNING_SERVICE	0	実行中のポートまたはサービスで脆弱性が検出されました。脆弱性が悪用される可能性があります。
AFFECT_RUNNING_SERVICE	利用不可	脆弱性は関連の脆弱性ではありません。
AFFECT_EXPLOITABLE_CONFIG	1	ホスト構成のため、脆弱性が悪用される可能性はありません。
AFFECT_EXPLOITABLE_CONFIG	0	ホスト構成のため、脆弱性が悪用される可能性があります。
AFFECT_EXPLOITABLE_CONFIG	利用不可	脆弱性は関連の脆弱性ではありません。

Qualys インポートの追加のフィルターパラメーターの設定

Qualys 脆弱性統合を使用してスケジュール設定済みクエリのフィルタリングパラメーターをカスタマイズすると、サポートされている Qualys 統合でインポートする脆弱性データをさらに絞り込むことができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
ユースケース：脆弱性マネージャーまたはアナリストは、特定の脆弱性の詳細のみを確認できるように、クエリからデータを除外できます。たとえば、特定の IP または IP 範囲でフィルタリングされたインポート済み脆弱性を表示するとします。または、スコープ内にあるマシンのみ (外部デバイスではない企業ネットワーク内のマシンのみなど) をインポートします。

このデータを収集するには、Qualys パラメーターを追加して、必要な特定の脆弱性の詳細をインポートします。

この機能を使用すると、API コールを追加したり追加のコーディングをしたりすることなく、Now Platform の Qualys パラメーターを使用して HTTP 要求情報をカスタマイズできます。サポートされている Qualys 脆弱性統合の Qualys 統合の REST メソッドにある HTTP メソッドレコードで、これらの値を変更または追加します。

必要なロール：sn_vul.vulnerability_admin

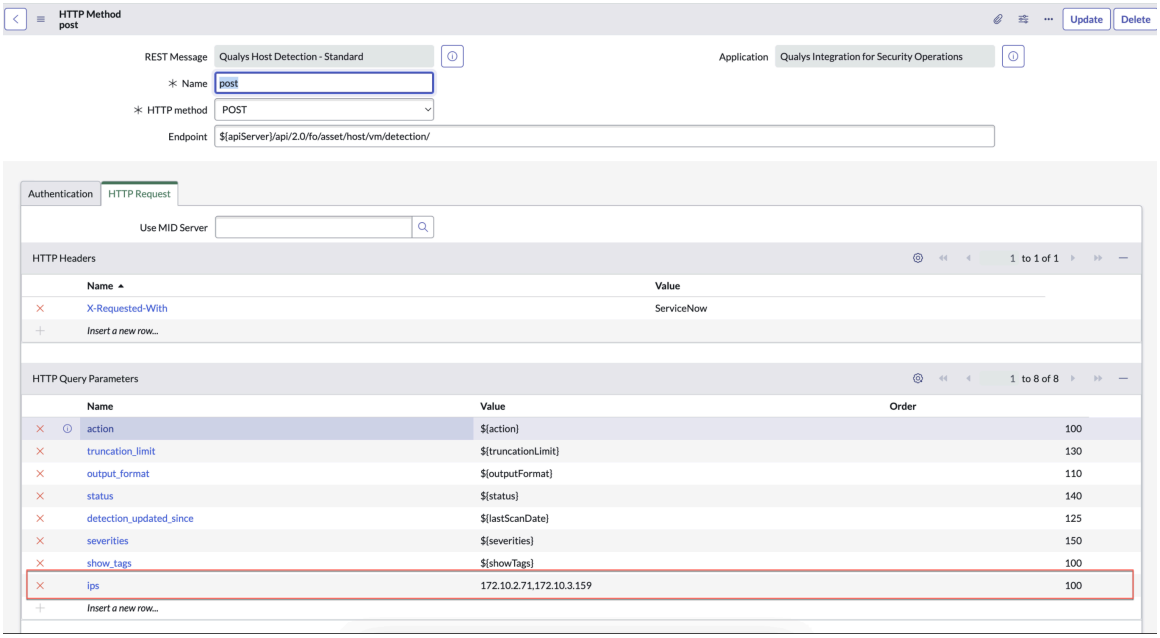
手順

1. フィルタリングに使用する開発者サイトで、Qualys 製品でサポートされているパラメーターを見つけます。
   Qualys 製品から入力するパラメーターと値は、Now Platform の統合インスタンスレベルでのみサポートされます。すべての Qualys 統合は、クエリパラメーターを使用したフィルタリングをサポートしています。
2. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > アドミニストレーション > プライマリ統合.
3. [Qualys 統合] リストページで、レコードを開く統合のレコードをクリックします。
4. [Qualys REST 詳細] タブを選択した状態で、REST メソッドの情報アイコン (I) を見つけてクリックし、続いて [レコードを開く] をクリックして HTTP メソッドレコードを開きます。
5. **[HTTP** 要求] タブを選択します。
6. 要求本文の [HTTP クエリパラメーター (HTTP Query Parameters)] で、Qualys 開発者サイトから取得した値を追加します。

   次の画像では、例として、特定の IP アドレス/範囲のみを取り込むパラメーター *ips={value}* が追加されています。この場合、[値] は指定した 1 つ以上の IP/範囲です。複数のエントリーは「172.10.2.71, 172.10.3.159」のようにカンマ区切りにし、範囲は「10.10.10.1-10.10.10.100」のようにハイフンで指定します。詳細については、Qualys 開発者サイトを参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



複数のパラメーターを入力する場合は、各値を区切る方法の詳細について、Qualys ドキュメントを参照してください。

> **注:**
> API 要件を把握しておく必要があります。これらの API プロパティをクエリパラメーターまたは本文のコンテンツに追加する必要が生じる場合があります。

Qualys 開発者サイトに記載されている役に立つと思われるその他のパラメーター：

- `ag_ids`：取得する資産グループリスト ID。このパラメーターは、スコープ内のマシンのみが取り込まれるようにします。
- `qids`：このパラメーターは、結果を特定の脆弱性 (サードパーティのエントリーテーブルの QID) のみに制限します。この設定により、システムが情報レコードであふれるのを防ぎます。

7. [更新] をクリックします。

Qualys Vulnerability Integration の問題の解決

よく発生する問題とワークアラウンドについて説明します。

インポート後に添付ファイルが表示されない

サードパーティの統合インポート後に添付ファイルが想定どおりに表示されない場合や、セキュリティインシデントで表示されない場合は、IP 制限を確認してください。

安全な IP からログインしていないと、IP アクセス制限により、添付ファイルが表示されないことがあります。インポートするたびに新しい添付ファイルが追加されるため、削除する必要がある重複が発生する可能性があります。

たとえば、サードパーティのホストインポート統合を実行するときにデータソースに添付ファイルが表示されない場合は、インポートする前に IP 制限を確認し、ユーザーをセーフリストに追加します。

変換マップの変更

変換マップは基本構成で提供され、通常はこれで十分です。組織のニーズに応じて変換マッピングを変更できます。

始める前に

必要なロール：sn_vul_qualys.admin + import_admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > システムインポートセット > アドミニストレーション > 変換マップ をクリックして REST メッセージを表示します。
2. 結果のリストをアプリケーションでフィルタリングし、リストを **[Qualys Vulnerability Integration]** アプリケーションに制限します。
3. 顧客の要件に従って変換マップを変更します。

   Qualys API によって提供されるデータの詳細については、Qualys API のドキュメント を参照してください。

XML 添付ファイルのプロパティサイズのチェック

大きなファイルに対して XML 添付ファイルプロパティが十分であることを確認します。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > システムプロパティ > インポートエクスポート.
2. 下にスクロールして プロパティをインポート > **XML** 形式 関連する検出

3. 必要に応じて値を 250 に変更し、[保存] をクリックします。

関連情報

利用可能なシステムプロパティ

データ検索の制限

デフォルトでは、Qualys からのデータの取得方法に制限はありません。多くのレコードは、顧客が脆弱性対応プロセスを使用して修正しようとしない、重大度の低い脆弱性に関連している可能性があります。対応する REST メッセージ/メソッドのパラメーターを更新すると、この動作が変更される場合があります。

この更新を処理する REST メッセージ/メソッドは、**[Qualys** ホスト検出 **-** 標準/投稿 **(Qualys Host Detection – Standard/post)]** です。値を更新するには、次の値を使用して新しい HTTP クエリパラメーターを post メソッドに追加します。

- 名前：重大度
- 値：3 ～ 5 (または必要な適切な重大度)

Qualys ナレッジベース統合の失敗の解決

Qualys から受信したペイロード添付ファイルのサイズを指定された制限まで縮小して、Qualys ナレッジベース統合を解決します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_vul.vulnerability_admin

手順

1. ペイロード添付ファイルのサイズが指定された制限内であることを確認します。
   a. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > 統合インスタンス.
   b. [統合インスタンスパラメーター] タブを選択します。
   c. **[max_delta_days]** を選択し、デフォルト値を 3 に変更します。
2. それでも統合に失敗する場合は、次の手順を実行します。
   a. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > プライマリ統合.
   b. **[Qualys** ナレッジベース] を選択します。
   c. [**Integration Details**] を選択します。
   d. [開始日時 **(Start time)]** フィールドで、現在の日付を選択して、その日の実行をスキップします。
   e. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > 統合インスタンス.
   f. [統合インスタンスパラメーター] タブを選択します。
   g. **[kb_backfill_full_import]** を選択し、デフォルト値を true に変更します。

タスクの結果
Qualys ナレッジベースバックフィル統合を実行すると、システム内のすべてのサードパーティエントリ (TPE) が更新されます。Qualys ホスト検出統合ではプレースホルダーエントリが作成されますが、Qualys ナレッジベースバックフィル統合ではプレースホルダーエントリが更新されます。

Qualys 脆弱性統合 のレポート

Qualys クラウドプラットフォーム の概要は、脆弱性アクティビティのエグゼクティブビューです。傾向、レポート、および特定のデータへのドリルダウンを表示できるため、アドミニストレーターまたはアナリストは問題のある領域をすばやく特定できます。チャートには、脆弱性一致アイテムと Qualys ナレッジベースデータが取得された後にデータが入力されます。

脆弱性対応 のワークスペースのデータの可視化

脆弱性対応 ワークスペースには、修復の進捗状況を監視するのに役立つデータの可視化が含まれています。脆弱性データの変更に応じて更新される動的なデータ表示で組織にとって重要なアクティブな脆弱性の数と重大度を表示することで、組織に対する脅威のレベルを判断できます。利用可能な動的なデータ表示方法の詳細については、「脆弱性対応 ワークスペース」、「Vulnerability Manager ワークスペース」および「IT 修復ワークスペース の探索」を参照してください。

脆弱性対応 の以前のバージョン

脆弱性アナリストは、クラシック環境のデフォルトのダッシュボードを使用して脆弱性データを監視することもできます。詳細については、「デフォルトの 脆弱性対応 ダッシュボードを使用する」を参照してください。

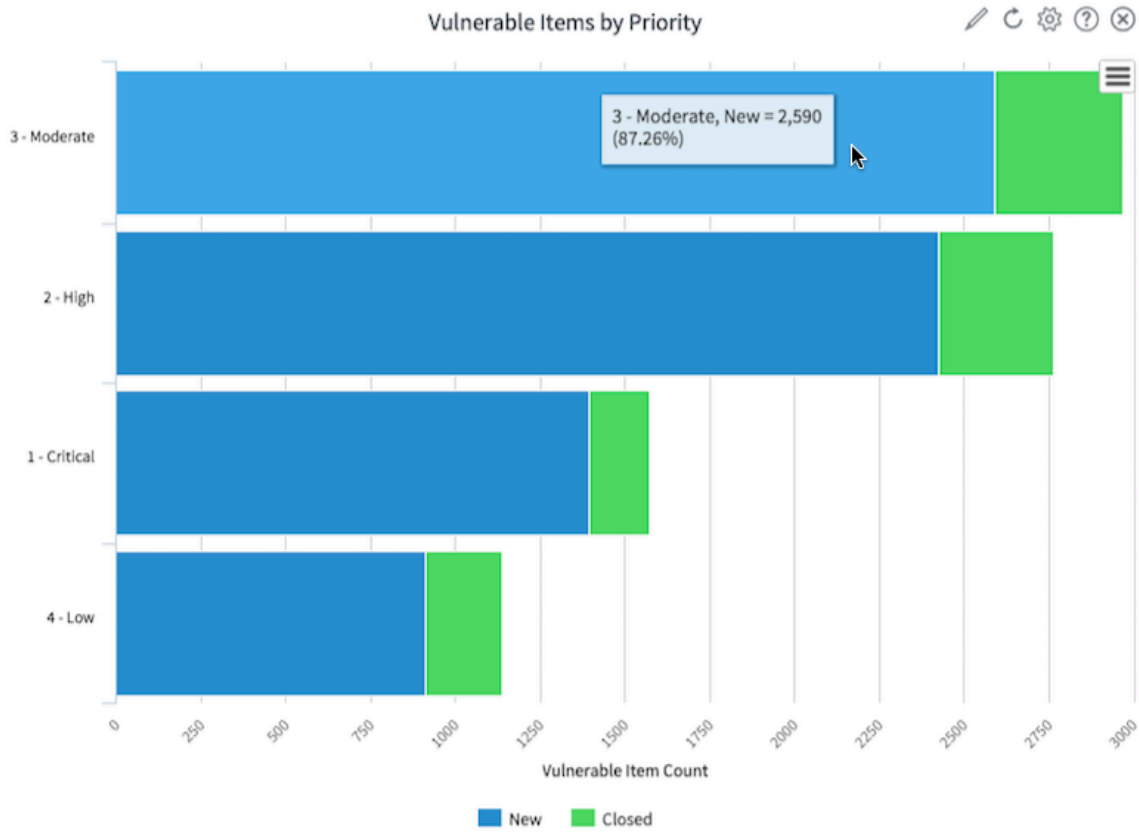
注:
Qualys クラウドプラットフォーム Vulnerability Integration を使用するには、インスタンスで調整、テスト、および展開が実行されていることが前提です。これらの機能は、製品ドキュメントでは扱っていません。カスタマーサービス & サポートにサポートを依頼してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

各チャートで、チャートの任意の部分 (棒、円、データポイントなど) をポイントして、その部分に固有の一般的なデータを表示できます。レポートの任意の部分をクリックすると、詳細な情報を提供するリストが開きます。

Qualys 脆弱性統合のサンプルチャート



Qualys クラウドプラットフォーム ホームページでは、次のレポートを利用できます。

Qualys 脆弱性統合の概要レポート

名前	ビジュアル	説明
Qualys と同期された CI	棒グラフ	CI ごとに記録されたオープンな脆弱性一致アイテムの数を多い順に表示します。
未解決の Qualys 脆弱性一致アイテム	棒グラフ	脆弱性に関連付けられたオープンな脆弱性一致アイテムの数 (CVE レコード) を多い順に表示します。
Qualys 脆弱性一致アイテムの合計	棒グラフ	7 日以内に期限切れになるようにスケジュール設定された無視された脆弱性一致アイテムの数を表示します。
優先度別の脆弱性一致アイテム	傾向図	毎週記録された脆弱性エントリーの数を表示します。
QID まん延	棒グラフ	モデルごとに記録された脆弱性一致アイテムの数を多い順に表示します。
未解決の Qualys 脆弱性一致アイテム	リスト	公開者ごとに記録された脆弱性一致アイテムの数を多い順に表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Qualys 統合実行状況チャート

[Qualys 連携実行状況] モジュールは、Qualys 統合実行のステータスをグラフィカルに表示します。

統合実行のステータスを表示するには、次に移動します: **Qualys Vulnerability Integration** > 統合実行ステータス.

脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で使用可能です。

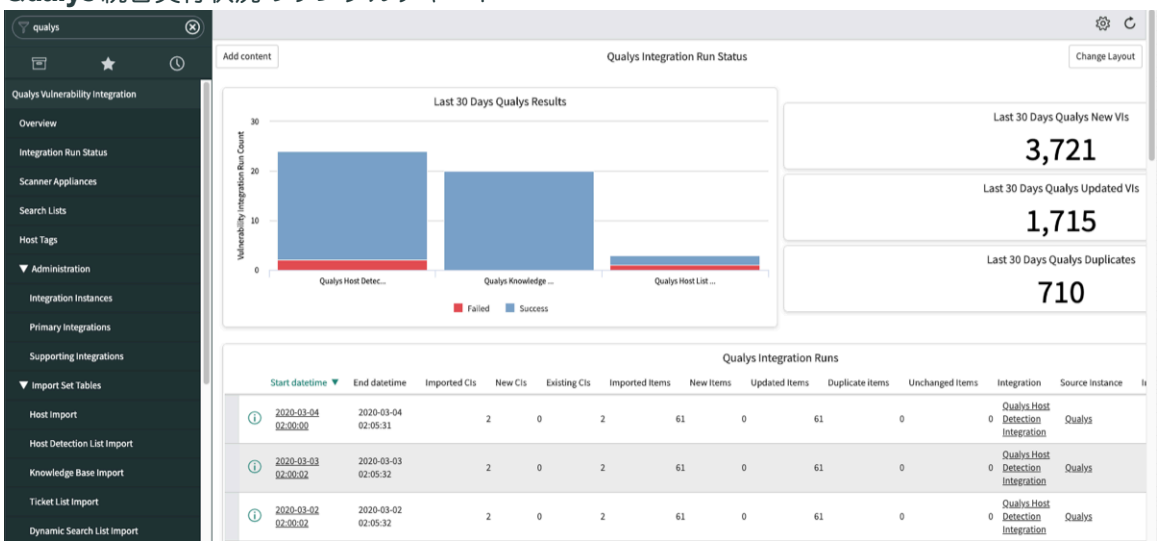
> **注:**
> Tokyo を使用している場合は、Next Experience UI でダッシュボードを表示できますが、一部の機能が失われます。

チャートで、任意の部分 (棒、円、データポイントなど) をポイントして、その部分に固有の一般的なデータを表示できます。レポートの任意の部分をクリックすると、詳細な情報を提供するリストが開きます。

Qualys 統合実行状況には、過去 30 日間の脆弱性統合実行状況が表示されます。Qualys[qualys] 更新済み VI 数は、同じ資産内の一意の検出数を示します。その後、VI は新しい検出で更新されます。

> **注:**
> 脆弱性統合の実行数は、アクティブ状況に設定されている統合にのみ表示されます。次のように移動する。 **Qualys Vulnerability Integration** > アドミニストレーション > プライマリ統合をクリックし、ステータスをアクティブに設定します。

Qualys 統合実行状況のサンプルチャート



- [インポートされたアイテム (Imported Items)] 列の値は、統合実行から作成されるレコードの合計数を表します。
- [新規アイテム (New Items)] 列には、統合実行から作成されるレコードの数が表示されます。
- [重複アイテム] 列には入力されなくなりました。この列を表示から削除することもできます。
- [更新されたアイテム] 列には、統合実行中のレコードの更新回数が表示されます。この値は、更新される一意のレコードの数ではありません。たとえば、統合実行中にレコードが 2 回更新された場合、2 回とカウントされ、更新済みアイテムが 2 つと表示されます。
- [未変更のアイテム (Unchanged items)] 列には、既にデータベースに存在し、統合実行中に検出されたものの、関連するフィールド値が変更されていないために更新されなかったレコードが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:
[新規 **CI]**、[既存の **CI]**、[新規アイテム]、[更新されたアイテム] の 4 つの値がすべてゼロの場合、統合を実行すると、これらの値は **[Qualys** 連携実行] リストから除外されます。

Qualys 統合実行状況チャートレポート

名前	説明
過去 30 日間の Qualys 結果	各統合で完了した統合実行の数。成功した実行と失敗した実行の両方が表示されます。視覚的な棒グラフで実行されます。
過去 30 日間の Qualys 新規 VI	過去 30 日間にインポートされた新規レコードの数。整数として表示されます。
過去 30 日間の Qualys 更新済み VI	過去 30 日間にインポートされた更新済みレコードの数。整数として表示されます。
過去 30 日間の Qualys 重複	過去 30 日間にインポートされた重複レコードの数。整数として表示されます。
Qualys 統合実行	リストの統合実行レコード 注: V16.1：この統合の検出を検証するには、検出または検出結果を *sn_vul_detection* テーブルの ServiceNow 検出データと比較します。 統合の進行中は、検出数または検出結果数が変更される可能性があります。このレポートでは、統合実行の完了後に、インスタンスの [現在までの数] 列に検出数が表示されます。
過去 30 日の Qualys 脆弱性一致アイテムの取り込みパフォーマンスメトリクス	過去 30 日間の脆弱性一致アイテムの日次パフォーマンスメトリクス
過去 30 日の Qualys 脆弱性一致アイテムの取り込みパフォーマンススループット	過去 30 日に測定された Qualys ホスト検出統合の脆弱性一致アイテムの日次取り込みスループット

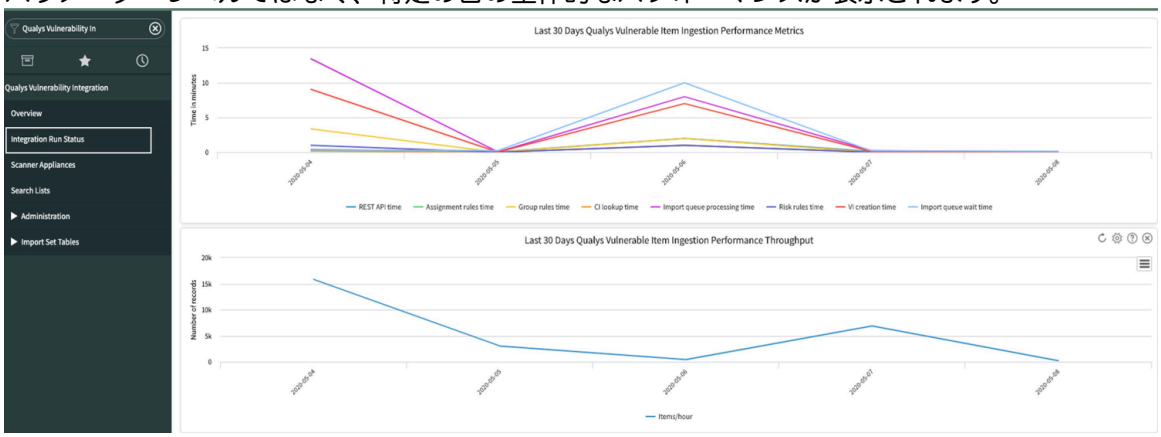
データ量やこのデータの処理にかかる時間など、複数の要因によって統合実行のパフォーマンスが影響を受ける可能性があります。次の 2 つのグラフでパフォーマンスメトリクスを比較します。

- Qualys 脆弱性一致アイテムの取り込みパフォーマンスメトリクス：アサインルール、グループルール、リスクルール、キュー待機時間、キューの処理時間、および過去 30 日間の脆弱性一致アイテムのその他の統計に関する日次パフォーマンスメトリクスを比較して、パフォーマンスの逸脱の原因を特定します。パフォーマンスは、各アクティビティにかかった時間に基づいて計算されます。これらのパラメーターは、統合実行レベルで計算され、関連付けられます。各パラメーターは、簡単に識別できるように色分けされています。
- Qualys 脆弱性一致アイテムの取り込みパフォーマンススループット：Qualys ホスト検出統合について、脆弱性一致アイテム取り込みスループットを毎日比較します。ス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ループットは 1 時間あたりのアイテム数で測定されます。このレポートには、個々のパラメーターレベルではなく、特定の日の全体的なパフォーマンスが表示されます。



Qualys データ変換

Qualys から取得されたデータは、一連のデータソースと変換によって処理されます。

Qualys 脆弱性統合のほとんどの変換は、変換スクリプトを使用して実行されます。これらのスクリプトは内部使用のためのものであり、削除は推奨されません。変更するには、コーディングや高度な ServiceNow または Qualys 脆弱性統合 の専門知識が必要です。残りのマップはこのセクションに一覧表示され、フィールドマップを使用します。

注:
インストール時に、正規化された重大度マップ (インポートされた Qualys クラウドプラットフォーム 重大度レベルを標準の ServiceNow 重大度レベルに変換) が 脆弱性対応 の [正規化された重大度マッピング] モジュールにインストールされます。詳細については、「脆弱性対応 重大度マップの作成」を参照してください。

動的検索リストインポート

Qualys 動的検索リスト変換マップは、Qualys 動的検索リストを変換およびインポートするために使用されます。この変換を変更すると、動的検索リストの処理方法とシステムへの挿入方法が変更されます。

この変換マップにアクセスするには、次に移動します: **Qualys Vulnerability Integration** > インポートセットテーブル > 動的検索リストインポート.

テーブルには、現在変換中のフィールドが表示されます。

Qualys 動的検索リスト変換マップのフィールド

ソースフィールド	ターゲットフィールド	説明
u_id	id	Qualys 動的検索リストの識別子として使用されます。
[Script]	list_type	検索リストのタイプ。[動的] は、動的検索リスト変換のデフォルトです。
u_title	title	この検索リストの Qualys での名前。

フィールドマッピングに加えて、変換プロセス中に実行される変換スクリプトもあります。

次の表は、このスクリプトが実行されるタイミングと使用目的を示しています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Qualys 動的検索リスト変換マップスクリプトのタイミングと目的

スクリプトが実行されるタイミング	スクリプトの目的
onAfter (インポートセットが変換を完了した後)。	検索リストとそれに関連する脆弱性の関係を作成します。 内部使用。変更または削除することはお勧めしません。

静的検索リストインポート

Qualys 静的検索リスト変換マップは、Qualys 静的検索リストを変換およびインポートするために使用されます。この変換を変更すると、静的検索リストの処理方法とシステムへの挿入方法が変更されます。

この変換マップにアクセスするには、次に移動します: **Qualys Vulnerability Integration** > インポートセットテーブル > 静的検索リストインポート.

テーブルには、現在変換中のフィールドが表示されます。

Qualys 静的検索リスト変換マップのフィールド

ソースフィールド	ターゲットフィールド	説明
u_id	id	Qualys 静的検索リストの識別子として使用されます。
u_title	title	この検索リストの Qualys での名前。
[Script]	list_type	検索リストのタイプ。[静的] は、静的検索リスト変換のデフォルトです。

フィールドマッピングに加えて、変換プロセス中に実行される変換スクリプトもあります。

次の表は、このスクリプトが実行されるタイミングと使用目的を示しています。

Qualys 静的検索リスト変換マップスクリプトのタイミングと目的

スクリプトが実行されるタイミング	スクリプトの目的
onAfter (インポートセットが変換を完了した後)。	検索リストとそれに関連する脆弱性の関係を作成します。 内部使用。変更または削除することはお勧めしません。

資産グループインポート

Qualys 資産グループアプライアンス変換マップは、Qualys 資産グループデータを変換してスキャナーアプライアンスレコードを作成するために使用されます。この変換を変更すると、スキャナーアプライアンスの作成方法と変更方法が変更されます。

この変換マップにアクセスするには、次に移動します: **Qualys Vulnerability Integration** > インポートセットテーブル > 資産グループインポート.

テーブルには、現在変換中のフィールドが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Qualys 資産グループ変換マップのフィールド

ソースフィールド	ターゲットフィールド	説明
u_id	id	Qualys 資産グループの識別子として使用されます。
[Script]	manual	ターゲットレコードがどのように作成されたかを判別するスクリプト値。変換によって作成された場合、このフィールドは常に false です。
[Script]	ips	変換中の資産グループに関連付けられている IP アドレス
u_default_appliance_id	appliance_id	この資産グループ内のデフォルトアプライアンスの Qualys アプライアンス識別子
u_title	asset_group_name	Qualys 資産グループの名前

フィールドマッピングに加えて、変換プロセス中に実行される変換スクリプトもあります。

次の表は、このスクリプトが実行されるタイミングと使用目的を示しています。

Qualys 資産グループ変換マップスクリプトのタイミングと目的

スクリプトが実行されるタイミング	スクリプトの目的
onBefore (インポートセットの変換が完了する前)。	資産グループのインポートをデフォルトのアプライアンスとマップされた IP アドレスのセットのみに制約するスクリプト 内部使用。変更または削除することはお勧めしません。

自動翻訳

アプライアンスインポート

Qualys アプライアンス変換マップは、Qualys アプライアンスデータをアプライアンスレコードに変換するために使用されます。これは、最初に資産グループインポートから作成されるアプライアンスレコードを更新するために使用されます。この変換を変更すると、アプライアンスレコードをアプライアンスの詳細で更新する方法が変更されます。

この変換マップにアクセスするには、次に移動します: **Qualys Vulnerability Integration** > インポートセットテーブル > アプライアンスインポート.

テーブルには、現在変換中のフィールドが表示されます。

Qualys アプライアンス変換マップのフィールド

ソースフィールド	ターゲットフィールド	説明
u_name	appliance_name	Qualys スキャナーアプライアンスの名前
u_status	appliance_status	Qualys スキャナーアプライアンスの最後にレポートされたステータス
u_id	appliance_id	Qualys アプライアンス識別子

フィールドマッピングに加えて、変換プロセス中に実行される変換スクリプトもあります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の表は、このスクリプトが実行されるタイミングと使用目的を示しています。

Qualys アプライアンス変換マップスクリプトのタイミングと目的

スクリプトが実行されるタイミング	スクリプトの目的
onBefore (インポートセットの変換が完了する前)。	指定された ID のアプライアンス名とステータスを更新するために使用されます。 内部使用。変更または削除することはお勧めしません。

Qualys REST メッセージ

Qualys REST メッセージは、Qualys API の呼び出しに使用されます。

Qualys のバージョン 12.9.2 以降では、ベーシック認証と OAuth のどちらでも選択できるようになっています。インスタンスパラメーターの Qualys クラウド認証方法は、基本認証用に事前構成されています。OAuth を使用する場合は、統合インスタンスパラメーターを変更してから、OAuth の REST メッセージを直接設定する必要があります。

Qualys ホスト検出 REST メッセージ

Qualys ホスト検出 REST メッセージは、Qualys ホスト検出統合のホストリスト検出 API を最初に呼び出します。

Qualys ホスト検出 **REST** メッセージのパラメーター

パラメーター名	値	説明
action	リスト	要求された操作のタイプを示します。 必要なパラメーター。変更は必要ありません。
output_format	XML	Qualys によって返されるレポートの形式を設定します。 さまざまなスクリプトや変換では XML が想定されるため、値の変更は推奨されません。
detection_processed_after	${lastScanDate}	特定の日時以降に検出ステータスが変更された検出のみを表示します。一度も変更されていない検出の場合、日付は最後の検出日に適用されます。
truncation_limit	500	要求に従ってデータを取得するホストの数。このパラメーターは、ページネーションの目的で使用されます。 デフォルト値は 500 ですが、これより大きい値または小さい値を使用できます。システム負荷が大幅に増加するため、100 未満に設定しないでください。 値が小さいほど Qualys API の呼び出し回数が多くなり、値が大きいほど処理する結果セット

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Qualys ホスト検出 **REST** メッセージのパラメーター (続く)

パラメーター名	値	説明
		が大きくなり、データ検索/処理のタイムアウトが発生する可能性があります。
status	新規、修正済み、アクティブ、再オープン	Qualys から取得する検出ステータス。 デフォルトでは、すべてのステータスが取得されます。大量のデータをプルする場合 (多くの場合、データの最初のプル)、このリストから [修正済み] ステータスを除外すると便利です。 既にシステムに存在する脆弱性を更新する場合は、[修正済み] ステータスを含めることが重要です。

Qualys ホスト検出ページネーション **REST** メッセージ

ホスト検出ページネーション REST メッセージは、ホスト検出 API へのページネーション要求を処理します。

プライマリホスト検出を実行する場合、Qualys API がデータの次のページをフェッチするための URL を提供すると、この REST メッセージはその追加データを取得します。このデータは、ホスト検出ページネーションハンドラーによって使用されます。

ホスト検出ページネーション REST は特殊な REST メッセージであり、変更することを意図したものではありません。

Qualys ナレッジベース (バックフィル) **REST** メッセージ

Qualys ナレッジベース (バックフィル) REST メッセージは、Qualys ナレッジベース統合の脆弱性データが最後に変更された時点のタイムスタンプに基づいて、Qualys ナレッジベースデータを取得します。

REST メッセージメソッドレコードを変更すると、ナレッジベース情報を取得するための Qualys への要求が影響を受けます。

次の表に、送信される要求パラメーターを示します。

Qualys ナレッジベース (バックフィル) **REST** メッセージのパラメーター

パラメーター	値	説明
action	リスト	要求されている操作のタイプを示します。 必要なパラメーター。変更は推奨されません。
details	すべて	取得された脆弱性の詳細レベルを示します。 必要に応じて安全に変更できます。
ids	${qids}	Qualys から取得する QID を指定します。 コードで参照されます。変更は推奨されません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Qualys ナレッジベース (日付ベース) REST メッセージ

Qualys ナレッジベース (日付ベース) REST メッセージは、脆弱性データが最後に変更された時点のタイムスタンプに基づいて、Qualys ナレッジベースデータを取得するのに使用されます。このメッセージは、Qualys ナレッジベース統合によって使用されます。

REST メッセージメソッドレコードを変更すると、ナレッジベース情報を取得するための Qualys への要求が影響を受けます。

次の表に、送信される要求パラメーターを示します。

Qualys ナレッジベース (日付ベース) REST メッセージのパラメーター

ソースフィールド	ターゲットフィールド	説明
action	リスト	要求された操作のタイプを示します。 必要なパラメーター。変更は推奨されません。
details	すべて	取得された脆弱性の詳細レベルを示します。 必要に応じて安全に変更できます。
last_modified_after	${dateStart}	履歴データの取得をいつ開始するかを示します。 開始時間を決定し、ページネーションを支援するためにコードで使用されます。 変更または削除は推奨されません。
last_modifiedbefore	${dateEnd}	履歴データの取得をいつ終了するかを示します。終了時間を決定し、ページネーションを支援するためにコードで使用されます。 変更または削除は推奨されません。

Qualys チケット REST メッセージ

Qualys チケット REST メッセージは、Qualys チケット統合の Qualys チケット情報を取得します。REST メッセージメソッドレコードを変更すると、チケット情報を取得するための Qualys への要求が影響を受けます。

次の表に、送信される要求パラメーターを示します。

Qualys チケット REST メッセージのパラメーター

パラメーター名	値	説明
modified_since_datetime	${lastRunDatetime}	統合の最終実行日と、その後のデータをプルする日付を示します。 コードで使用されます。変更は推奨されません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Qualys チケット **REST** メッセージのパラメーター (続く)

パラメーター名	値	説明
since_ticket_number	${lastTicketNumber}	Qualys から最後に取得されたチケットを示します。 ページネーションに使用されます。変更は推奨されません。
show_vuln_details	1	脆弱性の詳細を取得するかどうかを示します。

Rapid7 脆弱性統合の概要

ServiceNow Rapid7 脆弱性統合 では、Rapid7 データウェアハウスまたは Rapid7 InsightVM 製品からインポートされたデータを使用して、悪意のある可能性がある脅威の影響度と優先度を判断できます。

Rapid7 Nexpose センサーがデータを収集して Rapid7 データウェアハウス (オンプレミス) または Rapid7 InsightVM (クラウドベース) 製品に自動的に送信すると、情報が継続的に分析され、関連付けられます。ServiceNow 脆弱性対応 と簡単に統合して、脆弱性を CI およびサービスにマッピングします。Rapid7 脆弱性統合はインスタンスの脆弱性データを拡張します。

Rapid7統合は、Rapid7 データウェアハウスまたは Rapid7 InsightVM 製品とやり取りするエントリーポイントであり、スケジュール済みジョブとして呼び出されます。スケジュール済みジョブでは、インスタンスを他の脆弱性管理システムと同期させることで、脆弱性修復ライフサイクルを簡素化します。スケジュール済みジョブは、指定した順序で自動的に実行されます。スケジュール済みジョブを手動で実行することもできます。

注:

Rapid7 データウェアハウスと Rapid7 InsightVM の両方をデータのソースとして使用すると、脆弱性レコードが重複するリスクがあります。

注:
[データウェアハウス] 統合タイプから **[InsightVM]** タイプに移行するときに、既存のデータウェアハウスレコードを重複排除できます。詳細については、「Rapid7 脆弱性統合データウェアハウスレコードの重複排除」を参照してください。

Rapid7 InsightVM 脆弱性統合を複数展開している場合は、展開ごとに統合を追加できます。 複数のサードパーティの展開と脆弱性によって識別される資産は、CMDB と統合され、調整されます。この統合は、複数の展開間でスキャンプロセスが重複している場合でも行われます。各展開から供給されたデータは、脆弱性対応 の単一インスタンスで識別されて利用可能です。

注:
元の脆弱性統合は削除できませんが、無効にすることはできます。無効になったテンプレートから作成された統合は、デフォルトで無効になっています。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

利用可能バージョン

Yokohama のリリースバージョン	リリースノート
Rapid7 脆弱性統合 v13.6、13.7	互換性情報については、「KB0856498 脆弱性対応 互換性マトリクスおよびリリーススキーマの変更」を参照してください。

ロール

Rapid7 脆弱性統合タスクには、次のロールが関与します。

- sn_vul_r7.admin：レコードの読み取り、書き込み、削除を実行できます。
- sn_vul_r7.user：レコードの読み取りおよび書き込みを実行できます。
- sn_vul_r7.read：レコードの読み取りを実行できます。

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

Rapid7 脆弱性統合 の統合

Rapid7 脆弱性統合を表示するには、次に移動します: **Rapid7** > アドミニストレーション > 統合.

ベースシステムには、次の統合が含まれています。

Rapid7 データウェアハウス統合

統合	説明
Rapid7 脆弱性統合	Rapid7 Nexpose から脆弱性データを取得し、インスタンスで処理します。
Rapid7 資産リスト統合	Rapid7 Nexpose データウェアハウスからスキャンデータを週に 1 回取得し、インスタンスの [検出されたアイテム] モジュールに保存します。[前回スキャン] の日付を使用すると、最近スキャンされていない資産を特定するのに役立ちます。脆弱性対応 の [検出されたアイテム] リストに [前回スキャン] の時間を表示します。
Rapid7 カテゴリ統合	Rapid7 Nexpose からカテゴリ情報を取得します。カテゴリは、脆弱性を高レベルで分類します。
Rapid7 Exploit Integration	Rapid7 Nexpose からエクスプロイト情報を取得します。
Rapid7 マルウェアキット統合	Rapid7 Nexpose からマルウェアキット情報を取得します。
Rapid7 参照統合	CVE やベンダー固有の脆弱性の参照情報など、外部の各種法令・基準等への参照を取得します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Rapid7 データウェアハウス統合 (続く)

統合	説明
Rapid7 ソリューション統合	Rapid7 Nexpose からソリューションデータを取得し、特定の脆弱性に対する推奨ソリューションを提供します。
Rapid7 優先ソリューション統合	優先されるソリューションに関する情報を取得します。
Rapid7 前提条件ソリューション統合	他のソリューションの前提条件であるソリューションに関する情報を取得します。この統合が実行されると、Rapid7 データウェアハウスからソリューションと前提条件ソリューションのマッピングがフェッチされます。 **注:** この統合は、脆弱性ソリューション管理 プラグインがアクティブ化されている場合にのみ機能します。
Rapid7 脆弱性ソリューションマップ統合	ソリューションを脆弱性に関連付けるためのマッピングを取得します。
Rapid7 脆弱性一致アイテム統合	Rapid7 Nexpose から脆弱性一致アイテムデータを取得し、インスタンスで処理します。 この統合の出力は脆弱性一致アイテムです。
Rapid7 脆弱性一致アイテム解決統合	Rapid7 Nexpose でクローズ済みとマークされた脆弱性一致アイテムに関する情報を取得し、脆弱性対応 の対応する脆弱性一致アイテムをクローズします。
Rapid7 サイト統合	Rapid7 Nexpose からサイトデータを取得します。サイトは、スキャンの対象となる資産のコレクションです。
Rapid7 資産リスト統合	Rapid7 データウェアハウスからホストタグとスキャンデータを週に 1 回取得し、インスタンスの [検出されたアイテム] モジュールに保存します。[前回スキャン] の日付を使用すると、最近スキャンされていない資産を特定するのに役立ちます。脆弱性対応 の [検出されたアイテム] リストに [前回スキャン] の時間を表示します。
Rapid7 包括的脆弱性一致アイテム統合	前回の正常な統合実行以降にスキャンされたすべての構成アイテムのすべての Rapid7 検出をインポートします。[古い脆弱性一致アイテムの自動クローズ (Auto-Close Stale Vulnerable Items)] モジュールが有効になっている場合、インポートされた最新のデータに基づいて、スキャン中に最近検出されなかった脆弱性一致アイテムが [クローズ済み] に自動的に移行します。

Rapid7 InsightVM の統合

統合	説明
Rapid7 脆弱性一致アイテ	Rapid7 InsightVM から脆弱性一致アイテムデータを取得し、インスタンスで処理します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Rapid7 InsightVM の統合 (続く)

統合	説明
ム統合 — API	
Rapid7 脆弱性統合 — API	Rapid7 InsightVM から参照、カテゴリ、エクスプロイト、マルウェアキット、および脆弱性データを取得し、インスタンスで処理します。
Rapid7 資産リスト統合 - API	Rapid7 InsightVM からホストタグとスキャンデータを週に 1 回取得し、インスタンスの [検出されたアイテム] モジュールに保存します。[前回スキャン] の日付を使用すると、最近スキャンされていない資産を特定するのに役立ちます。脆弱性対応 の [検出されたアイテム] リストに [前回スキャン] の時間を表示します。
Rapid7 包括的脆弱性一致アイテム統合 - API	前回の正常な統合実行以降にスキャンされたすべての構成アイテムのすべての Rapid7 検出をインポートします。[古い脆弱性一致アイテムの自動クローズ (Auto-Close Stale Vulnerable Items)] モジュールが有効になっている場合、インポートされた最新のデータに基づいて、スキャン中に最近検出されなかった脆弱性一致アイテムが [クローズ済み] に自動的に移行します。
Rapid7 サイト統合	Rapid7 InsightVM 製品からサイトデータを取得します。この統合は週 1 回 00:00:00 に実行するように設定されます。

インポート中に、まだ存在しない CVE レコードは NVD レコードとして作成され、デフォルトで Rapid7 のサードパーティエントリーで参照されます。Rapid7 のテンプレート統合は削除できません。代わりに無効にします。

Rapid7 のサービスグラフコネクタ

バージョン 2.0 以降、Rapid7 のサービスグラフコネクタは ServiceNow® Store から入手できます。詳細については、「Service Graph Connector for Rapid7」を参照してください。

CI ルックアップルール

CI ルックアップルールにより、脆弱性一致アイテムレコードの [構成アイテム] フィールドの入力方法が決定します。

CI ルックアップルールの詳しい仕組みについては、「脆弱性対応 サードパーティ脆弱性統合の構成アイテムを識別するための CI ルックアップルール」を参照してください。

ルックアップルールを作成または編集するには、「脆弱性対応 CI ルックアップルールの作成」を参照してください。

注:
ルールは、一度削除すると元に戻せません。新しいルールを作成する場合は、既存のルールを削除せずに非アクティブ化します。

検出されたアイテム

このモジュールは、Rapid7 脆弱性一致アイテム統合 (データウェアハウスまたは InsightVM API) および Rapid7 資産リスト統合 - API からのインポート中に検出された構成アイテムをリストします。Rapid7 資産リスト統合 - API は、前回の統合実行以降に脆弱性がスキャンされたすべての Rapid7 資産をインポートします。Rapid7 データウェアハウス資産リスト統合が含まれています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

> **注:**
> このリストのデフォルトのフィルターは [不一致] に設定されています。フィルターを削除すると、インポートから検出されたすべてのアイテムを表示できます。

[検出されたアイテム] モジュールの詳細については、脆弱性対応 の「検出されたアイテム」を参照してください。

ホストタグ

ホストタグは、Rapid7 資産リスト統合 - Rapid7 InsightVM の API 統合の一部としてインポートされます。これらは、主に Rapid7 InsightVM の 脆弱性対応 アサインおよび修復タスクルールでのフィルタリングに使用されます。これらは [検出されたアイテム] フォームに表示されます。

ホストタグ

> **注:**
> Rapid7 資産リスト統合 - API 統合は、脆弱性一致アイテムがインポートされてグループ化される前にすべてのタグがルール内に存在できるように、脆弱性対応 でのアサインルールまたは修復タスクルールを作成する前に実行する必要があります。

- タグストレージでは大文字と小文字は区別されません。**[San Diego]** タグが作成されると、**[SAN DIEGO]** タグを [ホストタグ] テーブルに格納できなくなります。「San Diego」と「SAN DIEGO」は同じホストタグと見なされます。最初にインポートされたタグが優先されます。
- 修復タスクルールのグループキーとしてホストタグを使用すると、予期しない結果になることがあります。ホストタグは、条件ビルダー専用です。
- ホストタグは、グローバルシステムプロパティ **sn_vul.import_host_tags** で制御されます。このプロパティはデフォルトで [true] に設定されています。タグをオフにすると、すべてのインスタンスでオフになります。

サイト

サイトは、スキャンの対象となる資産のコレクションです。サイトは、ターゲット資産、スキャンテンプレート、1 つ以上のスキャンエンジン、およびその他のスキャン関連の設定 (スケジュールやアラートなど) で構成されます。サイトは Rapid7 アプリケーションによって管理されます。

構成中に Rapid7 脆弱性統合サイトをフィルタリングすると、インポート中にサイト別に資産を分類して要求できます。フィルタリングのインポートについては、「Rapid7 サイト別のフィルタリング」を参照してください。

Rapid7 データウェアハウスと Rapid7 InsightVM サイト統合は、週次のスケジュール済みジョブとしてサイトをインポートします。

インポートされたサイトをリストで表示するには、 **Rapid7** > 拠点.

スキャンによってクローズされていない解決済みの脆弱性一致アイテムの再オープン

Now Platform インスタンスで [解決済み] に設定されていても後続の統合実行によって [クローズ済み]/[修正済み] に移行されていない脆弱性一致アイテムは、再スキャン中に検出された場合に再オープンされます。

Rapid7 検出の場合、インスタンスの [Rapid7 構成] ページで、解決済みの VI を経過時間別に再オープンするオプションが利用可能になりました。有効にすると、[解決済み] に設定されていても、後続のスキャンで [クローズ済み]/[修正済み] に移行しなかった VI は、入力した日数後に [オープン] に戻ります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

識別および調整エンジン (IRE) を使用した CI の作成

既存の CI がサードパーティのスキャナーからインポートされたホストと一致しない場合、識別および調整エンジン (IRE) を使用して新しい CI を作成できます。新しいクラスを使用して CI を作成するには、CMDB CI クラスモデルプラグインを有効にします。これを行わない場合は、一致しない CI が [不一致] CI クラスに作成されます。詳細については、「識別および調整エンジンを使用して 脆弱性対応 の CI を作成する」を参照してください。一致しないクラウドリソースの分類を優先 CI クラスに構成する方法の詳細については、「一致しないクラウド資産の CI クラスの更新」を参照してください。

脆弱性一致アイテムの再スキャン

Rapid7 プラットフォームで再スキャンを開始し、スケジュールされたスキャンサイクル間で脆弱性一致アイテムが修正されたことを確認します。「Rapid7 脆弱性統合の再スキャンの開始」を参照してください。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

Rapid7 ソリューション管理

脆弱性ソリューション管理 プラグインをアクティブにすると、Rapid7 データウェアハウスと Rapid7 InsightVM の両方の Rapid7 ソリューションが脆弱性ソリューション [sn_vul_solution] テーブルに入力されます。ただし、脆弱性ソリューション管理 プラグインをアクティブ化していない場合、Rapid7 脆弱性統合はそのまま機能し、カスタム [sn_vul_r7_solution] テーブルのソリューションをインポートします。詳細については、「Rapid7 ソリューション管理」を参照してください。

Rapid7 脆弱性統合 の準備

統合を成功させるには、統合前のタスクを計画して慎重に実行する必要があります。これらのタスクを実行して、統合の準備をします。Rapid7 脆弱性統合は、ユーザーが Rapid7 データウェアハウスまたは Rapid7 InsightVM 製品のスキャンに精通しており、環境で実行していることを前提としています。

始める前に
必要なロール：admin

このタスクについて
Rapid7 スキャナーは、脆弱性対応 アプリケーションではデフォルトで無効になっています。これらのアプリケーションをソースとする脆弱性一致アイテムまたは修復タスクから再スキャンを実行しようとすると、[再スキャン] ボタンは使用できません。

ServiceNow® Store から Rapid7 脆弱性統合 アプリケーションをダウンロードしてインスタンスにインストールする前に、統合タイプに関する次の情報を確認し、情報を設定します。

ServiceNow® Store で利用可能な Rapid7 脆弱性統合 に含まれている統合には、次の 2 つのタイプがあります。

- Rapid7 InsightVM
- Rapid7 データウェアハウス

Rapid7 データウェアハウスタイプ：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- Rapid7 データウェアハウスサーバーの URL と認証情報が必要です。
- MID サーバーが必要です。
- PostgresSQL ドライバーを使用してデータウェアハウスでクエリを実行します。
- 複数のインスタンスをサポートしていません。

Rapid7 InsightVM 統合タイプ

- クラウドベースであり、REST API を使用します。この統合には Rapid7 インサイトアカウント内の API キーが必要です。
- 複数のインスタンスをサポートしています。

これらの統合タイプのセットアップ要件の詳細については、「Rapid7 データウェアハウス統合のセットアップ」および「Rapid7 InsightVM 統合のセットアップ」を参照してください。

Rapid7 データウェアハウス統合のセットアップ

Rapid7 データウェアハウス統合は、Rapid7 脆弱性統合 Rapid7 脆弱性統合 に含まれる統合タイプの 1 つです。

始める前に
Rapid7 データウェアハウス統合を実行する前に、次のセットアップタスクを完了します。

- Rapid7 データウェアハウスアドオンを取得します。このアドオンを取得してインストールするには、Rapid7 Web サイト とドキュメントを参照してください。
- 最新の PostgresSQL ドライバーを取得します。https://jdbc.postgresql.org/ に移動し、最新のドライバーをダウンロードします。
- データウェアハウスへのクエリを実行する MID サーバー。MID サーバーのセットアップ方法の詳細については、「MID サーバー」を参照してください。

  データウェアハウス名をメモします。Rapid7 データウェアハウス統合タイプは、スタンドアロン MID サーバーのみをサポートします。クラスター化された MID サーバーはサポートされていません。

- Rapid7 データウェアハウスサーバーの URL と認証情報を取得し、アクセス可能な状態にします。

必要なロール：システムアドミニストレーター [admin] がアプリをダウンロードしてインストールします。 sn_vul.vulnerability_admin または sn_vul.admin は、構成を監視し、期待される結果を検証します。

手順

1. Rapid7 脆弱性統合アプリケーションをインストールする Now Platform インスタンスにログインします
2. 前にリストしたセットアップタスクでダウンロードした PostgreSQL JAR ファイルをインストールします。

   a. Now Platformインスタンスで、 **All** (すべて) > **MID Server** > **JAR** ファイル.

   b. [**New**] をクリックします。

   c. 以前にダウンロードした PostgresSQL ドライバーの名前を入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

必要に応じて、[バージョン]、[ソース] および [説明] の情報を入力します。[アクティブ] チェックボックスをオンのままにします。

d. ヘッダーのペーパークリップアイコン を使用して、ダウンロードした JAR ファイルを添付します。

e. [Submit] をクリックします。

Rapid7 データウェアハウス統合のセットアップが完了しました。Rapid7 脆弱性統合をインストールする前に Rapid7 InsightVM 統合の要件を確認していない場合は、「Rapid7 InsightVM 統合のセットアップ」および「Rapid7 脆弱性統合 の準備」を参照してください。

Rapid7 脆弱性統合のエンタイトルメントの取得、ダウンロード、およびインストールの手順については、「Rapid7 脆弱性統合 をインストールする」を参照してください。

Rapid7 InsightVM 統合のセットアップ

Rapid7 InsightVM 統合は、Rapid7 脆弱性統合 Rapid7 脆弱性統合 に含まれる統合タイプの 1 つです。

始める前に
Rapid7 InsightVM 統合を実行する前に、次のセットアップタスクを完了します。

必要なロール：システムアドミニストレーター [admin] がアプリをダウンロードしてインストールします。 sn_vul.vulnerability_admin または sn_vul.admin は、構成を監視し、期待される結果を検証します。

手順

1. Rapid7 InsightVM 統合タイプの場合は、リージョンと API キーを用意してください。
   Rapid7 に問い合わせ、適切なリージョンと API キーを取得してください。
   Rapid7 InsightVM 統合のセットアップが完了しました。Rapid7 脆弱性統合をインストールする前に Rapid7 データウェアハウス統合の要件を確認していない場合は、「Rapid7 データウェアハウス統合のセットアップ」 および「Rapid7 脆弱性統合 の準備」を参照してください。
2. Rapid7 脆弱性統合のエンタイトルメントの取得、ダウンロード、およびインストールの手順については、「Rapid7 脆弱性統合 をインストールする」を参照してください。

Rapid7 脆弱性統合 をインストールする

脆弱性対応 と適切に統合できるように統合のセットアップ手順を完了したら、エンタイトルメントを取得し、Now Platform インスタンスにアプリケーションをダウンロードしてインストールします。

始める前に
必要なロール：admin (ダウンロードおよびインストール)、sn_vuln.admin は構成を監視し、予想される結果を検証します。

1. Rapid7 脆弱性統合の統合タイプとセットアップ要件の詳細については、「Rapid7 脆弱性統合 の準備」、「Rapid7 データウェアハウス統合のセットアップ」および「Rapid7 InsightVM 統合のセットアップ」を参照してください。
2. ダウンロードとインストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。
3. アプリケーションをアクティブ化したら、次の手順に従って Rapid7 脆弱性統合を構成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

セットアップタスク	説明
脆弱性対応 アプリケーションがインストールされ、アクティブ化されていることを確認します。	このアプリケーションがアクティブ化されていることを確認するには、次の場所に移動します サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応 のインストール」を参照してください。
インスタンスに必要な Now Platform ロールがあることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。 脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。 • システムアドミニストレーター [admin] がアプリをインストールします。まだアサインされていない場合、アドミニストレーターは脆弱性アドミン [sn_vul.vulnerability_admin または sn_vul.admin] ロールをアサインします。 • 脆弱性アドミニストレーターは、構成を監視して予想される結果を確認します。 Rapid7 admin ロールは、脆弱性対応 (VR) アプリケーションで管理ロールがアサインされたときに継承されます。
インポートする予定の脆弱性一致アイテムの数に基づいて、インスタンスのサイジングを検証します。	インスタンスが小さすぎると、ロードに時間がかかることがあります。インスタンスのサイズがわからない場合は、カスタマーサービス & サポート にお問い合わせください。
フィルタリングをセットアップ	フィルタリングを使用して初期インポートのアイテム数を制限し、後続のインポートでフィルターを調整して展開を段階的に行います。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
脆弱性算出を無効化	脆弱性算出を使用しない場合は、定義した他の脆弱性算出に加えて、次の操作を実行します - 使用しないデフォルトの脆弱性算出の無効化。脆弱性算出は、脆弱性一致アイテムレコードが作成または更新されるたびに実行され、初期インポートのパフォーマンスに影響を与える可能性があります。
run-as ユーザーのデフォルト値を保持	統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。
ホストタグの使用	脆弱性対応 アサインルールまたは修復タスクルールでホストタグを使用する場合は、ルールを作成する前に Rapid7 資産リスト統合を実行します。
既存のデータレコードの重複排除	[データウェアハウス] 統合タイプから **[InsightVM]** タイプに移行するときに、既存のデータウェアハウスレコードを重複排除できます。詳細については、「Rapid7 脆弱性統合データウェアハウスレコードの重複排除」を参照してください。

手順

1. Rapid7 脆弱性統合 アプリケーションをインストールするインスタンスにログインします。
2. ServiceNow Storeに移動してログインします。
3. ServiceNow Storeで、Rapid7 脆弱性統合 アプリケーションを検索します。

   注:
   ServiceNow Storeでは、アプリケーションの名前は Rapid7 Integration for Security Operations です。このアプリケーションにはサブスクリプションが必要です。

4. アプリケーションタイルをクリックします。
   インストールしているアプリケーションに関する詳細情報が表示されます。

   注:
   該当する場合は、[他の要件] および [依存関係] セクションを読むことを検討してください。

5. [アプリを要求] をクリックし、Now Support ログイン認証情報を入力します。
6. [取得] をクリックします。
7. [インスタンス名] と [インスタンスの理由] を入力し、[インスタンスを検証] をクリックします。
8. [要求] をクリックします。
   詳細なインストール手順が記載されたメールが届きます。
9. Now Platformインスタンスで、 システムアプリケーション > すべてのアプリケーション > **All** (すべて).
10. アプリケーションを見つけて選択し、[インストール] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[インストール] ダイアログに依存関係のステータスが表示されます。依存関係アプリケーションが必要な場合は、必要なアプリケーションが表示されます。ダイアログのプロンプトに従って、Rapid7 脆弱性統合 アプリケーションをインスタンスにインストールします。

注:
これで、脆弱性アドミニストレーターがアプリケーションの構成を完了することができます。「Rapid7 脆弱性統合 の構成」を参照してください。

Rapid7 脆弱性統合 の構成

アプリケーションをインストールして Now Platform® でアクティブ化したら、Rapid7 脆弱性統合を構成します。

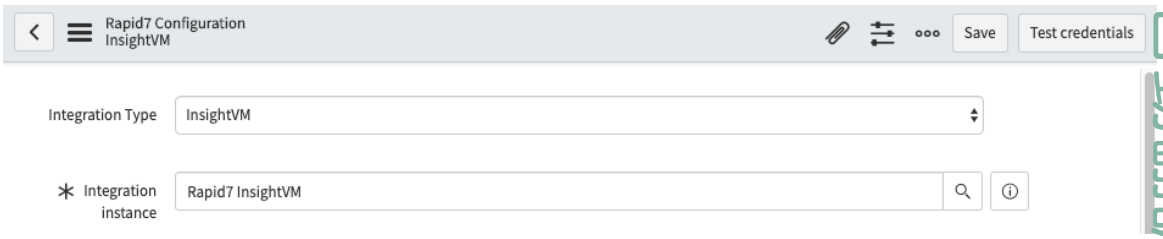
始める前に

必要なロール：アドミニストレーター [admin] がアプリをダウンロードしてインストールします。sn_vul.vulnerability_admin または sn_vul.admin は、構成を監視し、期待される結果を検証します。

手順

1. アプリケーションをアクティブ化 (インストール) したら、次に移動します: **Rapid7 Vulnerability Integration** > アドミニストレーション > 構成.
2. リストから [Integration Type (統合タイプ)] を選択します。

統合タイプリスト



3. 統合インスタンスを選択します。
デフォルトでは、デフォルトの Rapid7 InsightVM 統合インスタンスが選択されています。それが必要な統合タイプである場合は、次の手順に従います。Rapid7 データウェアハウス統合タイプを構成する場合は、手順 4 に進みます。

   a. 表示されたフォームで [統合セットアップ] タブを選択し、フィールドに入力します。

InsightVM 統合タイプの [統合セットアップ] タブ

フィールド	説明
InsightVM 地域	Rapid7 サイトから取得したサーバー URL
API キー	Rapid7 インサイトアカウントから取得した API キー
検証ステータス	読み取り専用：認証情報検証プロセスのステータス

   b. [認証情報をテスト] をクリックして、構成が正常であることを確認します。
   構成中にエラーメッセージが表示される場合は、データを再入力します。

   c. テストが成功したら、[保存] をクリックします。

   d. [構成のインポート] タブをクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

表示されるフォームのフィールドに入力します。

InsightVM の [構成のインポート] タブ

フィールド	説明
最小 CVSS スコア	インポート中に脆弱性一致アイテムをフィルタリングするために使用される脆弱性一致アイテムの最小 CVSS スコア。
最大 CVSS スコア	インポート中に脆弱性一致アイテムをフィルタリングするために使用される脆弱性一致アイテムの最大 CVSS スコア
サイトフィルター	[サイト] リストから選択した Rapid7 InsightVM サイトにデータを制限します。「Rapid7 サイト別のフィルタリング」を参照してください。複数のサイトを選択できます。デフォルト (空) では、すべてのサイトが取り込まれます。[サイト] リストに事前入力するには、このフィールドを設定する前に Rapid7 サイト統合 - API を実行します。 サイトフィルタリングの使用方法については、「Rapid7 サイト別のフィルタリング」を参照してください。
CVE エントリーの自動作成	CVE エントリーを作成するためのシステムプロパティは、デフォルトではアクティブ (true) です。CVE ID が存在しない場合、Rapid7 ナレッジの取り込みにより CVE プレースホルダーが自動的に作成されます。 この機能を非アクティブにするには、[システムのプロパティ] リストから [sn_vul_r7.create_cve_for_vulnerabilities] プロパティを非アクティブ化します。
経過時間による解決済みを再オープン	選択すると、解決されたもののクローズされていない日数が [解決後に再オープン] フィールドに表示される値と一致すると、脆弱性一致アイテムが自動的に再オープンされます。

e. [保存] をクリックします。

Rapid7 InsightVM 統合タイプの複数展開の場合：

f. [統合インスタンス] フィールドで、[ルックアップ] リストの🔍を開いて既存の統合インスタンスを選択するか、ポップアップメニューで [新規] をクリックします。

g. [新規] の場合は、統合インスタンスの [名前] を入力し、[送信] クリックします。
統合タイプが [Rapid7 構成] フォームに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
デフォルトを除く任意の統合インスタンスを削除できます。インスタンスを削除すると、以下が削除されます (VI を除く)。

- 統合
- インスタンスパラメーター
- 統合実行
- 統合プロセス
- VI の [インスタンス] 列が空とマークされる

h. [認証情報をテスト] をクリックして、構成が正常であることを確認します。

i. テストが成功したら、[保存] をクリックします。

4. [統合タイプ] フィールドで、リストを展開し、[データウェアハウス] をクリックします。

a. [統合セットアップ] タブを選択します。

表示されるフォームのフィールドに入力します。

データウェアハウス統合タイプの [統合セットアップ] タブ

フィールド	説明
JDBC 認証情報名	データウェアハウス認証情報の名前
ユーザー名	Rapid7 データウェアハウスのユーザー名
パスワード	Rapid7 データウェアハウスのパスワード
検証ステータス	読み取り専用：認証情報検証プロセスのステータス
検証の詳細	読み取り専用：データウェアハウスのみ。[認証情報をテスト] を 1 回以上クリックした後に、検証チェックに関する追加情報を表示します。これは、セットアップのデバッグに役立ちます (たとえば、MID サーバーが正しく構成されていない場合や、認証情報が間違っている場合など)。
データベースサーバー DNS/IP	データウェアハウスの DNS または IP アドレス
データベースポート	データウェアハウス統合に使用するポート

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
データベース名	データウェアハウスの名前
データ遅延オフセット (日数)	データ遅延オフセットは、Rapid7 Nexpose スキャナーのリアルタイムデータとデータウェアハウスのデータ間の遅延の要因となります。
MID サーバー	使用する MID サーバー。スタンドアロン MID サーバーのみがサポートされています。クラスター化された MID サーバーはサポートされていません。
MID サーバータイムアウト (分)	統合実行がタイムアウトになるまで MID サーバーの応答を待機する時間 (分)。

b. [認証情報をテスト] をクリックして、構成が正常であることを確認します。

c. テストが成功したら、[保存] をクリックします。

d. [構成のインポート] タブをクリックします。

表示されるフォームのフィールドに入力します。

データウェアハウスの [構成のインポート] タブ

フィールド	説明
v12.0 より前：[CVE エントリーを作成 (Create CVE entry)] チェックボックス	オンにすると、まだ存在しない CVE のプレースホルダーが NVD レコードとして作成され、Rapid7 のサードパーティエントリーで参照されます。オフにすると、これらの CVE は無視されます。
最小 CVSS スコア	インポート中に脆弱性一致アイテムをフィルタリングするために使用される脆弱性一致アイテムの最小 CVSS スコア。
最大 CVSS スコア	インポート中に脆弱性一致アイテムをフィルタリングするために使用される脆弱性一致アイテムの最大 CVSS スコア
サイトフィルター	インポートされたサイト統合データを選択したサイトに制限します。複数選択できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: デフォルト設定ではすべてのサイトからデータをインポートするため、すべてのサイトが必要な場合はフィルターを使用する必要はありません。これを行うと、要求の処理速度が低下します。
経過時間による解決済みを再オープン	選択すると、解決されたもののクローズされていない日数が [解決後に再オープン] フィールドに表示される値と一致すると、脆弱性一致アイテムが自動的に再オープンされます。

5. [保存] をクリックします。
6. オプション: Rapid7 脆弱性統合 - API および Rapid7 脆弱性一致アイテム統合 - API 統合レコードに開始日を設定して、Rapid7 スキャンからの初期インポート中に履歴データを取得する場合は、次の手順を実行します。
このデータは、「脆弱性対応 での古い検出のクローズ」で役立つ可能性があります。

   a. 次のように移動する。 **Rapid7 Vulnerability Integration** > アドミニストレーション > 統合.
   [Rapid7 統合] リストが表示されます。

   b. いずれかの統合レコードをクリックして開きます。

   (Optional) フォームの上部近くにある [こちらから] リンクをクリックしてレコードを編集します。

   Rapid7 統合の [次以降にインポート] 日付フィールドは、Rapid7 脆弱性統合 - API および Rapid7 脆弱性一致アイテム統合 - API を除き、デフォルトでは空白です。これらの統合の場合、これらのフィールドは 1998-12-31 または 1999-01-01 に設定されます。

   Rapid7 スキャンからの初期インポート中に履歴データを取得するには、該当の統合レコードに開始日を設定します。このプロセスは、次の例外を除いてすべての Rapid7 統合に対して機能します。

   - Rapid7 エクスプロイトとマルウェアキットの統合では、デルタ更新を実行せず、[次以降にインポート] フィールドを使用しないため、このフィールドは表示されません。
   - Rapid7 資産リスト統合では、すべてのデータの取得が目的であるため、フィールドは無視されます。
   - [古い脆弱性一致アイテムの自動クローズ (Auto-Close Stale Vulnerable Items)] モジュールが有効で、[次以降にインポート] フィールドが空白のままになっている場合の Rapid7 InsightVM 包括的脆弱性一致アイテム統合 - API の初回実行時。

     自動クローズ機能を有効にする場合は、Rapid7 包括的脆弱性一致アイテム統合または Rapid7 包括的脆弱性一致アイテム統合 - API が正常に実行される必要があります。これらの統合はデフォルトで無効になっています。

     Rapid7 InsightVM 包括的脆弱性一致アイテム統合 - API を有効にしている場合、[統合設定] ページで [次以降にインポート] フィールドを空白のままにすると、[古い脆弱性一致アイテムの自動クローズ (Auto-Close Stale Vulnerable Items)] フォームの [日前] フィールドの値も最初の統合実行の [次以降にインポート] の日付に使用されます。[古い脆弱性一致アイテムの自動クローズ (Auto-Close Stale Vulnerable Items)] のデフォルト値は (90 日) です。

     たとえば、[古い脆弱性一致アイテムの自動クローズ (Auto-Close Stale Vulnerable Items)] フォームの [日前] フィールドの値が 90 で、Rapid7 包括的脆弱性一致アイテム統合 - API

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

構成ページの [次以降にインポート] フィールドが空白の場合、最初の統合実行で過去 90 日のデータがインポートされます。

[次以降にインポート] フィールドと [日前] フィールド間のこの関係は、最初の統合実行のみに適用されます。その後、[古い脆弱性一致アイテムの自動クローズ (Auto-Close Stale Vulnerable Items)] フォームの [日前] フィールドを変更しても、Rapid7 包括的脆弱性一致アイテム統合 - API 構成ページの [次以降にインポート] フィールドには影響しません。フィールドは、後続の統合実行でデルタ情報のみがインポートされるように、最初の実行の開始時間に変更されます

[次以降にインポート] フィールドは編集可能で、統合ごとに必要な値を入力できます。

7. 次のように移動する。 **All** (すべて) > **sn_sec_int_impl.list** > **Rapid7 InsightVM**.

   a. **import_startime_buffer_comprehense** 統合インスタンスパラメーターは、[次以降にインポート] フィールドに指定された時刻までの 24 時間をバッファー時間として設定します。これにより、このバッファー時間からスキャンされる資産が **Rapid7 Comprehensive Vulnerable Item Integration - API** の統合実行中にフェッチされるようになります。
   このバッファー時間は要件に応じて変更できます。

   b. オプション: **close_stale_detections** パラメーターを *true* に設定して、**Rapid7 Comprehensive Vulnerable Item Integration - API** を介して Rapid7 API からスキャンおよび取得された資産について、Rapid7 API を経由しなくなった古い検出をクローズします。

Rapid7 脆弱性統合 のセットアップ、インストール、構成の手順が正常に完了しました。これで、インポートされたデータをレビューおよび検証する準備ができました。

次のタスク
Rapid7 および Qualys スキャナーは、脆弱性対応 アプリケーションではデフォルトで無効になっています。これらのアプリケーションをソースとする脆弱性一致アイテムまたは修復タスクから再スキャンを実行しようとすると、[再スキャン] ボタンは使用できません。

これらのスキャナーをアクティブにするには、sn_vul.vulnerability_admin ロールのユーザーとして、次の操作を実行します。

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性スキャン > スキャナー.
2. アクティブ化するスキャナー製品を見つけ、レコードをクリックして開きます。
3. [アクティブ] チェックボックスをオンにします。
4. [更新] をクリックします。

   アクティブ化した製品は、次のインポート後に脆弱性一致アイテムおよび修復タスクレコードの [ソース] フィールドに表示され、[再スキャン] は UI アクションとして使用できます。

環境でドメインセパレーションインポートが必要な場合は、「統合のためのドメインセパレーションインポートの作成」を参照してください。

インポート前にルックアップルールを作成または調整するには、「脆弱性対応 CI ルックアップルールの作成」を参照してください。

Rapid7 サイト別のフィルタリング

Rapid7 InsightVM 統合タイプおよび Rapid7 Nexpose データウェアハウス統合タイプをサイト別にフィルタリングします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

注:
サイトフィルタリングを使用すると、パフォーマンスが影響を受ける可能性があります。サイトフィルタリングを使用する前のパフォーマンスおよびその他の考慮事項については、KB0789221 を参照してください。

このタスクについて

手順

1. 次のように移動する。 **All** (すべて) > **Rapid7 Vulnerability Integration** > 構成.
2. 統合インスタンスを選択します。
3. [構成のインポート] タブをクリックします。

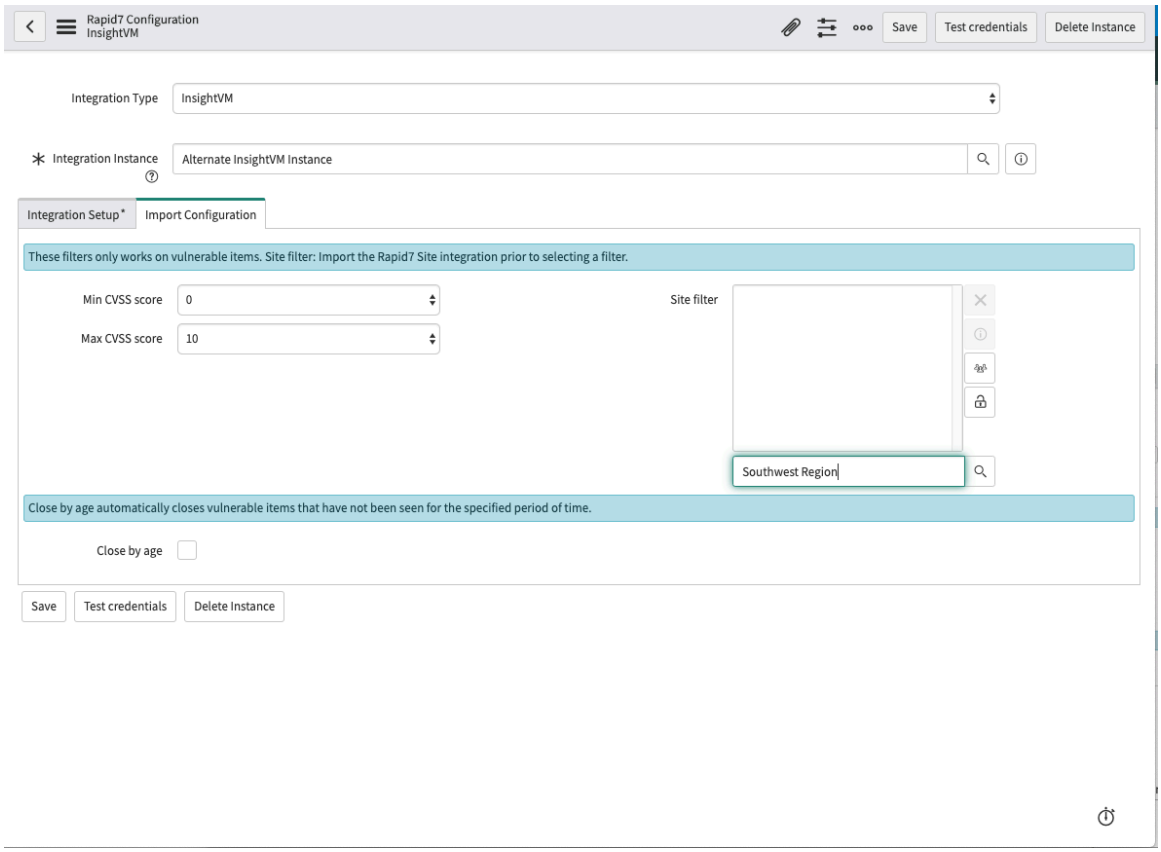
   注:
   すべてのサイトが必要な場合は、[サイトフィルター] フィールドを空のままにします。サイトフィルターがないと、すべてのサイトが追加されます。

   サイトは統合インスタンス固有です。サイトフィルタリングのルックアップリストには、Rapid7 InsightVM と Rapid7 Nexpose の両方のデータウェアハウス統合インスタンスサイトが表示されます。選択したサイトが選択した統合インスタンスと一致していることを確認してください。たとえば、誤ってデータウェアハウスサイトを選択した場合、そのサイトは Rapid7 InsightVM によるサイトフィルタリングでは機能しません。

4. ルックアップリストをクリックすると、現在の統合インスタンスのサイトレコードが表示されます。
5. サイトフィルターに追加するサイトをリストから追加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



6. 選択を繰り返してサイトを追加します。
7. [保存] をクリックします。
   これらのサイトは、次のインポート中にサイト別にフィルタリングするために使用されます。サイトデータへのプリフィックス SITE の追加については、「Rapid7 InsightVM サイトタグへの SITE の追加」を参照してください。

Rapid7 InsightVM サイトタグへの SITE の追加

Rapid7 InsightVM サイトタグにプリフィックス SITE を追加して、タグのリスト内でハイライト表示します。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

> **注:**
> 必要に応じて、Rapid7 Integration for Security Operations にスコープを切り替えます。

手順

1. 左側のナビゲーションボックスに「*sys_properties.list*」と入力します。
2. [名前] で、*sn_vul_r7.prefix_site_to_rapid7_tags* を検索します。
3. [*sn_vul_r7.prefix_site_to_rapid7_tags*] を開きます。
4. [値] を **[True]** に変更します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

5. [更新] をクリックします。
   Rapid7 InsightVM の次のインポート中に、新規および既存のサイトタグにプリフィックスが付けられます。

Rapid7 脆弱性統合データウェアハウスレコードの重複排除

[データウェアハウス] 統合タイプから **[InsightVM]** 統合タイプに移行する場合、既存のデータウェアハウスの脆弱性一致アイテムが Rapid7 InsightVM データと同じソースデータに属している限り、重複を排除できます。

始める前に

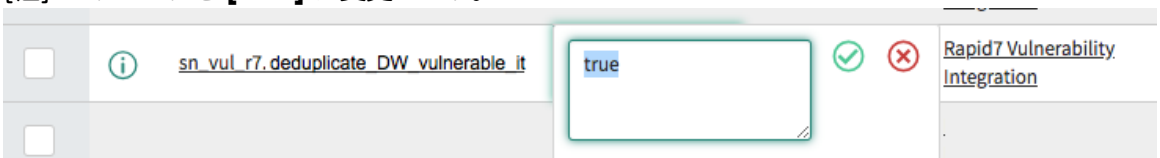
必要なロール：sn_vul_r7.admin、sn_vul.vulnerability_admin または sn_vul.admin (非推奨)
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

このタスクについて

この重複排除は、Rapid7 Nexpose データウェアハウスから Rapid7 InsightVM 脆弱性一致アイテム統合への移行時にのみ機能します。

手順

1. 次のように移動する。 **All** (すべて) > ラピッド **7** > 統合.
2. すべての Rapid7 Nexpose データウェアハウス統合の [アクティブ] 列の設定を **[False]** に設定し、統合を無効にします。
3. 左側のナビゲーションパネルで「sys_properties.list」と入力します。
4. [名前]：sn_vul_r7.deduplicate_DW_vulnerable_item を検索します。
5. [値] フィールドを **[True]** に変更します。



6. 緑色のチェックマークアイコン をクリックします。
   次の Rapid7 InsightVM 脆弱性一致アイテム統合インポート中に、既存のデータウェアハウスレコードと一致すると、重複する脆弱性一致アイテムは作成されません。

Rapid7 脆弱性統合実行状況チャート

Rapid7 Nexpose センサーがデータを収集して Rapid7 Nexpose または Rapid7 InsightVM 製品に自動的に送信すると、情報が継続的に分析され、関連付けられます。

脆弱性対応 のワークスペースのデータの可視化

脆弱性対応 ワークスペースには、修復の進捗状況を監視するのに役立つデータの可視化が含まれています。脆弱性データの変更に応じて更新される動的なデータ表示で組織にとって重要なアクティブな脆弱性の数と重大度を表示することで、組織に対する脅威のレベルを判断できます。利用可能な動的なデータ表示方法の詳細については、「脆弱性対応 ワークスペース」、「Vulnerability Manager ワークスペース」および「IT 修復ワークスペース の探索」を参照してください。

Rapid7 脆弱性統合は 脆弱性対応 と簡単に統合して、脆弱性を CI およびビジネスサービスにマッピングして、悪意がある可能性のある脅威の影響度と優先度を判別します。Rapid7 脆弱性統合統実行状況モジュールは、Rapid7 脆弱性統合実行のステータスをグラフィカルに表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このデータを従来のビューで表示するには、次に移動します: **All** (すべて) > すべての **Rapid7** 脆弱性統合 > 統合実行ステータス.

脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で使用可能です。

> **注:**
> Tokyo を使用している場合は、Next Experience UI でダッシュボードを表示できますが、一部の機能が失われます。

脆弱性対応 の前のバージョン

チャートで、任意の部分 (棒、円、データポイントなど) をポイントして、その部分に固有の一般的なデータを表示できます。レポートの任意の部分をクリックすると、詳細な情報を提供するリストが開きます。

データ量やこのデータの処理にかかる時間など、複数の要因によって統合実行のパフォーマンスが影響を受ける可能性があります。次の 2 つの新しいグラフでパフォーマンスメトリクスを比較します。

- Rapid7 脆弱性一致アイテムの取り込みパフォーマンスメトリクス：アサインルール、グループルール、リスクルール、キュー待機時間、キューの処理時間、および過去 30 日間の脆弱性一致アイテムのその他の統計に関する日次パフォーマンスメトリクスを比較して、パフォーマンスの逸脱の原因を特定します。
- Rapid7 脆弱性一致アイテムの取り込みパフォーマンススループット：Rapid7 脆弱性一致アイテム統合 - API について、脆弱性一致アイテム取り込みスループットを毎日比較します。スループットは 1 時間あたりのアイテム数で測定されます。

> **注:**
> Rapid7 では、これらのグラフは Insight VM 統合でのみサポートされています。

Rapid7 統合実行状況

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Rapid7 脆弱性統合実行状況のサンプルチャート

- [インポートされたアイテム] 列の値は、統合実行から作成される脆弱性一致アイテムの合計数を表します。
- [新規アイテム] 列には、統合実行から作成される脆弱性一致アイテムの数が表示されます。
- [重複アイテム] 列には入力されなくなりました。この列を表示から削除することもできます。
- [更新されたアイテム] 列には、統合実行中の脆弱性一致アイテムの更新回数が表示されます。この値は、更新される一意の脆弱性一致アイテムの数ではありません。たとえば、統合実行中に脆弱性一致アイテムが 2 回更新された場合、2 回とカウントされ、更新済みアイテムが 2 つと表示されます。
- [未変更のアイテム] 列には、既にデータベースに存在し、統合実行中に検出されたものの、関連するフィールド値が変更されていないために更新されなかった脆弱性一致アイテムが表示されます。

注:
[新規 **CI]**、[既存の **CI]**、[新規アイテム]、[更新されたアイテム] の 4 つの値はすべて、**[Rapid7** 統合実行] リストから除外されます。

Rapid7 脆弱性統合実行状況チャートレポート

名前	説明
過去 30 日間の Rapid7 結果	各統合で完了した統合実行の数。成功した実行と失敗した実行の両方が表示されます。視覚的な棒グラフで実行されます。
過去 30 日間の Rapid7 新規 VI	過去 30 日間にインポートされた新規脆弱性一致アイテムの数。整数として表示されます。
過去 30 日間の Rapid7 更新済み VI	過去 30 日間にインポートされた更新済み脆弱性一致アイテムの数。整数として表示されます。
過去 30 日間の Rapid7 重複	過去 30 日間にインポートされた重複脆弱性一致アイテムの数。整数として表示されます。
Rapid7 統合実行	リストの統合実行レコード

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Rapid7 脆弱性統合実行状況チャートレポート (続く)

名前	説明
	注: V16.1：この統合の検出を検証するには、検出または検出結果を *sn_vul_detection* テーブルの ServiceNow 検出データと比較します。 統合の進行中は、検出数または検出結果数が変更される可能性があります。このレポートでは、統合実行の完了後に、インスタンスの [現在までの数] 列に検出数が表示されます。
過去 30 日の Rapid7 脆弱性一致アイテムの取り込みパフォーマンスメトリクス	過去 30 日間の脆弱性一致アイテムの日次パフォーマンスメトリクス
過去 30 日の Rapid7 脆弱性一致アイテムの取り込みパフォーマンススループット	過去 30 日に測定された Rapid7 脆弱性一致アイテム統合 - API の脆弱性一致アイテムの日次取り込みスループット

Rapid7 脆弱性統合インポート実行状況ダッシュボードの表示

Rapid7 脆弱性インポート実行状況ダッシュボードを使用して、統合実行の成功を確認し、問題を特定して、修復の決定を通知します。

始める前に

必要なロール：sn_vuln.admin

このタスクについて

この手順は、以下を前提としています。

- 脆弱性対応 と Rapid7 脆弱性統合をインストールして構成している。
- Rapid7 脆弱性統合インポートがスケジュールおよび実行されている。
- Rapid7 統合実行状況チャートが使用中である。

統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、脆弱性対応 のバージョン 19.0 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

手順

1. 次のように移動する。 **Rapid7** > 統合実行ステータス.

   脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で使用可能です。

   注:
   Tokyo を使用している場合は、Next Experience UI でダッシュボードを表示できますが、一部の機能が失われます。

2. Rapid7統合実行状況チャートを使用していない場合は、次に移動します: **Rapid7** > 統合.
   a. 統合を選択します。
   b. [脆弱性統合実行] 関連リストをクリックします。
3. すべてのインポートが成功したことを確認します。

   Trouble?

   実行が失敗した場合の一般的な原因：

   ○ ネットワーク中断

   ○ データ転送が少し低下することによる、変換中のデータの破損
   これらのすべての条件について、[今すぐ実行] をクリックして統合を再実行します。

Rapid7 脆弱性統合の再スキャンの開始

Rapid7 プラットフォームで再スキャンを開始し、スケジュールされたスキャンサイクル間で脆弱性一致アイテムが修正されたことを確認します。

始める前に

注:
Rapid7 データウェアハウス脆弱性一致アイテムの再スキャンはサポートされていません。

脆弱性対応ワークスペースから再スキャンを開始できます。詳細については、「でのレコードと修復タスクの再スキャン Vulnerability Manager ワークスペース」と「IT 修復ワークスペースでの脆弱性一致アイテムと修復タスクの再スキャン」を参照してください。

必要なロール：sn_vul.write_all または sn_vul.write_assigned

このタスクについて
クラシック環境での再スキャン方法については、次のセクションを参照してください。

再スキャンがサポートされています。Now Platform® インスタンスの Rapid7 InsightVM 統合からインポートしたの脆弱性一致アイテムの再スキャンをオンデマンドで開始できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

> **注:**
> Rapid7 スキャナーは、脆弱性対応 アプリケーションではデフォルトで無効になっています。Rapid7 アプリケーションをソースとする脆弱性一致アイテムまたは修復タスクから再スキャンを実行しようとすると、[再スキャン] ボタンは使用できません。

修復オーナー、IT スペシャリスト、脆弱性アナリスト、または脆弱性マネージャーは、スケジュール設定済みのフルスキャンに関連するオーバーヘッドとボリュームを削減するために、環境内の資産 (構成アイテム) の特定の脆弱性についてターゲットの再スキャンをオンデマンドで開始できます。脆弱性一致アイテム (VI)、修復タスク (RT)、サードパーティエントリー (TPE)、または Now Platform　インスタンスから検出されたアイテムレコードから再スキャンを開始できます。

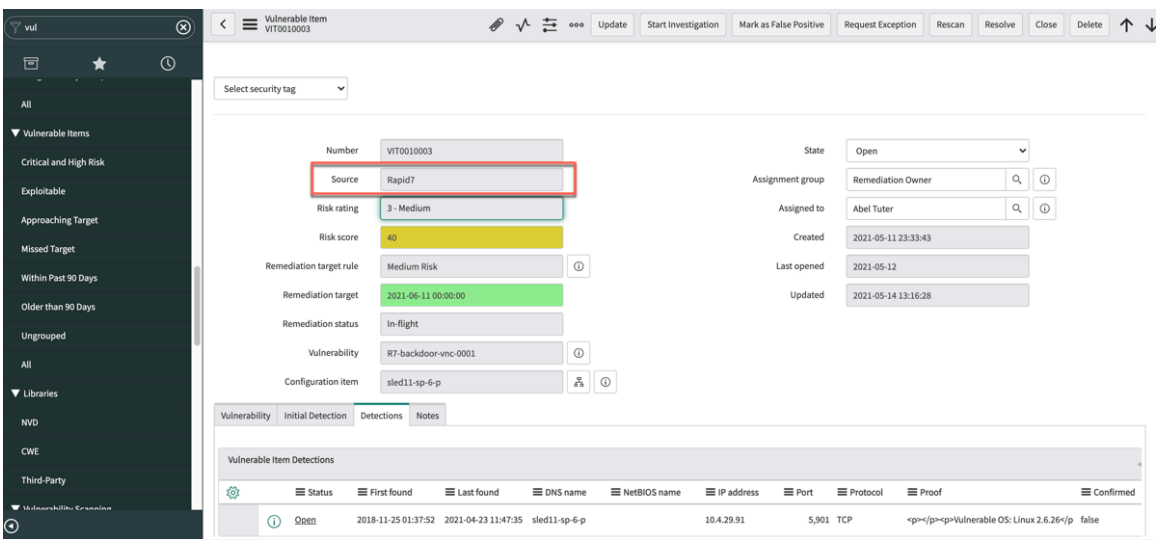
再スキャンにより、修復アクティビティ、パッチ、およびその他のアクションによって構成アイテム (CI) の特定の脆弱性が正常に修正されたことを確認できます。

たとえば、3 週間に 1 回環境全体をスキャンするとします。最新のフルスキャンは 1 週間前に完了しましたが、重大な脆弱性を修正するために昨日パッチを適用しました。この脆弱性の特性を考えると、この脆弱性が修正されたことを確認するのに次のスケジュール済みスキャンまで 2 週間待つことはできません。以前のスキャン中に検出された重大な脆弱性がパッチによって正常に修正されたことを確認するために、Now Platform for Rapid7 脆弱性一致アイテムからターゲット再スキャンを開始できます。Rapid7 InsightVM 脆弱性と脆弱性一致アイテム統合の次回のインポート予定で、脆弱性一致アイテムの更新された結果を表示できます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム.
2. 再スキャンをトリガーする脆弱性一致アイテムレコードを見つけて開きます。

> **注:**
> ソースが Rapid7 の VI の再スキャンのみを開始できます。VI リストビューの [ソース] 列、または個々のレコードの [ソース] フィールドに Rapid7 が表示されていることを確認します。条件ビルダーを使用して、VI をソース別にグループ化できます。または、[ソース] 列が VI リストビューに表示されていない場合は、リストの左上にある歯車アイコンをクリックし、[ソース] を [利用可能] から [選択済み] に移動します。
>
> 再スキャンを開始するときは、複数のソースから 1 つのソース ID のスキャンを同時にトリガーしないようにしてください。最新のスキャン要求がエラーになります。
>
> たとえば、VI レコードから VI の再スキャンを開始し、同じ VI を含む修復タスクレコードから別の再スキャンも要求すると、2 番目の要求が失敗する可能性があります。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. または、 脆弱性対応 > 修復タスク または 脆弱性対応 > ライブラリー > サードパーティ は、それぞれ再スキャンに使用する修復タスクまたはサードパーティのエントリーレコード用です。

   選択内容に応じて、次のレコードで [再スキャン] ボタンを使用できます。

   - 単一の VI レコードでは、VI のソースが Rapid7 製品で、[クローズ済み] 以外のステータスである必要があります。複数の VI レコードの場合、リストビューから選択するすべての VI のソースが Rapid7 製品で、[クローズ済み] 以外のステータスである必要があります。
   - 修復タスクレコードでは、修復タスクは [クローズ済み] を除くあらゆるステータスをとることが可能ですが、関連する VI はすべてソースが Rapid7 製品である必要があります。
   - サードパーティエントリー (TPE) レコードには、[クローズ済み] 以外のステータスでソースが Rapid7 製品の関連する VI レコードが少なくとも 1 つ必要です。
   - 検出されたアイテムレコードでは、VI のソースが Rapid7 製品で、[クローズ済み] 以外のステータスである必要があります。

4. レコードの右上にある [再スキャン] をクリックします。
   リストビューの場合は、リストから再スキャンする VI を選択し、[選択した行のアクション **(Action on selected rows)]** リストから、[再スキャン] を選択します。

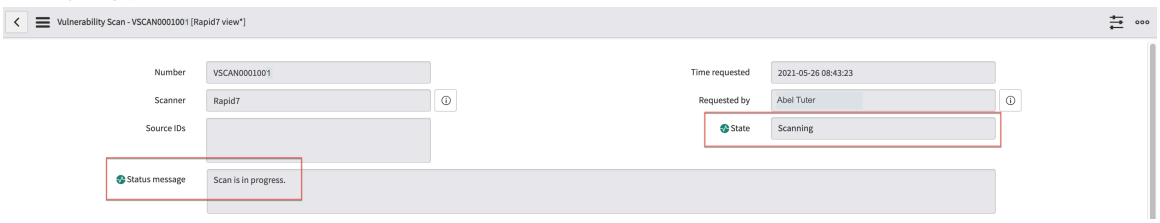
5. 表示されるポップアップで、再スキャンを確認します。
   スキャンが処理されていることを示すメッセージが表示されます ([キューに格納])。メッセージで [詳細を表示] リンクをクリックして、再スキャンのステータスを確認し、レコードから開始された他の再スキャンを表示します。すべての再スキャンのステータスは、再スキャンの開始に使用する VI、修復タスク、TPE、および検出されたアイテムレコードの [スキャン] 関連リストでいつでも確認できます。

   スキャンの進行中は、[ステータス (State)] フィールドが [スキャン] に変わり、[ステータスメッセージ] フィールドに [スキャンが進行中です] と表示されます。

   > **注:**
   > 各再スキャンは、スキャンごとに 500 資産をサポートします。要求に 500 を超える資産がある場合は、さらに子スキャンが要求されます。

   Now Platform® インスタンスは、正常に完了するか設定された追跡期間がタイムアウトするまで、再スキャンステータスを追跡します。

   処理中の再スキャン

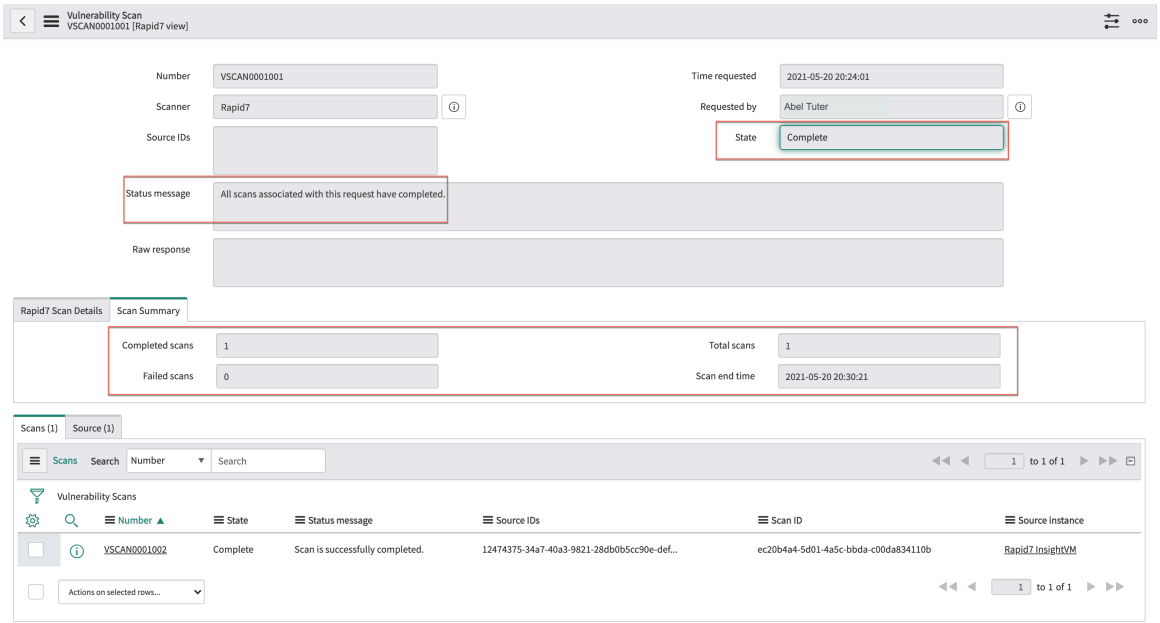
   

   タイムアウトしてもスキャンは停止しません。タイムアウトは、実際の再スキャンが停止したときではなく、Now Platform® が再スキャンステータスの追跡を停止したときです。[クローズ済み]/[修正済み] に移行した、または移行する予定のすべての VI は、Rapid7 統合の次のスケジュール済みインポートとともにインポートされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

再スキャン完了



または、特定の資産の特定の脆弱性についてオンデマンドで再スキャンを開始できます。スキャンを開始した更新された VI、修復タスク、TPE、および検出されたアイテムレコードでスキャンが完了すると、これらのスキャンの結果を表示できます。

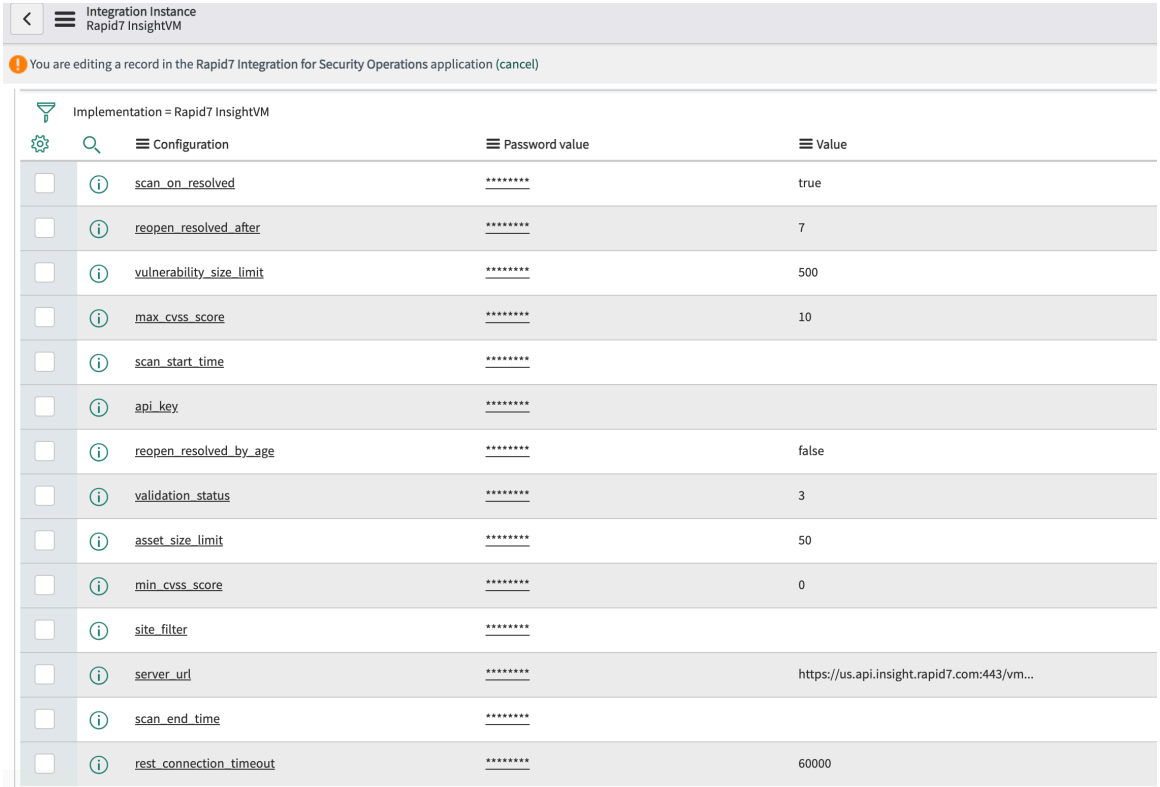
脆弱性スキャンレコードの [ステータス (State)] フィールドの値は Rapid7 からインポートされます。スキャンが正常に終了すると、ステータスは [完了] に設定されます。スキャンが正常に完了しなかった場合は、エラー値が表示されます。

自動スキャンとスケジュール設定済みスキャン

脆弱性マネージャーまたはアナリストは、VI および RT の再スキャンをいつ開始するかを指定してスケジュール設定できます。解決するように設定された VI および修復タスクの自動スキャンを有効にすることもできます。

6. 統合インスタンスの統合パラメーターを変更するには、次に移動します: **Rapid7 Vulnerability Integration** > アドミニストレーション > 構成.
7. [Rapid7 構成] レコードで [統合タイプ] リストから **[Rapid7 InsightVM]** を選択します。
8. [統合] フィールドの右側にある情報アイコンをクリックし、続いて [レコードを開く] をクリックします。
9. 統合インスタンス Rapid7 InsightVM レコードで、スキャンをスケジュールするためのパラメーターを見つけ、必要に応じて編集します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



scan_on_resolved は、脆弱性が解決されたときにスキャンを開始するかどうかを示します。デフォルトでは **false** (無効) になっています。

このパラメーターを true に設定すると、VI または RT が [解決済み] に設定されるたびに、それぞれの VI と修復タスクを再スキャンするワークフローが自動的にトリガーされます。

scan_start_time

再スキャンを可能にする開始時間に対して、スキャン開始時間を **HH:mm** (24 時間形式、UTC タイムゾーン) で設定します。

デフォルト値は 00:00 です。

scan_end_time

スキャンを可能にする終了時間に対して、スキャン終了時間を **HH:mm** (24 時間形式、UTC タイムゾーン) で設定します。

デフォルト値は 23:59 です。

スケジュールされた時間内にスキャンが開始されると、すぐに開始されます。スキャンが時間外に開始された場合は、次のスケジュール設定済み時間のキューに入れられます。

たとえば、*scan_start_time* パラメーターに開始時刻の 00:00 を入力し、*scan_end_time* に同じ日の朝の 10:00 AM を入力すると、深夜 0 時から午前 10 時までの時間帯以外にスケジュール設定されたスキャンまたは手動で開始されたスキャンがキューに入り、翌日の時間帯の開始時間 00:00 に起動されます。

同じ例で、午前 11:00 に再スキャンを手動で開始した場合、利用可能な構成済みスキャン時間外であるため、再スキャンはすぐには開始されません。スキャン要求は、翌日の時間帯の開始 (この例では 00:00) までキューに入ったままになります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Rapid7 InsightVM インポートの追加のフィルターパラメーターの設定

セキュリティオペレーションの Rapid7 統合 を使用してスケジュール設定済みクエリのフィルタリングパラメーターをカスタマイズすると、Rapid7 InsightVM 製品でインポートする脆弱性データをさらに絞り込むことができます。

始める前に

ユースケース：脆弱性マネージャーまたはアナリストは、特定の脆弱性の詳細のみを確認できるように、クエリからデータをフィルタリングできます。たとえば、[重要] および [重大] であるインポートされた脆弱性のみを表示できます。

このデータを収集するには、Rapid7 パラメーターを追加して、必要な特定の脆弱性の詳細をインポートします。

v13.4 以降のこの機能を使用すると、API コールを追加したり追加のコーディングをしたりすることなく、Now Platform の Rapid7 InsightVM パラメーターを使用して HTTP 要求情報をカスタマイズできます。次の Rapid7 InsightVM 統合は、要求本文に JSON コンテンツを追加することによってフィルタリングをサポートしています。

- Rapid7 InsightVM 脆弱性一致アイテム統合 API
- Rapid7 InsightVM 脆弱性統合 API
- Rapid7 InsightVM

この機能の JSON 文字列の使用方法を理解している必要があります。

必要なロール：sn_vul.vulnerability_admin

手順

1. フィルタリングに使用する Rapid7 開発者サイトで、Rapid7 InsightVM 製品でサポートされているパラメーターを見つけます。

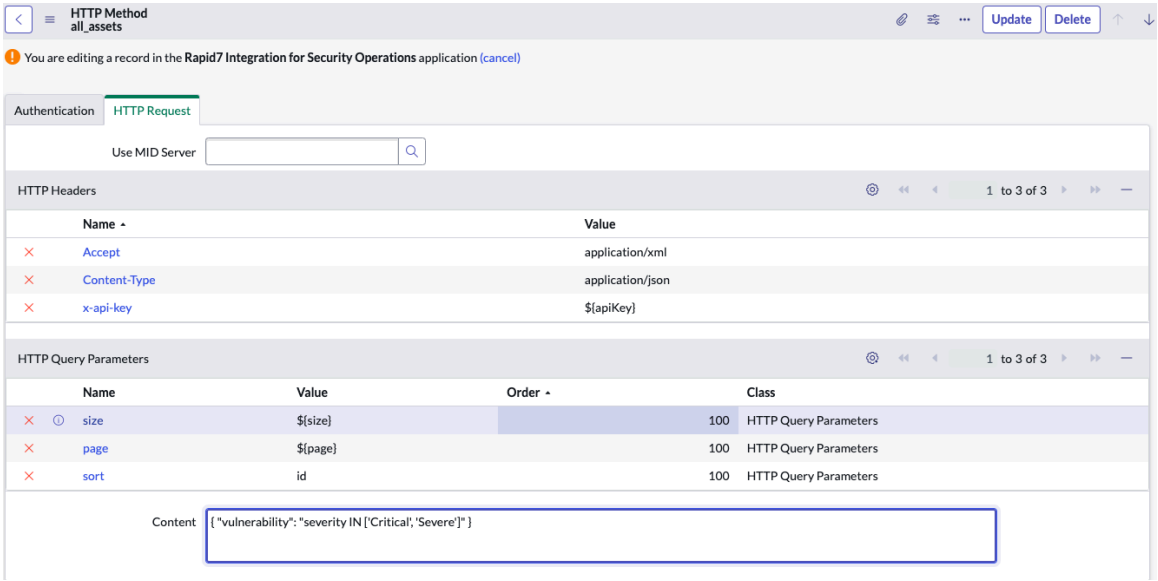
   Rapid7 ドキュメントを参照して、要求本文のパラメーターを作成できます。Rapid7 InsightVM 製品から入力するパラメーターと値は、統合インスタンスレベルでのみサポートされます。

2. 次のように移動する。 **All** (すべて) > **Rapid7 Vulnerability Integration** > アドミニストレーション > 統合.
3. [Rapid7 統合] リストページで、レコードを開く Rapid7 InsightVM 統合のレコードをクリックします。
4. ページの右側で、REST メッセージの情報アイコン (!) をクリックし、続いて [レコードを開く] をクリックします。
5. [HTTP 要求] タブを選択した状態で、[HTTP メソッド] の [名前] 列でアイテムをクリックして HTTP クエリパラメーターを開きます。
6. [HTTP メソッド] レコードの [HTTP クエリパラメーター (HTTP Query Parameters)] の [コンテンツ] フィールドに、Rapid7 開発者サイトで見つけたパラメーター値を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の画像では、重大度の文字列が追加されていま



す。

複数のパラメーターを入力する場合は、各値を区切る方法の詳細について、Rapid7 ドキュメントを参照してください。

7. [更新] をクリックします。

Shodan Exploit Integration の概要

ServiceNow Shodan Exploit Integration アプリケーションは、Shodan 検索エンジンからインポートされたデータを使用して、悪意のある可能性があるエクスプロイトの影響度と優先度を判断します。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

Shodan Exploit Integration

Shodan 検索エンジンはエクスプロイトデータを収集し、Shodan API がそのデータベースを Now Platform で利用できるようにします。ServiceNow 脆弱性対応 アプリケーションと簡単に統合し、エクスプロイトをサードパーティ脆弱性にマッピングして、エクスプロイトデータをインスタンスに拡張します。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

スケジュール済みジョブにより、統合がリストされている順序で毎日自動的に呼び出されます。スケジュール済みジョブを手動で実行することもできます。スケジュール済みジョブでは、インスタンスを他の脆弱性管理システムと同期させることで、脆弱性修復ライフサイクルを簡素化します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

利用可能バージョン

Yokohama のリリースバージョン	リリースノート
Shodan Exploit Integration v10.6、10.7	互換性情報については、「KB0856498 脆弱性対応 互換性マトリクスおよびリリーススキーマの変更」を参照してください。

ロール

Shodan Exploit Integration タスクには、次のロールが関与します。

- sn_vul_shodan.admin：このロールを持つユーザーは、レコードの読み取り、書き込み、削除を実行できます。
- sn_vul_shodan.user：このロールを持つユーザーは、レコードの読み取りと書き込みを実行できます。
- sn_vul_shodan.read：このロールを持つユーザーは、レコードの読み取りを実行できます。

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

Shodan Exploit Integration

Shodan Exploit 統合を表示するには、次の場所に移動します **All** (すべて) > **Shodan Exploit Integration** > 統合.

ベースシステムには、次の統合が含まれています。これらの統合はデフォルトでアクティブになっています。

Shodan Exploit Integration

統合	説明
Shodan ExploitDB Integration	Shodan から ExploitDB データを取得し、サードパーティ脆弱性データを拡張します。この統合は毎日 03:15:00 に実行するように設定されます。
Shodan Metasploit Integration	Shodan から Metasploit 情報を取得し、サードパーティ脆弱性データを拡張します。この統合は毎日 01:15:00 に実行するように設定されます。

スケジュールされた統合インポートのデフォルトの開始時間を変更するには、「Shodan Exploit Integration インポート時間の設定」を参照してください。

サードパーティの脆弱性のエクスプロイトデータを表示するには、「脆弱性対応 脆弱性ライブラリの表示」を参照してください。

その他の Shodan Exploit Integration の設定を変更するには、ServiceNow および 脆弱性対応 の高度な専門知識が必要です。これについては製品ドキュメントでは扱っていません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Shodan Exploit Integration の準備

Shodan Exploit Integration を成功させるには、事前統合タスクを計画して慎重に実行する必要があります。これらのタスクを実行して、統合の準備をします。Shodan Exploit Integration では、Shodan 検索エンジンと API に精通していることを前提としています。

始める前に
Shodan Exploit Integration には API キーが必要です。このキーを取得するには、Shodan Web サイト で無料サブスクリプションに登録してください。

必要なロール：admin

このタスクについて

注:
統合を実行する前に、要件に基づいて必要な構成変更を行います。

- NIST 脆弱性データベース (NVD) データを 脆弱性対応 にインポートしていない場合は、Shodan Exploit Integration をインストールする前にインポートします。NVD データをインポートすると、共通脆弱性識別子 (CVE) データによってエクスプロイトレコードが自動的に入力されます。

  NVD データがないと、エクスプロイトレコードにプレースホルダーが作成され、次の NVD 更新まで入力されません。NVD の詳細については、「NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理」を参照してください。

- 統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

Shodan Exploit Integration for セキュリティオペレーション のインストールと構成

インスタンスで Shodan Exploit Integration を実行する前に、ServiceNow Store からダウンロードしてインストールします。このアプリケーションは別のサブスクリプションとして利用できます。

始める前に
インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

セットアップタスク	説明
脆弱性対応 アプリケーションと Shodan Exploit Integration for セキュリティオペレーション アプリケーションの有効な ServiceNow エンタイトルメントがあることを確認します。	エンタイトルメントを確認するには、次の場所に移動します: サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 ServiceNow Store から セキュリティオペレーション アプリケーションのエンタイトルメントを取得する方法の詳細については、「セキュリティオペレーション 製品またはアプリケーショ

自動翻訳

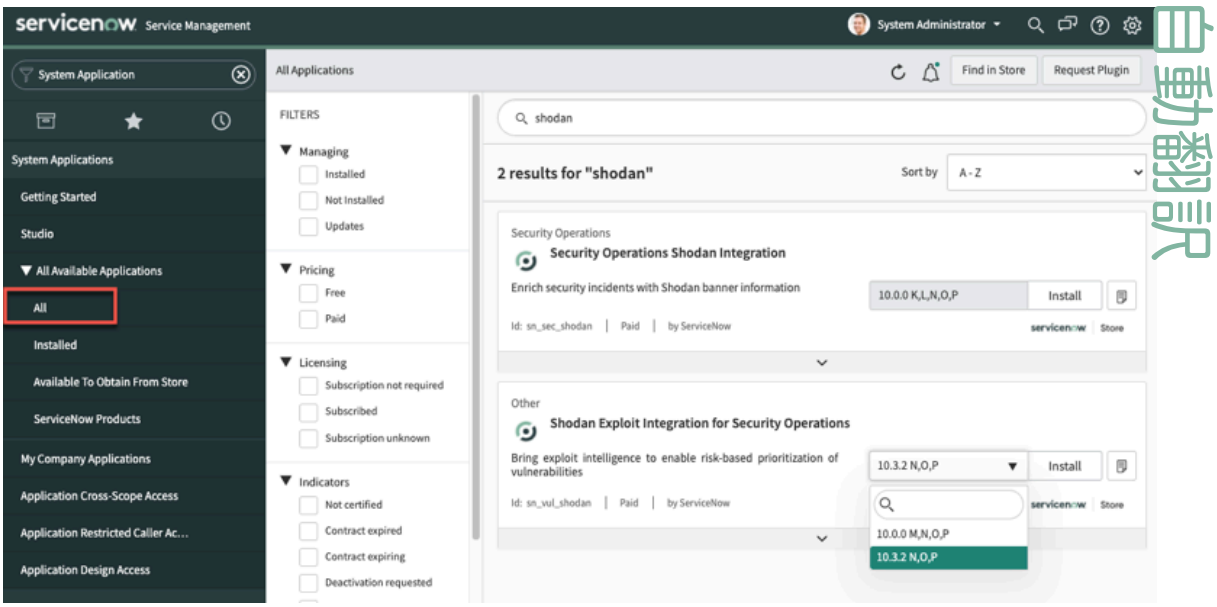
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	ンのエンタイトルメントの取得」を参照してくださ。
(オプション) まだインストールしてアクティブ化していない場合は、サードパーティアプリケーションをインストールする前に 脆弱性対応 アプリケーションをインストールすることもできます。	脆弱性対応 アプリケーションのインストールとアクティブ化の詳細については、「脆弱性対応のインストール」を参照してください。
Shodan Exploit Integration API キーを用意してください。	「Shodan Exploit Integration の準備」を参照してください。

必要なロール：admin

手順

1. Shodan Exploit Integrationアプリケーションをインストールする Now Platform インスタンスにログインします
2. 次のように移動する。 システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて).
3. Shodan Exploit Integration for セキュリティオペレーション アプリケーションを見つけて、使用するバージョンを選択し、[インストール] をクリックします。

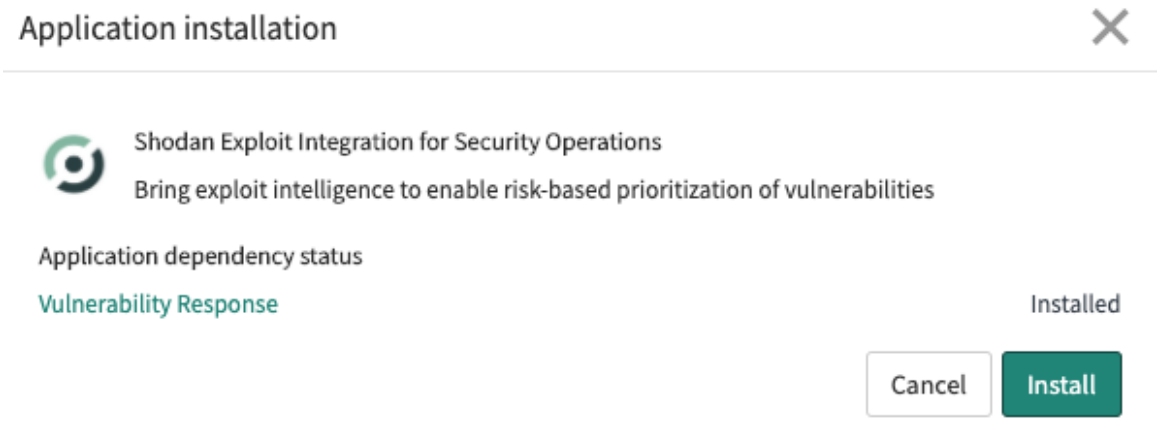


> **注:**
> このアプリケーションの更新権限がある場合は、[更新] ボタンが表示されます。

[アプリケーションのインストール] ダイアログに、アプリケーション依存関係ステータスが表示されます。まだインストールされていない必要な依存関係は、アプリケーションとともに自動的にインストールされます。

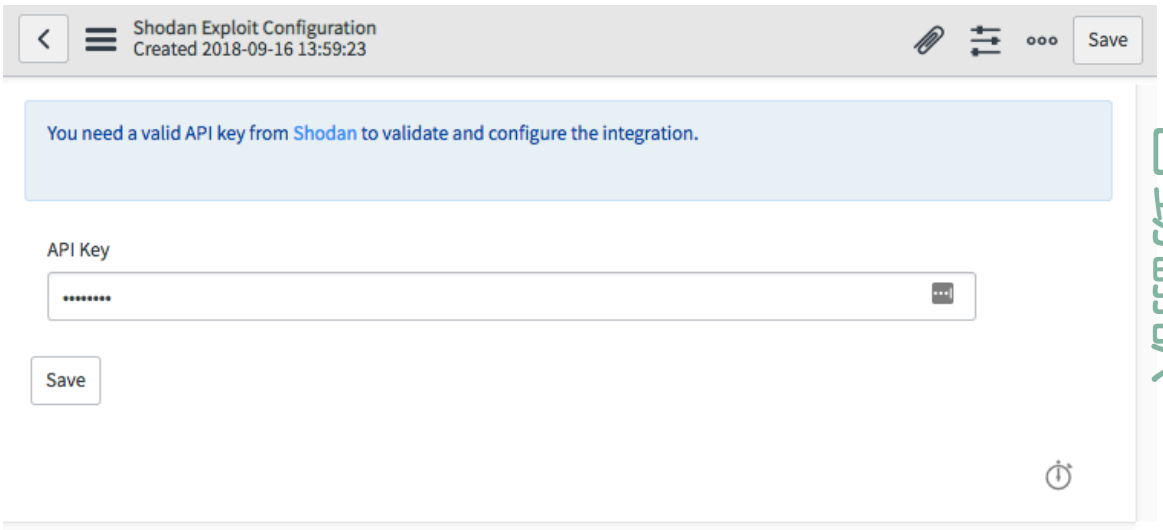
4. ダイアログで [インストール] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



インストールが正常に完了すると、[インストール] ダイアログに示されます。

5. [インストール] ダイアログを閉じます。
6. 次のように移動する。 **Shodan Exploit Integration** > 構成.
7. Shodan API キーを入力します。



8. **[Save** (保存)] をクリックします。
   Shodan Exploit Integration 構成が完了しました。

Shodan Exploit Integration インポート時間の設定

必要に応じて Shodan Exploit Integration の開始時間をリセットできます。

始める前に
必要なロール：admin

このタスクについて
最初のインポート後、完全インポートが要求されない限り、Shodan Exploit Integration によってデルタデータが取り込まれます。完全インポートの詳細については、「手動での Shodan Exploit インポートの実行」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > **Shodan Exploit Integration** > 統合.
2. 統合を選択します。
3. リンクをクリックしてレコードを編集します。
4. 新しい [実行] および [時刻] オプションを設定します。
   時間は現地時間で時間単位で計算されます。Shodan Exploit インポートのデフォルト時間は 03:15:00 です。
5. [更新] をクリックします。
   新しい時間は、次のスケジュール済みインポートに使用されます。

手動での **Shodan Exploit** インポートの実行

初期インポートに失敗した場合、またはスケジュールされた初期インポートを待ちたくない場合は、日次スケジュール済みジョブから独立して完全なデータインポートを実行できます。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > **Shodan Exploit Integration** > 統合.
2. 統合を選択します。
3. [完全データインポート] チェックボックスをオンにします。
4. [今すぐ実行] をクリックします。
   インポートが完了すると、チェックボックスがオフになり、デルタインポートが再開されます。

Shodan Exploit Integration インポート実行状況の表示

[脆弱性統合実行] 関連リストを使用して、統合実行の成功を確認し、問題を特定して、修復の決定を通知します。

始める前に
Shodan インポート実行状況を表示するには、次の手順を実行します。

- 脆弱性対応 アプリケーションと Shodan Exploit Integration をインストールして構成する必要があります。
- Shodan Exploit Integration インポートがスケジュールされ、実行されている必要があります。

必要なロール：sn_vuln.admin

このタスクについて
統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、 脆弱性対応のバージョン 18.2.4 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

手順

1. 次のように移動する。 **All** (すべて) > **Shodan Exploit Integration** > 統合.
2. 統合を選択します。
3. [脆弱性統合実行] 関連リストをクリックします。
4. すべてのインポートが成功したことを確認します。

Trouble?

実行が失敗した場合の一般的な原因は次のとおりです。

- ネットワーク中断
- データ転送が少し低下することによる、変換中のデータの破損

これらの条件のいずれかが発生した場合は、[完全データインポート] チェックボックスをオンにし、[今すぐ実行] をクリックして統合を再実行します。

Tenable 脆弱性統合の概要

Tenable 脆弱性統合の ServiceNow エンジニアリングによって開発された Vulnerability Response Integration with Tenable アプリケーションでは、Tenable.io および Tenable.sc 製品からインポートしたデータを使用して、資産の脆弱性に優先順位を付けて修正できます。アプリケーションは ServiceNow Store の個別のサブスクリプションで利用できます。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

Tenable 脆弱性統合では、資産と脆弱性に関するサードパーティのスキャナーデータをインポートできるように Tenable.io と Tenable.sc の 2 つの Tenable 統合を採用しています。Vulnerability Response Integration with Tenable アプリケーションは、バージョン 5.13 以降の Tenable.sc 製品をサポートしています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

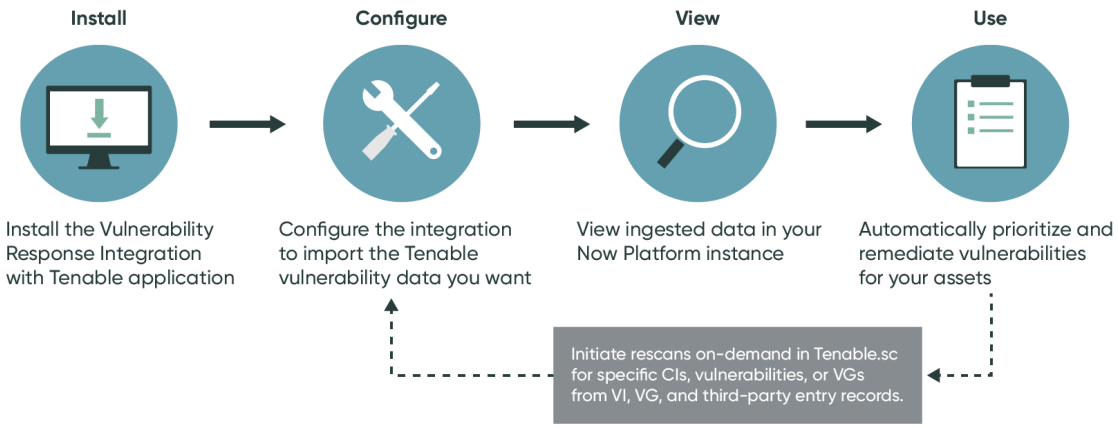
自動翻訳

- Tenable.io はクラウドベースのエンタープライズ統合です。
- Tenable.sc は、Tenable.sc 製品と Now Platform インスタンスが同じ環境にある場合に MID サーバーを使用するオプションを提供するオンプレミスの統合です。
- Tenable.sc 製品と Now Platform インスタンスが同じ環境にない場合は、MID サーバーを使用する必要があります。

Vulnerability Response Integration with Tenable アプリケーションは ServiceNow Store の別のサブスクリプションで利用できます。

Tenable 脆弱性統合の統合のリストと説明については、「脆弱性対応 および コンフィグレーション コンプライアンス アプリケーションとの Tenable.io 統合」および「脆弱性対応 アプリケーションとの Tenable.sc 統合」を参照してください。

Tenable 脆弱性統合



Yokohama の利用可能バージョン

リリースバージョン	リリースノート
Vulnerability Response Integration with Tenable v3.5、v3.6	互換性情報については、「KB0856498 脆弱性対応互換性マトリクスおよびリリーススキーマの変更」を参照してください。

統合に関する用語と主な機能

脆弱性一致アイテムと脆弱性

次の場合に Now Platform インスタンスに脆弱性一致アイテムが作成されます。

- サードパーティのスキャナーからインポートした脆弱性が既存の資産 (CMDB の構成アイテム) と一致する。Tenable 製品では、これらの一致を [脆弱性] と呼びます。
- サードパーティのスキャナーからインポートした脆弱性が CMDB の既存の資産と一致しない。この場合、脆弱性一致アイテムとともに一致しない CI も作成されます。

  CI が一致せず、既存の CI がホストと一致しない場合、識別および調整エンジン (IRE) を使用して CI を 2 つのクラスに作成することもできます。それ以外の場合は、一致しない CI が [不一致] CI クラスに作成されます。詳細については、「識別および調整エンジンを使用して 脆弱性対応 の CI を作成する」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

サードパーティ脆弱性エントリーとプラグイン

サードパーティ脆弱性エントリーはサードパーティスキャナーからインポートされ、Now Platform インスタンスの [サードパーティ脆弱性エントリー] テーブルにリストされます。脆弱性対応 v24.0 以降、[サードパーティ脆弱性エントリー] テーブルの [ソフトウェア] 列には、サードパーティ エントリーに関連付けられた共通プラットフォーム一覧 (CPE) が入力されます。Tenable からのサードパーティ脆弱性エントリーが 脆弱性対応 に取り込まれ、CMDB にリストされている既存の資産と照合されます。Tenable では、サードパーティ脆弱性エントリーを [プラグイン] と呼びます。

構成アイテム (CI)

構成アイテムは、CMDB にリストされている既存の資産です。

検出されたアイテム

Tenable 資産インポートから取り込まれた資産は、CMDB の既存の構成アイテムと照合されます。インポートされた資産は更新されます。

一致するものが見つからない場合は、CMDB の [一致しない CI] クラスに CI が作成されます。CMDB CI クラスモデルプラグインが有効の場合、識別および調整エンジン (IRE) が新しいクラスを使用して新しい CI を作成します。詳細については、「識別および調整エンジンを使用して 脆弱性対応 の CI を作成する」を参照してください。元の一致しない CI が再分類され、検出されたアイテムレコードを更新してステータスが反映されます。検出されたアイテムにより、資産がどのように識別され、CMDB の CI にマッピングされるかを把握できます。

CI ルックアップルール

サードパーティ統合からデータがインポートされると、脆弱性対応はホスト (資産) データを自動的に使用して、Configuration Management Database (CMDB) で一致するものを検索します。CI ルックアップルールは CI の識別に使用され、修復に使用できるように、VI が作成されると VI レコードに追加されます。

再スキャンと修復スキャン

Now Platform インスタンス内の脆弱性一致アイテム、修復タスク、およびサードパーティの脆弱性エントリーレコードから、特定の構成アイテム、修復タスク、またはサードパーティのエントリーでターゲットの再スキャンコマンドを開始できます。Tenable では、この再スキャンを [修復スキャン **(remediation scan)]** と呼びます。

古い VI を自動的にクローズします。

Now Platform の [古い脆弱性一致アイテムの自動クローズ (Auto-Close Stale Vulnerable Items)] モジュールを使用すると、サードパーティ統合によって最近検出されていない古い脆弱性一致アイテム (VI) をクリーンアップできます。これらの VI を [クローズ済み] に移動すると、アクティブな脆弱性一致アイテムと修復タスクの数を減らし、CMDB の資産を調整できます。Vulnerability Response Integration with Tenable との統合をすべて使用して、古い VI を自動的にクローズできます。

インスタンス

この用語は、Now Platform® アプリケーションの個別の発生を指します。

統合

統合は、Tenable.io 資産統合や Tenable.sc プラグイン統合などの統合への製品固有の参照です。これらは、インスタンスの Tenable 脆弱性統合の特定の Tenable 製品に属する個別の統合です。

統合インスタンス

この用語は、Tenable.io および Tenable.sc 製品によってリストされている個別の Tenable 統合を指します。

展開

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

統合でマルチソースがサポートされている場合、単一の個別の統合の存在は、統合の展開と呼ばれます。この用語は、環境全体での統合と製品を指すのに使用されます。たとえば、Tenable.io および Tenable.sc 製品のさまざまな統合を環境に複数展開する場合があります。

Tenable.io および Tenable.sc の統合には、次の主な機能もあります。

- 構成アセスメントの結果 (テスト結果と、ポリシー、構成テスト (コントロール)、および信頼できるソースの引用) を Tenable.io 製品で コンフィグレーションコンプライアンス アプリケーションにインポートできます。この統合が コンフィグレーションコンプライアンス アプリケーションでどのように機能するかの詳細については、「脆弱性対応 および コンフィグレーションコンプライアンス アプリケーションとの Tenable.io 統合」および「コンフィグレーションコンプライアンスの詳細」を参照してください。
- v2.1 の Tenable 脆弱性統合 から、同じ IP アドレスを共有する環境内の資産に対して、異なるネットワークパーティション識別子を含む一意の構成アイテム (CI) を作成します。環境全体で個別の資産を特定し、検出された既存のアイテム、脆弱性一致アイテム、および検出レコードで CI を更新して、脆弱性に関する詳細を提供します。
- すべての Tenable.io および Tenable.sc 統合でジョブを実行するタイミングをスケジュールできます。スケジュール済みジョブをオンデマンドで手動実行することもできます。
- Tenable.io を使用した資産インポートでは、資産タグを有効にして Tenable.io 環境の CMDB にリストされている資産を整理して追跡できます。
- Tenable.io および Tenable.sc 統合では、Now Platform CMDB の構成アイテム (CI) を特定するためにサードパーティソースの資産データを使用する方法を CI ルックアップルールで定義できます。
- Tenable.io および Tenable.sc 統合では、必要な脆弱性のみを Tenable からインポートできるように、脆弱性インポート時にインポートフィルターを設定できます。Tenable.io には、脆弱性インポートを使用して Tenable から [修正済み] の脆弱性をインポートするオプションがあります。
- Tenable.sc には、Now Platform インスタンスの脆弱性一致アイテム、修復タスク、およびサードパーティエントリーレコードから直接オンデマンドで再スキャンを開始するオプションがあります。VI が [クローズ済み]/[修正済み] に移行しても、インスタンスでまだ更新されていない場合は、特定の構成アイテムの脆弱性が修正されていることを確認できます。「Tenable.sc 統合の再スキャンの開始」を参照してください。

次のセクションでは、Tenable 統合の詳細について説明します。

必要な **Now Platform** ロール

統合タスクには、Now Platform インスタンスで次のロールが必要です。

admin

システムアドミニストレーターは、セットアップアシスタントを使用して Vulnerability Response Integration with Tenable アプリケーションをインストールします。アサインされていない場合、アドミニストレーターはセットアップアシスタントで脆弱性アドミン (sn_vul.vulnerability_admin) およびその他のロールをアサインします。

sn_vul.vulnerability_admin

アサインされると、脆弱性アドミニストレーターはセットアップアシスタントで Tenable 統合の構成を比較します。このロールは、脆弱性対応 (VR) アプリケーションとそのレコードに完全にアクセスできます。脆弱性アドミニストレーターは、インストールされたサードパーティ統合のすべての VR アプリケーションとルールを構成します。

sn_vul_tenable.configure_integration

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このロールには詳細なロール sn_vul_tenable.read_integration が含まれており、このロールを持つユーザーは Vulnerability Response Integration with Tenable アプリケーションを設定できます。

sn_vul_tenable.read_integration

このロールを持つユーザーは、Vulnerability Response Integration with Tenable アプリケーションのレコードを表示 (読み取り) できますが、編集することはできません。

脆弱性対応グループ

デフォルトで脆弱性対応グループはセットアップアシスタントで利用可能になっています。脆弱性対応グループにアサインされたユーザーは sn_vul.read_all および sn_vul.remediation_owner ロールを自動的に継承します。

脆弱性一致アイテム

脆弱性一致アイテムは、修復タスクルールに従って修復タスクにグループ化され、アサインルールに基づいて修復にアサインされます。詳細については、「脆弱性対応修復タスクとタスクルールの概要」と「脆弱性対応 アサインルールの概要」を参照してください。

構成アイテム (CI) ルックアップルール

CI ルックアップルールでは、CI を識別して、それらを脆弱性一致アイテムに追加するタイミングを決定します。CI ルックアップルールの詳しい仕組みについては、「脆弱性対応 サードパーティ脆弱性統合の構成アイテムを識別するための CI ルックアップルール」を参照してください。

注:
ルールは、一度削除すると元に戻せません。新しいルールを作成する場合は、既存のルールを削除せずに無効にします。

次の Tenable.io ルックアップルールはベースシステムに付属しています。

- MAC_ADDRESS
- FQDN
- NetBIOS
- HostName
- DNS
- IP

注:
Tenable.io CI ルックアップルールは、検出されたアイテムの通常の FDQN、IPV4、および MacAddress 値よりも、空でないネットワークインターフェイス値 (FDQN、IPV4、および MacAddress) を優先して入力します。これらのネットワークインターフェイスの値が空の場合、通常の FDQN、IPV4、および MacAddress の値が検出されたアイテムに設定されます。

次の Tenable.sc ルックアップルールはベースシステムに付属しています。

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
ip_address、mac_address、fqdns、および network_interfaces の複数の値が資産に使用されます。すべての値が照合用の CI ルックアップルールで考慮されます。IRE を使用して複数のネットワークアダプターを作成するためにすべての値が使用されます。

一致しないクラウドリソースの分類を優先 CI クラスに構成する方法の詳細については、「一致しないクラウド資産の CI クラスの更新」を参照してください。

IP アドレスを無視する新しいプロパティ

Tenable.io では、CI ルックアップルールの一部として、複数の IP アドレスまたは複数の Mac アドレスを無視する場合に使用できるプロパティが 2 つあります。

ignoreIPAddress
: CI のルックアップと CI の作成で無視する IP アドレスのリスト

ignoreMacAddress
: CI のルックアップと CI の作成で無視する MAC アドレスのリスト

検出されたアイテム

このモジュールは、Tenable 脆弱性一致アイテム統合および Tenable 資産統合からのインポート中に検出された構成アイテムをリストします。

注:
このリストのデフォルトのフィルターは [不一致] に設定されています。フィルターを削除すると、インポートから検出されたすべてのアイテムを表示できます。

[検出されたアイテム] モジュールの詳細については、「検出されたアイテム」を参照してください。

資産タグ

資産タグ (ホストタグとも呼ばれます) は、組織の資産の整理と追跡に使用されます。資産にタグを割り当てることができます。これにより、スキャンを開始するときに、スキャンする資産に関連付けられたタグを選択できます。資産タグモジュールを使用すると、スケジュールに基づいて Tenable.io からインスタンスに資産タグデータをダウンロードできます。資産タグを含む資産データは Tenable.io からプルされ、Tenable.io 資産変換統合変換マップを使用して変換されます。

すべての資産タグは Tenable.io 資産統合の一部としてインポートされます。資産タグは、主に 脆弱性対応 アサインルールおよび修復タスクルールでのフィルタリングに使用されます。タグは [検出されたアイテム] フォームに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
脆弱性対応 アプリケーションで 脆弱性対応 アサインルールまたは修復タスクルールを作成する前に Tenable.io 資産統合を実行し、脆弱性一致アイテムをインポートしてグループ化する前に、これらのルールですべてのタグを使用できるようにします。タグに関する次の点にも注意してください。

- タグストレージでは大文字と小文字は区別されません。たとえば、San Diego の場所で資産を説明するタグを作成し [San Diego] タグを作成する場合、[SAN DIEGO] タグを作成して資産タグテーブルに保存することはできません。San Diego と SAN DIEGO は同じホストタグと見なされます。最初にインポートされたタグが格納され、以後認識されるようになります。
- 修復タスクルールのグループキーとして資産タグを使用すると、予期しない結果になることがあります。資産タグは条件ビルダー専用です。
- 資産タグは、グローバルシステムプロパティ sn_vul.import_asset_tags で制御されます。このプロパティはデフォルトで [true] に設定されています。タグを無効にすると、すべての Now Platform® インスタンスで無効になります。

データ検索フィルター

データ検索設定は、Tenable アプリケーションから Now Platform® インスタンスにインポートするデータのタイプとスコープを具体的に決定するのに役立ちます。最も一般的に使用される設定のリストについては、「Tenable 脆弱性統合のデータ検索設定」を参照してください。

脆弱性優先評価 (VPR)

脆弱性優先評価 (VPR) は、脆弱性対応 の新しいデフォルトのリスク算出でインポートして使用される Tenable 製品の属性です。Tenable リスクルールは、脆弱性対応 の脆弱性算出のデフォルトのリスク算出の一部として Vulnerability Response Integration with Tenable アプリケーションとともにインストールされます。

このリスクルールデフォルトでは無効になっています。

Tenable リスク算出ルールを有効にすると、インポートされた VPR 値が脆弱性一致アイテムのリスクスコアの計算に使用されます。このリスク算出のデフォルトの重み付け分布：VPR = 70%、資産 = 15%、ビジネス上の重要度 = 15%。この Tenable リスク算出ルールを有効にすると、データ取り込みのパフォーマンスが影響を受ける可能性があります。脆弱性対応 算出と Tenable リスク算出ルールの詳細については、「脆弱性対応 の算出と脆弱性算出ルール」を参照してください。

インストールと構成

ServiceNow® Store から Vulnerability Response Integration with Tenable をダウンロードすると、インストールと構成は 脆弱性対応 のセットアップアシスタントでサポートされます。詳細については、「セットアップアシスタントを使用した 脆弱性対応 の構成」を参照してください。

脆弱性対応 および コンフィグレーションコンプライアンス アプリケーションとの **Tenable.io** 統合

Vulnerability Response Integration with Tenable アプリケーションの Tenable.io 統合は、脆弱性対応 および コンフィグレーションコンプライアンス アプリケーションで使用できます。

Tenable.io 統合のリスト

マルチソースは Tenable.io および Tenable.sc のすべての統合でサポートされます。脆弱性対応 のセットアップアシスタントから、次の統合の複数のインスタンスを環境全体に追加して展開できます。セットアップアシスタントから Vulnerability Response Integration with Tenable アプリケーションをインストールして構成することもできます。

Tenable.io はクラウドベースのエンタープライズ統合です。Tenable.io 製品でサポートされている統合の名前と説明については、次の表を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Tenable.io コンプライアンス結果統合と Tenable.io コンプライアンス結果バックフィル統合は、デフォルトでは非アクティブです。

それらをアクティブ化するには、次の手順を実行します。

1. 次のように移動する。 **Tenable** 脆弱性統合 > アドミニストレーション > 統合.
2. [Tenable 脆弱性統合] リストで、統合名をクリックしてレコードを開き、[アクティブ] チェックボックスをオンにして有効にします。これらの統合を開始するには、スケジュール設定をデフォルト値のままにすることをお勧めします。

Tenable.io の統合

統合	説明
Tenable.io 資産統合	• 資産タグを含むすべての資産データを Tenable.io 製品から取得して、インスタンスで処理します。 • v3.0 以降では、Tenable.io コンプライアンス結果統合がアクティブになっている場合は、インポートされた資産データとともに安全な構成アセスメントデータをインポートできます。このデータは、資産の構成関連の脆弱性を特定して対応するのに役立ちます。 • 一致しない資産に対して一意の CI を作成するか、同じ IP アドレスを共有する環境全体の資産に対してネットワークパーティション識別子属性を使用して既存の CI を更新します。 • 資産 API への REST メッセージ呼び出しを調整します。 • この統合の出力は検出されたアイテムです。 • データはチャンクでインポートされ、[sn_vul_tenable_chunk_status] テーブルに格納されます。テーブルクリーナーは、保存されたデータを 30 日後にこのテーブルから自動的に削除します。 • v2.2 以降では、脆弱性がある資産に対してのみ *Last Scan Time* がインポートされて更新されます。
Tenable.io コンプライアンス結果統合	• v3.0 以降、資産統合からインポートされたデータとともに、コンプライアンス結果統合からインポートされた安全な構成アセスメントデータは、資産の構成関連の脆弱性を特定して対応するのに役立ちます。 • 有効にすると、高レベルの安全な構成アセスメントデータを取得し、Now Platform インスタンスで処理します。インポートされたデータには、ポリシー、構成テスト (コントロール)、信頼できるソースの引用とともにテスト結果が含まれます。 • 不足している資産または資産 ID のない資産のアセスメントデータはインポートされません。 • テスト結果がインポートされ、対応する資産がインスタンスで一致しない場合、テスト結果は無視され、不足している資産の

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.io の統合 (続く)

統合	説明
	ID が [sn_vul_tenable_missing_asset] テーブルの一時レコードに保存されます。 • 無視された (不足している) 資産の合計値は、この統合の統合実行レコードの [構成] タブの [無視された **CI]** フィールドに一覧表示されます。
Tenable.ioコンプライアンス結果バックフィル統合	• アクティブにすると、資産統合がチェーン統合実行の一部として正常に完了した後に、この統合が自動的に実行されます。この統合は、[sn_vul_tenable_missing_asset] テーブルにリストされている不足している資産と構成アセスメントデータを照合します。 • 資産統合のインポートが正常に完了した後に、インスタンスで検出またはインスタンスに存在する不足している資産について、最大 200 の資産 ID をインポートします。 • 対応する構成アセスメントデータと資産を照合できる場合、[sn_vul_tenable_missing_asset] テーブルから一時レコードを削除します。
Tenable.ioスキャン認証情報統合	• この統合は、Tenable.io で構成されたスキャン認証情報を取得します。 • 認証情報 API への REST メッセージ呼び出しを調整します。 • この統合の出力は、[sn_vul_tenable_scan_credential] テーブルに入力されるスキャン認証情報です。 • インポートされた認証情報は、スキャン要求が Now Platform から開始されたときにスキャナーにアクセスするために使用されます。 • この統合は毎週実行されるようにスケジュールされています。
Tenable.ioテンプレート統合	再スキャン中にテンプレートレコードが Tenable.io に送信されます。この統合は、再スキャンに使用する利用可能な Tenable.io 認証情報を取得します。認証情報はインスタンス固有であり、単一のテンプレートレコードがインポートされ、[sn_vul_tenable_io_template] テーブルに一時的に安全に格納されます。
Tenable.io プラグイン統合	• Tenable.io 製品からプラグインデータを取得します。取得されるデータは、Tenable.io 統合実行によってプラグインが最後に更新された日付に基づいています。 • このインポートにより、Tenable.io 識別子 (10 個の ID) が最新の状態になります。 • プラグイン API への REST メッセージ呼び出しを調整します。 • この統合の出力はサードパーティ脆弱性です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.io の統合 (続く)

統合	説明
Tenable.io の修正された脆弱性統合	• 重大度フィルターに基づいて、Tenable.io 製品から脆弱性データを取得し、インスタンスで処理します。脆弱性一致アイテムは「オープン」および「再オープン」ステータスの検出レコードに対して作成されます。これらのレコードには修復が必要なためです。検出が「修正済み」の場合、既存の脆弱性一致アイテムは脆弱性対応によって更新されますが、Tenable は「修正済み」の脆弱性を「脅威緩和」とみなすため、デフォルトでは「 修正済み」の検出に対して脆弱性一致アイテムは作成されません。 • セットアップアシスタントで「修正済みの脆弱性検出に対して脆弱性一致アイテムを作成」フラグがアクティブ化されている場合、新しい VI は「修正済み」ステータスで作成されるため、それらを作成した検出を表示できます。VI はインスタンスにまだ存在しない「修正済み 」の検出に対して作成されるため、インポートのパフォーマンスに悪影響を与える可能性があります。この機能を非アクティブのままにして、 修正済みの検出によって既存の脆弱性一致アイテムの状況だけが更新されるようにすることもできます。 • 一致しない資産に対して一意の CI を作成するか、同じ IP アドレスを共有する環境全体の資産に対してネットワークパーティション識別子属性を使用して既存の CI を更新します。 • 脆弱性 API への REST メッセージ呼び出しを調整します。 • この統合の出力は [クローズ済み]/[修正済み] の脆弱性一致アイテム (VI) です。これは、資産とサードパーティのエントリーが存在しない場合にも作成されます。 • データはチャンクでインポートされ、[sn_vul_tenable_chunk_status] テーブルに格納されます。テーブルクリーナーは、保存されたデータを 30 日後にこのテーブルから自動的に削除します。 この統合実行はスケジュールされています。これはチェーン統合であり、実行が正常に完了すると、後述のオープンな脆弱性統合がトリガーされます。 Tenable v3.3 以降では、脆弱性統合の実行に関する次の情報を表示できます。 • 合計チャンク：Tenable によって生成されているチャンクの合計数 • 利用可能なチャンク：ServiceNow のダウンロード可能なチャンクの数
Tenable.io のオープンな脆弱性統合	• この統合は、Tenable.io の修正された脆弱性統合が正常に完了するとトリガーされます。 • 重大度フィルターに基づいて、Tenable.io 製品から脆弱性データを取得し、インスタンスで処理します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.io の統合 (続く)

統合	説明
	• 一致しない資産に対して一意の CI を作成するか、同じ IP アドレスを共有する環境全体の資産に対してネットワークパーティション識別子属性を使用して既存の CI を更新します。 • 脆弱性 API への REST メッセージ呼び出しを調整します。 • この統合の出力は [新規]/[再オープン] の脆弱性一致アイテム (VI) です。これは、構成アイテムとサードパーティのエントリーが存在しない場合にも作成されます。Tenable はアクティブな脆弱性を [累積] (現在) と見なします。 • データはチャンクでインポートされ、[sn_vul_tenable_chunk_status] テーブルに格納されます。テーブルクリーナーは、保存されたデータを 30 日後にこのテーブルから自動的に削除します。 Tenable v3.3 以降では、脆弱性統合の実行に関する次の情報を表示できます。 • 合計チャンク：Tenable によって生成されているチャンクの合計数 • 利用可能なチャンク：ServiceNow のダウンロード可能なチャンクの数

脆弱性対応 アプリケーションとの **Tenable.sc** 統合

Vulnerability Response Integration with Tenable アプリケーションとの Tenable.sc 統合。

脆弱性対応 v20.0 以降では、資産がエージェントによってスキャンされた場合、[エージェントが存在します] 列に、それが本物のスキャンであることを示す値、true が [検出されたアイテム] リストに表示されます。

Tenable.sc 統合のリスト

マルチソースは Tenable.io および Tenable.sc のすべての統合でサポートされます。脆弱性対応 のセットアップアシスタントから、次の統合の複数のインスタンスを環境全体に追加して展開できます。セットアップアシスタントから Vulnerability Response Integration with Tenable アプリケーションをインストールして構成することもできます。

- Tenable.sc は、Tenable.sc 製品と Now Platform インスタンスが同じ環境にある場合に MID サーバーを使用するオプションを提供するオンプレミスの統合です。
- Tenable.sc 製品と Now Platform インスタンスが同じ環境にない場合は、MID サーバーを使用する必要があります。

Tenable.sc の統合

統合	説明
Tenable.sc 資産統合	インポートされた資産データで検出されたアイテムが重複して作成されるのを避けるために、Tenable.sc 製品の資産統合は 2 つの統合で構成されています。 Tenable.sc オープン資産統合

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.sc の統合 (続く)

統合	説明
	この統合により、Tenable が累積 (現在) またはオープンと見なす資産に関する脆弱性データがインポートされます。このインポートされた資産データを使用してインスタンスで作成された脆弱性一致アイテム (VI) は、オープンしている、つまり [オープン] ステータスにあると見なされます。これらの脆弱性一致アイテムは調査が必要で、修正が必要な場合があります。 Tenable.sc 固定資産統合 この統合により、Tenable が脅威緩和 (脆弱性なし) または修正済みと見なす資産に関する脆弱性データがインポートされます。スキャンの結果、脆弱性がなくなったことが示されるため、これらの資産の脆弱性一致アイテムは、インスタンスで [オープン] ステータスから [クローズ済み]/[修正済み] ステータスに移行します。 • すべての資産データを Tenable.sc 製品から取得して、インスタンスで処理します。 • 一致しない資産に対して一意の CI を作成するか、同じ IP アドレスを共有する環境全体の資産に対してネットワークパーティション識別子属性を使用して既存の CI を更新します。 • 資産 API への REST メッセージ呼び出しを調整します。 • この統合の出力は検出されたアイテムです。 • セットアップアシスタントで選択した Tenable クエリフィルターは、Tenable.sc 資産統合にも適用されます。クエリフィルターの条件に一致する脆弱性がある資産のみがインポートされます。
Tenable.sc プラグイン統合	• Tenable.sc 製品からプラグインデータを取得します。取得されるデータは、Tenable.sc 統合実行によってプラグインが最後に更新された日付に基づいています。 • このインポートにより、Tenable.sc 識別子 (10 個の ID) が最新の状態になり、アクティブな脆弱性のみがインポートされます。 • プラグイン API への REST メッセージ呼び出しを調整します。 • この統合の出力はサードパーティ脆弱性です。
Tenable.sc の修正された脆弱性統合	• 重大度フィルターに基づいて、Tenable.sc 製品から脆弱性データを取得し、インスタンスで処理します。脆弱性一致アイテムは「オープン」および「再オープン」ステータスの検出レコードに対して作成されます。これらのレコードには修復が必要なためです。検出が「修正済み」の場合、既存の脆弱性一致アイテムは脆弱性対応によって更新されますが、Tenable は「修正済み」の脆弱性を「脅威緩和」とみなすため、デフォル

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.sc の統合 (続く)

統合	説明
	トでは「 修正済み」の検出に対して脆弱性一致アイテムは作成されません。 • セットアップアシスタントで「修正済みの脆弱性検出に対して脆弱性一致アイテムを作成」フラグがアクティブ化されている場合、新しい VI は「修正 済み」ステータスで作成されるため、それらを作成した検出を表示できます。VI はインスタンスにまだ存在しない「修正済み 」の検出に対して作成されるため、インポートのパフォーマンスに悪影響を与える可能性があります。この機能を非アクティブのままにして、 修正済みの検出によって既存の脆弱性一致アイテムの状況だけが更新されるようにすることもできます。 • 一致しない資産に対して一意の CI を作成するか、同じ IP アドレスを共有する環境全体の資産に対してネットワークパーティション識別子属性を使用して既存の CI を更新します。 • 脆弱性 API への REST メッセージ呼び出しを調整します。 • この統合の出力は [クローズ済み]/[修正済み] の脆弱性一致アイテム (VI) です。これは、資産とサードパーティのエントリーが存在しない場合にも作成されます。 この統合実行はスケジュールされた実行です。これはチェーン統合であり、実行が正常に完了すると、後述の Tenable.sc オープンな脆弱性統合がトリガーされます。 **注:** デフォルトでは、ファミリー ID 0 と 39 はこの統合から除外されます。
Tenable.sc のオープンな脆弱性統合	• この統合は、Tenable.sc の修正された脆弱性統合が正常に完了するとトリガーされます。 • 選択したクエリフィルターに基づいて、Tenable.sc 製品から脆弱性データを取得し、インスタンスで処理します。 • アクティブな脆弱性に対応する脆弱性一致アイテムを作成します。 • 一致しない資産に対して一意の CI を作成するか、同じ IP アドレスを共有する環境全体の資産に対してネットワークパーティション識別子属性を使用して既存の CI を更新します。 • 脆弱性 API への REST メッセージ呼び出しを調整します。 • この統合の出力は、[更新]/[新規作成] の脆弱性一致アイテム (VI) となります (まだ存在しない場合)。これは、構成アイテムとサードパーティのエントリーが存在しない場合にも作成されます。 **注:** デフォルトでは、ファミリー ID 0 と 39 はこの統合から除外されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.sc の統合 (続く)

統合	説明
Tenable.sc スキャン認証情報統合	• この統合は、Tenable.sc で構成されたスキャン認証情報を取得します。 • 認証情報 API への REST メッセージ呼び出しを調整します。 • この統合の出力は、テーブル [sn_vul_tenable_scan_credential] に入力されるスキャン認証情報です。 • インポートされた認証情報は、スキャン要求が Now Platform から開始されたときにスキャナーにアクセスするために使用されます。 • この統合は毎週実行されるようにスケジュールされています。
Tenable.sc バックフィル脆弱性統合	• このバックフィル統合は、インポート中に見落とされた可能性があるオープンおよび修正された脆弱性をインポートします。 • この統合では、過去 7 日間のオープンな脆弱性と修正された脆弱性の両方をインポートして、検出と脆弱性一致アイテムを更新します。 • この統合により、パフォーマンスが影響を受ける可能性があります。 • この統合はデフォルトで無効になっています。 • 脆弱性データを更新し、潜在的なパフォーマンスの問題を回避するために、他のスキャンが実行されていないときに Tenable.sc の修正された脆弱性とオープンな脆弱性統合をスケジュールすることをお勧めします。 • この統合の出力は次のようになります。 ○ [クローズ済み]/[修正済み] 脆弱性一致アイテム (VI)。これは、資産とサードパーティのエントリーが存在しない場合にも作成されます。 ○ [更新]/[新規作成] の脆弱性一致アイテム (VI) (まだ存在しない場合)。これは、構成アイテムとサードパーティのエントリーが存在しない場合にも作成されます。

ユーザー認証と **Tenable.sc**

ユーザー認証は、Now Platform® インスタンスとバージョン 5.13 の Tenable.sc 製品でサポートされています。バージョン 5.12 以前の Tenable.sc 製品を使用している場合は、ユーザー認証が必要です。

Tenable.sc 統合のユーザー認証を選択すると、統合の実行中にトークンが期限切れになり、置き換えられる可能性があります。トークンの有効期限が切れると、脆弱性統合実行レコード (VIN) の [メモ] 列に、[エラー：トークンの検証に失敗しました (Error: Token validation is failed)] のメッセージが表示されます。このメッセージが表示された場合は、アクションは必要ありません。期限切れのトークンはバックグラウンドで自動的に更新され、メッセージには統合プロセスの一時停止やエラーは表示されません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Tenable 脆弱性統合の準備

次のセットアップタスクを実行して ServiceNow® Tenable 脆弱性統合を準備します。

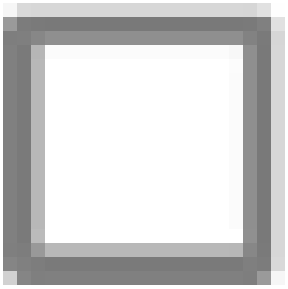
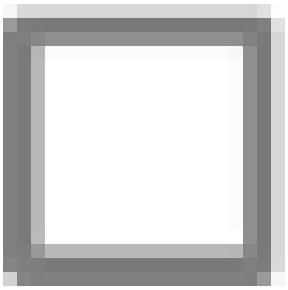
事前準備

統合を成功させるには、統合前のタスクを計画して慎重に実行する必要があります。Vulnerability Response Integration with Tenable アプリケーションのインストールと構成をスムーズに行えるように、アプリケーションをインストールして、脆弱性データを Now Platform® インスタンスにインポートする前に、次のチェックリストを印刷し、リストされているアイテムが完了していることを確認することをお勧めします。

注:
Tenable でビルドされた統合を使用してデータをインポートし、ServiceNow® Vulnerability Response Integration with Tenable の使用を開始する場合は、次を参照してください。

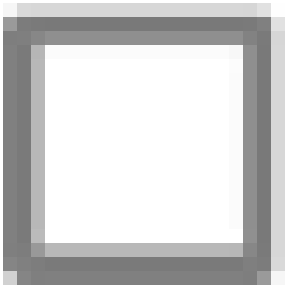
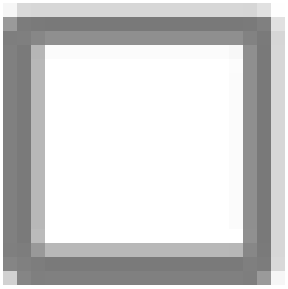
Tenable でビルドされた統合から ServiceNow によってビルドされた統合への現在のデータのクリーンアップおよび移行情報については、「Guidelines to migrate from the Tenable Vulnerability Response Integration to the ServiceNow Vulnerability Response Integration with Tenable [KB0960667] (Tenable Vulnerability Response Integration から ServiceNow Vulnerability Response Integration with Tenable への移行に関するガイドライン [KB0960667])」の記事を参照してください。

必要なロール：アプリケーションをダウンロードしてインストールするアドミン

タスク	説明
	(オプション) まだインストールしてアクティブ化していない場合は、サードパーティアプリケーションをインストールする前に 脆弱性対応 アプリケーションをインストールすることもできます。 脆弱性対応 アプリケーションのインストールとアクティブ化の詳細については、「脆弱性対応 のインストール」を参照してください。この統合には、脆弱性対応 のバージョン 12.1 以降が必要です。
	まだインスタンスにない場合は、エンタイトルメントを取得して、Vulnerability Response Integration with Tenable アプリケーションを Now Platform® インスタンスにダウンロードします。Vulnerability Response Integration with Tenable アプリケーションは、バージョン 5.13 以降の Tenable.sc 製品をサポートしています。 「」を参照してください。

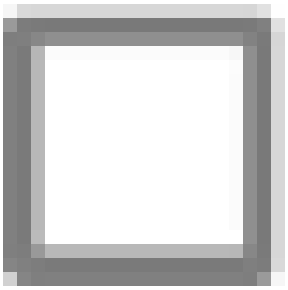
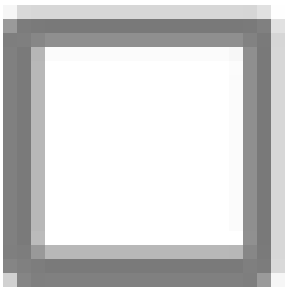
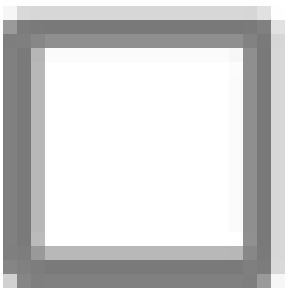
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスク	説明
	インポートする予定の脆弱性一致アイテムの数を見積もります。 インポートする予定の脆弱性一致アイテムの数をインスタンスが受け入れることができることを確認します。インスタンスが小さすぎると、ロードに時間がかかることがあります。インスタンスのサイズがわからない場合、またはサポートが必要な場合は、ServiceNow テクニカルサポートにお問い合わせください。
	統合を管理し、脆弱性一致アイテムを修正するグループまたはユーザーがいることを確認します。 admin システムアドミニストレーターは、セットアップアシスタントを使用して Vulnerability Response Integration with Tenable アプリケーションをインストールします。アサインされていない場合、アドミニストレーターはセットアップアシスタントで脆弱性アドミン (sn_vul.vulnerability_admin) およびその他のロールをアサインします。 sn_vul.vulnerability_admin アサインされると、脆弱性アドミニストレーターは Tenable 統合の構成を完了します。このロールは、脆弱性対応 (VR) アプリケーションとそのレコードに完全にアクセスできます。すべての VR アプリケーションとルールを構成し、サードパーティ統合を構成します。 sn_vul_tenable.configure_integration Tenable 脆弱性統合を構成できます。このロールには、sn_vul_tenable.read_integration の詳細なロールが含まれます。 sn_vul_tenable.read_integration Tenable 脆弱性統合のレコードを表示 (読み取り) できます。 脆弱性対応グループ デフォルトで脆弱性対応グループはセットアップアシスタントで利用可能になっています。Vulnerability Response (脆弱性対応) グループにアサインされたユーザーは sn_vul.read_all および sn_vul.remediation_owner ロールを自動的に継承します。 システムアドミンは、ユーザーとグループへのロールの最初のアサインをセットアップアシスタントで実行して統合します。デフォルトで、Vulnerability Response (脆弱性対応) グループは利用可能になっています。まだ作成されていない場合は、セットアップアシスタントを使用する前に、追加のグループを作成し、ユーザー管理モジュールでインスタンスにユーザーを追加することをお勧めします。「ユーザーグループを作成」を参照してください。 脆弱性対応アプリケーションでユーザーが実行および表示できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セット

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスク	説明
	アップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。
	最初のインポートのパフォーマンスを改善するには、インスタンスの特定の機能、ルール、またはジョブを無効にすることをお勧めします。 • 脆弱性算出を使用しない場合は無効にします。これらの算出では、定義した算出に加え、脆弱性一致アイテムレコードが作成および更新されるたびに実行されます。「脆弱性算出を無効化」を参照してください。 • レコードの最初のインポート中に、特定の通知関連のビジネスルールによって大量の通知が生成され、パフォーマンスが影響を受ける可能性があることを確認します。最初のインポートの前に、「Tenable 脆弱性統合のインポートの変更」で説明されているように通知関連のビジネスルールを無効にすることをお勧めします。
	統合に必要なインスタンス内の機能、ルール、依存関係プラグイン、またはジョブが有効になっていることを確認します。 • Tenable.sc は、Vulnerability Response Integration with Tenable 製品と Now Platform インスタンスが同じ環境にある場合に MID サーバーを使用するオプションを提供するオンプレミスの統合です。Tenable.sc 製品と Now Platform インスタンスが同じ環境にない場合は、MID サーバーを使用する必要があります。インスタンスの MID サーバーの詳細については、「MID サーバー」を参照してください。 • IntegrationHub プラグインがンストールされ、アクティブ化されていることを確認します。このプラグインにより、ベースシステムコンポーネントが統合 API を使用して外部システムを呼び出せるようになり、REST などのプロトコルステップをアクティブ化します。 次のように移動する。 システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて) をクリックし、プラグインを見つけます。インスタンスにインストールされていない場合は、インストールしてアクティブ化します。
	Tenable 資格証明を取得します。 Tenable 製品にアクセスするために必要なアカウント名、パスワード、その他のサービス情報があることを確認します。 Tenable.io には 64 以上の権限属性を持つアドミニストレーターアクセスが必要です。Tenable.sc にはセキュリティアナリストまたはマネージャーアクセスが必要です。 **注:** Vulnerability Response Integration with Tenable の v3.8 以降、Tenable.io へのアクセスにアドミン権限は不要になりました。権限属性が 16 に等しい基本ユーザーも製品にアクセスできます。

これで、「セットアップアシスタントを使用して、Vulnerability Response Integration with Tenable アプリケーションをインストールします。」に進む準備が整いました。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

セットアップアシスタントを使用して、**Vulnerability Response Integration with Tenable** アプリケーションをインストールします。

ServiceNow® Tenable 脆弱性統合を実行する前に、ServiceNow Store から Vulnerability Response Integration with Tenable アプリケーションをダウンロードし、脆弱性対応 アプリケーションのセットアップアシスタントを使用してインストールおよび構成する必要があります。

始める前に

Tenable アプリケーションをインストールする前に、「Tenable 脆弱性統合の準備」のチェックリストのすべてのアイテムを完了していることを確認します。

> **注:**
> このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

必要なロール：sn_vul.vulnerability_admin ロールを最初にアサインし、セットアップアシスタントで Tenable アプリケーションをインストールするアドミン。インストール後に、セットアップアシスタントでアプリケーションを構成する脆弱性アドミンロール (sn_vul.vulnerability_admin または sn_vul.admin (使用廃止))。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合アプリケーションのインストール.

   しばらくすると、インスタンスにインストールできるアプリケーションが表示されます。

2. **Tenable (Tenable** プラットフォーム) タイルを見つけて、[インストール] をクリックします。

   このアクションにより、ServiceNow Store からダウンロードした Vulnerability Response Integration with Tenable アプリケーションがインストールされます。

3. セットアップアシスタントで表示されるプロンプトに従い、インストールを続行します。
4. セットアップアシスタントを使用したアプリケーションのインストールの詳細については、「セットアップアシスタントを使用した 脆弱性対応 サードパーティアプリケーションのインストール」を参照してください。

次のタスク

セットアップアシスタントでインストールを完了したら、セットアップアシスタントで [統合設定] > [スキャナー統合] に移動して、構成を続行します。セットアップアシスタントで表示されるプロンプトを補足する詳細情報を確認する場合は、「セットアップアシスタントを使用した Tenable 脆弱性統合の構成」を参照してください。

Tenable 脆弱性統合のデータ検索設定

次のデータ検索設定は、ServiceNow® Tenable 脆弱性統合から Now Platform® インスタンスにインポートするデータのタイプとスコープを具体的に決定するのに役立ちます。

次のセクションで説明する設定は、インポートするデータを制御するのに役立ちます。さらに、これらのフィルターの値は統合インスタンスで設定できます。統合インスタンスを表示するには、次に移動します: **Tenable** 脆弱性統合 > 統合インスタンス をクリックし、統合、 Tenable.io 、または Tenable.scをクリックします。

表示される [統合インスタンス] ページで、[統合インスタンスパラメータ] をクリックして、パラメーターのリストを表示するか、[脆弱性統合] タブでスケジュール、REST 詳細、統合の詳細、データソース、および統合実行情報を表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Now Platform インスタンスの **Tenable.io** および **Tenable.sc** の一般的な重大度と取得の設定およびフィルター

次の設定は、Now Platform インスタンスの Tenable.io および Tenable.sc 統合で使用できます。これらの構成設定およびその他の構成設定は、Now Platform インスタンスの [統合インスタンス] ページに表示されます。最初の数回の実行では、これらの設定をデフォルトのままにすることをお勧めします。

Tenable.io

insert_fixed

脆弱性インポート統合のセットアップアシスタントで **insert_fixed** フラグを有効にすると、インスタンスにまだ存在しない [修正済み] ステータスの検出に対して新しい VI が作成されます。

severity_critical

このフィルターは、Tenable.io のオープンな脆弱性統合と Tenable.io の修正された脆弱性統合から最重要の重大度の脆弱性を受信できるようにデフォルトで有効になっています (true)。

severity_high

このフィルターは、Tenable.io のオープンな脆弱性統合と Tenable.io の修正された脆弱性統合から高レベルの重大度の脆弱性を受信できるようにデフォルトで有効になっています (true)。

severity_medium

このフィルターは、デフォルトでは非アクティブです (false)。Tenable.io のオープンな脆弱性統合と Tenable.io の修正された脆弱性統合から中レベルの重大度の脆弱性を受信するには、このフィルターを有効にします。

severity_info

このフィルターは、デフォルトでは非アクティブです (false)。Tenable.io のオープンな脆弱性統合と Tenable.io の修正された脆弱性統合から情報レベルの重大度の脆弱性を受信するには、このフィルターを有効にします。

severity_low

このフィルターは、デフォルトでは非アクティブです (false)。Tenable.io のオープンな脆弱性統合と Tenable.io の修正された脆弱性統合から低レベルの重大度の脆弱性を受信するには、このフィルターを有効にします。

size

この設定では、Tenable.io プラグイン統合からの結果セットに含めるプラグインレコードの数を定義します。int32 形式である必要があります。デフォルト値は 1,000 です。最大サイズは 10,000 です。

num_assets

Tenable.io の修正された脆弱性統合と Tenable.io のオープンな脆弱性統合からエクスポートされたチャンクあたりの脆弱性の最大数。デフォルト値は 50 です。

chunk_size

Tenable.io 資産統合によってエクスポートされたチャンクあたりの資産数を指定します。デフォルトは 1,000 です。

Tenable.sc

async_request

このパラメーターは、デフォルトでは非アクティブです (false)。Tenable.sc を使用して非同期または同期 API コールを実行するには、このパラメーターを有効または無効にします。同期呼び出しで 30 秒でタイムアウトする場合は、Tenable 製品の

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サポートに連絡してボックスを調整してください。このパラメーターを有効にすると、Tenable.sc のすべての統合に適用されます。既存の顧客が非同期呼び出しを使用している場合は、既存の Tenable.sc 統合インスタンスに新しい async_request パラメーターを追加する修正スクリプトを利用できます。修正スクリプトを表示するには、次に移動します: システム定義 > 修正スクリプト.

insert_fixed

脆弱性インポート統合のセットアップアシスタントで **insert_fixed** フラグを有効にすると、インスタンスにまだ存在しない [修正済み] ステータスの検出に対して新しい VI が作成されます。

offset

1 回の統合実行でインポートされる資産、プラグイン、および脆弱性の数を指定します。

クエリフィルター

クエリフィルターは、Tenable コンソール内から構成されます。これらのクエリフィルターには、セットアップアシスタントまたは Now Platform インスタンスの [統合インスタンス] ページから選択できる ID があります。これらのフィルターは、Tenable.sc 統合からデータを取得するときに適用されます。

Tenable 脆弱性統合の **REST** メッセージ

ServiceNow® Tenable 脆弱性統合 REST メッセージは、Tenable API の呼び出しに使用されます。

Tenable.io 資産 **REST** メッセージ

Tenable.io 資産 REST メッセージは、Tenable.io 資産統合の資産情報を取得します。REST メッセージメソッドレコードを変更すると、資産情報を取得するための Tenable.io への要求が影響を受けます。資産のエクスポートジョブは、次のフィルターを使用して送信されます。

- "is_deleted"：false
- "is_licensed"：true

Tenable.io プラグイン **REST** メッセージ

Tenable.io プラグイン REST メッセージは、Tenable.io プラグイン統合のプラグイン情報を取得します。REST メッセージメソッドレコードを変更すると、プラグイン情報を取得するための Tenable.io への要求が影響を受けます。

Tenable.io 脆弱性 **REST** メッセージ

Tenable.io 脆弱性 REST メッセージは、Tenable.io 脆弱性統合からオープンとクローズ済みの両方の脆弱性の脆弱性情報を取得します。REST メッセージメソッドレコードを変更すると、脆弱性情報を取得するための Tenable.io への要求が影響を受けます。

Tenable.sc クエリ **REST** メッセージ

Tenable.sc クエリ REST メッセージは、クエリフィルターが構成されている Tenable.sc 資産統合および Tenable.sc 脆弱性統合のクエリフィルター情報を取得します。

Tenable.sc プラグイン **REST** メッセージ

Tenable.sc プラグイン REST メッセージは、Tenable.sc プラグイン統合のプラグイン情報を取得します。REST メッセージ Get プラグインメソッドレコードを変更すると、プラグイン情報を取得するための Tenable.sc への要求が影響を受けます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

パラメーター名	値	説明
type	active	Tenable がデータをプルするソースを示します。コードで使用されます。変更は推奨されません。
fields	id、description、cvssVector、cvssV3Vector、cvssV3TemporalVector、sync	Tenable からインポートされたフィールドのリストを示します。

Tenable.sc 脆弱性 REST メッセージ

Tenable.sc 脆弱性 REST メッセージは、Tenable.sc 統合から脆弱性情報を取得します。REST メッセージの [脆弱性をフェッチ (Fetch Vulnerabilities)] または [パッチが適用された脆弱性をフェッチ (Fetch Patched Vulnerabilities)] メソッド (v14.0 の 脆弱性対応 および Tenable 脆弱性統合の v2.2 以降の場合は、[バックフィル脆弱性のフェッチ (Fetch Backfill Vulnerabilities)] レコード) を変更すると、脆弱性情報を取得するための Tenable.sc への要求が影響を受けます。

Tenable.sc スキャン認証情報 REST メッセージ

Tenable.sc ポリシー REST メッセージ

Tenable.sc ポリシーの POST REST メッセージは、要求されたプラグインのポリシーを追加します。生成されたポリシーは Tenable.sc スキャン要求で使用されます。

Tenable.sc スキャン REST メッセージ

Tenable.sc スキャン POST REST メッセージは、REST メッセージの要求本文で定義されたアクセスと権限に依存するスキャンを追加します。スキャン要求の要求本文でポリシー、プラグイン ID、および IP を使用します。

Tenable.sc スキャン結果 REST メッセージ

Tenable.sc スキャン結果 GET REST メッセージは、スキャン REST メッセージを使用して生成されたスキャンの詳細を提供します。スキャン REST メッセージの応答で scanResultId を使用し、トリガーされたスキャンの詳細を取得します。

Tenable.sc スキャン認証情報

Tenable.sc スキャン認証情報 REST メッセージは、Tenable.sc から認証情報を取得します。REST メッセージ「Import」メソッドレコードを変更すると、認証情報を取得するための Tenable.sc への要求が影響を受けます。

パラメーター名	値	説明
fields	id、name、description、type	Tenable.sc からインポートされたフィールドのリストを示します。
filter	usable	統合が Tenable.sc から使用可能な認証情報のみをプルすることを示します。 どちらのパラメーターも変更しないことをお勧めします。

Tenable 脆弱性統合のデータ変換

インポートするデータを特定すると、Tenable 製品からデータが取得され、インスタンス内の一連のデータソースと変換によって処理されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

インストール時に、正規化された重大度マップが [正規化された重大度マッピング (Normalized Severity Mapping)] モジュールにインストールされます。これらのマップ変換では、Tenable 重大度レベルを標準の重大度レベルにインポートし、インスタンス処理します。重大度マップの作成については、脆弱性対応 ドキュメントの Vulnerability Response 重大度マップの作成についてを参照してください。

Tenable.io 資産インポート

インポートされた資産データは、最初に Tenable.io 資産インポート [sn_vul_tenable_io_asset_import] テーブルにロードされます。

Tenable.io 資産統合変換マップは、インポートされた資産情報の変換に使用されます。この変換を変更すると、Tenable 資産インポートからのデータの処理方法が変更されます。この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ. 「Tenable.io Asset Transform」を検索します。

次の表に、統合別の変換マップフィールドを示します。

Tenable.io 資産変換マップのフィールド

ソースフィールド	ターゲットフィールド	説明
u_id	source_id	Tenable は資産の一意の ID を提供して、検出されたアイテムレコードにマッピングし、CI ルックアップに使用されます。
u_ipv4s	ip_address	最初の ip 値を検出されたアイテムレコードの ip_address フィールドにマッピングします。
u_mac_addresses	mac_address	最初の mac_address 値を検出されたアイテムレコードの mac_address フィールドにマッピングします。
u_fqdns	fqdn	最初の fqdn 値を検出されたアイテムレコードの fqdn フィールドにマッピングします。
u_netbios_names	netbios	最初の netbios 値を検出されたアイテムレコードの netbios フィールドにマッピングします。
u_operating_systems	os	最初の OS 値を検出されたアイテムレコードの os フィールドにマッピングします。
(v 14.0 の 脆弱性対応 および v2.2 の Tenable 脆弱性統合より前)u_last_scan_time	last_scan_date	検出されたアイテムレコードの last_scan_date フィールドにマッピングします。
u_last_authenticated_scan_date	last_auth_scan_date	検出されたアイテムレコードの last_auth_scan_date フィールドにマッピングします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.io 資産変換マップのフィールド (続く)

ソースフィールド	ターゲットフィールド	説明
[script]	name	スクリプトのロジックを使用してホスト名をマッピングします。
u_tags		タグは sn_sec_cmn_host_tag に保存されます。タグから資産へのマッピングは sn_sec_cmn_m2m_src_ci_tag に保存されます。

変換プロセスでは、3 つの変換スクリプトが実行されます。次の表に、各スクリプトが実行されるタイミングとその目的を示します。

Tenable.io 資産変換マップスクリプトのタイミングと目的

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	この変換は、統合プロセスの import_set の値を初期化するために使用されます。内部使用。変更または削除することはお勧めしません。
onBefore (インポートセットの変換が完了する前)。	ホストの値を更新し、ホストが既に存在するかどうかを確認するために使用される機能。結果に基づいて、import_set の値を変更します。内部使用。変更または削除することはお勧めしません。
onComplete (インポートセットが変換を完了したとき)	この変換は、作成された新しい CI と更新されて無視された CI の値を設定するために使用されます。内部使用。変更または削除することはお勧めしません。

Tenable.io プラグイン統合

Tenable.io プラグイン変換マップは、Tenable.io からインポートされたプラグインを変換するために使用されます。

注:
この変換マップを変更すると、Tenable プラグインから取得するデータの処理方法が変更されます。

この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ. Tenable.io プラグイン変換を検索します。

Tenable.io プラグインのペイロードには、sn_vul_tenable_io_plugin_import テーブルの u_attributes 列のすべてのフィールドが含まれます。次の表に示すように、属性フィールドが解析され、サードパーティのエントリーテーブルレコードにマッピングされます。

ソースフィールド	ターゲットフィールド	説明
id	id	ソースから ID をマッピングし、TEN プリフィックスを追加します。たとえば、受信

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ソースフィールド	ターゲットフィールド	説明
		した ID が 12345 の場合、ターゲットテーブルの ID は TEN-12345 です。
説明	summary	プラグインの説明を summary 列にマッピングします。
[script]	source	インポートされた TPE のソースは Tenable.io です。
[script]	source_instance	このレコードをインポートする Tenable 展開への参照
family	category	プラグインのファミリを category 列にマッピングします。
plugin_modification_date	last_modified	plugin_modification_date を最後に変更されたフィールドにマッピングします。
plugin_publication_date	date_published	plugin_publication_date を公開日にマッピングします。
has_patch	remediation_type	has_patch 値から修復タイプをマッピングします。
synopsis	threat	この脆弱性に関する脅威情報をマッピングします。
cvss_base__score	score	cvss ベーススコアをサードパーティのエントリーテーブルの score 列にマッピングします。
solution	solution	スキャナーによって提供されたソリューションをサードパーティのエントリーテーブルの solution 列にマッピングします。
exploit_available	exploit	スキャナーによって提供された exploit_available をサードパーティのエントリーテーブルの exploit 列にマッピングします。
vpr.score	source_risk_score	スキャナーによって提供された vpr スコアをサードパーティのエントリーテーブルの source_risk_score にマッピングします。
[script]	source_risk_rating	スコア範囲に基づいて、vpr スコアを標準リスク評価にマッピングします。 • 9 ～ 10 - 重大 • 7 ～ 9 – 高

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
		• 4 ～ 7 - 中 • 0 ～ 4 - 低
vpr.drivers.age_of_vuln	age_of_vuln	スキャナーからの脆弱性の経過時間をサードパーティのエントリーテーブルの age_of_vuln 列にマッピングします。
vpr.drivers.exploit_code_maturity	exploit_code_maturity	スキャナーからのエクスプロイトコードの成熟度をサードパーティのエントリーテーブルの exploit_code_maturity にマッピングします。
vpr.drivers.product_coverage	product_coverage	スキャナーからの製品範囲をサードパーティのエントリーテーブルの product_coverage にマッピングします。
vpr.drivers.threat_sources_last28	threat_sources	スキャナーからの過去 28 日間の脅威ソースをサードパーティテーブルの threat_sources にマッピングします。
vpr.drivers.threat_intensity_last28	threat_intensity	スキャナーからの過去 28 日間の脅威の強さをサードパーティのエントリーテーブルの threat_intensity にマッピングします。
vpr.drivers.threat_recency	threat_recency	スキャナーからの脅威の最新性情報をサードパーティのエントリーテーブルの threat_recency にマッピングします。
vpr.drivers.cvss3_impact_score	v3_impact_subscore	cvss3 影響スコアをサードパーティのエントリーテーブルの v3_impact_subscore 列にマッピングします。
cvss_temporal_score	cvss_temporal_score	CVSS v2 の一時スコアをマッピングします。
cvss_v3_temporal_score	v3_temporal_score	CVSS v3 の一時スコアをマッピングします。
risk_factor	source_severity	サードパーティのエントリーテーブルのソース重大度にマッピングします。
name	name	プラグインの名前をサードパーティのエントリーテーブルの名前にマッピングします。
stig_severity	stig_severity	スキャナーによって提供された vpr スコアをサードパーティのエントリーテーブルの

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
		source_risk_score にマッピングします。
plugin_type	check_type	プラグインタイプをサードパーティのエントリーテーブルの check_type にマッピングします。
unsupported_by_vendor	unsupported_by_vendor	unsupported_by_vendor フィールドを unsupported_by_vendor 列にマッピングします。
[script]	exploit_attack_vector	サードパーティのエントリーテーブルの exploit_attack_vector 列は、列の exploit_available と v3_attack_vector に基づいて入力されます。

direct フィールドに加えて、その他の情報が関連リストとしてサードパーティのエントリーに追加されます。

ソースフィールド	説明
cve	CVE 関連データを参照テーブル (sn_vul_nvd_entry) に挿入します。NVD エントリーテーブル (sn_vul_nvd_entry) で同じ CVE が見つかった場合、現在の脆弱性が NVD エントリーに関連付けられます。マッピングは sn_vul_m2m_entry_cve にあります。
bid	バグトラックのリストが参照として追加されます。
see_also	URL のリストが参照として追加されます。
xref	X-REF のリストが参照として追加されます。
[script]	そのプラグインのエクスプロイトのリスト。該当するエクスプロイトフレームワークとプラグインの sn_vul_m2m_framework_vul へのマッピングを挿入します。

変換プロセスでは、3 つの変換スクリプトが実行されます。次の表に、各スクリプトが実行されるタイミングとその目的を示します。

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	この変換は、統合プロセスの import_set の値を初期化するために使用されます。内部使用。変更または削除することはお勧めしません。
onBefore (インポートセットの変換が完了する前)。	サードパーティエントリーの値を更新し、サードパーティエントリーが既に存在するかどうかを確認するために使用される機能。結果に基づいて、サードパーティエントリーの値を変更し

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

スクリプトが実行されるタイミング	目的
	ます。内部使用。変更または削除することはお勧めしません。
onComplete (インポートセットが変換を完了したとき)	この変換は、作成された新しい CI と更新されて無視された CI の値を設定するために使用されます。内部使用。変更または削除することはお勧めしません。

TenableIOPluginsImportProcessor スクリプトインクルードは onBefore 変換スクリプトから呼び出されます。Tenable.io プラグイン統合からの出力を取得し、Now Platform サードパーティの脆弱性エントリーに変換します。このスクリプトインクルードを変更すると、サードパーティのエントリーテーブルの Tenable.io プラグインデータの変換が変更される可能性があります。

Tenable.io 脆弱性のインポート

Tenable.io 脆弱性一致アイテム変換マップは、Tenable.io からインポートされたオープンおよび修正された脆弱性情報を変換するために使用されます。

注:
この変換マップを変更すると、Tenable 脆弱性インポートからのデータの処理方法が変更されます。

Tenable.io の修正された脆弱性統合と Tenable.io のオープンな脆弱性統合の両方に同じ変換マップが使用されます。この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ. 「Tenable.io Vulnerable Item transform map」を検索します。

ソースフィールド	ターゲットフィールド	説明
u_asset.uuid	id	uuid は cmdb_ci レコードの id フィールドにマッピングされます。
u_asset.ipv4	ip_address	ipv4 フィールドは cmdb_ci レコードの ip_address フィールドにマッピングされます。
u_asset .last_authenticated_results	last_auth_scan_date	前回の認証済みスキャン日は、cmdb_ci レコードの前回の認証済みスキャン日にマッピングされます。
u_asset.mac_addess	mac_address	MAC アドレスは cmdb_ci レコードの host mac address フィールドにマッピングされます。
u_asset.netbios_name	netbios	netbios は、cmdb_ci レコードの netbios フィールドにマッピングされます。
u._plugin.cvss3_base_score	v3_base_score	CVSS v3 ベーススコアは、サードパーティのエントリーレコードの v3 ベーススコアにマッピングされます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ソースフィールド	ターゲットフィールド	説明
u._plugin.cvss3_temporal_score	v3_temporal_score	CVSS v3 一時スコアは、サードパーティのエントリーレコードの v3 一時スコアにマッピングされます。
u._plugin.cvss_base_score	score	CVSS ベーススコアは、サードパーティのエントリーレコードの score フィールドにマッピングされます。
u._plugin.cvss_temporal_score	temporal_score	一時スコアは、サードパーティのエントリーレコードの一時スコアにマッピングされます。
u_plugin.description	summary	説明は、サードパーティのエントリーレコードの summary フィールドにマッピングされます。
u_plugin.family	category	プラグインのファミリをサードパーティのエントリーレコードの category 列にマッピングします。
u_plugin.modification_date	last_modified	最終変更日は、サードパーティのエントリーレコードのプラグインの最終変更日にマッピングされます。
u_plugin.publication_date	date_published	公開日は、サードパーティのエントリーレコードの date_published フィールドにマッピングされます。
u_plugin.risk_factor	source_severity	リスク要因は、サードパーティのエントリーレコードの source_severity フィールドにマッピングされます。
u_plugin.solution	solution	ソリューションは、サードパーティのエントリーレコードの solution フィールドにマッピングされます。
u_plugin.synopsis	threat	概要は、サードパーティのエントリーレコードの threat フィールドにマッピングされます。
u_severity_id	priority	優先度は、ペイロードの重大度 ID にマッピングされます。デフォルト値は 5 です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
u_plugin.exploit_available	exploit	スキャナーによって提供された exploit_available をサードパーティのエントリーテーブルの exploit 列にマッピングします。
vpr.score	source_risk_score	スキャナーによって提供された vpr スコアをサードパーティのエントリーテーブルの source_risk_score にマッピングします。
[script]	source_risk_rating	スコア範囲に基づいて、vpr スコアを標準リスク評価にマッピングします。 • 9 ～ 10 - 重大 • 7 ～ 9 – 高 • 4 ～ 7 - 中 • 0 ～ 4 - 低
u_plugin.vpr.drivers.age_of_vuln	age_of_vuln	スキャナーからの脆弱性の経過時間をサードパーティのエントリーテーブルの age_of_vuln にマッピングします。
u_plugin.vpr.drivers.exploit_code_maturity	exploit_code_maturity	スキャナーからのエクスプロイトコードの成熟度をサードパーティのエントリーテーブルの exploit_code_maturity にマッピングします。
u_plugin.vpr.drivers.product_coverage	product_coverage	スキャナーからの製品範囲をサードパーティのエントリーテーブルの product_coverage にマッピングします。
u_plugin.vpr.drivers.threat_sources_last28	threat_sources	スキャナーからの過去 28 日間の脅威ソースをサードパーティのエントリーテーブルの threat_sources にマッピングします。
u_plugin.vpr.drivers.threat_intensity_last28	threat_intensity	スキャナーからの過去 28 日間の脅威の強さをサードパーティのエントリーテーブルの threat_intensity にマッピングします。
u_plugin.vpr.drivers.threat_recency	threat_recency	スキャナーからの脅威の最新性情報をサードパーティのエントリーテーブルの

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
		threat_recency にマッピングします。
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	CVSS3 v3 影響スコアをサードパーティのエントリーテーブルの v3_impact_subscore 列にマッピングします。
u_plugin.type	check_type	プラグインタイプをサードパーティのエントリーテーブルの check_type にマッピングします。
u_plugin.unsupported_by_vendor	unsupported_by_vendor	プラグインの unsupported_by_vendor フィールドを unsupported_by_vendor 列にマッピングします。
[script]	exploit_attack_vector	サードパーティのエントリーテーブルの exploit_attack_vector 列は、列の exploit_available と v3_attack_vector に基づいて入力されます。
u_plugin.family_id	family_id	プラグインのファミリ ID をサードパーティのエントリーテーブルの family_id 列にマッピングします。
port	port	ポートは、脆弱性一致アイテムレコードの port フィールドにマッピングされます。
protocol	protocol	プロトコルは、脆弱性一致アイテムレコードの protocol フィールドにマッピングされます。
u_first_found	first_found	初回検出は、脆弱性一致アイテムレコードの first_found フィールドにマッピングされます。
u_last_found	last_found	前回検出は、脆弱性一致アイテムレコードの last_found フィールドにマッピングされます。
u_state	state	ステータスは、脆弱性一致アイテムレコードの [ステータス (State)] フィールドにマッピングされます。
[script]	source	統合のソースが入力されます。この統合から作成さ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
		れた脆弱性一致アイテムには、Tenable.io がソースとして含まれています。
[script]	integration_instance	integration_instance は、脆弱性一致アイテムのインポート元のインスタンスの名前です。
u_plugin.name	name	プラグインの名前をサードパーティのエントリーテーブルの名前にマッピングします。
u_plugin.stig_severity	stig_severity	プラグインの stig 重大度をサードパーティのエントリーテーブルの stig_severity 列にマッピングします。

direct フィールドに加えて、その他の情報が関連リストとしてサードパーティのエントリーに追加されます。

ソースフィールド	説明
cve	CVE 関連データを参照テーブル (sn_vul_nvd_entry) に挿入します。NVD エントリーテーブル (sn_vul_nvd_entry) で同じ CVE が見つかった場合、現在の脆弱性が NVD エントリーに関連付けられます。マッピングは sn_vul_m2m_entry_cve にあります。
bid	バグトラックのリストが参照として追加されます。
see_also	URL のリストが参照として追加されます。
xref	X-REF のリストが参照として追加されます。
[script]	そのプラグインのエクスプロイトのリスト。該当するエクスプロイトフレームワークとプラグインの sn_vul_m2m_framework_vul へのマッピングを挿入します。

変換プロセスでは、3 つの変換スクリプトが実行されます。次の表に、各スクリプトが実行されるタイミングとその目的を示します。

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	この変換は、インポートセットを使用して Tenable.io からデータをインポートする TenableIOVulnerabilitiesProcessor をトリガーし、各レコードを CMDB CI テーブル、脆弱性一致アイテムテーブル、およびサードパーティ脆弱性テーブルに内部使用のためにロードします。変更または削除することはお勧めしません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スクリプトが実行されるタイミング	目的
onBefore (インポートセットの変換が完了する前)。	サードパーティのエントリーと検出が既に存在するかどうかを確認する機能。そうでない場合、これらのレコードはそれぞれのテーブルに作成されます。内部使用。変更または削除することはお勧めしません。
onComplete (インポートセットが変換を完了したとき)	この変換は、Tenable.io からインポートされた CI、VI および検出の数を更新するのに使用されます。内部使用。変更または削除することはお勧めしません。

Tenable.sc 資産インポート

Tenable.sc からインポートされた資産データは、最初に Tenable.sc 資産インポートテーブル (sn_vul_tenable_sc_asset_import) にロードされます。Tenable.sc 資産統合変換マップは、インポートされた資産情報の変換に使用されます。この変換を変更すると、Tenable 資産インポートからのデータの処理方法が変更されます。この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ. 「Tenable.sc Asset Transform」を検索します。

ソースフィールド	ターゲットフィールド	説明
u_uuid	id	uuid は Tenable API から入力されないため、「u_uniqueness」属性を使用して資産の一意の uuid フィールドを作成し、それを cmdb_ci レコードにマッピングします。
u_ip	ip_address	API からの ip フィールドを cmdb_ci レコードの ip_address フィールドにマッピングします。
u_macaddress	mac_address	API からの macaddress フィールドを cmdb_ci レコードの address フィールドにマッピングします。
u_dnsname	fqdn	API からの dnsname フィールドを cmdb_ci レコードの fqdn フィールドにマッピングします。
u_netbiosname	netbios	API からの netbios フィールドを cmdb_ci レコードの netbios フィールドにマッピングします。
u_oscpe	os	OS 情報はペイロードの oscpe 属性から抽出され、cmdb_ci レコードの os フィールドにマッピングされます。
u_lastauthrun	last_auth_scan_date	API からの lastauthrun フィールドを、検出されたアイテムレコードの last_auth_scan_date

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
		フィールドにマッピングします。
u_lastauthrun および u_lastunauthrun	last_scan_date	lastauthrun は、Tenable API または lastunauthrun から抽出されます。検出されたアイテムレコードの last_scan_date フィールドは、ペイロードに表示される値に基づいて入力されます。

変換プロセスでは、3 つの変換スクリプトが実行されます。次の表に、各スクリプトが実行されるタイミングとその目的を示します。

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	この変換は、統合プロセスの import_set の値を初期化するために使用されます。内部使用。変更または削除することはお勧めしません。
onBefore (インポートセットの変換が完了する前)。	ホストの値を更新し、ホストが既に存在するかどうかを確認するために使用される機能。結果に基づいて、import_set の値を変更します。内部使用。変更または削除することはお勧めしません。
onComplete (インポートセットが変換を完了したとき)	この変換は、作成された新しい CI と更新されて無視された CI の値を設定するために使用されます。内部使用。変更または削除することはお勧めしません。

Tenable.sc プラグインのインポート

Tenable.sc からインポートされたプラグインデータは、最初に Tenable.sc プラグインインポートテーブル (sn_vul_tenable_sc_plugin_import) にロードされます。Tenable.sc プラグイン変換マップは、インポートされたプラグイン情報の変換に使用されます。この変換を変更すると、Tenable プラグインインポートからのデータの処理方法が変更されます。この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ. 「Tenable.sc Plugin Transform Map」を検索します。

ソースフィールド	ターゲットフィールド	説明
u_id	id	ソースから ID をマッピングし、TEN プリフィックスを追加します。たとえば、受信した ID が 12345 の場合、ターゲットテーブルの ID は TEN-12345 です。
u_description	summary	プラグインの説明を summary 列にマッピングします。
[script]	source	この統合からインポートされた TPE には、Tenable.sc がソースとして含まれています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ソースフィールド	ターゲットフィールド	説明
[script]	source_instance	このレコードをインポートする Tenable 展開への参照
u_family	category	プラグインのファミリオブジェクトの name フィールドを category 列にマッピングします。
u_plugin_modification_date	last_modified	plugin_modification_date を最後に変更されたフィールドにマッピングします。
u_plugin_publication_date	date_published	plugin_publication_date を公開日にマッピングします。
u_has_patch	remediation_type	has_patch 値から修復タイプをマッピングします。
u_synopsis	threat	この脆弱性に関する脅威情報をマッピングします。
u_cvss_base_score	score	CVSS ベーススコアをサードパーティのエントリーテーブルの score 列にマッピングします。
u_solution	solution	スキャナーによって提供されたソリューションをサードパーティのエントリーテーブルの solution 列にマッピングします。
u_cvss_temporal_score	cvss_temporal_score	CVSS v2 の一時スコアをマッピングします。
u_cvss_v3_temporal_score	v3_temporal_score	CVSS v3 の一時スコアをマッピングします。
u_risk_factor	source severity	サードパーティのエントリーテーブルのソース重大度にマッピングします。
u_cvss_v3_base_score	v3_base_score	サードパーティのエントリーテーブルの CVSS ベーススコアをマッピングします。
u_exploit_available	exploit	スキャナーによって提供された exploitAvailable をサードパーティのエントリーテーブルの exploit 列にマッピングします。
u_vpr_score	source_risk_score	スキャナーからの VPR スコアをサードパーティのエントリーテーブルのソースリスクスコアにマッピングします。
[script]	source_risk_rating	スコア範囲に基づいて、vpr スコアを標準リスク評価にマッピングします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
		• 9 ～ 10 - 重大 • 7 ～ 9 – 高 • 4 ～ 7 - 中 • 0 ～ 4 - 低
u_vpr_context[id=age_of_vuln]	age_of_vuln	スキャナーからの脆弱性の経過時間をサードパーティのエントリーテーブルの age_of_vuln にマッピングします。
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	スキャナーからのエクスプロイトコードの成熟度をサードパーティのエントリーテーブルの exploit_code_maturity にマッピングします。
u_vpr_context[id=product_coverage]	product_coverage	スキャナーからの製品範囲をサードパーティのエントリーテーブルの product_coverage にマッピングします。
u_vpr_context[id="threat_sources_last_28"]	threat_sources	スキャナーからの過去 28 日間の脅威ソースをサードパーティテーブルの threat_sources にマッピングします。
u_vpr_context[id="threat_intensity_last_28"]	threat_intensity	スキャナーからの過去 28 日間の脅威の強さをサードパーティのエントリーテーブルの threat_intensity にマッピングします。
u_vpr_context[id="threat_recency"]	threat_recency	スキャナーからの脅威の最新性情報をサードパーティのエントリーテーブルの threat_recency にマッピングします。
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	スキャナーからの CVSS v3 影響スコアをサードパーティのエントリーテーブルの v3_impact_subscore にマッピングします。
u_name	name	プラグインの名前をサードパーティのエントリーテーブルの name 列にマッピングします。
u_stig_severity	stig_severity	プラグインの stig_severity フィールドをサードパーティのエントリーテーブルの stig_severity にマッピングします。
u_check_type	check_type	チェックタイプをサードパーティのエントリーテーブルの

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
		check_type にマッピングします。
u_family.id	family_id	プラグインの family_id をサードパーティのエントリーテーブルの family_id にマッピングします。
[script]	exploit_attack_vector	サードパーティのエントリーテーブルの exploit_attack_vector 列は、列の exploit_available と v3_attack_vector に基づいて入力されます。

direct フィールドに加えて、その他の情報が関連リストとしてサードパーティのエントリーに追加されます。

ソースフィールド	説明
u_cpe	CPE のリストが参照として追加されます。
u_see_also	URL のリストが参照として追加されます。
u_exploit_frameworks	そのプラグインのエクスプロイトのリスト。該当するエクスプロイトフレームワークとプラグインの sn_vul_m2m_framework_vul へのマッピングを挿入します。

変換プロセスでは、3 つの変換スクリプトが実行されます。次の表に、各スクリプトが実行されるタイミングとその目的を示します。

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	この変換は、統合プロセスの import_set の値を初期化するために使用されます。内部使用。変更または削除することはお勧めしません。
onBefore (インポートセットの変換が完了する前)。	サードパーティエントリーの値を更新し、サードパーティエントリーが既に存在するかどうかを確認するために使用される機能。結果に基づいて、サードパーティエントリーの値を変更します。内部使用。変更または削除することはお勧めしません。
onComplete (インポートセットが変換を完了したとき)	この変換は、作成されて無視されたプラグインの値を設定するために使用されます。内部使用。変更または削除することはお勧めしません。

TenableSCPluginsImportProcessor スクリプトインクルードは onBefore 変換スクリプトから呼び出されます。Tenable.sc プラグイン統合からの出力を取得し、Servicenow サードパーティの脆弱性エントリーに変換します。このスクリプトインクルードを変更すると、サードパーティのエントリーテーブルの Tenable.sc プラグインデータの変換が変更される可能性があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.sc 脆弱性インポート

Tenable.sc のオープンな脆弱性変換マップは、Tenable.sc のオープンな脆弱性統合からインポートされたデータを変換するために使用され、Tenable.sc および修正された脆弱性変換マップは、Tenable.sc の修正された脆弱性統合からインポートされたデータを変換するために使用されます。

注:
これらの変換マップを変更すると、[修正済み]/[オープン] の Tenable 脆弱性インポートからのデータの処理方法が変更されます。

Tenable.sc オープンおよび修正された脆弱性変換マップにアクセスするには、次に移動します: **Tenable** 脆弱性統合 > アドミニストレーション > 統合インスタンス > **Tenable.sc** 修正済み/オープンな脆弱性統合 > データソース > オープン/修正された脆弱性 **Tenable.sc** > 変換.

ソースフィールド	ターゲットフィールド	説明
u_pluginID	Id	プラグインの識別子として使用されます。このフィールドは、サードパーティのエントリーレコードの plugin Id にマッピングされます。
u_riskfactor	source_severity	このフィールドは、サードパーティのエントリーレコードの source_severity にマッピングされます。
u_severity	priority	priority フィールドは重大度にマッピングされます。デフォルト値は 5 です。
u_hasbeenmitigated	state	hasbeenmitigated は、脆弱性レコードの [ステータス (State)] フィールドにマッピングされます。修正された脆弱性統合では、すべての VI が [クローズ済み] ステータスになっています。
u_ip	ip_address	IP アドレスは、cmdb_ci テーブルの host ip フィールドにマッピングされます。
u_port	port	ポートは、脆弱性一致アイテムレコードの port フィールドにマッピングされます。
u_protocol	protocol	プロトコルは、脆弱性一致アイテムレコードの port フィールドにマッピングされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
u_firstSeen	first_found	初回検出値は、VI レコードの first_found フィールドにマッピングされます。
u_lastSeen	last_found	前回検出値は、VI レコードの last_found フィールドにマッピングされます。
u_exploitAvailable	exploit	exploitAvailable は、サードパーティのエントリーレコードの exploit フィールドにマッピングされます。
u_synopsis	threat	概要は、サードパーティのエントリーレコードの threat フィールドにマッピングされます。
u_description	summary	説明は、サードパーティのエントリーレコードの summary フィールドにマッピングされます。
u_solution	solution	ソリューションは、サードパーティのエントリーレコードの solution フィールドにマッピングされます。
u_basescore	score	baseScore は、サードパーティのエントリーレコードの score フィールドにマッピングされます。
u_temporalScore	temporal_score	一時スコアは、サードパーティのエントリーレコードの一時スコアにマッピングされます。
u_cvssv3basescore	v3_base_score	cvssv3basescore は、サードパーティのエントリーレコードの v3_base_score にマッピングされます。
u_cvsstemporalscore	v3_temporal_score	cvssv3temporal スコアは、サードパーティのエントリーレコードの v3_temporal_score にマッピングされます。
u_pluginpubdate	date_published	プラグイン公開日は、サードパーティのエントリーレコードのプラグイ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
		ン公開日にマッピングされます。
u_pluginmoddate	last_modified	最終変更日は、サードパーティのエントリーレコードのプラグインの最終変更日にマッピングされます。
u_dnsname	fqdn	dnsName は cmdb_ci レコードの FQDN フィールドにマッピングされます。
u_macaddress	mac_address	macAddress は cmdb_ci レコードの mac_address フィールドにマッピングされます。
u_netbiosName	netbios	netbiosName は、cmdb_ci レコードの NETBIOS フィールドにマッピングされます。
u_ip	ip	IP は cmdb_ci レコードの IP フィールドにマッピングされます。
hostUniqueness	uuid	ホストの一意性はどのフィールドにもマッピングされませんが、ホストの uuid を決定するために使用されます。
u_family	category	プラグインのファミリオブジェクトの name フィールドをサードパーティのエントリーレコードの category 列にマッピングします。
u_plugintext	proof	プラグインテキストは tpe レコードの proof にマッピングされます。
[script]	source	統合のソースが入力されます。この統合から作成された脆弱性一致アイテムには、Tenable.sc がソースとして含まれています。
[script}	integration_instance	integration_instance は、脆弱性一致アイテムのインポート元のインスタンスの名前です。
u_vpr_score	source_risk_score	スキャナーからの VPR スコアをサードパーティ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
		のエントリーテーブルのソースリスクスコアにマッピングします。
[script]	source_risk_rating	スコア範囲に基づいて、vpr スコアを標準リスク評価にマッピングします。 • 9 ～ 10 - 重大 • 7 ～ 9 – 高 • 4 ～ 7 - 中 • 0 ～ 4 - 低
u_vpr_context[id=age_of_vuln]	age_of_vuln	スキャナーからの脆弱性の経過時間をサードパーティのエントリーテーブルの age_of_vuln にマッピングします。
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	スキャナーからのエクスプロイトコードの成熟度をサードパーティのエントリーテーブルの exploit_code_maturity にマッピングします。
u_vpr_context[id=product_coverage]	product_coverage	スキャナーからの製品範囲をサードパーティのエントリーテーブルの product_coverage にマッピングします。
u_vpr_context[id=”threat_sources_last_28]	threat_sources	スキャナーからの過去 28 日間の脅威ソースをサードパーティテーブルの threat_sources にマッピングします。
u_vpr_context[id=”threat_intensity_last_28]	threat_intensity	スキャナーからの過去 28 日間の脅威の強さをサードパーティのエントリーテーブルの threat_intensity にマッピングします。
u_vpr_context[id=”threat_recency”]	threat_recency	スキャナーからの脅威の最新性情報をサードパーティのエントリーテーブルの threat_recency にマッピングします。
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	スキャナーからの CVSS v3 影響スコアをサードパーティのエントリーテーブルの

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
		v3_impact_subscore にマッピングします。
u_pluginname	name	プラグインの名前をサードパーティのエントリーテーブルの name 列にマッピングします。
u_stigseverity	stig_severity	プラグインの stig_severity フィールドをサードパーティのエントリーテーブルの stig_severity にマッピングします。
u_checktype	check_type	チェックタイプをサードパーティのエントリーテーブルの check_type にマッピングします。
u_family.id	family_id	プラグインの family.id をサードパーティのエントリーテーブルの family_id にマッピングします。
[script]	exploit_attack_vector	third_party_entry テーブルの exploit_attack_vector 列は、列の exploit_available と v3_attack_vector に基づいて入力されます。

ソースフィールド	説明
u_cve	CVE 関連データを参照テーブル (sn_vul_nvd_entry) に挿入します。NVD エントリーテーブル (sn_vul_nvd_entry) で同じ CVE が見つかった場合、現在の脆弱性が NVD エントリーに関連付けられます。マッピングは sn_vul_m2m_entry_cve にあります。
u_bid	バグトラックのリストが参照として追加されます。
u_cpe	CPE のリストが参照として追加されます。
u_seealso	URL のリストが参照として追加されます。
u_xrefs	X-REF のリストが参照として追加されます。
u_exploitframeworks	そのプラグインのエクスプロイトのリスト。該当するエクスプロイトフレームワークとプラグインの sn_vul_m2m_framework_vul へのマッピングを挿入します。

変換プロセスでは、3 つの変換スクリプトが実行されます。次の表に、各スクリプトが実行されるタイミングとその目的を示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	この変換は、統合プロセスの import_set の値を初期化するために使用されます。内部使用。変更または削除することはお勧めしません。
onBefore (インポートセットの変換が完了する前)。	脆弱性の値を更新し、脆弱性が既に存在するかどうかを確認するために使用される機能。結果に基づいて、脆弱性一致アイテムテーブルの値を変更します。内部使用。変更または削除することはお勧めしません。
onComplete (インポートセットが変換を完了したとき)	この変換は、作成された新しい VI と更新されて無視された VI の値を設定するために使用されます。内部使用。変更または削除することはお勧めしません。

Tenable.io インポートの追加のフィルターパラメーターの設定

Tenable 脆弱性統合 を使用してスケジュール設定済みクエリのフィルタリングパラメーターをカスタマイズすると、Tenable.io 製品でインポートする脆弱性データをさらに絞り込むことができます。

始める前に

ユースケース：脆弱性マネージャーまたはアナリストは、特定の脆弱性の詳細のみを確認できるように、クエリからデータを除外できます。たとえば、*cidr_range*、*num_assets*、*indexed_at*、および *plugin_family* でフィルタリングされたインポート済み脆弱性を表示するとします。または、1 つは重大な脆弱性のみを 4 時間ごとにインポートし、もう 1 つは重大でない他のすべての脆弱性を 24 時間ごとにフェッチするなど、Tenable.io 統合を実行するとします。

このデータを収集するには、Tenable サポートのパラメーターを追加して、必要な特定の脆弱性の詳細をインポートします。

この機能を使用すると、API コールを追加したり追加のコーディングをしたりすることなく、Now Platform の Tenable パラメーターを使用して HTTP 要求情報をカスタマイズできます。次の Tenable.io 統合は、要求本文に JSON コンテンツを指定することによってフィルタリングをサポートしています。

- 資産統合
- 修正された脆弱性統合
- オープンな脆弱性統合

この機能の JSON 文字列の使用方法を理解している必要があります。

必要なロール：sn_vul.vulnerability_admin

手順

1. フィルタリングに使用する開発者サイトで、Tenable.io 製品でサポートされているパラメーターを見つけます。

   Tenable.io 製品から入力するパラメーターと値は、統合インスタンスレベルでのみサポートされます。

2. 次のように移動する。 **All** (すべて) > **Tenable** 脆弱性統合 > アドミニストレーション > 統合.
3. [Tenable 統合] リストページで、開く Tenable.io 統合のレコードをクリックします。
4. [Tenable REST メソッド (Tenable REST methods)] タブを選択した状態で、REST メソッドの情報アイコン (I) を見つけてクリックし、続いて [レコードを開く] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

5. **[HTTP** 要求] タブを選択します。
6. レコードを編集するには、ページの上部にあるリンクをクリックします。レコードを編集するには、[ここ] をクリックします。
7. [コンテンツ] フィールドの REST メソッドレコードで、要求本文の一部として必要な JSON コンテンツを入力します。

   たとえば、インポートされた脆弱性の重大度パラメーターを Tenable.io 資産統合の重大度パラメーターを `{"filters": {"severity": ["critical"]}}` に設定すると、重大な脆弱性 (CVSS スコア 10.0) のみがインポートされます。

   複数のパラメーターを入力する場合は、各値を区切る方法の詳細について、Tenable.io ドキュメントを参照してください。
8. [更新] をクリックします。

Tenable 脆弱性統合レポート

脆弱性対応 ダッシュボードで脆弱性と脆弱性一致アイテムに関するレポートを表示します。

脆弱性対応 のワークスペースのデータの可視化

脆弱性対応 ワークスペースには、修復の進捗状況を監視するのに役立つデータの可視化が含まれています。脆弱性データの変更に応じて更新される動的なデータ表示で組織にとって重要なアクティブな脆弱性の数と重大度を表示することで、組織に対する脅威のレベルを判断できます。利用可能な動的なデータ表示方法の詳細については、「脆弱性対応 ワークスペース」、「Vulnerability Manager ワークスペース の探索」および「IT 修復ワークスペース の探索」を参照してください。

脆弱性対応 の前のバージョン

脆弱性対応概要ダッシュボード (脆弱性管理) では、脆弱性と脆弱性一致アイテムに関するエグゼクティブビューが用意されており、脆弱性アドミニストレーターが懸念事項をすばやく特定するのに役立ちます。脆弱性対応修復ダッシュボード (脆弱性修復) を使用すると、修復スペシャリストが担当するする修復タスクと脆弱性一致アイテムに集中できます。

詳細については、「デフォルトの 脆弱性対応 ダッシュボードを使用する」を参照してください。

必要なロール：修復オーナー

脆弱性対応アプリケーションでユーザーが実行および表示できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。

詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

ダッシュボードを表示するには、次に移動します: 脆弱性対応 > 修復の概要.

Tenable 脆弱性統合の統合実行状況チャート

[Tenable 統合実行状況] モジュールは、Tenable 統合実行のステータスをグラフィカルに表示します。

チャートで、グラフの任意の部分をポイントすると、その部分に固有のデータの概要が表示されます。棒グラフの任意の部分をクリックすると、より詳細な情報を提供するリストが開きます。

必要なロール：脆弱性管理者

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性対応アプリケーションでユーザーが実行および表示できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。

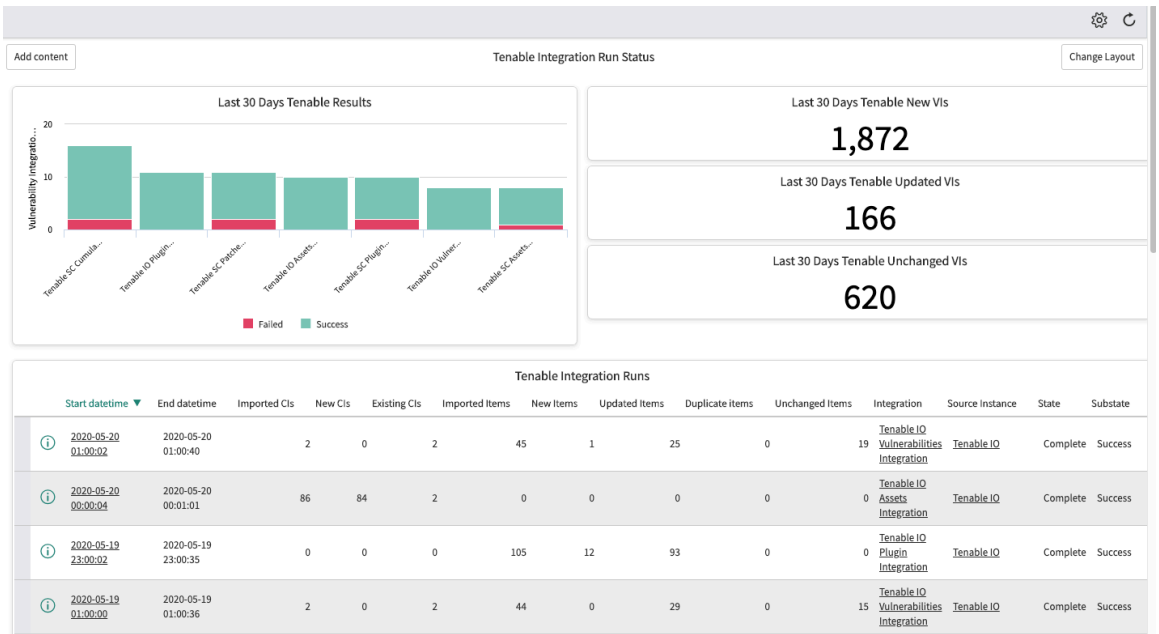
詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

データを表示するには、次に移動します: **All** (すべて) > **Tenable** 脆弱性統合 > 統合実行ステータス.

脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で使用可能です。

注:
Tokyo を使用している場合は、Next Experience UI でダッシュボードを表示できますが、一部の機能が失われます。

実行ステータス



Start datetime	End datetime	Imported CIs	New CIs	Existing CIs	Imported Items	New Items	Updated Items	Duplicate items	Unchanged Items	Integration	Source Instance	State	Substate
2020-05-20 01:00:02	2020-05-20 01:00:40	2	0	2	45	1	25	0	19	Tenable IO Vulnerabilities Integration	Tenable IO	Complete	Success
2020-05-20 00:00:04	2020-05-20 00:01:01	86	84	2	0	0	0	0	0	Tenable IO Assets Integration	Tenable IO	Complete	Success
2020-05-19 23:00:02	2020-05-19 23:00:35	0	0	0	105	12	93	0	0	Tenable IO Plugin Integration	Tenable IO	Complete	Success
2020-05-19 01:00:00	2020-05-19 01:00:36	2	0	2	44	0	29	0	15	Tenable IO Vulnerabilities Integration	Tenable IO	Complete	Success

Tenable 統合実行状況チャートレポート

名前	説明
過去 30 日間の Tenable 結果	各統合で完了した統合実行の数。成功した実行と失敗した実行の両方が表示されます。各実行は棒グラフで表示されます。
過去 30 日間の Tenable 新規 VI	過去 30 日間にインポートされた新規脆弱性一致アイテムの数。整数として表示されます。
過去 30 日間の Tenable 更新済み VI	過去 30 日間にインポートされた更新済み脆弱性一致アイテムの数。整数として表示されます。
過去 30 日間の Tenable 未変更 VI	過去 30 日間にインポートされた重複脆弱性一致アイテムの数。整数として表示されます。
Tenable 統合実行	リストの統合実行レコード

自動翻訳

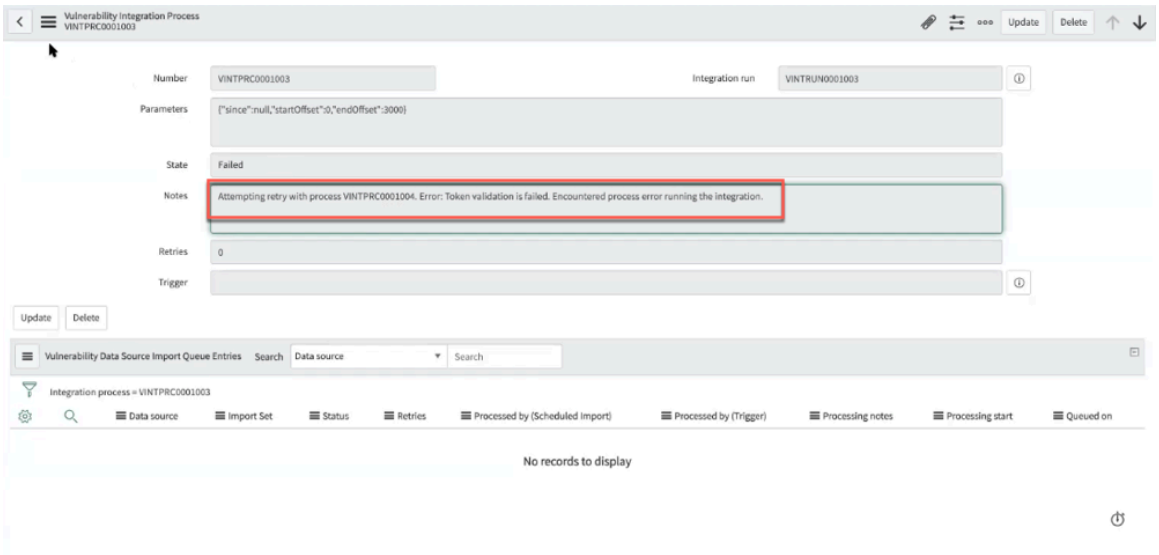
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	説明
	注: V16.1：この統合の検出を検証するには、検出または検出結果を *sn_vul_detection* テーブルの ServiceNow 検出データと比較します。 統合の進行中は、検出数または検出結果数が変更される可能性があります。このレポートでは、統合実行の完了後に、インスタンスの [現在までの数] 列に検出数が表示されます。

トークン検証の有効期限

何らかの理由で Tenable.sc 統合の実行に失敗した場合、Tenable.sc の認証トークンは自動的に期限切れになり、脆弱性統合プロセスレコードにメッセージが表示されます。

期限切れのトークンメッセージ



次の統合プロセス用に新しいトークンが自動的に生成されます。すべての統合プロセス (失敗および成功) は、脆弱性統合プロセスレコードの [脆弱性統合プロセス] タブに表示されます。

Tenable.sc 統合の再スキャンの開始

Tenable プラットフォームで再スキャンを開始し、スケジュールされたスキャンサイクル間で脆弱性一致アイテムが修正されたことを確認します。Now Platform インスタンスから Tenable.sc 製品の脆弱性一致アイテムの再スキャンをオンデマンドで開始できます。

始める前に
必要なロール：sn_vul.write_all または sn_vul.write_assigned

注:
Tenable.sc は、エージェントベースのマシンでの再スキャンの開始をサポートしていません。

開始する前に、スキャナーがアクティブ化されていることを確認します。次のように移動する。 脆弱性対応 > 脆弱性スキャン > スキャナー.

このタスクについて
ワークスペースから再スキャンを開始するには、「脆弱性対応 ワークスペースからの Tenable.io および Tenable.sc 脆弱性一致アイテムの再スキャン」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

クラシック環境で再スキャンを開始するには、以下の手順に従います。

修復オーナー、IT スペシャリスト、脆弱性アナリスト、または脆弱性マネージャーは、スケジュール設定済みのフルスキャンに関連するオーバーヘッドとボリュームを削減するために、環境内の資産 (構成アイテム) の特定の脆弱性についてターゲットの再スキャンをオンデマンドで開始できます。脆弱性一致アイテム (VI)、修復タスク (RT)、サードパーティエントリー (TPE)、または Now Platform インスタンスから検出されたアイテムレコードから再スキャンを開始できます。

再スキャンにより、修復アクティビティ、パッチ、およびその他のアクションによって構成アイテム (CI) の特定の脆弱性が正常に修正されたことを修復オーナーおよび脆弱性アナリストが確認できます。

たとえば、3 週間に 1 回環境全体をスキャンするとします。最新のフルスキャンは 1 週間前に完了しましたが、重大な脆弱性を修正するために昨日パッチを適用しました。この脆弱性の特性を考えると、この脆弱性が修正されたことを確認するのに次のスケジュール済みスキャンまで 2 週間待つことはできません。以前のスキャン中に検出された重大な脆弱性がパッチによって正常に修正されたことを確認するために、Now Platform for Tenable.sc 脆弱性一致アイテムからターゲット再スキャンを開始できます。

注:
Now Platform® インスタンスから再スキャンを要求する場合、Vulnerability Response Integration with Tenable 認証情報の選択はオプションです。ServiceNow® Tenable.sc スキャン認証情報統合は、インスタンスの Tenable.sc 製品からスキャナー認証情報をインポートして更新します。この統合は毎週実行され、Tenable 認証情報データをインポートして安全に保存します。

このインポートされたデータには、Tenable パスワードやその他の機密性の高い Tenable アカウント情報は含まれません。Tenable.sc 脆弱性統合 (Tenable.sc のオープンな脆弱性統合および修正された脆弱性統合) を構成すると、インスタンスのセットアップアシスタント内から ServiceNow® Tenable.sc スキャン認証情報統合が自動的に有効 ([アクティブ]) になります。

ユーザーが必要に応じて Now Platform インスタンスから表示できるように、インポートする認証情報に関する次の情報に注意してください。

- Tenable.sc アドミンユーザーロールで作成された認証情報は、すべての組織のユーザーが使用できます。
- Tenable.sc 組織ユーザーロールで作成された認証情報は、その組織内のユーザーのみが使用できます。これらの認証情報は、インスタンスへの接続に使用されているユーザーのアカウントと共有されない限り、作成者の組織外のユーザーの Now Platform にはインポートされません。

詳細については、Tenable.sc のドキュメントを参照してください。

Tenable.sc アプリケーションの構成の詳細については、「セットアップアシスタントを使用した Tenable 脆弱性統合の構成」を参照してください。スキャン認証情報統合の詳細を表示するには、次に移動します: **All** (すべて) > **Tenable** 脆弱性統合 > 統合 > **Tenable.sc** スキャン認証情報統合.

統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、 脆弱性対応のバージョン 18.2.4 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム.
2. 再スキャンをトリガーする脆弱性一致アイテムレコードを見つけて開きます。

   注:
   ソースが Tenable.sc の VI の再スキャンのみを開始できます。VI リストビューの [ソース] 列、または個々のレコードの [ソース] フィールドに Tenable.sc が表示されていることを確認します。条件ビルダーを使用して、VI をソース別にグループ化できます。または、[ソース] 列が VI リストビューに表示されていない場合は、リストの左上にある [リストをカスタマイズ] アイコン (歯車アイコン) をクリックし、スラッシュバケットを使用して [ソース] を [利用可能] から [選択済み] に移動します。

3. または、 **All** (すべて) > 脆弱性対応 > 修復タスク または 脆弱性対応 > ライブラリー > サードパーティ は、それぞれ再スキャンに使用する修復タスクまたはサードパーティのエントリーレコード用です。

   選択内容に応じて、次のレコードで [再スキャン] ボタンを使用できます。

   - 単一の VI レコードでは、VI のソースが Tenable.sc 製品で、[クローズ済み] 以外のステータスである必要があります。複数の VI レコードの場合、すべての VI のソースが Tenable.sc 製品で、[クローズ済み] 以外のステータスである必要があります。
   - RT レコードでは、修復タスクは [クローズ済み] を除くあらゆるステータスをとることが可能ですが、関連する VI はすべてソースが Tenable.sc 製品である必要があります。
   - サードパーティエントリー (TPE) レコードには、[クローズ済み] 以外のステータスでソースが Tenable.sc 製品の関連する VI レコードが少なくとも 1 つ必要です。

4. レコードの右上にある [再スキャン] をクリックします。
   スキャナーにアクセスするためのスキャナー認証情報を選択するように求められます。これらは、Tenable.sc スキャン認証情報統合によってインポートされた認証情報です。
5. ダイアログで、必要なフィルターと認証情報タイプを選択します。
6. [スキャンの要求 **(Request Scan)]** をクリックします。

   スキャンが処理されていることを示すメッセージが表示されます。すべての再スキャンのステータスは、再スキャンの開始に使用した VI、RT、および TPE レコードの [スキャン] 関連リストでいつでも確認できます。メッセージで [詳細を表示] をクリックして再スキャンのステータスを表示し、指定されたレコードから開始された他の再スキャンを表示します。

   すべての子スキャンが正常に完了すると、親スキャンレコードの [ステータス (State)] フィールドが完了としてマークされます。子はインポートデータをスキャンします。親スキャンレコードは、子スキャンのコンテナです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Now Platform® インスタンスは、正常に完了するか設定された追跡期間がタイムアウトするまで、再スキャンステータスを追跡します。 タイムアウトしてもスキャンは停止しません。タイムアウトは、実際の再スキャンが停止したときではなく、Now Platform® が再スキャンステータスの追跡を停止したときです。[クローズ済み]/[修正済み] に移行した、または移行する予定のすべての VI は、Tenable.sc の修正された脆弱性統合の次のスケジュール済みインポートとともにインポートされます。

Tenable.io 統合の再スキャンの開始

Tenable プラットフォームで再スキャンを開始し、スケジュールされたスキャンサイクル間で脆弱性一致アイテムが修正されたことを確認します。Now Platform® インスタンスから Tenable.io 製品の脆弱性一致アイテムの再スキャンをオンデマンドで開始できます。

始める前に

必要なロール：sn_vul.write_all または sn_vul.write_assigned

開始する前に、スキャナーがアクティブ化されていることを確認します。次のように移動する。 脆弱性対応 > 脆弱性スキャン > スキャナー.

このタスクについて

- 脆弱性対応ワークスペースから再スキャンを開始するには、「でのレコードと修復タスクの再スキャン Vulnerability Manager ワークスペース」および「IT 修復ワークスペースでの脆弱性一致アイテムと修復タスクの再スキャン」を参照してください。
- クラシック環境で再スキャンを開始するには、以下の手順に従います。

注:
Tenable.io は、エージェントベースのマシンでの再スキャンの開始をサポートしていません。

修復オーナー、IT スペシャリスト、脆弱性アナリスト、または脆弱性マネージャーは、スケジュール設定済みのフルスキャンに関連するオーバーヘッドとボリュームを削減するために、環境内の資産 (構成アイテム) の特定の脆弱性についてターゲットの再スキャンをオンデマンドで開始できます。脆弱性一致アイテム (VI)、修復タスク (RT)、サードパーティエントリー (TPE)、または Now Platform インスタンスから検出されたアイテム (SDI) レコードから再スキャンを開始できます。再スキャンにより、修復アクティビティ、パッチ、およびその他のアクションによって構成アイテム (CI) の特定の脆弱性が正常に修正されたことを確認できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注: Now Platform® インスタンスから再スキャンを要求する場合、Vulnerability Response Integration with Tenable 認証情報の選択はオプションです。ServiceNow® Tenable.io スキャン認証情報統合は、インスタンスの Tenable.io 製品からスキャナー認証情報をインポートして更新します。この統合は毎週実行され、Tenable 認証情報データをインポートして安全に保存します。

このインポートされたデータには、Tenable パスワードやその他の機密性の高い Tenable アカウント情報は含まれません。

次の情報では、ユーザーが必要に応じて Now Platform インスタンスから表示できるように、インポートする認証情報について説明しています。

- Tenable.io アドミンユーザーロールで作成された認証情報は、すべての組織のユーザーが使用できます。
- Tenable.io 組織ユーザーロールで作成された認証情報は、その組織内のユーザーのみが使用できます。これらの認証情報は、インスタンスへの接続に使用されているユーザーのアカウントと共有されない限り、作成者の組織外のユーザーの Now Platform にはインポートされません。

  詳細については、Tenable.io のドキュメントを参照してください。

- 再スキャンを開始する前に、Tenable.io テンプレート統合と Tenable.io スキャン認証情報統合をアクティブにする必要があります。スキャン認証情報統合の詳細を表示するには、次に移動します: **Tenable** 脆弱性統合 > 統合 > **Tenable.io** スキャン認証情報の統合.

  テンプレートとスキャンの認証情報統合はデフォルトで非アクティブになっています。Tenable.io の認証情報を入力すると、すべての Tenable.io 統合が自動的にアクティブになります。これらの統合を手動でアクティブまたは非アクティブにするには、次の手順を実行します。

  1. 次のように移動する。 **All** (すべて) > **Tenable** 脆弱性統合 > アドミニストレーション > 統合.
  2. 表示されるリストで、必要な Tenable.io 統合レコードを見つけます。
  3. 各レコードを開き、[アクティブ] チェックボックスをオンにして統合をアクティブ化します。
  4. [更新] をクリックして変更を保存します。
  5. セットアップアシスタントに戻り、脆弱性対応 で Tenable 脆弱性統合の構成を続行します。

Tenable.io および Tenable.sc 製品の構成の詳細については、「セットアップアシスタントを使用した Tenable 脆弱性統合の構成」を参照してください。

たとえば、3 週間に 1 回環境全体をスキャンするとします。最新のフルスキャンは 1 週間前に完了しましたが、重大な脆弱性を修正するために昨日パッチを適用しました。この脆弱性の特性を考えると、この脆弱性が修正されたことを確認するのに次のスケジュール済みスキャンまで 2 週間待つことはできません。以前のスキャン中に検出された重大な脆弱性がパッチによって正常に修正されたことを確認するために、Now Platform for Tenable.io 脆弱性一致アイテムからターゲット再スキャンを開始できます。

スキャンを開始したレコードの更新された結果は、修正された脆弱性統合の次のスケジュール設定済みのインポート後に表示できます。

統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロー

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ドサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、 脆弱性対応のバージョン 18.2.4 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム.
2. 再スキャンをトリガーする脆弱性一致アイテムレコードを見つけて開きます。

   注:
   Tenable.io スキャナーを使用している場合は、ソースが Tenable.io の VI の再スキャンのみを開始できます。VI リストビューの [ソース] 列、または個々のレコードの [ソース] フィールドに Tenable.io が表示されていることを確認します。条件ビルダーを使用して、VI をソース別にグループ化できます。または、[ソース] 列が VI リストビューに表示されていない場合は、リストの左上にある [リストをカスタマイズ] アイコン (歯車アイコン) をクリックし、スラッシュバケットを使用して [ソース] を [利用可能] から [選択済み] に移動します。

3. または、 **All** (すべて) > 脆弱性対応 > 修復タスク または 脆弱性対応 > ライブラリー > サードパーティ 再スキャンに使用するレコード用。

   選択内容に応じて、次のレコードで [再スキャン] ボタンを使用できます。

   - 単一の VI レコードでは、VI が [クローズ済み] 以外のステータスである必要があります。複数の VI レコードの場合、すべての VI のソースが Tenable.io 製品で、[クローズ済み] 以外のステータスである必要があります。
   - 修復タスクレコードの場合、[クローズ済み] 以外のステータスの修復タスクのみがサポートされます。関連するすべての VI は [クローズ済み] 以外のステータスで、ソースとして Tenable.io を使用する必要があります。
   - サードパーティエントリー (TPE) レコードには、[クローズ済み] 以外のステータスでソースが Tenable.io 製品の関連する VI レコードが少なくとも 1 つ必要です。
   - [検出されたアイテム] レコードには、[クローズ済み] 以外のステータスの Tenable.io 製品の関連する VI レコードが少なくとも 1 つ必要です。
   - [脆弱性一致アイテム] リストから、再スキャンする個々の脆弱性一致アイテムを選択できます。画面の左下にある [選択した行のアクション] メニューを使用して、再スキャンを開始します。認証情報を入力するように求められます。

4. レコードの右上にある [再スキャン] をクリックします。

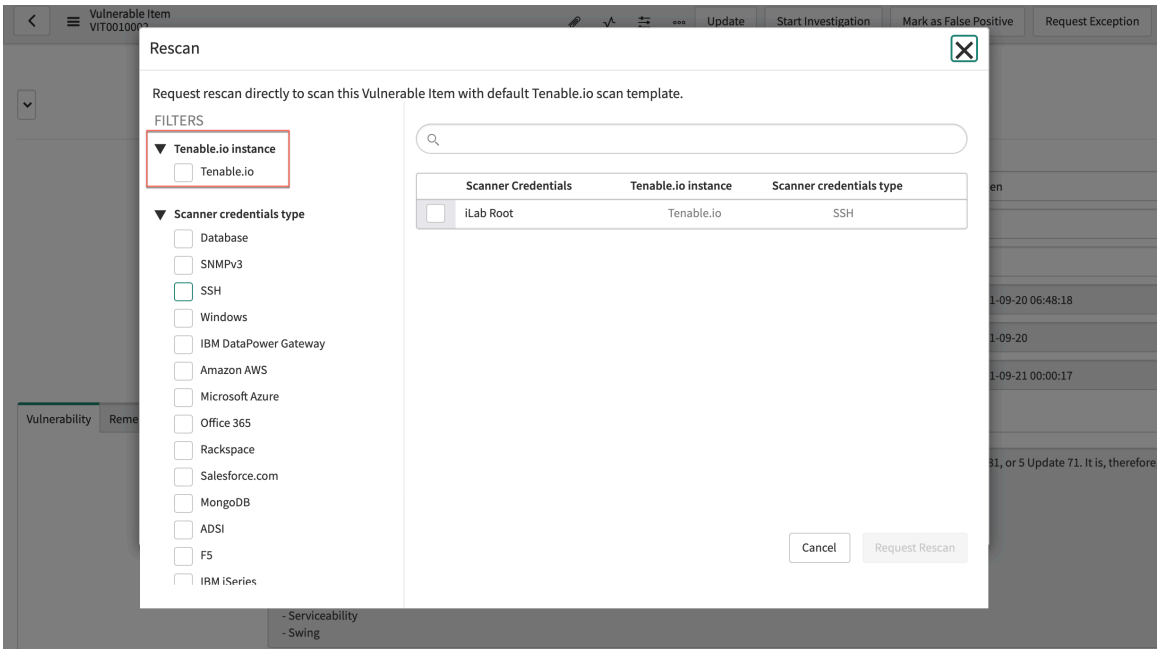
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

再スキャンのインスタンスとスキャナーへのアクセスに使用するスキャナー認証情報を選択するように求められます。表示される認証情報は、Tenable.io スキャン認証情報統合によってインポートされた認証情報です。

5. ダイアログで、使用するインスタンス (1 つまたは複数) と認証情報タイプを選択します。

次の画像では、1 つの統合インスタンス Tenable.io が表示されています。複数の Tenable.io インスタンスがある場合、それらはすべてフォームの [Tenable.io] セクションに表示されます。



6. [再スキャンを要求] をクリックします。

スキャンが処理されていることを示すメッセージが表示され、親スキャンレコードが作成されます。すべての子スキャンのステータスは、再スキャンの開始に使用した VI、修復タスク、TPE、および SDI レコードの [スキャン] 関連リストでいつでも確認できます。メッセージで [詳細を表示] をクリックして再スキャンのステータスを表示し、指定されたレコードから開始された他の再スキャンを表示します。

すべての子スキャンが正常に完了すると、親スキャンレコードの [ステータス (State)] フィールドが完了としてマークされます。子はインポートデータをスキャンします。各スキャンは、統合インスタンス、TPE、IP、およびネットワーク ID の一意の組み合わせをサポートしています。親スキャンレコードに複数の子スキャンが表示される場合があります。たとえば、子スキャンでサポートできる IP アドレスの最大数は 1000 です。脆弱性一致アイテムに 1002 個の IP がある場合、要求をサポートするために 2 つの子スキャンが作成され、[スキャン] 関連リストに一覧表示されます。親スキャンレコードは子スキャンのコンテナであり、そのステータスは子スキャンのステータスを反映します。

Now Platform® インスタンスは、正常に完了するか設定された追跡期間がタイムアウトするまで、再スキャンステータスを追跡します。 タイムアウトしてもスキャンは停止しません。タイムアウトは、実際の再スキャンが停止したときではなく、Now Platform® が再スキャンステータスの追跡を停止したときです。[クローズ済み]/[修正済み] に移行した、または移行する予定のすべての VI は、Tenable.io の修正された脆弱性統合の次のスケジュール済みインポートとともにインポートされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エラーが発生したスキャンについては、親スキャンレコードで子スキャンを確認できます。子スキャンの応答ペイロードのエラーを表示します。

スキャンを開始したレコードの更新された結果は、修正された脆弱性統合の次のスケジュール設定済みのインポート後に表示できます。

Tenable 脆弱性統合 のネットワークパーティション識別子で構成アイテムを更新する

IP アドレスを共有する環境内の資産に対して、一意の構成アイテム (CI) を作成します。環境全体で個別の資産を特定し、検出された既存のアイテム、脆弱性一致アイテム、および検出レコードで CI を自動的に更新して、脆弱性に関する詳細を提供します。

始める前に
必要なロール：admin

このタスクについて
デフォルトでは、脆弱性対応 アプリケーションで資産を識別する方法の 1 つは IP アドレスです。場合によっては、資産は IP アドレスを共有できますが、それらは 1 つの CI として CMDB に保存されます。

たとえば、次の表に示すように、環境内の複数の資産 (CI) が IP アドレスを共有できますが、ネットワークとリポジトリの ID は一意です。ただし、デフォルトでは、これらの資産は通常、IP アドレスのルックアップ中に単一の CI（CI 1）として識別され、保存されます。

デフォルトの **IP** ルックアップと **CI** の作成

ソース	IP アドレス	Network_id	構成アイテム
Tenable.io：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

ソース	IP アドレス	Repository_id	構成アイテム
Tenable.sc：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

同じ IP アドレスを持つ資産に対して個別の CI を作成して、それらを個別の資産として識別できるようにすることができます。新規のデータのインポートから開始し、スケジュール済みジョブ *`Update existing discovered items with network partition identifier`* を実行することで、ネットワークパーティション識別子 [network_partition_identifier] を含む既存の CI をより細かく更新できます。

このスケジュール済みジョブは、デフォルトでは非アクティブです。セットアップアシスタントで Tenable.io と Tenable.sc 製品の資産と修正済みおよびオープンな脆弱性の統合に対してこの機能をアクティブ化して、この識別子をレコードに表示します。

このスケジュール済みジョブを有効にすると、インポートされたデータから既存の CI レコードにネットワークパーティション識別子 [network_partition_identifier] が追加されます。IRE によって作成された既存の CI も更新されます。スケジュール済みジョブは、次のインポートから始まるネッ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

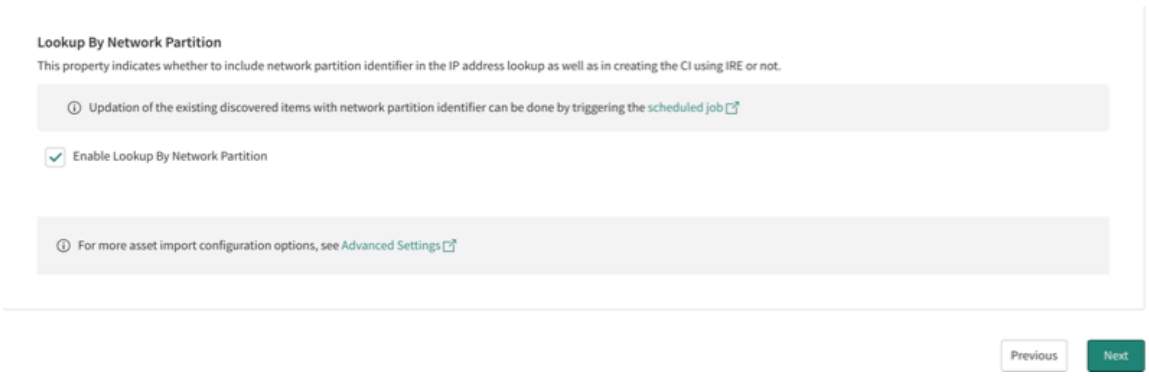
トワークパーティション識別子を含む CI も作成します。または、オンデマンドでジョブを開始して既存のデータを更新することもできます。

脆弱性対応 の v14.0 および Tenable 脆弱性統合の v12.1 以降、アップグレード時に CMDB CI クラスモデル (1.0.21.) がサポートされています。クラスモデルでは、識別および調整 (IRE) 識別ルールにネットワークパーティション識別子 [network_partition_identifier] があります。

オプション	説明
スケジュール済みジョブをオンデマンドで実行します。	検出された既存のアイテムを更新します。既存の Tenable データの CI は、ネットワークパーティション識別子の粒度を含むように作成または更新されます。検出されたアイテム、脆弱性一致アイテム、および検出レコードはすべて新しい CI で更新されます。
次のスケジュール済みジョブとの統合からの新しいデータのインポートを待機します。	次のスケジュール済みジョブから始まるネットワークパーティション識別子を使用して、新しい資産ごとに CI を作成します。CI、脆弱性一致アイテム、および検出レコードはすべて、新しい粒度を含むように更新されます。完全一致が見つからない場合は、新しい CI が作成されます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > セットアップアシスタント > 統合設定 > スキャナー統合.
2. Tenable.io 統合または Tenable.sc 統合を選択します。
3. 必要な統合を編集します。
4. 選択 資産インポート構成.
5. 選択 ネットワークパーティションによるルックアップを有効化 のチェックボックス ネットワークパーティションによるルックアップを有効化 節。



6. [次へ] をクリックします。

   ネットワークパーティション識別子 NETWORK_ID および REPOSITORY _ID が含まれており、既存の CI を更新するか、次のスケジュール済みジョブで CI を作成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

IP ルックアップと **CI** の作成に含まれるネットワークパーティション識別子属性

ソース	**IP** アドレス	**NETWORK_ID**	ネットワークパーティション識別子のない資産の **CI**	ネットワークパーティション識別子のある **CI** 資産
Tenable.io：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

ソース	**IP** アドレス	**REPOSITORY_ID**	ネットワークパーティション識別子のない資産の **CI**	ネットワークパーティション識別子のある **CI** 資産
Tenable.sc：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

次のスケジュール済みジョブでは、Tenable.io および Tenable.sc 製品の資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合からデータをインポートできるように、IP アドレスおよび不完全な IP アドレス CI の識別ルックアップルールにネットワークパーティション識別子属性が自動的に含まれます。

システムのプロパティを有効にしてレコードを保存した後、スケジュール済みジョブをオンデマンドで起動して、ネットワークパーティション識別子を含む CI で検出された既存のアイテムを更新することもできます。

自動翻訳

Tenable 脆弱性統合のインポートの変更

ServiceNow® Tenable 脆弱性統合の Tenable 脆弱性インポート統合に特化したオプションの変更を構成し、一部のデータを簡素化します。

始める前に

必要なロール：sn_vul.vulnerability_admin

このタスクについて

この一連のタスクには、Now Platform に関するコーディングと高度な知識が必要です。

Tenable 脆弱性統合のドメインセパレーションインポートを作成するには、次の手順に従います。次の例は、Tenable.io のオープンな脆弱性統合用ですが、この内容は他の Tenable 統合にも適用できます。

手順

1. ドメインを作成します。
2. 作成するドメインごとに、ユーザーを作成してそのドメインにアサインします。

   このユーザーは、Tenable.io のドメインの run_as プレースホルダーと考えてください。

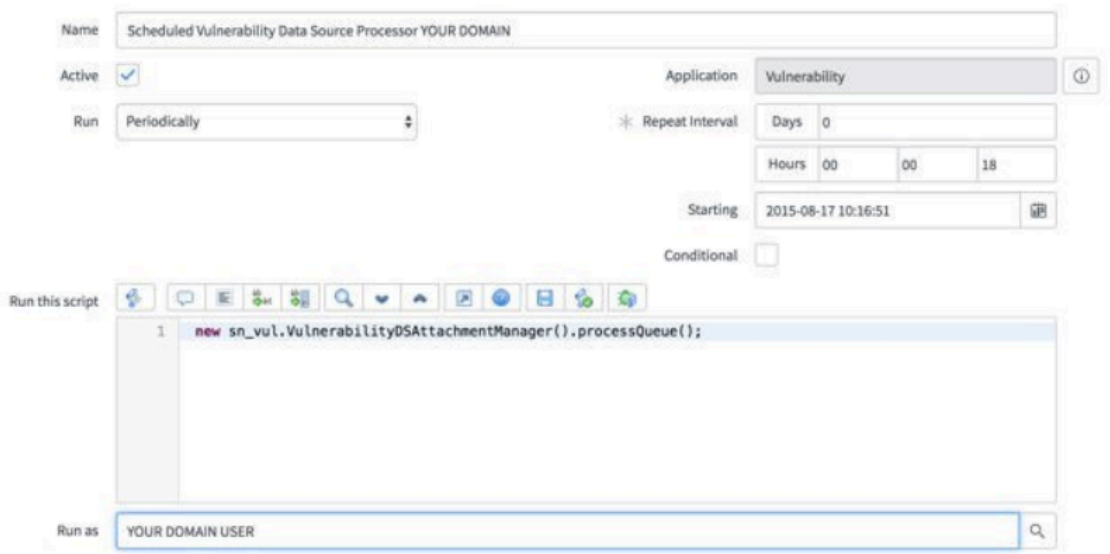
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 脆弱性統合を開きます。
   ユーザーは、グローバルドメイン内の VR.System ユーザーに相当し、ロール sn_vul.tenable_configure_integration、import_admin、および sn_vul.vulnerability_write が必要です。このユーザーには、データソース、変換マップおよび脆弱性データへのアクセスが必要です。

   注:
   このユーザーをこのロールに固有のものと見なします。ユーザーに他の目的はありません

4. 各ドメインで、[スケジュール設定済み脆弱性データソースプロセッサー] をコピーしてスケジュール済みジョブを作成します。 システム定義 > スケジュール済みジョブ.
5. スケジュール済みジョブを識別する名前にドメインを追加します。
6. run_as ユーザーを前のステップで作成したユーザーに変更します。

   注:
   次の UI アクションを編集して、統合が run_as ユーザードメインで実行されるようにします。



7. Tenable.io のオープンな脆弱性統合の [今すぐ実行] UI アクションを編集して、このコードブロックをファイルの先頭に追加します。
   `//sys id below is of Tenable.io integration if(current.sys_id == "4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }`

   注:
   次のスクリプトインクルードを編集して、統合が run_as ユーザードメインで実行されるようにします。

8. VulnerabilityIntegrationUtils スクリプトインクルードメソッド addIntegrationRun を編集して、ハイライト表示されたコードを追加します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. VulnerabilityIntegrationUtils スクリプトインクルードのメソッド addProcessRun を編集して、ハイライト表示されたコードを追加します。

```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. DataSourceVulnReportRefreshProcessor スクリプトインクルード メソッド _processFromDataSourceGroups を編集して、元のコード _processFromDataSourcesGroups コードを Edited _processFromDataSourcesGroups コードに変更します。

11. VulnerabilityDSAttachmentManager スクリプトインクルードメソッドの queueItem を編集して、ハイライト表示されたコードブロックの queueItem、_getNext、_processQueueEntry 関数を追加します。

ドメインセパレーションされたホスト検出インポートの準備ができました。

インポート前に算出を無効にする

使用しない場合は、次の手順に従ってデフォルトの算出を無効にします。脆弱性算出を使用しない場合は、定義した他の脆弱性算出に加えて、デフォルトの算出を無効にすることをお勧めします。脆弱性算出は、脆弱性一致アイテムレコードにアクセスするたびに実行され、インスタンスのパフォーマンスに影響を与える可能性があります。

必要なロール：sn_vul.vulnerability_admin。

12. 次のように移動する。 **All** (すべて) > 脆弱性 > アドミニストレーション > 脆弱性の算出.

13. [脆弱性影響 (Vulnerability Impact)] グループを開きます。

14. スコアとサービスに基づく影響の算出を開きます。

15. [アクティブ] フィールドの選択を解除して、産出を非アクティブ化します。

16. [更新] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

デフォルトの算出を無効にしました。

最初のインポート前に通知ベースのビジネスルールを無効にします。

次の手順に従い、レコードの最初のインポート前に通知関連のビジネスルールを無効にします。レコードの最初のインポート中に、特定の通知関連のビジネスルールによって大量の通知が生成され、パフォーマンスが影響を受ける可能性があることを確認します。これらのビジネスルールは、インポート中に無効になるように変更する必要があります。

必要なロール：sn_vul.vulnerability_admin

17. 次のように移動する。 **All** (すべて) > システム定義 > ビジネスルール.
18. [影響を受ける CI 通知 (Affected ci notifications)] を検索します。
19. ビジネスルールを開き、条件「 `current.sys_class_name != "sn_vul_vulnerable_item"`」を挿入します。
20. [更新] をクリックします。
21. 次のビジネスルールについてこの手順を繰り返します。
    - 影響を受けるコストセンター通知
    - 影響を受けるグループ通知
    - 影響を受ける場所の通知

    注:
    最初のレコードのインポートが完了した後、これらのビジネスルールを再度有効にすることができます。ただし、無効にしておくことを検討してください。大量の通知が生成され、インスタンスのパフォーマンスに影響を与える可能性があります。

最初の開始日の変更

最初の開始日を変更するには、次の手順に従います。セットアップアシスタントを使用してインストール中に、Tenable 統合の最初の開始日を設定します。その開始日は、次のステップに示すように、セットアップアシスタントまたはプライマリ統合からリセットできます。

22. 次のように移動する。 **All** (すべて) > **Tenable** 脆弱性統合 > アドミニストレーション > 統合.
23. 統合をクリックします。
24. [統合の詳細] をクリックします。
25. [開始時間] フィールドを過去の値に設定すると、その時間以降にスキャンおよび検出されたすべての脆弱性が検出されます。

    セットアップアシスタントを使用して Tenable を構成した場合、[開始時間] フィールドには、最初に今日の日付の 3 か月前、その後は今日の日付が事前に入力されます。注意：過去最大 1 か月前の値を設定することを検討してください。これにより、大量のデータで Tenable API レート制限を超えることがなくなり、実行タイムアウトがトリガーされなくなります。

26. [送信] または [更新] をクリックします。
27. オプション: [今すぐ実行] をクリックして、今すぐ実行します。

脆弱性インスタンスに基づいて **Tenable** 検出を分割し、脆弱性一致アイテムを分割します

ServiceNow® 脆弱性対応では、Tenable スキャナーからの検出を分割して、検出された脆弱性インスタンスごとに一意の脆弱性一致アイテム (VIT) を作成できます。この分割により、VIT をさまざまな修復チームにアサインできるため、脆弱性の管理と追跡が強化されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：admin

このタスクについて
Tenable スキャナーのペイロードには検出データが含まれており、実証内の各パスが検出の分割に使用されます。ペイロードの出力タグは脆弱性の場所を識別し、特定のパスに従って脆弱性を正確に特定および管理を容易にします。

手順

1. サードパーティ統合テーブル [sn_sec_int_integration] で、Tenable.io と Tenable.sc の **[VI** キー列に証明を含める] の値を true に設定します。
2. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > **VI** の粒度の構成.
3. [ポートを含める] フォームで、[ポートを含める] チェックボックスをオンにして、[ここをクリック] リンクを選択します。
4. [VI キーに証明を追加] リストで、[新規] を選択します。
5. [VI キー新規レコードに実証を追加 (Add proof to the VI key- New record)] フォームの [脆弱性] フィールドに、実証を含める Tenable ID を追加します。

   注:
   パス情報のみに基づいて、またはパスとバージョンの詳細を組み合わせて、検出を分割できます。詳細については、このページの「Tenable スキャナーからの検出の分割」セクションを参照してください。

6. **[Tenable VIT** を分割する正規表現] フィールドで、次の操作を行います。
   - パスのみに基づいて検出を分割するには、「パス\s+:\s+([A\n]+)」と入力します。
   - 「パス\s+:\s+([A\n]+)\n\s+Installed\s+version\s+:\s+([A\n]+)\n\s+Fixed\s+version\s+:\s+([A\n]+)」と入力して、パス、インストール済みバージョン、および修正済みバージョンに基づいて検出を分割します。
7. [**Submit** (送信)] を選択します。

Example: Tenable スキャナーからの検出の分割

Tenable スキャナーからの次の検出は、パスとバージョンの両方の情報を含む出力タグの証明を示しています。

```
    "results":


            "asset":
                "agent_uuid": *92124caabdb9459baa9d053186df48b9",
               "bios_uuid": "ec2cbbfd-dc9e-efbf-acdd-485daZe8c7df"
               "device_ type": "aws-ec2-instance",
                "fqdn": "ip-ac0a0004. secops.com",
                "hostname": "ip-ac0a0004",
        "uuid": "486acb3b-674f-477a-bc37-660a7bba37b3",
                "ipv4": "18.220.145.158",
                "last_authenticated_results": "2024-05-17T03:34:04.424Z",

                "mac_address": "0a:3e:8b:ed:63:e6",
               "netbios name": "IP-AC0A0094".
               "operating_system": [
```

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

```
                    "Microsoft Windows Server 2019 Datacenter Build 17763"


                "network_id": "00000000-0000-0000-0000-000000000008",

               "tracked": true


          "output": "In                    C: 11 Program Files (x86) \ \Common
Files\\0racle\\Java\\javapath_target_119044062511\n Installed version : 1.8.0_361.9\n Fixed
version
                                                                    Path
          "plugin":
               "bid":
                    123456


               "checks_for_default_account": false,
              "checks_for malware": false,

                "coe":
               "cpe:/a:notepad-plus-plus:notepad%5c%2b15ck2b"


                "cvSs3_base_score": 7.8,
               "cvss3 temporal score": 7.0,

               "cvss3_temporal_vector": {
                    "exploitability": "Proof-of-Concept",
                    "remediation level": "Official Fix",
                     "report_confidence": "Confirmed",
                     "raw": "E: P/RL:0/RC: C"
```


自動翻訳

Atlassian Jira と 脆弱性対応 の統合の概要

Atlassian Jira と 脆弱性対応 の統合により、さまざまな問題追跡およびアジャイル管理ツールを活用して、脆弱性修復作業を追跡できます。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

概要

ServiceNow® 脆弱性対応 と Atlassian Jira の統合により、脆弱性に対応する問題を作成し、Jira の問題エンティティと 脆弱性対応 の脆弱性一致アイテムを双方向で同期して最新の更新を反映できるようになりました。脆弱性マネージャーは、ServiceNow 脆弱性対応 に存在する脆弱性一致アイテムを作成し、Atlassian Jira などの各自が使用する SoR および問題管理ツールで修復ユーザー (アプリケーション脆弱性対応 の場合は開発者) にアサインする必要があります。問題管理ツールで脆弱性に対して実行された処理の進捗状況を ServiceNow 脆弱性対応 で更新して、脆弱性マネージャーが把握できるようにする必要があります。さらに、脆弱性対応 で脆弱性マネージャーが脆弱性一致アイテムに対して行った更新をイシュー管理ツールにも渡して、修復ユーザーが把握できるようにする必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

利用可能バージョン

リリースバージョン	リリースノート
脆弱性対応	脆弱性対応統合のリリースノート
コンテナ用 Vulnerability Response および Configuration Compliance	Container Vulnerability Response リリースノート
Jira スポーク	Jira Spoke リリースノート

Jira 脆弱性統合

Jira脆弱性統合を表示するには、次に移動します: **All** (すべて) > **VR** の **Agile Management** > **Agile** ツールを構成 .

ベースシステムには、次の統合が含まれています。デフォルトでは、これらの統合はすべて有効ではありません。

最初の実行後、毎日スケジュール済みジョブが連結され、統合が順番に自動的に実行されます。スケジュール済みジョブを手動で実行することもできます。スケジュール済みジョブでは、インスタンスを他の脆弱性管理システムと同期させることで、脆弱性修復ライフサイクルを簡素化します。

Jira 脆弱性対応 統合の準備

Jira Vulnerability 統合を成功させるには、統合前のタスクを計画して実行する必要があります。これらのタスクを実行して、統合の準備をします。Jira 脆弱性対応 統合では、Jira 製品と API に精通していることを前提としています。

Agile Integration for 脆弱性対応 および Jira Integration for Vulnerability Response とともにインストールされるコンポーネント

いくつかのタイプのコンポーネント (テーブル、ユーザーロールなど) が、Agile Integration for Vulnerability Response および Jira Integration for Vulnerability Response プラグインのアクティブ化とともにインストールされます。

インストールされるロール

ロールタイトル [名前]	説明
Agile ツールアドミン [sn_vul_agile.agile_tool_admin]	問題の作成または更新のための Agile Management の構成ルールを作成できます。Agile Management のルール構成を作成します。
JIRA アドミン [sn_vul_jira.admin]	Agile ツールを選択して、選択したエンティティテーブルの問題を作成できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インストールされるテーブル

テーブル	説明
Agile ツール構成 (Agile Tool Configuration) [sn_vul_agile_tool_rule_config]	Agile プラットフォームで問題を作成するための構成ルールが含まれています。
Agile ツールフィールドマッピング (Agile Tool Field Mapping) [sn_vul_agile_tool_field_mapping]	構成ルールのフィールドマッピングが含まれています。
Agile ツールステータスマッピング (Agile Tool State Mapping) [sn_vul_agile_tool_field_mapping]	Jira の問題状況と、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、アプリケーション修復タスクおよびコンテナ修復タスクの状況のステータスマッピングが含まれています。
Agile ツールマニフェスト (Agile Tool Manifest) [sn_vul_agile_tool_manifest]	問題作成のペイロードが含まれています。
Agile ツールデータリソース (Agile Tool Data Resource) [sn_vul_agile_tool_data_resource]	作成された Jira 問題に関する情報が含まれています。
JIRA アドミン [sn_vul_jira.admin]	Agile ツールを選択して、選択したエンティティテーブルの問題を作成できます。

Vulnerability Response Integration with Jira のインストール

インスタンスで統合を実行する前に、インストールと構成のステップを完了して、アプリケーション脆弱性対応 が Jira 製品と適切に統合されるようにします。このアプリケーションは別のサブスクリプションとして利用できます。

始める前に
必要なロール：admin
インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

セットアップタスク	説明
脆弱性対応アプリケーションがインストールされ、アクティブ化されていることを確認します。	• Jira Integration for Vulnerability Response には、脆弱性対応アプリケーションが必要です。 • 脆弱性対応の Jira 統合の最新バージョンについては、最新バージョンの脆弱性対応がインストールされていることを確認します。「KB0856498 脆弱性対応互換性マトリクス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	およびリリーススキーマの変更」を参照してください。 • アプリケーションがインストールもアクティブ化もされていない場合は、「Install Vulnerability Response (脆弱性対応のインストール)」を参照してください。
IntegrationHub プラグインがインストールされていることを確認します。	• Jira Spoke には IntegrationHub が必要です。 • IntegrationHub のインストールについては、「KB1112383」を参照してください。 • 詳細については「法務スケジュール - IntegrationHub の概要」を参照してください。
最新バージョンの Jira Spoke がインストールされていることを確認します。	Jira Spoke のインストールについては、「KB0792632」を参照してください。
Vulnerability Response Integration with Agile Management がインストールされていることを確認します。	Vulnerability Response Integration with Atlassian Jira には、この統合が必要です。

手順

1. Jira 脆弱性対応 統合をインストールするインスタンスにログインします。
2. ServiceNow Store に移動します。
3. ServiceNow Store で、脆弱性対応 Integration with Jira アプリケーションを検索します。
4. アプリケーションタイルをクリックします。
   インストールしているアプリケーションに関する詳細情報が表示されます。

   注:
   該当する場合は、[他の要件] および [依存関係] セクションを読むことを検討してください。

5. [アプリを要求] をクリックし、Now Support ログイン認証情報を入力します。
6. [取得] をクリックします。
7. [インスタンス名] と [インスタンスの理由] を入力し、[インスタンスを検証] をクリックします。
8. [要求] をクリックします。
   詳細なインストール手順が記載されたメールが届きます。
9. 次のように移動する。 システムアプリケーション > アプリケーション.
10. アプリケーションを見つけて選択し、[インストール] をクリックします。
    アプリケーションはインスタンスに自動でインストールされます。

Agile ツール構成でのルールの構成

アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、アプリケーション修復タスク、およびコンテナ修復タスクで作成されたレコードが、Agile ツール構成で作成されたルールに一致する場合は、Jira プラットフォームで Jira の問題が作成されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：
sn_vul.app_read_all、sn_vul_container.read_all、sn_vul_agile.agile_tool_admin、または sn_vul_jira.admin。

手順

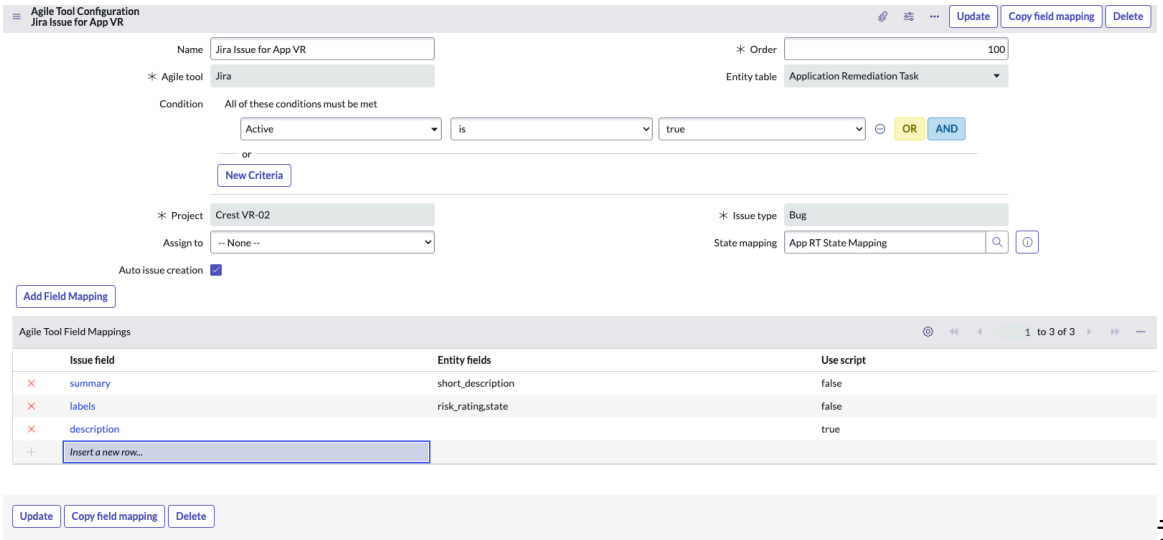
1. 次のように移動する。 **All** (すべて) > **VR** の **Agile Management** > **Agile** ツールを構成.
2. [Agile ツール構成 (Agile Tool configuration)] で新しい構成ルールを作成するには、[新規] を選択します。
3. フォームのフィールドに入力します。

[Agile ツール構成 (Agile Tool configuration)] フォーム

フィールド	説明
名前	Agile ツール構成の名前。
順序	Agile ツール構成の順序。
Agile ツール	特定の Agile プラットフォームで問題を作成するための Agile ツール。
エンティティテーブル	構成ルールが適用されるテーブル。
条件	Agile プラットフォームで問題を作成するための、選択したエンティティテーブルに対するフィルター条件。
自動問題の作成	このチェックボックスがオンになっている場合にのみ、選択したエンティティテーブルに新しいレコードが作成されたときに構成ルールが照会されます。 **注:** ユーザーはリストアクションを使用して、既存のエンティティレコードの問題を作成する必要があります。
プロジェクト	Jira の問題を作成するプロジェクト。
問題タイプ	特定のプロジェクトで作成する問題のタイプ。
アサイン先	問題の作成時に問題をアサインするアサイニー。作成した問題を未アサインのままにするには、[なし (None)] を選択します。
ステータスマッピング	[Agile ツールステータスマッピング (Agile Tool State Mapping)] テーブルの既存の状況マッピングを使用するか、Agile プラットフォームの問題ステータスと ServiceNow エンティティテーブルの状況間の新しいステータスマッピングを作成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



デフォルトでは、アプリケーションがインストールされると、[Agile ツール構成 (Agile Tool Configuration)] フォームの [エンティティテーブル] フィールドに [アプリケーション修復タスク (Application Remediation Task)] と [コンテナ修復タスク] が表示されます。

4. [エンティティテーブル] 選択リストに [アプリケーション脆弱性一致アイテム] と [コンテナ脆弱性一致アイテム] を追加するには、[システムのプロパティ] > **[sn_vul_agile.tablesToShow]** に移動し、[値] フィールドに all を追加します。

システムプロパティフォーム

フィールド	説明
選択肢	選択リストのカンマ区切り値。
値	プロパティの目標値を設定します。プロパティ値はすべて文字列として格納されます。gs.getProperty() メソッドを使用してプロパティを取得する場合は、結果を文字列として扱います。 たとえば、true|false プロパティでは、相当するブーリアン値ではなく、「true」または「false」の文字列が返されます。

5. 既存のステータスマッピングレコードを選択するか、[Agile ツールステータスマッピング (Agile Tool State Mapping)] で新しいステータスマッピングを作成します。

[Agile ツールステータスマッピング **(Agile Tool State Mapping)]** フォーム

フィールド	説明
名前	ステータスマッピングの一意の名前を挿入します。
Agile ツール	Agile ツールを選択します。
エンティティテーブル	ステータスマッピングを作成するソーステーブルを選択します。
プロジェクト	ステータスをマッピングするプロジェクトを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ServiceNow エンティティステータス	Agile ツールのステータスにマッピングするステータスを選択します。
Agile ツールステータス	脆弱性一致アイテム状況から、マッピングする状況を選択します。

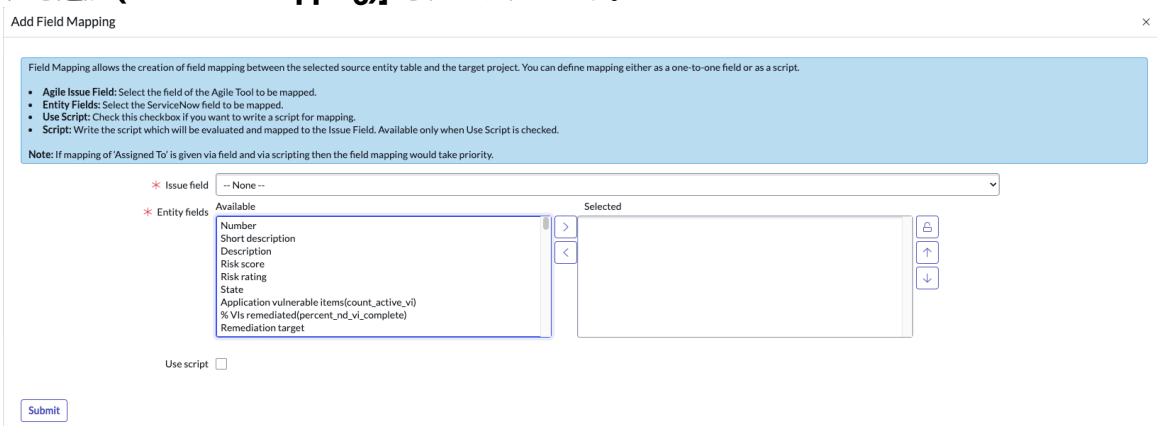
6. [プロジェクトを保存してフェッチ **(Save and Fetch Projects)]** をクリックして、[プロジェクト] フィールドの構成ルールでプロジェクトをフェッチし、Agile ツールの認証情報を検証します。

   ヒント:
   ページごとに特定の数のプロジェクトをフェッチするには、システムプロパティ **projectsPageSize** を設定できます。

7. [システムのプロパティ] > **[sn_vul_jira.projectsPageSize]** に移動し、Jira Cloud の [値] フィールドに、ページあたりのフェッチするプロジェクトの数を追加します。
8. プロジェクトがフェッチされたら、構成ルールで [プロジェクト]、[問題タイプ]、および [アサイン先] を選択します。

   Agile ツールフィールドマッピングの埋め込みリストには、デフォルトのフィールドマッピングが入力されます。デフォルトでは、問題の [サマリー] フィールドと [説明] フィールドがマッピングされます。

9. 問題の他のフィールドを ServiceNow のフィールドにマッピングするには、[フィールドマッピングを追加 **(Add Field Mapping)]** をクリックします。



注:

- [文字列] および [選択肢] タイプのフィールドのみをマップする必要があります。
- Agile ツールの必須の問題フィールドがすべて、エンティティフィールドに適切にマッピングされていることを確認します。

[Agile ツールステータスマッピング **(Agile Tool State Mapping)]** フォーム

フィールド	説明
問題フィールド (Issue Field)	構成ルールで現在選択されているプロジェクトと問題タイプの問題フィールドが含まれています。
エンティティフィールド (Entity Fields)	構成ルールで選択されているエンティティテーブルのフィールドが含まれています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
スクリプトを使用 (Use the Script)	問題のフィールドをエンティティのフィールドにマッピングするためにスクリプトを使用する場合に選択します。
スクリプト	問題のフィールドをエンティティのフィールドにマッピングするスクリプト。

10. Glide モーダルで [送信] をクリックして、[Agile ツールフィールドマッピング (Agile Tool Field Mappings)] テーブルのフィールドマッピングレコードを送信します。

    注:
    必須フィールドをマッピングしない場合、その構成ルールに対して問題は作成されません。

    必須フィールドは、[Agile ツール構成 (Agile Tool configuration)] フォームの上部に表示されます。
    特定の構成ルールのフィールドマッピングはすべて、[Agile ツール構成 (Agile Tool configuration)] テーブルの [Agile ツールフィールドマッピング (Agile Tool Field Mappings)] テーブルの埋め込みリストに表示されます。
11. ヘッダーを右クリックして、変更を保存します。
    保存されたレコードは、[Agile ツール構成 (Agile Tool configuration)] テーブルに表示されます。アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、アプリケーション修復タスク、およびコンテナ修復タスクで作成されたレコードが、構成ルールに一致する場合、構成ルールのマッピングに従ってそのレコードに対して問題が作成されます。
12. [システムのプロパティ] > **[sn_vul_jira.cloudBulkSize]** に移動し、バッチごとに作成する問題の数を [値] フィールドに設定します。

    注:
    Jira Cloud でバッチごとに作成できる問題の最大数は 50 です。

    Jira Server で問題を作成するためのバッチサイズを設定できます。
13. [システムのプロパティ] > **[sn_vul_jira.onPremBulkIssue]** に移動し、バッチあたりの作成する問題の数を [値] フィールドに設定します。
    システムプロパティの [値] フィールドにエラー数を設定することで、マニフェストテーブルのレコードを処理して、特定のエラー数まで Jira の問題を作成することもできます。
14. [システムのプロパティ] > **[sn_vul_agile.ManifestErrorCount]** に移動し、エラーのあるマニフェストを処理する最大回数を設定します。

リストアクションを使用して **Agile** の問題を手動で作成する

[Jira の問題を作成 (Create Jira Issue)] リストアクションがトリガーされたら、ルール構成条件に一致するレコードが「Jira の問題を作成」の対象として考慮され、構成ルールで選択されているマッピングを使用して sn_vul_agile_tool_manifest テーブルに取り込まれる必要があります。

始める前に

必要なロール：sn_vul_agile.agile_tool_admin または sn_vul_jira.admin、sn_vul.app_read_all、sn_vul_container.read_all。

手順

1. 次のように移動する。 **All** (すべて) > ワークスペース > 脆弱性マネージャーワークスペース > リスト > 修復タスク/アプリケーション脆弱性一致アイテム/コンテナ脆弱性一致アイテム.
2. Jira の問題を作成する複数のレコードを選択し、**[Jira** の問題を作成 **(Create Jira Issue)]** をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

選択したレコードでは、関連 Agile ツールのフィールドマッピングとステータスマッピングを考慮する必要があります。
選択したレコードが構成ルール条件を満たしている場合、それらのレコードは Jira の問題の作成対象であり、*sn_vul_agile_tool_manifest* テーブルに追加される必要があります。

フォームアクションを使用して **Agile** の問題を手動で作成する

フォームアクションを使用して Agile の問題を手動で作成します。レコードがいずれかの構成ルール条件に一致している場合には、構成ルールで選択されている値が入力されたポップアップボックスが表示されます。レコードがどの条件にも一致しない場合、ユーザーが事前定義フィールドの値を選択できます。

始める前に
Agile ツールの必須の問題フィールドがすべて、エンティティフィールドに適切にマッピングされていることを確認します。

必要なロール：sn_vul_agile.agile_tool_admin または sn_vul_jira.admin、sn_vul.app_read_all、sn_vul_container.read_all。

手順

1. 次のように移動する。 **All** (すべて) > ワークスペース > 脆弱性マネージャーワークスペース > リスト > 修復タスク/アプリケーション脆弱性一致アイテム/コンテナ脆弱性一致アイテム.
2. 任意のレコードを選択して、Agile の問題を手動で作成します。
3. **[Agile** の問題を作成 **(Create Agile Issue)]** を選択します。
4. 次に示すフィールドに有効な詳細情報を挿入します。

   レコードがいずれかの構成ルールの条件を満たしている場合、次に示すフィールドには構成済みの値が入力されており、ユーザーはフィールド値を変更できます。

フィールド	説明
プロジェクト	Jira の問題を作成するプロジェクトを選択します。
問題タイプ	特定のプロジェクトで作成する問題のタイプを選択します。
アサイン先	問題の作成時に問題をアサインするアサイニーを選択します。
フィールドマッピング	Agile ツールの問題タイプのフィールドを選択し、選択したフィールドの値を直接挿入します。

5. **[Agile** の問題を作成 **(Create Agile Issue)]** をクリックしてレコードを送信します。
   レコードを送信すると、sn_vul_agile_tool_manifest テーブルにそのレコードのエントリが作成されます。

Jira の問題のステータスの手動同期

1 つのレコードのステータスを更新するには、フォームコンテキストメニューの **[Agile** ステータスを同期 **(Sync Agile Status)]** ボタンをクリックします。複数レコードのステータスを更新するには、脆弱性マネージャーのワークスペースでアプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、および修復タスクのテーブルのリストアクション **[Agile** ステータスを同期 **(Sync Agile Status)]** をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：sn_vul_agile.agile_tool_admin または sn_vul_jira.admin、sn_vul.app_read_all、sn_vul_container.read_all。

このタスクについて
ServiceNow でエンティティステータスがクローズ済みの場合、またはエンティティが再度オープンされた場合 (ステータスは [オープン])、ServiceNow から Agile ツールにステータスが同期されます。他のすべてのステータスは、Agile ツールから ServiceNow に反映されます。ユーザーは、関連する構成済みルールにステータスマッピングがないレコードのステータス、またはフォームアクションから直接作成された問題のステータスを同期することはできません。

手順

1. 次のように移動する。 **All** (すべて) > ワークスペース > 脆弱性マネージャーワークスペース > リスト > 修復タスク/アプリケーション脆弱性一致アイテム/コンテナ脆弱性一致アイテム.
2. Jira の問題を作成する複数のレコードを選択し、**[Agile** ステータスを同期 **(Sync Agile Status)]** をクリックします。
   問題が既に作成されているレコードのステータスが更新されるのは、そのレコードがクローズ済みステータスでない場合、かつ構成ルールで選択されたレコードに対してステータスマッピングが存在する場合です。
3. 次の条件に該当する場合、レコードを開くと、**[Agile** ステータスを同期 **(Sync Agile Status)]** がフォームのコンテキストメニューに表示されます。
   - レコードに対して問題が作成されており、レコードのステータスが [クローズ済み] ではない
   - レコードのステータスマッピングが存在する
4. **[Agile** ステータスを同期 **(Sync Agile Status)]** をクリックして、Agile ステータスをマッピングされたステータスと同期します。
   システムプロパティを設定して、Jira から問題ステータスをフェッチするためのバッチサイズを設定できます。
5. [システムのプロパティ] > **[sn_vul_jira.bulkIssueStatusSize]** に移動します。
   - Jira Server の場合、返される問題の最大数 (デフォルトは 50)。最大許容値は、Jira プロパティ「jira.search.views.default.max」によって決まります。この数より大きい値を指定すると、検索結果が切り捨てられます。
   - 問題がフォームアクションから作成された場合、または構成されたルールにステータスマッピングがない場合、それらのレコードはステータス同期の対象とは見なされません。

問題を自動的に作成するようにスケジューラーを構成する

スケジューラーを実行し、sn_vul_agile_tool_manifest テーブルに作成されたレコードに対応する Jira の問題を自動的に作成するようにスケジューラーを構成します。

始める前に
必要なロール：admin または schedule_admin

このタスクについて
sn_vul_agile_manifest テーブルに作成されているアプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、アプリケーション修復タスク、およびコンテナ修復タスクのすべてのレコードが、Jira での問題の作成対象として考慮されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > システム定義 > スケジュール済みジョブ > **Jira** の問題を作成.
2. スケジュール設定済みスクリプトの [実行]、[タイムゾーン]、および [時間] フィールドを変更できます。

スケジュール済みスクリプト実行フォーム

フィールド	説明
実行	スケジュール済みジョブの実行に使用する時間間隔： ○ 日次：指定された時刻に毎日実行されます。 ○ 週次：毎週、指定された曜日の指定された時刻に実行されます。 ○ 月次：毎月、指定された日時に実行されます。 ○ 定期的：指定した繰り返し間隔で実行されます。 ○ 1 回：1 回のみ実行されます。 ○ オンデマンド：オンデマンドですぐに実行されます。 ○ ビジネスカレンダー：エントリ開始：このフィールドで選択したビジネスカレンダーのエントリ開始日に実行されます。ビジネスカレンダーに定義した各ビジネスエントリの開始日に、スケジュール済みジョブが実行されます。たとえば、ビジネスカレンダーが会計年度を表し、各エントリの開始日が会計月である場合、スケジュール済みジョブは毎月最初の日に実行されます。 ○ ビジネスカレンダー：エントリ終了：このフィールドで選択したビジネスカレンダーの終了日に対して実行されます。この選択は、[ビジネスカレンダー：エントリ開始] と同じ方法で実行されますが、関連するビジネスカレンダーエントリの終了日に対して実行されます。 **注:** [ビジネスカレンダー：エントリ開始 (Business Calendar: Entry Start)] または [ビジネスカレンダー：エントリ終了 (Business Calendar: Entry End)] を選択すると、オフセット係数を適用して、選択したビジネスカレンダーの時間スパンの前または後にジョブを実行するようにスケジュールを設定できます。詳細については、[オフセットタイプ] フィールドと [オフセット] フィールドを参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	ビジネスカレンダーの作成と使用、およびビジネスカレンダーエントリの定義の詳細については、「Create a business calendar」および「Define business calendar entries」を参照してください。
曜日	スケジュール済みジョブを実行する日。 ○ [実行] が [週次] の場合は、曜日を選択します。たとえば、水曜日を選択します。 ○ [実行] が [月次] に設定されている場合は、月の日を選択します。たとえば、毎月 25 日の場合、25 を選択します。 このフィールドは、[実行] フィールドで [月次] または [週次] を選択した場合にのみ表示されます。
繰り返し間隔	スケジュール設定された各ジョブ実行の繰り返し間隔の期間。期間を日数、時間数、または分数で入力します。例： ○ 4 日ごとにスケジュール済みジョブを実行するには、[日数] フィールドに「04」と入力します。 ○ 26 時間ごとに実行するには、[時間] フィールドに「26」と入力します。 ○ 13:30:25 の間隔で繰り返す必要がある場合は、[時間] フィールドに「13」と入力し、その後のラベルのない 2 つのフィールドに「30」と「25」を入力します。
時刻	スケジュール済みジョブを実行する時刻。時間、分、秒を 24 時間形式で表します。[タイムゾーン] フィールドで選択した内容によって、このエントリのタイムゾーンが決まります。
タイムゾーン	スケジュール済みジョブの実行時間を指定するときに [時間] フィールドエントリで使用するタイムゾーン。タイムゾーンエントリを次のように選択します。 ○ なし：スケジュール済みジョブを作成しているログインユーザーのデフォルトのタイムゾーンを使用します。たとえば、ユーザーのアサインされたタイムゾーンが米国太平洋標準時であり、[時間] フィールドに 16:45 と入力した場合、スケジュール済みジョブは米国太平洋標準時の午後 4 時 45 分に実行されます。 ○ システムのタイムゾーンを使用：実行するインスタンスに指定されたデフォルトのシス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	テムタイムゾーンを使用します。たとえば、インスタンスのデフォルトのシステムタイムゾーンがヨーロッパ/ロンドンであり、[時間] フィールドに 22:15 と入力した場合、スケジュール済みジョブはロンドン時間の午後 10 時 15 分に実行されます。 ○ 実際のタイムゾーン。 ○ たとえば、[米国/東部] を選択し、[時間] フィールドに「13:30」と入力した場合、スケジュール済みジョブは米国東部標準時の午後 1 時 30 分に実行されます。
run_as	デフォルトでは、[run_ as] フィールドの値は空です。特定のドメインの問題を作成するには、ドメインユーザーの値としてその値を設定します。

問題を自動的に更新するようにスケジューラーを構成する

スケジューラーを実行し、sn_vul_agile_tool_manifest テーブルに追加されたレコードに対応する Jira の問題を自動的に更新するようにスケジューラーを構成します。

始める前に
必要なロール：admin または schedule_admin

このタスクについて
sn_vul_agile_manifest テーブルに作成されているアプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、アプリケーション修復タスク、およびコンテナ修復タスクのすべてのレコードが、Jira での問題の更新対象として考慮されます。レコードがクローズされ、コメントが追加された場合、それらの値も関連付けられている Jira の問題に更新される必要があります。

注:

- 選択した Agile 問題プロジェクトのワークフローで、ユーザーが別のステータスからステータスを直接変更できないように制限されている場合、「問題の更新」スケジュール済みジョブは Jira のステータスを更新しません。
- 追加のコメントを含むエンティティレコードをクローズすると、更新時には最後のコメントのみが考慮され、次回の更新では、関連付けられている Jiraにすべてのコメントが追加されます。

手順

1. 次のように移動する。 **All** (すべて) > システム定義 > スケジュール済みジョブ > **Jira** の問題を更新.
2. スケジュール設定済みスクリプトの [実行]、[タイムゾーン]、および [時間] フィールドを変更できます。

スケジュール済みスクリプト実行フォーム

フィールド	説明
実行	スケジュール済みジョブの実行に使用する時間間隔：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	○ 日次：指定された時刻に毎日実行されます。 ○ 週次：毎週、指定された時刻と曜日に実行されます。 ○ 月次：毎月、指定された日の時刻に実行されます。 ○ 定期的：指定した繰り返し間隔で実行されます。 ○ 1 回：1 回のみ実行されます。 ○ オンデマンド：オンデマンドですぐに実行されます。 ○ ビジネスカレンダー：エントリ開始：このフィールドで選択したビジネスカレンダーのエントリ開始日に実行されます。ビジネスカレンダーに定義した各ビジネスエントリの開始日に、スケジュール済みジョブが実行されます。たとえば、ビジネスカレンダーが会計年度を表し、各エントリの開始日が会計月である場合、スケジュール済みジョブは毎月最初の日に実行されます。 ○ ビジネスカレンダー：エントリ終了：このフィールドで選択したビジネスカレンダーの終了日に対して実行されます。この選択は、[ビジネスカレンダー：エントリ開始] と同じ方法で実行されますが、関連するビジネスカレンダーエントリの終了日に対して実行されます。 **注:** [ビジネスカレンダー：エントリ開始 (Business Calendar: Entry Start)] または [ビジネスカレンダー：エントリ終了 (Business Calendar: Entry End)] を選択すると、オフセット係数を適用して、選択したビジネスカレンダーの時間スパンの前または後にジョブを実行するようにスケジュールを設定できます。詳細については、[オフセットタイプ] フィールドと [オフセット] フィールドを参照してください。 ビジネスカレンダーの作成と使用、およびビジネスカレンダーエントリの定義の詳細については、「Create a business calendar Define business calendar entries」を参照してください。
曜日	スケジュール済みジョブを実行する日。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ [実行] が [週次] の場合は、曜日を選択します。たとえば、水曜日を選択します。 ○ [実行] が [月次] に設定されている場合は、月の日を選択します。たとえば、毎月 25 日の場合、25 を選択します。 このフィールドは、[実行] フィールドで [月次] または [週次] を選択した場合にのみ表示されます。
繰り返し間隔	スケジュール設定された各ジョブ実行の繰り返し間隔の期間。期間を日数、時間数、または分数で入力します。例： ○ 4 日ごとにスケジュール済みジョブを実行するには、[日数] フィールドに「04」と入力します。 ○ 26 時間ごとに実行するには、[時間] フィールドに「26」と入力します。 ○ 13:30:25 の間隔で繰り返す必要がある場合は、[時間] フィールドに「13」と入力し、その後のラベルのない 2 つのフィールドに「30」と「25」を入力します。
時刻	スケジュール済みジョブを実行する時刻。時間、分、秒を 24 時間形式で表します。[タイムゾーン] フィールドで選択した内容によって、このエントリのタイムゾーンが決まります。
タイムゾーン	スケジュール済みジョブの実行時間を指定するときに [時間] フィールドエントリで使用するタイムゾーン。タイムゾーンエントリを次のように選択します。 ○ なし：スケジュール済みジョブを作成しているログインユーザーのデフォルトのタイムゾーンを使用します。たとえば、ユーザーのアサインされたタイムゾーンが米国太平洋標準時であり、[時間] フィールドに「16:45」と入力した場合、スケジュール済みジョブは米国太平洋標準時の午後 4 時 45 分に実行されます。 ○ システムのタイムゾーンを使用：実行するインスタンスに指定されたデフォルトのシステムタイムゾーンを使用します。たとえば、インスタンスのデフォルトのシステムタイムゾーンがヨーロッパ/ロンドンであり、[時間] フィールドに 22:15 と入力した場合、スケジュール済みジョブはロンドン時間の午後 10 時 15 分に実行されます。 ○ 実際のタイムゾーン。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ たとえば、[米国/東部] を選択し、[時間] フィールドに 13:30 と入力した場合、スケジュール済みジョブは米国東部標準時の午後 1 時 30 分に実行されます。
run_as	デフォルトでは、**[run_ as]** フィールドの値は空です。特定のドメインの問題を作成するには、ドメインユーザーの値としてその値を設定できます。

Jira のステータスを **ServiceNow®** に自動的に同期するようにスケジューラーを構成する

Jira 問題のステータスを、sn_vul_agile_manifest テーブルのアプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、およびタスクと同期するように、スケジューラーを構成します。

始める前に
必要なロール：schedule_admin または admin

このタスクについて
スケジューラーは、設定されたスケジュールに従って自動的に実行されます。アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、アプリケーション修復タスク、およびコンテナ修復タスクのテーブルに作成されたレコードのうち、Jira で問題が作成されているレコードのステータスは、Jira プラットフォームでの問題の現在のステータスと、構成ルールのステータスマッピングに基づいて更新されます。

sn_vul_agile_manifest テーブルに作成されているアプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、アプリケーション修復タスク、およびコンテナ修復タスクのすべてのレコードが、Jira での問題の作成対象として考慮されます。

手順

1. 次のように移動する。 **All** (すべて) > システム定義 > スケジュール済みジョブ > 同期ステータス.
2. スケジュール設定済みスクリプトの [実行]、[タイムゾーン]、および [時間] フィールドを変更できます。

スケジュール済みスクリプト実行フォーム

フィールド	説明
実行	スケジュール済みジョブの実行に使用する時間間隔： ○ 日次：指定された時刻に毎日実行されます。 ○ 週次：毎週、指定された時刻と曜日に実行されます。 ○ 月次：毎月、指定された日の時刻に実行されます。 ○ 定期的：指定した繰り返し間隔で実行されます。 ○ 1 回：1 回のみ実行されます。 ○ オンデマンド：オンデマンドですぐに実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ ビジネスカレンダー：エントリ開始：このフィールドで選択したビジネスカレンダーのエントリ開始日に実行されます。ビジネスカレンダーに定義した各ビジネスエントリの開始日に、スケジュール済みジョブが実行されます。たとえば、ビジネスカレンダーが会計年度を表し、各エントリの開始日が会計月である場合、スケジュール済みジョブは毎月最初の日に実行されます。 ○ ビジネスカレンダー：エントリ終了：このフィールドで選択したビジネスカレンダーの終了日に対して実行されます。この選択は、[ビジネスカレンダー：エントリ開始] と同じ方法で実行されますが、関連するビジネスカレンダーエントリの終了日に対して実行されます。 **注:** [ビジネスカレンダー：エントリ開始 (Business Calendar: Entry Start)] または [ビジネスカレンダー：エントリ終了 (Business Calendar: Entry End)] を選択すると、オフセット係数を適用して、選択したビジネスカレンダーの時間スパンの前または後にジョブを実行するようにスケジュールを設定できます。詳細については、[オフセットタイプ] フィールドと [オフセット] フィールドを参照してください。 ビジネスカレンダーの作成と使用、およびビジネスカレンダーエントリの定義の詳細については、「Create a business calendar」および「Define business calendar entries」を参照してください。
曜日	スケジュール済みジョブを実行する日。 ○ [実行] が [週次] の場合は、曜日を選択します。たとえば、水曜日を選択します。 ○ [実行] が [月次] に設定されている場合は、月の日を選択します。たとえば、毎月 25 日の場合、25 を選択します。 このフィールドは、[実行] フィールドで [月次] または [週次] を選択した場合にのみ表示されます。
繰り返し間隔	スケジュール設定された各ジョブ実行の繰り返し間隔の期間。期間を日数、時間数、または分数で入力します。例：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ 4 日ごとにスケジュール済みジョブを実行するには、[日数] フィールドに「04」と入力します。 ○ 26 時間ごとに実行するには、[時間] フィールドに「26」と入力します。 ○ 13:30:25 の間隔で繰り返す必要がある場合は、[時間] フィールドに「13」と入力し、その後のラベルのない 2 つのフィールドに「30」と「25」を入力します。
時刻	スケジュール済みジョブを実行する時刻。時間、分、秒を 24 時間形式で表します。[タイムゾーン] フィールドで選択した内容によって、このエントリのタイムゾーンが決まります。
タイムゾーン	スケジュール済みジョブの実行時間を指定するときに [時間] フィールドエントリで使用するタイムゾーン。タイムゾーンエントリを次のように選択します。 ○ なし：スケジュール済みジョブを作成しているログインユーザーのデフォルトのタイムゾーンを使用します。たとえば、ユーザーのアサインされたタイムゾーンが米国太平洋標準時であり、[時間] フィールドに 16:45 と入力した場合、スケジュール済みジョブは米国太平洋標準時の午後 4 時 45 分に実行されます。 ○ システムのタイムゾーンを使用：実行するインスタンスに指定されたデフォルトのシステムタイムゾーンを使用します。たとえば、インスタンスのデフォルトのシステムタイムゾーンがヨーロッパ/ロンドンであり、[時間] フィールドに 22:15 と入力した場合、スケジュール済みジョブはロンドン時間の午後 10 時 15 分に実行されます。 ○ 実際のタイムゾーン。 ○ たとえば、[米国/東部] を選択し、[時間] フィールドに 13:30 と入力した場合、スケジュール済みジョブは米国東部標準時の午後 1 時 30 分に実行されます。
run_as	デフォルトでは、[run_ as] フィールドの値は空です。特定のドメインの問題を作成するには、必要なドメインユーザーの値としてその値を設定します。

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute の統合

Prisma Cloud Compute 統合を使用すると、ホストをスキャンして脆弱性を検出できます。

脆弱性対応 のバージョン 24.02.0 以降では、Prisma Cloud Compute 統合を使用して、実行中のホストに脆弱性をインポートできます。Prisma ホスト API を使用すると、特定のホストの包

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

括的な脆弱性情報を取得でき、特定の時点でのホスト脆弱性のスナップショットも提供します。この API を使用すると、Prisma と ServiceNow インスタンス間の定期的な同期が可能になります。Prisma は Software as a Service (SaaS) とオンプレミスソリューションの両方として提供されるため、ServiceNow インスタンスから Prisma API を呼び出すには MID サーバーを使用する必要があります。さらに、Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute製品とNow Platformインスタンスが同じ環境にない場合は、MID サーバーを使用する必要があります。詳細については、「MID Server system requirements (MID サーバーのシステム要件)」を参照してください。

脆弱性対応ダッシュボードで脆弱性と脆弱性一致アイテムに関するレポートを表示することもできます。また、これらの脆弱性に優先順位を付けて修正することができます。

統合の表示

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute の一部である統合を表示できます。統合を表示するには、次に移動します: **All** (すべて) > **Prisma Cloud Compute** 統合 > 統合.

次の統合を使用できます。

実行シーケンス	スケジュール	統合	説明
1	日次	Prisma クラウドコンピューティングホスト統合	ホストの脆弱性を取得し、ホストの VIT、検出、および検出されたアイテムを作成します。

注:
Container Vulnerability Response プラグインがインストールされている場合は、Container Vulnerability Response 関連の統合を表示することもできます。

Prisma 統合 プロセス

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute が実行されると、脆弱性情報データベース (NVD) テーブルに共通脆弱性識別子 (CVE) が存在するかどうかが確認されます。既に存在する場合は、既存の情報が使用されます。ただし、CVE が見つからない場合は、プレースホルダーレコードが NVD テーブルに生成されます。これらのプレースホルダー NVD レコードの作成時に、最初は CVE とその名前のみが入力されます。その他の詳細は、入力されません。NVD 統合によって後で入力されることを前提としているためです。統合インスタンスパラメーター *update_nvd* が true に設定されている場合、プレースホルダーの NVD レコードが更新されます。デフォルトでは、インスタンスパラメーターは false に設定されています。ただし、少なくとも NVD 統合が実行されてこれらの詳細が入力されるまでは、重大度や問題に関する基本情報など、CVE についてある程度理解する必要があります。この要件を満たすために、[エクスプロイト有無] フィールドと [修復メモ] フィールドには、Prisma から取得した詳細が入力されます。さらに、この構成はカスタマイズ可能であり、Prisma によって提供される情報に基づいて NVD エントリを他のフィールドに入力するよう指定できます。

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute の準備

次のセットアップタスクを実行して、Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute を準備できます。

事前準備

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute アプリケーションをインストールして設定するには、次のチェックリストを印刷してください。アプリケー

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ションをインストールして脆弱性データを Now Platform® インスタンスにインポートする前に、リストされている項目が完了していることを確認します。

統合準備チェックリスト

タスク	説明
☐	次の情報セットがあることを確認します。 • API ベース URL • ユーザー名とパスワード これらの認証情報は、Prisma Cloud Compute 統合から脆弱性をプルするために使用されます。詳細については、「https://pan.dev/compute/api/」を参照してください。 **注:** MID サーバー はオプションです。 Prisma Cloud Compute 統合に使用されるユーザー認証情報には、画像を監視するための権限が必要です。次のコードを参照してください。 `{"permission":"monitorImages","saas":true,"self-hosted":true}`
☐	まだインストールしてアクティブ化していない場合は、サードパーティアプリケーションをインストールする前に 脆弱性対応 アプリケーションをインストールします。 脆弱性対応 アプリケーションのインストールとアクティブ化の詳細については、「脆弱性対応 のインストール」を参照してください。この統合には、脆弱性対応 のバージョン 16.1 以降が必要です。
☐	エンタイトルメントを取得して、Vulnerability Response Integration with Palo Alto® Networks Prisma Cloud Compute アプリケーションを Now Platform® インスタンスにダウンロードします。
☐	インポートする予定の脆弱性一致アイテムの数を見積もります。 インポートする予定の脆弱性一致アイテムの数をインスタンスが受け入れることができることを確認します。インスタンスが小さすぎると、ロードに時間がかかることがあります。インスタンスのサイズがわからない場合、またはサポートが必要な場合は、ServiceNow テクニカルサポートにお問い合わせください。
☐	統合を管理し、脆弱性一致アイテムを修正する次のグループまたはユーザーがいることを確認します。 admin Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute アプリケーションをインストールします。アサインされていない場合、アドミニストレーターはコンテナ脆弱性アドミン (sn_vul_container.vulnerability_admin) およびその他のロールをアサインします。 sn_vul_container.vulnerability_admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統合準備チェックリスト (続く)

タスク	説明
	Prisma Cloud Compute 統合の構成を完了します。このロールは、コンテナ脆弱性対応 (CVR) アプリケーションとそのレコードに完全にアクセスできます。このアドミニストレーターは、コンテナ脆弱性対応 で統合とルールを設定します。 脆弱性対応グループ デフォルトで脆弱性対応グループは利用可能になっています。脆弱性対応グループにアサインされたユーザーは sn_vul.read_all、sn_vul_container.read_all を継承します。 コンテナ修復オーナーグループ デフォルトでは、コンテナ修復オーナーグループが利用可能です。このグループにアサインされたユーザーは、sn_vul_container.remediation_owner を継承します。コンテナ修復オーナーは、自分または所属するグループにアサインされたコンテナの脆弱性を修復します。 脆弱性アナリスト コンテナ脆弱性アナリストグループにアサインされたユーザーは、sn_vul.vulnerability_analyst を継承します。脆弱性アナリストは、すべての脆弱性一致アイテムの修復を監視します。 まだ作成されていない場合は、追加のグループを作成して、ユーザー管理モジュールでインスタンスにユーザーを追加することをお勧めします。詳細については、「ユーザーグループの作成」を参照してください。
☐	脆弱性対応 Integration with NVD をインストールし、NIST National Vulnerability Database Integration - API (CVE のみ) を実行します。

これで、「Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute アプリケーションの構成」に進む準備が整いました。

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute をインストールする

インスタンスで統合を実行する前に、インストールと構成の手順を完了して、Prisma Cloud Compute 製品が 脆弱性対応 および コンテナ脆弱性対応 と適切に統合されるようにします。このアプリケーションは別のサブスクリプションとして利用できます。

始める前に
インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

必要なロール：admin

手順

1. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute をインストールするインスタンスにログインします。
2. ServiceNow Store に移動します。
3. ServiceNow Store で、Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute アプリケーションを検索します。
4. アプリケーションタイルをクリックします。
   インストールしているアプリケーションに関する詳細情報が表示されます。

   注:
   必要に応じて、「その他の要件」および「依存関係」のセクションをお読みください。

5. [アプリを要求] をクリックし、Now Support ログイン認証情報を入力します。
6. [取得] をクリックします。
7. [インスタンス名] フィールドと [インスタンスの理由] フィールドを更新し、[インスタンスを検証] をクリックします。
8. [要求] をクリックします。
   詳細なインストール手順が記載されたメールが届きます。
9. 次のように移動する。 システムアプリケーション > アプリケーション.
10. アプリケーションを見つけて選択し、[インストール] をクリックします。

タスクの結果
アプリケーションはインスタンスに自動でインストールされます。

次のタスク
環境に Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute を構成します。「Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute アプリケーションの構成」を参照してください。

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute アプリケーションの構成

Prisma Cloud Compute からデータをインポートするように Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute アプリケーションをインストールして構成します。インポートされたデータを使用して、ホストの脆弱性に優先順位を付けて修正できます。

始める前に
必要なロール：admin

手順

1. 統合に関する ServiceNow からのメールを開きます。
2. アドミニストレーターとしてインスタンスにログインします。
3. メールの指示に従って Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute を取得します。
4. 次のように移動する。 **All** (すべて) > **Prisma Cloud Compute** 統合 > アドミニストレーション > 構成.
   Prisma Cloud Compute 構成フォームの各フィールドに記入します。詳細については、「Prisma Cloud Compute の構成フォーム」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. [プロジェクト] リストから、[すべてのプロジェクト] または [特定のプロジェクト **(Specific Projects)]** のいずれかを選択して、すべてのプロジェクトまたは選択したプロジェクトをそれぞれ構成します。
   [特定のプロジェクト **(Specific Projects)]** を選択すると、[利用可能] リストからプロジェクトを選択できます。
6. [完了] または [認証情報を保存してテスト] を選択して、構成を完了します。
   - プロジェクトを構成した場合は、[完了] を選択します。
   - プロジェクトを構成していない場合は、[認証情報を保存してテスト] を選択します
7. 次に移動して新しく作成されたインスタンスを表示します。 **Prisma Cloud Compute** 統合 > アドミニストレーション > 統合インスタンス.
8. [統合インスタンスパラメーター] を選択して、以前に構成したプロジェクトを表示します。
9. 新しく作成された統合インスタンスを実行して、脆弱性一致アイテムをインポートします。
   VIT は、粒度に基づいてさらに作成されます。
10. 脆弱性一致アイテムの粒度を構成します。

    a. 次のように移動する。 **Prisma Cloud Compute** 統合 > イメージ脆弱性キーを構成

    b. 必要なチェックボックスをオンにして、VIT の粒度を設定します。
    脆弱性一致アイテムは、次回のインポート時に選択したキーに基づいて作成されます。

    > **注:**
    > デフォルトでは、[イメージリポジトリ]、 [脆弱性]、および [イメージタグ] の組み合わせに対して VIT が作成されます。キーにコンポーネントを追加して、さらに詳細に設定することができます。たとえば、イメージリポジトリ、脆弱性、イメージタグ、クラスターの組み合わせに対して CVIT を作成できます。脆弱性一致アイテムまたは脆弱性一致アイテムの検出結果が作成されると、チェックボックスは編集できなくなります。

Prisma Cloud Compute 統合の統合実行状況チャート

Prisma Cloud Compute 統合実行状況モジュールは、Prisma Cloud Compute 統合実行のステータスをグラフィカルに表示します。

チャートで、グラフの任意の部分をポイントすると、その部分に固有のデータの概要が表示されます。棒グラフの任意の部分をクリックすると、より詳細な情報を提供するリストが開きます。

必要なロール：脆弱性管理者

Vulnerability Response (脆弱性対応) アプリケーションでユーザーが実行および表示できる内容を管理できるように、ペルソナと詳細なロールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。

詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

データを表示するには、次に移動します: **All** (すべて) > **Prisma Cloud Compute** 統合 > 統合実行ステータス.

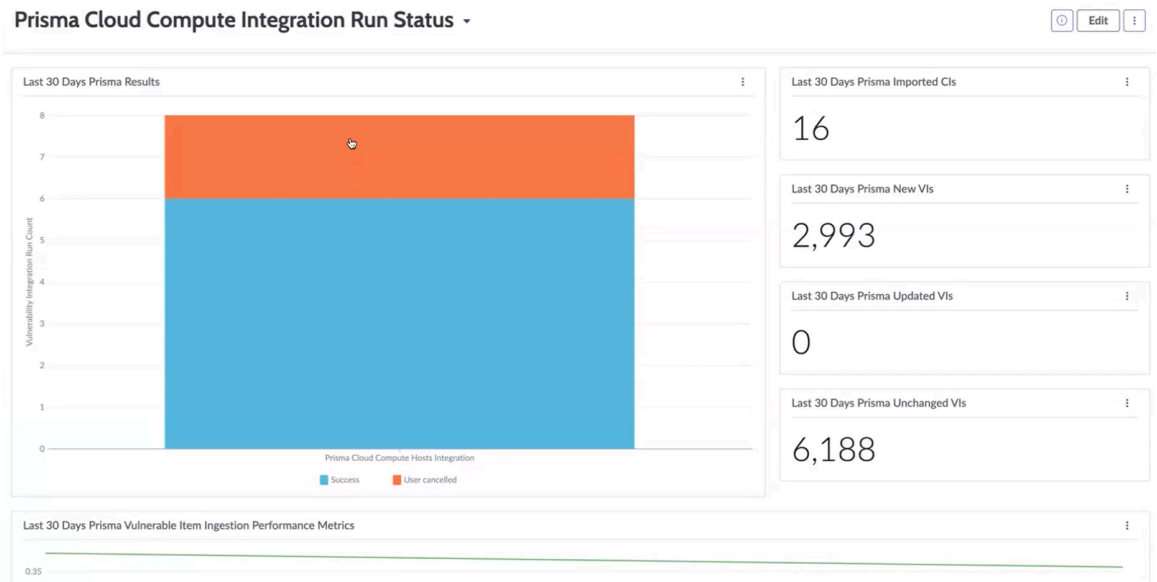
脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で使用可能です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
Tokyo を使用している場合は、Next Experience UI でダッシュボードを表示できますが、一部の機能が失われます。

実行ステータス



Prisma Cloud Compute 統合実行状況チャートレポート

名前	説明
過去 30 日間の Prisma 結果	統合のために完了した統合実行の数。成功した実行と失敗した実行の両方が表示されます。各実行は棒グラフで表示されます。
過去 30 日間の Prisma インポート済み CI	過去 30 日間に Prisma によってインポートされた構成アイテム (CI) の数。整数として表示されます。
過去 30 日間の Prisma 新しい VI	過去 30 日間にインポートされた新規脆弱性一致アイテムの数。整数として表示されます。
過去 30 日間の Prisma 更新済み VI	過去 30 日間にインポートされた更新済み脆弱性一致アイテム (VI) の数。整数として表示されます。
過去 30 日間の Prisma 未変更の VI	過去 30 日間にインポートされた重複脆弱性一致アイテムの数。整数として表示されます。
過去 30 日間の Prisma 脆弱性一致アイテムの取り込みパフォーマンスメトリクス	過去 30 日間の脆弱性一致アイテムの日次パフォーマンスメトリクス

脆弱性統合を手動で作成する

脆弱性統合は、顧客やベンダーが外部システムやベンダーからデータを取得することによって、そのインスタンスの脆弱性データを強化する機能を提供するものです。この機能により、インスタンスを他の脆弱性管理システムと同期させることで、脆弱性修復ライフサイクルを簡素化します。

統合を作成する詳細な手順については、「新しい脆弱性統合の定義」を参照してください。

新しい脆弱性統合の定義

脆弱性統合は、通常は脆弱性データを取得し、データソースまたはカスタムプロセッサを使用してそのレポートデータを処理するために、サードパーティシステムからレポートデータを取り込みます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性 > アドミニストレーション > 統合.
2. [**New**] をクリックします。
3. 必要に応じて、フィールドに入力します。

脆弱性統合

フィールド	説明
名前	統合の記述名。
有効	統合がアクティブかどうかを示します。特定の期間実行しない場合は、使用するパラメーターを設定してジョブを非アクティブ化することができます。
実行	統合を実行する頻度、[日次 (Daily)]、[週次 (Weekly)]、[定期的 (Periodically)] など。前述のとおり、このフィールドの設定に基づいて後続のフィールドが表示または非表示になります。
曜日	統合を実行する日。 ○ [実行] フィールドで [週次 **(Weekly)]** を選択した場合、このフィールドには曜日が表示されます。 ○ [実行] フィールドで [月次 **(Monthly)]** を選択した場合、このフィールドには月日が表示されます。
時刻	統合を開始する時刻。このフィールドは、[実行] フィールドで [日次]、[週次]、または [月次] を選択した場合にのみ表示されます。
アプリケーション	[読み取り専用] この統合が作成されたアプリケーションの名前。
繰り返し間隔	[実行] フィールドで [定期的 **(Periodically)]** を選択した場合、このフィールドには統合が再度実行されるまでの日数と時間が表示されます。
開始中	[実行] フィールドで [定期的 **(Periodically)]** を選択した場合、このフィールドには定期的な更新の起点として使用される日付と時刻が表示されます。
条件付き	条件付きパラメーターを追加する場合は、このフィールドを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
条件	[条件付き **(Conditional)**] チェックボックスをオンにした場合は、ここに条件を入力します。
統合の詳細	
統合スクリプト	統合の実行時に実行される VulnerabilityIntegrationBase を拡張するスクリプトインクルードを選択します。このスクリプトは、サードパーティシステムからデータを取得する方法を定義します。
統合ファクトリスクリプト	統合スクリプト用に選択されたスクリプトインクルードのビルド方法を定義するスクリプトを入力します。詳細については、「統合ファクトリスクリプトのフィールド」を参照してください。 **注:** スクリプトには ServiceNow と 脆弱性対応 の両方の専門知識が必要です。
プロセッサ戦略をレポート	統合の実行時に統合スクリプトによって返されたデータを処理するために使用する戦略を選択します。 ○ データソースを使用してデータを処理する場合は、[データソース添付ファイル] を選択します。 ○ [カスタムレポートプロセッサ] を選択して、カスタムプロセッサを選択します。
プロセッサをレポート	[プロセッサ戦略をレポート] フィールドで [カスタムレポートプロセッサ] を選択した場合は、統合の実行時に実行される VulnerabilityReportProcessorBase スクリプトインクルードを拡張するスクリプトインクルードを選択します。 このスクリプトで、統合スクリプトによって返されるデータの処理方法を定義します。
プロセッサ生成スクリプト	レポートプロセッサ用に選択されたスクリプトインクルードのビルド方法を定義するスクリプトを入力します。

4. **[Submit]** をクリックします。

関連情報

- 脆弱性統合スクリプト
- プロセッサ戦略をレポート
- 統合ファクトリスクリプトのフィールド
- 手動での脆弱性統合の実行

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性統合スクリプト

脆弱性統合フォームでは、統合スクリプトは VulnerabilityIntegrationBase スクリプトインクルードを拡張するスクリプトインクルードへの参照となります。

このスクリプトに含まれる機能は、VulnerabilityIntegrationController によって呼び出され、外部データソースからデータを取得する方法を管理します。VulnerabilityIntegrationBase の各サブクラスは、呼び出しプロセスに関するコンテキスト情報へのアクセスを有しています。この情報は、次のメンバー変数を介して利用できます。

- integrationGr：統合の実行を要求した脆弱性統合レコードの GlideRecord。
- integrationProcessGr： 統合の現在のプロセスのコンテキスト情報を提供する GlideRecord。

脆弱性プロセスには、一般的にページネーションの目的で、統合内で使用される特別なパラメーターが含まれています。脆弱性統合の各実行 (脆弱性統合実行と呼ばれる) には、少なくとも 1 つの関連する脆弱性統合プロセスがあります。マルチコール統合の場合、脆弱性統合実行ごとに 1 つ以上の脆弱性統合プロセスレコードがあります。

スクリプトインクルードは、retrieveData() メソッドの実装を提供し、レポートプロセッサスクリプトによって処理されるオブジェクトを返す必要があります。retrieveData によって返されるオブジェクトは、コンテンツ、contentType、および拡張のプロパティを持つシンプルなオブジェクトです。

VulnerabilityIntegrationBase.retrieveData() のスクリーンショットを次に示します。

VulnerabilityIntegrationBase.retrieveData()

```
/**
 * Retrieves data (generally from an external system) to be passed to a report processor.
 * Subclasses (i.e. concrete implementations of a Vulnerability Integration) should implement/override this
 * function.
 * The class should return an object structured as follows:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 * For multipage integrations (where multiple calls/integration processes must run), this function should check
 * the integrationProcessGr's parameters.
 */
retrieveData: function() {
    return {contents: "", contentType: "", extension: ""};
},
```

retrieveData() のロジックは、データの取得に必要なインターフェイスによって異なります。たとえば、プルされるデータのソースに REST API がある場合、このメソッドの本体は RESTMessageV2 を介して REST エンドポイントを呼び出すことができます。その後、呼び出しの応答を解析したり、添付ファイルに格納したりすることが可能で、その詳細を使用して戻りオブジェクトをビルドできます。

単一コール統合

単一コール (単一ページ) 統合スクリプトは、最も簡単なタイプの統合です。このスクリプトでは、データを取得するために 1 回のコール (多くの場合、外部データソースに対するコール) が必要です。単一ページ / 単一コールの統合では、retrieveData() のみを実装する必要があります。

簡単な単一コール統合スクリプトを示すサンプルを次に示します。RESTMessageV2 を作成して実行します。次に、応答本文をコンテンツとして使用し、想定される contentType および拡張子とともにオブジェクトを返します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

単一コール統合スクリプト

```
var SingleRunVulnerabilityIntegration = Class.create();
SingleRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.
     */
    retrieveData: function() {
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'SingleRunVulnerabilityIntegration'
});
```

複数コール統合

複数のコール (または複数のページ) の統合スクリプトは少し複雑です。データを取得するには、データソースを複数回呼び出す必要があります。

単一コール統合と同様に、複数コール統合にも retrieveData() が実装されている必要があります。retrieveData() の本体では、統合は VulnerabilityIntegrationBase によって提供される hasMoreData() および setNextRunParameters() メソッドを使用します。

hasMoreData() メソッドは、VulnerabilityIntegrationController に、より多くのデータをプルするためのプロセスを挿入するよう指示する単一のブール値を受け入れます。hasMoreData() に true を渡すと、次のプロセスにコンテキストを提供するために setNextRunParameters() が呼び出されます。

setNextRunParameters() メソッドは、次に retrieveData() を呼び出す際に使用されるコンテキスト情報を提供する単一のオブジェクトを受け入れます。このオブジェクトは、後続の retrieveData() の呼び出しにステータスを渡すために使用されます。ユースケースの例としては、現在のページ番号とページサイズを示すオブジェクトを Web サービスに渡すことが挙げられます。

複数コール統合の場合、各 retrieveData() コールが最初に現在のプロセスパラメーターをチェックします。_getProcessParameters() メソッドは、すべての VulnerabilityIntegrationBase に、前のプロセスで設定されたパラメーターを取得する利便性として提供されます。パラメーターがない場合は、最初のプロセスであることを示します。

次のスクリーンショットは、複数コール統合スクリプトのサンプルを示しています。このスクリプトでは、単一コール統合の例を拡張して、基本的なページネーションをサポートする REST エンドポイントの呼び出しを示しています。1 ページのデータを取得し、取得するデータがまだあることを認識して、次のプロセスに取得するページを指示する方法を示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

複数コール統合スクリプト

```
var MultiRunVulnerabilityIntegration = Class.create();
MultiRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'MultiRunVulnerabilityIntegration'
});
```

retrieveData() の戻り値としての添付ファイル

retrieveData() から添付ファイルを返すことが望ましい場合もあります。添付ファイルを作成したり、取得したりするロジックは実装に固有のものですが、添付ファイルが判明した後、その情報を返すことができます。

添付ファイルを提供するために、retrieveData() は次のようなオブジェクトを返します。

```
{
    contents: "attachment-sys-id",
    contentType: "sys_attachment"
}
```

前の例を拡張して、REST メッセージの応答本文を統合プロセスレコードに保存する例を示します。その後、その添付ファイル識別子をリターンオブジェクトのコンテンツとして返します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

retrieveData から添付ファイルを返す

```
var MultiRunAttachVulnerabilityIntegration = Class.create();
MultiRunAttachVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     *
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);

        var table = this.integrationProcessGr.getTableName();
        var sysId = this.integrationProcessGr.getUniqueValue();
        var fileName = this.integrationProcessGr.getValue("number") + ".xml";
        message.saveResponseBodyAsAttachment(table, sysId, fileName);
        var response = message.execute();
        var responsSysId = response.getResponseAttachmentSysid();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responsSysId, contentType: "sys_attachment", extension: "xml"};
    },

    type: 'MultiRunAttachVulnerabilityIntegration'
});
```

プロセッサ戦略をレポート

[脆弱性統合] フォームの [プロセッサ戦略をレポート] フィールドを使用して、脆弱性統合プロセスの実行時に脆弱性統合スクリプトによって返されたデータの処理方法を選択します。

デフォルト値は [データソース添付ファイル]です。このメソッドは、取得したデータを受け取り、それをデータソースに渡してシステムにインポートするベースライン実装です。[カスタムレポートプロセッサ] を選択すると、データを処理するためのカスタムプロセッサスクリプトを選択できます。

データソース添付ファイルレポートプロセッサ戦略の使用

データソース添付ファイルレポートプロセッサ戦略は、統合スクリプトによって取得されたデータを、構成済みのデータソースに渡すために使用されます。

始める前に

必要なロール：sn_vul.vulnerability_write

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性 > アドミニストレーション > 統合 をクリックし 、新しい統合を作成します。
2. [プロセッサ戦略をレポート] フィールドで、[データソース添付ファイル] を選択します。
3. フォームヘッダーを右クリックし、[保存] をクリックします。
4. [脆弱性統合データソース] 関連リストで、[新規] をクリックします。
5. 使用するデータソースを定義します。
6. **[Submit]** をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

7. 追加のデータソースが必要な場合は、手順 4 ～ 6 を繰り返します。
   複数のデータソースが情報を送信する順序を [順序] フィールドで必ず指定します。
8. [更新] をクリックします。

カスタムレポートプロセッサのスクリプトについて

脆弱性統合フォームでは、レポートプロセッサは VulnerabilityReportProcessorBase スクリプトインクルードを拡張するスクリプトインクルードへの参照となります。このスクリプトに含まれる機能は VulnerabilityIntegrationController によって呼び出され、統合スクリプトによって返されたデータを処理する方法を定義します。

VulnerabilityReportProcessorBase の各サブクラスは、呼び出しプロセスに関するコンテキスト情報へのアクセスを有しています。この情報は、次のメンバー変数を介して利用できます。

- integrationGr：統合の実行を要求した脆弱性統合レコードの GlideRecord。
- integrationProcessGr： 統合の現在のプロセスのコンテキスト情報を提供する脆弱性プロセスの GlideRecord。

スクリプトインクルードは、`processReport()` メソッドの実装を提供する必要があります。processReport() に渡されるオブジェクトは、retrieveData によって返されるオブジェクトであり、そのため、コンテンツ、contentType、および拡張のプロパティを持つシンプルなオブジェクトです。processReport() の実際のロジックは実装に固有のものであり、提供されるレポートデータに依存します。

VulnerabilityReportProcessorBase.processReport() のスクリーンショットを次に示します。

カスタムレポートプロセッサのスクリプト

```
/*
 * Processes the reportData that was pulled by a Vulnerability Integration's retrieveData().
 * The expectation is that retrieveData() will return an object that matches this function's input parameter.
 *
 * @param reportData = object with the following format:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 */
processReport: function(reportData) {
    return;
},
```

統合ファクトリスクリプトのフィールド

脆弱性統合フォームには、統合ファクトリスクリプト、および [カスタムレポートプロセッサ] レポートプロセッサ戦略が選択されている場合はプロセッサファクトリスクリプトが含まれます。これらのフィールドは、個別にスクリプトインクルード参照フィールド、統合スクリプト、およびレポートプロセッサによって定義されたオブジェクトを実際にインスタンス化するロジックを提供するために使用されます。

スクリプトインクルードが選択されると、両方のフィールドに引数なしのコンストラクタ呼び出しが事前に入力されます。多くの場合はこれで十分ですが、スクリプトオブジェクトをインスタンス化するためにさらに多くのロジックが必要になる場合があります。

integrationProcessGr レコードはファクトリスクリプトのフィールドに公開されるため、必要に応じてプロセス固有の情報を使用できます。

手動での脆弱性統合の実行

脆弱性統合は、スケジュールに基づいて実行するように構成されています。ただし、必要に応じて手動で実行することもできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：sn_vul.vulnerability_write

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

このタスクについて
統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、 脆弱性対応のバージョン 18.2.4 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性 > アドミニストレーション > 統合.
2. 実行する統合を開きます。
3. [今すぐ実行] をクリックします。

脆弱性の手動取り込み

脆弱性を 脆弱性対応 アプリケーションに手動で取り込み、スキャナーの結果を待たずに迅速に修復できるようにします。

Rapid7 などのサードパーティのスキャナーは、脆弱性データを 脆弱性対応 にインポートし、データを処理して検出結果を報告するのに役立ちます。手動取り込み統合を使用すると、スキャナーがリスクにさらされている資産について報告するのを待つのではなく、事前対応的に脆弱性を取り込み、修復することができます。脆弱性を手動で取り込むことで、ゼロデイエクスプロイトなどの不明な脅威から資産を効果的に保護します。

脆弱性の手動取り込み

次のファイル形式でテンプレートをアップロードすることで、脆弱性データをインポートできます。

- Excel
- カンマ区切り値 (CSV)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

テンプレートにアクセスしてダウンロードするには、 **All** (すべて) > 脆弱性対応 > 手動脆弱性一致アイテム取り込み > ファイル **UI** をアップロード.

テンプレートにレコードを入力するときは、次の重要なポイントに注意してください。

- [重大度/ステータス] 列のレコードで入力を間違えないでください。入力を間違えると、そのレコードはスキップされます。
- 列名は変更しないでください。
- 最初の行以外は列名を入力しないでください。
- Microsoft Excelテンプレート内のシートの順序は変更しないでください。脆弱性データは常に 2 枚目のシートに存在する必要があります。
- 手動検出入力シート以外のシートには、脆弱性の詳細を記載しないでください。
- ファイル名には、英数字および特殊文字 (ダッシュ (-)、ピリオド (.)、プラス (+)、アンダースコア (_)、スペース、丸括弧 ((、))、記号 (@) など) 以外の文字は使用しないでください。

テンプレートにデータを入力する方法については、「脆弱性の手動取り込み用テンプレート」を参照してください。

脆弱性対応 v24.0.6 以降、Microsoft Excelテンプレートに追加の列を作成することもできます。詳細については、「 KB1646630 」を参照してください。

手動取り込み統合

ファイルがアップロードされると、統合がトリガーされます。アップロードされたファイルのタイプに基づいて、関連する統合がトリガーされます。

統合を表示するには、次に移動します: **All** (すべて) > 脆弱性対応 > 手動脆弱性一致アイテム取り込み > 統合.

次のベースシステムの手動取り込みの統合は、デフォルトで使用できます。

統合

統合タイプ	説明
手動取り込み Excel 統合	脆弱性取り込みプッシュキューテーブルからアップロードされた最新の Microsoft Excel ファイルをフェッチしてデータを取得し、添付ファイルをそれぞれの統合実行にコピーします。
手動取り込み CSV 統合	脆弱性取り込みプッシュキューのテーブルからアップロードされた最新の CSV ファイルをフェッチすることでデータを取得し、添付ファイルをそれぞれの統合実行にコピーします。

手動取り込みのサードパーティ統合では、デフォルトで次の 2 つの統合インスタンスパラメーターを持つ統合インスタンスが作成されます。

- max_input_records：テンプレートで作成できるレコードの数を定義します。このパラメーターで指定した数を上回るレコードを追加すると、追加レコードはスキップされます。レコードの数は [値] 列で更新できます。テンプレートでのレコードの推奨作成回数は 1000 です。この値を超えると、パフォーマンスが低下する可能性があります。
- insert_fixed: 修復された脆弱性検出をインポートします。

統合インスタンスパラメーターを表示するには、次に移動します: **All** (すべて) > 脆弱性対応 > 手動脆弱性一致アイテム取り込み > 統合 をクリックし、統合のソースインスタンスをクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

または、 **All** (すべて) > 脆弱性対応 > 統合インスタンス をクリックし、[手動取り込み] をクリックします。

脆弱性を手動で取り込む

脆弱性データを含むテンプレートをアップロードして、脆弱性を手動で取り込みます。

始める前に

必要なロール：sn_vul.vulnerability_admin

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 手動脆弱性一致アイテム取り込み > ファイル **UI** をアップロード.
2. Excel または CSV のリンクをクリックし、それぞれの形式でテンプレートをダウンロードします。
3. テンプレートで、レコードの脆弱性データを入力します。
   テンプレートにデータを入力する方法については、「脆弱性の手動取り込み用テンプレート」を参照してください。
4. [ファイルをインポート] をクリックし、更新されたテンプレートをアップロードします。
5. **[Submit]** をクリックします。
   脆弱性統合プッシュキューのページが表示されます。統合実行が完了した後、統合インスタンスのリスト、統合実行のステータス、およびログメモを表示できます。

次のタスク

ファイルをアップロードしたら、次の場所に移動します: **All** (すべて) > 脆弱性対応 > 手動脆弱性一致アイテム取り込み > 統合. 統合の実行が成功したことを確認します。

手動統合の実行の確認

統合の実行が成功したことを確認します。統合の実行によって作成または更新された個々の検出数と脆弱性一致アイテム (VI) の数を表示します。

始める前に

必要なロール：sn_vul.vulnerability_admin

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 手動脆弱性一致アイテム取り込み > 統合.
2. アップロードされたファイルタイプに基づいて、統合の名前をクリックします。
3. [脆弱性統合実行] タブをクリックします。
4. 統合実行番号をクリックします。
5. [アイテム] タブをクリックします。
6. [アイテム] タブの情報を確認します。

[アイテム] タブ

タブ/フィールド	説明
[アイテム] タブ	インポートされた VI の合計数を表示します。[ディスカバリー] タブにリストされている数値の加算によって、インポートされた検出の合計を確認できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タブ/フィールド	説明
新規アイテム	この統合実行から作成される脆弱性一致アイテムの数を表示します。
インポートされたアイテム	このセクションのすべてのフィールドの合計を表示します。
重複アイテム	重複アイテムを表示します。このフィールドは入力されなくなりました。
更新されたアイテム	この統合実行中の脆弱性一致アイテムの更新回数を表示します。この値は、更新される一意の脆弱性一致アイテムの数ではありません。たとえば、統合実行中に脆弱性一致アイテムが 2 回更新された場合、2 回とカウントされ、更新済みアイテムが 2 っと表示されます。
未変更のアイテム	統合実行中に検出されたが、関連するフィールド値が変更されていないために更新されなかった、データベースに存在する脆弱性一致アイテムを表示します。

次のタスク

統合の実行が成功したことを確認したら、次に移動します: **All** (すべて) > 脆弱性対応 > 手動脆弱性一致アイテム取り込み > ファイル履歴をアップロード. 失敗したレコードがあるかどうかをメモを見て確認します。

手動検出の自動クローズの構成

手動検出の自動クローズを有効にして、古い手動検出を自動的にクローズします。

始める前に

必要なロール：sn_vul.vulnerability_admin

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 手動脆弱性一致アイテム取り込み > ファイル **UI** をアップロード.
2. [自動クローズ構成を変更] をクリックします。
3. [手動検出] タブをクリックします。
4. [手動検出を自動クローズ] チェックボックスが選択されていることを確認します。
5. [最後に発見された手動検出 (日前)] フィールドに、手動検出をクローズするまでの日数を入力します。
   デフォルトは 90 日です。日数には任意の正の値を入力できます。

アップロードステータスの確認

脆弱性統合の実行が成功したか、部分的に成功したか、失敗したかを確認します。

始める前に

必要なロール：sn_vul.vulnerability_admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 手動脆弱性一致アイテム取り込み > ファイル履歴をアップロード.
2. [脆弱性統合プッシュキュー] テーブルで、アップロードの時刻とアップロードのステータスをそれぞれ [作成日時] 列と [ステータス] 列で確認します。
3. オプション: [メモ] フィールドで、失敗の理由を確認します。

脆弱性の手動取り込み用テンプレート

テンプレートには、脆弱性と構成アイテム (CI) データを入力する必要がある列が用意されています。テンプレートが入力されてアップロードされた後、データが処理されます。

テンプレートの入力手順

テンプレートに詳細を入力するには、次の表の指示に従ってください。

テンプレートの手順

列	必須/オプション?	文字列の長さ (最大)/有効な値	説明
資産 ID	オプション	255	ユニバーサルユニーク識別子 (UUID) または資産 ID。スキャナーによって生成された値にすることができます。
次の 5 つの列の少なくとも 1 つに情報を入力します。			
MAC アドレス	必須	24	ホストまたは資産情報。指定されたすべての値の組み合わせは、資産に対して一意である必要があります。
FQDN	必須	255	
NETBIOS	必須	255	
IP アドレス	必須	255	
ホスト名	必須	255	
残りの列は互いに依存しません。			
脆弱性 ID	必須	255	脆弱性情報データベース (NVD) の脆弱性、またはサードパーティのスキャナーから返された ID を表します。
脆弱性のサマリー	オプション	512	脆弱性の簡単な説明。 脆弱性 ID が利用できない場合にのみデータベースに追加されます。
重大度	オプション	重大、高、中、低、なし	脆弱性の重大度。 脆弱性 ID が利用できない場合にのみデータベースに追加されます。レコードが空の場合、デフォルトでは「重大」と見なされます。
ポート	オプション	適用外	脆弱性が検出されるポート。 値は有効な整数である必要があります。無効な入力がある場合、レコードはスキップされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テンプレートの手順 (続く)

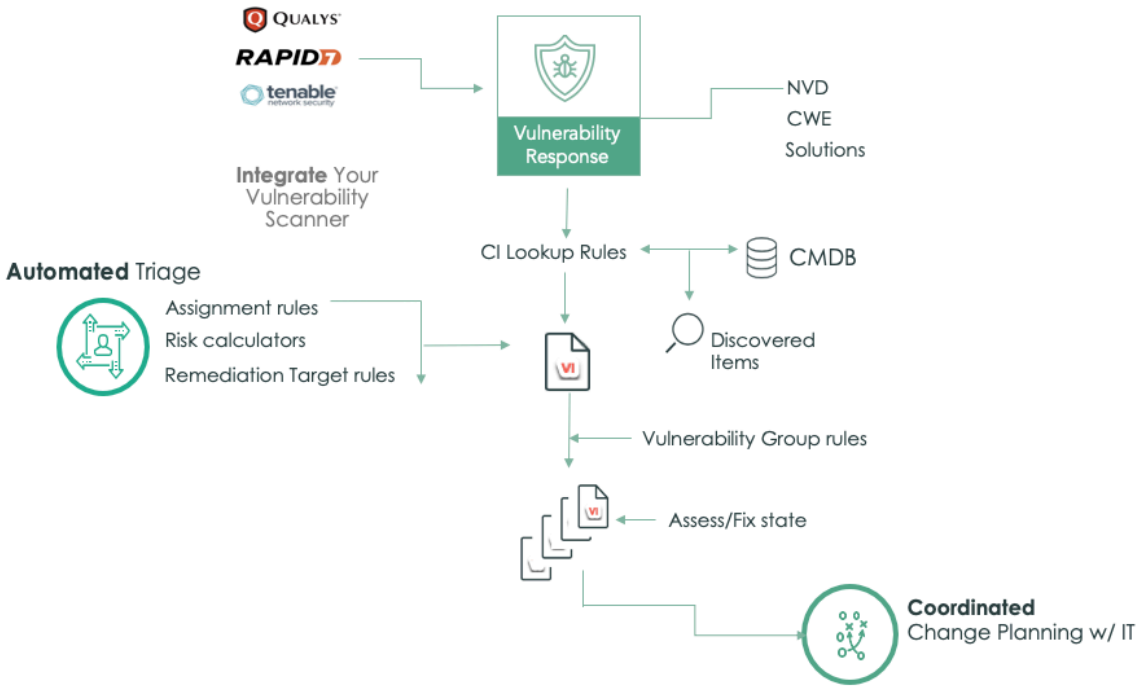
列	必須/オプション?	文字列の長さ (最大)/有効な値	説明
プロトコル	オプション	40	使用されているネットワークプロトコルのタイプ。
実証	オプション	4000	脆弱性の場所またはシステムパスを表します。
状態	オプション	オープン、修正済み	検出のステータス。 レコードが空の場合、デフォルトでは「オープン」と見なされます。

脆弱性対応 の修復の概要

脆弱性対応 の修復は、インポート完了の確認、新しい脆弱性のトリアージ、完了までの進捗状況の監視から成る段階的なプロセスです。このようにアプローチすることで、修復は管理しやすく、タイムリーで、さまざまな意味で自動化されるようになります。

会社の資産全体のセキュリティ体制を理解することで、修復の対象となる最も重要な脆弱性を識別することができます。この修復プロセスでは、脆弱性対応 および Qualys 脆弱性統合 などのサードパーティ統合がインストールされ、設定されている必要があります。

Vulnerability Response 統合プロセスフロー



サードパーティ統合のインポートが正常に完了したことを確認する

このプロセスの最初のフェーズでは、すべてが正しく機能していることを確認します。脆弱性対応は、脆弱性情報データベース (NVD) および共通脆弱性タイプ一覧 (CWE) の脆弱性をダウンロードするように事前設定されています。サードパーティインポートは、脆弱性一致アイテムと修復タスクの作成に必要なデータを提供します。修復が成功するかどうかは、脆弱性と脆弱性一致アイテムを一貫して正常にインポートできるかどうかに依ります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

インポート時に CI ルックアップルールで、サードパーティ資産と 構成管理データベース (CMDB) の資産を照合します。すべての資産は、[検出されたアイテム] モジュールに保存されます。CI 情報はソリューションの実装にとって重要なものです。

> **注:**
> サードパーティ統合がインストール、設定されると、たとえば、サードパーティベンダーが API 呼び出しをスロットル (制限) した場合など、インポートが失敗する可能性はほとんどありません。インポートが失敗した場合は、迅速な対応が必要です。

サポートされているサードパーティ統合の統合ステータス実行レポートはアプリケーションに付属しており、インポートの概要を図示することができます。このレポートを使用するか、独自のレポートを作成することで、最新のインポートが成功したかどうかは簡単に判断できます。サポートされている統合の詳細については、「脆弱性対応 の統合」を参照してください。

脆弱性と脆弱性一致アイテムのレビューとトリアージ

修復の次のフェーズでは、新しい脆弱性と脆弱性一致アイテムをレビューする必要があります。脆弱性一致アイテム (VI) とは、脆弱性と構成アイテム (CI) の組み合わせが検出されたものです。脆弱性一致アイテムが形成されると、VI をアサインし、そのリスクを判断し、修復ターゲットを設定するさまざまなルールが実行されます。必要に応じてルールを調整し、脆弱性一致アイテムが正常にトリアージされたことを確認します。

既存の脆弱性修復の進捗状況を監視する

修復の最終フェーズは、進捗状況の監視から成ります。

- 表示されていないパッチ実装のインポートステータスを確認し、IT 運用でフォローアップします。
- 規制コンプライアンス義務の進捗状況を追跡し、その完了を確認します。
- 保留されたアイテムのステータスを確認し、修復を変更または実装します。
- 脆弱性管理ダッシュボードを監視します。傾向を確認し、レポートをリアルタイムで表示し、修復ターゲットの達成率を追跡するメトリクスを使用するには、パフォーマンスアナリティクス 向け脆弱性対応アプリケーションを使用してプロセスを監視することをお勧めします。
- 脆弱性対応 での古い検出のクローズ。

脆弱性対応 統合のインポートの正常完了の確認

インポートが正常に完了したかどうかを判断する最も簡単な方法は、統合実行状況ダッシュボードを使用することです。統合実行状況ダッシュボードには、サードパーティ統合実行のステータスに関するグラフィカルビューの例が表示されます。

Qualys および Rapid7 の脆弱性統合には、統合実行状況ダッシュボードがあります。チャートの内容の詳細については、「Qualys 統合実行状況チャート」または「Rapid7 脆弱性統合実行状況チャート」を参照してください。

> **注:**
> ServiceNow® によって提供されていない統合のチャートは、ダッシュボードのレポートから作成できますが、ServiceNow の専門知識が必要な場合があります。レポートとダッシュボードの作成の詳細については、「レポートの概要」および「ダッシュボード」を参照してください。

脆弱性対応 脆弱性一致アイテム検出データの表示

脆弱性対応 とのサードパーティスキャナー統合によって収集された全データは、脆弱性一致アイテムレコード (VIT) の [ディスカバリー] タブと [初期検出] タブに表示されます。このデータは Now Platform® インスタンスの脆弱性一致アイテム検出リストの検出レコードにも表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
サードパーティ統合によって脆弱性一致アイテム検出データが取得されます。検出は、スキャナーによって報告される脆弱性の個別の発生です。検出データは脆弱性一致アイテムとペアリングされ、検出のステータスに基づいて VI ステータスが更新されます。VI が見つからない場合は、新しい VI が作成されます。検出は、スキャナーによって直接検出されたデータによってのみオープンまたはクローズされます。

必要なロール：

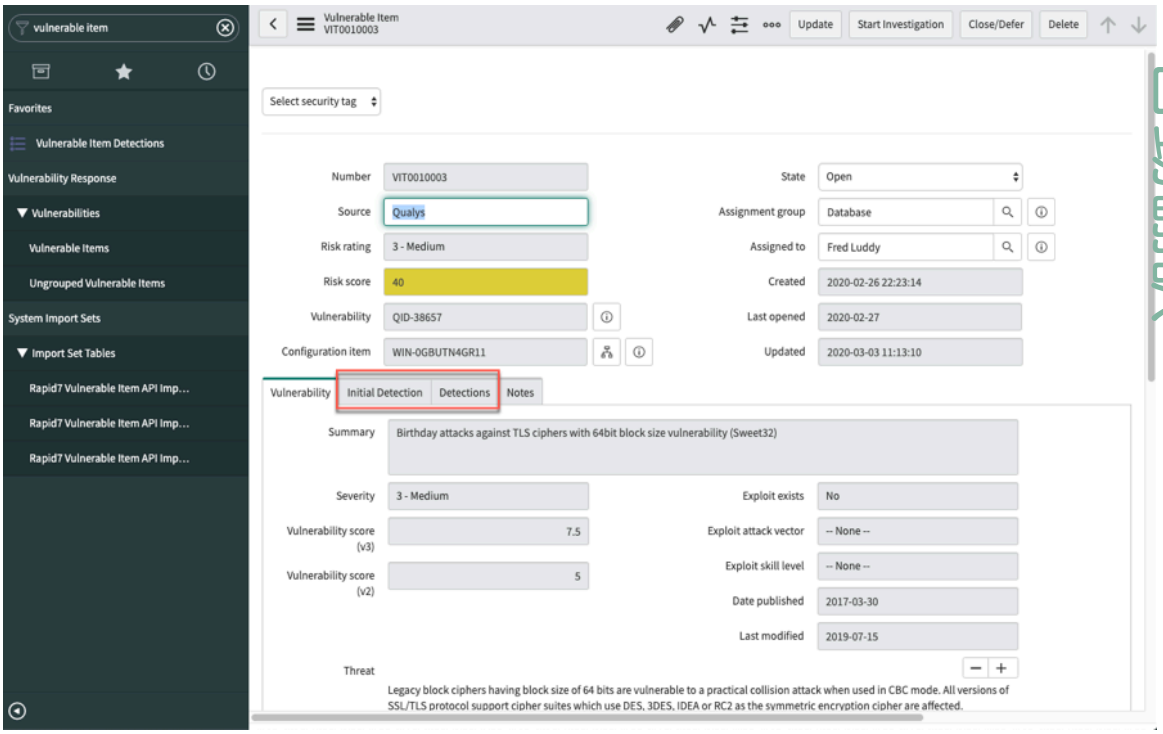
- sn_vuln.admin は統合実行を開始し、脆弱性一致アイテム検出データを表示します。
- sn_vul.remediation_owner は、脆弱性一致アイテム検出から作成された脆弱性一致アイテムにアサインされ、VI レコードのデータを表示します。

手順

1. 脆弱性一致アイテム検出データを表示するには、脆弱性一致アイテムレコードに移動してそれを開きます。

   レコードは [初期検出] タブと [ディスカバリー] タブに表示されます。

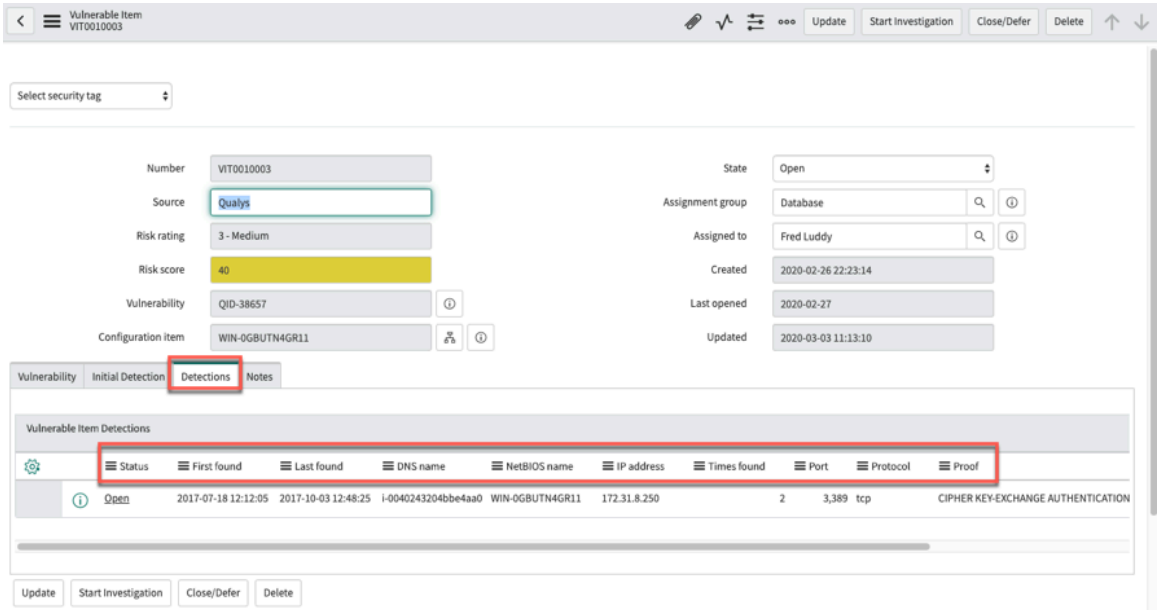
   注:
   以前に [構成の詳細] タブに表示されていたデータは、 [初期検出] タブと [ディスカバリー] タブに他の検出データとともに表示されます。



2. [ディスカバリー] タブをクリックします。

   サードパーティスキャンの結果から脆弱性一致アイテムが作成されると、次の図に示すように、スキャンのデータが検出レコードに表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[脆弱性一致アイテムの検出] セクションの各行は、個別の検出からのデータを表します。[初回検出] 列には、脆弱性一致アイテムがスキャナーによって最初に検出された日付が表示されます。[前回検出] 列には、最新の検出日が表示されます。[ソース] フィールドには、データを取得したスキャナーが表示されます。

注:
Qualys の脆弱性一致アイテム検出では、VI レコードの以下のフィールドが廃止され、入力されなくなりました。

- Qualys 重大度
- ソースによる最終更新

また Qualys では、前の図に示すように、VI がスキャンから作成されると、スキャンの結果の値が検出レコードの [実証] 列に表示されます。ただし、この値は VI レコードの上部には表示されません。

Rapid7 の場合、VI がスキャンから作成されると、スキャンの [実証] の値は検出レコードの [実証] 列と VI レコードの上部の両方に表示されますが、デフォルトでは表示されません。この値を VI レコードの上部に表示するには、フォームレイアウトから [実証] フィールドを選択します。

3. オプション: レコードの [ディスカバリー] タブのレイアウトを構成するには、次の手順を実行します。

   a. デフォルトでは、以下の列が [ディスカバリー] タブに表示されます。
   - ステータス
   - 初回検出 (データ)
   - 最終検出日 (日付)
   - DNS 名
   - Net BIOS 名
   - IP アドレス
   - 検出回数

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ポート
- プロトコル
- 実証
- SSL

注:

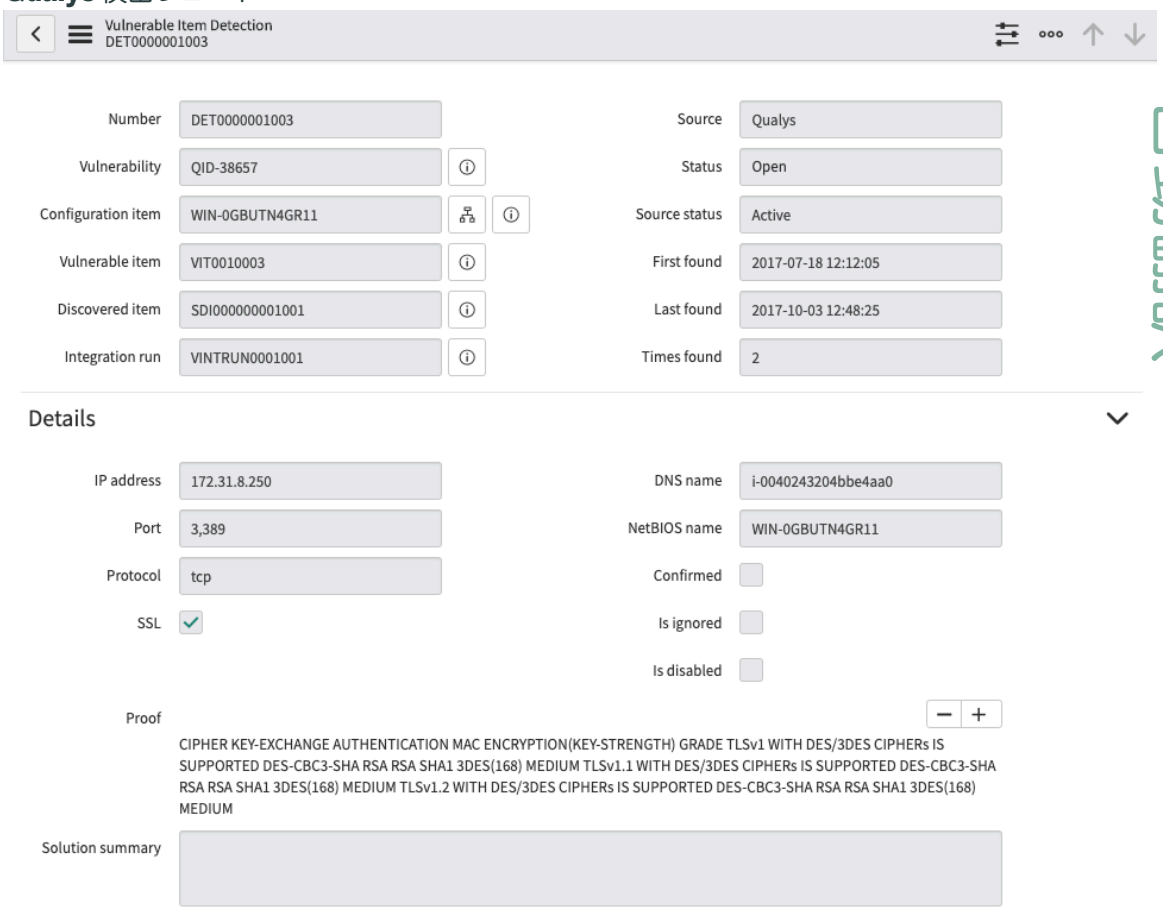
(Optional) 注意：列に値がない場合、そのフィールドのデータはスキャナーによって検出されていません。

b. 歯車アイコン ( ) をクリックしてビューをカスタマイズします。

c. スラッシュバケットから特定のデータを表示する列を選択し、**[OK]** をクリックします。

4. [ディスカバリー] タブを選択した状態で、 [ステータス] 列でアイテムをクリックして検出レコードを開き、その脆弱性一致アイテムに関連付けられた、ソリューションサマリー (Rapid7 InsightVM 統合のみ) などの詳細を表示します。

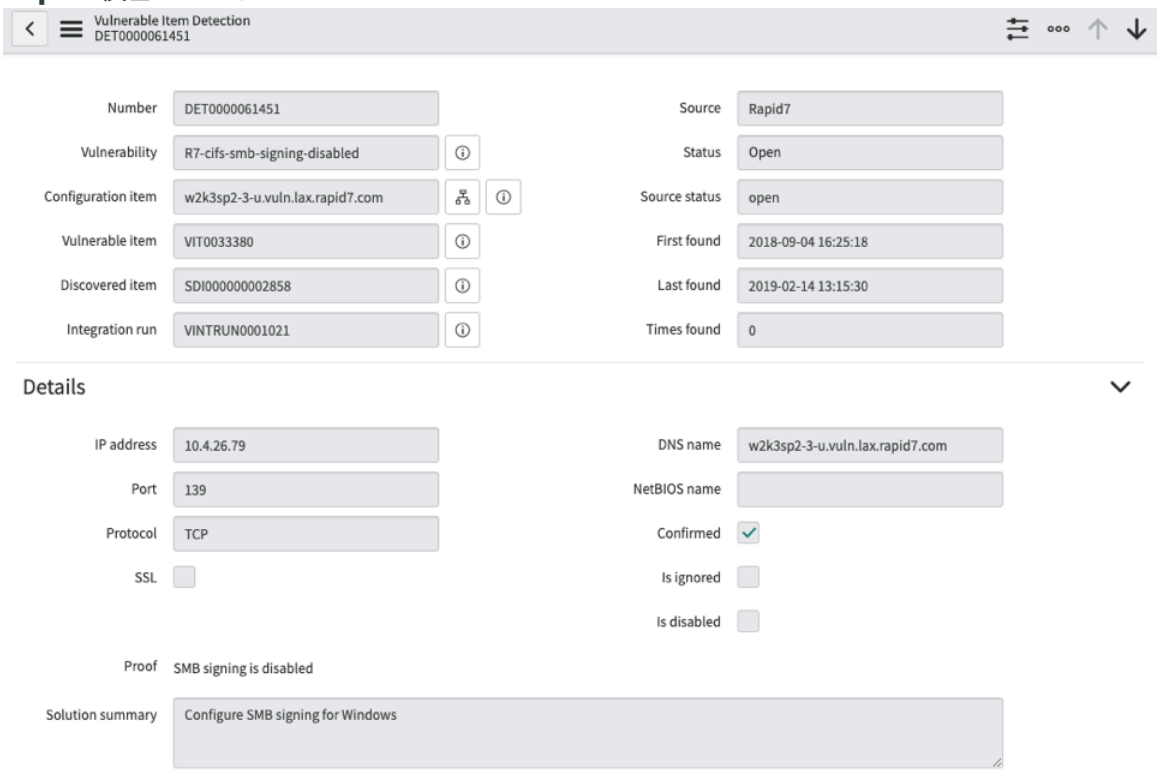
Qualys 検出レコード



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Rapid7 検出レコード

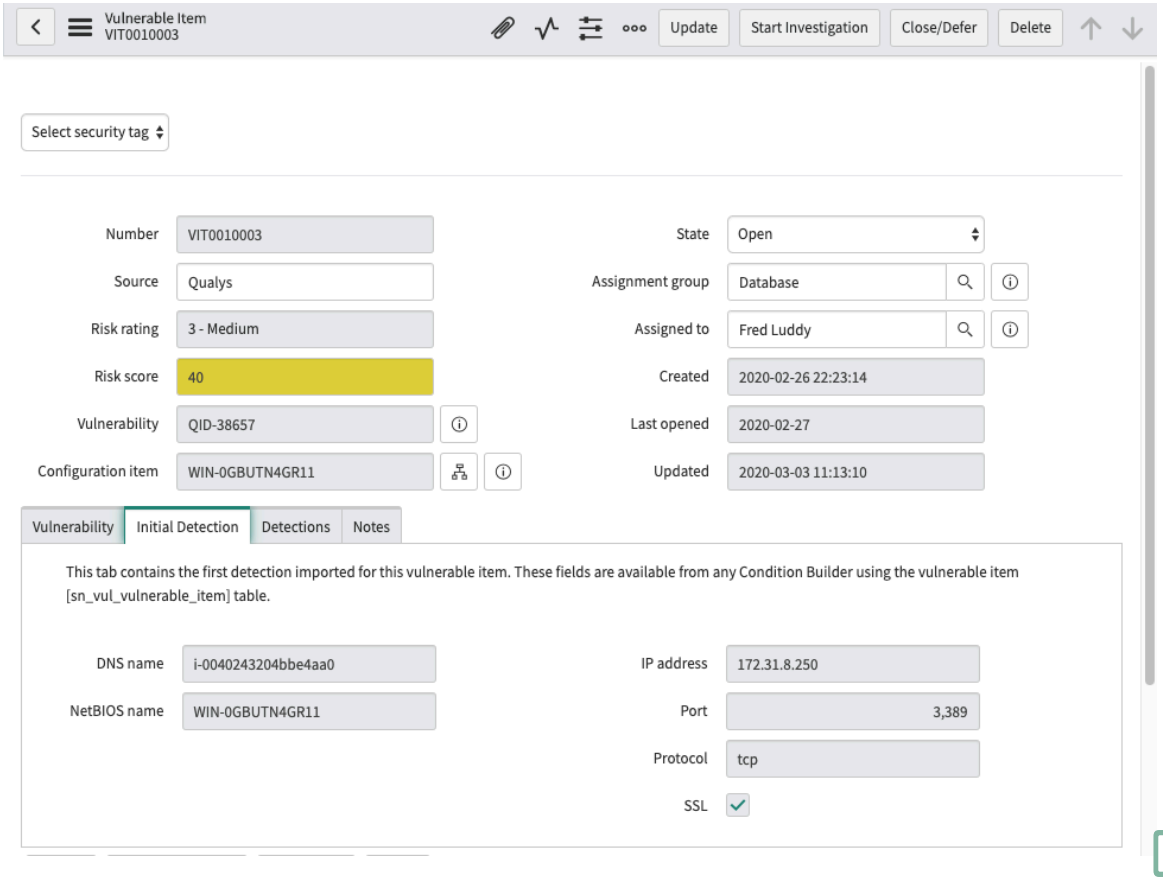


5. レコードに戻り、[初期検出] タブを選択します。

[初期検出] タブには、最初の検出でサードパーティのスキャナーからインポートされたデータが表示されます。[初期検出] タブのこの情報は、検出データが更新されても変更されません。

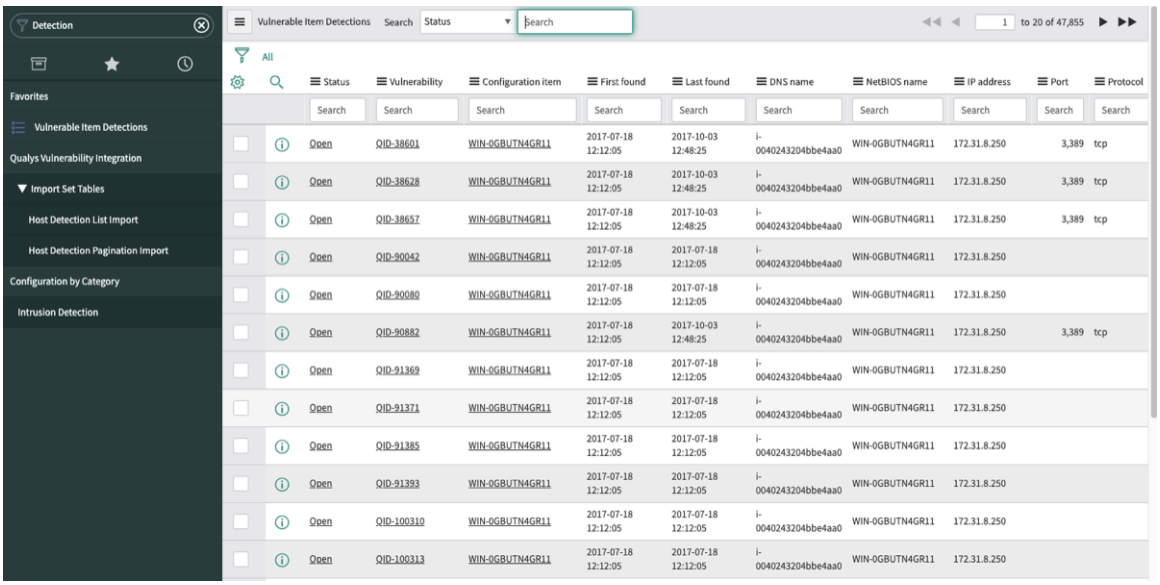
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



6. オプション: [脆弱性一致アイテムの検出] に移動して、脆弱性一致アイテムの検出リストを表示します。

   (Optional) [脆弱性一致アイテムの検出] リストが表示されます。[脆弱性一致アイテムの検出] リストの各行は、個別の検出を表します。列には VI レコードと同じデータが表示されます。



検出はスキャナーによって検出されたデータによってのみオープンまたはクローズされ、VI からロールダウンされることはありません。検出がインポートされると、それを使用して VI が作成され、VI の状況が更新されます。脆弱性一致アイテムのすべての検出がクローズされた場合、その脆弱性一致アイテムはクローズされます。VI レコードでは、ステータスが [クローズ済み]、サブステートが [修正済み] になります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
エラーは次のときにログに記録されます。

- スキャナーから取得された添付ファイルを処理しているとき。
- 検出または脆弱性一致アイテムを作成または更新しているとき。

検出エラーの処理については、「検出のエラー処理」を参照してください。

修復タスクに対してすべての VI がクローズされると、その修復タスクはクローズされます。

サブステートが [修正済み] または [古い] であるクローズ済みの VI は、新しい検出が作成され、VI が新しい脆弱性と一致する場合に再オープンされます。

インスタンスで [解決済み] に設定されていても後続の統合実行によって [クローズ済み]/[修正済み] に移行されていない脆弱性一致アイテムは、再スキャン中に検出された場合に再オープンされます。

修復タスクに対してすべての VI がクローズされると、そのレコードはクローズされます。

インスタンスで [解決済み] に設定されていても後続の統合実行によって [クローズ済み]/[修正済み] に移行されていない脆弱性一致アイテムは、再スキャン中に検出された場合に再オープンされます。

Rapid7 検出の場合、インスタンスの [Rapid7 構成] ページで、解決済みの VI を経過時間別に再オープンするオプションが利用可能になりました。有効にすると、[解決済み] に設定されていても、後続のスキャンで [クローズ済み]/[修正済み] に移行しなかった VI は、入力した日数後に [オープン] に戻ります。

Qualys 検出で、[解決済み] に設定されていても後続のスキャンで [クローズ済み]/[修正済み] に移行されていない VI をスキャナーが引き続き検索する場合、最終検出日が解決日より後であると、これらの VI が [オープン] に戻ります。

次のタスク
アイテム数や検出数などのデータをさらに表示するには、「統合実行 (VINTRUN) レコードの 脆弱性対応 脆弱性一致アイテム検出データの検証」を実行します。

統合実行 (VINTRUN®) レコードの 脆弱性対応 脆弱性一致アイテム検出データの検証

Now Platform インスタンスの統合実行レコードから、スキャンの日時に基づいてサードパーティ統合の脆弱性一致アイテム検出データを見つけることができます。スキャンが正常に完了したことを確認し、個々の検出数 (カウント) と、スキャンの結果として直接作成または更新された脆弱性一致アイテム (VI) を表示します。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vuln.admin (非推奨)
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

以下のリストから特定のレコードを見つけられるように、脆弱性一致アイテムレコードまたは検出レコードから、統合実行情報と、スキャンの日時または統合実行レコード番号 (VINTRUN#) のいずれかを入手することをお勧めします。

手順

1. 1 つ選択して続行します。

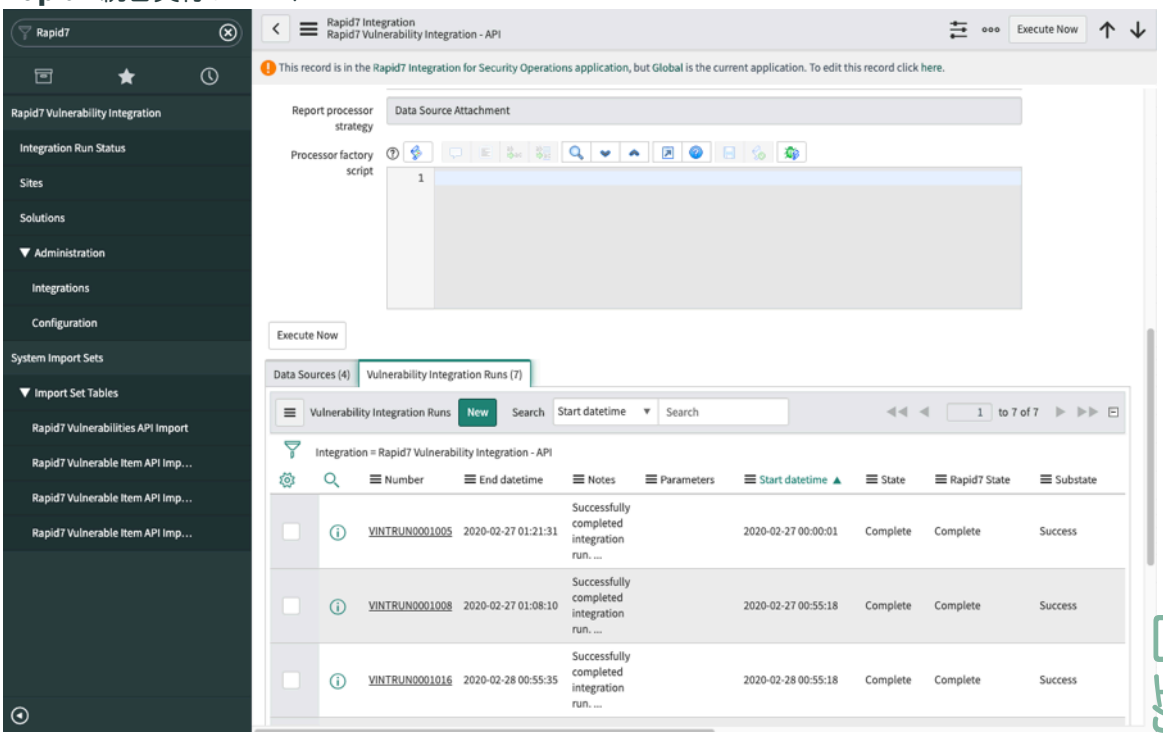
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

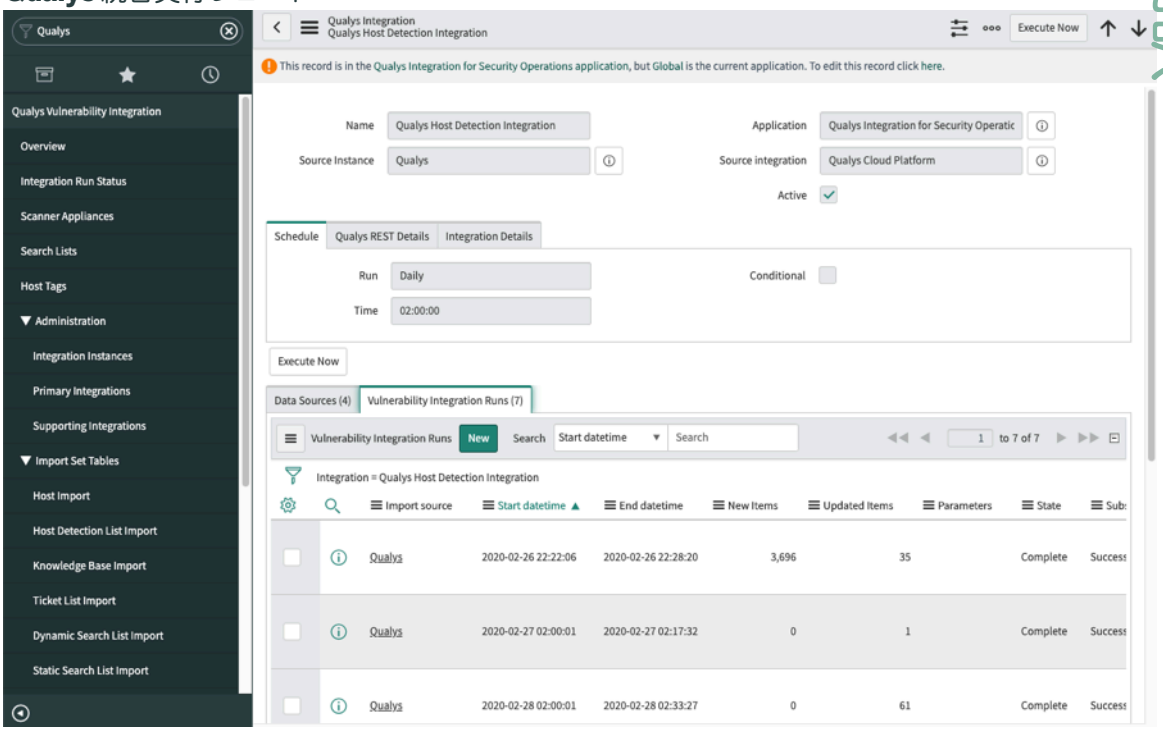
2. 表示されるページの下部で、[脆弱性統合実行] タブをクリックします。
3. [番号] 列または [インポートソース] 列のアイテムをクリックして、レコードを開きます。

   統合実行レコードが表示されます。

Rapid7 統合実行レコード



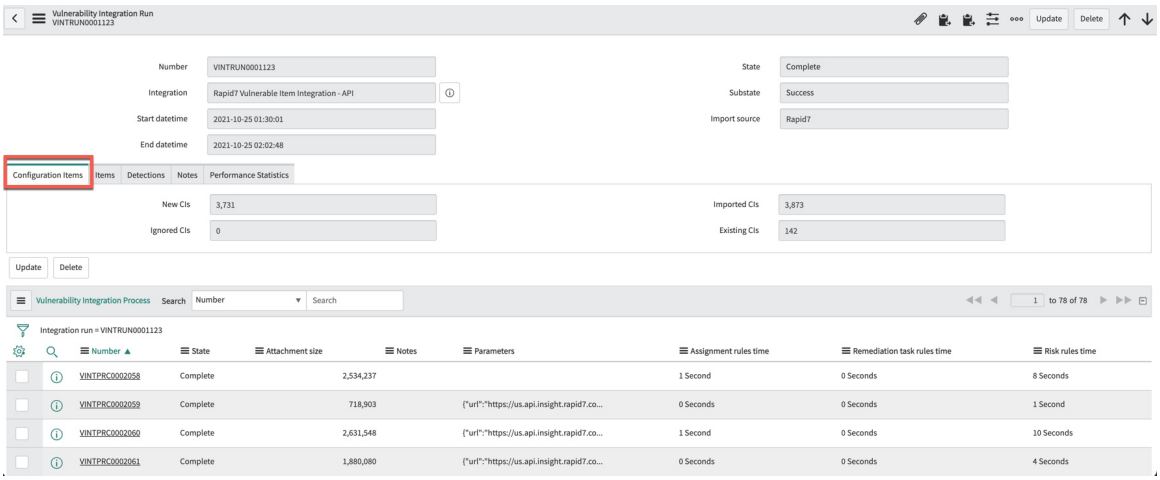
Qualys 統合実行レコード



統合実行レコードが表示されます。[ステータス] フィールドで、統合が正常に実行されたことを確認できます。[構成アイテム] タブを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

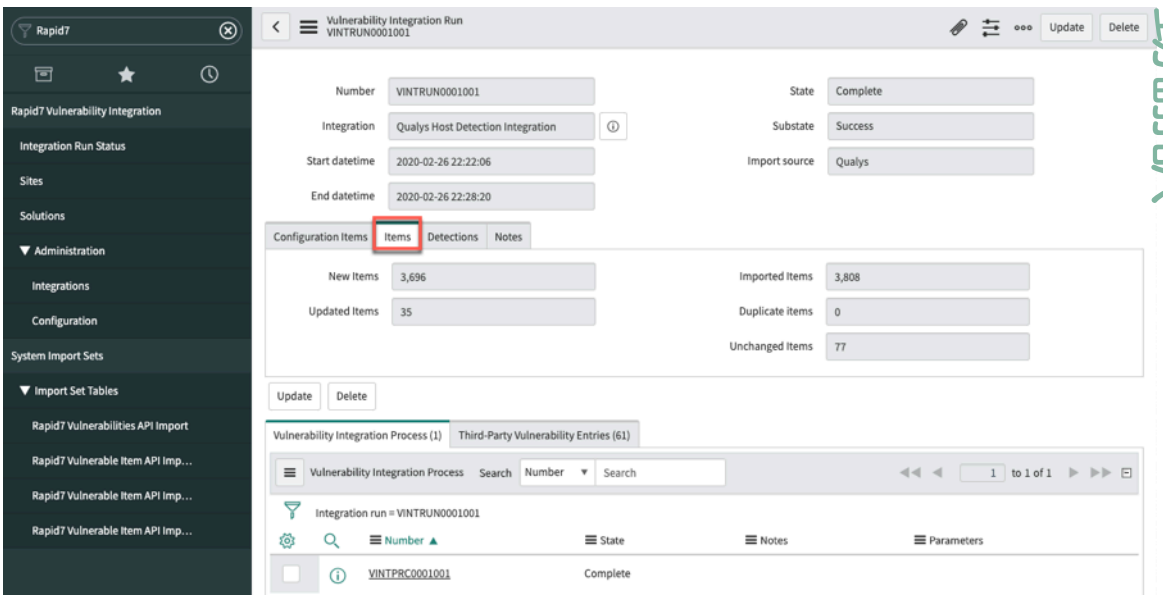
自動翻訳



[構成アイテム] タブには、以下の情報が表示されます。

- [構成アイテム] タブには、インポートされた構成アイテムの合計数が表示されます。
- [新規 CI (New CIs)] フィールドには、この統合実行の一環として作成された CI の数が表示されます。
- [インポートされた CI] フィールドには、このセクションのすべての CI の合計が表示されます。
- 脆弱性対応統合の場合、[無視された CI] フィールドの値は常に 0 です。
- [既存の CI] フィールドには、既に存在する CI の合計数が表示されます。

[アイテム] タブをクリックします。



[アイテム] タブには、以下の情報が表示されます。

- [アイテム] タブには、インポートされた VI の合計数が表示されます。[ディスカバリー] タブにリストされている数値の加算によって、インポートされた検出の合計を確認できます。
- [新規アイテム] フィールドには、この統合実行から作成される脆弱性一致アイテムの数が表示されます。
- [インポートされたアイテム] フィールドには、このセクションのすべてのフィールドの合計が表示されます。
- [重複アイテム] フィールドには入力されなくなりました。

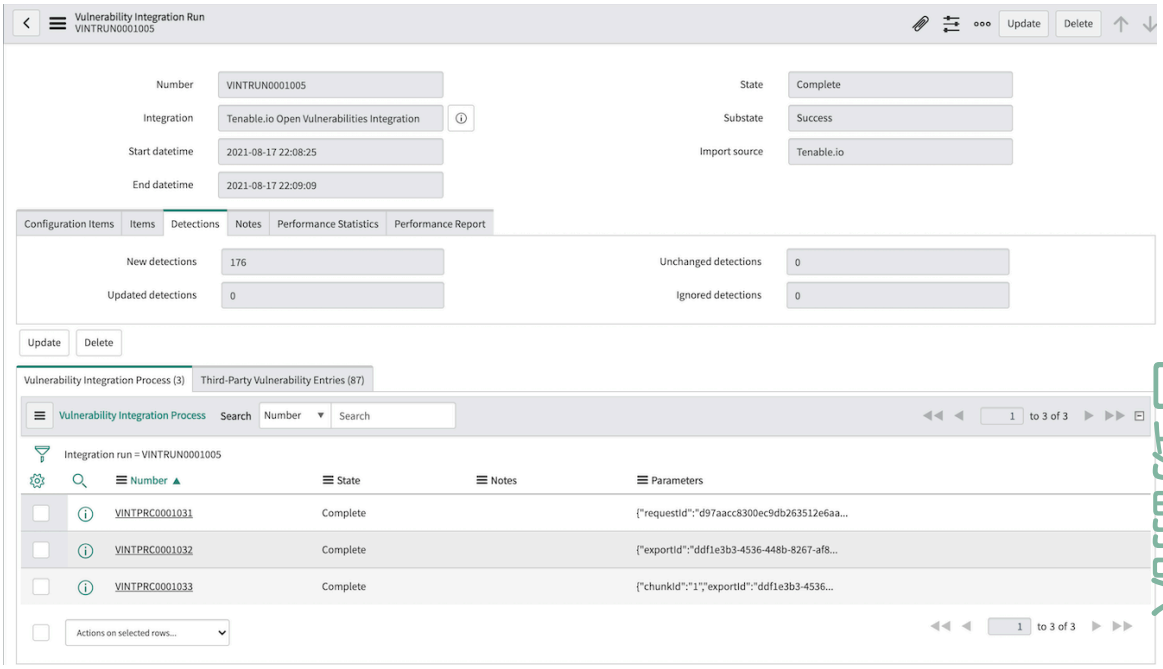
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [更新されたアイテム] フィールドには、この統合実行中の脆弱性一致アイテムの更新回数が表示されます。この値は、更新される一意の脆弱性一致アイテムの数ではありません。たとえば、統合実行中に脆弱性一致アイテムが 2 回更新された場合、2 回とカウントされ、更新済みアイテムが 2 つと表示されます。
- [未変更のアイテム] フィールドには、統合実行中に検出されたけれども、関連するフィールド値が変更されていないために更新されなかった、データベースに存在する脆弱性一致アイテムが表示されます。

4. [ディスカバリー] タブをクリックします。

このタブは、統合実行で何らかの検出がある場合にのみ表示されます。リストされている数値の加算によって、インポートされた検出の合計を確認できます。

VR v15.0 の [ディスカバリー] タブ



注:
v15.0 より前では、無視される検出のフィールドはありませんでした。

[ディスカバリー] タブには、以下の情報が表示されます。

- v15 以降では、以前に無視された検出を追跡するために、[無視された検出] フィールドが追加されています。この実装により、インポートされた検出数と統合実行レコードで追跡される数が一致するようになりました。この機能は、すべてのスキャナー (Qualys 脆弱性統合、Rapid7 脆弱性統合、Tenable 脆弱性統合、および Microsoft TVM) に実装されています。
- [新しい検出] フィールドには、この統合実行中に作成された新しい検出が表示されます。
- [未変更の検出] フィールドには、統合実行中に検出されたけれども、関連するフィールド値が変更されていないために更新されなかった、データベースに存在する検出が表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [更新された検出] フィールドには、この統合実行中の検出の更新回数が表示されます。この値は、更新される一意の検出の数ではありません。たとえば、統合実行の一環として検出が 2 回更新された場合、2 回とカウントされ、更新済み検出が 2 と表示されます。

  注:
  こうした数に表示されない検出は、クローズ済みステータス (修正済み) の検出です。修正済みレコードを使用して既存の VI を更新するため、そのようになります。このような検出レコードの可視化を高めたい場合は、一致する既存のオープンステータスの VI がないときに作成されたクローズ済み VI を表示できます。Qualys 統合のセットアップアシスタントで有効にできる修正済みステータスの脆弱性の詳細については、「セットアップアシスタントを使用した 脆弱性対応 の構成」を参照してください。

5. [番号] 列または [インポートソース] 列のアイテムをクリックして、レコードを開きます。

脆弱性対応 でのパッチデータの表示とパッチ適用のスケジューリング

脆弱性対応 の v16.1 以降では、クラシック環境と Now Platform インスタンスの 脆弱性対応 ワークスペースの両方で、パッチをスケジュールし、パッチデータとソリューションおよびレコードのその他の脆弱性情報を表示できます。

必要なロール

ユーザーがデータを表示しパッチをスケジュールするには、パッチのインポートに使用しているパッチオーケストレーション統合に固有のロールが必要です。詳細については、サポートされている統合を参照してください。

- 「脆弱性対応 との HCL BigFix パッチオーケストレーション統合の概要」および「脆弱性対応 Patch Orchestration Integration with Microsoft SCCM の概要」。
- クラシック環境における 脆弱性対応 ダッシュボードでのパッチオーケストレーションデータの表示。
- 脆弱性対応 ワークスペース でスコアカード上のデータを表示します。

パッチのスケジューリング

次のレコードからパッチをスケジュールできます。

- パッチ更新 (VPU)
- 修復タスク (RT)
- 検出されたアイテム (SDI)

クラシック環境内のパッチデータ

脆弱性対応 アプリケーションのクラシック環境から：

- パッチ更新レコードを表示するには、次に移動します: **All** (すべて) > 脆弱性対応 > パッチ.
- ソリューションを表示するには、次に移動します: **All** (すべて) > 脆弱性対応 > ソリューション.
- 自分にアサインされていてパッチがある VI を表示するには、次に移動します: **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム > パッチで自分にアサイン済み.
- 修復タスクを表示するには、次に移動します: **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム > パッチで自分にアサイン済み
- 検出されたアイテムレコードを表示するには、次に移動します: **All** (すべて) > セキュリティオペレーション > 検出済みアイテム.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性対応 のパッチオーケストレーションでのパッチデータとステータスのロールアップ

脆弱性対応 の v16.1 以降、パッチデータと状況は 脆弱性対応 アプリケーションのパッチ更新レコードおよびその他のレコードにロールアップされます。

脆弱性対応 のクラシック環境のワークスペースにあるパッチ更新レコード

パッチ、脆弱性ソリューション、および脆弱性に関する情報はすべて 脆弱性対応 アプリケーション内で関連付けられています。

パッチデータとパッチロールアップデータおよびステータスは、インスタンス内のレコードに表示されます。パッチレコードは、脆弱性対応 との統合のパッチオーケストレーション機能の一部として含まれています。IT 修復ワークスペースのリストビューから、脆弱性対応ワークスペースのパッチ (VPU) レコードを表示します。クラシックビューと脆弱性対応ワークスペースの両方のパッチ更新レコードには、以下のデータが含まれています。

- Vulnerability Solution Management アプリケーションによってインポートされたパッチベンダーからの脆弱性ソリューションデータと情報。
- ソース修復ステータス。これには、パッチによって修正できる脆弱性があるデバイスと、更新が欠落しているデバイスの合計数が含まれます。
- 修復された VI の割合と、優先パッチがある合計 VI を含む修復ステータス。
- クラスビューのレコードの関連リンクにある関連デバイス、脆弱性一致アイテム、パッチ展開、およびパッチ要求。このデータは、脆弱性対応ワークスペースのレコードのタブに表示されます。
- 修復オーナーが承認のために送信したパッチ要求。

必要なロール

ユーザーには、データの表示やパッチのスケジューリングに使用している、パッチオーケストレーション統合に固有のロールが必要です。詳細については、サポートされている統合を参照してください。

- 「脆弱性対応 との HCL BigFix パッチオーケストレーション統合の概要」および「脆弱性対応 Patch Orchestration Integration with Microsoft SCCM の概要」。
- クラシック環境における 脆弱性対応 ダッシュボードでのパッチオーケストレーションデータの表示。
- 脆弱性対応 ワークスペース でスコアカード上のデータを表示します。

パッチデータとステータスのロールアップ

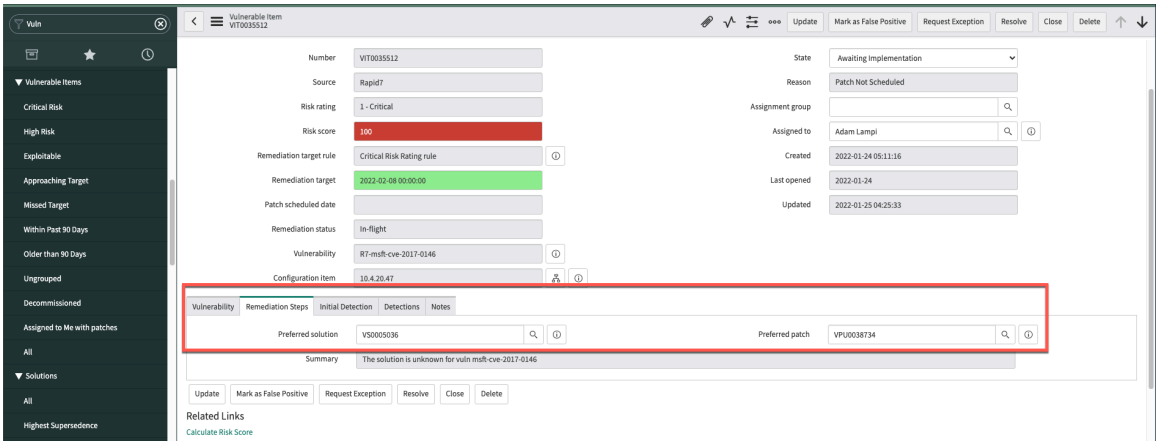
クラシック環境でパッチが適用され、自分にアサインされている脆弱性一致アイテムを表示するには、 **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム > パッチで自分にアサイン済み.

脆弱性一致アイテムレコードに優先パッチが入力されている場合、VI のステータスが [クローズ済み]、[解決済み]、[保留]、[レビュー中] でない場合にのみ、自動的に [実装待ち] に移行します。データをドリルダウンして優先ソリューションやその他のデータを表示するには、VI レコードの [修復] タブをクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[修復手順] タブ



優先パッチを含む VI は、以下の場合に [実装待ち] に移行します。

- コレクションインポートに含まれている CI へのパッチの展開がスケジュールされており、CI に VI が関連付けられている場合、その VI が [実装待ち] になる理由は [スケジュール済みのパッチ] となっているためです。
- コレクションインポートに含まれている CI へのパッチの展開がスケジュールされており、CI に VI が関連付けられている状態で、修復ターゲット日 (期限) が修復までの時間 (TTR) の日付より後である場合、その VI のステータスは [実装待ち] になります。その理由は、[スケジュール済みのパッチ (ターゲット日なし)] となっているためです。
- コレクションインポートに含まれている CI へのパッチの展開がスケジュールされていない場合、その VI のステータスは [実装待ち] になります。その理由は、[スケジュールされていないパッチ] となっているためです。

[優先パッチ] 情報アイコンをクリックしてパッチ更新を開き、関連リンクで以下の情報を表示します。

脆弱性一致アイテム
: このパッチに関連付けられている脆弱性一致アイテム。

関連デバイス
: 更新があるデバイスと更新がないデバイス。

パッチ展開
: 個々のマシン (資産) または資産のグループでこのパッチに対してスケジュールされている展開。

パッチ要求
: 展開がスケジュールされる前に承認のために送信されたパッチ要求のリスト。

潜在的なパッチ
: 脆弱性に対処する可能性のあるパッチ。

[優先パッチ情報] アイコンをクリックしてレコードを開き、以前にリストされた情報と以下のパッチ更新データを表示します。

ソース修復ステータス
: このパッチを必要とするデバイスと、パッチが適用されていないデバイスの合計。

修復ステータス
: この優先パッチを持つ VI のステータス (合計 VI、修正済みの割合、保留された VI)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

優先パッチとソリューション

インポートされた脆弱性が 構成管理データベース (CMDB) の資産と一致する場合、脆弱性一致アイテム (VI) が 脆弱性対応 に作成されます。この VI に関連付けられている構成アイテム (CI) がサードパーティのパッチベンダーからもインポートされ、同じ脆弱性に対するパッチがないと表示される場合は、優先パッチがリストされ、ソリューションにロールアップされます。この情報により、ある資産 (CI) に利用可能なパッチからの修正があり、それが脆弱性への対処に最適であることがわかります。

ソリューションのないパッチの表示

インポート後に、利用可能な脆弱性ソリューションデータがない場合、パッチ更新レコードの [脆弱性ソリューション] フィールドは空白のままになります。こうしたタイプのパッチに関する情報の表示方法の詳細については、「脆弱性対応 でのソリューションのないパッチの表示」を参照してください。

脆弱性対応 でのソリューションのないパッチの表示

脆弱性対応 の v16.0 以降では、インポート後にソリューションがないパッチについて、脆弱性レコードでこうしたパッチを表示できるように、脆弱性参照データ内のパッチ ID が検索されます。

ソリューションのないパッチ

必要なロール：sn_vul.vulnerability_admin。

パッチオーケストレーションと脆弱性ソリューションアプリケーション、およびパッチスキャナー統合からインポートされた、パッチ更新レコードのデータは、脆弱性対応 アプリケーションで処理され、関連付けられ、表示されます。

脆弱性のソリューションが存在する場合は、関連情報がインスタンスに関連付けられ、パッチから脆弱性ソリューション、および脆弱性にロールアップされます。この情報を表示するには、次に移動します: **All** (すべて) > 脆弱性対応 > パッチ > **All** (すべて).

インポート後に、利用可能な脆弱性ソリューションデータがない場合、パッチ更新レコードの [脆弱性ソリューション] フィールドは空白のままになります。こうしたパッチに関連するソリューション情報を表示できるように、システムプロパティ [**sn_vul_patch_orch.no_solution_patch_rollup**] がインスタンスにおいてデフォルトでアクティブ化されています。このプロパティは、スキャナーインポートから脆弱性参照データ内のセキュリティ情報 ID と記事 ID を検索します。一致が見つかると、関連データが潜在的なパッチテーブルに入力され、この情報が脆弱性レコードの関連リストに表示されます。

多数の脆弱性がある場合、またはロールアップスケジュール済みジョブの完了に時間がかかる場合は、考えられるパフォーマンスの問題を回避するために、このシステムプロパティを非アクティブ化することをお勧めします。ただし、このシステムプロパティを非アクティブ化すると、インポートされたソリューションデータは検索されず、ソリューションなしの脆弱性にロールアップされることもありません。

sn_vul.vulnerability_admin ロールを持つユーザーとして、 システムプロパティを非アクティブ化するには、次の手順を実行します。

1. 次のように移動する。 **sys.properties.list**.
2. **sn_vul_patch_orch.no_solution_patch_rollup** を見つけてクリックし、レコードを開きます。
3. [値] フィールドに「false」と入力します。
4. [更新] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 ダッシュボードでのパッチオーケストレーションデータの表示

v16.1 以降、脆弱性対応 アプリケーションに付属するダッシュボードのクラシック環境でパッチ更新データを表示できます。

脆弱性対応 ワークスペースには、修復の進捗状況を監視するのに役立つデータの可視化が含まれています。脆弱性データの変更に応じて更新される動的なデータ表示で組織にとって重要なアクティブな脆弱性の数と重大度を表示することで、組織に対する脅威のレベルを判断できます。詳細については、「Vulnerability Manager ワークスペース」と「IT 修復ワークスペース の探索」を参照してください。

パフォーマンスアナリティクス のサブスクリプションがある場合は、CISO ダッシュボードや Vulnerability Management (PA) ダッシュボードでもこのデータを表示できます。

クラシック環境でパッチデータを表示することもできます。脆弱性対応 アプリケーションに付属するクラシック環境の 脆弱性対応 ダッシュボードおよび個別のサブスクリプションが必要なダッシュボードで必要なロールと、データを表示する方法の詳細については、「デフォルトの 脆弱性対応 ダッシュボードを使用する」を参照してください。

ソリューションの表示

すべてのソリューション、最高優先度のソリューション、および脆弱性一致アイテムに関連するソリューションを表示して、修復アクティビティを通知します。

始める前に

必要なロール：sn_vul.read、sn_vul.vulnerability_admin、または sn_vul.remediation_owner
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

このタスクについて

脆弱性アナリストまたは修復オーナーは、脆弱性一致アイテムに関連するさまざまなソリューションセットを表示できます。

> **注:**
> ソリューションレコードは、[内部メモ] セクションの [メモ] やユーザーが作成したソリューションを除き、読み取り専用です。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > ソリューション.
2. ソリューションリストを選択します。

   > **注:**
   > 製品名にワイルドカードを使用して、ソリューションリストをフィルタリングできます。

3. 確認するには、各アイテムをクリックします。
4. オプション: [メモ] タブでメモを入力し、[保存] を右クリックしてそのページに留まるか、[更新] をクリックして保存して [脆弱性ソリューション] リストに戻ります。

   > **注:**
   > sn_vul.read ロールしかない場合は、この手順を実行できません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性ソリューションの作成

脆弱性ソリューションを作成して、サードパーティソリューションのコンテンツでカバーされていない脆弱性ソリューションを追跡できるようにします。

始める前に
必要なロール：admin、sn_vul.vulnerability_admin または sn_vul.admin (非推奨)、または vulnerability.write
脆弱性ソリューション管理 は 脆弱性対応 アプリケーション内で利用できる機能です。脆弱性ソリューション管理 には別のサブスクリプションが必要です。

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

このタスクについて
いずれかのソリューションリストからソリューションを作成できます。ソリューションを作成する前に、Vulnerability Solution Management アプリケーションをインストールする必要があります。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > ソリューション.
2. ソリューションリスト ([すべて]、[最高優先度]、または [脆弱性一致アイテムを使用 **(With Vulnerable Items)**]) を選択します。
3. [新規] をクリックします。
4. 必要に応じて、フォームの編集可能フィールドに入力します。
   未使用のフィールドは空白のままにしておくことができます。個々のフィールドの詳細については、「ソリューションフォームのフィールド」を参照してください。
5. ヘッダーで [保存] を右クリックします。
   ソリューションレコードが追加され、デフォルトで [すべて] および [最大の置き換え] リストに表示されます。
6. 関連リストが表示されます。

   このソリューションを [脆弱性一致アイテム]、[サードパーティ脆弱性]、 **[CVE]**、[優先ソリューション]、[先行するソリューション] の各関連リストに関連付けることができます。脆弱性またはソリューションを選択し、[送信] をクリックします。

   注:

   脆弱性レコードがソリューションに手動で関連付けられている場合、脆弱性ソリューション管理 は脆弱性一致アイテムと修復タスクをソリューションに自動的に関連付けます。

   別のソリューションに手動で再アサインされた脆弱性一致アイテムは、脆弱性レベルでのソリューションの変更によって自動的に更新されることはありません。

   修正している CI に関連していないか、お使いの環境では問題ないために、サードパーティ脆弱性とソリューション間の関係を除外する場合は、「サードパーティのレコードからのソリューションの手動での除外 (またはその逆)」を参照してください。

サードパーティのレコードからのソリューションの手動での除外 (またはその逆)

修正している CI に関連していないか、お使いの環境では問題ないために、サードパーティ脆弱性とソリューション間の関係を除外します。サードパーティの脆弱性またはソリューションレコードを使用して、ソリューションを手動で除外します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

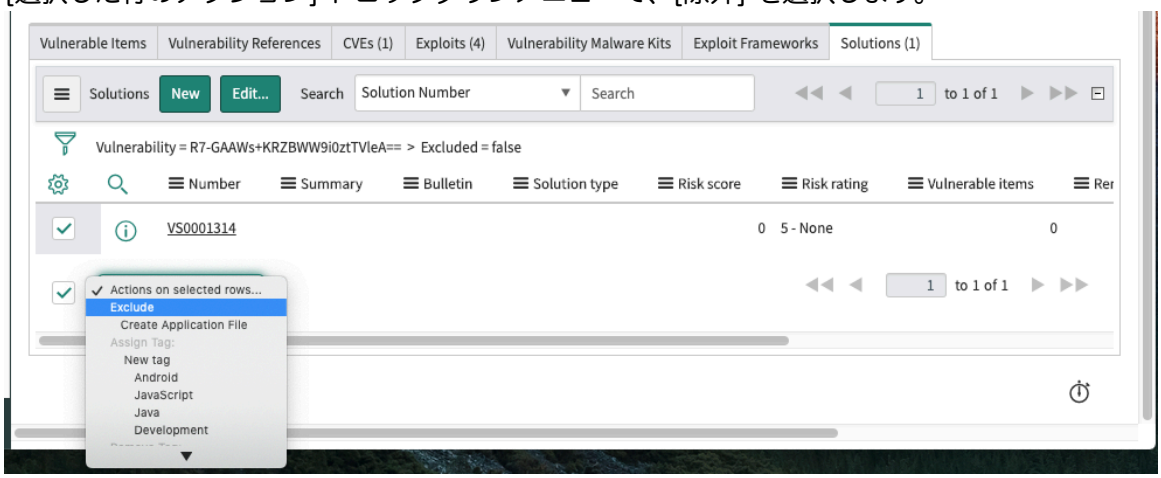
始める前に
必要なロール：

- sn_vul.write
- sn_vul.remediation_owner

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > ライブラリー > サードパーティ または 脆弱性対応 > すべてのソリューション
2. サードパーティの脆弱性またはソリューションレコードを開きます。
   a. サードパーティレコードの場合：[ソリューション] 関連タブを選択します。
   b. ソリューションレコードの場合：[サードパーティ脆弱性] 関連タブを選択します。
3. 除外する各脆弱性またはソリューションレコードの横にあるチェックボックスをオンにします。
4. [選択した行のアクション] ドロップダウンメニューで、[除外] を選択します。



サードパーティまたはソリューションレコードが関連タブに表示されなくなります。

ソリューションに対するサードパーティ脆弱性の関係も、ソリューションが更新された場合、または夜間ジョブが有効になっている場合は除外されます。

ソリューションに対するサードパーティ脆弱性の関係は、夜間スケジュール済みジョブで除外されます。

サードパーティ脆弱性を除外すると、そのソリューションは優先ソリューション評価の要素ではなくなります。除外の影響：

- サードパーティ脆弱性、脆弱性一致アイテム (VI)、およびサードパーティ脆弱性に添付された構成アイテム (CI) はソリューションに影響しないため、すべてがソリューションにとって重要です。
- サードパーティ脆弱性に対する優先ソリューション、さらには添付された VI および VI を含む修復タスクの優先ソリューションの決定に影響します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性を自動的にトリアージ

修復を確実に成功させるには、新しい脆弱性のレビューとトリアージが必要です。自動化された脆弱性一致アイテム (VI) のアサイン、リスク計算、修復ターゲット、および VI のグループ化を使用して、脆弱性のインポートを修復タスクに変換します。

インポートされた脆弱性から始めて、CMDB にない資産を調整し、結果を優先順位付けして、自動的にアサインされる修復アクティビティに変換し、修復プロセスをオーケストレーションし、検証スキャンで完了を確認します。

通常、新しい脆弱性一致アイテムは、修復タスクルールに基づいてインポート時に修復タスクに分類されます。脆弱性一致アイテムをグループ化できない場合や、認識される構成アイテムが含まれていない場合があります。

脆弱性トリアージプロセスの概要：

- 脆弱性対応 インスタンスにログインします。
- 脆弱性一致アイテムのルール (CI ルックアップ、アサイン) が想定どおりに機能していることを検証します。CI ルックアップルールの変更については、「脆弱性対応 サードパーティ脆弱性統合の構成アイテムを識別するための CI ルックアップルール」を参照してください。アサインルールについては、「脆弱性対応 アサインルールの概要」を参照してください。

  注:
  大量のデータをインポートするため、脆弱性一致アイテムの自動アサインには注意が必要です。

- 修復ターゲットが正しいことを検証します。修復ターゲットルールの仕組みと変更方法については、「脆弱性対応 の修復ターゲットルール」を参照してください。
- グループ解除済み脆弱性一致アイテムの表示
  - グループ解除済み脆弱性一致アイテムを確認し、グループルールを変更して再スキャンすることを検討してください。詳細については、「脆弱性対応 修復タスクルールの作成または編集」を参照してください。
  - 脆弱性一致アイテムを手動でグループ化します。詳細については、「脆弱性対応 での修復タスクの手動作成」を参照してください。
  - 修復タスクの脆弱性一致アイテムのリスクスコアを変更します。詳細については、「脆弱性対応 の算出と脆弱性算出ルール」を参照してください。
  - サードパーティ統合によって最近検出されていない古い脆弱性一致アイテムをクローズします。詳細については、「脆弱性一致アイテムと検出の自動クローズ」を参照してください。
- 一致しない構成アイテムの表示と再分類。
- 修復のために行う必要があることを調査します。

  このステップでは、以下を行います。

  - すぐに処理すべきことと保留できることを決定します。この決定は、多くの場合、リスクスコア、影響を受けるシステム、および変更時間帯が指定されているパッチに基づきます。

    注:
    修復ターゲットルールは脆弱性一致アイテムに属しています。こうしたルールは、脆弱性一致アイテムのインポート時に実行されます。この各ルールは、以前にセットアップアシスタントで作成されたものです。

  - 必要に応じて、脆弱性一致アイテムをリフレッシュし、脆弱性対応 脆弱性一致アイテムの修復ターゲットステータスの表示を行います。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 変更要求を作成し、修復のために修復タスクをアサイン先グループ (IT 運用) にアサインします。

  注:
  脆弱性がセキュリティインシデントを構成しており、セキュリティインシデントレスポンス プラグイン (com.snc.security_incident) がアクティブ化されている場合は、代わりに修復タスクからセキュリティインシデントレコードを作成できます。

- 1 つ以上の変更要求を送信した後、グループステータスを [調査中] に移行します。

脆弱性対応 での脆弱性一致アイテムの一括編集

フィールドを選択し、バックグラウンドで非同期一括編集ジョブを実行することにより、脆弱性一致アイテムを一括で編集して時間を節約します。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

このタスクについて
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

重要:
Vulnerability Manager ワークスペース内のホスト脆弱性一致アイテムで利用可能な一括編集機能。詳細については、「Vulnerability Manager ワークスペース での一括編集の使用」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性 > 脆弱性 > 脆弱性一致アイテム.
2. 次のいずれかのアクションを実行して、脆弱性一致アイテムを選択します。
   - #unique_131_Connect_42_entry-be-record-selection フィールドで [選択されているアイテムのみ **(Only Selected Items)**] オプションを使用する場合は、各アイテムの横にあるチェックボックスをオンにします。
   - #unique_131_Connect_42_entry-be-record-selection フィールドの [フィルターと一致するすべての脆弱性一致アイテム **(All vulnerable items that match filter)**] オプションを使用する場合は、フィルターを適用します。
3. [一括編集] ボタンを選択します。
4. [一括編集] モーダルで、フィールドに入力します。

フィールド	説明
レコード選択	更新するレコード。選択肢は次のとおりです。 ○ 選択された脆弱性一致アイテムのみ ○ フィルターと一致するすべての脆弱性一致アイテム ○ 修復タスク ○ 脆弱性エントリー
状態	脆弱性一致アイテムのステータスの変化。選択肢は次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ 更新しない ○ オープン ○ 調査中 ○ 実装待ち ○ 保留 注: ▪ このオプションを選択すると、[理由 (Reason)]、[簡単な説明 (Short description)]、[期限 (Until)]、および [補足情報 (Additional information)] フィールドが表示されます。 ▪ VIT を保留すると、修復タスクが作成され、このタスクが承認のために送信されます。 ○ クローズ済み 注: ▪ このオプションを選択してレコードを誤検出としてマークすると、[理由]、[簡単な説明]、[まで]、および [補足情報] フィールドが表示されます。 ▪ レコードを誤検出としてマークすると、修復タスクが作成され、このタスクが承認のために送信されます。 ○ 解決済み
優先ソリューション	一括編集用に選択したすべての脆弱性一致アイテムの修正を対象としたソリューション。脆弱性一致アイテム (VIT) の [優先ソリューション] フィールドに対する変更を選択します。選択した VIT で利用可能な優先ソリューションのルックアップリストからの選択肢があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: ○ 利用可能な優先ソリューションのセットは、選択したすべての VIT と、脆弱性のすべての見込みのある解決策との共通部分です。 ○ 選択時 レコード選択 > 脆弱性エントリー 一括編集の場合、脆弱性のすべての VIT が選択された優先ソリューションに設定されます 注: この操作では脆弱性エントリーレベルで優先ソリューションが設定されません。脆弱性エントリレベルで優先ソリューションを設定すると、以降すべての新しい VIT に対して優先ソリューションが設定されます。一括編集では、現在の VIT セットのみが変更されます。 ○ 選択基準全体での個別の脆弱性は 500 に制限されています。500 を超える個別の脆弱性がある場合は、[優先ソリューション] の設定基準が異なる VIT を選択するように求める警告メッセージが表示されます。 ○ ルックアップリストに表示できるソリューションの合計数は 170 に制限されています。170 を超えるソリューションがある場合は、警告メッセージが表示されます。 更新された値は、脆弱性一致アイテムリストビューに表示されます。
優先パッチ	一括編集用に選択したすべての脆弱性一致アイテムの修正を対象としたパッチ。 注: ○ 優先パッチのリストを表示するには、パッチオーケストレーションをインストールする必要があります。 ○ 利用可能な優先パッチのセットは、選択したすべての VIT と、すべての見込みのあるパッチとの共通部分です。 ○ 選択基準全体での個別の脆弱性は 500 に制限されています。500 を超える個別の脆弱性がある場合は、[優先パッチ] の設定基準が異なる VIT を選択するように求める警告メッセージが表示されます。 ○ ルックアップリストに表示できるパッチの合計数は 170 に制限されています。170 を超えるパッチがある場合は、警告メッセージが表示されます。
理由	レコードを保留する理由： ○ メンテナンス期間待ち ○ 修正が利用不可 ○ リスクの受容 ○ コントロールの緩和を実施 ○ その他

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	レコードをクローズする理由： ○ 誤検出 **注:** ▪ このオプションを選択すると、[簡単な説明]、[まで]、および [補足情報] フィールドが表示されます。 ▪ レコードを誤検出としてマークすると、修復タスクが作成され、このタスクが承認のために送信されます。 ○ キャンセル ○ 固定 **注:** このフィールドは、[ステータス] で [保留] または [クローズ済み] を選択すると表示されます。
簡単な説明	保留およびクローズ済み誤検出要求の理由を説明する簡単なメモ。この情報は、保留要求およびクローズ済み誤検出要求に対して作成された修復タスクの [説明] フィールドに反映されます。 **注:** このフィールドは、[ステータス] で [保留] および [クローズ済み - 誤検出 (Closed-False positive)] を選択すると表示されます。
期限	レコードの保留状態が終了する日付。 **注:** このフィールドは、[ステータス] で [保留] を選択すると表示されます。
追加情報	その他の必要な情報。この情報は、[概要] タブの [補足情報] フィールドに反映されます。保留要求が承認されると、この補足情報が VIT と修復タスクの両方の保留メモとして表示されます。 **注:** このフィールドは、[ステータス] で [保留] および [クローズ済み - 誤検出 (Closed-False positive)] を選択すると表示されます。
アサイン解除	アサイン先グループおよび修復オーナーに対して選択したすべてのアイテムのアサインが解除されます。修正オーナーが脆弱性一致アイテムからアサインを解除する方法の詳細については、「自分または自分のグループの脆弱性一致アイテムのアサイン解除」を参照してください。 **注:** ○ このフィールドは、[ステータス] で [更新しない] を選択すると表示されます。 ○ レコードをアサイン解除すると、修復タスクが作成され、このタスクが承認のために送信されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
アサイン先グループ	VIT のアサイン先グループ。手動で選択するか、有効になっている場合は [アサインの推奨] を使用します。 注: [アサイン解除] チェックボックスをオンにすると、このフィールドは無効になります。
作業メモ	変更を説明するために入力するテキスト。

5. **[OK]** を選択します。
   一括編集の非同期ジョブにより、選択したレコードが更新されます。ジョブ番号とリンクが [脆弱性一致アイテム] ページに表示され、そのステータスを確認できます。脆弱性一致アイテムを一括で保留、アサイン解除、またはクローズ (誤検出) すると、選択した脆弱性一致アイテムで修復タスクが作成されます。そして、この修復タスクが承認のために送信されます。

グループ解除済み 脆弱性対応 脆弱性一致アイテム

脆弱性一致アイテムは、インポート時に自動的に修復タスクにアサインされます。ただし、脆弱性一致アイテム (VI) を手動で作成すると、VI が孤立するなどの現象が起こることがあります。グループ解除済み脆弱性一致アイテムモジュールでは、グループのない脆弱性一致アイテムがリストされます。

注:
統合自動化プロセスでは孤立が発生しないため、このユースケースは小規模であることが想定されます。

グループ解除済みとなるのは、脆弱性一致アイテムが脆弱性なしで作成された場合、または VI をグループにアサインする修復タスクルールがない場合です。

その場合は、次に移動して、グループ解除済みの脆弱性一致アイテムのリストを確認します **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム > 修復タスク未割り当て.

レビュー後の選択肢は次のとおりです。

- 脆弱性対応 修復タスクルールの作成または編集 を行い、このリストに表示されるアイテムを取得できます。
- 脆弱性対応 での修復タスクの手動作成 を行い、このリストからアイテムを手動でグループに追加したり、こうしたアイテムに一致する条件を定義したりすることができます。
- ステータスが「オープン」または「調査中」であれば、既存の修復タスクを開き、関連する脆弱性一致アイテムをグループに追加できます。

注:
手動で追加された脆弱性一致アイテムは、修復タスクルールまたはグループ条件によって自動的に修復タスクから削除されることはありません。

修復タスクとタスクルールの動作の詳細については、「脆弱性対応修復タスクとタスクルールの概要」を参照してください。

グループ解除済みの 脆弱性対応 脆弱性一致アイテムの表示

グループにアサインされていない脆弱性一致アイテムは、表示可能なリスト内に配置されます。

始める前に

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性 > 脆弱性 > 修復タスク未割り当ての脆弱なアイテム.
2. リスト内の脆弱性一致アイテムを確認します。
3. 各脆弱性一致アイテムをクリックして表示し、グループに含める方法を決定します。

脆弱性一致アイテムを修復タスクに手動で追加する

脆弱性一致アイテムがグループ化されていない場合は、修復タスクに追加できます。

始める前に

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

手順

1. 脆弱性番号を記録します。
2. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 修復タスク.
3. 脆弱性一致アイテムに対して修復タスク (VUL) を選択します。
4. 右下の [編集] を選択します。
5. [コレクション] の検索フィールドに脆弱性一致アイテムの番号を入力します。
6. コレクションから脆弱性一致アイテムを選択し、リストに追加します。
7. [保存] をクリックします。

脆弱性一致アイテムのアサインを解除する

脆弱性対応 および アプリケーション脆弱性対応 アプリケーションの脆弱性一致アイテムレコードを再アサインします。

始める前に

必要なロール： sn_vul.remediation_owner

このタスクについて

脆弱性一致アイテム (VIT) が修復範囲外であると判断した場合、またはレコードが自分または自分のグループに誤ってアサインされていると思われる場合、脆弱性一致アイテムレコードや修復タスクレコードの [アサイン先] および [アサイン先グループ] のフィールドから自分または自分のグループを削除できます。

[アサイン解除] ボタンは、[クローズ済み] または [解決済み] 以外のステータスの以下のレコードに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- クラシック環境と 脆弱性対応 ワークスペースの両方での修復タスク (VUL)。修復タスクがこの機能で更新されると、関連するすべての VIT の [アサイン先] フィールドと [アサイン先グループ] フィールドもクリアされます。
- クラシック環境と 脆弱性対応 ワークスペースの両方での脆弱性一致アイテム (VIT)。
- アプリケーション脆弱性一致アイテム (AVI)。
- コンテナ脆弱性一致アイテム (CVIT)。

重要:
Vulnerability Manager ワークスペース では、ホスト脆弱性一致アイテムのアサインを一括で解除できます。詳細については、「Vulnerability Manager ワークスペース での一括編集の使用」を参照してください。

手順

1. クラシック環境または IT 修復オーナーワークスペースで、[クローズ済み] または [解決済み] 以外のステータスの、自分にアサインされた脆弱性一致アイテム (VIT) レコードに移動します。
2. [アサイン先] および [アサイン先グループ] フィールドをクリアするには、レコードの上部にある [アサイン解除] を選択します。
3. オプション: あるいは、自分または自分のグループにアサインされている AVIT に移動し、[アサイン解除] をクリックしてアサインフィールドをクリアします。
4. [アサイン解除 (Unassign)] ダイアログで作業メモを入力し、[送信] を選択します。
5. オプション: リスト上の複数の VIT のアサインフィールドをクリアする場合は、必要な VIT を選択してから、[一括編集] を選択します。

   a. [脆弱性一致アイテムの一括編集] ダイアログで、[レコード選択] フィールドの [選択された脆弱性一致アイテムのみ] を選択し、[アサイン解除] チェックボックスをオンにして、**[OK]** を選択します。
   一括編集の詳細については、「Bulk edit Vulnerability Response vulnerable items (脆弱性対応での脆弱性一致アイテムの一括編集)」を参照してください。

   b. 通知に表示される修復タスク ID を選択します。

6. 次の情報を表示します。
   - 入力した作業メモが [メモ] セクションに表示されます。
   - [ステータス変更承認] タブでは、ステータス変更承認レコードが [レビュー中] ステータスで表示されるため、承認ワークフローを追跡するの役立ちます。
   - [要求済みの承認 **(Requested Approvals)]** タブでは、自分または自分のアサイン先グループの削除要求が[要求済み] ステータスで表示されます。

タスクの結果
要求は、デフォルトの 1 レベルの承認ワークフローを使用して承認されます。詳細については、「脆弱性マネージャーワークスペースでの要求の承認」を参照してください。

- 要求が承認されると、ステータス変更承認レコードと要求された承認レコードが [承認済み] ステータスに移行します。自分と自分のグループが [アサイン先] フィールドと [アサイン先グループ] フィールドから削除されます。[未アサイン (Unassigned)] が [アサインタイプ] フィールドに表示され、修復タスクと VIT が コンフィグレーションコンプライアンス の [未アサイン (Unassigned)] モジュールのリストに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レコードが未アサインであるという通知は、[通知のアサイン解除 (Unassign notification)] グループの脆弱性マネージャーまたはアナリストに自動的に送信されます。承認フラグ、通知、およびデフォルトのアサイン先グループを設定するには、「脆弱性一致アイテムと修復タスクからのアサインの削除」を参照してください。

- 要求が却下されると、ステータス変更承認レコードのステータスと要求された承認レコードが [却下] ステータスに移行します。

注:
脆弱性アドミニストレーターは、*sn_vul.unassign_vr.approval_required* システムプロパティを **[false]** に設定して、承認プロセスを無効にできます。

次のタスク
脆弱性対応 および アプリケーション脆弱性対応 コンテナ脆弱性対応 アプリケーションの [未アサイン (Unassigned)] モジュールに移動し、スコープ内の該当する可能性があるアイテムの未アサインレコードを監視し、それを自分に再アサインします。

脆弱性対応 でアサイン解除要求を承認または却下する

脆弱性対応 アプリケーションのアサイン先グループまたは個々のユーザーからの脆弱性一致アイテムの削除要求を承認します。

始める前に
必要なロール：承認をアサイン解除するには、承認者 - レベル 1 グループに 1 人の承認者が必要です。

- AVIT および VIT の sn_vul.unassign_approver
- CVIT の sn_vul_container.unassign_approver

このタスクについて
デフォルトでは、承認構成が提供され、アサイン解除承認グループが作成されます。アサイン解除承認者 - レベル 1 グループのユーザーが要求を承認できます。デフォルトでは、このグループにはアサイン解除承認者ロール sn_vul.unassign_approver が含まれています。新しいグループを変更または作成し、承認構成を更新できます。承認ルールを構成するには、承認ルールモジュールで次のいずれかの承認ルールを選択して、[承認構成] タブの承認構成に移動します。

- 脆弱性一致アイテム用の*Vulnerable item field change request*。
- 修復タスク用の*Vulnerability field change request*。
- アプリケーション脆弱性一致アイテム (AVIT) 用の*Application vulnerability field change request*。
- コンテナ脆弱性一致アイテム (CVIT) 用の*Approval for container management*。

承認ルールと承認構成の詳細については、「アサイン解除要求の承認ワークフロー構成」を参照してください。

重要:
Vulnerability Manager ワークスペース で要求を承認または却下できます。詳細については、「Vulnerability Manager ワークスペース で要求を承認または却下」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 自分の承認 VIT および AVIT の場合。
   または、 **All** (すべて) > **Container Vulnerability Response** > 自分の承認 CVITの場合。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. キューから要求を選択します。
3. 適切なコメントを添えて、要求を承認または却下します。

脆弱性一致アイテムと検出の自動クローズ

自動クローズルールモジュールを使用して、廃止された CI に関連付けられた古い検出と脆弱性一致アイテム (VI) を自動的にクローズできます。

次のシナリオでは、古い検出と VI を自動的にクローズできます。

- 脆弱性対応 での古い検出の自動クローズ
- 廃止された CI に関連する脆弱性一致アイテムを自動的にクローズする

廃止された構成アイテムの操作については、「 廃止された構成アイテムの操作 と 自動クローズルールを作成する」を参照してください。

廃止された構成アイテムの操作

廃止された構成アイテム (CI) は、構成管理データベース (CMDB) では [廃止]、[アーカイブ化済み]、または [削除済み] ステータスに移行されます。脆弱性対応 には、CI で構成される脆弱性一致アイテム (VI) が含まれています。CI のステータスが [廃止] に更新されると、関連する VI は「CI 廃止」サブステートでクローズされます。

> **注:**
> 脆弱性対応 の v25.0.3 以降、廃止された CI に関連する脆弱性一致アイテムと検出をクローズするために、新しい自動クローズルール「CI 廃止」が導入されました。

CMDB で CI のライフサイクルステージのステータスが [廃止] に変わった場合は、関連する VI を自動的にクローズするように選択できます。関連する VI の自動クローズの詳細については、「廃止された CI に関連する脆弱性一致アイテムを自動的にクローズする」を参照してください。

廃止された CI はアーカイブされるか、最終的に CMDB から完全に削除されます。

CI の廃止による影響：

- 検出されたアイテムへの影響 **(Impact on discovered items)**：CI が廃止されると、関連するディスカバリーアイテム (DI) は「CI 廃止」とマークされます。
- 脆弱性一致アイテムへの影響：DI のステータスが「CI 廃止」に更新されると、関連する VI がクローズされ、[メモ] セクションが自動的に更新されます。

  > **注:**
  > CI のライフサイクル状況が更新されるたびに、DI のステータスが自動的に「CI 廃止」に更新されます。一方、VI のステータスは、[廃止された **CI** にリンクされた **VI** の自動クローズ] オプションが有効の場合のみ [クローズ済み] に更新されます。関連する VI の自動クローズの詳細については、「廃止された CI に関連する脆弱性一致アイテムを自動的にクローズする」を参照してください。

スケジュール済みジョブ [*Close detections/VIs for decommissioned CIs*] は、更新された DI に対して毎日実行されます。廃止された CI に対して自動クローズ構成オプションが有効になっている場合は、廃止された CI を含む DI が識別され、サブステートが「CI 廃止」である関連 VI がクローズされます。修復タスク内のすべての VI がクローズされ、そのサブステートが「CI 廃止」の場合、修復タスクもクローズされ、サブステートは「キャンセル」になります。廃止された VI を表示するには、次に移動します: 脆弱性対応 > 脆弱性一致アイテム > 廃止.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
CI が「廃止」ステータスから元のステータスに戻ると、「検出されたアイテム」エントリーも更新されます。スキャナーから再度データが取り込まれると、VI が自動的にオープンされます。

廃止された **CI** に関連する脆弱性一致アイテムを自動的にクローズする

構成管理データベース (CMDB) が構成アイテム (CI) のライフサイクルステージのステータスを [廃止] に変更した場合は、関連する脆弱性一致アイテム (VI) および検出を自動的にクローズすることを選択できます。

始める前に
必要なロール：sn_vul.admin

このタスクについて
脆弱性対応 の v22.0 以降では、関連する VI と検出を自動的にクローズするには、廃止された CI に関連付けられている VI を自動クローズするシステムプロパティ *sn_vul_cmn.auto_close_vis_linked_retired_cis* を有効にする必要があります。このオプションを有効にするには、値フィールドを「1」に設定します。逆に、このオプションを無効にするには、値フィールドを「0」に設定します。

アップグレード中に、脆弱性対応の v21.0 でシステムプロパティ *sn_vul_cmn.auto_close_vis_linked_retired_cis* が選択されている場合、値は「1」のままになります。このオプションを有効にすると、同じ CI について報告された新規または既存の VI および検出は、自動的に「クローズ済み」ステータスで作成または更新されます。これは、スキャナーペイロードの資産 ID と検出されたアイテムエントリーのステータスに基づいています。廃止された CI の影響の詳細については、「廃止された構成アイテムの操作」を参照してください

。

注:

- CI のライフサイクル状況が更新されるたびに、DI のステータスが「CI 廃止」に更新されます。一方、VI のステータスは、[廃止された **CI** にリンクされた **VI** の自動クローズ] オプションが有効の場合のみ [クローズ済み] に更新されます。
- 次の手順で提供される情報は、脆弱性対応 v22.0 より前のバージョンにのみ適用されます。脆弱性対応 v22.0 以降では、追加の検索オプションを構成できます (オプション)。詳細については、「自動クローズルールを作成する」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 自動クローズ構成 > 構成アイテム **(CI)** のライフサイクル.
2. 廃止された CI に関連付けられた脆弱性一致アイテムを自動的にクローズするには、[廃止された **CI** にリンクされた **VI** の自動クローズ] チェックボックスをオンにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [更新] を選択します。

> **注:**
> [廃止された **CI** にリンクされた **VI** の自動クローズ] オプションが有効になる前に CI が既に廃止されている場合、VI はスキャナーからの新しい検出に対してのみ作成されます。こうした VI のステータスは [クローズ済み] で、サブステートは [CI 廃止] です。
>
> ステータスが [CI 廃止] になっている VI を、[再オープン] または [一括編集] オプションを使用して手動で再オープンすることはできません。
>
> サブステートが [修正済み] または [古い] であるクローズ済みの VI は、新しい検出が作成され、VI が新しい脆弱性と一致する場合に再オープンされます。詳細については、「検出、修復タスク、および脆弱性一致アイテム状況」を参照してください。

脆弱性対応 での古い検出のクローズ

[古い検出を自動クローズ] モジュールを使用すると、サードパーティ統合によって最近検出されなかった古い脆弱性検出を自動的にクリーンアップすることができます。こうした検出を [クローズ済み] に移行すると、Now Platform インスタンスにあるアクティブな脆弱性一致アイテムと修復タスクの数を減らし、CMDB 内の資産を調整するのに役立ちます。

概要と主要な用語

検出データを脆弱性一致アイテムにより正確にロールアップするために、[古い検出を自動クローズ] モジュールを使用すると、サードパーティ統合によって最近検出されなかった古い脆弱性一致アイテムの検出をクリーンアップすることができます。この機能の詳細については、以下のユースケースと古い検出の自動クローズ [KB 0958638] の記事を参照してください。

脆弱性対応 の以前のバージョンでは、脆弱性一致アイテムの自動クローズモジュールにより、サードパーティのスキャナー統合によって最近検出も更新もされていない脆弱性一致アイテムが [クローズ済み - 古い] に自動的に移行されていました。

[古い検出を自動クローズ] 機能を有効にする前に、以下の用語と、状況が脆弱性一致アイテムと修復タスクにどのようにロールアップされるか、および検出データをインポートするサードパーティ統合の前提条件を確認してください。

機能を有効にするには、「脆弱性対応 での古い検出の自動クローズ」を参照してください。

主要な用語

古い検出
: Now Platform® インスタンス内の脆弱性一致アイテムに関連付けられた検出のうち、古く、長期間にわたってサードパーティの統合スキャンによって発見、更新、検出されていないものを指します。

最後に発見された検出
: この検索オプションは、サードパーティのスキャナーによって提供された日付と時刻を使用します。この用語は、スキャナーによって検出が再度見つかった最新の日時を指します。

前回スキャンされた資産
: この検索オプションは、サードパーティのスキャナーによって提供された日付と時刻を使用します。この用語は、サードパーティのスキャナーによって資産が前回スキャンされた日時を示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユースケース

資産 (構成アイテム) は、お使いの環境で廃止されたり、サードパーティのスキャナーによって消去されたりすることがあり、関連付けられた検出が脆弱性一致アイテムの検出によって更新されない場合があります。その結果、検出と関連する脆弱性一致アイテムは 脆弱性対応 アプリケーションで更新されず、非アクティブ (古い) になります。

変更されていない脆弱性一致アイテムデータがあるこのような古い検出をクローズし、次にアクティブな VI と修復タスク (RT) の数を減らすには、 [古い検出を自動クローズ] を有効にします。この機能により、設定した検索条件と経過日数に基づいて、サードパーティのスキャナー統合で最近検出も更新もされていない脆弱性一致アイテムの検出が自動的にクローズされます。

たとえば、特定の構成アイテム (CI) に複数の資産 ID があり、そのうちの 1 つの ID が過去 90 日間にサードパーティのスキャナーからの検出でインポートされていなかったとします。この機能により、新しい脆弱性データがないこの検出が自動的にクローズされるため、関連する VI をクローズできます。

VI には複数の検出が関連付けられている可能性があるため、この機能では、設定したパラメーターによって古いと判断された検出のみが移行されます。たとえば、VI に 4 つの検出が関連付けられており、2 つの検出が古い場合、つまり、過去 90 日間に新しい脆弱性データがインポートされていない場合、この機能では古い検出のみがクローズされます。VI をクローズするには、まず他の 2 つのオープンされている検出を修正する必要があります。

VI への検出状況のロールアップ

自動クローズされた検出とサードパーティのスキャナーによってクローズされた検出を区別するために、[ステータス] フィールドに新しい値として [古い] が追加されました。このフィールドに指定できる値は、 [オープン]、 [クローズ済み]、および [古い] です。[古い] は、検出の自動クローズ機能によって検出がクローズされたことを示します。

ステータスの優先順位：[オープン] > [クローズ済み] > [古い]。

1. 検出が [オープン] の場合、関連する VI のステータスは [オープン] のままになります。
2. 検出が [オープン] ではなく、一部が [クローズ済み] で、一部が [古い] 場合、関連する VI 状況は [クローズ済み - 修正済み (Closed - Fixed)] に移行します。
3. すべての検出が古い場合、関連する VI 状況は [クローズ済み - 古い (Closed - Stale)] に移行します。

   脆弱性対応 20.0 以降は、検出が [古い] で、関連する VI が [クローズ済み] ステータスの場合、VI のステータスは [クローズ済み - 古い (Closed - Stale)] に移行しません。これは、新しい検出が特定されたときに VI が再オープンしないようにすることで、誤検出の要求と承認プロセス全体を回避できるようにするためです。この動作を元に戻すには、[自動クローズ構成] フォームの [クローズされている **VI** の古い検出を無視する] チェックボックスをオフにします。詳細については、「脆弱性対応 での古い検出の自動クローズ」を参照してください。

修復タスク **(VUL)** への **VI** 状況のロールアップ

ステータスの優先順位：[オープン] > [クローズ済み - 修正済み (Closed - Fixed)] > [クローズ済み - 古い (Closed - Stale)]。

1. VUL (修復タスク) の VI が [オープン] の場合、VUL ステータスは変更されません。
2. 少なくとも 1 つの VI が [クローズ済み - 修正済み (Closed - Fixed)] で、残りが [クローズ済み - 古い (Closed - Stale)] の場合、VUL 状況は [クローズ済み - 修正済み (Closed - Fixed)] に移行します。
3. VUL 内のすべての VI が [クローズ済み - 古い (Closed - Stale)] の場合、VUL 状況は [クローズ済み - キャンセル (Closed - Canceled)] に移行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

自動クローズ検出とサードパーティ統合の要件

Microsoft TVM ユーザーと古い検出の自動クローズ

チェックリストアイテム	説明
Microsoft TVM 脆弱性統合	Microsoft TVM 脆弱性統合で検索のベースとして [最後に発見された検出] を選択した場合、この機能では過去 7 日以内に Microsoft TVM マシン脆弱性統合 (フルインポート) が正常に実行されている必要があります。この統合は毎週実行されます。 [古い検出を自動クローズ] が有効で [最後に発見された検出] に対して設定されていても、Microsoft TVM マシン脆弱性統合が無効になっている場合や、データインポートが過去 7 日以内に正常に完了していない場合、検出をクローズするスケジュール済みジョブは毎日実行されますが、一部の古い検出が想定どおりにクローズされないことがあります。 [前回スキャンされた資産] を検索のベースとして選択した場合、Microsoft TVM マシン脆弱性統合を実行する必要はありません。 この統合をアクティブ化するには： 1. 次のように移動する。 **Microsoft TVM** 脆弱性統合 > アドミニストレーション > **Integration** (統合). 2. **Microsoft TVM** マシン脆弱性 (フルインポート) を見つけて有効にします。
(オプション) Microsoft TVM 統合の複数のインスタンスを現在の環境に展開します。	必要に応じて、統合の複数のインスタンスを環境全体に展開できます。 古い検出の自動クローズはインスタンス固有ではなく、環境全体で有効または無効になります。統合実行が正常に完了したインスタンスでは、古い検出は自動的に [古い] に移行されます。 [古い検出を自動クローズ] が有効になっており、インスタンスで毎週実行される統合を無効にした場合でも、検出をクローズするスケジュール済みジョブは毎日実行されますが、一部の検出が想定どおりに自動的に [古い] に移行されないことがあります。

Qualys ユーザーと古い脆弱性一致アイテムの自動クローズ

- 検出データを取得するアクティブ化された Qualys サードパーティ統合は、このモジュールで実行できます。特定の Qualys アプリケーションは必要ありません。
- 必要に応じて、Qualys 統合の複数のインスタンスを環境全体に展開できます。
- 古い検出の自動クローズはインスタンス固有ではなく、環境全体で有効または無効になります。古い検出は、すべてのインスタンスで自動的に [古い] に移行されます。

Rapid7 ユーザーと古い検出の自動クローズ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリストアイテム	説明
Rapid7 脆弱性統合	[最後に発見された検出] を検索のベースとして選択する場合、この機能では、過去 7 日以内に Rapid7 の包括的な脆弱性一致アイテムの統合のいずれかが正常に実行されている必要があります。以下の包括的な統合が毎週実行されます。 • Rapid7 Nexpose データウェアハウスについては、Rapid7 の包括的な脆弱性一致アイテムの統合から正常に実行される必要があります。 • Rapid7 InsightVM については、Rapid7 の包括的な脆弱性一致アイテムの統合 - API から正常に実行される必要があります。 [古い検出を自動クローズ] が有効で [最後に発見された検出] に対して設定されていても、Rapid7 の包括的な脆弱性一致アイテム統合が無効になっている場合や、データインポートが過去 7 日以内に正常に完了していない場合、検出をクローズするスケジュール済みジョブは毎日実行されますが、一部の古い検出が想定どおりにクローズされないことがあります。 [前回スキャンされた資産] を検索のベースとして選択すると、包括的な Rapid7 統合を実行する必要はありません。 これらの統合をアクティブ化するには： **1.** 次のように移動する。 **Rapid7 Vulnerability Integration** > アドミニストレーション > **Integration** (統合). **2.** 必要な Rapid7 の包括的な脆弱性一致アイテムの統合を見つけて有効にします。 **注:** 毎週実行されるこれらの統合に加えて、Rapid7 Nexpose および Rapid7 InsightVM にはそれぞれ、毎日実行される VI 統合、Rapid7 脆弱性一致アイテム統合、および Rapid7 脆弱性一致アイテム統合 - API があります。 日次と週次の Rapid7 の統合が両方とも有効になっている場合でも、一度に実行される統合は 1 つだけです。これらの統合ジョブのいずれかが実行されている場合、もう一方の統合のジョブは次のスケジュール済みジョブまでスキップされます。
(オプション) Rapid7 統合の複数のインスタンスを現在の環境に展開します。	必要に応じて、包括的な統合の複数のインスタンスを環境全体に展開できます。 古い検出の自動クローズはインスタンス固有ではなく、環境全体で有効または無効になります。統合実行が正常に完了したインスタンスでは、古い検出は自動的に [古い] に移行されます。 [古い検出を自動クローズ] が有効になっており、インスタンスで毎週実行される統合を無効にした場合でも、検出をクローズするスケジュール済みジョブは毎日実行されますが、一部の検出が想定どおりに自動的に [古い] に移行されないことがあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable 脆弱性統合ユーザーと古い脆弱性一致アイテムの自動クローズ

- 検出データを取得する Tenable 脆弱性統合からアクティブ化された統合は、このモジュールで実行できます。特定の Tenable 脆弱性統合は必要ありません。
- 必要に応じて、Tenable 脆弱性統合の複数のインスタンスを環境全体に展開できます。
- 古い検出の自動クローズはインスタンス固有ではなく、環境全体で有効または無効になります。古い検出は、すべてのインスタンスで自動的に [古い] に移行されます。

統合が適切に構成されていることを確認したら、「脆弱性対応 での古い検出の自動クローズ」を参照して機能を有効にします。

古い脆弱性一致アイテムの自動クローズから古い検出の自動クローズへのアップグレード情報

[古い検出を自動クローズ] モジュールで、以前に古い脆弱性一致アイテムの自動クローズを使用していた場合：

- 古い脆弱性一致アイテムの自動クローズの [前回スキャンされた資産] オプションで入力した日数の値は、[古い検出を自動クローズ] の [前回スキャンされた資産] 用に自動的に保持されます。
- 古い脆弱性一致アイテムの自動クローズの [前回検出された脆弱性一致アイテム] オプションで入力した日数の値は、[古い検出を自動クローズ] の [最後に発見された検出] 用に自動的に保持されます。
- 脆弱性一致アイテムが [クローズ済み - 古い (Closed - Stale)] に設定されている既存のオープン状態の検出は、アップグレード後に *Auto-Close Stale Detections* スケジュール済みジョブが実行されると、自動クローズの構成設定に従って [古い] に移行されます。

ロールアップ情報

- 脆弱性一致アイテムがアップグレード前に [クローズ済み - 古い (Closed - Stale)] で、アップグレード後にすべての検出が [古い] とマークされている場合、VI ステータスは [クローズ済み - 古い (Closed - Stale)] のままになります。
- 脆弱性一致アイテムがアップグレード前に [クローズ済み - 古い (Closed - Stale)] で、アップグレード後に一部の検出のみが [古い] としてマークされ、残りがスキャナーによってクローズされた場合、脆弱性一致アイテムはロールアップロジックに従って [クローズ済み - 修正済み (Closed - Fixed)] に移行します。

脆弱性対応 での古い検出の自動クローズ

[古い検出を自動クローズ] を有効にすると、サードパーティ統合によって最近検出されなかった古い脆弱性検出が自動的にクローズされます。

始める前に

必要なロール：sn_vul.vulnerability_admin、sn_vuln.admin (非推奨)、または sn_vul.manage_auto_close_stale_vi 詳細ロールを持つ脆弱性マネージャー。

この機能、重要な用語、および検出データをインポートするサードパーティ統合に必要なセットアップの詳細については、「脆弱性対応 での古い検出のクローズ」を参照してください。

注:
次の手順で提供される情報は、脆弱性対応 v22.0 より前のバージョンにのみ適用されます。脆弱性対応 v22.0 以降では、追加の検索オプションを構成できます (オプション)。詳細については、「自動クローズルールを作成する」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 脆弱性対応 > アドミニストレーション > 自動クローズ構成 > 古い検出.
   [古い構成を自動クローズ (Auto-Close Stale Configuration)] フォームが表示されます。
2. フィールドに入力します。
3. [古い検出を自動クローズする基準] フィールドで、検索のオプションを 1 つ選択します。

   どちらの検索も、古くなった検出の経過時間 (日数) とスキャナーによって提供された日付とを照合します。

   > **注:**
   > 脆弱性対応 v22.0 以降、[最後に発見された検出] オプションと [前回スキャンされた資産] オプションがリスト形式で作成されます。

   - 最後に発見された検出。このオプションは、スキャナーによって検出が再度見つかった最新の日付を検索します。

     > **注:**
     > Rapid7 および Microsoft TVM のユーザーの場合、現在の検出情報が必要であることを示す警告メッセージが表示されます。
     >
     > [最後に発見された検出] を検索のベースとして選択する場合、この機能では、過去 7 日以内に Rapid7 の包括的な脆弱性一致アイテム統合のいずれかの統合実行が正常に行われている必要があります。
     >
     > [最後に発見された検出] を検索のベースとして選択する場合、この機能では、過去 7 日以内に Microsoft TVM マシン脆弱性統合 (フルインポート) の統合実行が正常に行われている必要があります。

   - 前回スキャンされた資産。このオプションは、サードパーティのスキャナーによって資産が前回スキャンされた最新の日付を検索します。
4. Rapid7 および Microsoft TVM のユーザーの場合のみ、必要な統合が有効になっていることを確認します。
   詳細については、「Rapid7 脆弱性統合の概要」と「Microsoft Threat and Vulnerability Management 脆弱性統合の概要」を参照してください。
5. モジュールを有効にするには、[アクティブ] チェックボックスをクリックしてオンにします。
6. [最後に発見された検出 (日前)] フィールドに、古くなった検出の経過日数を入力します。

   デフォルトは 90 日です。日数には任意の正の値を入力できます。この値は、スキャナーによって提供される日付と照合するために使用されます。[90] と [最後に発見された検出 (日前)] が表示されている場合、過去 90 日間に見つからなかった検出は自動的にクローズされます。[90] と [前回スキャンされた資産] が表示されている場合、過去 90 日間にスキャンされなかった資産に関連する検出は自動的にクローズされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

この機能の [最後に発見された検出/前回スキャンされた資産 (日前) **(Detections last found/Assets last scanned (days ago))]** フィールドと、Rapid7 包括的な脆弱性一致アイテム統合 - API および Microsoft TVM マシン脆弱性統合の [次以降にインポート] フィールドの間には関係があります。

これらの統合の構成ページの [次以降にインポート] フィールドは、デフォルトでは空です。

値を入力しない場合、またはフィールドに値がない場合は、[最後に発見された検出/前回スキャンされた資産 (日前) **(Detections last found/Assets last scanned (days ago))]** フィールドで設定された日数のデータが使用されます。

たとえば、自動クローズ構成フォームで定義された日数が 90 で、統合構成ページの [次以降にインポート] フィールドが空白の場合、最初の統合実行で過去 90 日のデータがインポートされます。 Rapid7 包括的な脆弱性一致アイテム統合 - API および Microsoft TVM マシン脆弱性統合の [次以降にインポート] フィールドは編集可能であるため、必要な値を指定することもできます。自動クローズ機能で誤検出がクローズされないように、フィールドが空の場合はデフォルトで 90 日の値が指定されます。

これらのフィールド間のこの関係は、最初の統合実行にのみ適用されます。その後、[古い脆弱性検出の自動クローズ (Auto-Close Stale Vulnerable detections)] フォームの [最後に発見された検出/前回スキャンされた資産 (日前) **(Detections last found/Assets last scanned (days ago))]** フィールドを変更しても、統合構成ページの [次以降にインポート] フィールドに影響はありません。このフィールドは、後続の統合実行でデルタ情報のみがインポートされるように、最初の実行の開始時間に変更されます。

7. オプション: 保留された VI または保留について現在レビュー中の VI にマッピングされている古い検出を無視するには、[保留された **VI** の古い検出を無視する] チェックボックスをオンにします。

   (Optional) このオプションを無効のままにすると、保留された VI または保留についてレビュー中の VI にマッピングされる、基準に一致するすべての検出がクローズされます。保留された VI またはこうした検出に対応するレビュー中の VI も、ロールアップロジックに基づいて自動的にクローズされます。ロールアップロジックの詳細については、「脆弱性対応 での古い検出のクローズ」を参照してください。

   このオプションを有効にすると、保留された VI または保留についてレビュー中の VI にマッピングされる、基準に一致するすべての検出は、自動クローズ時にスキップされます。

8. オプション: [クローズされている **VI** の古い検出を無視する] チェックボックスをオフにします。

   (Optional) デフォルトでは、このチェックボックスはオンになっており、このクローズ済み VI に関連する新しい検出が特定されたときにクローズ済み VI が再オープンされないようにします。ロールアップロジックの詳細については、「脆弱性対応 での古い検出のクローズ」を参照してください。

9. [更新] をクリックして変更を保存します。

   スケジュール済みジョブ [*Auto-Close Stale Detections*] を毎日実行します。このジョブでは、選択された日付が「最後に検出があった日付」と「最後に資産がスキャンされた日付」のどちらであるかを判断します。当該検出のステータスが [古い] に移行します。[古い検出を自動クローズ] 機能では、アクティブな統合インスタンスにおいて古い検出をクローズするだけであるということがポイントです。アクティブな統合インスタンスに関連付けられている脆弱性一致アイテムや検出はクローズされます。脆弱性対応 v22.0 以降、スケジュール設定済みのジョブが変更され、共通テーブル [sn_vul_cmn_auto_close_rule] が考慮されるようになりました。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

検出が [古い] とマークされた後、スキャナーがその検出の発見を再度報告すると、検出の [ステータス] フィールドは [オープン] に移行します。検出の対応する脆弱性一致アイテムも再オープンされます。

また、検出が [古い] とマークされていて、スキャナーがそれを [修正済み] であると判断した場合、検出は [クローズ済み] に移行します。ステータスも VI にロールアップされます。

自動クローズルールを作成する

自動クローズルールを使用して、設定したフィルター条件に基づいて古い検出を自動的にクローズします。

始める前に

必要なロール：sn_vul.manage_auto_close_stale_vi

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 自動クローズルール.

   ベースシステムには次の自動クローズルールが提供されます。

   - 前回スキャンされた資産：過去 90 日以内にスキャンされなかった資産に関連付けられる検出は、[古い] ステータスに移行されます。
   - 最後に発見された手動検出：過去 90 日以内に見つかっていない手動検出。[最後に発見された検出] レコードをアクティブ化する場合、この機能では、過去 7 日以内に Rapid7 包括的脆弱性一致アイテム統合と Microsoft TVM マシン脆弱性統合 (フルインポート) の統合実行が正常に行われている必要があります。
   - 最後に発見された検出：過去 90 日以内に見つかっていない検出。
2. [新規] を選択して、新しい自動クローズルールを作成します。
3. フォームのフィールドに入力します。

フィールド	値
名前	自動クローズルールの名前
アクティブ	ルールをアクティブ化するためのオプション有効にすると、フィルター基準に一致するすべての検出が自動的にクローズされます。
保留されたアイテムを無視	選択すると、[レビュー中] または [保留] ステータスにマッピングされた検出は無視され、クローズされません。このオプションをオフにすると、基準に一致するすべての検出がクローズされます。
実行順序	自動クローズルールの実行に対する一意の値。この値によって実行順序が決まります。デフォルト値は 100 です。
説明	自動クローズルールの説明。
条件	クローズする必要がある検出を識別するために使用されるフィルター条件。

4. [送信] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みジョブ [*Auto-Close Stale Detections*] を毎日実行します。指定された条件に基づいて検出を識別し、一致した検出を [古い] ステータスに移行します。このジョブは、次のシナリオを処理します。

- 脆弱性一致アイテム (VIT) 内のすべての検出が古いとマークされている場合、VIT はサブステートが [古い] に設定されてクローズされます。
- VIT 内でオープンのままの検出が少なくとも 1 つあり、他の検出が [古い] ステータスである場合、VIT はオープンのままになります。
- VIT 内に [クローズ済み] と [古い] の両方のステータスの検出がある場合、VIT はサブステートが [修正済み] に設定されてクローズされます。

最新バージョンの脆弱性対応にアップグレードすると、それに応じて自動クローズルールに設定された条件も更新されます。また、ルールが異なるドメインに関連付けられている場合、ルールはそれらのドメイン内に限定的に作成されます。

未分類のハードウェアの再分類

CI ルックアップルールを更新して、未分類のハードウェアを再分類します。

始める前に

必要なロール：sn_sec_cmn.admin

このタスクについて

ホストインポートマップ [sn_sec_cmn_src_cmdb_map] テーブルでは、ペイロードの受信変数とそれに対応するアサインメントが [検出されたアイテム] テーブルに表示されます。スキャナーとディスカバリーの間で命名規則に不一致があると、ハードウェアが未分類のままになることがあります。新しい未分類のハードウェア CI の作成中、ペイロード内の名前にはホスト名だけが含まれるようにします。後で、ディスカバリーでその資産が特定されたときに、適切な CI クラスに再分類できます。必要に応じて、ディスカバリーと構成管理データベース (CMDB) の両方の CI 名と一致する派生値を生成するスクリプトを記述できます。

識別および調整エンジン (IRE) がアクティブ化されている場合、検出されたアイテムからの再分類オプションはサポートされません。

手順

1. ホストインポートマップ [sn_sec_cmn_src_cmdb_map] テーブルに移動します。
2. ソースを選択します。
3. ターゲットフィールドリストから、[名前] を選択します。
   [スクリプトを使用] チェックボックスが表示されます。

注:

- スクリプトは、 ターゲットフィールドリストから [名前] が選択されている場合にのみ使用できます。
- ターゲットフィールドリストの他のオプションのスクリプトを追加するには、次の方法で UI ポリシーを無効にする必要があります。
  - [使用スクリプトを false に設定 (Set Use script false)] を無効にする。
  - [使用スクリプトを表示または非表示 (Show or Hide Use Script)] を無効にする。
  - [スクリプトポリシーを表示または非表示 (Show or Hide Script policy)] の条件 [ターゲットフィールドは名前 (target field is name)] を削除する。
- [ホストインポートマップ] テーブルが、[スクリプト] と [スクリプトを使用] の 2 つの新しい列で更新されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [スクリプトを使用] チェックボックスをオンにします。
   [スクリプト] フィールドにはデフォルトのスクリプトが表示されますが、カスタムスクリプトを作成することもできます。このフィールドでは、データベースの命名規則に合わせてソース値と派生値を指定できます。スクリプトによって生成された値は、sourcePayload['DERIVED'][rule.source_field] に格納されます。対応するテーブルをチェックインするときに、ソースペイロード、派生、およびターゲット属性の値を使用するように CI ルックアップルールが調整されていることを確認します。
5. 古い重複レコードにスクリプトを適用するには、次の操作を行います。
   a. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 検出済みアイテム.
   b. 重複レコードを選択します。
   c. [選択した行でアクションを実行] リストで、**[CI** ルックアップルールを再適用] を選択します。
   既存の資産との一致が表示されます。
6. Tenable.io のスクリプトを適用するには、次の操作を行います。
   a. 次のように移動する。 脆弱性対応 ホストインポートマップ。
   b. [ソース] フィールドで [NETBIOS]、[HOSTNAMES]、および [FQDNS] が指定されている行のスクリプトを選択します。
   c. 各要素のスクリプトを更新します。

   注:
   Tenable.io の場合、スキャナーはスクリプトが想定どおりに機能しない [NETBIOS]、[HOSTNAMES]、および [FQDNS] のアレイを返します。

   Tenable.io のホストインポートマップの [ソースフィールド] には **netBIOS_name** が含まれているため、スクリプトを記述する必要があります。ルックアップ中は、値のアレイを持つ別のソースフィールド **[NETBIOS]** が使用されます。したがって、新しい行がテーブルに追加され、同じロジックをスクリプトのループに記述する必要があります。**[FQDNS]** と **[HOSTNAMES]** に対しても同じようにします。
7. Rapid7 のスクリプトを適用するには、次の操作を行います。
   a. 次のように移動する。 **All** (すべて) > 脆弱性対応 ホストインポートマップ。
   b. Rapid7 の行に FQDN と HostName が指定されている 場合は、[ルックアップメソッド] を [スクリプト] に更新します。

   注:
   Rapid7 の場合、FQDN と HostName の CI ルックアップメソッドは [一致するフィールド] に設定されるため、スクリプトは使用できなくなります。

脆弱性対応 での修復タスクの手動作成

脆弱性一致アイテムを修復タスクルールの基準以外のものでグループ化する場合は、手動で修復タスクを作成します。たとえば、特定のマネージャーに対して、またはさまざまな脆弱性を含むランサムウェアなどのアクティブな新しいエクスプロイトに対して、タスクを作成できます。またその方法は、グループ化されていない脆弱性一致アイテムをグループ化するためにも使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重要:
ホスト修復タスクは、次の方法で作成できます。

- Vulnerability Manager ワークスペースsn_vul.vulnerability_analyst, または sn_vul.vulnerability_admin ロールを持つユーザーとして。
- IT 修復ワークスペース sn_vul.remediation_owner ロールを持つユーザーとして。

始める前に
必要なロール：sn_vul.vulnerability_analyst、sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 修復タスク.

   修復タスクルールは、以前の修復タスクルールと同じように機能し、引き続き使用できます。ただし、ワークスペースでセキュリティマネージャーと IT チームが使用できる機能に慣れてきたら、修復タスクルールを無効にしておくことをお勧めします。

2. タスクのカテゴリのいずれかを選択してリストを開きます。
3. [新規] をクリックします。
4. 必要に応じて、フォームのフィールドに入力します。
   特定のフィールドの詳細については、「修復タスクフォームフィールド」を参照してください。
5. **[Submit]** をクリックします。
   タスクが作成されると、[条件] または [フィルターグループ] フィルタータイプを使用して、[脆弱性一致アイテム] 関連リストで、一致するすべての脆弱性一致アイテムが検索され表示されます。

   ServiceNow® で開始されたスキャンを手動でトリガーするには、[脆弱性の再スキャン **(Re-scan for Vulnerabilities)]** 関連リンクを使用できます。脆弱性スキャナーの設定方法については、「Qualys 脆弱性スキャナーとスキャンの設定および管理」を参照してください。

   Qualys Vulnerability Integration の場合、デフォルトのスキャナーは脆弱性スキャナーモジュールにインストール済みです。このスキャナーはデフォルトで非アクティブ化されています。[アクティブ] および [デフォルト] のチェックボックスをオンにし、[修復タスク] および [脆弱性一致アイテム] フォームの [脆弱性のスキャン **(Scan for Vulnerabilities)]** 関連リンクを使用して Qualys スキャナーをアクティブ化します。

   [ステータスを更新 **(Update status)]** 関連リンクには、前回の更新の日時が表示されます。修復タスクの VI からの情報をロールアップします。詳細については、「修復タスクフォームフィールド」を参照してください。特定の脆弱性に基づいてタスクが形成されると、その脆弱性が修復タスクフォームに一覧表示されます。

   関連付けられた脆弱性一致アイテムを開くと、関連する修復タスクエントリーが [修復タスク **(Remediation Task)]** 関連リストタブの下に表示されます。

脆弱性対応グループへのユーザーの追加

クローズ/保留機能を使用して、スキャンを要求せずに脆弱性一致アイテムを保留またはクローズすると、その要求を承認または却下するように 脆弱性対応 グループに通知が出されます。適切なユーザーをアサインできます。

始める前に
必要なロール：admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > ユーザー管理 **(User Administration)** > グループ.
2. 脆弱性対応 グループを開きます。
3. [グループメンバー] 関連リストをクリックし、[編集] をクリックします。
4. [コレクション] リストで 1 つ以上の名前を選択します。
5. [追加] をクリックします。
6. [保存] をクリックします。

関連情報

ユーザーの作成

個々の脆弱性一致アイテムを手動で管理する

脆弱性一致アイテムは、特定の脆弱性を持つ 1 つの構成アイテム (CI) を表します。脆弱性一致アイテムは、サードパーティのソースからインポートされるか、SAM NVD 情報 (リンク) を使用して脆弱性エントリーとソフトウェア 資産管理 モジュールから取得されたソフトウェアレコードを比較します。

脆弱性一致アイテムは、脆弱性ルールによって定義された修復タスクに含まれています。通常、修復タスクとは、脆弱性一致アイテムのグループがアサインされて作業される場所です。

脆弱性一致アイテムは、[脆弱性一致アイテム] モジュールから一括で表示および編集できます。脆弱性一致アイテムレコードは、脆弱性からの情報を[脆弱性] タブに表示します。このタブでは、それぞれに公開エクスプロイトやアクティブなエクスプロイトがあるかどうかを示すことができます。また、パッチ、構成の変更、またはその両方の組み合わせによって修復可能かどうかも示されます。重複排除中に見つかった IP アドレスがある場合は、関連リストに表示されます。

CI が CMDB から削除されると、関連する脆弱性一致アイテムも同様に削除されます。

脆弱性一致アイテムが修復タスクに追加されると、そのグループが脆弱性一致アイテムの [修復タスク] リストに表示されます。

脆弱性一致アイテムに影響を与えるタスクが作成されると、そのタスクは脆弱性一致アイテムの [影響を受けるタスク **(Affecting Tasks)]** 関連リストに表示されます。

脆弱性一致アイテムは手動で作成できます。セキュリティインシデントまたは変更要求を作成し、それらを手動でクローズまたは保留することができます。修復タスクルールは、手動で作成された脆弱性一致アイテムに適用できます。

修復タスクと修復タスクルールは、タスクの機能が引き継がれるように拡張されました。脆弱性一致アイテムを親タスクとしてリンクすることはできません。

脆弱性対応 脆弱性一致アイテムの作成

複数の方法で脆弱性一致アイテム (VI) を作成します。最も一般的には、脆弱性スキャナーへの統合がインストールされ、夜間に結果をインポートするように構成されています。物理的なセキュリティの脆弱性のように、脆弱性一致アイテムレコードを手動で追加することをお勧めする場合があります。

始める前に
必要なロール：sn_vul.vulnerability_write

このタスクについて
手動で作成した VI と自動的に作成された VI は、修復タスクルールとグループ条件に基づいて修復タスクに対して自動的に追加されたり削除されたりします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム.
2. カテゴリを選択してリストを開きます。
3. [新規] をクリックします。
4. 必要に応じて、フォームのフィールドに入力します。
   脆弱性一致アイテムのフィールドについては、「脆弱性対応 脆弱性一致アイテムフォームフィールド」を参照してください。
5. フォームヘッダーを右クリックし、[保存] をクリックします。

   修復タスクルールでは、脆弱性一致アイテムを評価してそれを既存のタスクに追加するか、または新しいタスクを作成します。評価に失敗した場合、脆弱性一致アイテムは [グループ解除済み脆弱性一致アイテム] リストに追加されます。

   新しい脆弱性一致アイテムを保存すると、すべての有効な算出が実行されます。

   > **注:**
   > 一度に有効にできる算出は、ターゲットフィールドごとに 1 つのみです。いずれかをアクティブ化すると、同じターゲットフィールドを対象にした他のすべての算出が非アクティブ化されます。

6. 関連リストのいずれかをクリックして、追加情報を確認できます。

   ServiceNow® で開始されたスキャンを手動でトリガーするには、[脆弱性のスキャン **(Scan for Vulnerabilities)]** 関連リンクを使用できます。脆弱性スキャナーの設定方法については、「Qualys 脆弱性スキャナーとスキャンの設定および管理」を参照してください。

   Qualys Vulnerability Integration の場合、デフォルトのスキャナーは脆弱性スキャナーモジュールにインストール済みです。このスキャナーはデフォルトで非アクティブ化されています。[アクティブ] および [デフォルト] のチェックボックスをオンにし、[修復タスク] および [脆弱性一致アイテム] フォームの [脆弱性のスキャン **(Scan for Vulnerabilities)]** 関連リンクを使用して Qualys スキャナーをアクティブ化します。

   ヘッダーバーから、以下の編集オプションや修復オプションを使用できるようになります。

   - 更新：フォームの更新を保存します。
   - セキュリティインシデントを作成：セキュリティインシデントを作成します。
   - クローズ：アイテムをクローズします。グループ内のすべてのアイテムがクローズされると、修復タスクは自動的にクローズされます。
   - 例外の要求：アイテムを保留する要求を送信します。
   - 解決：アイテムを解決します。
   - 削除：脆弱性一致アイテムを削除します。

関連情報

脆弱性対応 での脆弱性一致アイテムの一括編集

脆弱性一致アイテムの保留

脆弱性一致アイテム (VIT) に関連する問題が低リスクで、それ以上分析することなくすぐに保留できると判断した場合は、[保留] 機能を使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

このタスクについて
スケジュール済みジョブで、再オープン日に達した保留中の脆弱性一致アイテムが毎日チェックされます。VI の保留が期限切れになる日に、レコードが再オープンされます。

脆弱性対応 v20.0 以降では、保留された VI を再オープンする前に、[脆弱性一致アイテムとグループの保留の有効期限の確認 (Check Vulnerable Item and Groups Deferment Expiration)] スケジュール済みジョブは、保留された VI に適用可能な例外ルールがあるかどうかをチェックし、例外ルールに従って [理由] フィールドと [まで] フィールドを更新します。VI のステータスは、最新の有効期限まで [保留 (Deferred)] のままです。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム.
2. 脆弱性一致アイテムを開きます。
3. [例外の要求] をクリックします。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
期限	保留ステータスが期限切れになり、修復タスクが再アクティブ化される日付を選択します。 **注:** 脆弱性対応 (VR) のバージョン 18.0 以降は、保留された脆弱性一致アイテムがクローズされ、例外期間が終了する前にスキャナーによって再オープンされると、VIT のステータスがアクティブな例外ウィンドウに従って [保留] ステータスに戻ります。この機能を有効にするには、システムプロパティ sn_vul.auto_defer_vit_in_active_exception_window の値を true に設定します。また、保留期限の日付は、脆弱性一致アイテムがクローズした後や例外の有効期限が切れた後も保持されます。必要なロールは、読み取りと書き込みの両方に sn_vul.manage_exception_configuration です。 レコードが送信された後、メール通知が定義されている場合、有効期限が 1 週間以内になると 脆弱性対応 グループのメンバーにメールが送信されます。保留日が期限切れになると、脆弱性一致アイテムは [オープン] に戻され、2 回目のメール通知が送信されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
理由	問題を保留する理由を入力します。 次の選択肢があります。 ○ メンテナンス期間待ち ○ 誤検出 ○ 修正が利用不可 ○ リスクの受容 ○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

5. **[Submit]** をクリックします。
   グループは [レビュー中] とマークされます。[再オープン **(Reopen)]** 関連リンクが表示されます。再オープンの日付と理由は、[ステータス変更承認] タブの作業メモに表示されます。

保留された脆弱性一致アイテムの延長の要求

保留された脆弱性一致アイテムがその保留された期限に達する前に、この脆弱性一致アイテムの延長を要求します。修復オーナーは、この要求を行うために保留期日まで待つ必要がなくなりました。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

このタスクについて
脆弱性対応 ワークスペースから延長を要求することもできます。詳細については、「脆弱性マネージャーのワークスペースでの保留された脆弱性一致アイテムの延長の要求」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム.
2. 保留されている脆弱性一致アイテムを開きます。
3. [拡張を要求] を選択します。

   注:
   [拡張を要求] ボタンは、脆弱性一致アイテムのステータスが [保留] の場合にのみ表示されます。

4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
拡張期限	保留された脆弱性一致アイテムを修復のために延長する必要がある期限を選択します。
理由	問題を保留する理由を入力します。 次の選択肢があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	○ メンテナンス期間待ち ○ 修正が利用不可 ○ リスクの受容 ○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

5. [要求承認] を選択します。
   要求が送信され、承認者によって後続のアクションが実行されると、メールがトリガーされます。

   注:
   - 要求は 2 段階の承認を経過します。
   - 保留された例外ルールが再度延長されると、バックエンドで延長保留カウントが増加します。

6. 要求が承認されると、[期限]、[理由]、および [保留メモ] が更新されます。

脆弱性対応 脆弱性一致アイテムのリフレッシュ

[ステータスを更新 **(Update status)]** 関連リンクを使用して、脆弱性一致アイテムを検査し、修復タスクに属する追加の脆弱性一致アイテムがあるかどうかを確認します。スケジュール済みジョブ以外で更新が必要な場合に使用します。

始める前に

必要なロール：sn_vul.vulnerability_write、sn_vul.vulnerability_admin、または sn_vul.admin (非推奨)
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

このタスクについて

[ステータスを更新 **(Update status)]** 関連リンクは、[オープン] または [調査中] 状況の修復タスクフォームでのみ、フィルターグループを使用するか、またはフィルタータイプを条件として編集できます。この検査は、[脆弱性一致アイテムの自動リフレッシュ **(Automatically refresh vulnerable items)]** チェックボックスのステータスに関係なく実行されます。

脆弱性対応の v22.0 以降では、Vulnerability Manager ワークスペース および IT 修復ワークスペース の修復タスクのレコードビューで [ステータスを更新 **(Update Status)]** ボタンを使用できます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 修復タスク.
2. [オープン] または [調査中] 状況のレコードを開きます。
3. [ステータスを更新 **(Update status)]** リンクをクリックします。
   新しい脆弱性一致アイテムが [脆弱性一致アイテム] タブに表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

サードパーティソフトウェアのセキュリティ問題の特定とエスカレーション

サードパーティのエントリーから返されたソフトウェアの脆弱性を表示して、修正を決定できます。この情報を使用して、脆弱なソフトウェアのエントリーを Software 資産管理 検出モデルと照合します。

始める前に
必要なロール：sn_vul.vulnerability_write

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性 > ライブラリー > サードパーティ.
   ダウンロードされた脆弱なソフトウェアのリストが表示されます。
2. ソフトウェアレコードをクリックして脆弱性情報を表示します。
3. 脆弱性を特定するための詳細情報を取得するには、次の関連リストをクリックします。
   脆弱性が特定され、脆弱性一致アイテムが作成された場合は、必要に応じて 修復タスクの解決 を実行できます。

NVD を使用したセキュリティ問題の特定とエスカレーション

共通脆弱性識別子 (CVE-ID) レコードは、脆弱性情報データベース (NVD) からダウンロードされると、ソフトウェア資産検出モデルによって識別された、会社のネットワーク内のソフトウェアと比較されます。CVE-ID がネットワーク内の脆弱なソフトウェアまたは構成アイテムと一致すると、脆弱性一致アイテムが作成されます。CVE-ID レコードの情報を使用して、脆弱性一致アイテムを修正のためにエスカレーションするかどうかを決定します。

始める前に
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > ライブラリー > **NVD**.
   NVD からダウンロードされた CVE-ID のリストが表示されます。NVD からの更新は、オンデマンドで実行することも、次の場所にある NIST National Vulnerability Database Integration レコードからスケジュールされた実行で実行することもできます。 **All** (すべて) > アドミニストレーション > 統合.
2. CVE レコードをクリックすると、以下の情報が表示されます。
   - CVE-ID のサマリー。
   - 共通脆弱性タイプ一覧 (CWE) エントリーへの参照 (該当する場合)。
   - 共通の脆弱性採点システム (CVSS) の CVE-ID の脆弱性スコア。CVSS の詳細については、「脆弱性情報データベース Web サイト」を参照してください。
3. 脆弱性の詳細については、関連リストをクリックしてください。

   脆弱性参照

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

指定された脆弱性とそれを参照する際の名前、説明、および URL。

エクスプロイト

詳細。

弱点

CWE 脆弱性のリスト。

4. 脆弱性を特定するための詳細情報を取得するには、次の関連リストをクリックします。
   脆弱性が特定され、脆弱性一致アイテムが作成された場合は、必要に応じて 修復タスクの解決 を実行できます。

CSW を使用したセキュリティ問題の特定とエスカレーション

脆弱性情報データベース (NVD) の共通脆弱性タイプ一覧 (CWE) レコードのライブラリを表示して、共通脆弱性識別子 (CVE) レコードとの関連性を理解します。この情報を使用して、脆弱なソフトウェアのエントリーを Software 資産管理 検出モデルと照合します。

始める前に

必要なロール：sn_vul.vulnerability_write

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性 > ライブラリー > **CWE**.
   ダウンロードされた脆弱なソフトウェアのリストが表示されます。
2. CWE ソフトウェアレコードをクリックして脆弱性情報を表示します。
3. 脆弱性を特定するための詳細情報を取得するには、次の関連リストをクリックします。
   脆弱性が特定され、脆弱性一致アイテムが作成された場合は、必要に応じて 修復タスクの解決 を実行できます。

脆弱性対応 脆弱性一致アイテムの修復ターゲットステータスの表示

修復ターゲットルールで定義されているように、脆弱性一致アイテムが修復ターゲット日に迫っている (またはその日を過ぎている) と、脆弱性一致アイテムレコードはステータスとともに更新されます。この情報は、アナリストが今後の修復アクティビティを積極的に監視するのに役立ちます。

始める前に

必要なロール：

- sn_vul.vulnerability_admin
- sn_vul.read_remediation_target_rules [読み取り専用]

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
[修復ターゲットを評価 **(Evaluate remediation targets)]** というスケジュール済みジョブ は、現在の日付を関連する修復ターゲットルールで指定された脆弱性一致アイテムの修復日と比較するために、 1 日に 1 回実行されます。現在の日付が修復期限切れまでの日数内にある場合、修復ステータスが脆弱性一致アイテムレコードに追加されます。

修復ターゲットルールの詳細については、「脆弱性対応 の修復ターゲットルール」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性 > 脆弱性一致アイテム.
2. 確認する脆弱性一致アイテムをクリックします。
   脆弱性一致アイテムの修正日が修復ターゲットルールで設定された条件の範囲内にある場合は、[修復ターゲットステータス] タブが表示されます。
3. [修復ターゲットステータス] タブをクリックします。
4. 修復ターゲットステータスレコードをクリックして確認します。

> **注:**
> [ターゲット間近]、[実行中]、および [過去のターゲット] である脆弱性一致アイテムの数を表示するには、「デフォルトの 脆弱性対応 ダッシュボードを使用する」を参照してください。

関連情報

脆弱性対応 修復ターゲットルールの作成または編集

一致しない **CI** の操作

脆弱性マネージャーおよびアナリストは、一致しない構成アイテム (CI) の表示と再分類、一致しない検出されたアイテムの調整、選択した検出されたアイテムへの CI ルックアップルールの再適用、既存の CI の重複排除を行うことができます。

一致しない構成アイテムの表示と再分類

構成管理データベース (CMDB) にない構成アイテム (CI) は、検出されたアイテムの表示可能なリストに配置されます。このリストは、一致しない CI を再分類する便利な方法です。

始める前に
必要なロール：
sn_vul.read (一致しない CI を表示するための最低ロール)
および

itil または asset (再分類)

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

このタスクについて
脆弱性アナリストは、一致しない CI を表示できます。

itil または asset ロールのいずれかがある場合、再分類アクションは *sn_sec_cmn_unmatched_ci* クラスの CI に対してのみ使用できます。CI が再分類されると、UI を使用して再分類することはできません。CI フォームまたは CI リストビューから、クラス値を変更することで再分類できます。詳細については、「Reclassify a CI 」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > **CMDB** > 検出済みアイテム.
2. 確認するには、各アイテムをクリックします。
3. [検出されたアイテム] フォームフィールドの情報を修正するには、このページで編集し、[保存] を右クリックします。
   これらのフィールドに追加されたデータや残されているデータは、再分類時に結果の [構成アイテム] に転送されます。
4. すべて正しい場合は、[再分類] をクリックします。
5. 選択リストから [クラス名] を選択し、[送信] をクリックします。
   [検出されたアイテムクラス **(Discovered Item Class)]** が更新され、[ステータス] フィールドが [再分類] に変更され、すべてのデータが CMDB に格納されます。

一致しない検出されたアイテムを調整

スケジュール済みジョブを作成して、一致しない検出されたアイテムを調整します。

始める前に
必要なロール：admin

このタスクについて
脆弱性一致アイテム (VI) は、脆弱性と構成アイテム (CI) で構成されています。VI を作成する際、作成時に追加される CI が古くなっていることがあります。CMDB 内の情報が変更された場合、一致しない CI 情報は調整されません。調整するには、CMDB が最新の構成アイテム (CI) で更新されたときに、一致しないステータスのアイテムに CI ルックアップルールを適用します。

スケジュール済みジョブをオンデマンドで実行し、一致しないステータスの検出されたアイテムに CI 一致ルールを再適用できます。ルックアップルールを再適用した後に CI が変更された場合、検出されたアイテムは新しい CI で更新されます。影響を受けた検出と脆弱性一致アイテムも更新されます。詳細については、「検出されたアイテムの CI 変更」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > **Security Operations >**一致しない検出済みアイテムを調整.
2. [バックグラウンドジョブ] ページで、[調整ジョブを作成] をクリックします。
3. フォームのフィールドに入力します。

> **注:**
> [パラメーター] フィールドのみを編集できます。

[バックグラウンドジョブ] フォーム

フィールド	説明
数値	一意のジョブ番号。
作成者	ジョブを作成したユーザー。
パラメーター	一致しない検出されたアイテムを調整するパラメーター：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ limit：調整される検出されたアイテムの最大数。値を入力しない場合、検出された 10,000 アイテムが調整されます。 ○ firstDiscovereditem：調整が必要な最初のディスカバリーアイテム。値を入力しない場合、調整プロセスは最初に検出されたアイテムから開始されます。
状態	バックグラウンドジョブの現在のステータス。
ステータスの説明	バックグラウンドジョブの現在のステータスの説明。
ジョブタイプ	ジョブのタイプ。値は、[一致しない検出されたアイテムを調整] です。
開始時刻	ジョブの開始時刻。
終了時刻	ジョブの完了時刻。
ジョブ期間	ジョブムの完了に要した合計時間。
サブステート	選択したステータスのサブステート。
メモ	処理されたレコードの数。

4. **[Submit]** をクリックします。

注:

- ジョブの実行を停止するには、[キャンセル] をクリックします。
- ホストまたは脆弱性一致アイテムのインポート時に、一致しない CI を調整したり、CI ルックアップルールを再適用したりすることはできません。

選択した検出されたアイテムへの **CI** ルックアップルールの再適用

検出されたアイテムのリストビューの選択アクションから、選択した検出されたアイテムに構成アイテム (CI) ルックアップルールを再適用します。ルールを再適用した後に CI が変更された場合、検出されたアイテムは新しい CI と影響を受けた検出で更新されます。脆弱性一致アイテムも更新されます。

始める前に
必要なロール：admin

このタスクについて
詳細については、「検出されたアイテムの CI 変更」を参照してください。

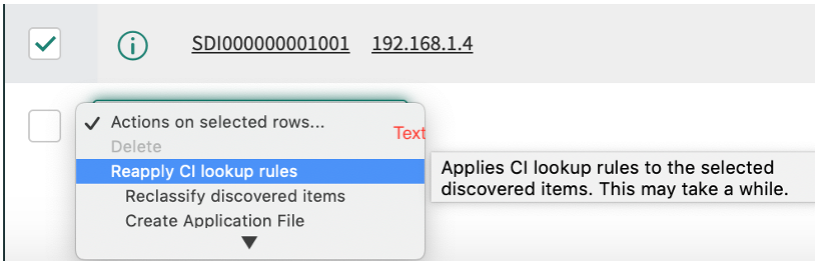
CI 照合と CMDB のコンセプト、検出されたアイテムのルックアップ、ルールベースの識別の詳細情報、および CI 照合の仕組みに関するその他の詳細情報については、HI ナレッジベースの記事「CI matching in Vulnerability Response (脆弱性対応における CI 照合) [KB0998706]」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > **CMDB** > 検出済みアイテム.
2. 必要な検出されたアイテムを選択し、[選択した行でアクションを実行] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳



3. リストから、**[CI** ルックアップルールを再適用] を選択します。

   注:

   脆弱性対応 v24.0.6 以降では、システムプロパティ*sn_sec_cmn.skipItemsWithCIDecommissioned*を有効にすることで、サブステートが「CI 廃止」の検出済みアイテムへの CI ルックアップルールの再適用をスキップできます。

   これらの検出されたアイテムにルールが再適用されます。

4. メッセージの [ステータスを表示] をクリックします。

   ステータスがバックグラウンドジョブフォームに表示されます。

   注:
   [メモ] フィールドで、[例外のため、ディスカバリーアイテムを処理できませんでした (Discovered items could not be process due to exception)] 属性の値が 0 以外の場合は、CI ルックアップルールの再適用中にエラーまたは例外が発生したことを示します。詳細については、システムログを確認してください。

CI ルックアップルールの再適用の機能強化

OS や NetBIOS などの選択した検出されたアイテムに構成アイテム (CI) ルックアップルールを再適用します。

始める前に
必要なロール：admin

このタスクについて

- ソースデータに存在する os と netbios の値は、検出されたアイテムのこれらのフィールドに入力されるときに、構成アイテムの前に入力されます。
- ソースデータの OS と NETBIOS の値が空の場合、検出されたアイテムテーブルのこれらのフィールドに値が入力される際に、値は構成アイテムから取得されます。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > **CMDB** > 検出済みアイテム.
2. 必要な検出されたアイテムを選択し、[選択した行でアクションを実行] を選択します。
3. リストから、**[CI** ルックアップルールを再適用] を選択します。

   これらの検出されたアイテムにルールが再適用されます。

脆弱性対応 **CI** ルックアップルールの実行後にレコードが重複または孤立しないようにするための手順

CMDB 内の構成アイテム (CI) の一致によって、重複レコードまたは孤立レコードが発生しないようにするための手順を実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性データのインポートはインスタンスに負荷をかける可能性があり、慎重にルールをビルドしないと、リソースのパフォーマンス問題が発生する可能性があります。CMDB 内で反復して照合を実行するために使用されるロジックでは、処理時間が長くなる可能性があります。ルール内の処理スクリプトを徹底的にテストしてデバッグすることで、プロセスの後半で発生する可能性のある問題を軽減できます。

重複レコードまたは孤立レコードの防止

- テストする CI ルックアップルールに固有の、小さいデータのサブセットを使用します。
  - テスト対象を除いて、すべての [CI ルックアップルール] を [非アクティブ] に設定します。
  - インポートされた CI を分析し、想定される動作を観測していること、照合が適切に行われていることを確認します。
- 一致した CI のレビュー
  - 一致した CI と一致しなかった CI の数を確認します。比率が許容範囲であることを確認します。最初のページを見るだけで済ませないでください。挿入された最初の 1 つである可能性があります。
  - 一部の CI を手動で検索します。
  - 命名またはフィールドの問題 (特定のドメインの検索など) がないかどうかを確認します。

    適切と思われる場合は、一致ルールを追加します。
- 一致しなかった CI のレビュー
  - [一致しない CI] テーブルに移動します。
  - 構成アイテムクラス別にグループ化します。
  - 正しくないと思われるクラス (証明書、ネットワークカード、イメージ) をレビューします。
    - なぜ正しい CI と一致しなかったのでしょうか？
    - クラスを除外する必要がありますか？
    - クラスを関連クラスに昇格させる必要がありますか？
- [廃止] などの CI 状況を確認します。
- テストデータの削除
  - CI の照合で正しい動作または予想される動作を観察し始めたら、最初からやり直します。
  - テストに使用したデータを削除して最初からやり直します (「テーブルからのデータの削除」セクションを参照)。
    - 検出されたアイテム
    - 脆弱性一致アイテム
    - 修復タスク
  - すべての CI 一致ルールを手動で再実行します。

CI ルックアップルールと Qualys の詳細については、KB0750656 の記事を参照してください。

CI ルックアップルールと Rapid7 の詳細については、「KB0818096」を参照してください。

テーブルからのデータの削除

データをインポートしたときに、問題があることに気付くことがあります。開発環境やパフォーマンス環境で何か問題が発生した場合、より良い環境から再クローンできることもありますが、いつもできるとは限りません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

> **注:**
> これらのアクションを実行するには、ServiceNow の専門知識が必要です。

テーブルからデータを削除するには、次の 4 つのオプションがあります。

- [テーブル構成] で [すべてのレコードを削除] を使用する。
- [自動フラッシュ] (sys_auto_flush.list) に移動し、新しい [自動フラッシュ] レコードを作成して、[テーブルクリーナー] を設定します。
- バックグラウンドスクリプトを使用して gs.truncateTable を切り捨てます。

  `truncateTable` を使用するには、バックグラウンドスクリプトの [ロールバック用に記録] チェックボックスをオフにする必要があります。オフにしないと、テーブルと関連するカスケードテーブルのコピーが作成され、時間がかかりすぎて多くの場合は失敗します。

  > **注:**
  > 本番環境では `truncateTable` を使用しないでください。本番環境や共有環境で大規模な削除を実行する場合は、事前にサポート担当者にご相談ください。

既存の構成アイテムの重複排除

重複排除タスクを使用して構成アイテム (CI) を更新するたびに、その CI に関連する検出済みアイテム (DI) も更新されます。脆弱性一致アイテム (VI) および検出も CI とともに更新されます。

詳細については、「検出されたアイテムの CI 変更」を参照してください。

関連情報

重複排除タスクの修正

修復タスクの解決

脆弱性対応 に固有の柔軟性により、セキュリティ組織に適した方法で脆弱性を修正できます。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

このタスクについて
変更の要求が解決されたことが通知されたら、修復タスクのステータスを [解決済み] にして、次のスキャンを待ちます。再スキャンは、セットアップアシスタントで設定されているサードパーティのスケジュール済みインポートによって自動的にトリガーされます。

> **注:**
>
> ステータスの同期がアクティブ化されている場合は、修復タスク (VUL) に関連付けられた変更要求が実装され、[レビュー] ステータスになった後、修復タスクは自動的に [解決済み] ステータスに移行されます。「脆弱性対応 の変更管理」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 修復タスク > 自分にアサイン済み.
2. [オープン] ステータスのレコードをクリックします。

   [オープン] ステータスは、レコードがまだ処理されていないことを示します。フォームには以下が表示されます。

   - 修復タスク情報
   - グループ構成の詳細
   - メモ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 関連する脆弱性一致アイテム
- SLA タスク
- 変更要求

3. グループの分析を実行します。
4. レコードに対する処理を開始する準備ができたら、次のいずれかのオプションを選択します。

オプション	説明
脆弱性一致アイテムが IT 環境にリスクをもたらす場合は、CHG レコードを作成し、変更管理 チームに問題をエスカレートします。	グループを適切なグループまたは個人にアサインし、[変更を作成] をクリックします。
脆弱性一致アイテムが組織に潜在的なセキュリティリスクをもたらす場合は、セキュリティインシデントレコードを作成し、問題を セキュリティインシデントレスポンス チームにエスカレートします。	[セキュリティインシデントを作成] をクリックします。 このボタンは、セキュリティインシデントレスポンス がアクティブ化されている場合にのみ表示されます。ビジネスインパクトの計算が適用され、インシデントがアサインされ、セキュリティインシデントが作成されます。

変更要求を作成すると、適切なレコードが [脆弱性グループ] フォームの [変更要求] 関連リストに表示されます。

5. 問題のリスクが低く、保留できると判断した場合は、[例外の要求] をクリックします。
修復タスクを保留する方法の詳細については、「修復タスクの保留」を参照してください。
6. 問題をそれ以上分析することなくすぐにクローズできると判断した場合は、[クローズ] をクリックします。
修復タスクをクローズする方法の詳細については、「修復タスクをクローズ」を参照してください。脆弱性対応の v23.0 以降では、修復タスクの [クローズ] ボタンが削除されました。

サードパーティ統合のスケジュール済みジョブは、設定された間隔でレコードを自動的に更新してスキャンします。脆弱性一致アイテムは、次のスケジュールされた日時にスキャンされます。または、[脆弱性のスキャン **(Scan for Vulnerabilities)]** 関連リンクを使用して、脆弱性スキャンを手動で開始することもできます。

スキャンで構成アイテムの脆弱性が再度検出され、[修正済み] とマークされていない場合、脆弱性一致アイテムは [調査中] ステータスに戻ります。変更要求を再オープンするには、IT 運用にお問い合わせください。

スキャンで脆弱性が検出されず、脆弱性一致アイテムが [修正済み] とマークされた場合、脆弱性一致アイテムは [クローズ済み - 修正済み (Closed - Fixed)] ステータスに移行し、インポート中にクローズされます。

タスク内のすべての脆弱性一致アイテムが [クローズ済み - 修正済み (Closed - Fixed)] ステータスの場合にのみ、修復タスクは自動的にクローズされます。[修正済み] ではない [クローズ済み] ステータスの脆弱性一致アイテムを対象にした修復タスクは、手動でクローズする必要があります。

修復タスクの保留

修復タスク (VUL) に関連する問題が低優先度で、それ以上分析することなくすぐに保留できると判断した場合は、[例外の要求 **(Request Exception)]** 機能を使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

このタスクについて
脆弱性対応 ワークスペースの修復タスクレコードから修復タスクを保留できます。要求を申請すると、その要求が承認のために送信されます。「IT 修復ワークスペースで例外を要求する」を参照してください。

スケジュール済みジョブで、再オープン日に達した保留中の修復タスクが毎日チェックされます。タスクの保留が期限切れになる日に、タスクが再オープンされます。

注:
状況同期を有効にした状態で、それぞれのレコードのライフサイクルの状況を介して変更要求と修復タスクを手動で移行することはできますが、CHG の状況が変化したことをシステムが登録したり、各自が CHG を追加したり、修復タスクから CHG を削除したりすると、状況同期によって手動による介入が無効になる可能性があります。ただし、変更要求の状況により、修復タスクの状況が [クローズ済み] または [保留] 状況から自動的に移行されることはありません。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 修復タスク.
2. レコードを開きます。
3. [例外の要求] をクリックします。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
期限	保留ステータスが期限切れになり、修復タスクが再アクティブ化される日付を選択します。 レコードが送信された後、メール通知が定義されている場合、有効期限が 1 週間以内になると 脆弱性対応 グループのメンバーにメールが送信されます。保留日が期限切れになると、修復タスクは [オープン] に戻され、2 回目のメール通知が送信されます。
理由	問題を保留する理由を入力します。 次の選択肢があります。 ○ メンテナンス期間待ち ○ 誤検出 ○ 修正が利用不可 ○ リスクの受容 ○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. **[Submit]** をクリックします。
   グループは [レビュー中] とマークされます。[再オープン **(Reopen)]** 関連リンクが表示されます。
   再オープンの日付と理由は、[ステータス変更承認] タブの作業メモに表示されます。

保留された修復タスクの延長の要求

保留された例外ルールがその保留された期限に達する前に、保留された修復タスク (VUL) の延長を要求します。修復オーナーは、この要求を行うために保留期日まで待つ必要がなくなりました。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

このタスクについて
脆弱性対応 ワークスペースから延長を要求することもできます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 修復タスク.
2. 保留された修復タスクを開きます。
3. [拡張を要求] を選択します。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
拡張期限	保留ステータスが期限切れになり、修復タスクが再アクティブ化される日付を選択します。
理由	問題を保留する理由を入力します。 次の選択肢があります。 ○ メンテナンス期間待ち ○ 修正が利用不可 ○ リスクの受容 ○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

5. [要求承認] を選択します。
   要求が承認されると、修復タスクに対する変更が、修復タスクの一部である脆弱性一致アイテムにもロールダウンされます。ただし、脆弱性一致アイテムが保留ステータスであり、現在の期限日が更新期限日より前である必要があります。要求が送信され、承認者によって後続のアクションが実行されると、メールがトリガーされます。

注:

- 要求は 2 段階の承認を経過します。
- [拡張を要求] ボタンは、例外ルールの一部として作成された修復タスクでは使用できません。
- 保留された修復タスクが再度延長されると、バックエンドで延長保留カウントが増加します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

修復タスクをクローズ

修復タスクに関連する問題をそれ以上分析することなくすぐにクローズできると判断した場合は、[クローズ] 機能を使用できます。脆弱性対応の v23.0 以降では、修復タスクの [閉じる] ボタンが削除され、修復タスクのクローズがスキャナーによって行われるようになりました。

始める前に

必要なロール：admin

このタスクについて

脆弱性対応 ワークスペースでは、修復タスクは、以前のバージョンの 脆弱性対応 での修復タスクと同じ状況に移行します。ある修復タスクのすべての脆弱性一致アイテム (VIT) がクローズされると、その修復タスクは [非アクティブ] ステータスに移行します。

重要:
状況同期を有効にした状態で、それぞれのレコードのライフサイクルの状況を介して変更要求と修復タスクを手動で移行することはできますが、CHG の状況が変化したことをシステムが登録したり、各自が CHG を追加したり、修復タスクから CHG を削除したりすると、状況同期によって手動による介入が無効になる可能性があります。ただし、変更要求の状況により、修復タスクのステータスが [クローズ済み] または [保留] 状況から自動的に移行されることはありません。

手順

1. レビューを要求するレコードを開きます。
2. [クローズ/保留] ボタンを選択します。
3. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
状態	ステータスを選択します。 選択肢は次のとおりです。 ○ 保留 ○ クローズ済み
期限	[保留] ステータスのポップアップでのみ使用できます。 [保留] ステータスが期限切れになり、修復タスクが再アクティブ化される日付を選択します。 レコードが送信された後、メール通知が定義されている場合、有効期限が 1 週間以内になると 脆弱性対応 グループのメンバーにメールが送信されます。保留日が期限切れになると、脆弱性一致アイテムは [オープン] に戻され、2 回目のメール通知が送信されます。
理由	問題をクローズする理由を入力します。
追加情報	その他の関連情報を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

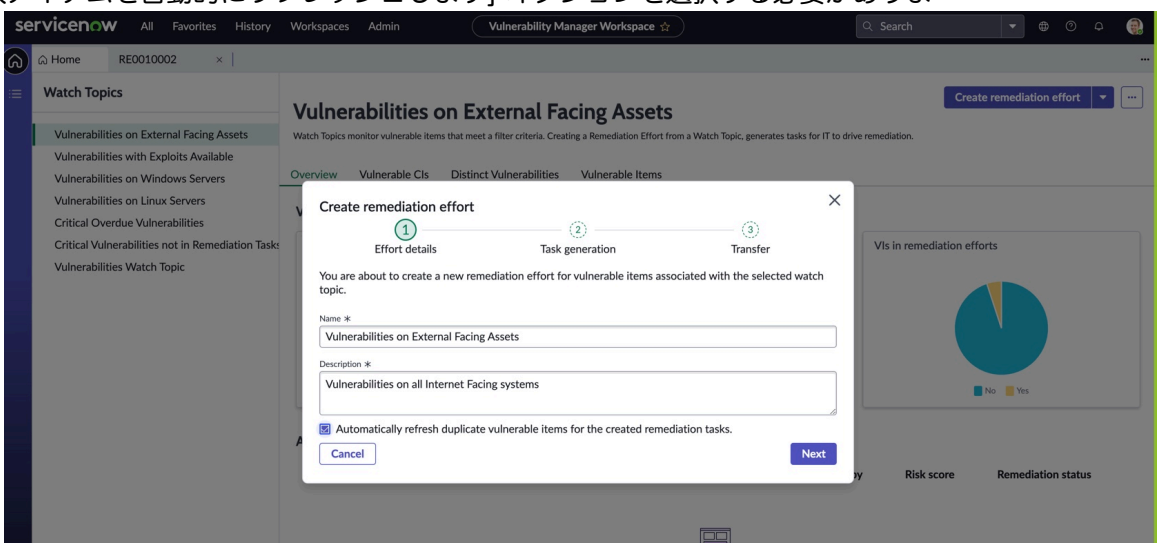
4. [送信] を選択します。
   修復タスクは [クローズ済み] とマークされます。

複数のスキャナーから重複する脆弱性一致アイテムを識別する

同じ資産で複数のスキャナーを使用して脆弱性を検出すると、複数の脆弱性一致アイテム (VI) が作成される可能性があります。これらの重複する VI を識別して、重複する脆弱性が修復オーナーにアサインされないようにすることができます。

この解決は、同じ一般的な脆弱性とエクスポージャー (CVE) など、同じ脆弱性が検出された場合にのみ可能です。脆弱性の組み合わせは、使用されているスキャナーによって異なります。たとえば、Qualys と Tenable には独自の脆弱性タイプ、つまりサードパーティエントリー (TPE) があり、Microsoft Defender for Endpoint などの他のスキャナーは CVE に基づいて脆弱性を検出します。

v 17.1 以降では、修復作業を作成しているときに、作成された修復タスクの重複する脆弱性一致アイテムを自動的にリフレッシュできます。重複する脆弱性一致アイテムを自動的にリフレッシュするには、 [作成された修復タスクの重複脆弱性一致アイテムを自動的にリフレッシュします] オプションを選択する必要があります。



[重複 **VI** を表示]：システム内の複数のスキャナーによって報告された重複する脆弱性一致アイテムを識別します。重複する VI を解決済みとしてマークできます。詳細については、「重複する脆弱性を自動的に解決する」を参照してください。重複するエントリーは、脆弱性の組み合わせが CVE を使用して作成された場合にのみ表示されます。詳細については、「脆弱性対応修復タスクと脆弱性一致アイテム状況」を参照してください。

重複の可能性があるのは、次の脆弱性の組み合わせの場合です。

スキャナーの組み合わせ	脆弱性タイプ
スキャナー 1 とスキャナー 2	CVE
スキャナー 1 とスキャナー 2	CVE と TPE

重複する脆弱性を自動的に解決する

脆弱性対応 (VR) v17.1 以降では、資産における重複する脆弱性を自動的に解決できます。

資産が複数のスキャナーでスキャンされると、異なるスキャナーによって同じ脆弱性が重複として識別される可能性があります。たとえば、Qualys と Microsoft のスキャナーが同じ脆弱性を識別した場合、重複する脆弱性を自動的に解決するように選択できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[サンプルシナリオ]

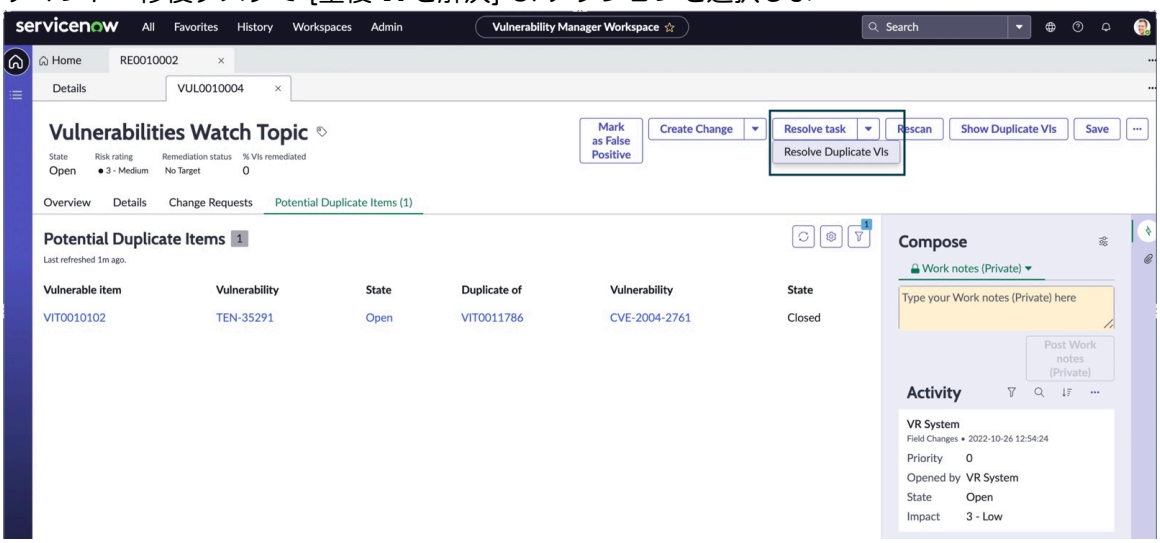
VR は、Microsoft Defender for Endpoint スキャナーから脆弱性 1 のレコード VI1 を作成します。同じ脆弱性に対して、Qualys スキャナーから 2 番目のレコード VI2 が作成されます。修復チームは、VI1 および VI2 レコードを解決できる可能性があるパッチを適用します。Qualys のスキャンスケジュールを 1 日以上設定すると、その時点で修復済みの脆弱性情報を Microsoft Defender が提供し、VR は VI1 レコードを [クローズ済み/修復済み] としてクローズします。

このシナリオでは、VI2 レコードはまだ [オープン] ステータスであり、VR は Qualys のスキャン結果を待ちます。この場合、パッチが適用され、VI がもう一方のスキャナーによって修復済みとして確認されても、2 番目のスキャナーの VI レコードは [オープン] ステータスのままになります。

この状況に対処するために、最初のスキャナーによって脆弱性がクローズされているという条件に基づいて、重複する脆弱性レコードを解決することを検討してください。

次の方法で脆弱性を解決します。

- オンデマンド：修復タスクで [重複 **VI** を解決] UI アクションを選択します。



- 自動：システムプロパティ `sn_vul.auto_resolve_duplicate_bit` を有効にして、重複する脆弱性一致アイテムを自動的に解決します。日次スケジュール済みジョブ [修復タスクで重複 VIT を自動的にリフレッシュして、解決する (Refresh and resolve duplicate VITs on remediation task)] は、重複アイテムを自動的にリフレッシュします。

重複する VI は解決済みとしてマークされます。

> **注:**
> スキャナーが [未修復 **(Not Fixed)**] と識別した場合、解決済みの脆弱性一致アイテムレコードが再オープンされます。

分類グループの作成と編集

このグループの基礎となるルールが条件に基づいてテーブルレコードを分類できるように、グループを作成します。ルールを使用して対応するテーブルの任意のフィールドを選択できます。

始める前に
必要なロール：sn_vul.manage_classification_rule

手順

1. システムプロパティテーブルに移動します。
2. *`sn_sec_cmn.classificationTables`* システムプロパティで、分類グループを作成するテーブルの名前を追加します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. グループに定義するテーブルのビジネスルールに次のコードスニペットを追加して、新しいビジネスルールを作成します。
```
var classificationCalc = new
sn_vul.VulnerabilityCalculator(current,true,false,'sn_vul_classification_group','sn_vul_classification_rule');
classificationCalc.calculate();
```

> **注:**
> ディスカバリーアイテムおよび脆弱性エントリテーブルの取り込み時に分類を実行するためのビジネスルールが提供されます。他のテーブルの場合、取り込み時に分類ルールを使用するには、ビジネスルールを追加する必要があります。

4. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 分類ルール.
5. 分類グループのコンテキストメニューで、[新規] をクリックします。
6. フォームのフィールドに入力します。

脆弱性の分類グループフォーム

フィールド	説明
名前	新しい分類グループの名前
有効	グループをアクティブ化するためのオプション
説明	新しい分類グループの説明
テーブル	ルールが実行されるテーブル。 **注:** 脆弱性対応ベースシステムには、検出されたアイテムと脆弱性を分類する分類グループが含まれています。

自動翻訳

分類ルールの作成と編集

受信した脆弱性を修正のために適切なチームに自動的に分類するルールを作成します。

始める前に
必要なロール：sn_vul.manage_classification_rule

このタスクについて
分類ルールを作成すると、脆弱性がプラットフォームまたはアプリケーションに属するものとして分類されます。こうしたルールを設定して、脆弱性エントリーの特定のフィールドの値を置き換えることができます。
このようなルールを使用して、計算をアップストリームのサードパーティ脆弱性エントリーテーブルに移動し、コンテンツを再利用できるようにします。

手順
1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 分類ルール.
2. 分類グループを表示するには、そのグループをクリックします。
3. [分類ルール] コンテキストメニューで、[新規] をクリックします。
4. フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[脆弱性の分類ルール] フォーム

フィールド	説明
名前	新しい分類ルールの名前。
有効	ルールをアクティブ化するためのオプション
説明	新しい分類ルールの説明。
実行順序	ルールを実行する順番。
詳細表示	タブセクションに追加のフィールドを表示するオプション。
この条件を満たしている場合	
条件タイプ	ルールの条件のタイプ。選択肢は次のとおりです。 ○ フィルター：ルールを使用するかどうかを決めるための基本的なフィルター条件。 ○ フィルターグループ：一緒に使用される複数の条件のセット。ルールは、フィルターグループで定義された条件に基づいて評価されます。 ○ スクリプト：このルールを適用するタイミングを決定するために使用されるスクリプト化された条件。 このフィールドは、[詳細表示] オプションが選択されている場合にのみ表示されます。
条件	ルールの条件。必要な脆弱性エントリー列で選択された列に基づいて条件を定義します。複数の条件を追加してルールを絞り込むことができます。このフィールドは、[条件タイプ] フィールドで [フィルター] が選択されている場合にのみ表示されます。 **注:** 複数の条件またはテンプレートを定義する場合は、親テーブルと子テーブルからのみ選択できます。2 つ以上の子テーブルから選択することはできません。
フィルターグループ	フィルターのグループ。グループは、一連の条件が複数個所で繰り返し使用される場合に定義されます。リストアイコン ( ) を使用してルックアップをクリックし、フィルターグループを選択します。詳細については、「Security Operations でのフィルターグループの作成と定義」を参照してください。このフィールドは、[条件タイプ] フィールドで [フィルターグループ] が選択されている場合にのみ表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
スクリプト	このルールを適用するタイミングを決定するために評価されるスクリプト。コードを記述して、応答を true または false に設定できます。このフィールドは、[条件タイプ] フィールドで [スクリプト] が選択されている場合にのみ表示されます。
これらの値を設定	
分類	ルールの分類。オプションを選択するには、電球アイコン ( ) をクリックします。リストには、プラットフォーム用とアプリケーション用のオプションが表示されます。または、リストにない独自の分類を入力することもできます。
分類タイプ	分類のタイプ。このフィールドには、[分類] フィールドで選択した値に基づいて、分類タイプのフィルター済みリストが表示されます。
値のタイプ	このルールを使用してアサインされる値のタイプ。選択肢は次のとおりです。 ○ テンプレート：テンプレートを選択します。必要なテンプレートを使用できます。 ○ スクリプト：既存のスクリプトを選択するか、独自のカスタムスクリプトを記述します。 このフィールドは、[詳細表示] オプションが選択されている場合にのみ表示されます。
テンプレート	[分類] フィールドおよび [分類タイプ] フィールド以外の、ルールのもう 1 つの条件。ルールの評価時に設定するフィールドと値の組み合わせを選択します。このフィールドは、[値タイプ] フィールドで [テンプレート] が選択されている場合にのみ表示されます。
スクリプト値	現在のレコードに値を設定するスクリプト。このフィールドで脆弱性エントリーのフィールドに設定する値を定義します。このフィールドは、[値タイプ] フィールドで [スクリプト] が選択されている場合にのみ表示されます。

5. 新しいルールを作成するには、[送信] をクリックします。

Example:
VR 分類ルールを使用して、脆弱性や検出されたアイテムなどのアップストリームのテーブルにロジックを追加し、それを計算します。出力を複数回再利用できるため、アサインルールなどのルールのパフォーマンスを向上させることができます。たとえば、サードパーティエントリー (TPE) を Java として分類し、その出力をアサインルールで複数回再利用します。アサインルールの例：

```
VI.TPE.Classfication Type
        | IS | Java
```

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

既存の脆弱性へのルールの適用

分類ルールを変更した場合は、すべての脆弱性エントリーに対してすべてのアクティブなルールを再実行します。既存の脆弱性に新しく作成された分類ルールを適用することで、既存の脆弱性を改善することもできます。

始める前に
必要なロール：sn_vul.manage_classification_rule

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性 > アドミニストレーション > 脆弱性分類ルール.
2. ルールを選択するには、ルールの横にあるチェックボックスをオンにします。
3. [変更を適用] をクリックします。
4. [再適用] をクリックします。

分類ルールの非アクティブ化または削除

不要になったまたは関連のない分類ルールを非アクティブ化または削除します。

始める前に
必要なロール：sn_vul.manage_classification_rule

このタスクについて
分類ルールが非アクティブ化または削除された場合、その削除されたルールによって [分類] および [分類タイプ] フィールドに入力されたデータはそれぞれのテーブルに残ります。

このデータをクリアする場合は、[分類] および [分類タイプ] フィールドの値が空のルールを作成し、グループを再適用します。この新しいルールが再適用されると、ルールの条件に基づいて、このルールが適用されるすべてのレコードに変更が反映されます。

脆弱性対応 の v24.0.6 以降では、分類ルールが削除または非アクティブ化されると、検出されたアイテムまたは脆弱性エントリーには適用されなくなり、[分類] フィールドと [**Classification_type**] フィールドのデータはクリアされます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性 > アドミニストレーション > 脆弱性分類ルール.
2. 削除するルールを選択するには、ルールの横にあるチェックボックスをオンにします。
3. ルールを削除するには、次のいずれかを実行します。
   - [選択した行のアクション] リストから、[削除] をクリックします。
   - ルールを選択して、[削除] ボタンをクリックします。
4. [変更を適用] をクリックします。

> **注:**
> このボタンをクリックしないと、ルールはシステムに存在し続けます。ルールによって参照される脆弱性は、引き続きそうしたルールを参照します。

除外ルールを作成する

取り込み中に検出が脆弱性一致アイテム (VIT) に変換されないようにフィルタリングまたは除外するルールを作成します。

始める前に
必要なロール：脆弱性管理者

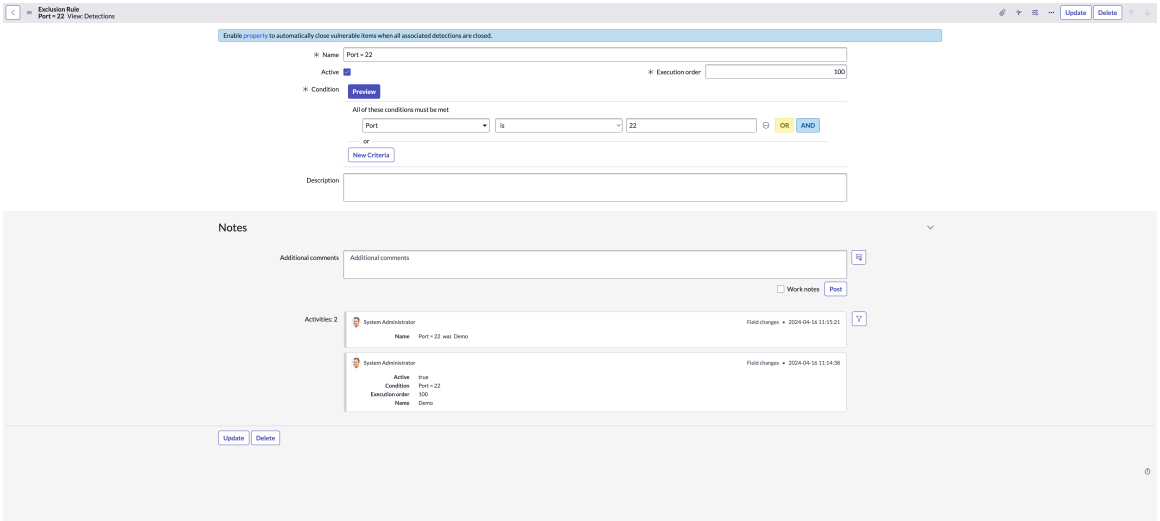
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 除外ルール.
2. [除外ルール] レコードページで、[新規] を選択してルールを作成します。



「関連するすべての検出がクローズされたときに、脆弱性一致アイテムを自動的にクローズするプロパティを有効にする (Enable property to automatically close vulnerable items when all associated detections are closed)」というメッセージが表示されます。このプロパティは、デフォルトでは非アクティブになっています。有効にするには、プロパティリンクを選択し、[値] フィールドに「True」の値を入力します。

3. フォームのフィールドに入力します。

除外ルールフォーム

フィールド	説明
名前	除外ルールの名前。
アクティブ	除外ルールをアクティブ化するためのオプション。
実行順序	各除外ルールの一意の順序。
条件	検出の処理中に定義できる検出のフィルター条件。 **注:** [除外ルール] または [脆弱性一致アイテム] フィールド条件を選択することはできません。
説明	除外ルールの説明。

4. [送信] を選択します。
アクティビティがシステムに記録されます。

注: 除外ルールが作成されると、後続の取り込み以降の検出に対して有効になります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 の 変更管理 タスク

修復タスク (RT) から、変更要求を作成するか、RT を既存の変更要求に関連付けるか、修復タスクを脆弱性一致アイテム (VI) のサブセットを含む新しいタスクに分割します。

CMDB 内のサポートされている構成アイテム (CI) を変更または削除するために何らかの手動制御のプロセスが必要な場合は、修復タスクから直接変更要求を作成および管理します。レコードから直接変更要求を作成して管理すると、脆弱性を迅速に調査して解決できます。

脆弱性対応 アプリケーションでの変更管理の仕組みの概要とシステム要件については、「脆弱性対応 の変更管理」を参照してください。

変更要求を作成する方法、修復タスクを既存の変更要求に関連付ける方法、および修復タスクを分割する方法については、この後のトピックを参照してください。変更要求 (CHG) のステータスフィールドで修復タスクを自動的に解決する仕組みについては、「変更要求と修復タスク間のステータスの同期」を参照してください。

修復タスクからの変更要求の作成

IT 修復オーナーは、グループ内のすべての脆弱性一致アイテムの修復タスク (VUL) から直接、変更要求 (CHG) を作成します。優先ソリューションを含む、事前設定された情報を使用して変更要求を作成し、手動操作が必要な脆弱性の調査を迅速化します。

始める前に

必要なロール：変更要求を作成する場合：itil ロールを持つ任意のユーザー。さらに sn_vul.remediation_owner ロールも、ユーザーに itil ロールがアサインされると自動的にアサインされます。

必要なロール：変更要求の承認の場合：itil、admin、sn_change_write、change_manager ロールを持つユーザー。

このタスクについて

脆弱性対応 ワークスペースから変更要求を作成する方法については、「IT 修復ワークスペースで変更要求を作成する」を参照してください。

クラシック環境から変更要求を作成するには、以下の手順に従います。

修復タスクから、変更要求を直接作成、承認、実装、レビュー、およびクローズすることができます。修復タスクから事前入力された情報を使用して、次の 3 つのタイプの変更要求を作成できます。

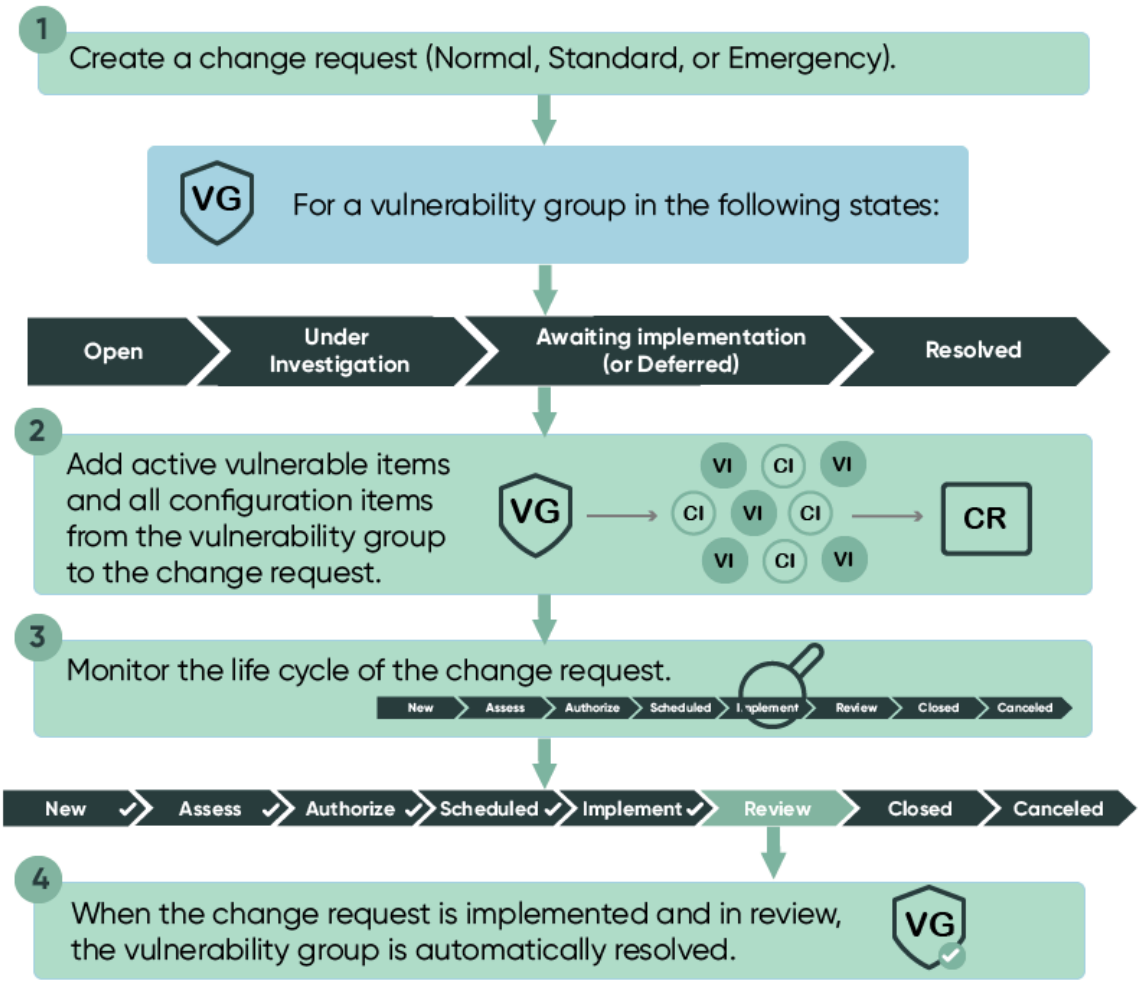
- 標準。事前に承認された、リスクの低い、比較的一般的な変更を指し、指定された手順または作業指示書に従って行います。
- 通常。通常の変更要求は、実装、レビュー、およびクローズする前に 2 レベルの承認が必要な規範的なプロセスに従います。
- 緊急。重大なインシデントを解決するための変更。

次の図は、VUL (修復タスク) から変更要求を作成する基本的なフローを示しています。このフローの詳細な手順は、図に沿って説明します。

修復タスクレコードは、以降のセクションでは VUL と呼びます。脆弱性対応 の以前のバージョンでは、修復タスクは脆弱性グループ (VG) と呼ばれていました。次の画像では、VG は修復タスクまたは VUL レコードを表しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

注:
新しい変更要求の作成に関する重要なポイント：

- [クローズ済み] 以外のステータスの任意の修復タスク (VUL) に対して、新しい変更要求を作成できます。
- 作成するか VUL に関連付ける標準 (事前承認済み) 以外の変更要求の承認者がいることを確認します。これにより、VUL の解決が迅速化されます。ユーザーの追加の詳細については、「脆弱性対応グループへのユーザーの追加」を参照してください。
- 修復タスクを解決する前に、VUL に関連付けられている少なくとも 1 つの CHG のすべてのタスクを完了して、変更要求を実装して [レビュー] ステータスに移行できるようにする必要があります。

手順

1. 既存の修復タスクレコードから完全な変更要求を作成するには、次に移動します: **All** (すべて) > 脆弱性対応 > 修復タスク > 所属グループにアサイン済み.
   自分のアサイン先グループにアサインされている修復タスクレコードのリストが表示されます。
2. オプション: 次のように移動する。 **All** (すべて) > 脆弱性対応 > 修復の概要 修復の概要ダッシュボードを表示し、自分または自分のアサイン先グループにアサインされた VUL を見つけます。
3. または、[番号] 列で修復タスクをクリックしてレコードを開き、詳細を表示します。
   レコードが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. 変更要求を作成する VUL レコードが表示されたら、レコードの右上にある [変更を作成] をクリックします。
   [変更要求の作成] フォームが表示されます。
5. フィールドに入力します。

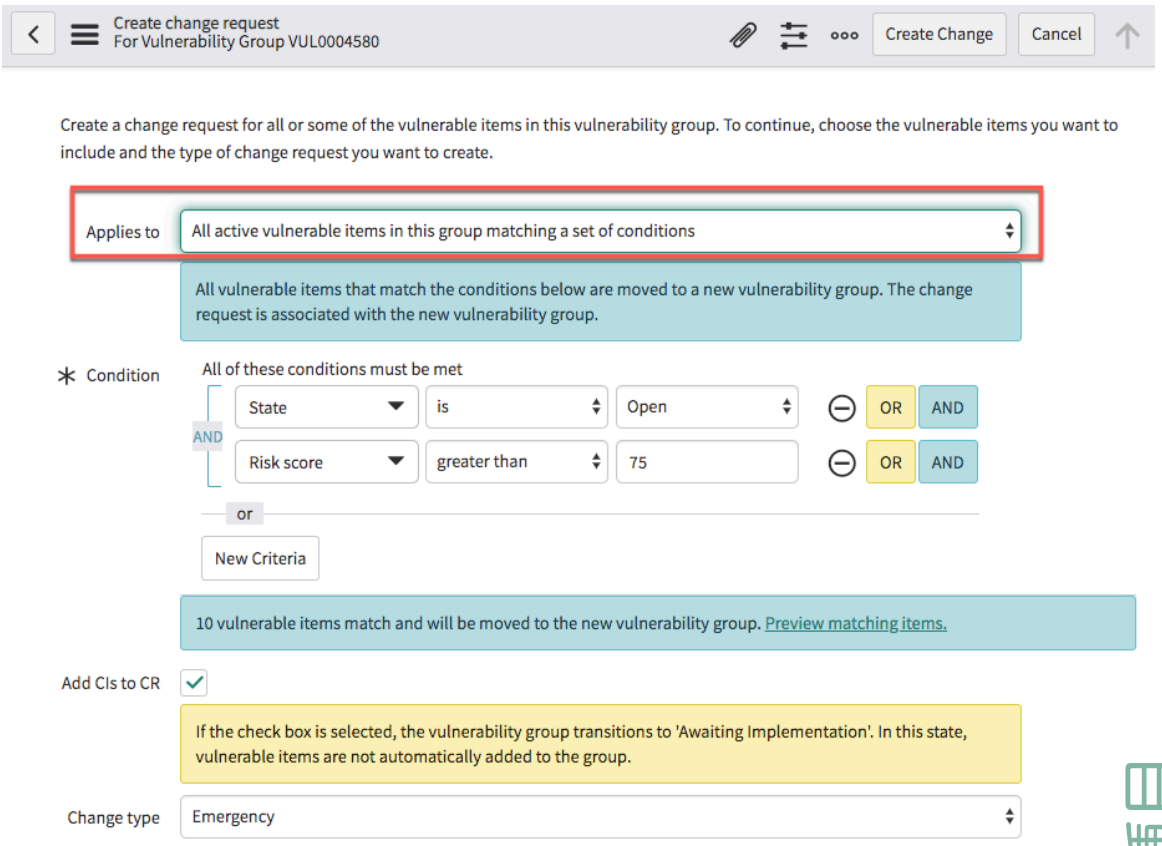
   a. [適用先] フィールドの選択リストから、いずれかを選択して続行します。

オプション	説明
このグループ内のすべてのアクティブな脆弱性一致アイテム	選択すると、ステータスが [クローズ済み] 以外のこの修復タスクからのアクティブな脆弱性一致アイテムすべてが、[変更を作成] のクリック後に変更要求に自動的に追加されます。
一連の条件に一致する、このグループ内のすべての脆弱性一致アイテム (All vulnerable items in this group matching a set of conditions)	選択すると、下の 2 番目の図に示すように条件ビルダーが表示されます。新しい変更要求に必要な脆弱性一致アイテムを特定するためのフィルター基準を入力します。 フィルターの例には、「特定の検索条件に一致する脆弱性一致アイテムのみ」などがあります。 [ステータス] [次の値に等しい] [オープン] かつ [リスクスコア] [次の値を超える] **[75]**。 条件を入力すると、基準 (10) に一致する VI の数を含むメッセージが表示されます。一致するアイテムをプレビューするためのリンク ([一致するアイテムをプレビュー **(Preview matching items)]**) が表示されます。 フィルター条件に一致するアイテムがない場合は、フィルターを調整するように指示するメッセージが条件ビルダーの下に表示されます。 [変更を作成] をクリックすると、この条件フィルターに一致するすべての脆弱性一致アイテムが、新しい修復タスクに移動されます。この変更要求が修復タスクに関連付けられます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

一連の条件に一致する、タスク内の脆弱性一致アイテムに対する変更要求フォームの作成



b. オプション: フォームに表示されている場合は、フィルター基準に一致する VI のリストの [一致するアイテムをプレビュー **(Preview matching items)]** リンクをクリックします。
修復タスクリストのプレビューが表示されます。このプレビューリストでアイテムを選択して、それに対して UI アクションを実行できますが、そうしたアクションは VUL に対しても実行されます。たとえば、プレビューリストから VI を削除すると、その VI も VUL から削除されます。

c. プレビューが完了したら、ブラウザーウィンドウを閉じて変更要求フォームに戻ります。

d. [CR に CI を追加] チェックボックスで、1 つを選択して続行します。

オプション	説明
[CR に CI を追加] チェックボックスをオン	デフォルトはオンです。チェックボックスをオンにすると、この修復タスクのアクティブな脆弱性一致アイテムに属する構成アイテム (CI) がこの変更要求に追加されます。VUL は自動的に [実装待ち] ステータスに移行されます。
[CR に CI を追加] チェックボックスをオフ	この修復タスクのアクティブな脆弱性一致アイテムの CI を新しい変更要求に追加しない場合は、このチェックボックスをオフにします。

自動翻訳

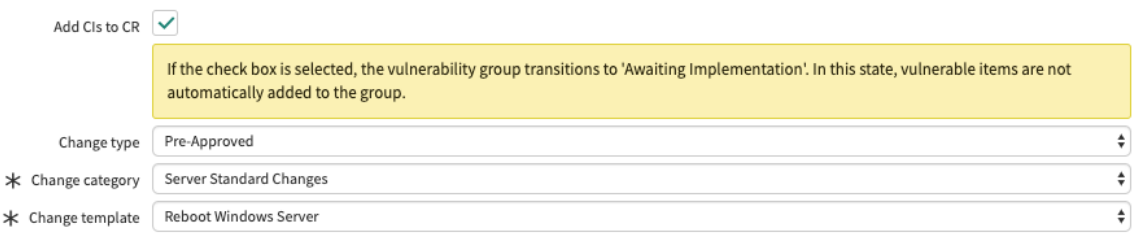
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
	無効にすると、変更要求状況は VUL に同期されず、VUL は現在のステータスのままになります。

e. [変更タイプ] フィールドの選択リストから、いずれかを選択して続行します。

変更タイプ	説明
緊急	重大なインシデントを解決するための変更。
通常	標準的な変更でも緊急の変更でもないサービスへの変更を実施するために使用される変更タイプ。
標準	事前に承認された低リスクの変更要求で、頻繁に実施されます。承認済みの標準的な変更要求をテンプレートのカタログで事前定義して、標準的な変更へのアクセスと要求をより効率的にすることができます。選択すると、次の図に示すように 2 つのフィールドが表示されます。各選択リストからいずれかを選択して、次のフィールドに入力します。 ▪ 変更カテゴリ：既存のカタログから変更のカテゴリを選択します。たとえば、[ハードウェア]、[サーバーの標準的な変更]、[ソフトウェア] などです。この例では、[標準的な変更のパッチ適用 (Patching Standard Changes)] が選択されています。 ▪ 変更テンプレート：事前定義されたサポートタスクを使用して、変更要求に利用可能なテンプレートをカタログから 1 つ選択します。この例では、[Microsoft 月次パッチ適用サイクル (Microsoft Monthly Patching Cycle)] テンプレートが選択されています。 ITSM の変更要求のカテゴリ、テンプレート、および変更タイプの詳細については、「変更タイプ」を参照してください。

この機能は、ITSM 変更管理のカタログで設定した変更要求のタイプを自動的に読み取ります。たとえば、ITSM の標準的な変更の要求の名前を「標準」から「事前承認済み」に変更すると、次の図に示すとおり、[変更要求の作成] フォームの [変更タイプ] 選択リストに新しい名前が自動的に表示されます。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フォームの [変更要求プレビュー] セクションのフィールドには、VUL の情報が事前に入力されています。これらのフィールド値は必要に応じて編集できます。たとえば、この後の図のフィールドの値を確認します。

終了予定日

この日付 (2019-10-10) は、VUL の [修復ターゲット日] フィールドに表示される値と同じです。この値は、VUL に属する脆弱性一致アイテムの最も早い修復ターゲット日から導出されます。修正日をさらに早める必要がある重大な問題の変更要求を作成している場合は、この値と [優先度] フィールドの値を編集することをお勧めします。

理由

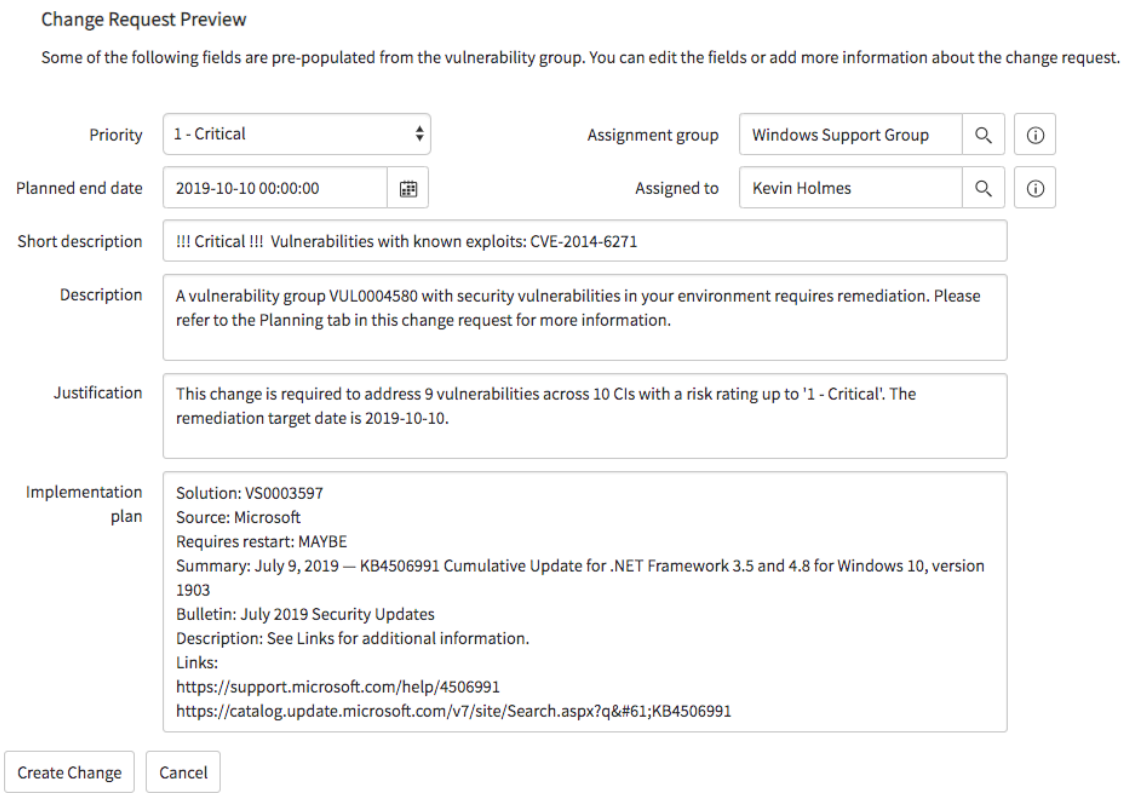
このフィールドには、CHG に追加された CI の数が表示されます。追加情報が必要な場合は、このテキストを編集することをお勧めします。たとえば、新しい VUL を作成するために使用したフィルターに関するメモ (「75 を超えるリスクスコア」など) をこのフィールドに追加することもできます。このテキストは、新しい変更要求と修復タスクを見つけるのに役立ちます。

実装計画

このフィールドには、脆弱性の優先ソリューションが表示されます。

アサイン先グループとアサイン先

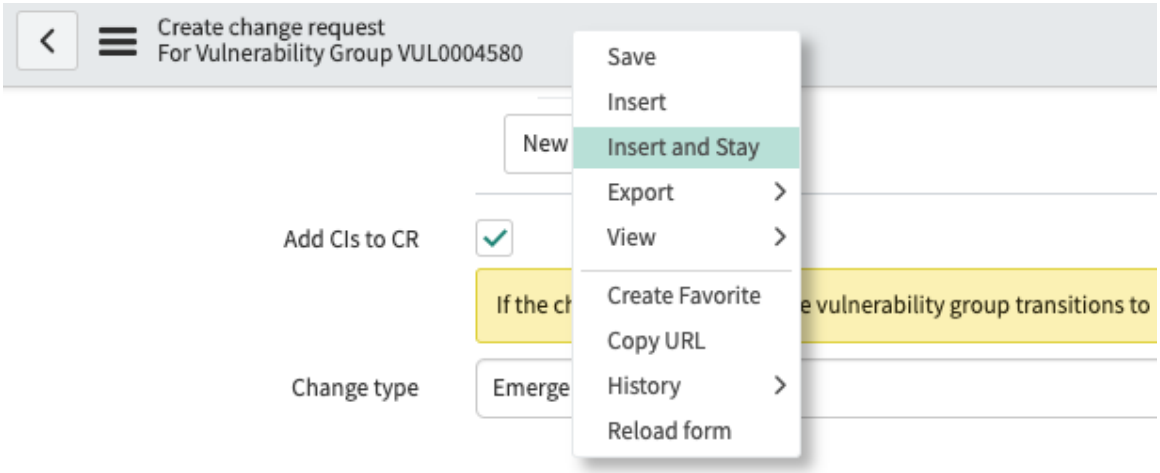
これらのフィールドを編集して、アサイン先グループを変更するか、いずれかのアサイン先グループのユーザーにこの変更要求を再アサインします。



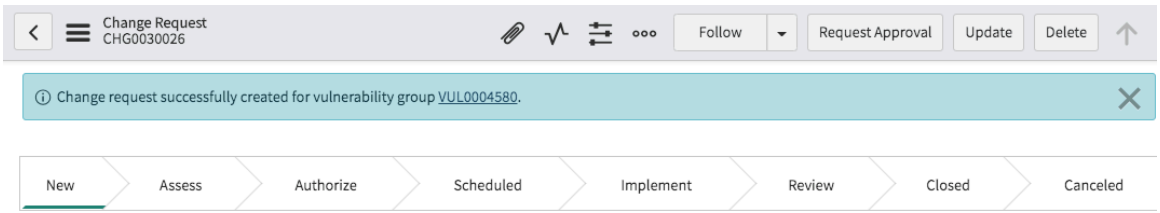
6. 必要に応じてフィールドのプレビューと編集を続行します。
7. 変更を保存してこのページに留まるには、フォームの上部にあるグレーのバナーを右クリックして、[挿入と維持] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



8. 編集が完了したら、いずれかを選択して続行します。



注:

[アサイン先グループ] および [アサイン先] のフィールドが未アサイン (空) の [オープン] ステータスの修復タスクの場合、[変更を作成] をクリックすると、現在のログオンユーザーが自動的にタスクにアサインされます。さらに、 [CI を CR に追加] チェックボックスをオンにする必要があります。VUL の上部に、このアサインを示す青色の確認メッセージが表示されます。

自動翻訳

次のタスク

変更要求と変更タスクを監視して、それらが完了し、変更要求が実装されていることを確認します。CHG が実装され [レビュー] ステータスに移行された後、ステータスの同期が有効になっていれば、VUL は自動的に [解決済み] に移行されます。ステータス同期の詳細については、「変更要求と修復タスク間のステータスの同期」を参照してください。

既存の変更要求への修復タスクの関連付け

IT 修復オーナーは、修復タスク (VUL) をインスタンスで既に利用可能な変更要求 (CHG) に関連付けることで、修復タスクの解決に取り組むときに重複した変更要求を作成しないようにします。

始める前に

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

必要なロール：itil ロールを持つ任意のユーザー。ユーザーに itil ロールがアサインされると、sn_vul.remediation_owner ロールも自動的にアサインされます。

このタスクについて

修復タスクを既存の変更要求に関連付ける方法の詳細については、「IT 修復ワークスペースで変更要求を作成する」を参照してください。

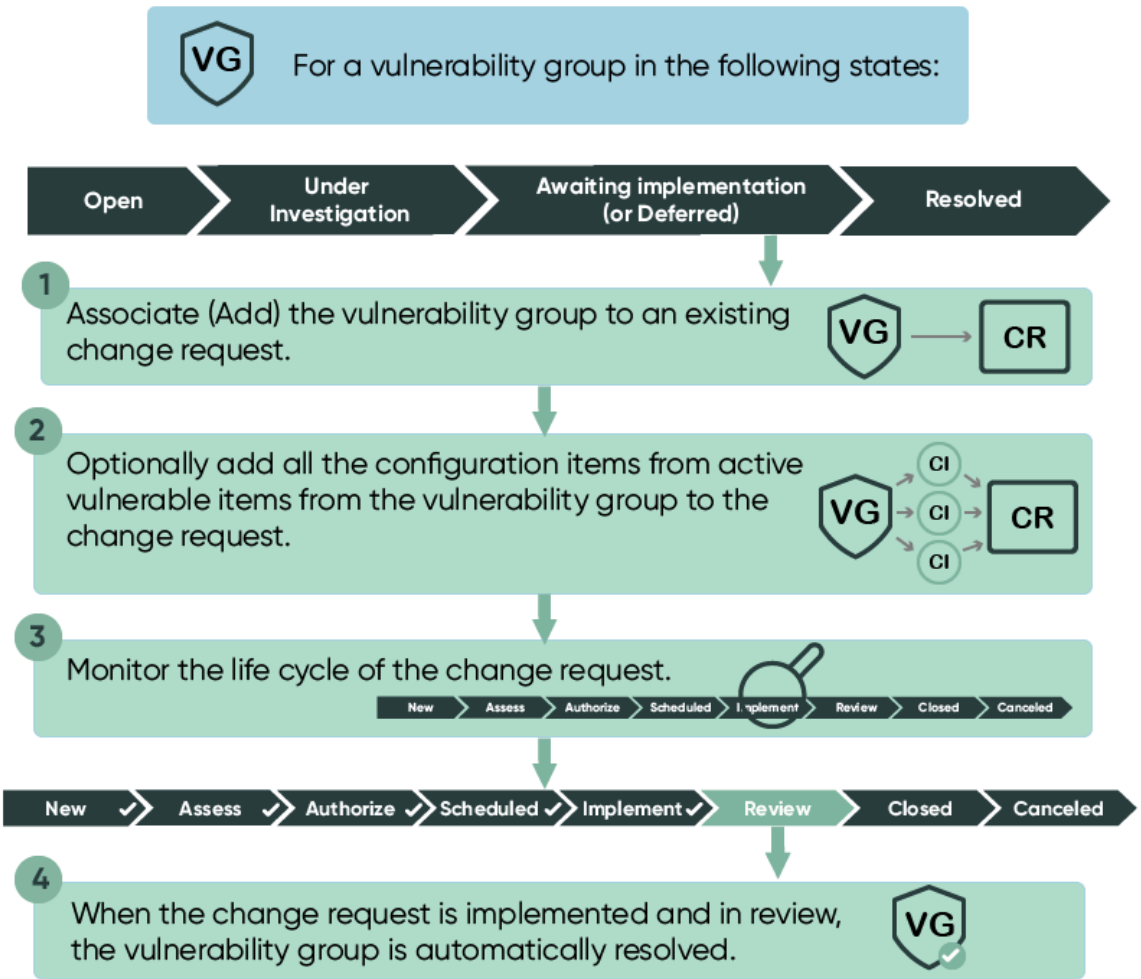
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクレコードは、以降のセクションでは VUL と呼びます。脆弱性対応 の以前のバージョンでは、修復タスクは脆弱性グループ (VG) と呼ばれていました。次の画像では、VG は修復タスクまたは VUL レコードを表しています。

修復タスクを既存の変更要求に関連付ける方法の詳細については、「IT 修復ワークスペースで変更要求を作成する」を参照してください。

修復オーナーは、自分または自分のアサイン先グループにアサインされた修復タスクを、修復タスクレコードから直接、既存の変更要求に関連付けることができます。次の図は、変更要求を既存の VUL (VG) に関連付ける基本的なフローを示しています。このフローの詳細な手順は、図に沿って説明します。

既存の変更要求に修復タスクを関連付けるためのワークフロー



注:
既存の変更要求を任意のステータス ([オープン]、[調査中]、[実装待ち]、[クローズ済み]、および [保留]) の VUL に関連付けることができます。変更要求を既存の VUL に関連付けると、アクティブな VI のみが変更要求に追加されます。

開始する前に、重複する変更要求を作成しないように、既に VUL に関連付けられている既存の変更要求を表示することをお勧めします。特定の VUL に関連する変更要求の数を簡単に追跡するには、[修復タスク] リストの [CR 数] 列を参照します。表示されていない場合は、右上の設定アイコン ( ) をクリックします。[CR 数] 列を [利用可能] から [選択済み] に移動して、**[OK]** をクリックします。

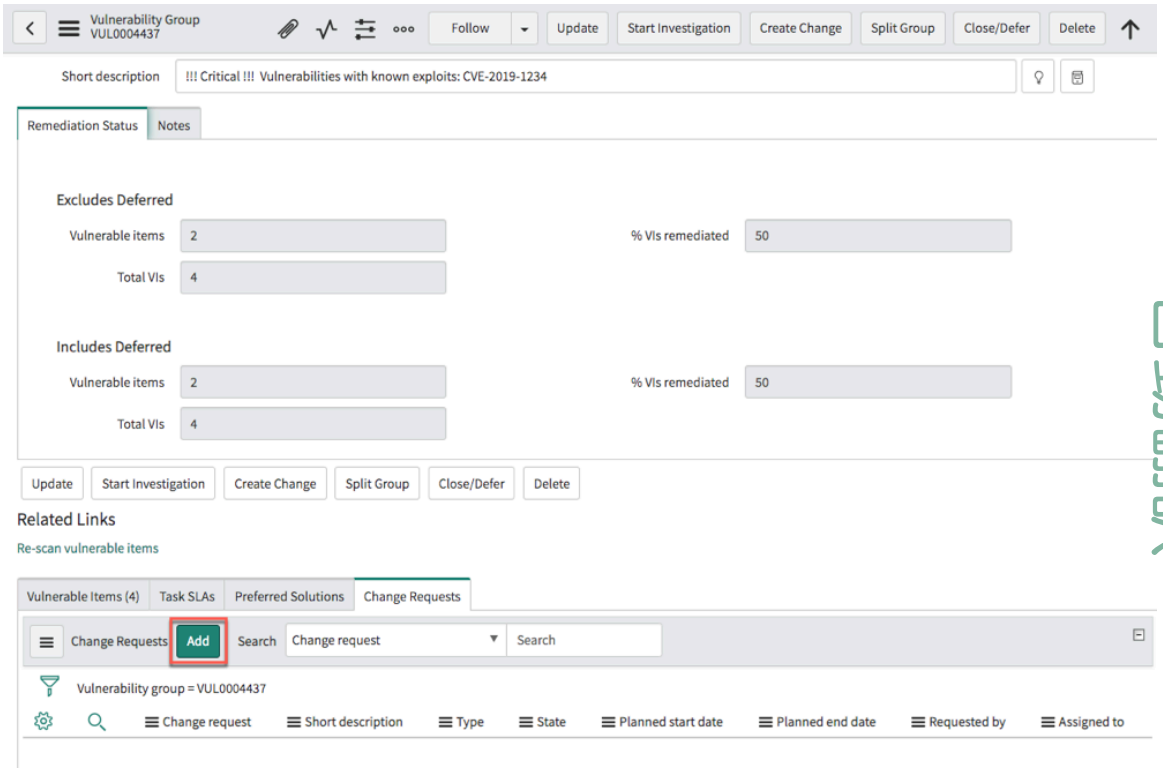
このテーブルに既存のデータがあるお客様に対して新しい列を自動的に入力するには、スケジュール済みジョブ [新しい CR カウント列を入力 (Populate new CR Count Column)] を実行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

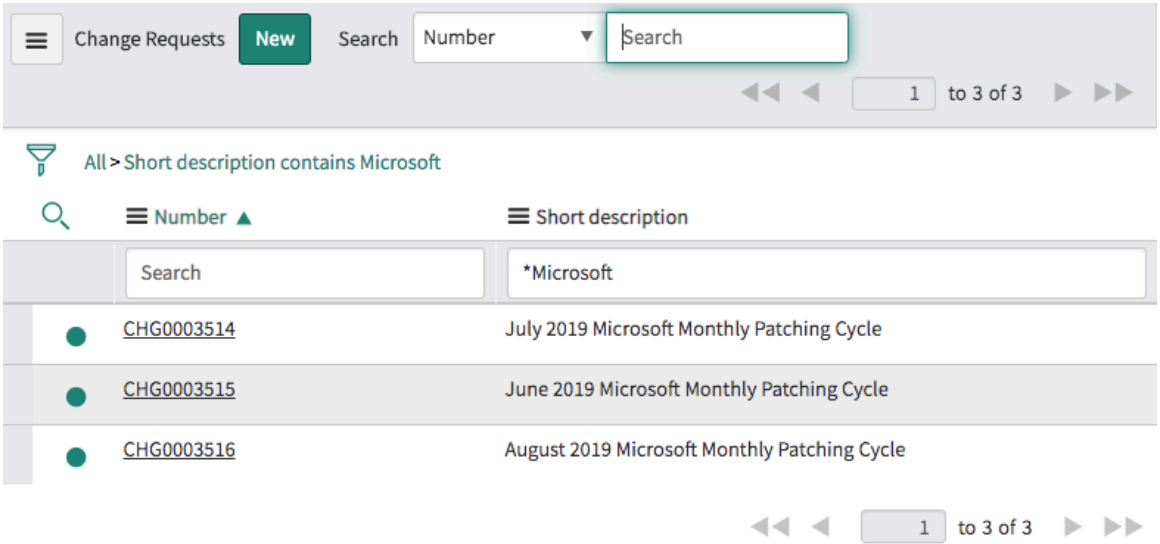
手順

1. 修復タスクを既存の変更要求に関連付けるには、次に移動します: **All** (すべて) > 脆弱性対応 > 修復タスク.
2. 作業する修復タスクを見つけます。
3. オプション: 次のように移動する。 **All** (すべて) > 脆弱性対応 > 修復の概要 修復の概要ダッシュボードを表示し、自分または自分のアサイン先グループにアサインされた VUL を見つけます。
4. [番号] 列で、VUL レコードをクリックして開きます。
   VUL レコードが表示されます。
5. 表示されていない場合は、開かれているレコードを表示した状態で、[変更要求] 関連リストまでスクロールして選択します。
   VUL に関連付けられている変更要求が [追加] ボタンとともに表示されます。次の図では、この VUL に既に関連付けられている変更要求はありません。



6. VUL を既存の CHG に関連付けるには、[追加] をクリックします。
   [既存の変更要求を修復タスクに追加] フォームが表示されます。
7. フォームで、検索アイコンをクリックします。
   次の図に示すように、既存の変更要求のリストビューが新しいウィンドウに表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



8. 表示されたリストからアイテムを選択するか、またはフィルター ( ) をクリックして検索結果を制限する条件を入力します。
9. [CR に CI を追加] チェックボックスで、1 つを選択して続行します。

   注:
   このチェックボックスは、[新規] ステータスの既存の変更要求に対してのみ表示されます。

オプション	説明
[CR に CI を追加] チェックボックスをオン	デフォルトはオンです。チェックボックスをオンにすると、この修復タスクのアクティブな脆弱性一致アイテムに属する構成アイテム (CI) がこの変更要求に追加されます。 オンの場合は、変更要求状況が VUL に同期されます。詳細については、「変更要求と修復タスク間のステータスの同期」を参照してください。
[CR に CI を追加] チェックボックスをオフ	この修復タスクのアクティブな脆弱性一致アイテムの CI を新しい変更要求に追加しない場合は、このチェックボックスをオフにします。 無効にすると、変更要求状況は VUL に同期されず、VUL は現在のステータスのままになります。

10. [変更の要求の検索] フィールドに、適切な変更要求番号を表示した状態で、[送信] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

VUL が表示されます。レコードの上部に、選択した変更要求が VUL に正常に関連付けられたことを示す青色の確認メッセージが表示されます。

注:
[アサイン先グループ] および [アサイン先] フィールドが未アサイン (空) の [オープン] ステータスの VUL の場合、[追加] をクリックすると、現在のログオンユーザーが自動的に VUL にアサインされます。さらに、 [CI を CR に追加] チェックボックスをオンにする必要があります。VUL の上部に、現在のユーザーがアサインされていることを示す青色の確認メッセージが表示されます。

次のタスク
VUL レコードを確認します。[変更要求] 関連リストの [変更要求] 列で、新しい CHG のリンクをクリックして CR レコードを表示します。開かれている CHG レコードで、変更要求状況を監視できます。影響を受ける構成アイテム (CI) と修復タスクが、[影響を受ける CI (Affected CIs)] および修復タスクの関連リストに表示されます。

修復タスクの分割

IT 修復オーナーは、既存の修復タスク (VUL) から、新しいグループに移動させる脆弱性一致アイテム (VI) のサブセットを特定します。

始める前に
注:

既存の VUL の VI を新しい修復タスクに分割するユースケースには、以下のような例が考えられます。

- 分割されたタスクに対して変更要求を作成する場合。
- 分割されたグループをアサイン先グループの別のユーザーに再アサインする場合。
- 特定の構成アイテム (CI) に関する一部の脆弱性が、指定された期間内に修正できないことが判明しているために、分割されたタスクの保留または例外を要求する場合。

必要なロール：VUL を分割するための itil ロールを持つ任意のユーザー。

注:
さらに sn_vul.remediation_owner ロールも、ユーザーに itil ロールがアサインされると自動的にアサインされます。

このタスクについて
脆弱性対応 ワークスペースでの修復タスクの分割の詳細については、「IT 修復ワークスペースでの修復タスクの分割」を参照してください。

クラシック環境または 脆弱性対応 の各バージョンで修復タスクを分割するには：

[オープン]、[調査中]、または [実装待ち] 状況の複数の脆弱性一致アイテムを含む既存の修復タスクを分割できます。特定の基準に一致する脆弱性一致アイテムを含む新しい VUL を作成することで、元の修復タスクに影響を与えることなく、特定の脆弱性一致アイテムのグループを処理できます。

条件ビルダーで新しい修復タスクに移動させる脆弱性一致アイテムの条件を指定すると、条件に一致するアクティブな VI のみが新しいグループに移動されます。

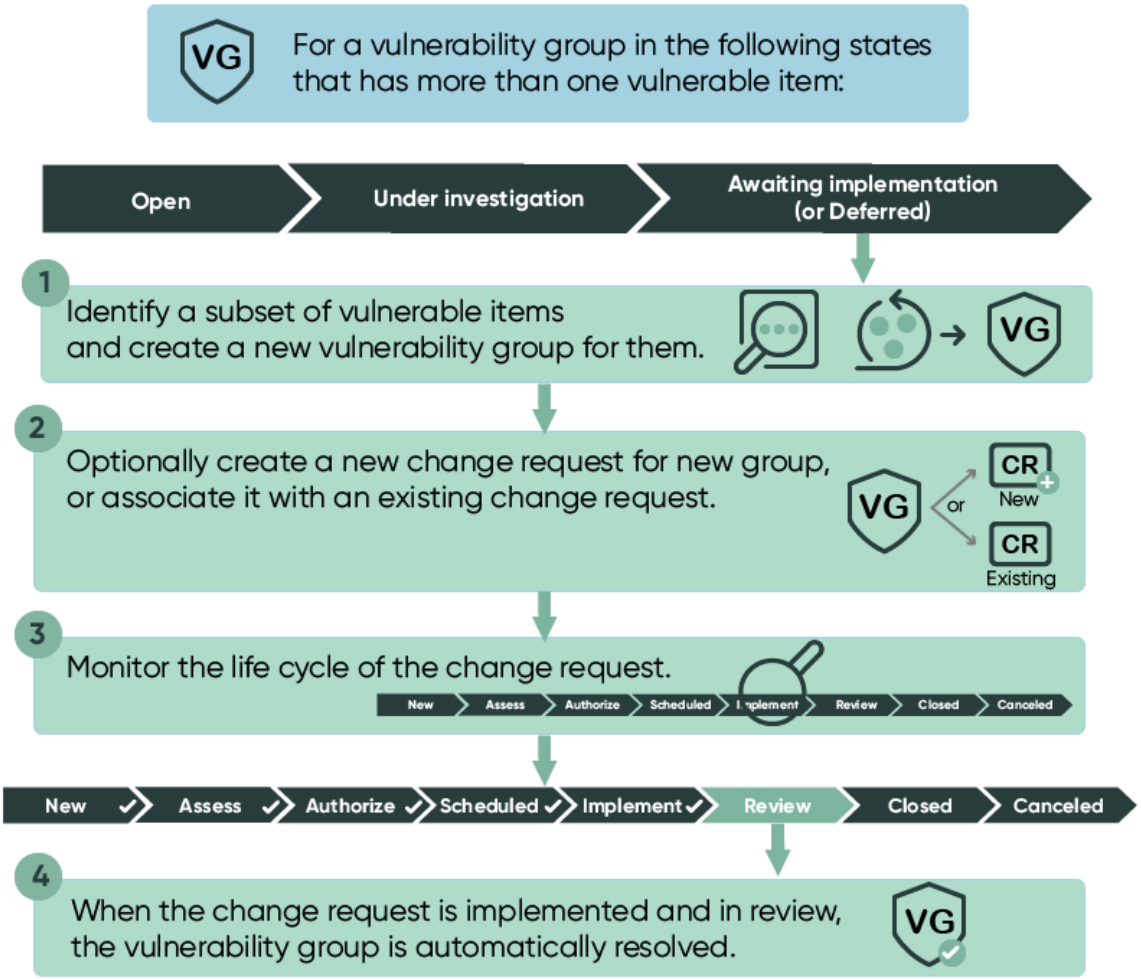
VUL を分割する場合、変更要求 (CHG) を作成する必要はありません。選択によって、変更要求を作成すると同時に VUL を分割するか、または変更要求を作成せずに VUL を分割することができます。次の図は、修復タスクを分割する基本的なフローを示しています。このフローの詳細な手順は、図に沿って説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクレコードは、以降のセクションでは VUL と呼びます。脆弱性対応 の以前のバージョンでは、修復タスクは脆弱性グループ (VG) と呼ばれていました。次の画像では、VG は修復タスクまたは VUL レコードを表しています。

修復タスクを分割するためのワークフロー

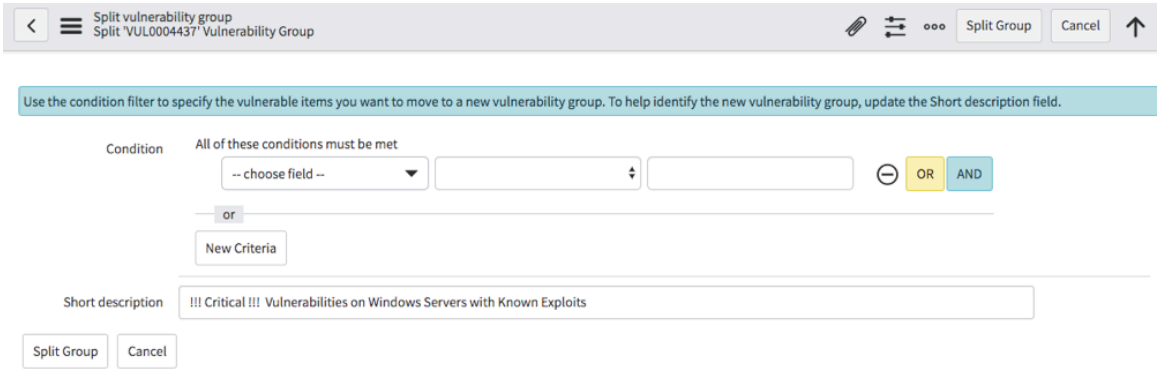


手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 修復タスク > 所属グループにアサイン済み.
   修復タスクのリストが表示されます。
2. [番号] 列で、レコードをクリックして開きます。
   レコードが表示されます。
3. VUL の右上にある [タスクを分割] をクリックします。
   [修復タスクを分割] フォームが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

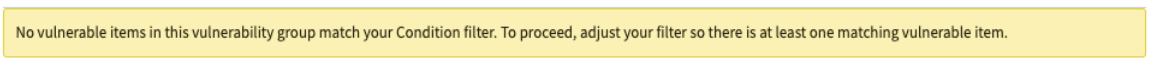


4. 条件ビルダーを表示した状態で、新しいタスクに移動させる脆弱性一致アイテムに対する条件を指定します。
   たとえば、以下の条件に一致する脆弱性一致アイテムのみを除外することができます。
   - [オープン] 状況になっている。
   - リスクスコアが 80 より大きい。
   - 「WINSV」を含む構成アイテム。
   - San Diego にある。

   たとえば、条件には次のように入力します。
   - [ステータス] - [次の値に等しい] - [オープン]
   - [リスクスコア] - [は次の値以上 (<=)] - [80]
   - 構成アイテム。[名前] - [contains (次の値含む)] - [WINSV]
   - 構成アイテム。[場所] - [次の値に等しい] - [San Diego]

   条件を入力した後、脆弱性一致アイテムがフィルターに一致する場合は、一致する脆弱性一致アイテムの数を含むメッセージが表示されます。

   注:
   フィルターに一致する脆弱性一致アイテムがないというメッセージが表示された場合は、少なくとも 1 つの脆弱性一致アイテムがフィルター基準に一致するように条件を調整します。

5. オプション: 必要に応じてフィルターを調整します。
6. オプション: 新しい VUL を作成後に特定しやすくするために、[簡単な説明] フィールドを更新することをお勧めします。
   編集した場合は、作成後に新しい VUL が見つけやすいように、検索条件として [簡単な説明] フィールドを使用します。たとえば、「SAN DIEGO にある」などと入力します。
7. オプション: フィルター基準に一致する脆弱性一致アイテムの詳細をプレビューするには、[タスクを分割] をクリックして新しい VUL を作成する前に、次の手順を実行します。
   こうした詳細には、このサブセットに既に関連付けられている既存の変更要求、このような脆弱性一致アイテムを含む VUL などがあります。プレビューでこの情報を表示することで、重複する VUL の作成を防ぐことができます。

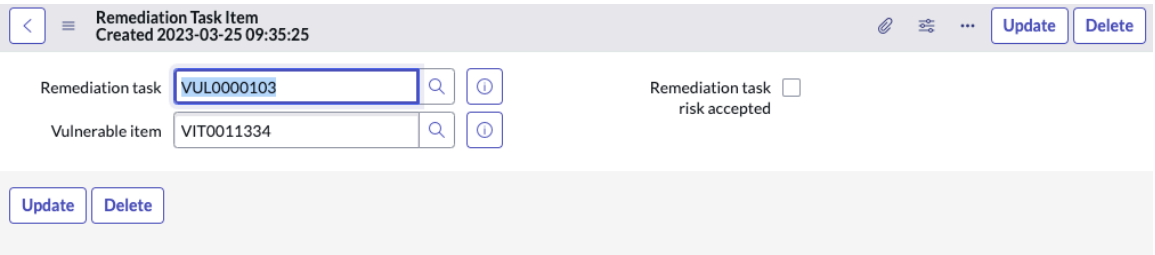
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. [修復タスクを分割] フォームの青色の確認メッセージで、[一致するアイテムをプレビュー **(Preview matching items)]** をクリックします。
[修復タスクアイテム (Remediation Task Item)] リストがブラウザーの新しいウィンドウに表示され、条件に一致する脆弱性一致アイテムのリストが示されます。

b. [番号] 列でアイテムをクリックしてレコードを開きます。

c. 表示されたレコードで、脆弱性グループまたは脆弱性一致アイテムフィールドの右側にある、脆弱性一致アイテムの情報アイコンをクリックして、レコードを表示します。



d. 表示されるダイアログで、[レコードを開く] をクリックします。
修復ターゲット日に関する情報が表示されます。[関連リスト] セクションで関連リストをクリックして、VI に関する詳細情報を表示します。

8. 条件を満たす VI を含む新しい VUL を作成する準備ができたら、プレビューウィンドウを閉じて別のウィンドウのタスク分割フォームに戻り、フォームの上部にある [タスクを分割] をクリックします。

注:

VI 数が 200 未満の場合、分割操作は同期的に実行されます。

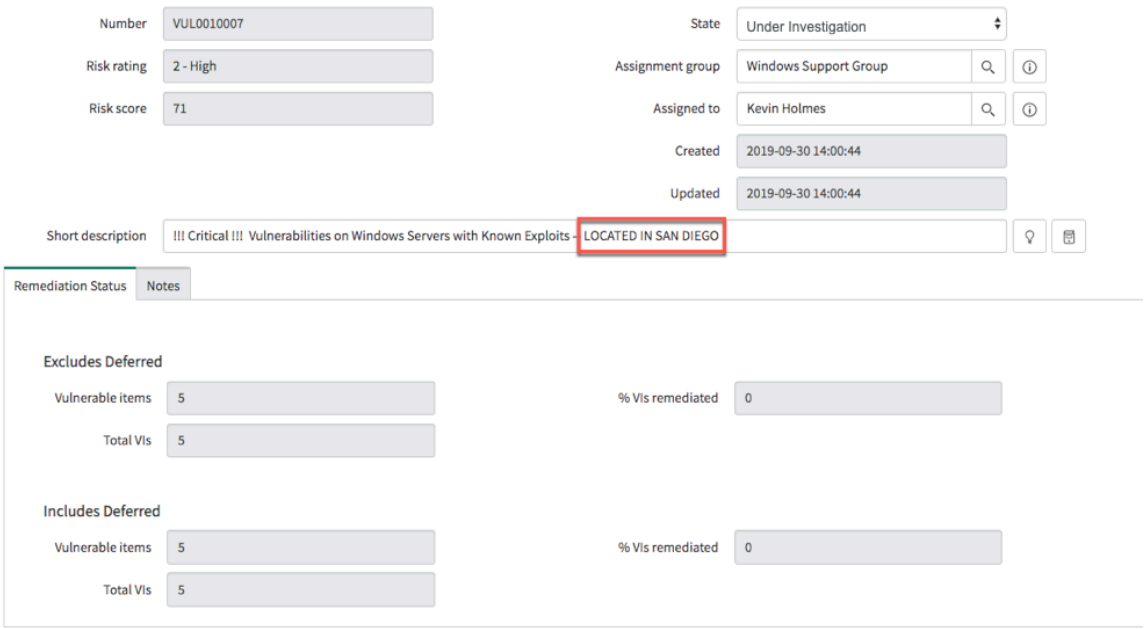
VI 数が 200 を超える場合、分割操作はバックグラウンドで非同期に実行され、VI が新しいグループに表示されるまでに数秒かかる場合があります。

すべてのアクティブな VI が新しいグループに移動されたことを示す確認メッセージが表示されます。新しい修復タスク番号も表示されます。まだ [調査中] になっていない場合、VUL は [調査中] に移行されます。[簡単な説明] フィールドで、新しい VUL に対して入力したテキスト「SAN DIEGO にある」の有無を確認します。

新しいグループのロールアップ計算が実行され、新しいリスクスコア、修復ターゲット日、およびその他のフィールド値が計算されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



脆弱性一致アイテム、優先ソリューション、および変更要求は、レコードの下部の関連リストに表示されます。この新しいタスクは、修復タスクの場合と同様に処理および監視します。

9. オプション: [メモ] 関連リストまでスクロールし、クリックして選択します。
   元の修復タスクの脆弱性一致アイテムの数がアクティビティストリームの新しいグループに移動されたことを確認します。
10. オプション: 新しい VUL で、[脆弱性一致アイテム] 関連リストから VI を再度選択して分割するには、修復タスクレコードの一番下までスクロールし、[脆弱性一致アイテム] 関連リストの [脆弱性一致アイテム] 列で移動する VI を選択した状態で、[選択した行のアクション] 選択リストから [タスクを分割] を選択します。
    [修復タスクを分割] フォームが表示されます。
11. グループを再度分割して、選択したアイテムを新しいグループに移動させるには、[タスクを分割] をクリックします。
    選択した VI が別の修復タスクに移動され、確認メッセージが表示され、新しいグループが表示されます。
12. いずれかを選択して調査または修正を続行します。

次のタスク

新しい VUL のステータスを監視して、解決を迅速化します。

変更要求と修復タスク間のステータスの同期

脆弱性対応 製品の修復タスク (VUL) のステータスフィールドと変更要求 (CHG) のステータスフィールド間には、同期関係があります。変更要求のライフサイクルが進むと、関連する修復タスクのステータスも自動的に変化します。

ステータスの同期

修復タスクレコードは、以降のセクションでは VUL と呼びます。脆弱性対応 の以前のバージョンでは、修復タスクは脆弱性グループ (VG) と呼ばれていました。次の画像では、VG は修復タスクまたは VUL レコードを表しています。

ステータスの同期は、脆弱性対応 アプリケーションをダウンロードすると、デフォルトでシステムプロパティ (sn_vul.cr_state_synch) によってインスタンスで有効になります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ステータスの同期を有効にすると、以下の場合に、CHG ステータスフィールドによって修復タスクのステータスフィールドが自動的に変更されます。

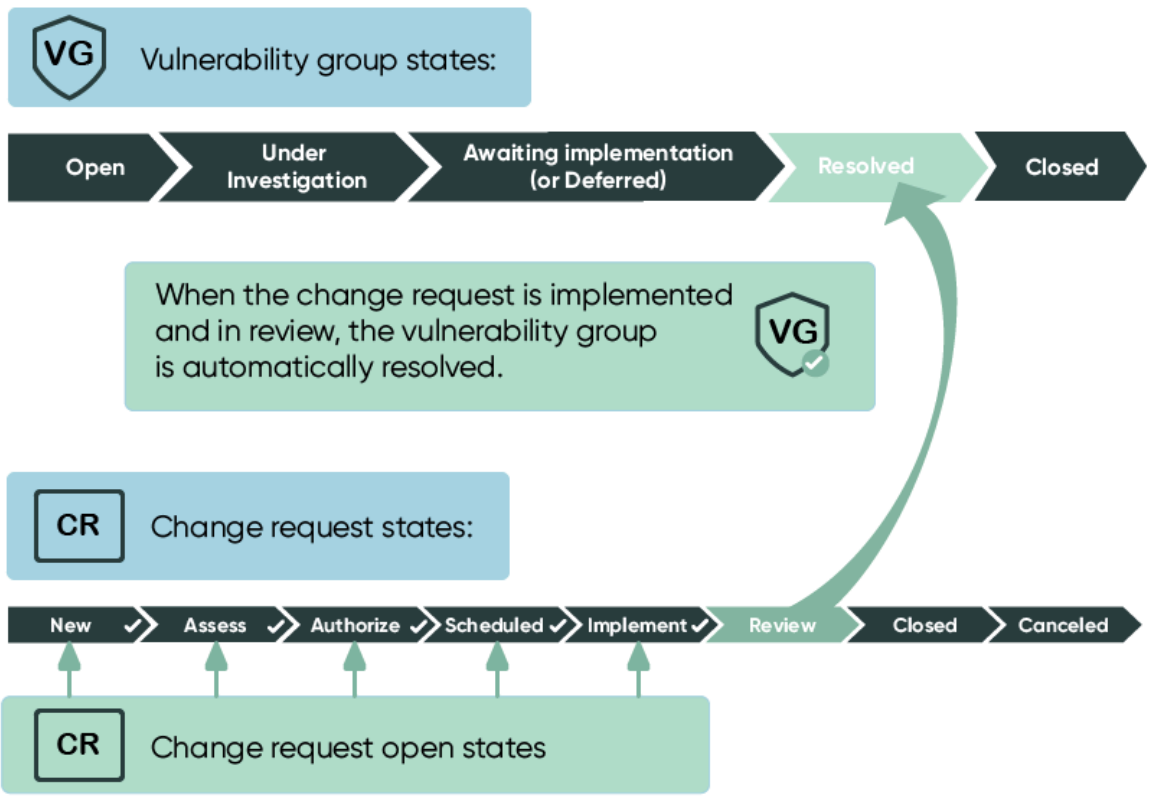
- 修復タスク (VUL) に対して新しい CHG が作成された場合、[実装待ち] でなければ、VUL のステータスは [実装待ち] に移行します。
- 既存の CHG が VUL に関連付けられた場合、[実装待ち] でなければ、VUL のステータスは [実装待ち] に移行します。
- CHG のタスクが完了 ([実装済み]) し、CHG が [レビュー] ステータスに移行すると、VUL は [解決済み] に移行します。

ステータス同期の詳細と例については、次のセクションを参照してください。

注:
状況同期を有効にした状態で、CHG と VUL のそれぞれのレコードのライフサイクル状況を手動で移行することはできますが、CHG の状況が変化したことをシステムが登録したり、CHG を追加したり、 VUL から CHG を削除したりすると、状況同期により手動操作が無効になる可能性があります。ただし、変更要求の状況は、VUL を [クローズ済み] または [保留] から自動的に移行させるものではありません。

ステータスの順方向同期

次の図は、CHG 状況が、VUL の状況をライフサイクルの順方向、つまり [オープン] から [解決済み] に自動的に移行される様子を示しています。



[クローズ済み] 以外のステータスの任意の修復タスクに対して、新しい変更要求を作成できます。状況同期により、VUL は [オープン]、[調査中]、[実装待ち]、および [解決済み] 状況を介して自動的に双方向に移行します。この移行は、変更要求におけるステータスフィールドの特定の値に基づいています。変更要求と修復タスク間のステータス同期は、自動的に呼び出されます。ただし、チェックボックス ([CR に CI を追加]) がフォームに表示されており、それをオフにした場合は除きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CHG がオープンステータスの場合、VUL は [解決済み] には移行しません。CHG のライフサイクルにおいて、[レビュー] より前の状況 ([新規]、[評価]、[許可]、[予約済み]、[実装] など) になっている部分 (前の図) は、その CHG のオープン状況と見なされます。オープン状況では、CHG の調査またはタスクが完了していないため、VUL の状況フィールドは移行されません。ステータス同期は、CHG が VUL に対して作成されるか関連付けられたとき、または CHG で既存の関係のステータスが変更されたときに呼び出されます。完了した CHG 状況は、[レビュー] および正常に [クローズ済み] となります。CHG が正常にクローズされると、そのクローズ済みコードは [成功] または [成功したが問題あり] となるため、VUL は [解決済み] に移行します。

ステータスの逆方向同期

CHG はライフサイクル中に処理されるため、ある時点でキャンセルされる場合があります。この場合、CHG が [キャンセル] または [クローズ済み] (クローズコードは [不成功]) の場合、VUL は自動的に [調査中] に戻されます。脆弱性を修正するアクティブな計画がないため、VUL は [調査中] に戻されます。

VUL が [解決済み] 状況にある場合、新しい CHG を作成するか、初期オープン状況のいずれかで既存の CHG に関連付けると、VUL は自動的に [実装待ち] に戻されます。CHG にアサインされている作業が増えるため、VUL はこのステータスに戻されます。

複数の **CHG** を含む **VUL**

[実装待ち] の VUL に複数の CHG が関連付けられている場合、ステータスの同期は、そのライフサイクルの最も早期のステータスである CHG のステータスに基づいています。たとえば、次の表に示すように、VUL に CHG1、CHG2、CHG3、および CHG4 の 4 つの CHG が関連付けられているとします。

CHG 番号	CHG ステータス
1	実装
2	キャンセル済み
3	クローズ済み (クローズコード [不成功])
4	クローズ済み (クローズコード [成功])

この場合、CHG と VUL 間のステータス同期は、4 つの CHG のうち最も早期のステータスである CHG1 ([実装]) に基づいています。この場合、VUL は [実装待ち] のままになります。

別の例では、VUL が [解決済み] ステータスにあり、実装済みで [レビュー] ステータスになっている既存の CHG があり、新しい CHG が作成された場合、VUL は [解決済み] から [実装待ち] に戻されます。ステータスの同期は、最も早期のステータスの CHG である [新規] ステータスの CHG に基づいています。

CHG 番号	CHG ステータス
1	レビュー
2	新規

また、VUL に複数の CHG があるときは、次の場合に VUL のステータスは自動的に移行されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- CHG が [レビュー] に移行すると、VUL に関連付けられている他のすべての CHG が [レビュー] または [クローズ済み] 状況 (正常なクローズコードあり) であれば、VUL は [解決済み] に自動的に移行されます。キャンセルされたり、正常にクローズされていない他の関連する CHG は無視されます。
- CHG が [キャンセル] または [クローズ済み] (クローズコード [不成功]) に移行すると、VUL に関連付けられている他のすべての CHG が同じステータスであれば、VUL は自動的に [調査中] に戻されます。

修復タスクの状況と各状況で実行できる処理の詳細については、「脆弱性対応 修復タスクと脆弱性一致アイテム状況」を参照してください。

脆弱なソフトウェアへのエクスポージャーの評価

ITSM ソフトウェア資産管理 (SAM) 基盤アプリケーションを使用して、エクスポージャーアセスメントモジュールに公開者と製品情報を入力し、脆弱なソフトウェアに対する資産のゼロデイ (当日) エクスポージャーを評価できます。

重要:
ソフトウェアと共通脆弱性識別子 (CVE) によるエクスポージャーアセスメントを実行して、脆弱性アセスメントワークスペースの追加機能を活用できます。詳細については、「脆弱性アセスメントのワークスペースの詳細」を参照してください。

始める前に

必要なロール：vulnerability admin (sn_vulnerability_write)
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

評価する脆弱なソフトウェアに関する以下の情報を用意します。

- パブリッシャー
- バージョン
- 製品
- Edition (エディション)

このタスクについて

システム要件の詳細については、「脆弱性エクスポージャーアセスメントの構成」を参照してください。

ソフトウェアエクスポージャーアセスメントモジュールを表示して、Now Platform® インスタンス内の脆弱性ソフトウェアのエクスポージャーアセスメントレコードをオンデマンドで作成および編集できます。

多数の資産に対する責任を負う大規模運用のために脆弱性対応のアクティビティを管理しているとします。担当の Security Operations Center (SOC) から、脆弱であることが判明したソフトウェアのバージョンについての連絡を受け取ります。資産のスキャンが最近完了しましたが、この脆弱性は見つからなかったことが判明しました。SOC チームは、脆弱性情報データベース (NVD)、共通脆弱性タイプ一覧 (CWE)、またはインスタンス内のその他のサードパーティライブラリ以外の信頼できるソースからこの脆弱性を把握しました。そのため、脆弱性スキャナーに、まだ脆弱性に対応するプラグインが追加されていないことが懸念されます。

スキャナーが次回のスキャンでこの脆弱性を検出できるように、この脆弱性のデータが NVD ですぐに更新されインポートされると確信していますが、潜在的なエクスポージャーの範囲が気がかりであ

自動翻訳

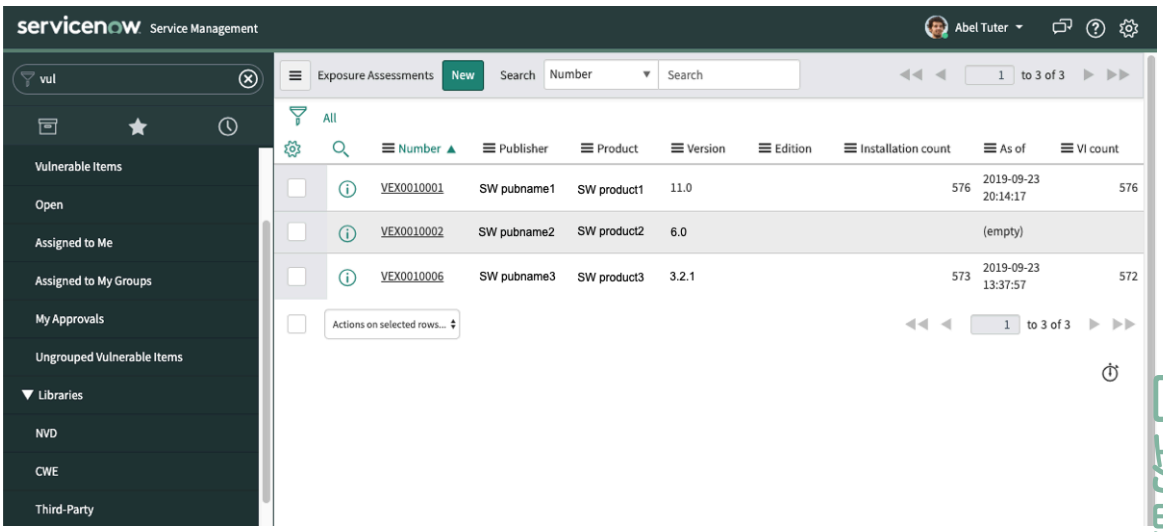
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

るため、このソフトウェアがインストールされている資産がネットワーク内にあるかどうかを今日把握したいと考えています。

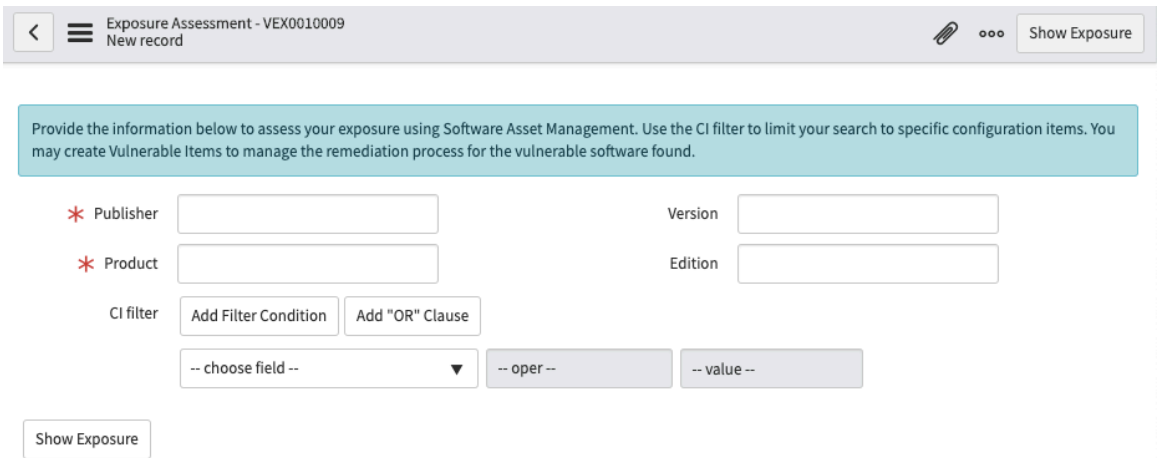
脆弱性対応 v23.0 以降、Pro または Enterprise サブスクリプションを利用している場合、[すべて] メニューの [エクスポージャーアセスメント] リンクを選択すると、ロールに応じてワークスペースの [エクスポージャーアセスメント] ページにリダイレクトされます。詳細については、「脆弱性エクスポージャーアセスメントの構成」を参照してください。

手順

1. 新しいエクスポージャーアセスメントを作成するには、次に移動します: **All** (すべて) > 脆弱性対応 > 脆弱性スキャン > エクスポージャーアセスメント.
   エクスポージャーアセスメントリストが表示されます。



2. [新規] を選択します。
   エクスポージャーアセスメントフォームが表示されます。



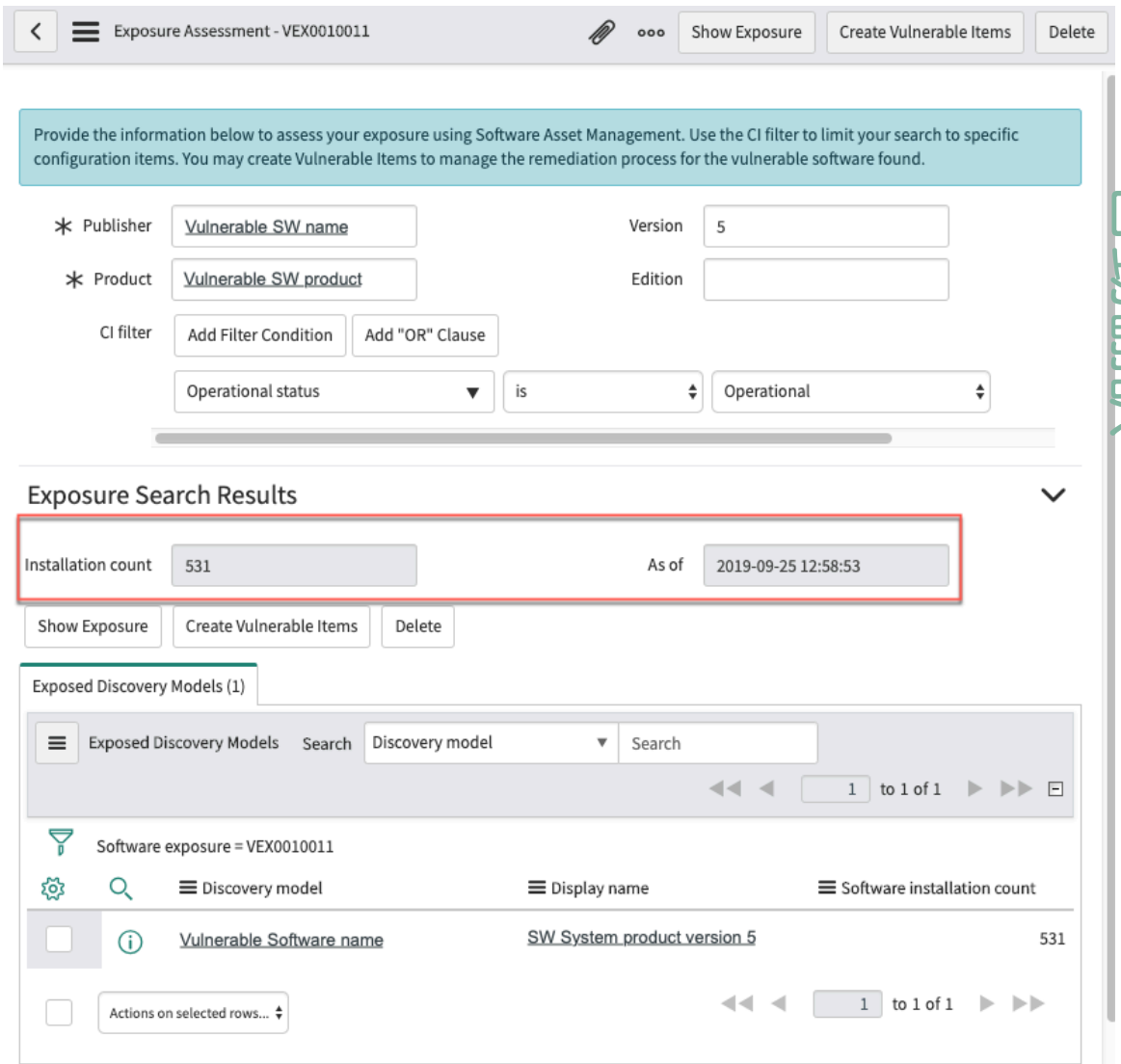
3. フォームに記入します。

フィールド	説明
パブリッシャー	ソフトウェア公開者の名前。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
(オプション) バージョン	資産の検索を絞り込むのに役立つバージョン番号を入力します。
製品	ソフトウェア製品の名前。
(オプション) エディション	資産の検索を絞り込むのに役立つエディションを入力します。
CI フィルター	構成アイテム (CI) フィルターの選択リストを使用して、検索を特定の構成アイテム (資産) に制限します。たとえば、このソフトウェアがインストールされている可能性があるアクティブな資産に対してのみクエリを送信できます。 [運用ステータス] [次の条件に一致] [稼働中 (Operational)]

4. [エクスポージャーを表示] を選択します。
特定日付時点の資産のディスカバリーモデルとソフトウェアのインストール数を含むエクスポージャーアセスメントレコードが表示されます。



5. 1 つ選択して続行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. オプション: 検索結果の脆弱性一致アイテムを作成します。

   注:
   脆弱性一致アイテムを作成した後は、このエクスポージャーレコードの検索条件は変更できません。

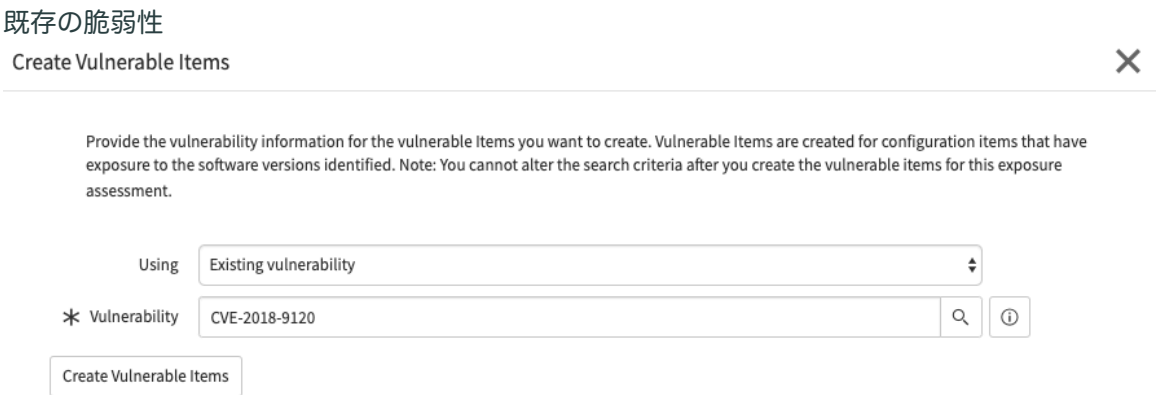
7. または、フィルター条件を変更して検索結果を絞り込みます。
8. 脆弱性一致アイテムを作成するには、次の手順を実行します。

   a. [脆弱性一致アイテムを作成] を選択します。
   [脆弱性一致アイテムを作成] ダイアログが表示されます。

   b. フィールドに入力します。

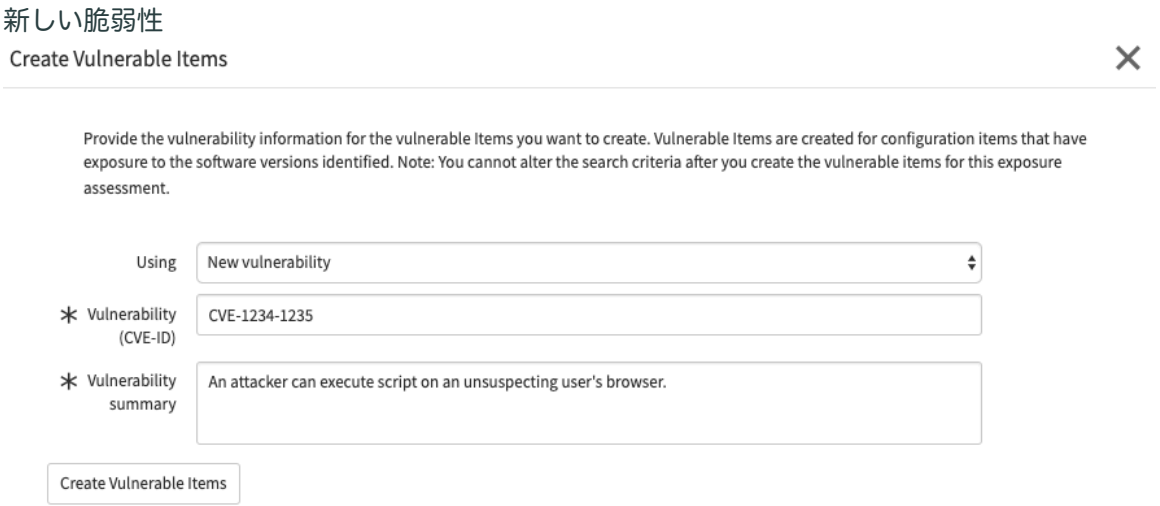
フィールド	説明
使用	選択リストから、いずれかを選択して続行します。 ▪ 既存の脆弱性。[脆弱性] フィールドの右側にある検索アイコンをクリックします。表示されるリストで [CVE-ID] を選択するか、既存の CVE-ID (CVE 2018-9120 など) を見つけるための検索条件を入力します。 注: これは、NVD 以外の脆弱性データベースからの CVE-ID であってもかまいません。 ▪ 新しい脆弱性。新しい脆弱性の CVE-ID を、xxxx-xxxx、xxxx-xxxxx、または xxxx-xxxxxxx の形式で入力します。
脆弱性のサマリー (Vulnerability summary) (新しい脆弱性のみ)	新しい脆弱性のサマリーとして「攻撃者は無防備なユーザーのブラウザー上でスクリプトを実行可能」などを入力します。

次の画像は、既存の脆弱性と新しい脆弱性の入力済みフォームの例を示しています。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



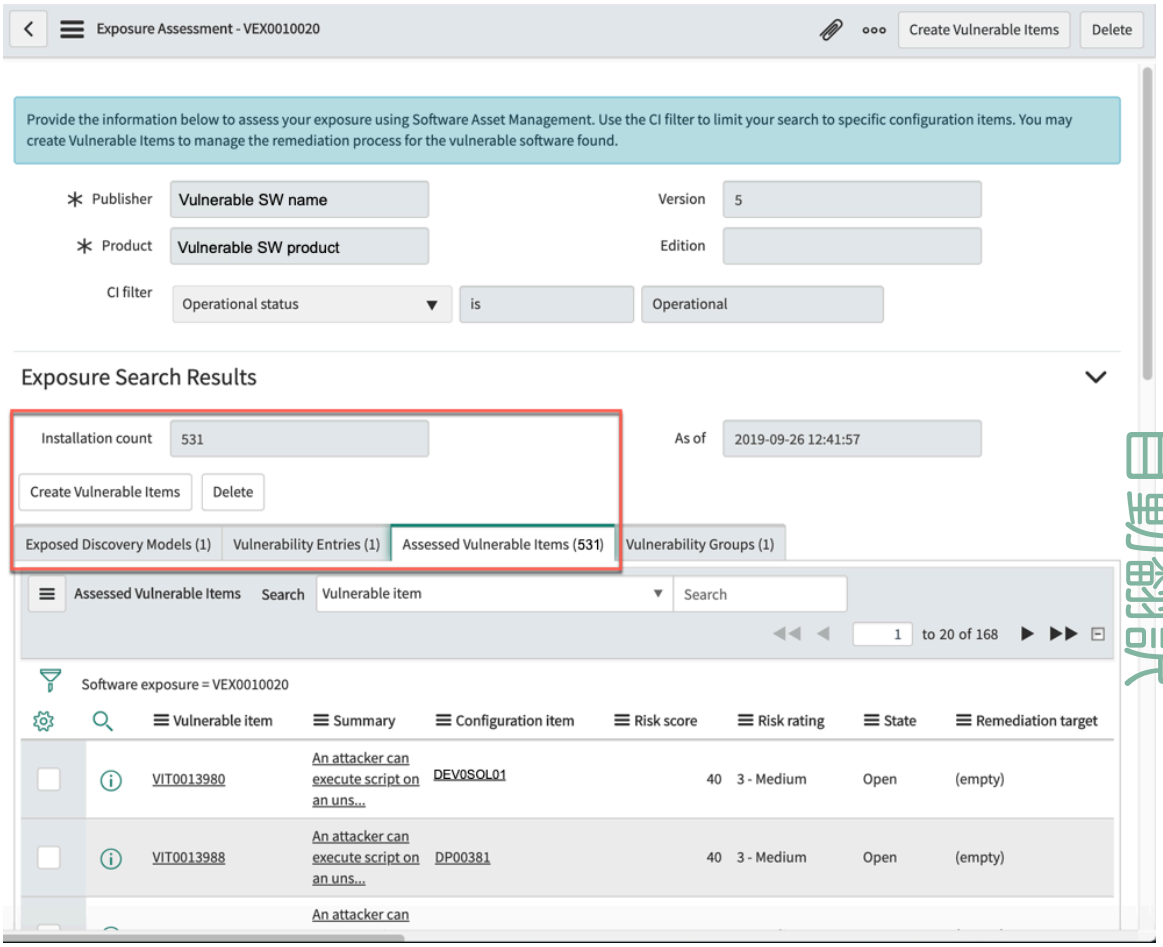
c. [脆弱性一致アイテムを作成] を選択します。
エクスポージャーアセスメントレコードが、脆弱性一致アイテムが作成されていることを示すステータスメッセージとともに表示されます。

d. 数秒後に、フォームの上部にあるグレーのバナーを右クリックして、ページを再ロードします。
次の図に示すように、[評価される脆弱性一致アイテム] タブ (531) に新しい脆弱性一致アイテムが表示されます。これらの脆弱性一致アイテムに対して作成された新しい修復タスクが、修復タスクタブ (1) に表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

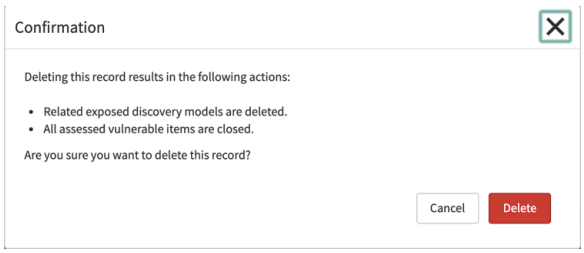
注:
この例では、「脆弱性 (Vulnerability)」という修復タスクルールのグループルールと条件に従って修復タスクが作成されます。このグループルールは、Now Platform インスタンスに脆弱性対応製品とともにインストールされているデフォルトの修復タスクルールです。この例では、このグループルールの条件によって、すべての脆弱性一致アイテムが単一の修復タスクに配置されています。エクスポージャーアセスメントの検索結果に一致する脆弱性一致アイテムに対して複数の修復タスクを作成する場合は、追加の修復タスクルールを設定することをお勧めします。修復タスクをさらに作成すると、多数の脆弱性一致アイテムを含む修復タスクが作成されるのを防ぐことができます。修復タスクルールの詳細については、「脆弱性対応修復タスクとタスクルールの概要」および「脆弱性対応 修復タスクルールの作成または編集」を参照してください。



9. 1 つ選択して続行します。

オプション	説明
修復タスク	[修復タスク] タブを選択した状態で、番号列でレコードをクリックして開き、修正用のタスクを確認してアサインします。アサイン先グループの詳細については、「Creating groups」を参照してください。
評価される脆弱性一致アイテム	[評価される脆弱性一致アイテム] タブを選択した状態で、[脆弱性一致アイテム] 列でレコードをクリックして開き、個々の脆弱性一致アイテムを確認してアサインします。
削除	エクスポージャーアセスメントレコードを削除します。確認ダイアログが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
	注: 脆弱性一致アイテムを作成した後にエクスポージャーレコードを削除すると、このレコードに対して作成した、別のエクスポージャーレコードに関連していない脆弱性一致アイテムは、自動的に [クローズ済み] ステータスに移行されます。クローズの理由は [キャンセル] です。
	

次のタスク
エクスポージャーアセスメントに基づいてゼロデイ (当日) の脅威に対応します。修復タスクの詳細および 脆弱性対応 の変更の管理の詳細については、「脆弱性対応修復タスクとタスクルールの概要」および「脆弱性対応 の変更管理」を参照してください。

アサインの推奨を表示する

アサイン先グループは、通常、アサインルールを使用して脆弱性一致アイテムにアサインされます。これらのルールは、サードパーティのスキャナーから受信したデータに基づいて正しいアサイン先グループがアサインされるように、脆弱性アドミニストレーターによって設定されます。

詳細については、「脆弱性対応 アサインルールの概要」を参照してください。一致するアサイン先グループが利用できない場合、または間違っている場合は、脆弱性アサインの推奨 を使用して別のアサイン先グループを表示できます。

脆弱性アサインの推奨 を使用して、次のアクションを実行します。

- 脆弱性一致アイテムのアサイン先グループの推奨事項の要求。
- 複数の脆弱性一致アイテムに対するアサイン先グループの推奨事項の要求。
- 修復タスクに対するアサイン先グループの推奨事項の要求。

脆弱性一致アイテムのアサイン先グループの推奨事項の要求

アサイン先グループの推奨事項を表示できるように、脆弱性アサインの推奨 を要求します。一致するアサイン先グループが利用できない場合、または脆弱性一致アイテム (VI) に対して正しくない場合は、推奨事項を要求できます。

始める前に
必要なロール： sn_vul.remediation_owner

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム をクリックし、VI を開きます。
   アイテムは、[オープン]、[保留]、[調査中]、または [実装待ち] ステータスである必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. その VI に対するアサイン提案の [アサイン先グループ] フィールドの横にある推奨アイコン ( ) をクリックします。
3. [アサイン先グループの推奨事項] ダイアログボックスで、信頼スコアに基づく推奨事項を選択します。
   信頼スコアは、VI に対する一致の関連性を予測します。詳細については、「脆弱性対応 の機械学習ソリューション」を参照してください。
4. [アサイン] をクリックします。

タスクの結果
選択したグループが [アサイン先グループ] フィールドに表示され、[アサインのタイプ] が [推奨事項 (Recommendation)] に変更されます。

複数の脆弱性一致アイテムに対するアサイン先グループの推奨事項の要求

一括編集を使用して複数の脆弱性一致アイテム (VI) に対するアサイン先グループの推奨事項を表示するには、脆弱性アサインの推奨 を使用します。複数の VI が選択されている場合、選択された VI のランダムサンプルで予測が実行されます。

始める前に
必要なロール： sn_vul.remediation_owner

このタスクについて
推奨事項とその信頼スコアは、選択した VI から取得されたサンプルに基づいて、呼び出されるたびにわずかに異なる場合があります。信頼スコアは、推奨されるアサイン先グループが脆弱性の解決に適しているとシステムが信頼しているかどうかを評価するものです。一括編集オプションを使用して修復タスク (VUL) および VI に対する脆弱性アサインの推奨を要求する場合は、assignment_recommendation_batchsize システムプロパティを使用してバッチサイズを設定します。このシステムプロパティのデフォルト値は、最適な予測パフォーマンス用に設定されています。

> **注:**
> デフォルト値を増やすと、これらのケースの 脆弱性アサインの推奨 の応答時間が変化する可能性があります。

手順
1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > **Vulnerable Item** (脆弱性一致アイテム) をクリックし、複数の VI を選択します。
   アイテムは、[オープン]、[調査中]、または [実装待ち] ステータスである必要があります。
2. [一括編集] をクリックします。
3. フォームのフィールドに入力します。

一括脆弱性一致アイテム **(Bulk Vulnerable Items)** フォーム

フィールド	説明
レコード選択	一括編集のために選択したレコード。
アサイン先グループ	選択した脆弱性一致アイテムに設定するアサイン先グループ。推奨されるアサイン先グループを表示するには、フィールドの横にある推奨アイコン ( ) をクリックします。信頼スコアに基づいて推奨事項を選択し、[アサイン] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
作業メモ	追加するメモ。

4. **[OK]** をクリックします。

タスクの結果
選択したグループが [アサイン先グループ] フィールドに表示され、選択したすべての VI の [アサインのタイプ] が [推奨事項 (Recommendation)] に変更されます。

修復タスクに対するアサイン先グループの推奨事項の要求

修復タスク (VUL) に対するアサイン先グループの推奨事項を表示するには、脆弱性アサインの推奨を使用します。

始める前に
必要なロール： sn_vul.remediation_owner

このタスクについて
一括編集オプションを使用して VUL および脆弱性一致アイテム (VI) に対する脆弱性アサインの推奨を要求する場合は、assignment_recommendation_batchsize システムプロパティを使用してバッチサイズを設定します。このシステムプロパティのデフォルト値は、最適な予測パフォーマンス用に設定されています。

> **注:**
> デフォルト値を増やすと、これらのケースの 脆弱性アサインの推奨 の応答時間が変化する可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 修復タスク をクリックし、VUL を選択します。
   グループは、[オープン]、[調査中]、または [実装待ち] ステータスである必要があります。
2. 選択した VUL に対するアサイン先グループの推奨事項の [アサイン先グループ] フィールドの横にある推奨アイコン ( ) をクリックします。
   [アサイン先グループの推奨事項] ダイアログボックスには、推奨されるアサイン先グループとそのグループ内のすべての VI の平均信頼スコアが表示されます。
3. [アサイン先グループ] リストから、信頼スコアに基づいて推奨事項を選択します。
   信頼スコアは、選択した VUL に対する一致の関連性を予測します。
4. [アサイン] をクリックします。
   選択したグループは [アサイン先グループ] フィールドに表示されます。
5. 更新された情報で修復タスクを保存します。

タスクの結果
アサイン先グループが VUL と同じすべての VI が、選択したアサイン先グループにアサインされます。VUL および変更されたすべての VI の [アサインのタイプ] が [推奨事項 (Recommendation)] に変更されます。

例外の要求と承認

脆弱性一致アイテムの修復または修復タスクを、指定した期間保留するように要求できます。たとえば、修復オーナーは、マシンにパッチが適用できない場合に例外を要求できます。アクセス権を持つ承認者は、他のユーザーからの要求を承認できます。

例外は 脆弱性対応 のワークスペースから要求できます。「IT 修復ワークスペースで例外を要求する」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 脆弱性一致アイテムに対する例外の要求
- 修復タスクに対する例外の要求
- 一括例外の要求

GRC: ポリシーとコンプライアンス管理 を使用してポリシーの例外を要求することもできます。

- GRC: ポリシーとコンプライアンス管理 を使用した例外の要求
- GRC: ポリシーとコンプライアンス管理 を使用した一括例外の要求

注:

例外管理の全ステージでメール通知が送信され、要求のステータスやその他の詳細情報が通知されます。たとえば、例外が要求されると、要求が発生したことを確認するメールが要求者に届きます。承認者にも、例外が要求されたことを示すメールが届きます。

脆弱性対応 の v21.0 以降では、誤検出と例外を承認する期間を設定できます。また、設定した日数経過後の承認者と要求者の両方に対するメール通知も可能です。要求が発生すると、脆弱性一致アイテムが [レビュー中] ステータスに変わり、ステータス変更レコードが作成されます。設定された期間内に承認者が応答しない場合、脆弱性一致アイテムまたは修復タスクは [オープン] ステータスに戻ります。以前のステータスは **[backup_state]** フィールドに保存されます。詳細については、「例外管理の承認ルールの構成」を参照してください。

脆弱性一致アイテムに対する例外の要求

すぐに修復できない脆弱性一致アイテム (VI) に対する例外を要求します。たとえば、マシンにパッチが適用できない場合に、修復オーナーとして例外を要求できます。

始める前に

必要なロール： sn_vul.remediation_owner

このタスクについて

重要:
脆弱性マネージャーワークスペースおよび IT 修復ワークスペースから例外を要求することができます。詳細については、「で修復タスクとレコードの例外を要求する Vulnerability Manager ワークスペース」と「IT 修復ワークスペースで例外を要求する」を参照してください。

クラシック環境の VI に対する例外を要求することもできます。

注:

脆弱性対応 の v21.0 以降では、誤検出と例外を承認する期間を設定できます。また、設定した日数経過後の承認者と要求者の両方に対するメール通知も可能です。要求が発生すると、脆弱性一致アイテムが [レビュー中] ステータスに変わり、ステータス変更レコードが作成されます。設定された期間内に承認者が応答しない場合、脆弱性一致アイテムまたは修復タスクは [オープン] ステータスに戻ります。以前のステータスは **[backup_state]** フィールドに保存されます。詳細については、「例外管理の承認ルールの構成」を参照してください。

手順

1. 次のように移動する。 脆弱性対応 > 脆弱性一致アイテム > **All** (すべて).
2. 例外を要求するアイテムを選択します。
   選択するアイテムは、[オープン]、[調査中]、または [実装待ち] ステータスである必要があります。
3. 脆弱性一致アイテムフォームで、[例外の要求] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

4. [例外管理] 画面で 脆弱性対応 が選択されている場合は、[例外管理] フォームのフィールドに入力します。

[例外の要求] フォーム

フィールド	説明
期限	例外要求の有効期限が切れる日付この日付は、次で選択した期間内である必要があります: **All** (すべて) > 脆弱性対応 > アドミニストレーション > 例外管理 スクリーン。 例外要求の有効期限が切れると、グループは [オープン] ステータスに戻ります。 **注:** 脆弱性対応 (VR) のバージョン 18.0 以降では、脆弱性一致アイテムが例外管理機能を使用した修復タスクのために保留された場合、スキャナーによって再オープンされた場合でも、脆弱性に設定された保留日は保持されます。この機能を有効にするには、*sn_vul.auto_defer_vit_in_active_exception_* システムプロパティの値を [true] に設定します。また、保留 [期限] の日付は、脆弱性一致アイテムがクローズした後や例外の有効期限が切れた後も保持されます。必要なロールは、読み取りと書き込みの両方に sn_vul.manage_exception_configuration です。
理由	要求の理由選択肢は次のとおりです。 ○ リスクの受容 ○ メンテナンス期間待ち ○ 修正が利用不可 ○ コントロールの緩和を実施 ○ その他 理由の新しい選択肢を追加する方法については、「ポリシー理由のマッピングの定義」を参照してください。
追加情報	この要求が行われている理由に関連する詳細情報。この必須フィールドは修復オーナーが更新します。

5. [承認要求] をクリックして例外要求を送信します。

タスクの結果

脆弱性一致アイテムのステータスが [レビュー中] に変わります。[ステータス変更承認] タブを使用して、例外要求のステータスを追跡します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクに対する例外の要求

修復タスクをすぐに解決できない場合に、修復タスクを指定された期間保留する例外を要求します。

始める前に

重要:

脆弱性マネージャーワークスペースおよび IT 修復ワークスペースから例外を要求することができます。「IT 修復ワークスペースで例外を要求する」を参照してください。

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

必要なロール： sn_vul.remediation_owner

クラシック環境の修復タスクに対して例外を要求することもできます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 修復タスク > **All** (すべて).
2. 例外を要求するグループを選択します。
   選択するタスクは、[オープン]、[調査中]、または [実装待ち] ステータスである必要があります。
3. 修復タスクレコード (VUL) で、[例外の要求] を選択します。
4. フォームのフィールドに入力します。

[例外の要求] フォーム

フィールド	説明
期限	例外要求の有効期限が切れる日付。この日付は、構成で定義された例外期間内である必要があります。
理由	例外を要求する理由。
追加情報	この要求が行われている理由に関連する詳細情報。このフィールドは修復オーナーが更新します。

5. [承認要求] をクリックします。

一括例外の要求

各アイテムを手動で選択する代わりに、一括編集オプションを使用して、複数の脆弱性一致アイテム (VIT) の例外を要求します。

始める前に

必要なロール：sn_vul.vulnerability_analyst

このタスクについて

複数の VIT が選択されている場合、これらのアイテムで修復タスク (VUL) が形成されます。複数の VIT を編集する方法の詳細については、「脆弱性対応 での脆弱性一致アイテムの一括編集」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重要:
以下の例外を要求できます。

- Vulnerability Manager ワークスペースとIT 修復ワークスペースからの VIT。詳細については、「IT 修復ワークスペースで例外を要求する」を参照してください。
- Vulnerability Manager ワークスペースからの複数の VIT。詳細については、「脆弱性マネージャーワークスペースでの一括例外の要求」を参照してください。

手順

1. 次のように移動する。 脆弱性対応 > 脆弱性一致アイテム > **All** (すべて) をクリックし、例外を要求するアイテムを選択します。
   選択するアイテムは、[オープン]、[調査中]、または [実装待ち] ステータスである必要があります。
2. [一括編集] をクリックします。
3. フォームのフィールドに入力します。

脆弱性一致アイテムの一括編集フォーム

フィールド	説明
レコード選択	一括編集用に選択したレコード。
状態	脆弱性一致アイテムのステータス。選択したアイテムの例外を要求するには、 [保留] ステータスを選択します。
理由	選択したステータスのサブステート。
簡単な説明	作成している修復タスクの名前。
期限	例外要求に指定する終了日。
追加情報	承認者に要求の理由を通知するために記載する詳細情報。
優先ソリューション	一括編集用に選択したすべての脆弱性一致アイテムの修正を対象としたソリューション。
アサイン先グループ	VI のアサイン先グループ。グループを手動で選択するか、[アサインの推奨] が有効になっている場合はその機能を使用することができます。
作業メモ	追加するメモ。

4. **[OK]** をクリックします。
   選択した VI を含む修復タスクが作成されます。この修復タスクは承認のために送信されます。

GRC: ポリシーとコンプライアンス管理 を使用した例外の要求

脆弱性対応 内の ポリシーとコンプライアンス管理 アプリケーションの GRC ポリシー例外管理機能を使用して、ポリシー例外を要求します。

始める前に
ポリシー例外統合を使用してポリシー例外を要求する前に、ServiceNow Store から GRC: ポリシーとコンプライアンス管理 アプリケーションをダウンロードする必要があります。

必要なロール： sn_vul.remediation_owner

クラシック UI で例外を要求することもできます。手順は次のとおりです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム (または [修復タスク]>[すべて] をクリックし、例外を要求するアイテムまたはグループを開きます。
   選択するアイテムまたはグループは、[オープン]、[調査中]、または [実装待ち] ステータスである必要があります。
2. 選択したフォームで、[例外の要求] をクリックします。
3. フォームのフィールドに入力します。

[例外の要求] フォーム

フィールド	説明
ポリシー	例外を要求している脆弱性管理ポリシー。
コントロール目標	選択したポリシーに関連付けられているコントロール目標。ポリシーが選択されていない場合は、すべてのコントロール目標が一覧表示されます。
有効開始日	例外が開始される日付。デフォルト値は現在の日付です。過去の日付にすることはできません。
有効期限	ポリシー例外が期限切れになり、脆弱性一致アイテムまたはグループのステータスが [保留] から [オープン] に変更される日付。 **注:** ポリシー例外が有効である日数を、ポリシーとコンプライアンスでポリシーに設定した [最大例外期間 (日数)] を超える日数に設定することはできません。詳細については、「ポリシーの作成」を参照してください。
理由	例外を要求する理由。
理由	この要求が行われている理由に関連する詳細情報。この必須フィールドは修復オーナーが入力する必要があります。

4. **[Submit]** をクリックします。
   ポリシー例外統合および修復オーナーとコンプライアンスマネージャー間の引き渡しの詳細については、「ポリシーとコンプライアンス管理オプションのセットアップ」を参照してください。

GRC: ポリシーとコンプライアンス管理 を使用した一括例外の要求

脆弱性一致アイテムのグループを選択し、一括例外を送信します。

始める前に

ポリシー例外統合を使用して一括例外を要求する前に、ServiceNow Store から GRC: ポリシーとコンプライアンス管理 アプリケーションをダウンロードする必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
この機能を使用するには、脆弱性対応 をアップグレードする前に GRC: ポリシーとコンプライアンス管理 をアップグレードする必要があります。GRC: ポリシーとコンプライアンス管理 より前に 脆弱性対応 をアップグレードした場合、この機能を使用するには、アップグレード手順を正しい順序で再度実行する必要があります。

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

必要なロール： sn_vul.remediation_owner

脆弱性対応 のクラシック環境で例外を要求することもできます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム > **All** (すべて) をクリックし、例外を要求するアイテムを選択します。
   選択するアイテムは、[オープン]、[調査中]、または [実装待ち] ステータスである必要があります。
2. [一括編集] をクリックします。
3. フォームのフィールドに入力します。

脆弱性一致アイテムの一括編集フォーム

フィールド	説明
レコード選択	一括編集用に選択したレコード。
状態	脆弱性一致アイテムのステータス。選択したアイテムの例外を要求するには、 [保留] ステータスを選択します。
簡単な説明	作成しているタスクの名前。
優先ソリューション	一括編集用に選択したすべての脆弱性一致アイテムの修正を対象としたソリューション。
アサイン先グループ	VI のアサイン先グループ。グループを手動で選択するか、[アサインの推奨] が有効になっている場合はその機能を使用することができます。
作業メモ	追加するメモ。

4. **[OK]** をクリックします。
   選択した脆弱性一致アイテムで修復タスクが作成されます。
5. フォームのフィールドに入力します。

[例外の要求] フォーム

フィールド	説明
ポリシー	例外を要求している脆弱性管理ポリシー。
コントロール目標	選択したポリシーに関連付けられているコントロール目標。ポリシーが選択されていない場合

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	は、すべてのコントロール目標が一覧表示されます。
有効開始日	例外が開始される日付。デフォルト値は現在の日付です。過去の日付にすることはできません。
有効期限	ポリシー例外が期限切れになり、脆弱性一致アイテムまたはグループのステータスが [保留] から [オープン] に変更される日付。 **注:** ポリシー例外が有効である日数を、GRC: ポリシーとコンプライアンス管理 でポリシーに設定した [最大例外期間 (日数)] を超える日数に設定することはできません。詳細については、「ポリシーの作成」を参照してください。
理由	例外を要求する理由。
理由	この要求が行われている理由に関連する詳細情報。この必須フィールドは修復オーナーが入力する必要があります。

6. **[Submit]** をクリックします。
   ポリシー例外統合および修復オーナーとコンプライアンスマネージャー間の引き渡しの詳細については、「ポリシーとコンプライアンス管理オプションのセットアップ」を参照してください。

脆弱性対応での例外要求の承認または拒否却下

すぐに修正できない脆弱性一致アイテムまたは修復タスクの例外要求を承認または却下します。これらの要求のリスクを評価した上で、修復できるまで保留にすることを承認する必要があります。

重要:

Vulnerability Manager ワークスペースで例外要求を承認または却下できます。詳細については、「Vulnerability Manager ワークスペース で要求を承認または却下」を参照してください。

始める前に
必要なロール：sn_vul.exception_approver
クラシック環境で例外要求を承認することもできます。

注:

脆弱性対応 の v21.0 以降では、誤検出と例外を承認する期間を設定できます。また、設定した日数経過後の承認者と要求者の両方に対するメール通知も可能です。要求が発生すると、脆弱性一致アイテムが [レビュー中] ステータスに変わり、ステータス変更レコードが作成されます。設定された期間内に承認者が応答しない場合、脆弱性一致アイテムまたは修復タスクは [オープン] ステータスに戻ります。以前のステータスは **[backup_state]** フィールドに保存されます。詳細については、「例外管理の承認ルールの構成」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 自分の承認.
2. キューから要求を選択します。
3. 適切なコメントを添えて、要求を承認または却下します。

例外ルールの操作

直ちに修正も保留もできない脆弱性、脆弱性一致アイテム (VI)、または構成アイテム (CI) に対して例外を要求できます。VI 保留プロセスを自動化することで、一致する VI が識別されたときにルールに基づいてそうした VI を保留できます。

例外ルールに対し、以下のタスクを実行できます。

- 例外ルールを作成する
- 例外ルール要求を承認する
- 例外ルールのアクティブ化
- 例外ルールの再オープン
- 承認された例外ルールの更新
- 例外ルールを削除する

注:

脆弱性対応 の v21.0 以降では、誤検出と例外を承認する期間を設定できます。また、設定した日数経過後の承認者と要求者の両方に対するメール通知も可能です。要求が発生すると、脆弱性一致アイテムが [レビュー中] ステータスに変わり、ステータス変更レコードが作成されます。設定された期間内に承認者が応答しない場合、脆弱性一致アイテムまたは修復タスクは [オープン] ステータスに戻ります。以前のステータスは **[backup_state]** フィールドに保存されます。詳細については、「例外管理の承認ルールの構成」を参照してください。

例外ルールを作成する

脆弱性一致アイテム (VI) のグループについて特定の条件の例外を自動的に要求するルール (これらの VI の脆弱性重大度に基づく条件を含むルールなど) を作成します。このルールでは、新規および既存の VI が承認済みルールの条件に一致する場合に、そうした VI を自動的に保留にすることができます。

始める前に

必要なロール：sn_vul.vulnerability_admin

このタスクについて

ルールは「有効期間開始日」から「有効期限終了」の日付まで適用されます。ルールが承認されると、修復タスク (VUL) が作成されます。この VUL のグループ化方法は、例外ルールと呼ばれます。VUL は [保留] ステータスで作成されます。この VUL をクローズ、再オープン、削除することはできません。新規および再オープンされた VI は、この VUL に追加され、「有効期間開始日」から「有効期限終了」の日付でグループが期限切れになるまで保留されます。

注:

メール通知は、例外ルールワークフローのすべてのステージで送信されます。こうしたメールには、要求のステータスとその他の詳細が記載されています。たとえば、例外ルールが要求されると、要求が送信されたことを確認するメールが要求者に届きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
ルールが却下された場合は、[ドラフト] ステータスで再オープンして更新し、承認のために再送信できます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 例外ルール.
2. 例外ルールの新規レコードページで、[新規] をクリックしてルールを作成します。
3. フォームのフィールドに入力します。

例外ルールフォーム

フィールド	説明
名前	例外ルールの名前。
有効開始日	このルールがアクティブになり、VI が保留される開始日付。
有効期限	修復タスクが新しい VI の受け入れを停止する日付。
理由	この例外ルールを作成する理由。
アサイン先グループ	保留された VI の追跡用に作成された修復タスクがアサインされているグループ。
追加情報	要求者が承認者に提供する追加情報。この情報は、修復タスクの説明フィールドに入力されます。
条件	VI の処理中に定義できる VI のフィルター条件。
既存のデータで実行	このルールが初めて実行されるときに既存のデータでこのルールを実行できるようにするオプション。
ワークフローステージ	例外ルールの現在の承認ステータス。
状態	例外ルールのステータス。
実行順序	各例外ルールの一意の順序。
保留期限	VUL および VI の保留期限となる日付。この日付になると、作成された VUL がクローズされ、すべての VI がグループから離脱し、グループルールが再適用されます。

4. ルールの作成時にアサイン先グループを追加します。
5. フォームを承認のために送信します。
   要求のステータスが [レビュー中] に変わります。例外ルールを送信するまで、[ドラフト] ステータスのままになります。

例外ルール要求を承認する

ユーザーからの例外ルール要求を評価して、こうした要求を承認または却下できるようにします。

始める前に
必要なロール：sn_vul.exception_approver

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタスクについて

例外承認者レベル 1 ユーザーグループのメンバーは、レベル 1 の例外ルール要求を承認できます。同様に、例外承認者レベル 2 ユーザーグループのメンバーは、レベル 2 の例外ルール要求を承認できます。デフォルトでは、両方のユーザーグループが例外承認者ロールを継承します。

注:

VR アプリケーションを初めて展開する場合は、例外管理のフローデザイナーがデフォルトで有効になります。既にワークフローを使用している場合は、フローデザイナーに更新できます。どちらの場合も、ワークフローに戻すことはできません。例外管理と誤検出の承認ルールを設定するには、「例外管理の承認ルールの構成」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 自分の承認.
2. キューから要求を選択します。
3. 要求を承認または却下し、要求を承認または却下した理由を説明します。
   例外ルールが承認されると、デフォルトでは修復タスク (RT) が [保留] ステータスで作成されます。「有効期間開始日」以降は、作成されたすべての VI と、ステータスが「クローズ済み」から「オープン」に移行した VI に対して、このルールが実行されます。定義された条件に一致する VI が RT に追加され、指定された期間保留されます。

   注:
   ルールが却下された場合は、[ドラフト] ステータスで再オープンして更新し、承認のために再送信できます。

例外ルールのアクティブ化

ルールは「有効開始日」にアクティブ化されます。アクティブ化すると、脆弱性一致アイテム (VI) の例外プロセスが自動化されます。

例外ルールのライフサイクルは次のとおりです。

1. 作成または再オープンされた、指定された条件を満たす新しい脆弱性一致アイテム (VI) は保留されます。例外ルールを初めて実行するときに [既存のデータで実行] オプションを有効にすると、例外ルールの条件に一致するすべてのアクティブな VI と保留されていない VI は新しく作成された修復タスク (RT) に移動され、そのステータスは [保留] に変更されます。
2. 新しく作成された VI が例外ルールの条件に一致する場合、その VI はルールに関連付けられている保留された RT に移動され、グループルールは実行されません。
3. 「有効期限開始」の日付で [既存のデータで実行] オプションを有効にすると、既存の VI が追加されます。
4. 「有効期限」の日付でルールが期限切れになると、RT は新しい VI の受け入れを停止します。RT は「保留期限」の日付まで存在し続けます。
5. 例外ルールは「有効期限」の日付で期限切れになります。

例外ルールの延長の要求

保留された例外ルールがその保留された期限に達する前に、この例外ルールの延長を要求します。修復オーナーは、この要求を行うために保留期日まで待つ必要がなくなりました。

始める前に

必要なロール：sn_vul.exception_approver

このタスクについて

脆弱性対応 ワークスペースから延長を要求することもできます。詳細については、「脆弱性マネージャーのワークスペースでの保留された脆弱性一致アイテムの延長の要求」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 例外ルール.
2. 承認済みの例外ルールを選択します。
3. [拡張を要求] を選択します。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
拡張期限	例外ルールを延長する必要がある期限の日付を選択します。
理由	例外ルールを保留する理由を入力します。 次の選択肢があります。 ○ リスクの受容 ○ メンテナンス期間待ち ○ 修正が利用不可 ○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

5. [要求承認] を選択します。
要求が承認されると、例外ルール、関連する修復タスク、および脆弱性一致アイテムの [保留期限]、[理由]、および [補足情報] フィールドが更新されます。要求が送信され、承認者によって後続のアクションが実行されると、メールがトリガーされます。

注:

- 要求は 2 段階の承認を経過します。
- [拡張を要求] ボタンは、例外ルールの一部として作成された修復タスクでは使用できません。
- 保留された例外ルールが再度延長されると、バックエンドで延長保留カウントが増加します。
- 脆弱性対応 の v21.0 以降では、誤検出と例外を承認する期間を設定できます。また、設定した日数経過後の承認者と要求者の両方に対するメール通知も可能です。要求が発生すると、脆弱性一致アイテムが [レビュー中] ステータスに変わり、ステータス変更レコードが作成されます。設定された期間内に承認者が応答しない場合、脆弱性一致アイテムまたは修復タスクは [オープン] ステータスに戻ります。以前のステータスは **[backup_state]** フィールドに保存されます。詳細については、「例外管理の承認ルールの構成」を参照してください。

例外ルールの再オープン

却下されたけれども再送信したい例外ルールを再オープンします。ルールを再オープンすると、[ドラフト] ステータスに移行します。

始める前に
必要なロール：sn_vul.vulnerability_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタスクについて
次に、承認のためにルールを更新して再送信できます。

手順
1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 例外ルール.
2. 再オープンするルールを検索し、[再オープン] をクリックします。
3. フォームを更新し、承認のために再送信します。

承認された例外ルールの更新

承認されたルールをキャンセルすると更新できるようになります。たとえば、日付を変更したり、承認済みルールに条件を追加したりする場合は、そのルールをキャンセルして修復タスク (VUL) を削除し、脆弱性一致アイテム (VI) を [オープン] ステータスに移行する必要があります。

始める前に
必要なロール：sn_vul.vulnerability_admin

このタスクについて
グループルールがこうした VI に再適用されます。変更を行った後にルールを送信し、承認プロセスをもう一度繰り返します。

手順
1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 例外ルール.
2. キャンセルする例外ルールを開き、[キャンセル] をクリックします。
3. [ルールをキャンセル] ダイアログボックスで、[ルールをキャンセル] をクリックします。
   ルールが [ドラフト] ステータスに戻り、関連する VUL が削除されます。関連する VI が再オープンされ、グループルールが個々の VI に適用されます。

例外ルールを削除する

不要になった例外ルールを削除します。たとえば、取り込み中に脆弱性一致アイテム (VI) を保留しない場合は、ルールを削除できます。

始める前に
必要なロール：sn_vul.vulnerability_admin

このタスクについて
ルールを削除すると、関連する修復タスク (VUL) がキャンセルされます。関連する VI が再オープンされ、グループルールが個々の VI に適用されます。

手順
1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 例外ルール.
2. 削除する例外ルールを開き、[削除] をクリックします。
3. [削除ルール] ダイアログボックスで、[削除ルール] をクリックして、選択したルールを削除します。
   関連する修復タスクも削除されます。関連する VI が再オープンされ、グループルールが個々の VI に適用されます。

誤検出のマークと承認

脆弱性一致アイテム (VI) と修復タスク (VUL) は誤検出としてマークできます。書き込みアクセス権を持つ承認者は、他のユーザーからのそのような要求を承認できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 誤検出としてマーク
- 誤検出の一括編集
- 誤検出の承認または却下

注:

誤検出ワークフローの全ステージでメール通知が送信され、要求のステータスやその他の詳細情報が通知されます。たとえば、VI または修復タスクが誤検出としてマークされると、要求者は確認メールを受信します。同時に、承認者は、VI または修復タスクが誤検出としてマークされたことを示すメールを受信します。

脆弱性対応 の v21.0 以降では、誤検出と例外を承認する期間を設定できます。また、設定した日数経過後の承認者と要求者の両方に対するメール通知も可能です。要求が発生すると、脆弱性一致アイテムが [レビュー中] ステータスに変わり、ステータス変更レコードが作成されます。設定された期間内に承認者が応答しない場合、脆弱性一致アイテムまたは修復タスクは [オープン] ステータスに戻ります。以前のステータスは **[backup_state]** フィールドに保存されます。詳細については、「例外管理の承認ルールの構成」を参照してください。

誤検出としてマーク

スキャナーによって発出された警告が実際には問題ではない場合、脆弱性一致アイテム (VI) または修復タスク (VUL) を誤検出としてマークします。たとえば、構成アイテムが廃止されてもスキャナーでそのアイテムに関連する問題がまだ発生している場合は、誤検出としてマークします。

始める前に
必要なロール：修復オーナー
脆弱性対応 ワークスペースから誤検出を要求できます。「脆弱性一致アイテムまたは修復タスクの誤検出を要求する」を参照してください。

クラシック環境の誤検出を要求することもできます。

手順

1. 次のように移動する。 脆弱性対応 > 脆弱性一致アイテム (または修復タスク) > **All** (すべて).
2. 誤検出としてマークする VI または VUL を開き、[誤検出としてマーク] をクリックします。
   VI または VUL は [オープン] ステータスである必要があります。
3. [誤検出] フォームで、[追加情報] に詳細を入力し、[承認要求] をクリックします。
   要求が承認のために送信され、VI または VUL のステータスが [レビュー中] に変わります。

誤検出の一括編集

一括編集を使用して、複数の脆弱性一致アイテム (VIT) を誤検出としてマークします。複数の VIT が選択されている場合、これらのアイテムで修復タスクが形成されます。

重要:
アドミンまたはアナリストは、脆弱性マネージャーワークスペースの一括編集機能を使用して、複数の VIT を誤検出としてマークできます。詳細については、「脆弱性マネージャーワークスペースで誤検出を一括編集」を参照してください。

始める前に
必要なロール：修復オーナー
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

クラシック環境の誤検出を要求することもできます。

手順

1. 次のように移動する。 脆弱性対応 > 脆弱性一致アイテム > **All** (すべて) をクリックし、誤検出としてマークするアイテムを選択します。
   選択するアイテムは、[オープン]、[調査中]、または [実装待ち] ステータスである必要があります。
2. [一括編集] をクリックします。
3. フォームのフィールドに入力します。

脆弱性一致アイテムの一括編集フォーム

フィールド	説明
レコード選択	一括編集のために選択したレコード。
状態	脆弱性一致アイテムのステータス。誤検出としてマークするには、 [クローズ済み] を選択します。
理由	選択したステータスのサブステート。[ステータス] として [クローズ済み] を選択した場合は、ここで [誤検出] を選択し、誤検出としてマークします。
未アサイン	要求を送信して [アサイン先] フィールドと [アサイン先グループ] フィールドをクリアします。
優先ソリューション	一括編集用に選択したすべての脆弱性一致アイテムの修正を対象としたソリューション。
アサイン先グループ	VI のアサイン先グループ。手動で選択するか、有効になっている場合は [アサインの推奨] を使用します。
作業メモ	追加するメモ。

4. **[OK]** をクリックします。
   選択した VI を含む新しい修復タスクが作成され、このタスクが承認のために送信されます。

誤検出の承認または却下

誤検出承認者は、他のユーザーからの誤検出要求を承認または却下できます。

重要:

誤検出承認者は、 Vulnerability Manager ワークスペースで誤検出要求を承認または却下できます。詳細については、「Vulnerability Manager ワークスペース で要求を承認または却下」を参照してください。

始める前に
必要なロール：

- sn_vul.false_positive_approver (脆弱性一致アイテムの場合)
- アプリケーション脆弱性一致アイテムの sn_vul.app_false_positive_approver

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性 > 自分の承認.
2. キューから要求を選択します。
3. 適切なコメントを添えて、要求を承認または却下します。

> **注:**
> 誤検出は期限を定めることができます。承認者のみが終了日を設定できます。

脆弱性対応 のアナリティクスおよびレポート作成ソリューション

脆弱性修復の監視には、傾向の表示、リスクの管理、およびアサイン先グループの監視が含まれます。高リスクの問題、アサイン先グループの作業負荷、保留、および再発する脆弱性を確認できます。脆弱性対応 は、そのプロセスをより生産的かつ効率的にするためのツール、レポート、および手順を提供します。

脆弱性対応 のワークスペースのデータの可視化

脆弱性対応 ワークスペースには、修復の進捗状況を監視するのに役立つデータの可視化が含まれています。脆弱性データの変更に応じて更新される動的なデータ表示で組織にとって重要なアクティブな脆弱性の数と重大度を表示することで、組織に対する脅威のレベルを判断できます。利用可能な動的なデータ可視化の詳細については、「Vulnerability Manager ワークスペース」および「IT 修復ワークスペース の探索」を参照してください。

脆弱性アナリストは、デフォルトの 脆弱性対応 ダッシュボードを使用することもできます **All** (すべて) > 脆弱性対応 > 概要.

> **重要:**
>
> 脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で表示することもできます。新しい UI でダッシュボードを表示するには、次に移動します: ワークスペース > 脆弱性マネージャーワークスペース をクリックし、[ダッシュボード] アイコンをクリックします。ロールに応じてデフォルトのダッシュボードが表示されます。他のダッシュボードを表示するには、ダッシュボード名の横にあるドロップダウンをクリックします。詳細については、「脆弱性マネージャーワークスペースのダッシュボード」および「IT 修復ワークスペースのダッシュボード」を参照してください。
>
> > **注:**
> > Tokyo を使用している場合は、ネクストエクスペリエンス UI でダッシュボードを表示できますが、一部の機能が失われます。

脆弱性対応 修復プロセス

ほとんどの脆弱性修復は、脆弱性対応 ワークスペース内の修復タスクレコードから行われます。「調査中」ステータスの修復タスク (RT) から、いくつかのタスクを実行できます。

- 変更要求を作成します。
- 修復タスク内に作業メモと脆弱性の説明を追加します。
- 修復タスクとその中の脆弱性一致アイテムを後日まで保留します。
- 修復タスクをクローズします。
- 通常は時間的制約のある新しい規制コンプライアンス義務を追跡します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 脆弱性対応 インスタンスにログインします。
- Vulnerability Management とサードパーティのダッシュボードおよびレポートを確認して、問題領域を特定します。たとえば、状況別の修復タスク (RT) の経過時間や、修復ターゲット日を過ぎた高リスク脆弱性一致アイテム (VI) を示すダッシュボードを表示します。
- 修復タスクのステータスをリスク順に確認します。
- リスクスコアが正しく計算されていない場合はリスクスコア算出を調整するか、必要に応じて VI または RT を保留して、タスクの優先順位付けを変更します。これらのオプションの詳細については、「脆弱性対応 の算出と脆弱性算出ルール」または「修復タスクの保留」を参照してください。
- 再開しようとしている保留された脆弱性一致アイテムを確認し、必要に応じてさらにアクションを実行します。資産、修復タスク、および対応する脆弱性一致アイテムに対して変更アクティビティを開始し、追跡する場合の詳細については、「脆弱性対応 の変更管理」を参照してください。
- IT 運用からのフィードバックを確認します。

  変更要求が解決されたことが通知されたら、次のスキャンを待ちます。スキャンは、セットアップアシスタントで設定されているサードパーティのスケジュール済みインポートによって自動的にトリガーされます。

- スキャン後、ステータスが [修正済み] の場合、インポート中に脆弱性一致アイテムが自動的にクローズされます。グループ内のすべての脆弱性一致アイテムが修正されると、グループはクローズされます。
- スキャン後、ステータスが [修正済み] でない場合、VI は自動的に [調査中] に戻ります。
- インスタンスで [解決済み] に設定されているがサードパーティの統合実行によって [クローズ済み]/[修正済み] に移行されていない脆弱性一致アイテムは、再スキャン中に検出された場合に再オープンされます。

  Qualys 検出で、[解決済み] に設定された VI が後続のスキャンで [クローズ済み]/[修正済み] に移行されていない場合、最終検出日が解決日より後であると、これらの VI が [オープン] に戻ります。

  Rapid7 検出では、インスタンスの Rapid7 構成ページに、解決済みの VI を経過時間別に再オープンするオプションが利用可能になりました。有効にすると、[解決済み] に設定されていても、後続のスキャンで [クローズ済み]/[修正済み] に移行されていない VI は、入力した日数の経過後に [オープン] に戻ります。

脆弱性ソリューション管理 展開の進捗状況

修復タスクと脆弱性エントリーの包括的な展開メトリクスは、脆弱性ソリューション管理 の脆弱性および脆弱性一致アイテムの [修復ステータス] に含まれています。解決の進行を遅らせている修復タスクまたは脆弱性が簡単に特定できます。脆弱性をどのように特定するか、または影響を受ける資産のどの部分が修復の問題を引き起こしている可能性があるかをドリルダウンします。脆弱性、ソリューション、および修復タスクフォームの [ステータスを更新] 関連リンクを使用して、メトリクスのステータスを更新します。

デフォルトの 脆弱性対応 ダッシュボードを使用する

脆弱性対応 概要ダッシュボード (脆弱性管理) では、脆弱性と脆弱性一致アイテムに関するエグゼクティブビューが用意されており、脆弱性アドミニストレーターが懸念事項をすばやく特定するのに役立ちます。脆弱性対応 修復ダッシュボード (脆弱性修復) を使用すると、修復スペシャリストが担当するする修復タスクと脆弱性一致アイテムに集中できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性対応 のワークスペースのデータの可視化

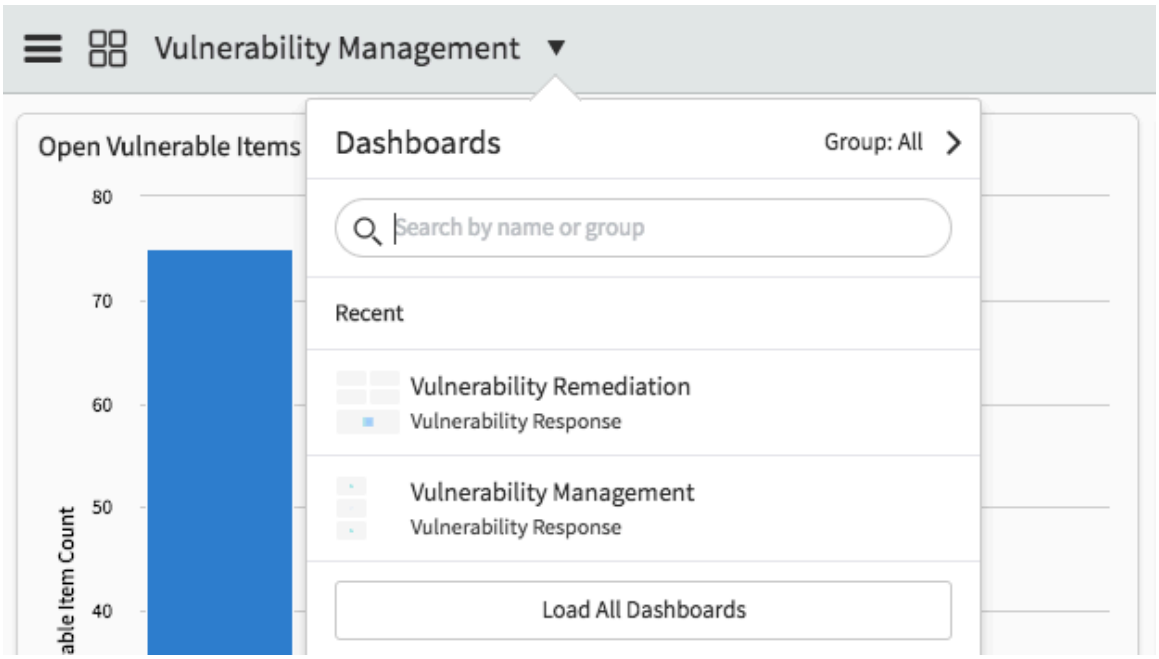
脆弱性対応 ワークスペースには、修復の進捗状況を監視するのに役立つデータの可視化が含まれています。脆弱性データの変更に応じて更新される動的なデータ表示で組織にとって重要なアクティブな脆弱性の数と重大度を表示することで、組織に対する脅威のレベルを判断できます。利用可能な動的なデータ表示方法の詳細については、「脆弱性対応 ワークスペース」、「Vulnerability Manager ワークスペース」および「IT 修復ワークスペース の探索」を参照してください。

脆弱性アナリストは、デフォルトの 脆弱性対応 ダッシュボードを使用することもできます。

必要なロール：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst、および sn_vul.vulnerability_read を持つ (または sn_vul.vulnerability_read ロールを継承する) ユーザー、および pa_viewer。

レガシー環境におけるデフォルトの 脆弱性対応 ダッシュボード

これらのレポートは 脆弱性対応のパフォーマンスアナリティクス アプリケーションの一部として含まれており、別のサブスクリプションは必要ありません。開くには、選択リストを選択して展開し、ダッシュボードを選択します。または、検索フィールドにダッシュボードの名前を入力します。



注:

脆弱性対応 アプリケーションの パフォーマンスアナリティクス コンテンツパックをインストールしてアクティブ化すると、脆弱性管理 (PA) ダッシュボードが概要モジュールに自動的に表示されます。このダッシュボードには、脆弱性管理ライフサイクルのすべてのステージをカバーするレポートが含まれています。

脆弱性対応 のパフォーマンスアナリティクスコンテンツパックに含まれるレポートについては、「Vulnerability Management [PA] dashboard (脆弱性管理 (PA) ダッシュボード)」を参照してください。

CISO ダッシュボードおよびスキャン範囲レポートについては、「Vulnerability Management CISO dashboard (脆弱性管理 CISO ダッシュボード)」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

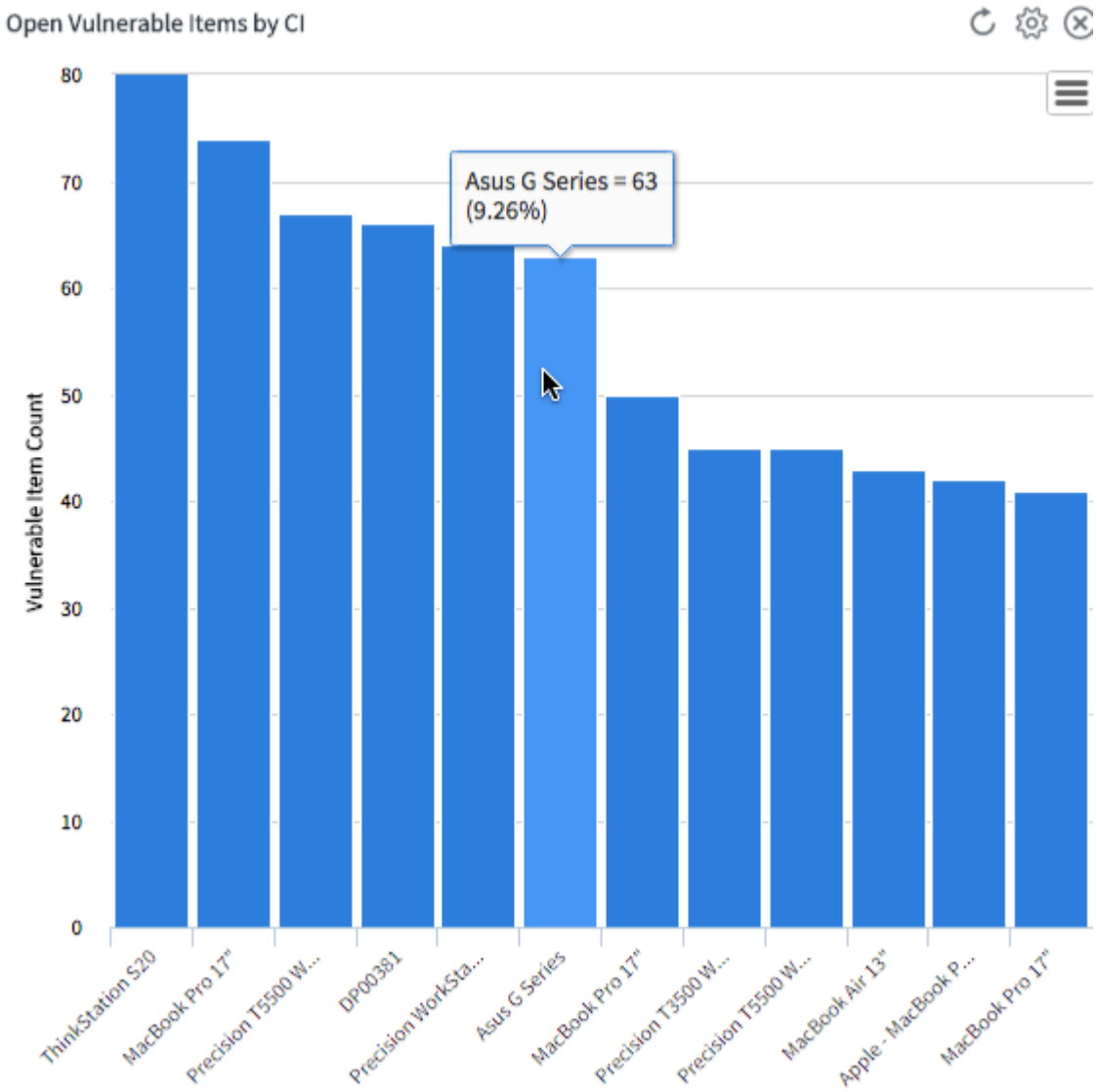
自動翻訳

脆弱性管理ダッシュボード

各チャートで、チャートの任意の部分 (棒、円、データポイントなど) をポイントして、その部分に固有の一般的なデータを表示できます。レポートの任意の部分をクリックすると、詳細な情報を提供するリストが開きます。

注:

ダッシュボードのカスタマイズが必要な場合、詳細については「Create and use dashboards (ダッシュボードを作成および使用する)」を参照してください。



脆弱性概要レポート

名前	ビジュアル	説明
CI 別のオープンな脆弱性一致アイテム	棒グラフ	構成アイテム (CI) ごとに記録されたオープンな脆弱性一致アイテムの数を多い順に表示します。
修復ターゲットステータス別の脆弱性一致アイテム	棒グラフ	[ターゲット間近]、[ターゲット内]、および [過去のターゲット] である脆弱性一致アイテムの数を表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性概要レポート (続く)

名前	ビジュアル	説明
		注: [保留]、[解決済み]、または [クローズ済み] ステータスのアイテムは含まれません。
今週期限切れになる保留脆弱性一致アイテム	グラフ	7 日以内の再アクティブ化がスケジュール設定されている保留された脆弱性一致アイテムの数を表示します。
脆弱性別のオープンな脆弱性一致アイテム	棒グラフ	脆弱性ごとにオープンな脆弱性一致アイテムの数を多い順に表示します。
モデル別の脆弱性	棒グラフ	モデル (CI クラス) ごとに記録された脆弱性一致アイテムの数を多い順に表示します。
週別の脆弱性	傾向図	毎週記録された脆弱性エントリーの数を表示します。
最も脆弱なモデル	ドーナツグラフ	最も脆弱性一致アイテムを含むモデル (CI クラス) を表示します。
公開者別の脆弱性	棒グラフ	公開者ごとに記録された脆弱性一致アイテムの数を多い順に表示します。
影響度別の脆弱性	棒グラフ	影響を受けるネットワークタイプの脆弱性エントリーの数を表示します。
最も脆弱な公開者	ドーナツグラフ	最も脆弱性一致アイテムを含む公開者を表示します。
最も脆弱な CI	ドーナツグラフ	最も脆弱な CI を含むモデルを表示します。
スコア別の脆弱性	棒グラフ	脆弱性スコア別の脆弱性エントリーの数を表示します。
再オープンされた脆弱性一致アイテム	リスト	再オープンされた脆弱性一致アイテムとその経過時間を一覧表示します。
クラス別の最も脆弱な CI	ドーナツグラフ	最も脆弱な CI を含むモデルを表示します。
脆弱性一致アイテムの経過時間	リスト	脆弱性一致アイテムが最後にオープンされて以降の日数を一覧表示します。
日付別の脆弱性を伴う CI	リスト	過去 30 日以内にスキャンされた構成アイテムを一覧表示します。
CI がスキャンされていません	リスト	脆弱性がスキャンされたことがない構成アイテムを一覧表示します。

脆弱性修復ダッシュボード

脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で使用可能です。

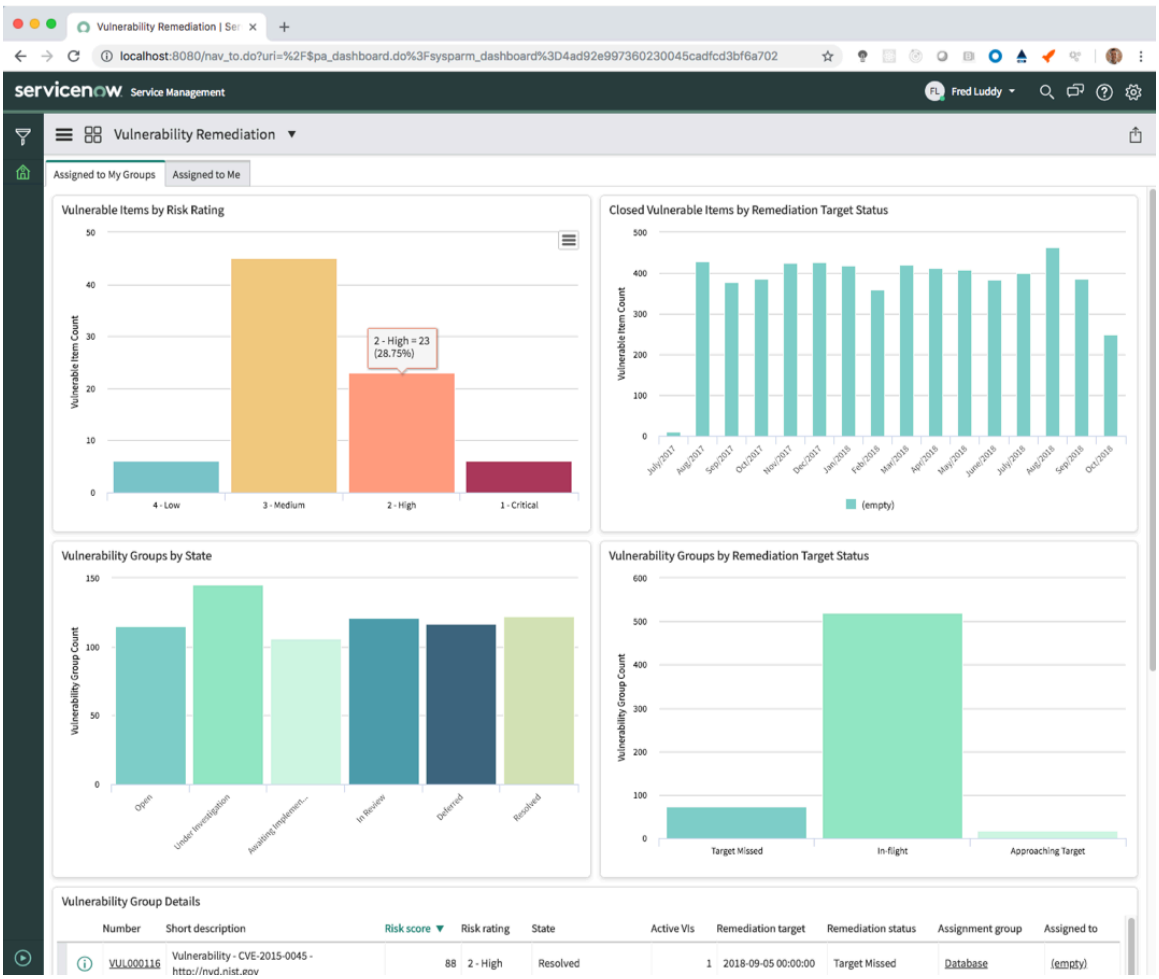
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
Tokyo を使用している場合は、Next Experience UI でダッシュボードを表示できますが、一部の機能が失われます。

脆弱性修復ダッシュボードには、[所属グループにアサイン済み]、[自分にアサイン済み]、および [自分からの要求] のタブが含まれています。[所属グループにアサイン済み] および [自分にアサイン済み] タブには同じレポートが表示されます。前者のタブには所属するアサイン先グループ別のレポート、後者には自分にアサインされた脆弱性一致アイテムまたは修復タスク別のレポートが示されます。[自分からの要求] タブには、要求した誤検出と例外が表示されます。

脆弱性修復ダッシュボード



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レポート

[所属グループにアサイン済み] および [自分にアサイン済み]

名前	ビジュアル	説明
リスク評価別の脆弱性一致アイテム	棒グラフ	選択した時間スパンにおけるリスク評価によってグループ化された、アクティブな脆弱性一致アイテムの数。
修復ターゲットステータス別のクローズされた脆弱性一致アイテム	棒グラフ	選択した時間スパンにおける修復ターゲットステータスによってグループ化された、クローズされた脆弱性一致アイテムの数。
ステータス別の修復タスク	棒グラフ	ステータスごとにグループ化されたアクティブな修復タスク (RT) の数。
修復ターゲットステータス別の修復タスク	棒グラフ	修復ターゲットステータスごとにグループ化されたアクティブな RT の数。 このレポートでは、保留された脆弱性一致アイテムは除外されます。
修復タスクの詳細	リスト	リスト内の修復タスクレコードの詳細。

自分からの要求

名前	ビジュアル	説明
例外および誤検出要求のステータス	棒グラフ	自分からのアクティブな要求の数。
期限切れ間近の保留および誤検出修復タスク	棒グラフ	[期限日] でグループ化された保留および誤検出の修復タスク (RT) の数。

脆弱性の承認ダッシュボード

脆弱性の承認ダッシュボードには、例外および誤検出承認者に関する次のレポートが含まれています。

脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で使用可能です。

注:
Tokyo を使用している場合は、Next Experience UI でダッシュボードを表示できますが、一部の機能が失われます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	ビジュアル	説明
自分の承認処理待ちの時間別の例外および誤検出要求	棒グラフ	作成日別にグループ化された、自分の処理待ちの承認の数。
自分の承認および却下された例外と誤検出要求	棒グラフ	承認ステータス別にグループ化された、承認および却下された承認要求の数。
承認処理待ちのリスク評価別のすべての修復タスク	棒グラフ	リスク評価別にグループ化された、承認処理待ちの修復タスクの数。
理由別にグループ化された、すべての処理待ちおよび誤検出の承認要求	棒グラフ	理由別にグループ化された処理待ちの承認要求の数。

脆弱性管理のための プラットフォームアナリティクスソリューション

プラットフォームアナリティクスソリューション には、他の Now Platform 製品とともに使用するために、パッケージ化された パフォーマンスアナリティクス と レポート のコンテンツが含まれています。 このアナリティクスおよびレポートのソリューションで、脆弱性のボリューム、パフォーマンス、および初期分析と検出から封じ込めや修復までの進捗状況を追跡できるようになります。アサイン先グループやエクスプロイト、リスク評価、ステータスでレポートをフィルタリングできます。

脆弱性対応のパフォーマンスアナリティクス コンテンツパックは、脆弱性対応 アプリケーションと一緒に自動的にはインストールされません。ServiceNow Store で、別のサブスクリプションとして利用できます。

脆弱性対応のパフォーマンスアナリティクス には次の 2 つのダッシュボードがあります。

- 脆弱性管理 (PA) ダッシュボード
- 脆弱性管理担当最高情報セキュリティ責任者 (CISO) ダッシュボード

必要なロール、インストール、およびダッシュボードの表示

このソリューションには、次のロールとタスクが関連付けられています。

- Now Platform 管理者 (admin)：この分析およびレポートのソリューションをインストールしてアクティブ化し、システムプロパティに必要な変更を加えます。
- パフォーマンスアナリティクス アドミン (pa_admin)：インジケーター、ブレークダウン、ウィジェット、およびダッシュボードを確認します。データ収集を設定して開始します。適切なステークホルダーとダッシュボードを共有します。

このアプリケーションをインストールするには、「脆弱性対応のパフォーマンスアナリティクス [PA] レポートのリアルタイム表示」を参照してください。

注:
非本番インスタンスでアナリティクスおよびレポートのソリューションを設定してテストしてから、本番環境で有効化してください。

アナリティクスおよびレポートのソリューションには、デフォルトアプリケーションの分析に必要なすべての設定レコードが用意されています。本番環境で使用するために、これらのレコードをカスタマイズします。詳細については、「分析およびレポートソリューションの構成」を参照してください。

脆弱性管理 (PA) ダッシュボードを表示するには、次に移動します: 脆弱性対応 > 概要 > .

脆弱性管理 CISO ダッシュボードを表示するには、次に移動します: 脆弱性対応 > **CISO** ダッシュボード > .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

主要な用語

パフォーマンスアナリティクス (PA)

管理ダッシュボードを作成し、KPI とメトリクスに関するレポートを作成し、重要なビジネス上の質問に回答することで、品質向上とコスト削減に役立つソリューション。

脆弱性一致アイテム (VI)

構成アイテム (CI) に存在する、サードパーティの脆弱性スキャナーによって報告されたセキュリティ脆弱性。☒

修復タスク

修復タスクは、脆弱性一致アイテムに関連付けられているグループに基づいて修復作業の中で作成され、IT チームに自動的にアサインされます。IT チームと修復責任者には、[IT 修復ワークスペース] に修復タスクが表示されます。詳細については、「脆弱性対応 ワークスペース」を参照してください。

。

PA インジケーター☒

ビジネスサービス、アクティビティ、または組織の動作の定期的な間隔で実行されるパフォーマンス測定値 ([保留されていない期限切れの重大な脆弱なアイテム] など) を定義します。

PA インジケーターソース

1 つのテーブルまたはデータベースのビューからレコードをフィルタリングするデータセット (VI アクティブなど)。

データの可視化をリアルタイムで表示

脆弱性対応 アプリケーションの最も重要なアイテムでそのとき起きていることを確認するには、脆弱性管理 (PA) ダッシュボードで特定のレポートをリアルタイムで表示します。これらのレポートを臨機応変に確認することで、最も重要な脆弱性一致アイテム (VI) を管理し、迅速に修正することができます。リアルタイムで表示できるレポートは次のとおりです。

- [概要] タブ：アサイン先グループ別の脆弱性一致アイテム
- [脆弱性一致 CI] タブ
  - 所有者のいない脆弱性一致構成アイテム (CI) (Vulnerable Configuration Items (CIs) without Owners)
  - アクティブな VI を持つ廃止または盗難された CI
- [例外] タブ
  - 理由別の保留された脆弱なアイテム
  - 期限切れ間近の保留要求 (Deferral Requests About to Expire)
  - CIO マネージャーによって保留された脆弱なアイテム (Deferred Vulnerable Items by CIO Manager)
- [修復] タブ：未アサインの脆弱なアイテム

詳細については、「脆弱性対応のパフォーマンスアナリティクス [PA] レポートのリアルタイム表示」を参照してください。

関連情報

アナリティクスおよびレポートのソリューション

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性管理 **CISO** ダッシュボード

脆弱性管理 CISO ダッシュボードでは、ユーザーが脆弱性の修復について重要業績メトリクス(KPI)などのデータを表示し、最も高いリスクやスキャン範囲を確認し、リスクを下げる方法を学ぶことができます。

必要な **Now Platform** ロール

- ダッシュボードを表示するための sn_vul.vulnerability_ciso
- ダッシュボードを編集するための sn_vul.ciso_write

CISO ダッシュボードの有効化

CISO ダッシュボードを有効にするには、脆弱性対応 のパフォーマンスアナリティクスをインストールし、パフォーマンスアナリティクスの対応するジョブを有効にする必要があります。詳細については、「Analytics and Reporting Solutions for Vulnerability Response (脆弱性対応のアナリティクスおよびレポートのソリューション)」を参照してください。

ユースケース

ユーザー	ダッシュボードの使用法
最高情報セキュリティ責任者 (CISO)	最高情報セキュリティ責任者 (CISO) は、CISO ダッシュボードを使用して、組織の脆弱性管理プログラムに関するインサイトを得ることができます。 このダッシュボードには、CISO が自社の環境の脆弱性を軽減する方法を一目で確認するために役立つデータが表示されます。

CISO ダッシュボードの使用方法

組織の最高情報セキュリティ責任者 (CISO) などの重役ユーザーは、Vulnerability Response の CISO ダッシュボードを見ることで、自社の脆弱性管理プログラムの有効性を把握できます。CISO ダッシュボードを表示するには、次の場所に移動します。 脆弱性対応 > **CISO** ダッシュボード. 最上位のフィルターを使用して、リスク評価、経過時間範囲、またはインターネットフェーシングを基準にレポートをフィルタリングします。レポートによっては、ある一定期間の傾向データが表示されます。重要なメトリクスの傾向を定期的に見たり、全体的なビジネス上のセキュリティリスクを分析したり、改善が必要な領域を特定したりできます。

脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で表示することもできます。新しい UI でダッシュボードを表示するには、次に移動します: ワークスペース > 脆弱性マネージャーワークスペース をクリックし、[ダッシュボード] アイコンをクリックします。ロールに応じてデフォルトのダッシュボードが表示されます。他のダッシュボードを表示するには、ダッシュボード名の横にあるドロップダウンをクリックします。詳細については、「脆弱性マネージャーワークスペースのダッシュボード」および「IT 修復ワークスペースのダッシュボード」を参照してください。

注:
Tokyo を使用している場合は、ネクストエクスペリエンス UI でダッシュボードを表示できますが、一部の機能が失われます。

スケジュール済みジョブの実行

次の順序でスケジュール済みジョブを実行して、レポートのデータを更新します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

1. ダッシュボードのテーブルの更新 (Update dashboard tables)
2. [PA VR] CISO ダッシュボード

CISO ダッシュボードのスケジュール済みジョブ

スケジュール済みジョブの名前	説明
ダッシュボードのテーブルの更新 (Update dashboard tables)	CISO データを収集するために、[PA VR] CISO ダッシュボードのジョブの前に実行する必要がある日次スケジュール済みジョブ。このスケジュール済みジョブを実行すると、[スキャン範囲] レポートが更新されます。 更新される情報には、過去 90 日間にスキャンされた運用中の構成アイテム (CI)、そのクラス、およびこれらのクラスに対応する運用中の CI の合計数が含まれます。このスケジュール済みジョブを実行すると、[推奨アクション] タブのレポートも更新されます。 **注:** 運用中 CI は、運用ステータスが [稼働] である CI を指します。
[PA VR] CISO ダッシュボード	[ダッシュボードのテーブルの更新 (Update dashboard tables)] のスケジュール済みジョブが完了したら、このスケジュール済みジョブを実行して、**[CISO** 概要] タブのすべてのレポートに入力します。

[CISO ダッシュボード] のタブ

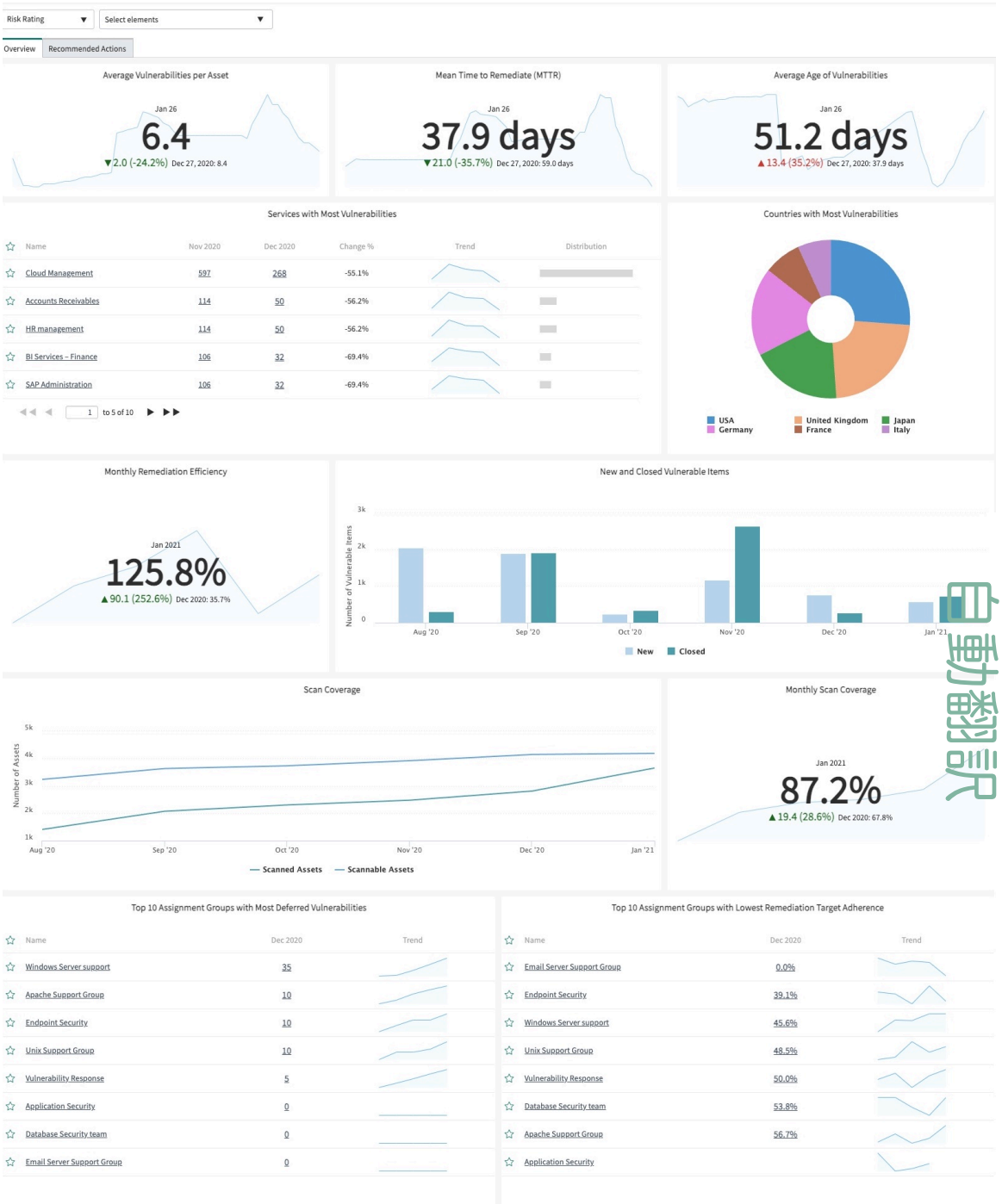
このダッシュボードは、脆弱性管理に存在するリスクに関するインサイトを提供します。脆弱性とそれに関連するデータを、地域、経過時間、サービス、その他のブレークダウンごとに見ることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[概要] タブ

[概要] タブには、組織のセキュリティ体制を一目で把握できるレポートが表示されます。

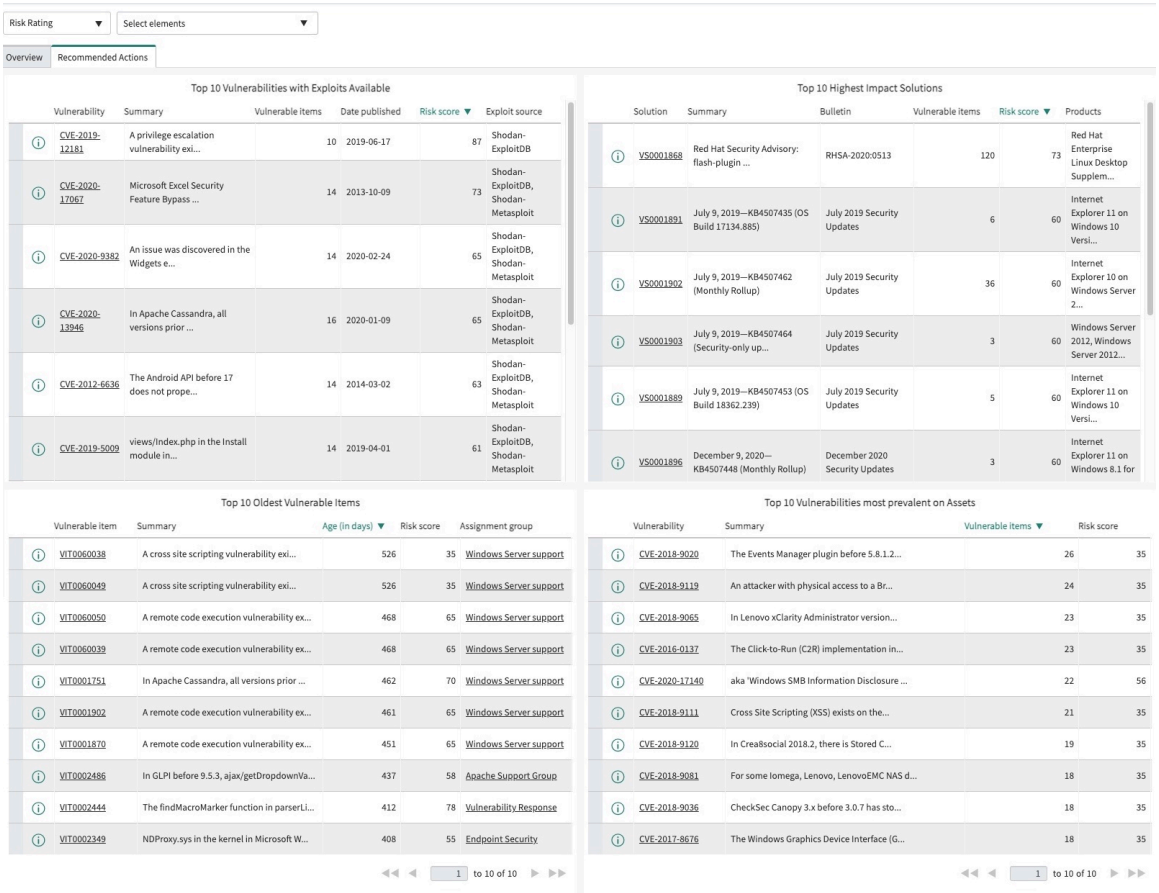


注:
最上位のフィルターは一部のレポートでのみ使用できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[推奨アクション] タブ

[推奨アクション] タブには、悪用可能な脆弱性や、発生してから時間の経った脆弱性、およびまん延している脆弱性に関するインサイトを示すレポートが表示されます。また、リスクを軽減するためのアクションを推奨する解決策も示されます。**[CISO** ダッシュボードのテーブルの更新] のスケジュール済みジョブを実行して、このタブのレポートを更新します。



インジケーター

インジケーターを表示するには、次に移動します: パフォーマンスアナリティクス > インジケーター.

1. [インジケーター] ページで、 [名前] 列で必要なインジケーター名を検索します。
2. インジケーター名をクリックすると、そのレコードを開いて詳細を確認できます。

CISO ダッシュボードのインジケーターは、デフォルトではレコードを収集しません。[レコードの収集] チェックボックスをオンにすると、レコードを収集できます。

クローズされた脆弱性一致アイテムの合計期間

クローズされた VI の合計期間は、日数単位で毎日測定されます。このインジケーターの目標はスコアの最小化です。

スキャンが可能な資産

スキャンされた資産は # 単位で毎日測定されます。このインジケーターの目標はスコアの最大化です。

最も脆弱なサービス

最も脆弱なサービスは # 単位で毎日測定されます。このインジケーターの目標はスコアの最小化です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

資産あたりの平均脆弱性

[[アクティブな脆弱性一致アイテム]] / [[アクティブな脆弱性一致構成アイテム]

クローズされた脆弱なアイテム

クローズされた脆弱なアイテムは、# 単位で毎日測定されます。このインジケーターの目標はスコアの最大化です。

脆弱性一般アイテムの平均修復時間

[[クローズされた脆弱なアイテムの所要時間合計]]/[[クローズされた脆弱なアイテム]]

現在のスキャン範囲

現在のスキャン範囲をパーセンテージとして計算します。

スキャンされた資産

スキャンされた資産は # 単位で毎日測定されます。このインジケーターの目標はスコアの最大化です。

クローズされた脆弱性一致アイテム (ターゲット達成)

クローズされた脆弱性一致アイテム (ターゲット達成) は、# 単位で毎日測定されます。このインジケーターの目標はスコアの最大化です。

クローズされたターゲットに一致した脆弱性一致アイテムの割合

[[クローズされた脆弱性一致アイテム (ターゲット達成)/月別合計]] /[[クローズされた脆弱性一致アイテム/月別合計]] *100

アクティブな脆弱性一致アイテム

アクティブな脆弱性一致アイテムは # 単位で毎日測定されます。このインジケーターの目標はスコアの最小化です。

脆弱なアイテムの平均経過時間

アクティブな VI の平均経過時間は、日単位で毎日測定されます。このインジケーターの目標はスコアの最小化です。

> **注:**
> 脆弱性一致アイテム (VI) の経過時間とクローズ所要時間の計算をカスタマイズすると、これらのメトリクスを含むパフォーマンスアナリティクス (PA) レポートが急激に増減する可能性があります。VI の経過時間およびクローズ所要時間の計算をカスタマイズする方法の詳細については、 KB1703270 KB 記事を参照してください。

アクティブな脆弱性一致構成アイテム

アクティブな脆弱な CI は # 単位で毎日測定されます。このインジケーターの目標はスコアの最小化です。

月次修復効率

[1 か月間にクローズされた脆弱性一致アイテムの数]/[同じ月に新規または再オープンされた脆弱性一致アイテムの数]

新しい脆弱なアイテム

新しい脆弱性一致アイテムは # 単位で毎日測定されます。このインジケーターの目標はスコアの最小化です。

保留された脆弱なアイテム

保留された VI は # 単位で毎日測定されます。このインジケーターの目標はスコアの最小化です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ブレークダウン

- アサイン先グループ：一部の VI レポートに適用されます。
- リスク評価：VI レポートに適用されます。
- 経過時間範囲：VI レポートに適用されます。
- クローズした経過時間：クローズした VI のレポートに適用されます。
- インターネットフェーシング：CI がハードウェアクラスに属しており、インターネットに接続されているかどうかを示します。
- リージョン：使用される CMDB CI パラメーターは [場所] です。この場所は、構成アイテムの出身国を示します。

注:
脆弱性一致アイテム (VI) の経過時間とクローズ所要時間の計算をカスタマイズすると、これらのメトリクスを含むパフォーマンスアナリティクス (PA) レポートが急激に増減する可能性があります。VI の経過時間およびクローズ所要時間の計算をカスタマイズする方法の詳細については、 KB1703270 KB 記事を参照してください。

データの可視化

名前	タイプ	説明
資産あたりの平均脆弱性	単一スコア	構成アイテムあたりのアクティブな脆弱性一致アイテムの平均数。
平均修復時間 (MTTR)	単一スコア	脆弱性一致アイテムを修正 (クローズ) する平均時間 (30 日間の実行平均として表示)。 **注:** [クローズした経過時間] の値は、データの収集時に計算されます。値は、[最終オープン日] の日付と収集ジョブの日時の差です。
脆弱性の平均経過時間	単一スコア	有効な脆弱性一致アイテムの平均経過日数。
最も脆弱なサービス	リストと折れ線グラフ	組織内のサービスのアクティブな脆弱性一致アイテムの月次平均。 **注:** 脆弱性対応のレポートおよび関連リストに表示するサービス分類の定義については、[脆弱性管理 (PA) ダッシュボード]の [サービス] タブを参照してください。
最も脆弱な国	ドーナッツ	脆弱性一致アイテムの数が最も多い上位 10 か国。
月次修復効率	単一スコア	クローズされた脆弱性一致アイテムを当月の新しい脆弱性一致アイテムで割った割合。
新規およびクローズされた脆弱なアイテム	棒グラフ	1 か月間にインポートされた脆弱性一致アイテムの数とクローズされた脆弱性一致アイテムの数。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	タイプ	説明
スキャン範囲	線グラフ	スキャン可能な資産の合計数に対するスキャンされた資産の数の比較を経時的に表示します。ウィジェットにある CI クラスは、[スキャン範囲構成] モジュールで指定されます。 スキャン範囲モジュールの構成については、「Configure the Scan Coverage reports (スキャン範囲レポートの構成)」を参照してください。
月次スキャン範囲	単一スコア	スキャンされた資産数を現在の月のスキャン可能な資産の合計数で割った割合。 スキャン範囲モジュールの構成については、「Configure the Scan Coverage reports (スキャン範囲レポートの構成)」を参照してください。
保留された脆弱性が最も多い上位 10 件のアサイン先グループ	リストと折れ線グラフ	月の平均に基づいて保留された脆弱性一致アイテムの数が最も多い上位 10 のアサイン先グループ。
修復ターゲットへの遵守が最も低い上位 10 のアサイン先グループ	リストと折れ線グラフ	修復ターゲットに対する脆弱性一致アイテムの遵守率が最も低い上位 10 のアサイン先グループ。

推奨アクション

名前	タイプ	ソーステーブル	説明
利用可能なエクスプロイトのある上位 10 件の脆弱性 (Top 10 Vulnerabilities with Exploits Available)	リスト	最大の脆弱性一致アイテム [sn_vul_analytics_top_item]	VR エクスプロイトフレームワークを使用するすべての脅威インテリジェンスベンダーが利用できるエクスプロイトを含むアクティブな脆弱性。
影響度が高い上位 10 件のソリューション (Top 10 Highest Impact Solutions)	リスト	最大の脆弱性一致アイテム [sn_vul_analytics_top_item]	アクティブな脆弱性一致アイテムのリスクスコアが最も高い優先ソリューションまたはパッチ。このレポートでは、Microsoft および Red Hat のパッチを環境内の脆弱性に関連付ける Vulnerability Solution Management (VSM) の機能を使用します。VSM は、脆弱性に対する優先ソリューションを特定するために役立ちます。
最も古い上位 10 件の脆弱性一致アイテム (Top 10 Oldest Vulnerable Items)	リスト	最大の脆弱性一致アイテム [sn_vul_analytics_top_item]	最も古いアクティブな脆弱性一致アイテム。[概要] タブでこれらのアイテムを解決して、脆弱性の平均経過時間を短縮します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

推奨アクション (続く)

名前	タイプ	ソーステーブル	説明
資産で最もまん延している上位 10 件の脆弱性 (Top 10 Vulnerabilities Most Prevalent on Assets)	リスト	最大の脆弱性一致アイテム [sn_vul_analytics_top_item]	最も多くの資産に対して利用できるアクティブな脆弱性一致アイテム。

スキャン範囲レポートの設定

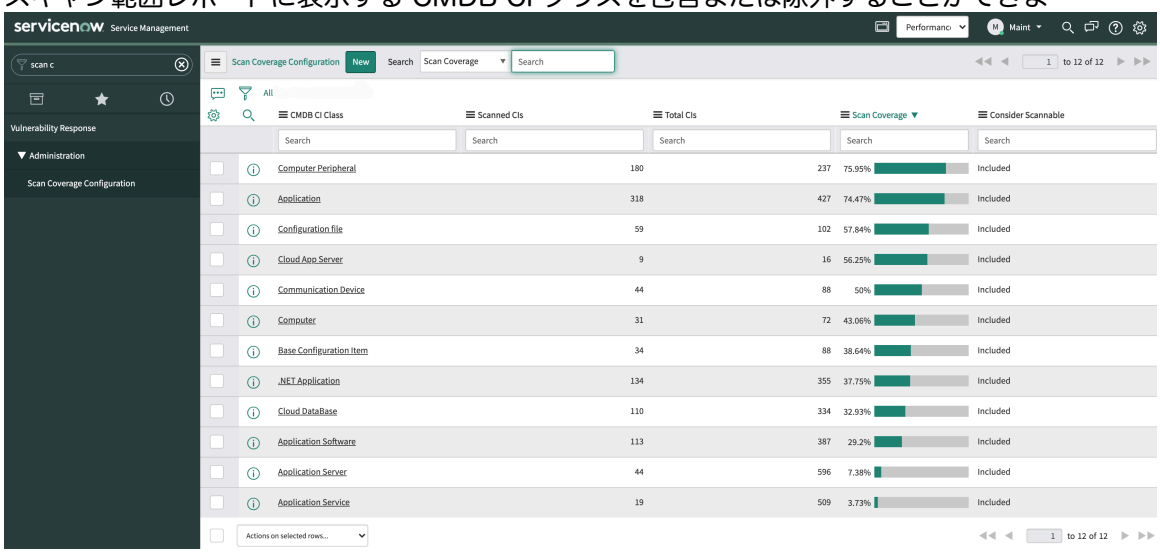
CISO ダッシュボードからスキャン範囲レポートをユーザーが実行できるようにします。このレポートを使用すると、一定期間における組織のスキャン範囲をユーザーが確認できます。

始める前に

必要なロール：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

このタスクについて

スキャン範囲は、過去 90 日間に脆弱性スキャナーによってスキャンされている、さまざまなクラスの資産の数を示します。こうした資産は、構成管理データベース (CMDB) 内のスキャン可能な資産の数と比較されます。デフォルトでは、スキャン範囲構成モジュールには、少なくとも 1 つのスキャン済み資産が一致する CMDB CI クラスが含まれています。CMDB から、CISO ダッシュボードに表示されるスキャン範囲レポートに CI クラスを追加できます。スキャン範囲レポートに表示する CMDB CI クラスを包含または除外することができます。



手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > スキャン範囲構成.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スキャン範囲構成フォーム

フィールド	説明
CMDB CI クラス	CISO ダッシュボード上のスキャン範囲レポートに追加する必要がある CI クラス。 **注:** CI クラスが既にスキャン範囲構成モジュールに存在する場合、このリストには追加されません。
スキャン可能を検討	CI クラスを含める必要があるかどうかを指定するオプション。スキャン範囲レポートにデータを追加する場合は、CI クラスを含めます。除外された場合、その CI クラスのデータは追加されません。

4. **[Submit]** をクリックします。

CISO ダッシュボードの PA インジケーターを構成する

インスタンス内の脆弱性データを管理できるように、自動化および定式化された CISO インジケーターを監視します。

始める前に
必要なロール：sn_vul.vulnerability_admin

このタスクについて
脆弱性対応 には、自動インジケーターと定式化インジケーターの両方があります。

主要な用語

インジケーター
: ビジネスサービス、アクティビティ、または組織行動の、定期的に取得されるパフォーマンス測定値を定義します。たとえば、アクティブな脆弱性一致アイテムがあります。

インジケーターソース
: 効率を高めるために 1 つのテーブルまたはデータベースビューからフィルタリングされたレコードで構成されるデータセット。たとえば、VI.Active (インターネット接続) があります。

ブレークダウン
: 優先度、カテゴリ、アサイン先グループなどの定性的属性を使用して、フィルターおよびグループインジケータースコアをブレークダウンします。

スケジュール済みジョブ
: インジケーターのソースデータを入力するためにスケジュール済みジョブが実行されます。[PA VR] CISO ダッシュボードの日次スケジュール済みジョブは、デフォルトでは無効になっています。CISO ダッシュボードのインジケータースコアを収集するには、これをアクティブ化する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > パフォーマンスアナリティクス > インジケーター をクリックし、次のいずれかを選択します。
   - インジケーター (自動)
   - インジケーター (計算)

   詳細については「パフォーマンスアナリティクスインジケーター」を参照してください。
2. [インジケーター] ページで、 [名前] 列で必要なインジケーター名を検索します。
3. インジケーター名をクリックすると、そのレコードを開いて詳細を確認できます。

   CISO ダッシュボードのインジケーターは、デフォルトではレコードを収集しません。[レコードの収集] チェックボックスをオンにすると、レコードを収集できます。

   注:
   インジケーターでレコードの収集をアクティブ化すると、データコレクションジョブの実行に必要な時間やメモリが多くなるなどのパフォーマンスの問題が発生する可能性があります。

   インジケーターソースに対してフェッチできる最大行数は 1,000,000 です。

SecOps 脆弱性対応ヘルスダッシュボード

脆弱性対応ヘルスダッシュボードは、組織が脆弱性対応アプリケーションの実装と使用に関する包括的なインサイトを得られるように設計されたツールです。

全体的なヘルスアセスメントは、構成、実装、統合、パフォーマンス、データ、およびプロセス全体にわたるさまざまな重要な要素を集計することによって決定されます。次のアプリケーションのカテゴリごとに集計ダッシュボードを表示します。

- Vulnerability Response
- アプリケーション脆弱性対応
- コンテナ脆弱性対応
- コンフィギュレーションコンプライアンス

SecOps 脆弱性対応ヘルスダッシュボードのインストール

Now Platform インスタンスで、脆弱性対応アプリケーションに SecOps 脆弱性対応ヘルスダッシュボードをインストールして構成するには、ServiceNow Store に移動して SecOps ヘルスアナリティクス (sn_sec_analytics) プラグインをアクティブ化します。

必要な Now Platform ロール

必要なロール：sn_sec_analytics.admin、sn_sec_analytics.read

スケジュール済みジョブ

スケジュール済みジョブを表示するには、次に移動します: **All** (すべて) > システムスケジューラ > スケジュール済みジョブ > 健全性ダッシュボードのメトリクスを収集. [健全性ダッシュボードメトリクスの収集 (Collect health dashboard metrics)] スケジュール済みジョブは、毎日 00:00 に実行されます。SecOps 脆弱性対応ヘルスダッシュボードのデータが生成されます。スケジュール済みジョブを手動で実行することも選択できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユースケース

組織内のユーザーがこのダッシュボードをどのように使用するかの例については、次のユースケースを参照してください。

ユーザー	ダッシュボードの使用法
脆弱性アドミン	脆弱性対応 アプリケーションの健全性スコアを理解するのに役立ちます。また、改善が必要な領域を強調することにも役立ちます。 脆弱性対応ヘルスダッシュボードは、実装と使用状況の健全性のみを対象にします。脆弱性や資産の管理には役立ちません。
サポートアドミン	KPI を使用して、パフォーマンス、カスタマイズ、および構成の問題を特定するのに役立ちます。アプリケーションの健全性に基づいて、追加の分析を実行したり、ユーザーに推奨事項を提供したりすることができます。
実装パートナー	構成、アドオン、カスタマイズ、および統合の脆弱性対応 実装の健全性を評価し、改善の推奨事項をユーザーに提供するのに役立ちます。

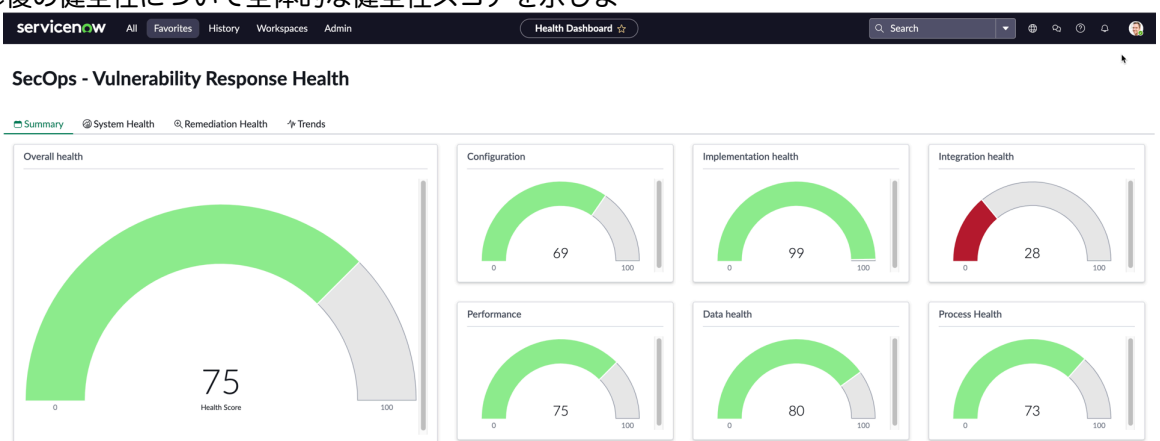
SecOps 脆弱性対応ヘルスダッシュボードのタブ

SecOps 脆弱性対応ヘルスダッシュボードを表示するには、次に移動します: セキュリティオペレーションヘルス > 脆弱性対応ヘルス. ダッシュボードの各色は以下を表しています。

- 緑：安全
- 黄：警告
- 赤：重大

[サマリー] タブ

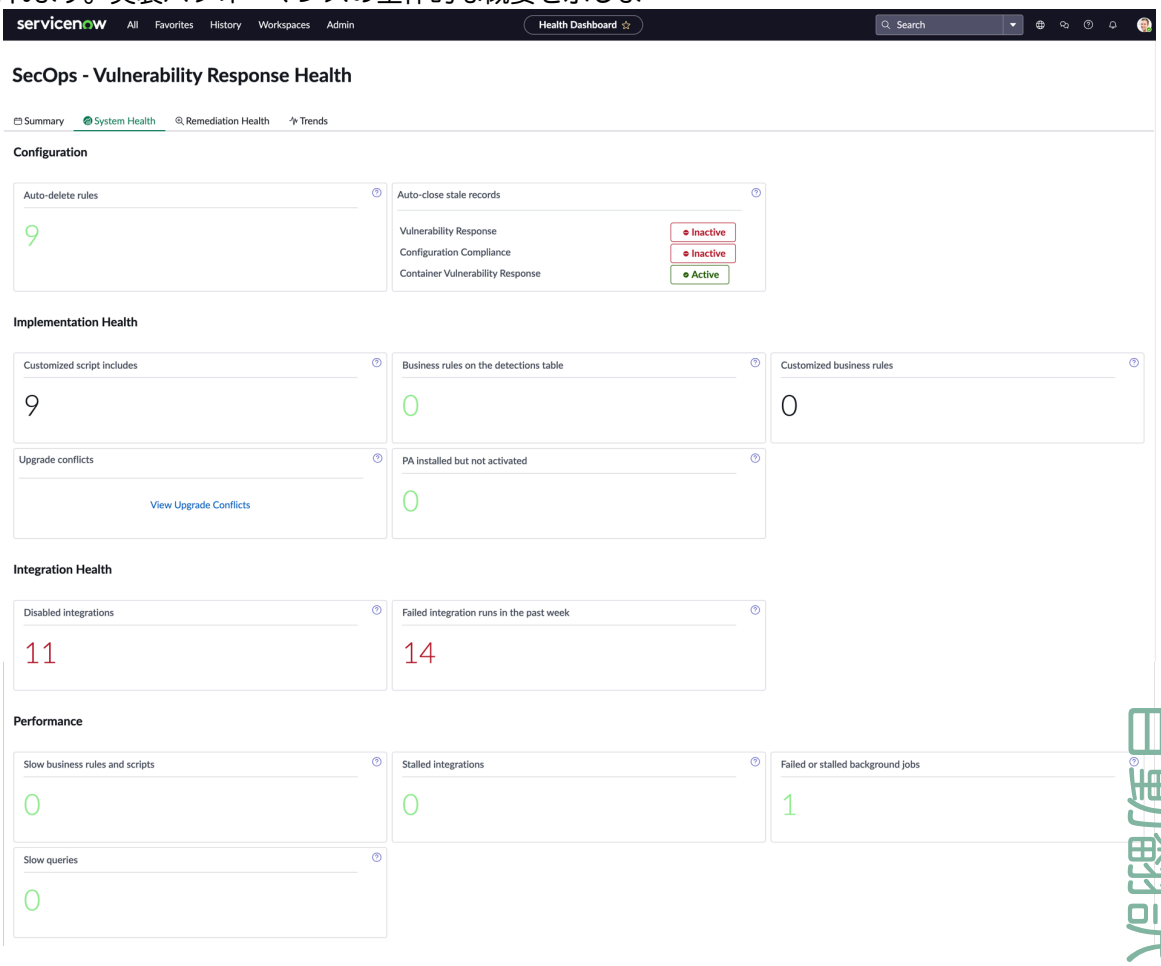
このダッシュボードは、VR アプリケーションの構成および修復の健全性について全体的な健全性スコアを示します。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[システム健全性] タブ

このダッシュボードには、実装の構成と統合の健全性が表示されます。実装パフォーマンスの全体的な概要を示します。

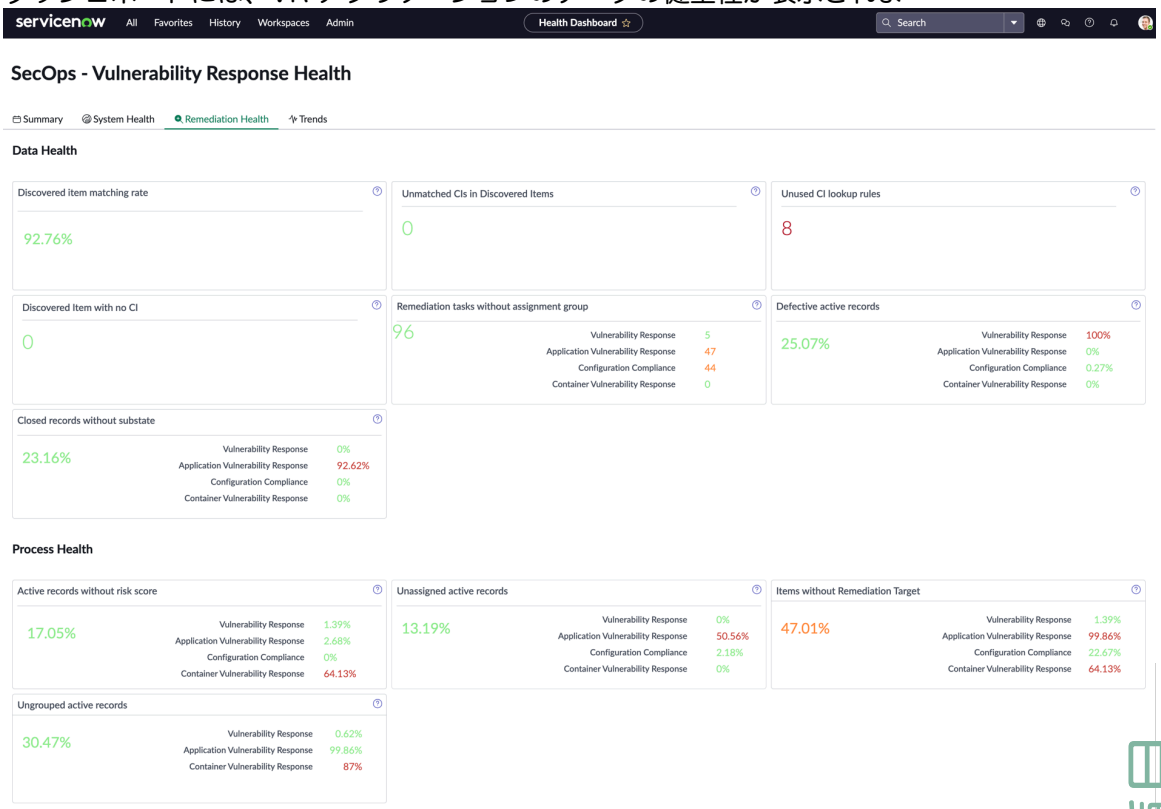


自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[修復の健全性] タブ

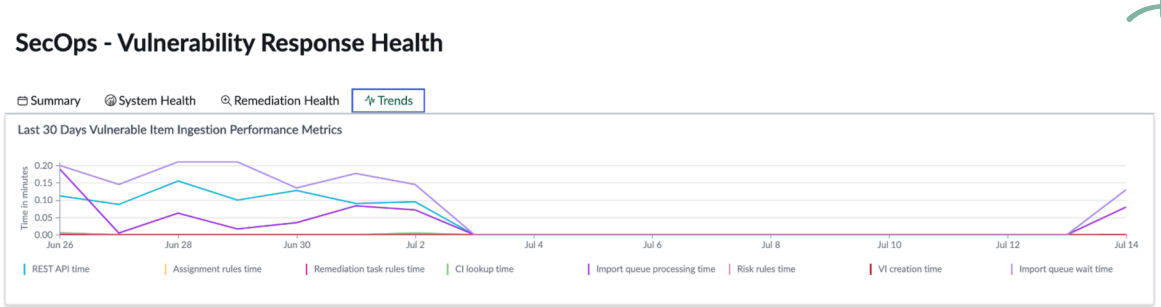
このダッシュボードには、VR アプリケーションのデータの健全性が表示されま



す。

[傾向 **(Trends)**] タブ

このダッシュボードには、VR アプリケーションの過去 30 日間の脆弱性一致アイテム取り込みパフォーマンスメトリクスの傾向が表示されま



す。

レポート

注:
しきい値はベースシステムの一部です。要件に基づいて値を設定できます。

まとめ

タイトル	説明
総合健全性	VR アプリケーションの全体的な健全性スコア。詳細については、メトリクスのレポートを参照してください。
構成	VR アプリケーションの全体的な構成健全性。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

まとめ (続く)

タイトル	説明
実装の健全性	VR アプリケーションの全体的な実装の健全性。
統合の健全性	VR アプリケーションの全体的な統合の健全性。
パフォーマンス	VR アプリケーションの全体的なパフォーマンス健全性スコア。
データの健全性	VR アプリケーションの全体的なデータの健全性。
プロセスの健全性	VR アプリケーションの全体的なプロセス健全性スコア。

システム健全性

タイトル	説明	パフォーマンス向上に関する考慮事項	しきい値警告	しきい値重大
構成				
ルールの自動削除	有効なルールの自動削除の数を表示します。	非アクティブなルールの自動削除を確認して解決します。	3	1
古いレコードの自動クローズ	古い検出を自動的にクローズします。詳細については、servicenow.com/docs の「脆弱性対応の古い検出を自動的にクローズする」トピックを参照してください。	古い検出の量を削減します。スキャナーによってクローズされない古い検出をクローズするには、このオプションを有効にします。	3	1
実装の健全性				
カスタマイズされたスクリプトインクルード	カスタマイズされた「スクリプトインクルード」の数。	カスタマイズされた「スクリプトインクルード」を最小限に抑えて、アップグレードを容易にします。	10	12
検出テーブルに対するビジネスルール	検出テーブル内のカスタマイズされたビジネスルールの数。	ビジネスルールを最小限に抑えて、アップグレードを容易にします。	4	8
カスタマイズされたビジネスルール	CMDB にレコードを作成する前にカスタマイズされたビジネスルールの数。	レコードに関するデフォルトのビジネスルールを使用します。	5	8

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システム健全性 (続く)

タイトル	説明	パフォーマンス向上に関する考慮事項	しきい値警告	しきい値重大
アップグレードの競合	アップグレードで特定されたビジネスルールやスクリプトなどの競合。	競合を確認し、解決します。	10	15
インストールされているが、アクティブ化されていない PA	パフォーマンスアナリティクスダッシュボードが有効になっていない場合にそれを示します。	PA ダッシュボードを有効にします。	10	15
統合の健全性				
無効化されている統合	無効化されている統合の数。	必要な統合を確認して有効にします。	6	9
過去 1 週間に失敗した統合実行。	過去 1 週間に成功しなかった統合実行の数。	失敗した統合実行の原因を確認して解決します。	9	12
パフォーマンス				
遅いビジネスルールとスクリプト	平均実行時間が 10 ミリ秒を超え、実行回数が 10,000 回を超えるビジネスルールおよびスクリプト。	実行速度の遅いビジネスルールを確認して解決します。	10	15
停止した統合	完了前にタイムアウトした統合の数。	停止した統合の原因を確認して解決します。	10	15
バックグラウンドジョブの失敗または停止	過去 1 週間に失敗またはタイムアウトしたバックグラウンドジョブ。	失敗したジョブの原因を確認して解決します。	5	10
遅いクエリ	平均実行時間が 10 ミリ秒を超え、実行回数が 10,000 回を超えるクエリ。	実行速度の遅いビジネスルールを確認して解決します。	10	15

修復の健全性

タイトル	説明	パフォーマンス向上に関する考慮事項	しきい値警告	しきい値重大
データの健全性				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復の健全性 (続く)

タイトル	説明	パフォーマンス向上に関する考慮事項	しきい値警告	しきい値重大
検出されたアイテム一致率	既存の CI に一致する検出されたアイテムの数。	CMDB と CI ルックアップルールのロジックの健全性を確認します。	50	20
検出されたアイテム内の一致しない CI	不一致ステータスの検出済みアイテム。	CMDB と CI ルックアップルールのロジックの健全性を確認します。	9	12
未使用の CI ルックアップルール	検出されたアイテムに関連付けられていない CI ルックアップルール。	未使用の CI ルックアップルールのステータスを非アクティブに変更します。	4	6
CI のない検出されたアイテム	構成アイテムがない検出されたアイテム。	CI ルックアップルールを確認して再適用します。	9	12
欠陥のあるアクティブレコード	構成アイテムまたは脆弱性がないレコード。	CMDB CI ライフサイクル管理のオプションを使用して CI を廃止します。 **注:** CI を直接削除すると、孤立 VIT が発生する可能性があります。	40	60
アサイン先グループのない修復タスク	アサイン先グループがまだアサインされていないアクティブな修復タスク。	修復タスクをアサイン先グループにアサインし、既存のアサインルールを確認します。	40	60
サブステートのないクローズ済みレコード	サブステートなしでクローズされたレコード。	レコードをクローズするときに [理由] フィールドに情報を入力します。	40	50
プロセスの健全性				
リスクスコアのないアクティブレコード	リスクスコアが 0 であるか、リスクスコアがアサインされていないアクティブなレコード。	リスクルールを確認して解決します。	40	60

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復の健全性 (続く)

タイトル	説明	パフォーマンス向上に関する考慮事項	しきい値警告	しきい値重大
未アサインのアクティブなレコード	アサイン先グループのないレコード。	レコードにグループをアサインし、既存のアサインルールを確認します。	30	50
修復ターゲットのないアイテム	修復ターゲット日付のないアイテム	修復ターゲットルールを確認して解決します。これらのルールには、すべてのレコードが含まれている必要があります。	30	50
グループ化されていないアクティブなレコード	修復タスクルールに含まれていないレコード。	修復タスクルールを確認します。	40	60

傾向

タイトル	説明
過去 30 日の脆弱性一致アイテムの取り込みパフォーマンスメトリクス	過去 30 日間に脆弱性一致アイテムの取り込みと複数のルールの処理にかかった平均時間。

しきい値の変更

設定に基づいて、SecOps VR 健全性ダッシュボードデータのしきい値を変更できます。

始める前に

必要なロール：admin

手順

1. 次のように移動する。 セキュリティオペレーションヘルス > 構成 > メトリクス.
2. [健全性ダッシュボードデータ] ページで、変更するレコードを開きます。
3. レコードを更新して保存します。

脆弱性管理 **(PA)** ダッシュボード

脆弱性の初期分析と検出から封じ込めや修復までのボリューム、パフォーマンス、および進捗状況を追跡します。アサイン先グループやエクスプロイト、リスク評価、ステータスなどで、レポートをフィルタリングできます。脆弱性エクスポージャーや、その影響を受けるビジネスサービスに関するインサイトを迅速に得ることができます。

必要な **Now Platform** ロール

必要なロール：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst、および sn_vul.vulnerability_read を持つ (または sn_vul.vulnerability_read ロールを継承する) ユーザー、および pa_viewer。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユースケース

組織内のさまざまなユーザーがこのダッシュボードをどのように使用するかの例については、次のユースケースを参照してください。

ユーザー	ダッシュボードの使用法
IT マネージャー、IT アナリスト、脆弱性修復責任者	最もリスクが高い脆弱性一致アイテムを効率的に判定することで、脆弱性の悪用によって増大するセキュリティインシデントへの対処を可能にします。これらのダッシュボードでは脆弱性一致アイテムのアクティビティがグラフィックで表示されるため、修復計画とステータスの進捗状況の設計に役立ちます。そのため、影響を受ける重要な資産や目立った脆弱性に関連する KPI に集中できます。

脆弱性管理 (PA) ダッシュボードを表示するには、次に移動します: 脆弱性対応 > 概要.

経時的な傾向データを示すレポートが表示されます。リアルタイムデータを含むレポートのリストを下に示します。重要なメトリクスの傾向を定期的に確認してビジネスプロセス全体を分析し、改善が必要な領域を特定します。

リアルタイムスコアを使用して PA レポートを表示する方法については、「脆弱性対応のパフォーマンスアナリティクス [PA] レポートのリアルタイム表示」を参照してください。

自動翻訳

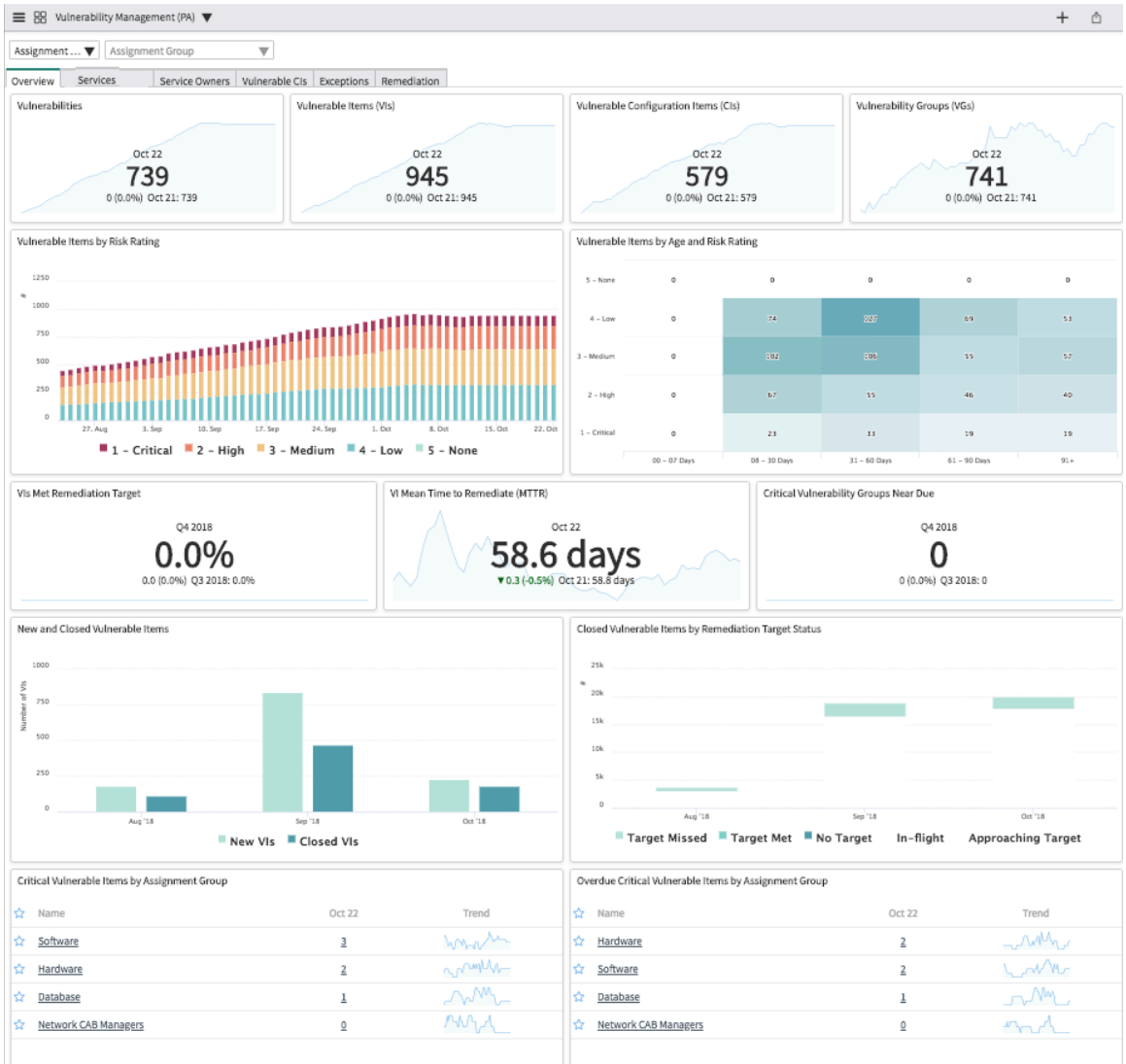
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性管理 (PA) ダッシュボードタブ

[概要] タブ

このダッシュボードでは、脆弱性のリスクとそのまん延、影響を受ける資産、修復ターゲットの遵守、および修復の進捗状況を確認できます。

[概要] タブでは、スケジュール済みジョブに基づいて実行される、アサイン先グループ別の重大な脆弱性一致アイテムのレポートを確認できます。



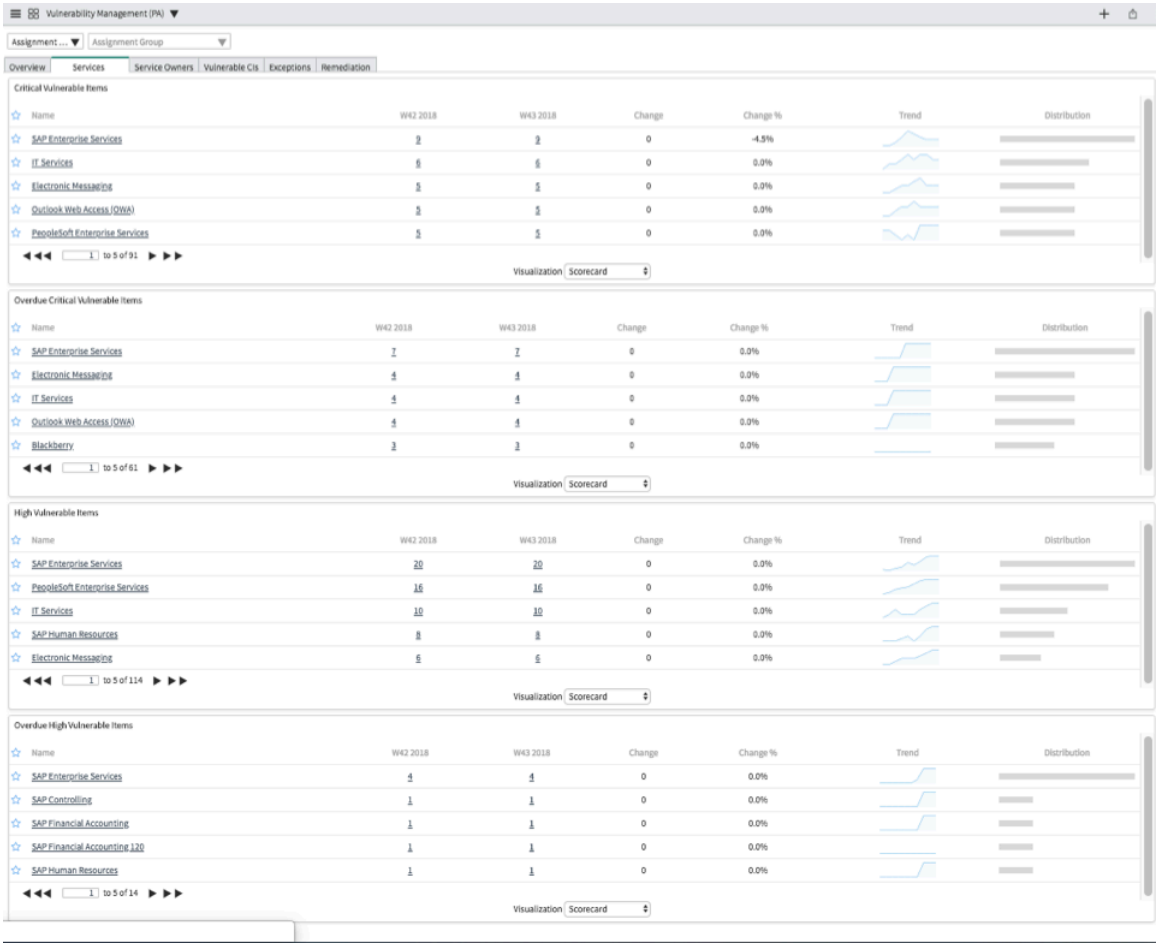
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[ビジネスサービス] タブ

このダッシュボードでは、ビジネスサービスのレベルで脆弱性リスクを示します。組織全体でこの情報を共有することで、サービスマネージャーが迅速かつ積極的に脆弱性を修復し、情報セキュリティの共有責任モデルを推進することが可能になります。

システムプロパティ sn_vul.service_classifications を使用すると、サービスクラスをテクニカルサービスまたはアプリケーションサービスに変更できます。

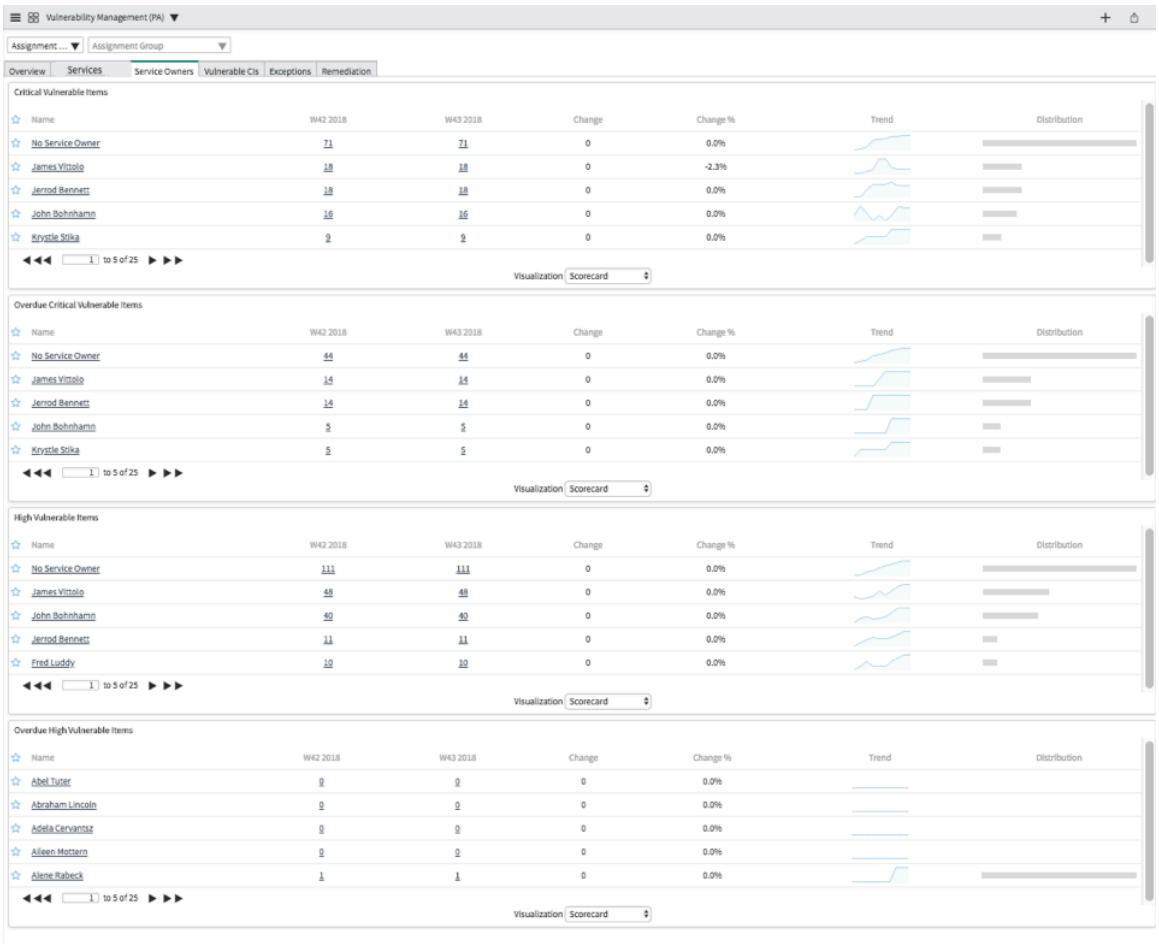


自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[サービスオーナー] タブ

このダッシュボードでは、ビジネスサービスレベルからサービスオーナー (ビジネスサービス担当の重役) レベルまでの脆弱性リスクをまとめて表示します。どの重役が脆弱性に対して最もリスクを負い、どの重役が迅速な修復アクティビティの旗振り役になるべきかを示します。



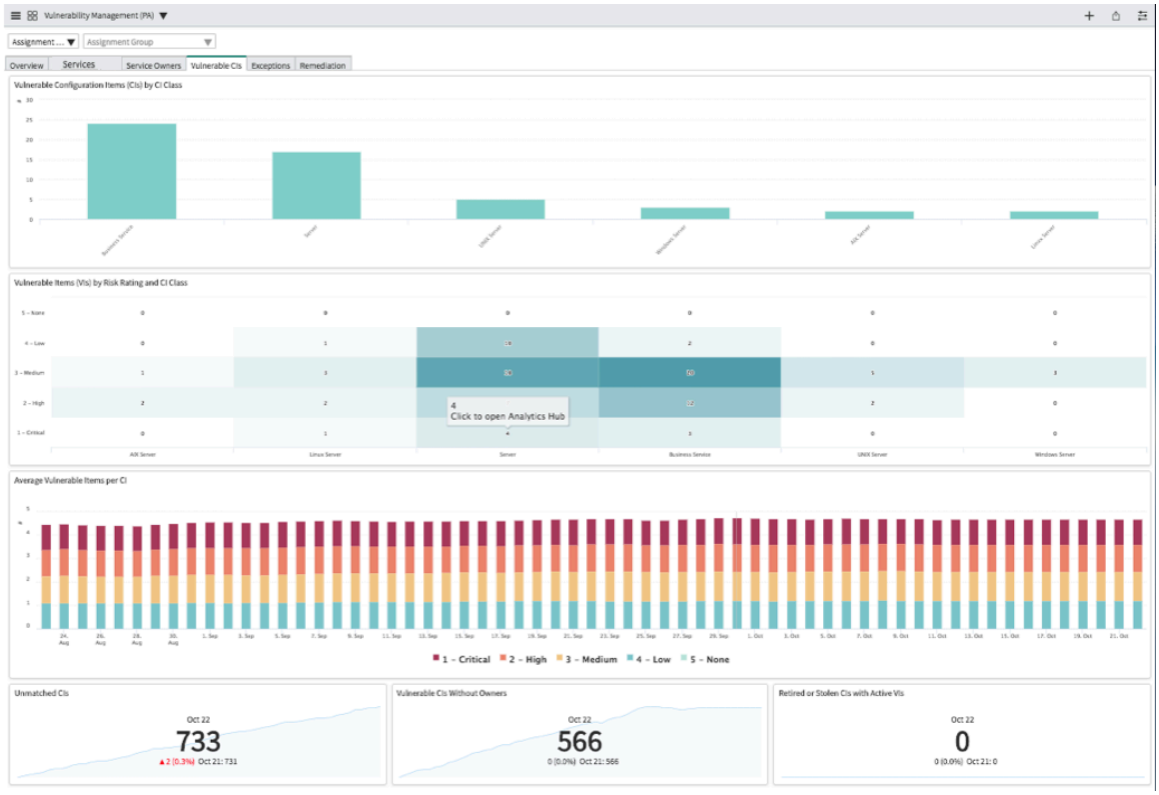
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[脆弱性一致 **CI**] タブ

このダッシュボードには、アクティブな脆弱性がある CI のスコープと構成、および最も注意が必要な CI のカテゴリーが表示されます。アクティブな脆弱性一致アイテムがある廃止済みの資産を特定し、その資産が廃止されていることを確認します。所有権情報が欠落している脆弱な CI の数を表示することで、システムに重大な脆弱性の影響が及ぶ前に、資産の所有者を特定できます。

[脆弱性一致 CI] タブでは、[所有者のいない脆弱性一致 CI (Vulnerable CIs Without Owners)] および [アクティブな VI を持つ廃止または盗難された CI] レポートを、リアルタイムで表示できます。



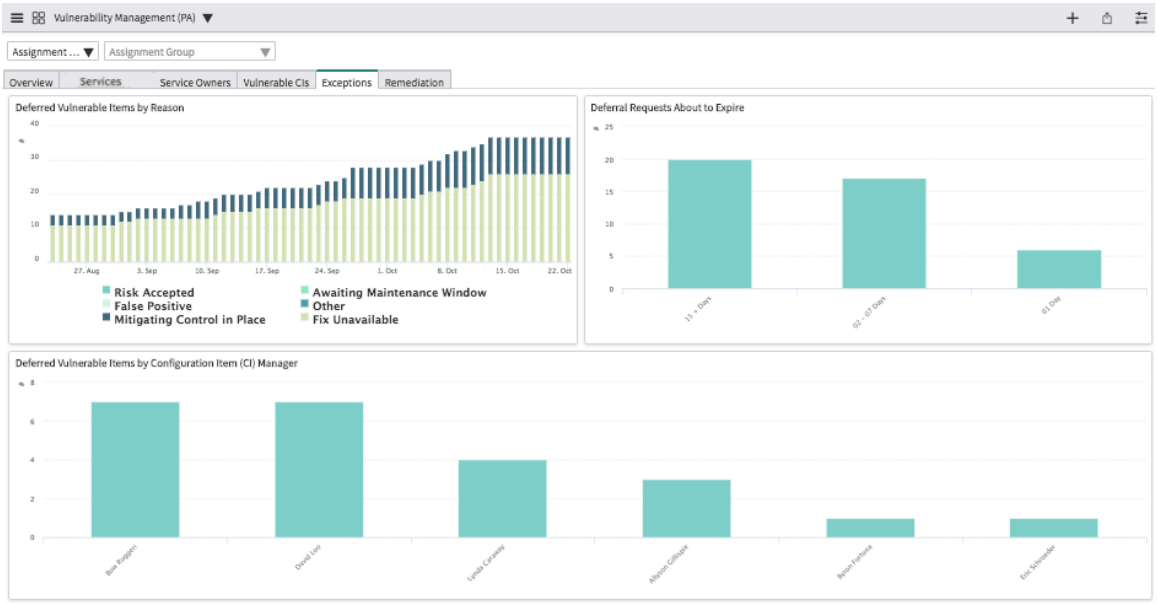
[例外] タブ

このダッシュボードは、組織が過度な保留によるリスクを負っていると思われる場所を把握し、修復オプションを再検討するために役立ちます。

[理由別の保留された脆弱なアイテム]、[期限切れ間近の保留要求]、[アサイン先グループ別の重大な脆弱性一致アイテムの例外]、および [要求者による例外要求] レポートを表示できます。

自動翻訳

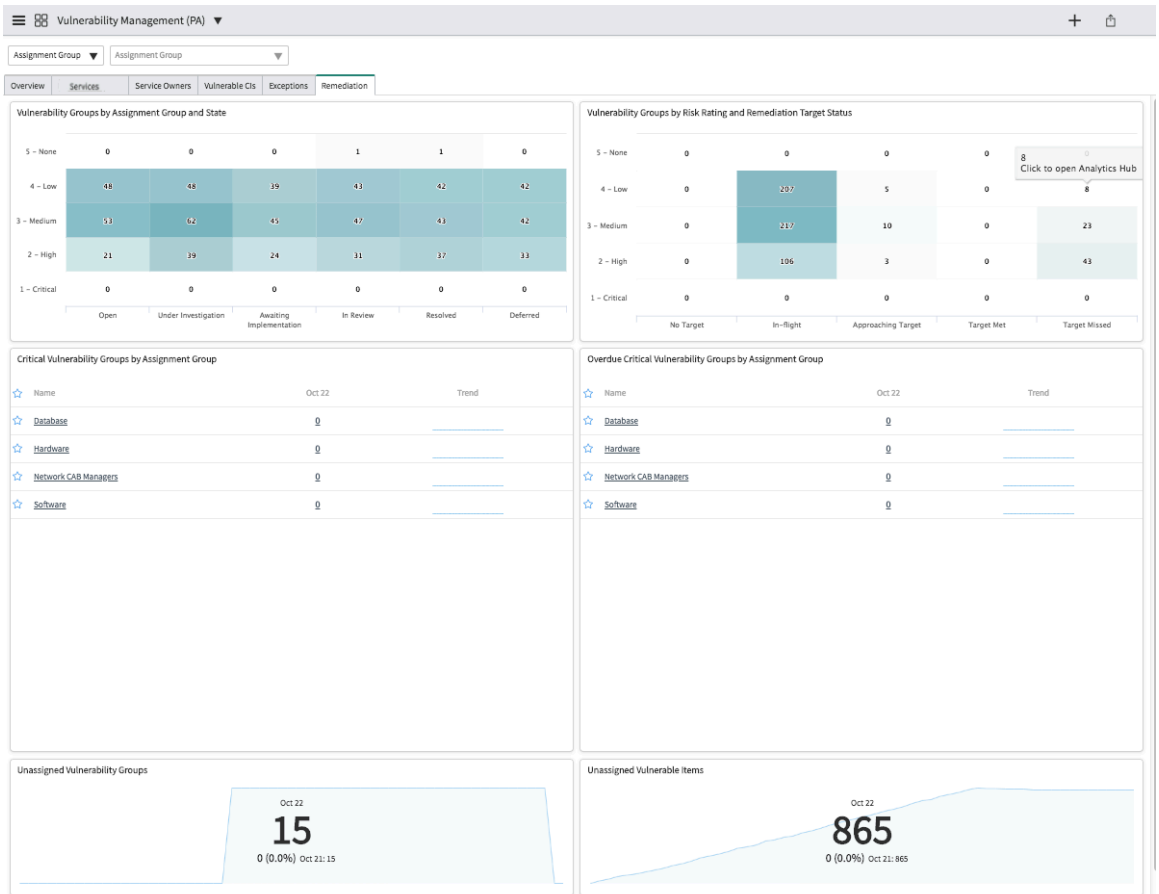
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[修復] タブ

このダッシュボードは、修復アクションの進捗状況と、その完了に最も支援が必要なサポートチームの把握に役立ちます。

[修復] タブでは、[未アサインの脆弱なアイテム] レポートをリアルタイムで表示できます。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インジケーター

脆弱性対応インジケーター

脆弱性対応 アプリケーションの脆弱性の修復の進捗状況を測定および追跡するために使用されるインジケーターは多数あります。

これらのインジケーターに対するレコードの収集オプションは、脆弱性対応 アプリケーションではデフォルトで無効になっています。このオプションが無効になっているのは、特定のレポートをリアルタイムで表示可能にするためです。手動でのレコードの収集を有効にして、スコアを構成するレコードを表示した方がよい場合は、これらのインジケーターで使用される傾向情報を引き続き使用できます。

個別の脆弱性

count_active_vi が 0 より大きい個別の脆弱性。目標は最小化することです。

保留されていない期限切れの重大な脆弱なアイテム

テーブル sn_vul_vulnerable_item を使用している VI.Active というデータソースのカウント。目標は最小化することです。

修復ターゲットを満たした脆弱なアイテムの割合

([[クローズされた脆弱なアイテム > 修復ターゲット = ターゲット達成]]/[[クローズされた脆弱なアイテム]]) * 100。目標は最大化することです。

未アサインの脆弱なアイテム

[アサイン先グループ] と [アサイン先] フィールドの両方が空である、すべてのアクティブな脆弱なアイテム。目標は最小化することです。

重大な脆弱なアイテム (サービス)

テーブル sn_vul_analytics_business_services_vi を使用しているアクティブな VI (サービス) データソースのカウント。目標は最小化することです。

期限切れの高脆弱なアイテム (サービス)

テーブル sn_vul_analytics_business_services_vi を使用しているアクティブな VI (サービス) データソースのカウント。目標は最小化することです。

未アサインの修復タスク

[アサイン先グループ] と [アサイン先] フィールドの両方が空であるすべてのアクティブな修復タスク。目標は最小化することです。

重大な脆弱なアイテム

テーブル sn_vul_vulnerable_item を使用している VI.Active というデータソースのカウント。目標は最小化することです。

脆弱性一致アイテム

テーブル sn_vul_vulnerable_item を使用している VI.Active というデータソースのカウント。目標は最小化することです。

新しい脆弱なアイテム

テーブル sn_vul_vulnerable_item を使用している VI.New というデータソースのカウント。目標は最小化することです。

脆弱性一致構成アイテム

テーブル sn_vul_vulnerable_item を使用している VI.Active というデータソースの個別のカウント。目標は最小化することです。

クローズ済み脆弱なアイテムの合計期間

テーブル sn_vul_vulnerable_item を使用している VI.Closed というデータソースの合計。目標は最小化することです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

保留されていない修復タスク

テーブル sn_vul_vulnerability を使用している VG.Active というデータソースのカウント。目標は最小化することです。

脆弱性一致アイテム平均修復時間

[[クローズされた脆弱なアイテムの所要時間合計]]/[[クローズされた脆弱なアイテム]]

重大な期限切れの脆弱なアイテム (サービス)

テーブル sn_vul_analytics_business_services_vi を使用しているアクティブな VI (サービス) データソースのカウント。目標は最小化することです。

廃止された構成アイテム

テーブル sn_vul_vulnerable_item を使用している VI.Active というデータソースの個別のカウント。目標は最小化することです。

保留要求

テーブル sn_vul_change_approval を使用しているアクティブな保留要求データソースのカウント。目標は最小化することです。

構成アイテムごとの脆弱性一致アイテム

テーブル sn_vul_analytics_vi_ci_class を使用しているアクティブな VI データソースのカウント。目標は最小化することです。

クローズされた脆弱なアイテム

クローズされた脆弱なアイテムは、# 単位で毎日測定されます。目標は最大化することです。

一致しない構成アイテム

サードパーティの脆弱性スキャナーによって検出され、CMDB 内の既存の CI と一致しないホストが一覧表示されます。

保留されていない期限切れの重大な修復タスク

テーブル sn_vul_vulnerability を使用している VG.Active というデータソースのカウント。目標は最小化することです。

サポートグループのない脆弱性一致構成アイテム

テーブル sn_vul_vulnerable_item を使用している VI.Open というデータソースのカウント。目標は最小化することです。

保留されていない重大な修復タスク

テーブル sn_vul_vulnerability を使用している VG.Active というデータソースのカウント。目標は最小化することです。

保留された脆弱なアイテム

テーブル sn_vul_vulnerable_item を使用している VI.Active というデータソースのカウント。目標は最小化することです。

高脆弱なアイテム (サービス)

テーブル sn_vul_analytics_business_services_vi を使用しているアクティブな VI (サービス) データソースのカウント。目標は最小化することです。

アクティブな脆弱なアイテムを持つ個別の構成アイテム

テーブル sn_vul_analytics_vi_ci_class を使用しているアクティブな VI を持つ CI データソースの個々のカウント。目標は最小化することです。

構成アイテムあたりの脆弱なアイテムの平均数

[[アクティブな脆弱なアイテム]]/[[脆弱な CI]]。目標は最小化することです。

修復タスク

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル sn_vul_vulnerability を使用している VG.Active というデータソースのカウント。目標は最小化することです。

保留された重大な脆弱性一致アイテム

テーブル sn_vul_vulnerable_item を使用している VI.Active というデータソースのカウント。目標は最小化することです。

保留要求 (作成済み)

テーブル sn_vul_change_approval を使用している Closed.Requests データソースのカウント。目標は最小化することです。

ブレークダウン

ダッシュボードのインジケーターに適用されるブレークダウン名は次のとおりです。

- 経過時間
- クローズした経過時間
- アサイン先グループ
- CI クラス
- CI マネージャー
- 保留経過時間
- 保留の理由
- 例外要求者
- エクスプロイト攻撃ベクトル
- エクスプロイト有無
- エクスプロイトスキルレベル
- 修復ターゲットルール
- 修復ターゲットステータス
- 修復ターゲットステータス (クローズ済み)
- リスク評価
- サービス
- サービス重要度
- サービスオーナー
- 重大度
- 状況

注:
脆弱性一致アイテム (VI) の経過時間とクローズ所要時間の計算をカスタマイズすると、これらのメトリクスを含むパフォーマンスアナリティクス (PA) レポートが急激に増減する可能性があります。VI の経過時間およびクローズ所要時間の計算をカスタマイズする方法の詳細については、 KB1703270 KB 記事を参照してください。

ブレークダウンソース

- アサイン先グループ：VI または/および RT レポートに適用されます。
- エクスプロイト有無：VI レポートに適用されます。
- エクスプロイト攻撃ベクトル：VI レポートに適用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- エクスプロイトスキルレベル：VI レポートに適用されます。
- 修復ターゲットステータス：VI および RT レポートに適用されます。
- リスク評価：VI および RT レポートに適用されます。
- 進捗状況：VI および RT レポートに適用されます。

データの可視化

タイトル	タイプ	説明
脆弱性	単一スコア	1 つ以上のアクティブな脆弱なアイテムに関連付けられた脆弱性の数。
脆弱なアイテム (VI)	単一スコア	アクティブな (クローズされていない) 脆弱なアイテムの数。
脆弱性一致構成アイテム (CI)	単一スコア	1 つ以上のアクティブな脆弱性一致アイテムに関連付けられた構成アイテム (CI) の数。
修復タスク	単一スコア	アクティブな (クローズされていない) 修復タスクの数。
リスク評価別の脆弱性一致アイテム	棒グラフ	選択した時間スパンにおけるリスク評価によってグループ化された、アクティブな脆弱なアイテムの数。
経過時間およびリスク評価別の脆弱性一致アイテム (Vulnerable Items by Age and Risk Rating)	ヒートマップ	リスク評価および経過時間 (日) でグループ化された、アクティブな脆弱性一致アイテムの数。
修正ターゲットを満たした VI	単一スコア	現在の四半期と前の四半期の修復ターゲット日を達成した、クローズされた脆弱性一致アイテムの割合。 修正ターゲットは、最後のオープン日に日数 (24 時間単位として測定) を加算して計算されます。
VI 平均修正時間 (MTTR)	単一スコア	脆弱性一致アイテムを修正 (クローズ) する平均時間 (30 日間の実行平均として表示)。 **注:** [クローズした経過時間] の値は、データの収集時に計算されます。値は、last_opened の日付と収集ジョブの日時の差です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タイトル	タイプ	説明
期限間近の重大な修復タスク	単一スコア	修復ターゲット日が近づいているアクティブな修復タスクの数。 修復タスクの修復ターゲット日は、グループ内のアクティブな脆弱性一致アイテムに属する最も近い期日に設定されます。 修正ターゲットは、最後のオープン日に日数 (24 時間単位として測定) を加算して計算されます。 このレポートでは、保留された修復タスクは除外されます。
新規およびクローズされた脆弱なアイテム	棒グラフ	選択した期間スパンにおける新規およびクローズされた脆弱なアイテムの数。 注: [クローズした経過時間] の値は、データの収集時に計算されます。値は、last_opened の日付と収集ジョブの日時の差です。
修復ターゲットステータス別のクローズされた脆弱性一致アイテム	棒グラフ	選択した時間スパンにおける修正ターゲットステータスによってグループ化された、クローズされた脆弱なアイテムの数。 注: [クローズした経過時間] の値は、データの収集時に計算されます。値は、last_opened の日付と収集ジョブの日時の差です。
アサイン先グループ別の重大な脆弱なアイテム	リストと折れ線グラフ	アサイン先グループごとにグループ化された、リスク評価が重大であるアクティブな脆弱性一致アイテムの数。
アサイン先グループ別の期限切れの重大な脆弱なアイテム	リストと折れ線グラフ	アサイン先グループごとにグループ化された、リスク評価が重大で修復ターゲット日が過去の日付になっている、アクティブな脆弱性一致アイテムの数。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タイトル	タイプ	説明
		修正ターゲットは、最後のオープン日に日数 (24 時間単位として測定) を加算して計算されます。 このレポートでは、保留された脆弱性一致アイテムは除外されます。

ビジネスサービス

名前	タイプ	説明
重大な脆弱なアイテム	リスト、折れ線グラフ、および分布棒	ビジネスサービスごとにグループ化された、リスク評価が重大であるアクティブな脆弱性一致アイテムの数。 現在の週と前の週の 1 週間あたりの平均、2 週の間の差 (カウントとパーセント)、および傾向を示します。 分布棒グラフには、スコアカードの現在のページにあるすべての値の間の差が表示されます。
期限切れの重大な脆弱なアイテム	リスト、折れ線グラフ、および分布棒	ビジネスサービスごとにグループ化された、リスク評価が重大で修復ターゲット日が過去の日付になっている、アクティブな脆弱性一致アイテムの数。 現在の週と前の週の 1 週間あたりの平均、2 週の間の差 (カウントとパーセント)、および傾向を示します。 分布棒グラフには、スコアカードの現在のページにあるすべての値の間の差が表示されます。 このレポートでは、保留された脆弱性一致アイテムは除外されます。
高脆弱なアイテム	リスト、折れ線グラフ、および分布棒	ビジネスサービスごとにグループ化された、リスク評価が高いアクティブな脆弱性一致アイテムの数。 現在の週と前の週の 1 週間あたりの平均、2 週の間の差 (カウントとパーセント)、および傾向を示します。 分布棒グラフには、スコアカードの現在のページにあるすべての値の間の差が表示されます。
期限切れの高脆弱なアイテム	リスト、折れ線グラフ、および分布棒	ビジネスサービスごとにグループ化された、リスク評価が高く修復ターゲット日が過去の日付になっている、アクティブな脆弱性一致アイテムの数。 現在の週と前の週の 1 週間あたりの平均、2 週の間の差 (カウントとパーセント)、および傾向を示します。 分布棒グラフには、スコアカードの現在のページにあるすべての値の間の差が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ビジネスサービス (続く)

名前	タイプ	説明
		このレポートでは、保留された脆弱性一致アイテムは除外されます。

サービスオーナー

名前	タイプ	説明
重大な脆弱なアイテム	リスト、折れ線グラフ、および分布棒	ビジネスサービスオーナーごとにグループ化された、リスク評価が重大であるアクティブな脆弱性一致アイテムの数。 現在の週と前の週の 1 週間あたりの平均、2 週の間の差 (カウントとパーセント)、および傾向を示します。 分布棒グラフには、スコアカードの現在のページにあるすべての値の間の差が表示されます。
期限切れの重大な脆弱なアイテム	リスト、折れ線グラフ、および分布棒	ビジネスサービスオーナーごとにグループ化された、リスク評価が重大で修復ターゲット日が過去の日付になっている、アクティブな脆弱性一致アイテムの数。 現在の週と前の週の 1 週間あたりの平均、2 週の間の差 (カウントとパーセント)、および傾向を示します。 分布棒グラフには、スコアカードの現在のページにあるすべての値の間の差が表示されます。 このレポートでは、保留された脆弱性一致アイテムは除外されます。
高脆弱なアイテム	リスト、折れ線グラフ、および分布棒	ビジネスサービスオーナーごとにグループ化された、リスク評価が高いアクティブな脆弱性一致アイテムの数。 現在の週と前の週の 1 週間あたりの平均、2 週の間の差 (カウントとパーセント)、および傾向を示します。 分布棒グラフには、スコアカードの現在のページにあるすべての値の間の差が表示されます。
期限切れの高脆弱なアイテム	リスト、折れ線グラフ、および分布棒	ビジネスサービスオーナーごとにグループ化された、リスク評価が高く修復ターゲット日が過去の日付になっている、アクティブな脆弱性一致アイテムの数。 現在の週と前の週の 1 週間あたりの平均、2 週の間の差 (カウントとパーセント)、および傾向を示します。 分布棒グラフには、スコアカードの現在のページにあるすべての値の間の差が表示されます。 このレポートでは、保留された脆弱性一致アイテムは除外されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性一致 CI

名前	タイプ	説明
CI クラス別の脆弱性一致構成アイテム (CI)	棒グラフ	CMDB 内の CI クラスによってグループ化された、アクティブな脆弱性を持つ構成アイテムの数。
CI クラスごとの脆弱性一致アイテム (VI)	ツリーマップ	CI クラス別のアクティブな VI の数。
CI あたりの平均脆弱なアイテム	棒グラフ	リスク評価によってグループ化された、構成アイテムに属する脆弱なアイテムの平均数。
一致しない CI	単一スコア	CMDB 内の既存の CI と一致しないインポートされた構成アイテムの数。
サポートグループのない脆弱性一致 CI	単一スコア	アサインされたサポートグループがない、脆弱な構成アイテムの数。
アクティブな VI を持つ廃止または盗難された CI	単一スコア	CMDB で [廃止] または [盗難] とマークされた、アクティブな脆弱性一致アイテムを持つ構成アイテムの数。

例外

名前	タイプ	説明
理由別の保留された脆弱なアイテム	棒グラフ	保留の理由によってグループ化された、保留された脆弱なアイテムの数。
期限切れ間近の保留要求 (Deferral Requests About to Expire)	棒グラフ	レビューのために再オープンしようとしている修復タスクや脆弱性一致アイテムに関連付けられた保留要求の数。要求は再オープンまでの残り日数ごとにグループ化されます。 メール通知が定義されていれば、メールが送信されます。
構成アイテム (CI) マネージャーによって保留された脆弱なアイテム (Deferred Vulnerable Items by Configuration Item (CI) Manager)	棒グラフ	関連する構成アイテムのマネージャーごとにグループ化された、保留された脆弱性一致アイテムの数。

修正

名前	タイプ	説明
リスク評価とステータス別の修復タスク	ヒートマップ	リスク評価とステータスごとにグループ化されたアクティブな修復タスクの数。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修正 (続く)

名前	タイプ	説明
リスク評価と修復ターゲットステータス別の修復タスク	ヒートマップ	リスク評価と修復ターゲットステータスごとにグループ化されたアクティブなタスクの数。 このレポートでは、保留された脆弱性一致アイテムは除外されます。
アサイン先グループ別の重大な修復タスク	リストと折れ線グラフ	アサイン先グループごとにグループ化された、リスク評価が重大であるアクティブな修復タスクの数。 このレポートでは、保留された修復タスクは除外されます。
アサイン先グループ別の期限切れの重大な修復タスク	リストと折れ線グラフ	アサイン先グループごとにグループ化された、リスク評価が重大で修復ターゲット日が過去の日付になっている、アクティブな修復タスクの数。 このレポートでは、保留された修復タスクは除外されます。
未アサインの修復タスク	単一スコア	アサイニーまたはアサイン先グループのないアクティブな修復タスクの数。
未アサインの脆弱なアイテム	単一スコア	アサイニーまたはアサイン先グループのないアクティブな脆弱なアイテムの数。

脆弱性対応のパフォーマンスアナリティクス **[PA]** レポートのリアルタイム表示

最も重要な脆弱性一致アイテム (VI) を管理し、それを迅速に修正できるようにするには、脆弱性管理 (PA) ダッシュボードでレポートをオンデマンドでリアルタイム表示します。脆弱性対応のパフォーマンスアナリティクス アプリケーションは、ServiceNow Store の別のサブスクリプションで利用できます。

始める前に

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

脆弱性対応のパフォーマンスアナリティクス のレポートの詳細については、「脆弱性管理 (PA) ダッシュボード」を参照してください。

脆弱性対応のパフォーマンスアナリティクス アプリケーションの設定とインストールの詳細については、「脆弱性対応のパフォーマンスアナリティクス [PA] アプリケーションのインストールと構成」を参照してください。

表示されていない場合、ダッシュボードを表示するには、次に移動します: 脆弱性対応 > 概要. ダッシュボードの上部にレポートタブが表示されます。

脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で表示することもできます。新しい UI でダッシュボードを表示するには、次に移動します: ワークスペース > 脆弱性マネージャーワークスペース をクリックし、[ダッシュボード] アイコンをクリックします。ロールに応じてデフォルトのダッシュボードが表示されます。他のダッシュボードを表示するには、

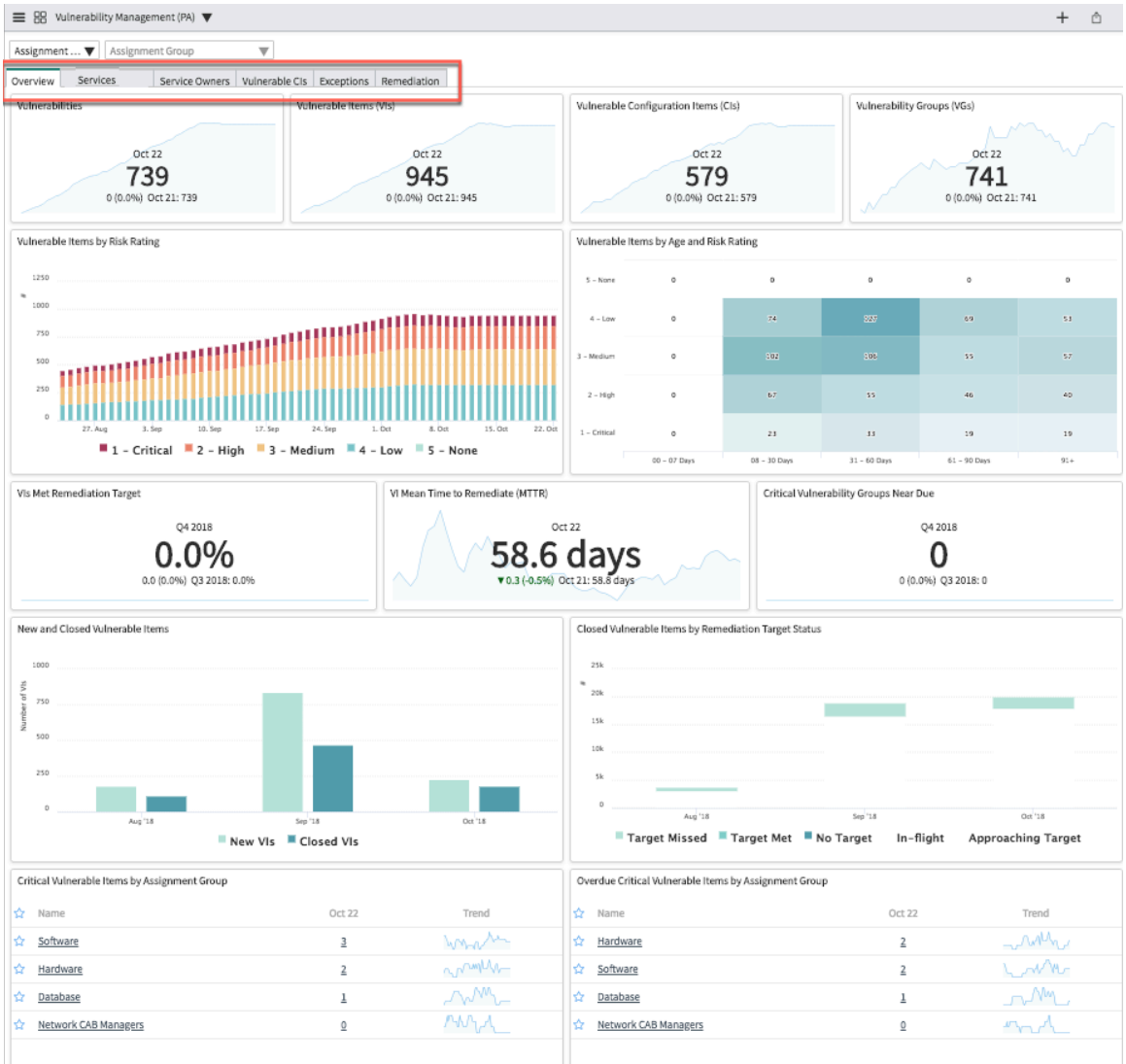
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ダッシュボード名の横にあるドロップダウンをクリックします。詳細については、「脆弱性マネージャーワークスペースのダッシュボード」および「IT 修復ワークスペースのダッシュボード」を参照してください。

注:
Tokyo を使用している場合は、ネクストエクスペリエンス UI でダッシュボードを表示できますが、一部の機能が失われます。

[概要] タブ



脆弱性管理 (PA) ダッシュボードのタブで、以下のレポートをリアルタイム表示します。

- [概要] タブ
  - アサイン先グループ別の重大な脆弱性一致アイテム
- [脆弱性一致 CI] タブ：
  - 所有者のいない脆弱性一致 CI (Vulnerable CIs Without Owners)
  - アクティブな VI を持つ廃止または盗難された CI
- [例外] タブ：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

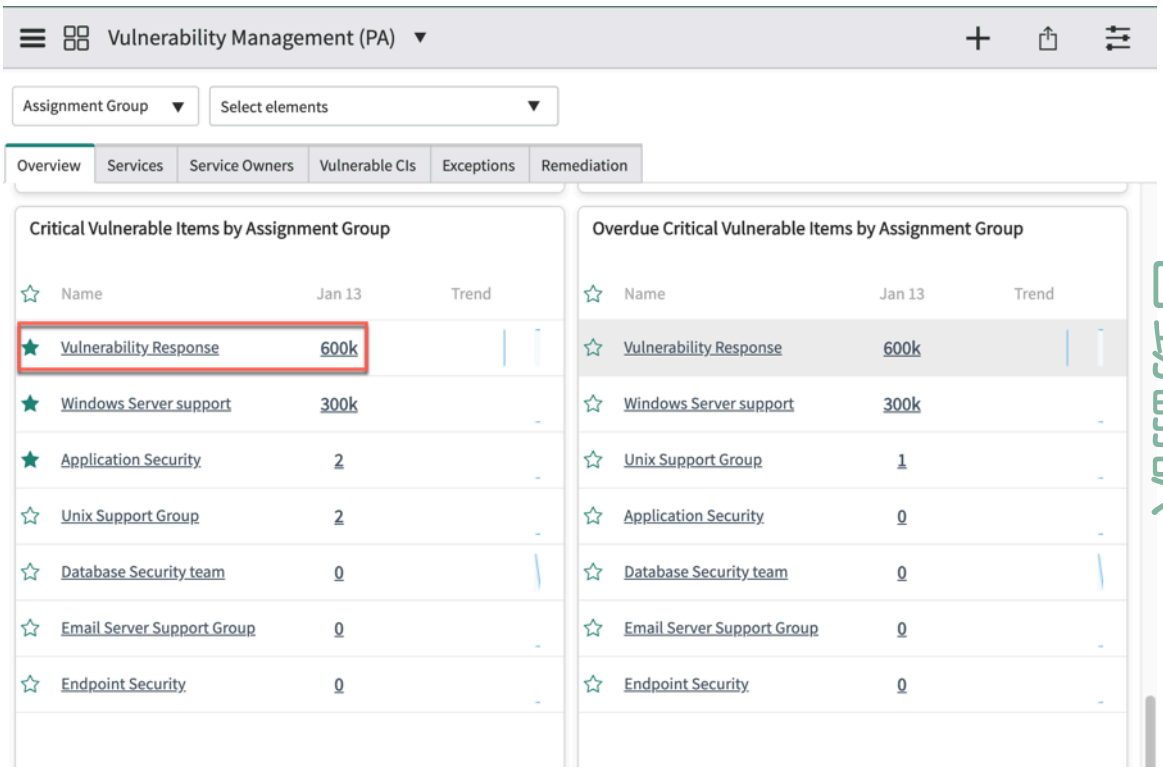
- 理由別の保留された脆弱性一致アイテム
- 期限切れ間近の保留要求 (Deferral Requests About to Expire)
- CIO マネージャーによって保留された脆弱性一致アイテム (Deferred Vulnerable Items by CIO Manager)

- [修正] タブ：
  - 未アサインの脆弱性一致アイテム

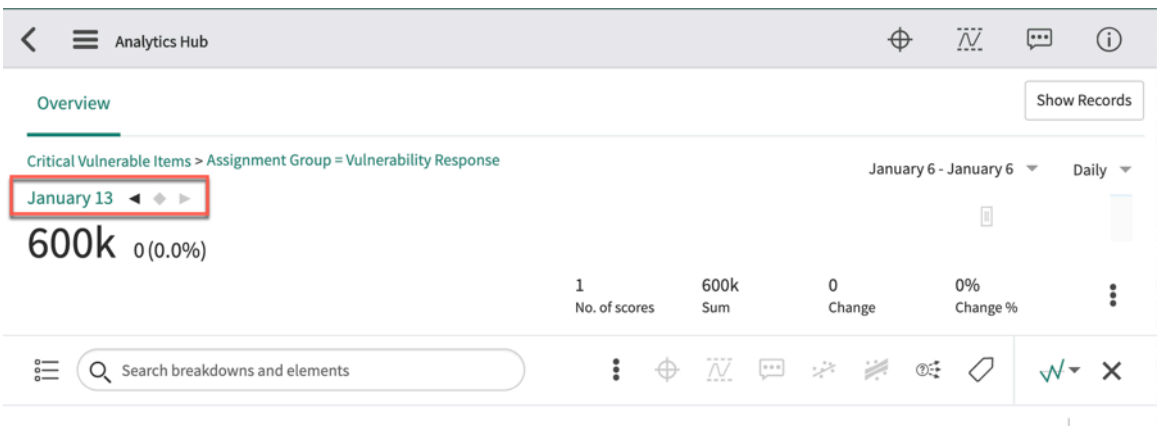
リアルタイムレポートを含むいずれかのタブを選択してリアルタイムスコアを表示するには、次の手順を実行します。

手順

1. [アサイン先グループ別の重大な脆弱性一致アイテム] などのレポートで、表示されているいずれかのリンクをクリックします。



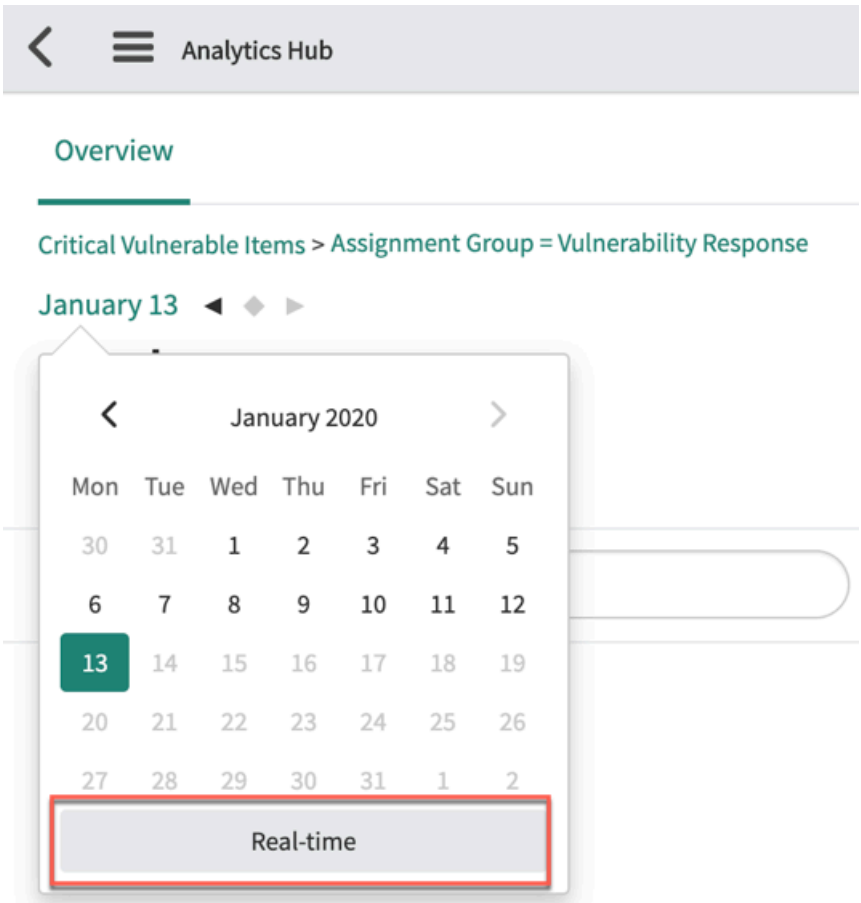
2. 表示されるレコードで、日付をクリックします。



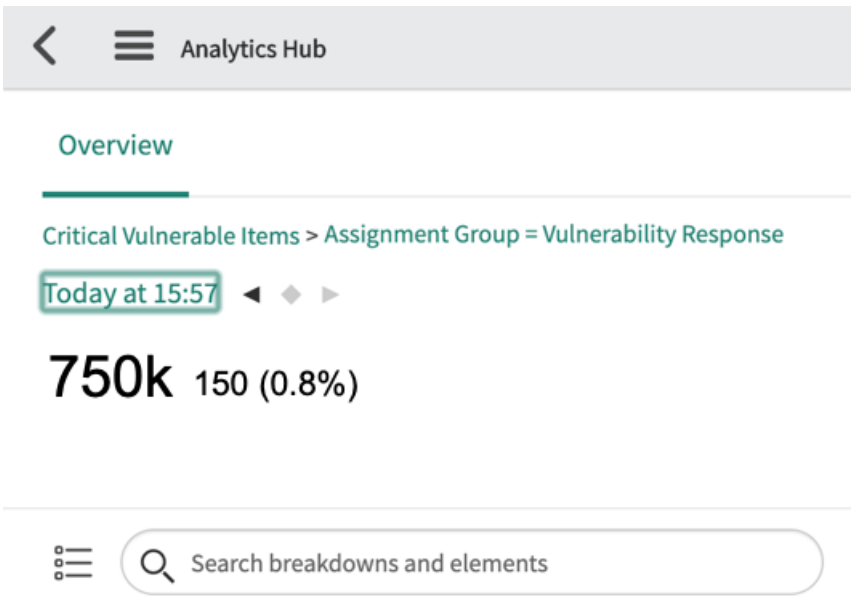
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 表示されるカレンダーで、[リアルタイム] をクリックします。

   レポートがリアルタイムスコアをサポートしていない場合、 [リアルタイム] ボタンはカレンダーに表示されません。



値が更新されるまでに少し時間がかかる場合があります。現在の日付、レコード、前回のレポート以降の新規レコードの数、および前回のレポートからの変化率も表示されます。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. オプション: リアルタイムレポートを表示した状態で、レポートを構成するレコードを表示するには、右上の [レコードを表示] をクリックします。
   スコアを構成するレコードのリストが表示されます。

脆弱性対応 の パフォーマンスアナリティクス **[PA]** インジケーターの表示

インスタンス内の脆弱性データを表す自動化され定式化された パフォーマンスアナリティクス インジケーターを表示します。

始める前に

インジケーターのレコード収集オプションは、パフォーマンスアナリティクス - コンテンツパック - 脆弱性対応アプリケーションでは、デフォルトで無効になっています。このオプションが無効になっているのは、特定のレポートをリアルタイムで表示可能にするためです。手動でのレコードの収集を有効にして、スコアを構成するレコードを表示した方がよい場合は、これらのインジケーターで使用される傾向情報を引き続き使用できます。

注:
インジケーターでレコードの収集をアクティブ化すると、パフォーマンスに悪影響が及び、データコレクションジョブの実行に必要な時間やメモリがかなり多くなる場合があります。

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

必要なロール：sn_vul.vulnerability_admin、sn_vul.admin (非推奨)、または pa.viewer

このタスクについて

脆弱性対応 には、自動インジケーターと定式化インジケーターの両方があります。

主要な用語

PA インジケーター
: ビジネスサービス、アクティビティ、または組織行動の、定期的に取得されるパフォーマンス測定値 ([保留されていない期限切れの重大な脆弱性一致アイテム] など) を定義します。

PA インジケーターソース
: 1 つのテーブルまたはデータベースのビューからレコードをフィルタリングするデータセット (VI アクティブなど)。

レコードの収集
: 有効にすると、レコードがメモリに保存され、アナリティクスハブにアクセスできるようになります。

ブレークダウン
: ブレークダウンは、収集されたレコードをフィルタリングしてグループ化します。ブレークダウンは、特にその数と多様性が増加すると、メモリ使用量が増加する可能性があります。

ブレークダウンの除外
: 除外により特定のブレークダウンが削除されます。これにより、メモリ消費量が減る可能性があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 自動インジケーターの場合は、次に移動します: パフォーマンスアナリティクス > インジケーター > インジケーター (自動).
2. 定式化されたインジケーターの場合は、次に移動します: パフォーマンスアナリティクス > インジケーター (計算).

   インジケーターの詳細については「パフォーマンスアナリティクスインジケーター」を参照してください。

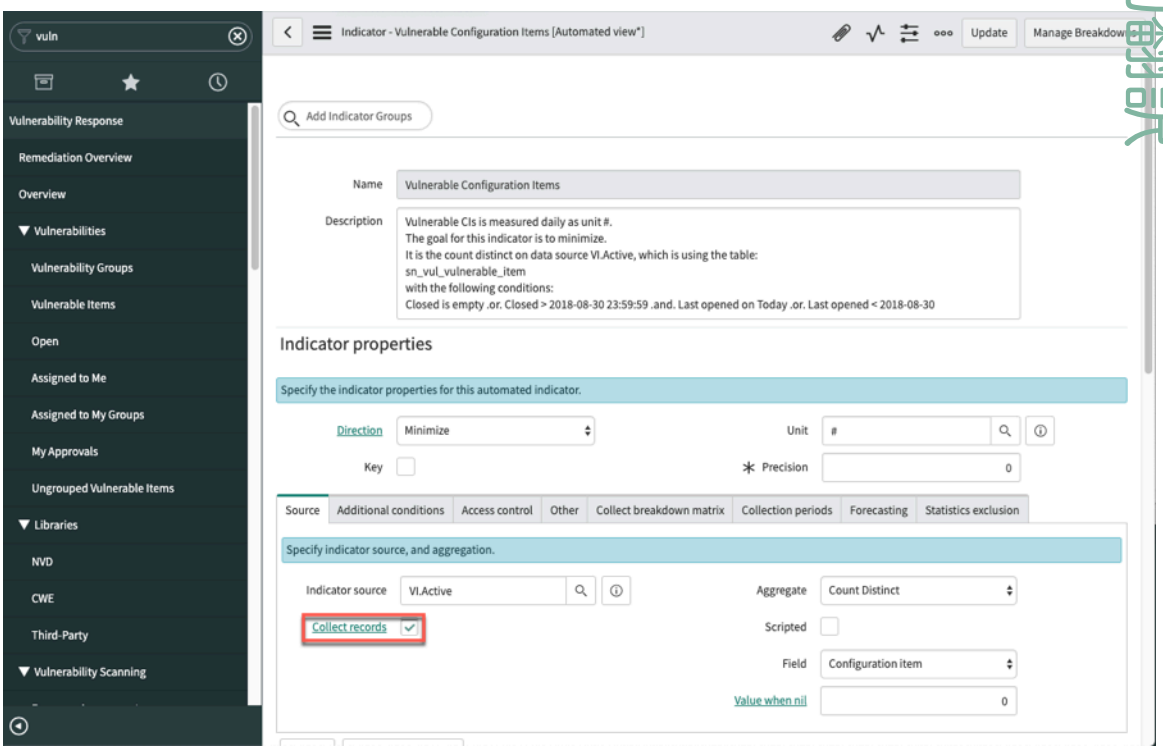
3. いずれの場合も、検索対象: アプリケーション > パフォーマンスアナリティクス.

   注:
   デフォルトのビューにない場合は、ページの左上隅にある歯車アイコン ( ) を使用して [アプリケーション] 列を追加します。[アプリケーション] 列が [検索] ドロップダウンメニューに表示されます。

4. オプション: 脆弱性対応 のパフォーマンスアナリティクスインジケーターでレコードの収集を有効にするには、次の手順を実行します。

   a. 自動インジケーターのリストを表示した状態で、[名前] 列で、レコードの収集を有効にするインジケーターをクリックします。
   インジケーターレコードが表示されます。

   b. [ソース] タブを選択した状態で、[インジケータープロパティ] セクションで [レコード収集] チェックボックスをオンにします。



   c. 1 つ選択して続行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

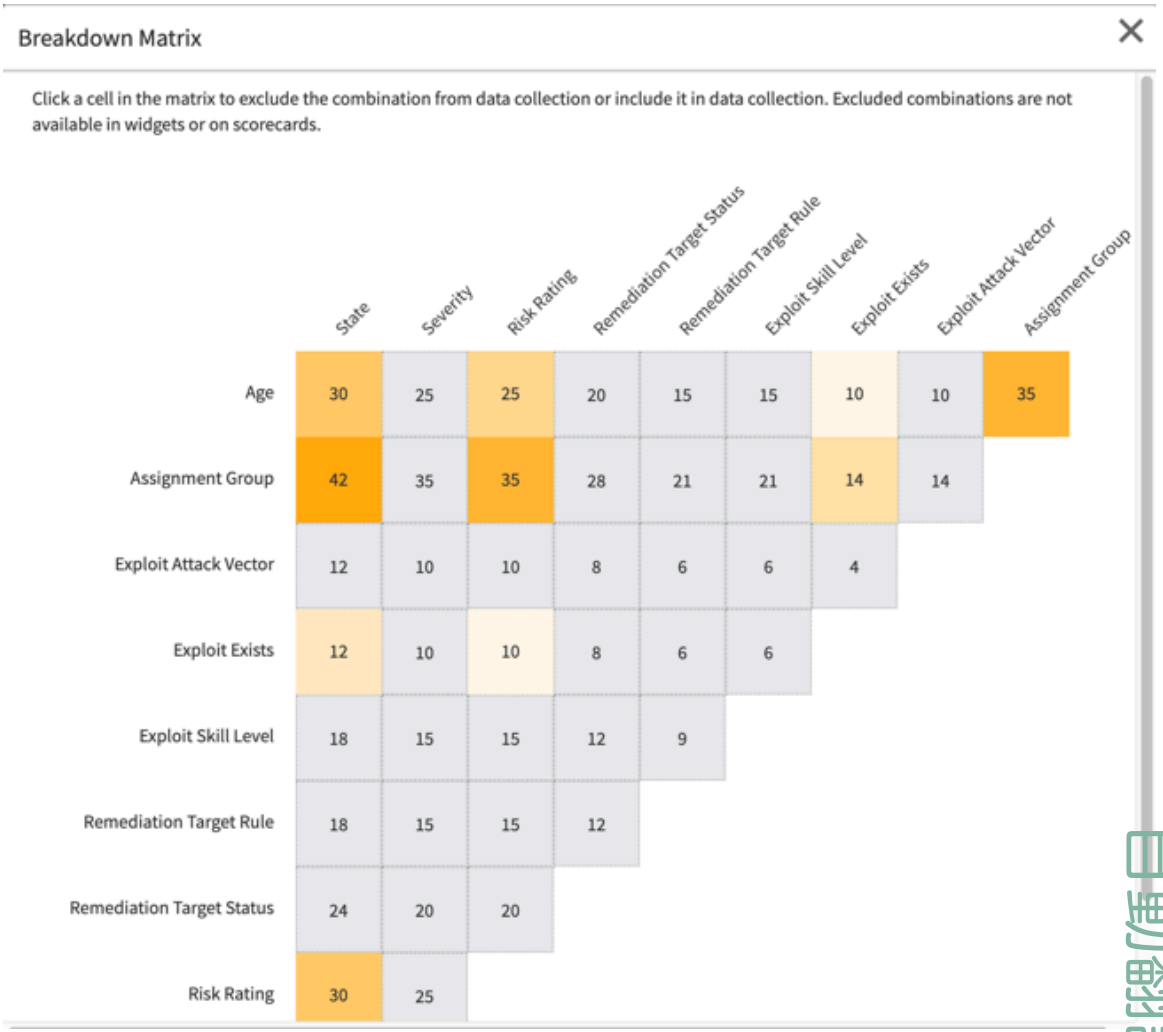
オプション	説明
更新	編集を保存してインジケーターリストに戻ります。
ブレークダウンを管理 **注:** 第 2 レベルのブレークダウンを再アクティブ化すると、メモリ消費量が大幅に増加し、データ収集ジョブの速度が低下する恐れがあります。 デフォルトでは、第 2 レベルのブレークダウンの除外は、以下のインジケーターに適用されています。 ▪ 脆弱性一致構成アイテム ▪ 廃止された CI ▪ 保留 VI	リストされたインジケーターの第 2 レベルのブレークダウンを再アクティブ化するか、他のインジケーターのブレークダウンを編集します。 (Optional) パフォーマンスアナリティクスのブレークダウンの詳細については、「パフォーマンスアナリティクスのブレークダウン」を参照してください。

d. [ブレークダウンを管理] をクリックします。

e. 表示されるフォームで、[ブレークダウンマトリクスを構成] をクリックします。
[ブレークダウンマトリクス] フォームが表示されます。次の図に示すように、除外された組み合わせが選択され、色付きで表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

f. 除外を削除し、除外した組み合わせを再アクティブ化するには、選択したセルをクリックします。

g. フォームの右上にある [クローズ] をクリックして、[ブレークダウンを管理] フォームに戻ります。

h. 戻る矢印をクリックして、インジケーターレコードに戻ります。

i. [更新] をクリックして編集内容を保存し、インジケーターリストに戻ります。

集計されたレポートフレームワーク

集計レポートフレームワークを使用すると、複雑で長時間実行されるオンザフライクエリを含むデータのレポートを作成して、パフォーマンスを向上させることができます。

集計されたレポートフレームワークは、次の方法でパフォーマンスを向上させます。

- より少ないリソース使用量で、迅速にレポートをレンダリングする
- データを集計し、集計とブレークダウン ([グループ分け基準]) を再利用する
- データベースへの照会を減らす

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性一致アイテムが 100 万を超える場合は、標準レポートとともに共通脆弱性対応で提供される集計レポートフレームワークを使用します。

必要なロール

このソリューションには、次のロールとタスクが関連付けられています。

- Now Platform アドミン (admin)：この プラットフォームアナリティクスソリューション をインストールしてアクティブ化し、システムのプロパティに必要な変更を加えます。
- パフォーマンスアナリティクス アドミン (pa_admin)：集計、ウィジェット、およびダッシュボードを確認します。データ収集を設定して開始します。適切なステークホルダーとダッシュボードを共有します。
- アドミン (sn_vul_cmn.admin)：集計を作成します。
- VR 書き込み (sn_vul_cmn.write)：集計および集計結果のデータを編集します。
- VR 読み取り (sn_vul_cmn.read)：集計および集計結果のデータを確認します。
- 脆弱性アナリスト [sn_vul.vulnerability_analyst]：集計結果を確認します。

関連情報

ソースデータの集計を構成する

複数の集計を同時に実行する

同時に実行できる集計の数を構成する

集計を使用してレポートを作成する

ソースデータの集計を構成する

ServiceNow テーブルに記録されているビジネスプロセス内の特定のファセットのパフォーマンスを分析するには、ファセットに固有の集計を作成し、この集計のレポートを作成します。

始める前に

必要なロール：sn_vul_cmn.admin

手順

1. 次のように移動する。 **All** (すべて) > 集計されたレポート > アグリゲーション定義 > **All** (すべて) をクリックし、[新規] をクリックします。
2. [名前] フィールドで、集計にわかりやすい名前を付けます。
3. [説明] フィールドに、集計の簡単な説明を入力します。
4. [ソース] タブで、フィールドに入力します。

[ソース] タブのフィールド

フィールド	説明
テーブル	レポートのデータの取得元となるテーブル。このドロップダウンには、app sec common、app-vul、app-vulc、app-vul-container、およびアプリケーション脆弱性テーブルのみが含まれています。
集計関数	[フィールド] で選択した列に適用する関数。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ [カウント **(Count)**]：レコードの数。 ○ [合計]：[フィールド] で選択した列の値の合計。 ○ [平均]：[フィールド] で選択した列のすべての値の平均。 ○ [最大]：[フィールド] で選択した列の最大値。 ○ [最小]：[フィールド] で選択した列の最小値。 ○ [個別のカウント]：[フィールド] で選択した列の一意の値。
フィールド	関数を適用する列。 **注:** [アグリゲート関数] フィールドで [カウント **(Count)**] が選択されている場合、このフィールドは表示されません。

5. [追加条件] タブで、[条件] フィールドに条件を入力して、集計結果を取得する特定のレコードセットを選択します。
6. [グループ分け基準] タブで、データのグループ化またはスタックの基準となるテーブルの列を選択します。
   最大 2 つのブレークダウンを選択できます。

   いずれかの [グループ分け基準] フィールドで [日付 **(Date)**] 列を選択すると、[傾向の基準 **(Trend by)**] フィールドが表示されます。[傾向の基準 **(Trend by)**] フィールドのオプションを選択すると、週、日、分などで分類された集計結果を取得できます。
7. [スケジュール] タブで、集計スケジュールを選択または作成します。集計スケジュールは、集計を実行してデータをフェッチできる頻度を定義します。
   集計スケジュールを作成するには、「複数の集計を同時に実行する」を参照してください。

   注: 非アクティブな集計定義に対する集計実行をスケジュールすることはできません。
8. [送信] をクリックして集計を作成します。
   集計が [集計] リストに表示されます。事前定義された頻度で集計が実行され、実行ごとにレコードが実行日時とともに [スケジュール済み実行] 関連リストに作成されます。
9. 次のように移動する。 **All** (すべて) > 集計された結果 をクリックし、集計を開いて [Aggregated Results] と [Scheduled Runs] を確認します。
   集計結果は、[集計された結果] 関連リストにリストされます。集計実行が失敗した場合、詳細については、[スケジュール済み実行] 関連リストの [メモ **(Notes)**] 列を参照してください。
10. オプション: 集計スケジュールに関係なく集計結果を収集するには、[今すぐ実行] を選択します。スケジュール実行が進行中に終了した場合、集計結果は変更されません。集計を削除または非アクティブ化することもできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のタスク
集計を使用したレポートを作成します。集計を使用したレポートの作成の詳細については、「集計を使用してレポートを作成する」を参照してください。

関連情報

- 集計されたレポートフレームワーク
- 複数の集計を同時に実行する
- 同時に実行できる集計の数を構成する
- 集計を使用してレポートを作成する

複数の集計を同時に実行する

単一の集計スケジュールを使用して、複数の集計の実行をスケジュールできます。

始める前に
必要なロール：sn_vul_cmn.admin

このタスクについて
6 つの集計を同時に実行するとします。集計スケジュールを作成し、それにすべての集計を追加します。これらの集計は、定義された頻度と時間で実行されます。

手順

1. 次のように移動する。 **All** (すべて) > 集計されたレポート > スケジュール.
2. **[New** (新規)] を選択します。
3. [集計スケジュー] フォームで、フィールドに入力します。

フィールド	説明
スケジュール名	集計スケジュールの名前。
ジョブをスケジュール	集計を実行する頻度を定義するスケジュール済みスクリプト実行。スケジュールジョブを作成するには、[新規] ボタンを選択します。

4. [送信] を選択します。
   集計スケジュールが [集計スケジュール] リストに表示されます。
5. 集計スケジュールを開きます。
6. [編集] を選択し、[集計リスト **(Aggregation List)]** に集計を追加して、[保存] を選択します。
   選択した集計が [集計 (Aggregations)] 関連リストに表示されます。

   注:
   スケジュールに非アクティブな集計を追加すると、スケジュールされた実行は開始されません。

7. [更新] を選択します。
   これらの集計は、集計スケジュールで定義された頻度で実行されます。

関連情報

- 集計されたレポートフレームワーク
- ソースデータの集計を構成する

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

同時に実行できる集計の数を構成する
集計を使用してレポートを作成する

同時に実行できる集計の数を構成する

新しいプロセッサーまたはバックグラウンドジョブである集計レポートフレームワークプロセッサーはベースシステムに付属しており、集計レポートフレームワークテーブルに関連するスケジュール済みジョブを実行します。これにより、サブシステム全体をバックグラウンドで実行でき、使用可能なときにシステムリソースをより有効に活用できます。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > バックグラウンドジョブ構成 **– Vulnerability Response** 共通:集計結果算出.
2. 同時に実行する集計の数を [最大同時スレッド] フィールドで定義し、[保存] を選択します。
   デフォルトでは、4 つの集計が同時に実行されます。
3. [Background Job Processor Pools] リストに移動します。
   sn_sec_cmn_background_job_processor_pool.listをクリックし、[新規] を選択して、集計レポートフレームワークのバックグラウンドジョブプロセッサを作成します。
   バックグラウンドジョブプロセッサープールの作成方法の詳細については、「脆弱性対応のバックグラウンドジョブの高度な並列処理」を参照してください。

   注:
   バックグラウンドジョブプロセッサーの数は、[バックグラウンドジョブ構成 - 脆弱性対応共通 - 集計結果算出 **(Background Job Configuration – Vulnerability Response Common-Aggregation Result Calculator)]** フォームで指定された最大同時スレッド数と同じである必要があります。ステップ 2 を参照してください。

関連情報

集計されたレポートフレームワーク
ソースデータの集計を構成する
複数の集計を同時に実行する
集計を使用してレポートを作成する

集計を使用してレポートを作成する

作成した集計に固有であるデータを視覚化して分析するには、条件ビルダーで集計の条件を指定してレポートを生成します。

始める前に
必要なロール：pa_admin

手順

1. 次のように移動する。 **All** (すべて) > レポート > 新規作成.
2. [データ] タブで、フィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[データ] タブのフィールド

フィールド	説明
レポート名	レポートの名前。
ソースタイプ	データのフェッチ元のソースのタイプ。[テーブル] を選択します。
テーブル	集計が作成されるテーブルの名前。集計結果テーブル [集計結果 **[sn_vul_cmn_aggregate_result]** を選択します。

3. 条件ビルダーで、レポートを生成する集計の条件を設定します。

条件ビルダーでの条件

部品	説明
フィールド	[集計] を選択します。
演算子	[次の値である **(is)]** を選択します。
値	アグリゲーションの名前。

4. [データ] タブで、 [次へ] を選択します。
5. [種類] タブで、データを視覚化する方法を選択し、[次へ] を選択します。
レポートタイプの詳細については、「 レポートの作成 」を参照してください。

   サポートされている可視化は、棒グラフ、円グラフ、ヒートマップです。折れ線グラフやその他の傾向の可視化を変更して、集計結果でサポートされている可視化を利用して、同じデータを表すことができます。リストビューはサポートされていません。

6. [構成] タブで、フィールドに入力します。

フィールド	説明
グループ	選択したフィールドでデータをグループ化します。 ここでは、集計の [#unique_468_Connect_42_group-by] タブの [**1** でグループ化] フィールドで選択したフィールドを選択します。
積み重ね基準	選択したフィールドに基づいてデータをレイヤーに整理します。 ここでは、集計の [#unique_468_Connect_42_group-by] タブの [2 でグループ化] フィールドで選択したフィールドを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: 棒グラフと水平棒グラフのレポートでのみ積み重ねデータを使用します。他のレポート タイプでは、グループ化のみが可能です。
集計	[最小] または [最大] 機能を [値 **(Value)**] に適用します。

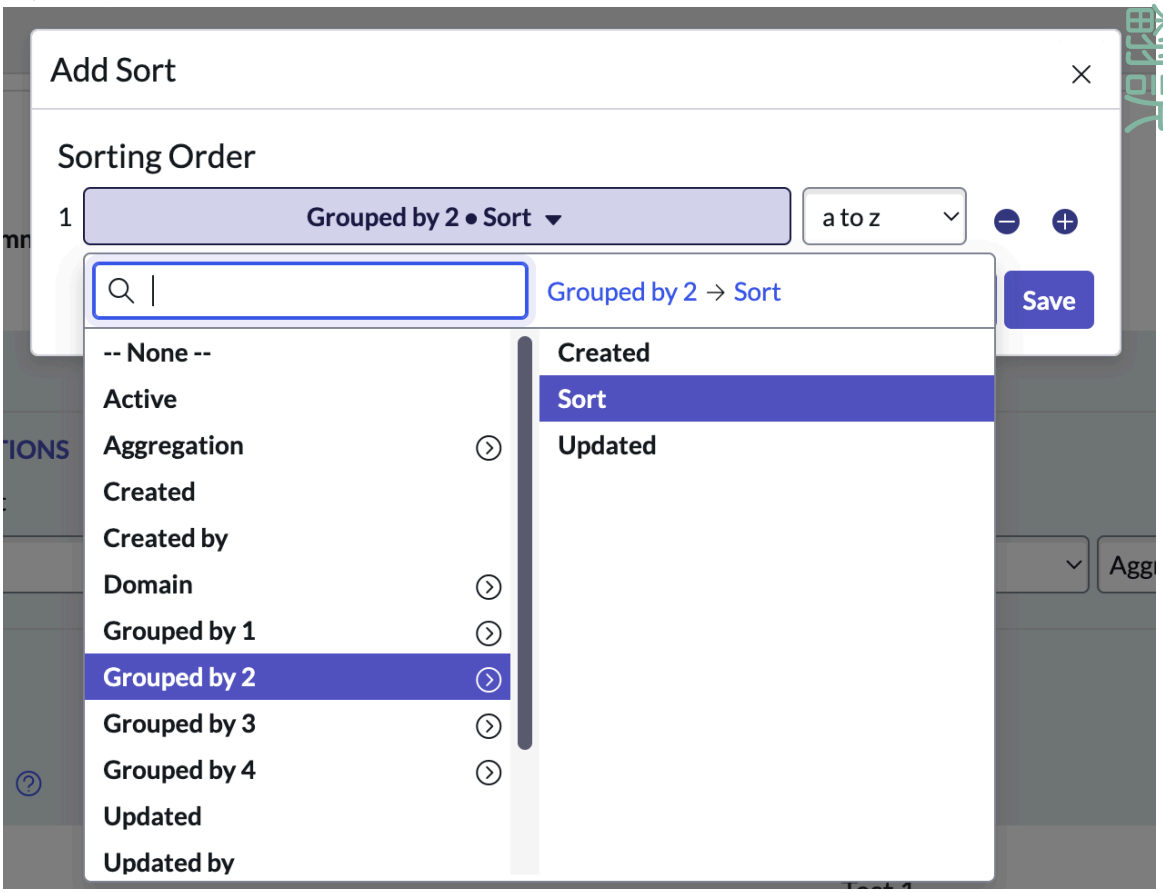
7. [スタイル] タブで、必要に応じてフィールドに入力し、[実行] を選択します。
[構成] タブと [スタイル] タブのフィールドの詳細については、「レポートの作成」のビデオを参照してください。
8. 条件ビルダーで、レポートを生成する集計の条件を設定し、[実行] を選択します。

   レポートが表示されます。
9. X 軸の値を並べ替えるには、 [並べ替えの追加] を選択します。

   a. 文字列の場合は、条件を [グループ化基準] **> [a ～ z]** または **[z ～ a]** と指定して、文字列をアルファベット順に並べ替えます。

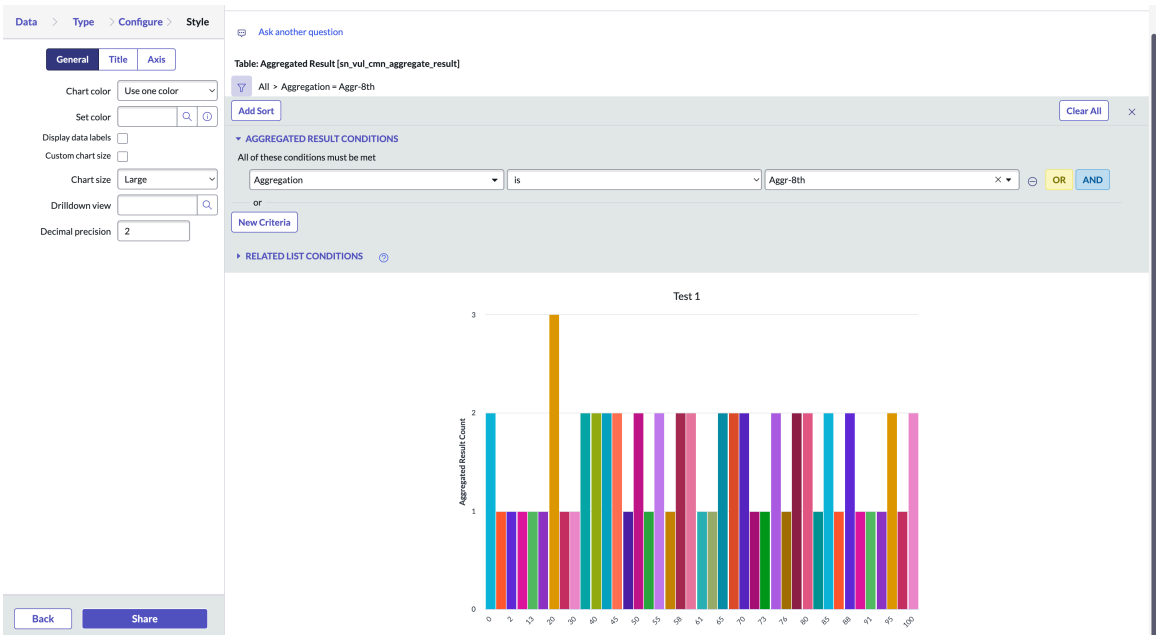
   b. 整数および日付データタイプの値の場合は、条件を [グループ化基準] [ソート] **> [a ～ z]** または **[z ～a]** と指定して、値をそれぞれ昇順または降順で並べ替えます。

X 軸の整数のソート



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

c. [実行] を選択します。
整数値と日付値は X 軸でソートされます。



10. [保存] を選択してレポートを保存します。
集計に対して生成されたレポートは、それぞれの [集計] フォームの [結果] タブに表示されます。

11. オプション: ダッシュボードにレポートを追加します。
ダッシュボードにレポートを追加する方法の詳細については、「レスポンシブダッシュボードにレポートを追加する」を参照してください。

キャッシュされたレポートフレームワークを使用して作成されたレポートで構成される [脆弱性管理 [集計]] ダッシュボードは、ベースシステムに付属しています。このダッシュボードを表示するには、次に移動します: **All** (すべて) > パフォーマンスアナリティクス > ダッシュボード > **All** (すべて) > 脆弱性管理 [集計]. このダッシュボードのレポートに対応するアクティブな集計がベースシステムに付属しています。

12. レポートを他のユーザーと共有します。
レポートを共有する方法の詳細については、「レポートの配布」を参照してください。

関連情報

ソースデータの集計を構成する

集計されたレポートフレームワーク

複数の集計を同時に実行する

同時に実行できる集計の数を構成する

脆弱性対応 の参照情報

以下のトピックでは、脆弱性対応 にあるフォームやレコードのフィールドデータのほかに、リンク、参照情報、トラブルシューティング、ナレッジ記事について説明します。

以下は、HI ナレッジベースにある「VR/CC のサポートとトラブルシューティングのためのナレッジベースリンク」記事へのリンクをはじめとする、役に立つと思われるその他のリソースへのリンクです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- VR/CC のサポートとトラブルシューティングのためのナレッジベースリンク
- アプリケーションと互換性の詳細については、「KB0856498 脆弱性対応互換性マトリックスおよびリリーススキーマの変更点」を参照してください。
- Security Operations ビデオ
- 開発者トレーニング
- 開発者ドキュメント
- 実装スペシャリストと協力して、Customer Success Center を使用して目的のビジネス成果を達成します。
- 脆弱性対応コースを活用して専門知識をビルドし、短期間で ROI を実現します。サインアップするには、ServiceNow のトレーニングと認定資格 サイトにアクセスしてください。
- アプリケーションとともにインストールされているコンポーネントの検索
- 脆弱性対応オーケストレーション
- 統合を作成するためのヒント
- Security Operations Community で質問や回答をする
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

脆弱性対応 アプリケーションの実装チェックリスト

このチェックリストには、Now Platform® インスタンスでの 脆弱性対応 アプリケーションの基本的な実装に必要な手順が記載されています。こうしたタスクを完了すると、ベースシステムの運用と検証の準備が整います。

始める前に

必要なロール：アプリケーションのダウンロードとアクティブ化、およびロールのアサインを行う場合は admin、脆弱性対応 を構成する場合は sn_vul.vulnerability_admin。

手順

1. 完了したらタスクをチェックできるように、このチェックリストの PDF を作成して印刷することを検討してください。
2. PDF を生成するには、トピックの上部にある **[PDF** として保存] アイコン ( ) をクリックし、[選択したトピック (Selected topic)] をクリックします。

アドミンの 脆弱性対応 基本実装チェックリストタスク

アイテム	説明
☐	admin ロールを持つユーザーとして、エンタイトルメントを取得し、ServiceNow Store から Now Platform インスタンスに以下のアプリケーションをダウンロード (インストール) していることを確認します。 ○ 脆弱性対応 ○ NIST National Vulnerability Database との 脆弱性対応 統合 ○ Qualys Integration for Security Operations

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アイテム	説明
	a. アプリケーションがインスタンスで利用可能であることを確認するには、**All** (すべて) > システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて) をクリックし、[sn_vul]、[sn_vul_nvd]、および [sn_vul_qualys] を検索します。 **b.** アプリケーションが見つからない場合、アプリケーションのエンタイトルメントの取得とダウンロードの詳細については、「セキュリティオペレーション および ServiceNow Store」を参照してください。
☐	admin ロールを持つユーザーとして、以下に移動します。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合アプリケーションのインストール をクリックし、脆弱性対応 アプリケーションを、Now Platformインスタンスへの依存関係とともにアクティブ化 (インストール) します。 **注:** 脆弱性対応 アプリケーションのインストール中に、デモデータをインストールするオプションがあります。 インストール後に自動テストを実行してインスタンスが機能することを確認する場合は、デモデータが必要です。データの破損や機能停止を避けるため、テストは、開発、テスト、およびその他の非本番インスタンスでのみ実行してください。デモデータやデモアカウントが作成されている場合は、非本番環境または本番環境でインスタンスを使用する前に、すべてのデモデータを削除する必要があります。 脆弱性対応 のセットアップアシスタントは、アプリケーションとともに自動的にインストールされます。脆弱性対応 アプリケーションを構成するには、セットアップアシスタントが必要です。さらにセットアップアシスタントは、この例で使用されている Qualys Integration for Security Operations アプリケーション、およびそのほかに 脆弱性対応 をサポートするアプリケーションや、それと互換性のあるアプリケーションのインストールと構成にも使用されます。 脆弱性対応 アプリケーションのインストールの詳細については、「脆弱性対応 のインストール」を参照してください。
☐	admin ロールを持つユーザーとして、セットアップアシスタントで次の場所に移動します: **All** (すべて) > 脆弱性対応ユーザーおよびグループ をクリックし、必要な 脆弱性対応 ペルソナロールをユーザーにアサインします。 **a.** セットアップアシスタント内から、[ユーザー管理モジュール] リンクをクリックして、既存のユーザーと既にアサインされているロールを表示します。 **b.** リストからユーザー名をクリックしてレコードを開き、[ロール] 関連リストをクリックします。このユーザーにアサインされているすべてのロールが表示されます。 **c.** に戻る 脆弱性対応ユーザーおよびグループ を選択し、プロンプトに従って sn_vul.vulnerability_admin ロールをアサインします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アイテム	説明
	注: 構成を続行するには、sn_vul.vulnerability_admin ロールが必要です。または、admin ロールを持つユーザーとして構成を続行することもできます。 (オプション) 構成アイテム (CI) マネージャー [sn_vul.ci_manager] および例外承認者 [sn_vul.exception_approver] ロールをアサインすることもできますが、これらのペルソナは残りのセットアップタスクには必要ありません。 セットアップアシスタントを使用したペルソナロールのアサインの詳細については、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。 ユーザーの詳細、およびユーザーとグループへのロールのアサインの詳細については、「ユーザー管理」を参照してください。
☐	**a.** 次のように移動する。 **All** (すべて) > アドミニストレーション > 統合 をクリックし、 **CWE Comprehensive 2000** 統合 がアクティブ化されていることを確認し、スケジュール済みジョブを実行してデータをインポートします。 **b.** admin ロールを持つユーザーとして、次の場所に移動します: システム アプリケーション > 利用可能なすべてのアプリケーション をクリックし、NVD の脆弱性対応統合アプリケーションをアクティブ化 (インストール) します。 NVD および CWE 統合は、脆弱性対応 の初期設定の一部として、サードパーティのスキャナー製品を使用してインスタンスに脆弱性データをインポートする前に実行します。 NVD および CWE ライブラリのインストール、構成、および表示に関する詳細については、「NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理」および「CWE レコードの更新のためのスケジュール済みジョブの構成および実行」を参照してください。
☐	admin ロールを持つユーザーとして、以下に移動します。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合 アプリケーションのインストール をクリックし、 Qualys Integration for Security Operations アプリケーションをアクティブ化します。ライブラリのある Qualys などのサードパーティスキャナー製品をインストールして実行する前に、まず NVD と CWE の統合をインストールして実行し、脆弱性データを取り込む必要があります。 詳細については、「セットアップアシスタントを使用した 脆弱性対応 サードパーティアプリケーションのインストール」を参照してください。
☐	(オプション) admin ロールを持つユーザーは、脆弱性対応 アプリケーションを使用してデモデータをインストールした場合、脆弱性対応 ATF テストスイートを実行して、アプリケーションが正常にインストールされていることを確認できます。 **注:** データの破損や機能停止を避けるため、テストは、開発、テスト、およびその他の非本番インスタンスでのみ実行してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アイテム	説明
	詳細については、「脆弱性対応 の自動テストフレームワーク (ATF) テストスイートの実行」を参照してください。 自動テストの詳細については、「自動テストフレームワーク (ATF)」を参照してください。

3. [脆弱性対応設定] セクションで開始するアプリケーションの構成を続行します。

これらの設定を確認すると、環境の設定を続行する際の 脆弱性対応 の仕組みを理解しやすくなります。この例で使用するスキャナー統合の場合は、設定を編集する必要があります。

この構成例で使用する、Qualys 製品の概念は、他のスキャナーアプリケーションにも適用されます。

アプリケーションを構成するには、Qualys の認証情報が必要です。Qualys 製品にアクセスするために必要なアカウント名、パスワード、およびその他のサービス情報があることを確認します。

必要なロール：sn_vul.vulnerability_admin、または admin。

脆弱性アドミンの 脆弱性対応 基本実装チェックリストタスク

タスク	説明
☐	脆弱性アサインルールを確認します。 アサインルールにより、 脆弱性一致アイテム (VI) は適切なアサイン先グループに自動的にアサインされます。詳細については、「脆弱性対応 アサインルールの概要」を参照してください。 セットアップアシスタントを使用した 脆弱性対応 の構成の詳細については、「セットアップアシスタントを使用した 脆弱性対応 の構成」を参照してください。
☐	修復タスクルールを確認します。 修復タスクルールにより、脆弱性一致アイテム (VI) は特定の条件に基づいてインポートされると、自動的にグループ化されます。詳細については、「脆弱性対応修復タスクとタスクルールの概要」を参照してください。
☐	リスク算出を確認します。 リスク算出では、優先順位付けのために脆弱性一致アイテムのスコアを付けます。構成アイテム (CI) の特性、エクスプロイトの可用性、および脆弱性アセスメント (スキャナー) ベンダーによって報告された脆弱性の重大度を組み込むように算出を構成できます。詳細については、「脆弱性対応 の算出と脆弱性算出ルール」を参照してください。
☐	修復ターゲットルールを確認します。 修復ターゲットルールでは、VI および修復タスクの修正タイムラインを定義します。詳細については、「脆弱性対応 の修復ターゲットルール」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスク	説明
☐	[統合構成] セクションで、Qualys アプリケーション設定を確認し、データインポートを定義してスケジュールします。 **a.** [スキャナー統合] をクリックします。 **b.** [インストール済みアプリケーション] ページで、[編集] をクリックします。 **c.** 認証情報を入力し、[次へ] をクリックします。 **d.** ナレッジベース設定の説明を読みます。 **e.** [ホスト検出設定] ページの [設定をインポート]、[CI ルックアップルール]、および [スケジュールをインポート] を確認します。 **f.** このページの設定に問題がなければ、[今すぐ実行] をクリックしてデータをインポートします。表示される [詳細を表示] リンクをクリックして、脆弱性統合実行のステータスを表示します。 **g.** (オプション) 構成設定の編集を続行します。 **h.** [完了] をクリックして、セットアップアシスタントでのインストールと構成を完了します。 Qualys アプリケーションの構成の詳細については、「セットアップアシスタントを使用した Qualys 脆弱性統合の構成」を参照してください。

次のタスク
おめでとうございます! セットアップアシスタントを使用して 脆弱性対応 アプリケーションが正常にインストールされ、スキャナーアプリケーションとともに構成されました。これで、ベースシステムの運用準備が整いました。

脆弱性対応 の他のアプリケーションをダウンロード、インストール、および構成するには、前のチェックリストで実行した同じ手順と概念に従います。詳細については、各アプリケーションに用意されている個々のトピックを参照してください。

脆弱性対応 向けに ServiceNow Store から入手できる、サポートされているアプリケーションの詳細については、「脆弱性対応 およびサポートされているアプリケーションのインストール」を参照してください。

脆弱性対応 の使用方法の詳細については、「脆弱性対応アプリケーションの詳細」を参照してください。

脆弱性対応 修復タスクステータス

サードパーティ統合では、新しい脆弱性一致アイテム (VIT) を作成したり既存の VIT を更新したりする脆弱性一致アイテム検出データをインポートします。検出ステータスは、「オープン」または「クローズ済み」の VIT のステータスを更新します。

検出のステータスが VIT のステータスにどのように影響するかの詳細については、「検出、修復タスク、および脆弱性一致アイテム状況」を参照してください。

「脆弱性対応 の変更管理」より、脆弱性対応製品の修復タスクのステータスフィールドと変更要求 (CHG) のステータスフィールドの間には同期関係があります。変更要求のライフサイクルが進むと、関連する修復タスクのステータスも自動的に変化します。変更要求が実装されると、修復タスクは自動的に解決されます。詳細については、「変更要求と修復タスク間のステータスの同期」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:
脆弱性対応 v23.0 以降：

- [修正タスクのステータス承認] ワークフローは廃止され、フローデザイナーの [修正タスクのステータス承認] フローに置き換わりました。
- 修復タスクの [閉じる] ボタンが削除され、修復タスクのクローズがスキャナーによって行われるようになりました。

次の表に、修復タスクの状況と、それぞれの状況で修復タスクに対して実行できるアクションを示します。

修復タスクステータス

状態	説明
オープン	作成時のステータス。このステータスから、次のことができます。 重複 VI を表示 システム内の複数のスキャナーによって報告された重複 VIT を特定します。重複する VIT を [解決済み] または [クローズ済み] としてマークできます。重複するエントリーは、脆弱性の組み合わせが共通脆弱性識別子 (CVE) を使用して作成された場合にのみ表示されます。詳細については、「脆弱性対応 修復タスクと脆弱性一致アイテム状況」を参照してください。 調査を開始 この修復タスクをユーザーまたはグループにアサインし、調査を開始する必要があります。 誤検出としてマーク スキャナーがシステムに脆弱性が存在することを報告したけれども、実際には脆弱性が存在しない場合、アイテムまたはグループを誤検出としてマークします。 例外の要求 例外、再オープン (期限) 日、理由を要求し、必要に応じて追加情報を入力します。例外が要求された日付までアイテムまたはグループの修正を保留します。 解決 アイテムまたはグループを「解決済み」としてマークし、解決済みステータスに移行します。 変更要求を作成 変更要求を作成するか、修復タスクを既存の変更要求に関連付けます。詳細については、「修復タスクからの変更要求の作成」と「既存の変更要求への修復タスクの関連付け」を参照してください。 修復タスクを分割 複数の脆弱性一致アイテムを含む修復タスクの場合は、一連の条件を使用して脆弱性一致アイテムのサブセットを除外し、修復タスクを分割します。選択したアイテムは自動的に新しい修復タスクに移動されます。詳細については、「IT 修復ワークスペースでの修復タスクの分割」を参照してください。 保留

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクステータス (続く)

状態	説明
	[保留] ステータス、再オープン日、理由を選択し、必要に応じて追加情報を入力します。再オープン日まで修復タスクのステータスを保留します。 削除 削除を確定します。グループを削除します。
調査中	[調査を開始] ボタンによってトリガーされます。このステータスから、次のことができます。 セキュリティインシデントの作成 詳細については、「Create a security incident (セキュリティインシデントを作成する)」を参照してください。 変更要求を作成 変更要求を作成するか、修復タスクを既存の変更要求に関連付けます。詳細については、「修復タスクからの変更要求の作成」と「既存の変更要求への修復タスクの関連付け」を参照してください。 タスクを分割 複数の脆弱性一致アイテムを含む修復タスクの場合は、一連の条件を使用して脆弱性一致アイテムのサブセットを除外し、修復タスクを分割します。選択したアイテムは自動的に新しい修復タスクに移動されます。詳細については、「修復タスクの分割」を参照してください。 変更要求の作成 詳細については、「修復タスクからの変更要求の作成」を参照してください。 実装待ち ステータスを [実装待ち] に変更します。このステータスは、修復タスクが 脆弱性対応 の外部で参照されたことを示します。 保留 [保留] ステータス、再オープン日、理由を選択し、必要に応じて追加情報を入力します。再オープン日まで修復タスクのステータスを保留します。 削除 削除を確定します。修復タスクを削除します。
保留	[例外の要求] ボタンによってトリガーされます。承認ワークフローの一環として、保留ステータスは [レビュー中] であり、承認されるまでクローズできません。 このステータスから、次のことができます。 変更要求を作成 変更要求を作成するか、修復タスクを既存の変更要求に関連付けます。詳細については、「修復タスクからの変更要求の作成」と「既存の変更要求への修復タスクの関連付け」を参照してください。 タスクを分割

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクステータス (続く)

状態	説明
	複数の脆弱性一致アイテムを含む修復タスクの場合は、一連の条件を使用して脆弱性一致アイテムのサブセットを除外し、修復タスクを分割します。選択したアイテムは自動的に新しい VG に移動されます。「修復タスクの分割」を参照してください。 セキュリティインシデントの作成 詳細については、「Create a security incident (セキュリティインシデントを作成する)」を参照してください。 再オープン [オープン] ステータスに戻します。 削除 削除を確定します。修復タスクを削除します。 [クローズ/保留] タブの下に保留情報が表示されます。保留日に、グループは修復のために再オープンされます。
実装待ち	[実装待ち] ボタンによってトリガーされます。このステータスから、次のことができます。 セキュリティインシデントの作成 詳細については、「Create a security incident (セキュリティインシデントを作成する)」を参照してください。 変更要求を作成 変更要求を作成するか、修復タスクを既存の変更要求に関連付けます。詳細については、「修復タスクからの変更要求の作成」と「既存の変更要求への修復タスクの関連付け」を参照してください。 タスクを分割 複数の脆弱性一致アイテムを含む修復タスクの場合は、一連の条件を使用して脆弱性一致アイテムのサブセットを除外し、修復タスクを分割します。選択したアイテムは自動的に新しい修復タスクに移動されます。詳細については、「修復タスクの分割」を参照してください。 変更要求の作成 詳細については、「修復タスクからの変更要求の作成」を参照してください。 保留 [保留] ステータス、再オープン日、理由を選択し、必要に応じて追加情報を入力します。再オープン日まで修復タスクのステータスを保留します。 解決 メモを追加します。ステータスが [解決済み] になります。[解決] タブの下にメモが表示されます。 削除 削除を確定します。修復タスクを削除します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクステータス (続く)

状態	説明
解決済み	[解決 **(Resolve)]** ボタンからトリガーされます。このステータスから、次のことができます。 セキュリティインシデントの作成 詳細については、「Create a security incident (セキュリティインシデントを作成する)」を参照してください。 変更要求を作成 変更要求を作成するか、修復タスクを既存の変更要求に関連付けます。詳細については、「修復タスクからの変更要求の作成」と「既存の変更要求への修復タスクの関連付け」を参照してください。 再オープン [オープン] ステータスに戻します。 削除 削除を確定します。修復タスクを削除します。 [メモ] タブの下にメモが表示されます。[解決] タブの下に解決情報が表示されます。
終結済み	スキャナーによってトリガーされました。このステータスから、次のことができます。 セキュリティインシデントの作成 詳細については、「Create a security incident (セキュリティインシデントを作成する)」を参照してください。 再オープン [オープン] ステータスに戻します。 削除 削除を確定します。修復タスクを削除します。 [クローズ/保留] タブの下にクローズ情報が表示されます。

- 修復オーナーは、脆弱性一致アイテムまたは修復タスクを「解決済み」としてマークすることしかできません。スキャナーからの確認に基づいて、この解決済みのアイテムまたは修復タスクを「クローズ済み」または「再オープン」としてマークできます。
- [削除] ボタンは、手動で作成された脆弱性一致アイテムが複数あり、アドミニストレーターがそれらをクローズまたは削除する必要がある場合に使用できます。
- アイテムが低リスクであると判断し、変更時間帯までまたはパッチ適用まで待つ場合は、定義された期間、修復タスクを [保留] ステータスに変更することができます。[例外の要求] オプションを使用して例外を要求できます。

  注:
  修復タスクが保留またはクローズされた場合は、解決策を指定して、その理由をさらに定義できます。

- 手動または自動で VIT を再オープンすると、次のようになります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- VIT のステータスが [オープン] に変わります。元の修復タスクのステータスは更新されません。
- VIT が再評価され、アクティブな修復タスクルールに基づいて新規または既存の修復タスクに配置されます。

これにより、履歴を保持しながらさらに修正することができます。

- 修復タスクが (自動または手動で) 作成または分割されると、その [ステータス]、[理由]、および [期限] フィールドが評価されます。分割アクションの場合、これらのフィールドは古い修復タスクと新しい修復タスクの両方に対して評価されます。VIT が更新されると、関連するすべての修復タスクの [ステータス]、[理由]、[期限] フィールドが評価されます。
  - 修復タスク内のすべての VIT が保留され、同じ理由である場合、修復タスクのステータスは [保留] に変更され、VIT の理由が修復タスクにアサインされます。VIT の理由が異なる場合、修復タスクの理由は [なし] に変更されます。
  - すべての VIT の最も近い [期限] 日が、修復タスクの [期限] フィールドで更新されます。
  - VIT を再オープンすると、修復タスクのステータスが [オープン] に変わります。

  この評価は、15 分ごとに実行されるスケジュール済みジョブ [*Rollup vulnerability item values to vulnerability and group*] によって行われます。

検出、修復タスク、および脆弱性一致アイテム状況

サードパーティ統合によって脆弱性一致アイテム検出データが取得されます。検出は、スキャナーによって報告される脆弱性の個別の発生です。

検出データは脆弱性一致アイテム (VI、VIT) とペアリングされ、検出のステータスに基づいて VI ステータスが更新されます。VI が見つからない場合は、新しい VI が作成されます。検出は、スキャナーによって直接検出されたデータによってのみオープンまたはクローズされます。

脆弱性一致アイテムのすべての検出がクローズされた場合、その脆弱性一致アイテムはクローズされます。VI レコードでは、ステータスが [クローズ済み]/[修正済み] になります。修復タスクに対してすべての VI がクローズされると、その修復タスクはクローズされます。それ以外の場合、状況フローは変わりません。

サブステートが [修正済み] または [古い] であるクローズ済みの VI は、新しい検出が作成され、VI が新しい脆弱性と一致する場合に再オープンされます。

脆弱性対応 v20.0 以降、検出のステータスが [古い]、関連する VI のステータスが [クローズ済み] の場合、VI のステータスは [クローズ済み - 古い (Closed - Stale)] に移行しません。これは、新しい検出が特定されたときに VI が再オープンしないようにすることで、誤検出の要求と承認プロセス全体を回避できるようにするためです。この動作を元に戻すには、[自動クローズ構成] フォームの [クローズされている **VI** の古い検出を無視する] チェックボックスをオフにします。詳細については、「脆弱性対応 での古い検出の自動クローズ」を参照してください。

スクリプトインクルード、*DetectionBase*、メソッド *_shouldReOpenVI()* により、VI が以前に [クローズ済み] でサブステートが [修正済み]、[古い]、または [CI 廃止] であった場合は再オープンされ、検出が既存の VIT にマッピングされます。

たとえば、VI のクローズ日が検出の前回検出日より後であるとします。このような VI レコードはクローズされたままであると想定されます。しかし、以前にクローズされた VI が再オープンされたということは、その VI が以前の検出によってクローズされ、脆弱性が後のスキャンで再度見つかったことを意味します。新しい検出が見つかり、それが VI の構成アイテムと同じ脆弱性があるクローズ済み VIT と一致すると、VI が再オープンされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクと脆弱性一致アイテム状況

修復タスクと脆弱性一致アイテムの状況は、相互に影響することがあります。ほとんどの場合、修復タスクのステータスで脆弱性一致アイテムのステータスが更新されます。その際は、最優先タスクのステータスを使用してグループ内の脆弱性一致アイテムが更新されます。

ステータスの優先順位は次のとおりです。

[保留] > [解決済み] > [実装待ち] > [調査中 > [オープン]

- 脆弱性一致アイテムのグループが 1 つの修復タスク内にあり、個々のレベルで変更されていない場合は、修復タスクと同じステータスになります。
- 修復タスクが [オープン] ステータスから [実装待ち] ステータスになると、修復タスク内のすべての VI が [実装待ち] ステータスに移行します。
- 修復タスクが保留されると、VI も同様に保留されます。バージョン 16.5 以降では、脆弱性一致アイテム、アプリケーションの脆弱性一致アイテム、コンテナの脆弱性一致アイテム、または修復タスクが保留された回数を追跡できます。スケジュール済みジョブである *set deferral counts* は毎日実行され、VR、AVR、CVR の複数の保留モジュールの [保留数] 列で複数回保留されたレコード数が提示されます。修復タスクが複数回保留された場合、修復タスクに関連付けられている VI のすべてのカウントが収集され、提示されます。

修復タスクによってのみ更新される脆弱性一致アイテム

個別に更新されていない場合、アイテムは修復タスクのステータスと一致しますが、以下の例外があります。

- 修復タスクのステータスが [クローズ済み] に変わり、その解決策が [キャンセル] または [例外ありで修正済み] に変わっても、アイテムは影響を受けず、それを含む他の修復タスクのステータスになります。脆弱性一致アイテムが他の修復タスクにない場合は、[オープン] ステータスに戻ります。
- 脆弱性一致アイテムのステータスが [クローズ済み]/[修正済み] (スキャンまたはインポートによって更新) の場合、修復タスクのステータスが変わっても、脆弱性一致アイテムのステータスは [クローズ済み]/[修正済み] のままになります。この条件は、修復タスクのステータスに関係なく true です。

状況が個別に設定される脆弱性一致アイテム

個別にクローズまたは保留されたアイテムなど、アイテムでステータスが更新された脆弱性一致アイテムは、修復タスクのステータスと自動的に一致することはありません。その代わりに、ステータスを関連するすべてのグループと比較して、適用する優先順位が最も高いステータスを見つけます。

> **注:**
> [クローズ済み]/[修正済み] ステータスは特殊なケースです。[クローズ済み]/[修正済み] ステータスに設定されている脆弱性一致アイテムでは、修復タスク内のすべての脆弱性一致アイテムが [クローズ済み]/[修正済み] に設定されている場合 (すべての脆弱性が修復されたことをスキャナーが検出した場合など)、修復タスクは自動的に [クローズ済み]/[修正済み] としてマークされます。

空のアサインフィールドが含まれている修復タスク

修復タスクの VI のステータスが [解決済み] から [オープン] に変わると、修復タスクのステータスも [解決済み] から [調査中] に更新されます。

ただし、修復タスクの [アサイン先] フィールドと [アサイン先グループ] フィールドの両方が空の場合、修復タスクは [解決済み] ステータスのままになり、[調査中] に移行しません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性一致アイテムのアサイン先グループは、修復タスクが更新されても更新されない場合がある

オープンステータスの VI のアサイン先グループが手動で更新された場合、修復タスクのアサイン先グループが更新されても再度更新されません。この情報が上書きされないのは、VI のアサイン先グループが意図的に更新されており、別の修復タスクの一部である可能性があるためです。

複数グループでの脆弱性一致アイテム (VI) の修復タスクステータス

ある VI が複数の修復タスクにあり (以下の表のグループ)、そのステータスが設定されていない場合は、次の表に示すように、優先度の高いグループのステータスによって VI のステータスが決定されます。

脆弱性一致アイテム状況の例

修復タスクステータス	脆弱性一致アイテムのステータス
グループA: オープン > 調査中 グループ B：[オープン]	調査中 グループ A が [調査中] で、グループ B が [オープン] の場合、VI は [調査中] に変わります。検索の結果、グループ A とグループ B のうち、グループ A のステータスの優先度が最も高くなります。
グループ A：[調査中] グループB: オープン > 調査中	[調査中] グループ B が [調査中] で、グループ A が [調査中] の場合、VI は [調査中] のままです。検索の結果、グループ A とグループ B のステータスは同じ優先度になります。
グループ A：[調査中] グループB: 調査中 > 実装待ち	実装待ち グループ B が [実装待ち] でグループ A が [調査中] の場合、VI は [実装待ち] に変わります。検索の結果、グループ A とグループ B のうち、グループ B のステータスの優先度が最も高くなります。
グループA: 調査中 > 保留 グループB: 実装待ち	保留 グループ A が [保留] でグループ B が [実装待ち] の場合、VI は [保留] に変わります。検索の結果、グループ A とグループ B のうち、グループ A のステータスの優先度が最も高くなります。

複数グループでの脆弱性一致アイテムの特殊ケース

修復タスクステータス	脆弱性一致アイテムのステータス
グループA: 調査中 グループB: 実装待ち > クローズ済み (修正済みまたはキャンセル済み)	調査中 グループ B が [クローズ済み]/[修正済み] または [クローズ済み]/[キャンセル]、グループ A が [調査中] の場合、VI は [実装待ち] (以前の最優先) から [調査中] (現在の最優先) に変わります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

複数グループでの脆弱性一致アイテムの特殊ケース (続く)

修復タスクステータス	脆弱性一致アイテムのステータス
グループ A：いずれかのステータス グループ B：いずれかのステータス	脆弱性一致アイテムのソースステータスが [修正済み] (スキャンまたはインポートによって更新) の場合、グループのステータスが変更されると、脆弱性一致アイテムのステータスが [クローズ済み]/[修正済み] に変更されます。この条件は、関連する他のグループの状況に関係なく true です。グループステータスに対する脆弱性一致アイテムの検索は行われません。

VI のステータスが個別に設定されている場合、他の修復タスクと同様に、優先度を評価するときにそのステータスが考慮されます。VI が複数の修復タスクに属している場合、行われる更新を次の表に示します。

脆弱性一致アイテムのステータスが個別に設定される特殊ケース

グループ内の脆弱性一致アイテムのステータス	脆弱性一致アイテムの最終ステータス
グループ A のステータス: 調査中 グループ B ステータス: 調査中 > 実装待ち 元の VI ステータス: 調査中 > **(VI** で設定)	実装待ち グループ B が [実装待ち] に移行し、グループ A が [調査中] のままである場合、VI は [実装待ち] (最優先) に変わります。
グループA: 調査中 グループB: 調査中 > 実装待ち 元の VI ステータス: 保留 > **(VI** で設定)	保留 グループ B が [実装待ち] に移行し、グループ A が [調査中] のままである場合、VI は [保留] ステータス (最優先) のままになります。

次の表は、共通の脆弱性一致アイテムを対象にした 2 つの修復タスクが保留された場合、最新の日付に達するまでステータスが保留されることを示しています。

脆弱性一致アイテムの保留ステータスの特殊ケース

グループ内の脆弱性一致アイテムのステータス	脆弱性一致アイテムの最終ステータス
グループ A のステータス: レビュー中 **(4** 月 **10** 日まで) グループ B ステータス: 調査中 > レビュー中**(4**月**30** 日まで) 元の VI ステータス: レビュー中 **(4** 月 **10** 日まで) > **(VI** で設定)	保留 **(4** 月 **30** 日まで) グループ B が [保留] (4 月 30 日まで) に移行し、グループ A が [保留] (4 月 10 日まで) のままの場合、VI は [保留] (4 月 5 日まで) から [保留] (4 月 30 日まで) ステータスに変わります。
グループA: レビュー中 **(7** 月 **15** 日まで) グループB: 調査中 > レビュー中**(7**月**10**日まで 元の VI ステータス: 保留 > **(7**月**15**日まで)	保留 **(7** 月 **15** 日まで) グループ B が [保留] (7 月 10 日まで) に移行し、グループ A が [保留] (7 月 15 日) のままになっている場合、VI は [保留] (7 月 15 日まで) のままになります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドメインセパレーションの追加の設定

正確な実行と結果を得るには、脆弱性対応、アプリケーション脆弱性対応、コンテナ脆弱性対応、およびコンフィグレーションコンプライアンスのドメインセパレーションに次の予防措置と設定が必要です。

問題を回避するためにグローバルドメインのビジネスロジックとプロセスを変更せず、アップグレードごとに最新の変更がすべて更新されるようにしてください。各ドメインのすべてのビジネスロジックとプロセスを個別に複製し、グローバルドメインで非アクティブになっていることを確認します。そのようになっていない場合、グローバルドメインのビジネスロジックとプロセスが子ドメインよりも優先されます。子ドメインにリスクルールを作成し、グローバルドメインにも同様のリスクルールがある場合には、グローバルドメインのルールが子ドメインのルールよりも優先されます。

算出とルールの再評価

v20.0 より前では、算出またはルールを再適用すると、再実行フラグが true に設定され、算出とルールを再適用するスケジュール済みジョブを実行するビジネスルールがトリガーされます。v20.0 以降では、再実行フラグに依存する必要はなくなりました。[算出を再適用] ボタンをクリックすると、算出とルールを再適用するバックグラウンドジョブがトリガーされます。これにより、すべてのドメインの算出とルールを作成できます。

ロールアップ算出の設定

ドメインでは、テーブルに対してアクティブにする必要があるロールアップ算出は 1 つだけです。たとえば、グローバルドメインの修復タスクテーブルとして、ロールアップ算出を使用する*sn_vul_vulnerability*、修復タスクロールアップについて考慮してみましょう。同じドメイン内の同じテーブルの重み付けを変更してこのロールアップ算出を複製すると、ロールアップ計算に不一致が生じます。したがって、同じドメイン内のテーブルに 2 つ以上のロールアップ算出がある場合は、必ず 1 つのロールアップ算出のみをアクティブ化にします。

[検出されたアイテム] フォームフィールド

資産は、[CI ルックアップルール] を使用してインポートされると、構成管理データベース (CMDB) で自動的に構成アイテム (CI) と照合されます。一致しない CI のレコードは、サードパーティ脆弱性統合のインポート中に自動的に作成され、検出されたアイテムに含まれます。ただし、CMDB CI に存在しないクラウド資産の場合、レコードはクラウドリソースクラスに作成されます。

[検出されたアイテム] フィールド

こうしたレコードの情報は、インポート中にサードパーティのレコードから取り込まれ、分類されます。

これらのフィールドは、検出されたアイテム [sn_sec_cmn_src_ci] テーブルにリストされているレコードにあります。

次の表にリストされているフィールドのインポートされたデータを表示するには、少なくとも sn_vul.read_all ロールが必要です。

フィールド	説明
数値	レコードにアサインされた識別子。
構成アイテム	サードパーティのソース統合からインポートされる構成アイテム。 v12.0 以降、構成アイテムは廃止された CI をフィルタリングした後の CI リストの最新 CI です。
クラス	インポート中に 脆弱性対応 によって CI に割り当てられたクラス。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ソース	サードパーティのソース統合からインポートされるソース。
CI 一致ルール	アイテムの作成に使用された CI 一致ルール。
V18.0：DI の一致タイプ	検出されたアイテムの作成に使用された一致タイプ。オプションは次のとおりです。 • VR により作成済み • IRE により作成済み • CI ルックアップにより一致 • IRE により一致 • 手動で照合 (脆弱性対応の v24.0.6 以降では、この追加オプションを表示できます。このオプションは、[検出されたアイテム] フォームで CI を手動で更新すると自動的に設定されます。 この情報は、脆弱性対応 v18.0 以降に入力されたデータに対してのみ使用できます。既存のデータでは、この列には値が含まれません。 注: CI ルックアップルールを再適用すると、DI の一部の CI が更新され、この列に値が入力される可能性があります。
その他の一致する CI	CI ルックアップルールに一致する他の構成アイテムのリスト。
状態	インポート中に決定される CI のステータス。選択肢は次のとおりです。 • 一致：CMDB で一致する構成アイテムが見つかりました。 • 不一致：CMDB で一致するものが見つかりませんでした。プレースホルダーレコードが作成されます。
作成済み	検出されたアイテムレコードが作成された日付。
更新日時	検出されたアイテムレコードが更新された日付。
更新者	データを更新したユーザー。
ホストタグ	インポート中にこの検出されたアイテムにアサインされたホストタグ。検出されたアイテムごとに最大 31 個のホストタグを設定できます。
完全修飾ドメイン名	CMDB で見つかったこの CI に関連付けられたデータ。
MAC アドレス	CMDB で見つかったこの CI に関連付けられたデータ。
オペレーティングシステム	この CI に関連付けられているオペレーティングシステム。
NetBIOS	サードパーティのソース統合からインポートされる NetBIOS。
IP アドレス	CMDB で見つかったこの CI に関連付けられたデータ。
ソースデータ	ソースからこの CI に関連付けられた最後のデータ。
V16：初期ソースデータ	ソースからこの CI に関連付けられた初期データ。
V16：再評価 CI	スキャナーからデータを受信します。更新されたデータがある場合、値は true に設定されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: ソースデータ値は、最新のソースデータに従って再計算されます。更新されたデータがスキャナーから取得されると、ソースデータが更新されます。既存のソースデータ値が最初のソースデータフィールドに移動されます。検出されたアイテムを再評価するには、[変更されたディスカバリーアイテムに CI ルックアップルールを再適用する (Re-apply CI Lookup Rules on the Changed Discovered items)] スケジュール済みジョブをアクティブ化します。
エージェントが存在します	エージェントが資産にインストールされている場合は true を示します。[ソースデータ] 列の hostUID と UUID の値が空の場合、この値は true と設定されます。 注: このフィールドは、脆弱性対応の v19.0 以降に表示されます。

脆弱性対応の v23.0 以降では、[テスト結果コンプライアンス **% (CI) (Test Result Compliance % (CI))]** 列には、対応する CI に準拠しているテスト結果の割合が表示されます。この値を取得するには、[修復メトリクスの更新 **(Update remediation metrics)]** スケジュール済みジョブで calcTRComplianceForCI を true に設定する必要があります。

注:
[テスト結果コンプライアンス **% (CI) (Test Result Compliance % (CI))]** の値は、[前回のコンフィグレーションコンプライアンススキャン日] 列または [インフラ以外の前回のコンプライアンススキャン日] 列のいずれかの値が空でない検出されたアイテムに対してのみ入力されます。

脆弱性対応 のバージョン 18.0 以降、Qualys、脆弱性対応の Tenable および Rapid7 のスキャナーは、クラウド資産について次の追加メタデータを受理できます。

フィールド	説明
クラウドサービスプロバイダー	クラウドコンピューティングサービスを提供するクラウドサービスプロバイダーの名前。たとえば、Amazon Web サービス (AWS)、Microsoft Azure、Google Cloud Platform (GCP) などです。
クラウドリージョン	リソースがホストされている場所。
クラウドアカウント	クラウドコンピューティングサービスにアクセスするために AWS、GCP などのクラウドサービスプロバイダーによって提供されるアカウント。
クラウドリソースタイプ	Amazon Elastic Compute Cloud (EC2) マシン、AWS S3 バケットなど、クラウドに存在する資産のタイプ。
リソース ID	クラウドコンピューティング環境でリソースにアサインされる一意の識別子。この ID は、リソースの識別と管理に使用されます。
リソース名	クラウドコンピューティング環境でリソースを識別および管理するために使用されるユーザー定義の名前。
画像	仮想マシンイメージまたはサーバーイメージは、オペレーティングシステム、アプリケーション、およびその他のソフトウェアを含む事前設定された仮想マシンです。たとえば、Amazon マシンイメージなどです。

クラウドメタデータに基づいてクラウド CI を照合するために、新しい CI ルックアップルールである「クラウドリソース ID」が導入されました。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性対応脆弱性フォームフィールド

脆弱性は、脆弱性情報データベース (NVD)、共通脆弱性タイプ一覧 (CWE)、またはサードパーティ統合からレコードがダウンロードされると自動的に作成され、脆弱性対応 の [ライブラリ] に保存されます。

NVD エントリーのフィールド

次の表にリストされているフィールドのインポートされたデータを表示するには、少なくとも sn_vul.read_all ロールが必要です。

これらのフィールドは、脆弱性情報データベース エントリ [sn_vul_nvd_entry] テーブルにリストされているレコードにあります。

フィールド	説明
ID	この脆弱性エントリーの識別子。
リスク評価	(脆弱性に関連付けられている VIT がない場合は非表示) 脆弱性一致アイテムを [重大]、[高]、[中]、[低]、および [なし] に分類する数値化された [リスクスコア] 。リスク評価の詳細については、「脆弱性対応の算出と脆弱性算出ルール」を参照してください。 注: この基本リスク評価は、ソリューションレコードのリスク評価と同じではありません。
リスクスコア	(脆弱性に関連付けられている VIT がない場合は非表示) 脆弱性一致アイテムが環境にもたらすリスク量を算出したもの。 注: この基本リスクスコアは、ソリューションレコードのリスクスコアと同じではありません。 詳細については、「脆弱性対応 の算出と脆弱性算出ルール」を参照してください。
重大度	この脆弱性の重大度を正規化したもの。重大度マップは、NVD および ServiceNow サードパーティ統合に提供されます。重大度マップの作成や調整の詳細については、「脆弱性対応 重大度マップの作成」を参照してください。
エクスプロイト有無	少なくとも 1 つのエクスプロイトがこの脆弱性に関連付けられている場合は、有り。
エクスプロイトスキルレベル	この脆弱性を利用するために必要な最低スキルレベル。
エクスプロイト攻撃ベクトル	この脆弱性のエクスプロイトの最も脆弱な攻撃ベクトル。 SAM NVD が有効になっている場合に使用できます。
アクティブな VI	(脆弱性に関連付けられている VIT がない場合は非表示)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	[クローズ済み] ステータスではない、この脆弱性に関連付けられた脆弱性一致アイテムの数。この脆弱性にアクティブな VI がない場合、[リスク評価] と [リスクスコア] は表示されません。
CWE エントリー	この脆弱性が最も適合する共通脆弱性タイプ一覧要素への参照。
公開日	この脆弱性が公開された日付。
最終変更日	この脆弱性が前回変更された日付。
まとめ	脆弱性の説明。
脅威インテリジェンス (脆弱性対応 バージョン 20.0 以降)	Qualys によって提供される脅威インテリジェンス。このデータを使用して、脅威アクターの動機、ターゲット、および攻撃動作を理解できます。
脆弱性の詳細	
CVSS v2	インポートされた CVSS v2 データ
CVSS v3	インポートされた CVSS v3 データ。2015 年より前は利用できません。
優先ソリューション	(脆弱性に関連付けられている VIT がない場合は非表示) この脆弱性で参照されたソリューションから導出された、チェーン内で最も優先度が高いソリューション。連結内に複数の最高優先度が存在する場合、値は設定されません。手動で設定した値は、後続のインポートで上書きできます。この値の手動設定は、脆弱性一致アイテムで行う必要があります。
CISA エクスプロイト (このタブは、CISA アプリケーションがインストールされている場合にのみ使用できます。)	
CISA の期日	脆弱性を解決する期限。
追加された日付	脆弱性が CISA カタログに追加された日付。
製品	脆弱性が特定された製品。
ベンダー/プロジェクト	特定された脆弱性に関連付けられたベンダー。
既知のランサムウェア 脆弱性対応 の v21.0 以降。	[ランサムウェアキャンペーンで使用されることがわかっている **(Known To Be Used in Ransomware Campaigns)]** フィールドが、CISA の既知の悪用された脆弱性 (KEV) カタログから取り込まれたときに選択されます。このフラグは、共通脆弱性識別子 (CVE) レベルで設定され、サードパーティエントリ (TPE) にロールアップされます。
修復ステータス (脆弱性に関連付けられている VI がない場合は非表示)	
保留を除外する	
脆弱性一致アイテム	この脆弱性があるアクティブな脆弱性一致アイテムの数。この数には、保留された脆弱性一致アイテムは含まれません。
合計 VI	この脆弱性がある脆弱性一致アイテムの合計数。この数には、保留された脆弱性一致アイテムは含まれません。
修復された VI の割合	この脆弱性がある脆弱性一致アイテムの修復の完了率。この数には、保留された脆弱性一致アイテムは含まれません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
保留を含める	
脆弱性一致アイテム	この脆弱性があるアクティブな脆弱性一致アイテムの数。
合計 VI	この脆弱性がある脆弱性一致アイテムの合計数。
修復された VI の割合	この脆弱性がある脆弱性一致アイテムの修復の完了率。
関連リンク	
ステータスを更新	前回の更新日時を表示します。 以下を更新します。 • 修復タスクステータス • リスクスコアと評価 • [修復ステータス] セクションのアクティブな VIT、合計 VIT などのメトリクス
関連リスト	
脆弱性一致アイテム	(脆弱性に関連付けられている VIT がない場合は非表示) この脆弱性に関連付けられた脆弱性一致アイテム。
脆弱性参照	NVD によって引用された、外部ソースからの脆弱性に関する情報。
エクスプロイト	この脆弱性に関連付けられているエクスプロイト。
ソリューション	(脆弱性に関連付けられている VIT がない場合は非表示) この脆弱性に関連付けられているすべての 脆弱性ソリューション管理 統合ソリューション。
弱点	共通脆弱性識別子 (CVE) に関連付けられたインポートされた脆弱性データ。
脆弱なソフトウェア	(ソフトウェアが CVE に関連付けられている場合は非表示) 脆弱性に関連するインポートされた共通プラットフォーム一覧 (CPE) データ。
脆弱性マルウェアキット	脆弱性について、さまざまなスキャナーソースからインポートされたマルウェア。

CWE 脆弱性エントリーフィールド

これらのフィールドは、CWE [sn_vul_cwe] テーブルにリストされているレコードにあります。

フィールド	説明
CWE ID	この脆弱性エントリーの識別子。この識別子はカテゴリと脆弱性の両方に使用され、2 つのデータセット間で一意です。
名前	この CWE-ID にアサインされた記述名。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
エクスプロイトの可能性	定性的スケールで脆弱性が利用される可能性。次のいずれかになります。 • 不明 • Low (低) • 中程度 • 高
OWASP 上位 10 位	OWASP 上位 10 リストにおけるこの脆弱性の数値的な位置。
SANS 上位 25 位	SAN 上位 25 リストにおけるこの脆弱性の数値的な位置。
クラス	脆弱性のタイプ
ステータス	次のいずれかになります。 • 未完了 • ドラフト • 安定 • 不使用 • 廃止 • 不安定
抽象化	次のいずれかになります。 • バリアント • クラス • ベース • 複合
更新日時	最後にインスタンスでレコードが更新された日時。
機能エリア	影響を受ける機能エリアのリスト。たとえば、[ファイル処理 **(File Processing)]**。24/862 の脆弱性についてのみ設定されます。
影響を受けるリソース	影響を受けるリソースのリスト。たとえば、[ファイル] または [ディレクトリ]。51/863 の脆弱性についてのみ設定されます。
URL	この脆弱性に関連付けられたナレッジベース記事。
説明	脆弱性の説明。
統合実行	この CWE がインポートされた統合実行。
セクション	
その他の詳細	脆弱性をさらに説明するソフトウェアの概念の説明。含まれる内容： • 詳細な説明 • バックグラウンドの詳細 • メモ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ディスカバリー方法	アプリケーションにおけるこの脆弱性を検出する方法の詳細。
導入モード	脆弱性が導入されるフェーズ ([実装 **(Implementation)]**、[アーキテクチャと設計 **(Architecture and Design)]** など)。
デモ例	脆弱性のコード例と説明。
緩和の可能性	アプリケーションライフサイクルのどのフェーズで発生するか、緩和の有効性など、脆弱性を防止する方法の詳細。
関連リスト	
関係	この脆弱性に関連付けられた CWE。この CWE とその他との関係を一覧表示します。parent/child、follows/precedes、requiredby/requires (複合的な脆弱性の場合)、CanAlsoBe、PeerOf、MemberOf を含めることができます。
観測された例	この脆弱性を表す CVE。
一般的な結果	悪用に成功した場合の結果、その範囲と影響。たとえば、 範囲：機密性 影響：アプリケーションデータの読み取り
メンバーシップ	この脆弱性を含む CWE メンバーシップ。
適用プラットフォーム	この脆弱性に関連付けられたプラットフォーム。
アプリケーション脆弱性エントリー	1 つに関連付けられた他のアプリケーション脆弱性エントリー。
外部参照	外部ソースからの脆弱性に関する情報。

自動翻訳

サードパーティ脆弱性エントリーフィールド

これらのフィールドは、サードパーティ脆弱性エントリ [sn_vul_third_party_entry] テーブルにリストされているレコードにあります。

フィールド	説明
ID	この脆弱性エントリーの識別子。
バージョン 16.0：CVE	このサードパーティの脆弱性に関連する複数の共通脆弱性識別子 (CVE)。
ソース	脆弱性の発生元 - スキャナーまたは物理テスト。
リスク評価	脆弱性一致アイテムを [重大]、[高]、[中]、[低]、および [なし] に分類する数値化されたリスクスコア。リスク評価の詳細については、「脆弱性対応 の算出と脆弱性算出ルール」を参照してください。 **注:** この基本リスク評価は、ソリューションレコードのリスク評価と同じではありません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
リスクスコア	脆弱性一致アイテムが現在の環境にもたらすリスク量をリスクスコアに基づいて算出したもの。 **注:** この基本リスクスコアは、ソリューションレコードのリスクスコアと同じではありません。 詳細については、「脆弱性対応 の算出と脆弱性算出ルール」を参照してください。
重大度	この脆弱性の重大度を正規化したもの。重大度マップは、NVD および ServiceNow サードパーティ統合に提供されます。重大度マップの作成や調整の詳細については、「脆弱性対応 重大度マップの作成」を参照してください。
エクスプロイト有無	少なくとも 1 つのエクスプロイトがこの脆弱性に関連付けられている場合は、有り。
エクスプロイトスキルレベル	この脆弱性を利用するために必要な最低スキルレベル。
エクスプロイト攻撃ベクトル	この脆弱性のエクスプロイトの最も脆弱な攻撃ベクトル。
アクティブな VI	[クローズ済み] ステータスではない、この脆弱性に関連付けられた脆弱性一致アイテムの数。
カテゴリ	サードパーティ統合によって提供される分類。アサインを支援します。
是正処置タイプ	修正アクションのタイプ。 • パッチ • 設定の変更 • 更新プログラムと設定の変更 • 対策
CWE エントリー	この脆弱性が最も適合する共通脆弱性タイプ一覧要素への参照。
PCI	このチェックボックスをオンにすると、脆弱性に、支払情報の公開に関する重大なリスクのフラグが付けられます。
PCI 重大度	支払情報の公開に関するリスクのレベル。[Qualys のみ。]
公開日	この脆弱性が公開された日付。
最終変更日	この脆弱性が前回変更された日付。
まとめ	脆弱性の説明。
脆弱性の詳細	
CVSS v2	インポートされた CVSS v2 データ
CVSS v3	インポートされた CVSS v3 データ。2015 年より前は利用できません。
脅威	この脆弱性に由来する脅威の説明。
優先ソリューション	この脆弱性で参照されたソリューションから導出された、チェーン内で最も優先度が高いソリューション。連結内に複数の最高優先度が存在する場合、

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	値は設定されません。手動で設定した値は、後続のインポートで上書きできます。この値の手動設定は、脆弱性一致アイテムで行う必要があります。
修復メモ	ベンダーから取得した修正ソリューションの説明。
修復ステータス	
保留を除外する	
脆弱性一致アイテム	この脆弱性があるアクティブな脆弱性一致アイテムの数。この数には、保留された脆弱性一致アイテムは含まれません。
合計 VI	この脆弱性がある脆弱性一致アイテムの合計数。この数には、保留された脆弱性一致アイテムは含まれません。
修復された VI の割合	この脆弱性がある脆弱性一致アイテムの修復の完了率。この数には、保留された脆弱性一致アイテムは含まれません。
保留を含める	
脆弱性一致アイテム	この脆弱性があるアクティブな脆弱性一致アイテムの数。
合計 VI	この脆弱性がある脆弱性一致アイテムの合計数。
修復された VI の割合	この脆弱性がある脆弱性一致アイテムの修復の完了率。
関連リンク	
ステータスを更新	前回の更新日時を表示します。 以下を更新します。 • 修復タスクステータス • リスクスコアと評価 • [修復ステータス] セクションのアクティブな VI、合計 VI などのメトリクス
関連リスト	
脆弱性一致アイテム	この脆弱性に関連付けられた脆弱性一致アイテム。
脆弱性参照	NVD によって引用された、外部ソースからの脆弱性に関する情報。
CVE	この脆弱性に関連付けられた共通脆弱性一覧 (CVE) レコード。
カテゴリ	この脆弱性に関連付けられたカテゴリ。
エクスプロイト	この脆弱性に関連付けられているエクスプロイト。
脆弱性マルウェアキット	この脆弱性に関連するマルウェアキット。
ソリューション (Rapid7)	Rapid7 ソリューション統合からのソリューション情報。利用可能な場合に表示されます。
エクスプロイトフレームワーク	この脆弱性に関連付けられているエクスプロイトフレームワーク。
ソリューション	この脆弱性に関連付けられている 脆弱性ソリューション管理 ソリューション。
CISA エクスプロイト	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
CISA が存在します	サードパーティ脆弱性エントリーテーブルに CISA エクスプロイトが存在します。
CISA の期日	脆弱性を解決する期限。

修復タスクフォームフィールド

修復タスクを使用すると、アナリストが進捗状況を監視し、修復プロセスをより効率的に進めることができます。

これらのフィールドは、修復タスク [sn_vul_vulnerability] テーブルにリストされているレコードにあります。

次の表にリストされているフィールドのインポートされたデータを表示するには、少なくとも sn_vul.read_all ロールが必要です。

修復タスクフィールド

フィールド	説明
数値	このレコードに対して自動的に生成された脆弱性一致アイテム (VI) 番号。
リスク評価	[重大]、[高]、[中]、[低]、および [なし] の範囲に分類された脆弱性一致アイテムリスクスコアのロールアップ。リスク評価の詳細については、「脆弱性対応 の算出と脆弱性算出ルール」を参照してください。 **注:** この基本リスク評価は、ソリューションレコードのリスク評価と同じではありません。
リスクスコア	この修復タスクに関連付けられているすべての脆弱性一致アイテムのリスクスコアのロールアップ。脆弱性一致アイテムの集合が現在の環境にもたらすリスクの量。 **注:** この基本リスクスコアは、ソリューションレコードのリスクスコアと同じではありません。
修復ターゲット	脆弱性一致アイテムを最初に特定してから、修正するまでの期日。 修復ターゲットの詳細については、「脆弱性対応 の修復ターゲットルール」を参照してください。
修復ステータス	タスクの修正のステータス。最も近い期日の脆弱性一致アイテムによって決定されます。 オープングループのステータスは次のとおりです。 • 実行中 • 該当 CI 確認中 • ターゲット経過 クローズ済みグループのステータスは次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

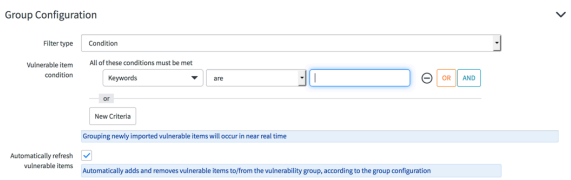
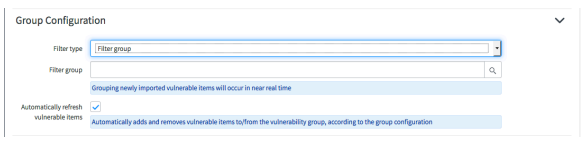
修復タスクフィールド (続く)

フィールド	説明
	• ターゲットなし • ターゲット達成 • ターゲット経過 算出された修復ターゲット日について、タスクがクローズされている場合は、クローズ済みのすべての脆弱性一致アイテムの全体的な修復ステータスがタスクに表示されます。それによって、タスクがターゲット日に間に合ったか否かが判断されます。クローズ済みのタスクの修復ステータスは、そのクローズ済みアイテムのどれにも修復ターゲット日がない場合、[ターゲットなし] になります。そのクローズ済みアイテムのいずれかがターゲット日を過ぎた場合、[ターゲット経過] になります。少なくとも 1 つのクローズ済み VI がターゲットを達成し、その他の VI が達成できなかった場合、[ターゲット達成] になります。
状態	タスクの進捗状況。 状況は次のとおりです。 • オープン • 調査中 • 実装待ち • 保留 • レビュー中 • 解決済み • クローズ済み 状況の詳細については、「脆弱性対応 修復タスクと脆弱性一致アイテム状況」を参照してください。
リスク削減の期限日	修復タスクに適用された補完コントロールの有効期限が切れる日付。 注: このフィールドは、値が入手できる場合にのみ表示されます。
アサイン先グループ	この修復タスクで作業するように選択されたグループ。
アサイン先	この脆弱性に対して作業する、選択されたアサイン先グループの個人。
作成済み	この修復タスクが作成された日付。
更新日時	この修復タスクの最終更新日付。
脆弱性	タスクに適用される脆弱性。(単一の脆弱性に基づいてグループが形成されている場合に表示されます。)
簡単な説明	この修復タスクの簡単な説明。
レビュー中 (RT が [レビュー中] ステータスの場合に表示)	
要求者	保留を要求した個人。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクフィールド (続く)

フィールド	説明
希望理由 (Desired reason)	保留の理由。
適切な状況	承認者から要求されたステータス。
適切なサブステート	承認者から要求された理由。
保留 (タスクが [保留] ステータスの場合に表示)	
保留要求元	タスクを保留した個人。
保留期限	保留の有効期限が切れる日付。
保留する理由 (Reason to defer)	保留の理由。
解決 (RT が [解決済み] ステータスの場合に表示)	
解決者	修復タスクを解決した個人。
解決日	修復タスクが解決された日付。
解決メモ	追加情報。
クローズ (RT が [クローズ済み] ステータスの場合に表示)	
クローズ担当者	修復タスクを解決した個人。
クローズ済み	修復タスクがクローズされた日付。
クローズメモ	追加情報。
グループ構成 (すべての状況で表示)	
フィルタータイプ	グループの脆弱性を選択するために使用するフィルタリングのタイプ： 条件  注: 1 時間に 1 回リフレッシュされます。 フィルターグループ  注: 1 時間に 1 回リフレッシュされます。 手動

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクフィールド (続く)

フィールド	説明
修復ステータス	
保留を除外する	
脆弱性一致アイテム	このタスク内のアクティブな脆弱性一致アイテムの数。この数には、保留された脆弱性一致アイテムは含まれません。
合計 VI	このタスク内の脆弱性一致アイテムの合計数。この数には、保留された脆弱性一致アイテムは含まれません。
修復された VI の割合	このタスク内の脆弱性一致アイテムの修復の完了率。この数には、保留された脆弱性一致アイテムは含まれません。
保留を含める	
脆弱性一致アイテム	このタスク内のアクティブな脆弱性一致アイテムの数。
合計 VI	このタスク内の脆弱性一致アイテムの合計数。
修復された VI の割合	このタスク内の脆弱性一致アイテムの修復の完了率。
メモ (すべての状況で表示)	
説明	グループまたは修正アクションの説明。
追加コメント	追加情報。
アクティビティ	システムメモ。
関連リンク	
脆弱性一致アイテムを再スキャン	脆弱性一致アイテムの再スキャンをトリガーして、修正されているかどうかを判断します。
ステータスを更新	前回の更新日時を表示します。 タスク内の VI から以下をロールアップします。 • 修復タスクステータス • リスクスコアとリスク評価 • 修復ターゲットの日付とステータス (該当する場合) • [修復ステータス] セクションのアクティブな VI、合計 VI などのメトリクス
関連リスト	
脆弱性一致アイテム	このタスクの脆弱性一致アイテム。
SLA タスク	このタスクに関連付けられたプラットフォーム SLA。
優先ソリューション	このタスクの脆弱性一致アイテムの優先ソリューション。
変更要求	このタスクに関連付けられた変更要求。
要求された承認	(タスクが [レビュー中] ステータスの場合に表示。) 承認者のリスト。保留が承認されると、修復タスクは [保留] ステータスに移行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[アンケート構成] フォームのフィールド

[VR 例外管理の設定 (Settings for VR Exception Management)] フォームの [VR アンケート構成] セクションで脆弱性タスクまたは修復タスクをそれぞれフィルタリングすることで、脆弱性または修復タスクの個別のコレクションに対して個別のアンケートを定義できます。

[アンケート構成] フォームは、[VR 例外管理の設定 (Settings for VR Exception Management)] フォームの [VR アンケート構成] セクションで [新規] ボタンを選択すると表示されます。

[アンケート構成] フォームのフィールド

フィールド	説明
名前	アンケートの名前。
承認ルール	アンケートが適用可能な承認ルール。 • 脆弱性グループの例外要求 • 脆弱性一致アイテムの例外要求 • 脆弱性グループの誤検出 • 脆弱性一致アイテムの誤検出 • 修復タスクのリスク削減要求に対して脆弱性グループのコントロールを補完するためのアンケート。 • 脆弱性一致アイテムのリスク削減要求に対して脆弱性一致アイテムのコントロールを補完するためのアンケート。
説明	アンケート構成の簡単な説明。
順番	順番が最も低いアンケートが要求中に表示されます。
有効	デフォルトで有効になっており、アンケートが使用中であることを示します。
テーブル	承認ルールが適用可能なテーブル。 • 脆弱性一致アイテムに関連する承認ルールの脆弱性一致アイテム [sn_vul_vulnerable_item]。 • 修復タスクに関連する承認ルールの修復タスク [sn_vul_vulnerability]。
条件	アンケートを表示する必要があるレコードの条件。 脆弱性一致アイテムと修復タスクの、[理由] を除くすべてのフィールドに条件を適用できます。
アンケート	修復オーナーが例外、誤検出、またはリスク削減を要求するときに表示されるアンケート。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連情報

脆弱性対応 の例外管理の設定

リスク削減のアンケートを構成する

脆弱性対応 脆弱性一致アイテムフォームフィールド

脆弱性一致アイテムは、サードパーティの脆弱性統合のインポート中に自動的に作成されます。

脆弱性一致アイテムフィールド

次の表にリストされているフィールドのインポートされたデータを表示するには、少なくとも sn_vul.read_all ロールが必要です。

これらのフィールドは、脆弱性一致アイテム [sn_vul_vulnerable_item] テーブルにリストされているレコードにあります。

SAM NVD 脆弱性スキャンを有効にしている場合、レコードは 構成管理データベース (CMDB) 内のソフトウェアと比較され、一致する脆弱なソフトウェアまたは構成アイテム (CI) が検出されます。

フィールド	説明
セキュリティタグを選択	レコードにメタデータを追加するか、このセキュリティインシデントレコードにアクセスする必要があるユーザーを識別するセキュリティタグ。このフィールドは、脆弱性一致アイテムが保存された後にのみ表示されます。
数値	このレコードに対して自動的に生成された脆弱性一致アイテム番号。
ソース	この脆弱性一致アイテムを検出したスキャナー。
リスク評価	脆弱性一致アイテムを [重大]、[高]、[中]、[低]、および [なし] に分類する数値化された [リスクスコア] 。リスク評価の詳細については、「脆弱性対応の算出と脆弱性算出ルール」を参照してください。 注: この基本リスク評価は、ソリューションレコードのリスク評価と同じではありません。
リスクスコア	脆弱性一致アイテムが環境にもたらすリスク量を算出したもの。 注: この基本リスクスコアは、ソリューションレコードのリスクスコアと同じではありません。 詳細については、「脆弱性対応 の算出と脆弱性算出ルール」を参照してください。
脆弱性	この脆弱性一致アイテムに関連付けられた脆弱性の ID。
構成アイテム	影響を受ける資産。
状態	このフィールドのデフォルトは [オープン] ですが、脆弱性をすぐに修正する準備ができている場合は [調査中] に変更できます。
リスク削減の期限日	脆弱性一致アイテムに適用された補完コントロールの有効期限が切れる日付。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: このフィールドは、[元のリスクスコア] の値が入手できる場合にのみ表示されます。
アサイン先グループ	この修復タスクで作業するように選択されたグループ。
アサイン先	この脆弱性に対して作業する、選択されたアサイン先グループの個人。
作成済み	この脆弱性一致アイテムがインスタンスに作成された日付。
最終オープン日時	この脆弱性一致アイテムが最後にインスタンスでオープンされた日付。初期状態では脆弱性一致アイテムの作成日と同じですが、クローズされた後に再オープンされると、最終オープン日には再オープン日時が含まれます。
更新日時	前回のスキャンの日付。
経過時間	VI が最後にオープンされてからアクティブになっている期間。VI がクローズされている場合、経過時間フィールドの値はゼロに設定されます。 [経過時間] フィールドの詳細については、「脆弱性一致アイテムの経過時間の計算と表示」を参照してください。経過時間の計算をカスタマイズする方法の詳細については、 KB1703270 記事を参照してください。
脆弱性	
まとめ	脆弱性の説明。
重大度	この脆弱性の重大度を正規化したもの。重大度マップは、NVD および ServiceNow サードパーティ統合に提供されます。重大度マップの作成や調整の詳細については、「脆弱性対応 重大度マップの作成」を参照してください。
脆弱性スコア (v3)	CVSS v3 スコア。
脆弱性スコア (v2)	CVSS v2 スコア。
エクスプロイト有無	この脆弱性一致アイテムに関連付けられた脆弱性に少なくとも 1 つのエクスプロイトが関連付けられている場合は、有り。
エクスプロイト攻撃ベクトル	この脆弱性一致アイテムに関連付けられた脆弱性のエクスプロイトの最も脆弱な攻撃ベクトル。
エクスプロイトスキルレベル	この脆弱性一致アイテムに関連付けられた脆弱性のエクスプロイトに必要な最低スキルレベル。
公開日	この脆弱性が公開された日付。
最終変更日	この脆弱性が前回変更された日付。
脅威	脅威に関する関連情報。脆弱性エントリーレコードから取得されます。 注: ここで変更を加えると、脆弱性エントリーレコードが更新されます。
修復メモ	脆弱性エントリーレコードから取得された、脅威に対する関連ソリューション。
修復 脆弱性ソリューション管理 でのみ使用できます。	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
優先ソリューション	脆弱性レコードからインポートされた優先ソリューション。 注: ここで手動で変更を行っても脆弱性レコードは変更されず、後続のインポート時に VI が未変更のままになります。
サマリー	ソリューションレコードからインポートされたサマリー。
ソリューションタイプ	見込みのある解決策または優先的な解決策。
初期検出	
DNS 名	ドメインネームサービスの名前。CI が指定されていない場合、このフィールドは一致する CI を検索するために使用されます (存在する場合)。
NetBIOS 名	NetBIOS の名前。CI が指定されていない場合、このフィールドは一致する CI を検索するために使用されます (存在する場合)。
IP アドレス	IPv4 または IPv6 アドレス。CI が指定されていない場合、このフィールドは一致する CI を検索するために使用されます (存在する場合)。
ポート	ポートのアドレス
プロトコル	プロトコルの名前。
SSL	SSL 暗号化が使用されているかどうか。
検出	
ステータス	検出のステータス。
初回検出	サードパーティソースでこの資産の検出が最初に見つかった日付。
前回検出	サードパーティソースでこの資産の検出が前回見つかった日付。
DNS 名	ドメインネームサービスの名前。CI が指定されていない場合、このフィールドは一致する CI を検索するために使用されます (存在する場合)。
NetBIOS 名	NetBIOS の名前。CI が指定されていない場合、このフィールドは一致する CI を検索するために使用されます (存在する場合)。
IP アドレス	IPv4 または IPv6 アドレス。CI が指定されていない場合、このフィールドは一致する CI を検索するために使用されます (存在する場合)。
ポート	ポートのアドレス
プロトコル	プロトコルの名前。
SSL	SSL 暗号化が使用されているかどうか。
検出回数	サードパーティソースによってこの資産でこの脆弱性が検出された回数。
統合実行	検出をインポートした統合実行。
クローズ 脆弱性一致アイテムが修正されてクローズされると、利用可能になります。このセクションのアイテムは読み取り専用です。	
クローズ担当者	脆弱性一致アイテムをクローズしたユーザー。
クローズ済み	脆弱性一致アイテムがクローズされた日付。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
クローズメモ	クローズに含まれる情報。
クローズ所要時間	VI がクローズされるまでの期間。VI が再オープンされた場合、 [クローズ所要時間] フィールドの値はゼロに設定されます。 [クローズ所要時間] フィールドの詳細については、「 脆弱性一致アイテムの経過時間の計算と表示」を参照してください。クローズ所要時間の計算をカスタマイズする方法の詳細については、 KB1703270 記事を参照してください。
メモ	
追加コメント / 作業メモ	関連情報。その他のコメントを追加するには、このチェックボックスをオンにします。 脆弱性対応 v20.0 以降では、保留された脆弱性一致アイテムの [メモ (Notes)] セクションに作業メモを追加できます。
アクティビティ	作業メモが作成された場合にのみ表示されます。
関連リンク	
リスクスコアを計算	[脆弱性重大度] または [リスクスコア] 算出のいずれかが有効になっている場合、[リスクスコア] フィールドが更新されます。

脆弱性一致アイテムの関連リストは次のとおりです。

関連リスト	説明
修復タスク	この脆弱性一致アイテムに関連付けられたタスク。
影響を受けるタスク	この脆弱性一致アイテムに関連付けられたタスク。
関連 IP アドレス	Qualys 脆弱性統合 脆弱性統合アプリケーションがインストールされている場合に使用できます。 重複排除中に検出された IP アドレス。
影響するサービス	この脆弱性一致アイテムの影響を受けるビジネスサービス。この情報が cmdb レコードで利用可能な場合に表示されます。この情報は、手動で入力するか、ServiceNow サービスマッピング アプリケーションを使用して入力できます。詳細については、「サービスマッピング 」を参照してください。 脆弱性一致アイテムに関連付けられた影響を受ける CI が追加または更新されると、レコードの保存時にこの関連リストの情報が自動的に更新されます。
ステータス変更承認	変更要求のステータスおよび VIT に関連付けられたその他の承認情報。
Qualys チケット	この脆弱性一致アイテムに関連付けられた Qualys チケット統合情報。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソリューションフォームのフィールド

レコードがサードパーティのソリューション統合からダウンロードされると、ソリューションが自動的に作成され、脆弱性対応 の [ソリューション] に保存されます。

ソリューション統合エントリーフィールド

次の表のインポートされたフィールドは読み取り専用です。

フィールド	説明
数値	ソリューションにアサインされた識別子。
ソース	ソリューションの作成元。
ソース ID	このソリューションのソース識別子。
リスク評価	ソリューションレコードのリスクスコアを [重大] から [なし] の範囲に分類します。ソリューションのリスク評価の詳細については、「脆弱性ソリューション管理」を参照してください。 **注:** ソリューションのリスク評価は、脆弱性一致アイテム、サードパーティの脆弱性エントリー、および修復タスクレコードのリスク評価と同じではありません。
リスクスコア	リスクスコアと、このソリューションを優先ソリューションとする脆弱性一致アイテムの数に基づく重み付け計算。ソリューションのリスクスコアの詳細については、「脆弱性ソリューション管理」を参照してください。 **注:** ソリューションレコードのリスクスコアは、脆弱性一致アイテム、サードパーティの脆弱性エントリー、および修復タスクレコードのリスクスコアと同じではありません。 SAM NVD が有効になっている場合に使用できますが、脆弱性に関連付けられたアクティブな脆弱性一致アイテム (VI) がない場合、ソリューションのリスクスコアはゼロに設定されます。
最高優先度	それより優先度が高いソリューションがないことを示します。
ソリューションタイプ	ソリューションの種類。選択肢は次のとおりです。 • ワークアラウンド • 緩和 • ベンダー修正 • パッチ • ロールアップ • エンタイトルメント • 修正されない • 利用可能なし
再起動が必要	再起動が必要です。選択肢は次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	• はい • いいえ • おそらく
公開日	この脆弱性がソースによって公開された日付。
最終変更日	この脆弱性がソースによって前回変更された日付。
まとめ	ソリューションの修正のサマリー。
セキュリティ情報	ソリューションに関連付けられたセキュリティ情報。
製品カテゴリ	ソリューションが適用される製品カテゴリ。
製品	ソリューションが適用される製品。
ソリューションの詳細	
説明	ソリューションソースから提供される内容がない場合は、詳細が記述された別の関連セクションまたはソリューションが示されます。
リンク	ソリューションに関連付けられたインポート済みインターネットリソース。
脆弱性の詳細	
脆弱性メモ	ソリューションによって修正された脆弱性のサマリー。
修復ステータス	
優先ソリューションターゲット これが優先ソリューションとなる、脆弱性一致アイテムとその一意の構成アイテム (CI) の修復ステータス。 **注:** 一意の CI とは、関連付けられている VI の数に関係なく、1 回だけカウントされる CI です。	
脆弱性一致アイテム	修復のためにこのソリューションが優先されるアクティブな (クローズされていない) 脆弱性一致アイテムの数。この数には、保留された脆弱性一致アイテムは含まれません。
合計 VI	修復のためにこのソリューションが優先されるアクティブおよびクローズ済みの脆弱性一致アイテムの数。この数には、保留された脆弱性一致アイテムは含まれません。
修復された VI の割合	脆弱性一致アイテム (VI) の修正の完了率。このソリューションが優先される VI に適用されます。この数には、保留された VI は含まれません。
残りの CI	修復のためにこのソリューションが優先される 1 つ以上のアクティブな脆弱性一致アイテムに関連付けられた一意の CI の数。この数には、保留された脆弱性一致アイテムの CI は含まれません。
合計 CI	修復のためにこのソリューションが優先される 1 つ以上のアクティブおよびクローズ済みの脆弱性一致アイテムに関連付けられた一意の CI の数。この数には、保留された脆弱性一致アイテムの CI は含まれません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
修復された CI の割合	修正された一意の CI の完了率 (その CI およびこのソリューションのすべての VI が修正されたことを意味します)。優先ソリューションで脆弱性一致アイテムに関連付けられた一意の CI の合計数に対する修正された CI の数によって決定されます。この数には、保留された脆弱性一致アイテムの CI は含まれません。
優先ソリューションターゲット (保留を含む) これが優先ソリューションとなる、脆弱性一致アイテムとその一意の CI の修復ステータス (保留を含む)。	
脆弱性一致アイテム	修復のためにこのソリューションが優先されるアクティブな (クローズされていない) 脆弱性一致アイテムの数。
合計 VI	修復のためにこのソリューションが優先されるアクティブおよびクローズ済みの脆弱性一致アイテムの数。
修復された VI の割合	脆弱性一致アイテム (VI) の修正の完了率。このソリューションが優先される VI に適用されます。
残りの CI	修復のためにこのソリューションが優先される 1 つ以上のアクティブな脆弱性一致アイテムに関連付けられた一意の CI の数。
合計 CI	修復のためにこのソリューションが優先される 1 つ以上のアクティブおよびクローズ済みの脆弱性一致アイテムに関連付けられた一意の CI の数。
修復された CI の割合	修正された一意の CI の完了率 (その CI およびこのソリューションのすべての VI が修正されたことを意味します)。優先ソリューションで脆弱性一致アイテムに関連付けられた一意の CI の合計数に対する修正された CI の数によって決定されます。この数には、保留された脆弱性一致アイテムの CI は含まれません。
見込みのある解決策のターゲット このソリューションに関連する脆弱性がある脆弱性一致アイテムとその一意の CI の修復ステータス。	
脆弱性一致アイテム	このソリューションが修復ソリューションとなる可能性があるアクティブな (クローズされていない) 脆弱性一致アイテムの数。この数には、保留された脆弱性一致アイテムは含まれません。
残りの CI	このソリューションが修正に対する見込みのある解決策となっている 1 つ以上のアクティブな脆弱性一致アイテムに関連付けられた一意の CI の数。この数には、保留された脆弱性一致アイテムは含まれません。
見込みのある解決策のターゲット (保留を含む) 優先ソリューション数を含めた、このソリューションによって修正可能な脆弱性がある脆弱性一致アイテムとその一意の CI の修復ステータス (保留を含む)。	
脆弱性一致アイテム	このソリューションが修復ソリューションとなる可能性があるアクティブな (クローズされていない) 脆弱性一致アイテムの数。
残りの CI	このソリューションが修正に対する見込みのある解決策となっている 1 つ以上のアクティブな脆弱性一致アイテムに関連付けられた一意の CI の数。
メモ	
内部メモ	修復スペシャリストに提供される編集可能なフィールド。
関連リンク	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ステータスを更新	修復ステータスが最後に更新された日時。 以下を更新します。 • 修復タスクステータス • リスクスコアと評価 • [修復ステータス] セクションのメトリクス
関連リスト	
脆弱性一致アイテム	修正のための優先ソリューションとしてこのソリューションに関連付けられた脆弱性一致アイテム。
サードパーティー脆弱性	このソリューションに関連するサードパーティの脆弱性。
CVE	このソリューションに関連する共通脆弱性識別子 (CVE) の脆弱性。
修復タスク	修正にこのソリューションが優先される、関連する脆弱性一致アイテムを含む修復タスク。
先行するソリューション	このソリューションの 1 つ以上の脆弱性を解決する、以前のソリューション。
優先ソリューション	このソリューションのすべての脆弱性を解決する、後発のソリューション。このリストは、[最高優先度] ボックスがオンになっている場合は空です。

アサイン解除要求の承認ワークフロー構成

自分自身および自分のグループの脆弱性一致アイテム (VI、VIT)、修復タスク、アプリケーション脆弱性一致アイテム (AVIT)、およびコンテナ脆弱性一致アイテム (CVIT) からアサインを解除するための承認ワークフローを設計できます。

VIT、修復タスク、AVIT、および CVIT にはそれぞれデフォルトの承認ルールがあります。各承認ルールには、デフォルトの承認構成があります。各承認構成には、デフォルトの承認レベルがあります。VIT、修復タスク、AVIT、および CVIT の承認ルールは、デフォルトで有効になっています。アドミニストレーターは、次の場所に移動して次のアクションを実行できます **All** (すべて) > 脆弱性対応 > 自分の承認 > 承認ルール をクリックし、適切な承認ルールを選択します。

- 承認ルールを有効または無効にする。
- 承認構成を作成および更新する。
- 承認ルールが適用される脆弱性一致アイテムと修復タスクの条件を定義する。
- 複数の承認者レベルを作成および更新する。

次の表に、ベースシステムに付属する VIT、修復タスク、AVIT、および CVIT のデフォルトの承認ルール、承認構成、および承認者レベルを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

デフォルトの承認ルール、承認構成、および承認者レベル

タイプ	承認ルール	承認構成	承認者レベル
VIT または VI	脆弱性一致アイテム フィールドの変更の要求	脆弱性一致アイテム フィールドの変更の要求	レベル 1：VI のアサイン解除要求
修復タスク	脆弱性グループフィールドの変更の要求	脆弱性フィールド変更要求	レベル 1：VG の要求をアサイン解除
AVIT	アプリケーションの脆弱性一致アイテム フィールドの変更の要求	アプリケーション脆弱性フィールド変更要求	アプリ脆弱性一致アイテムのアサイン解除
CVIT	コンテナ管理の承認	デフォルト構成：CVIT のアサイン解除	CVIT アサイン解除承認レベル：1

アサイン解除要求の承認方法の詳細については、「脆弱性対応 でアサイン解除要求を承認または却下する」を参照してください。

脆弱性対応 修復タスクルールの例

脆弱性とリスク、影響、または構成アイテム (CI) を使用する修復タスクルールの例。

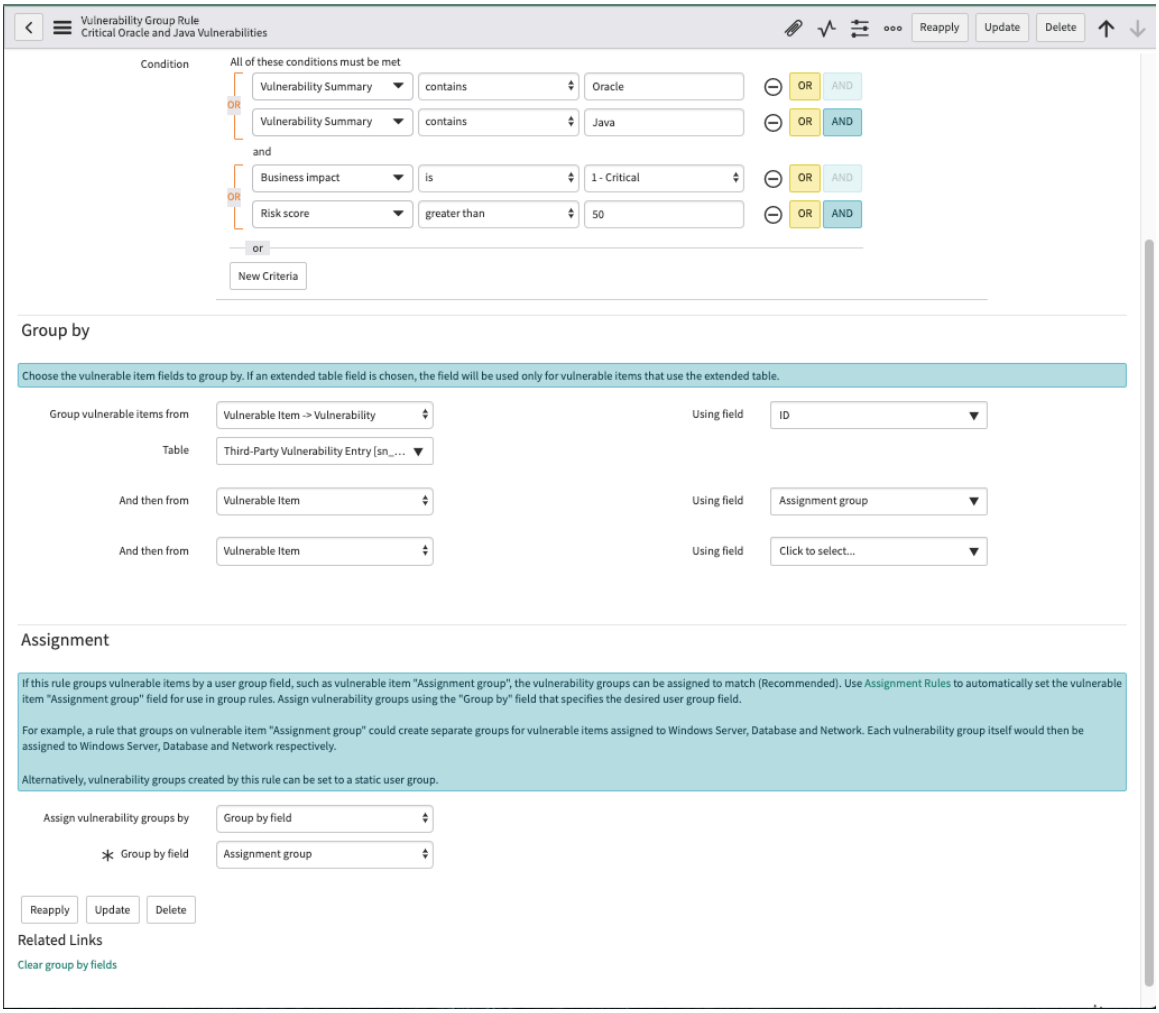
高リスクの **Java** および **Oracle** の脆弱性一致アイテムをグループ化するための修復タスクルール

この例は、Java および Oracle の脆弱性一致アイテムを脆弱性別にグループ化し、それぞれのサポートグループにアサインするルールのウォークスルーを示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクルールの例



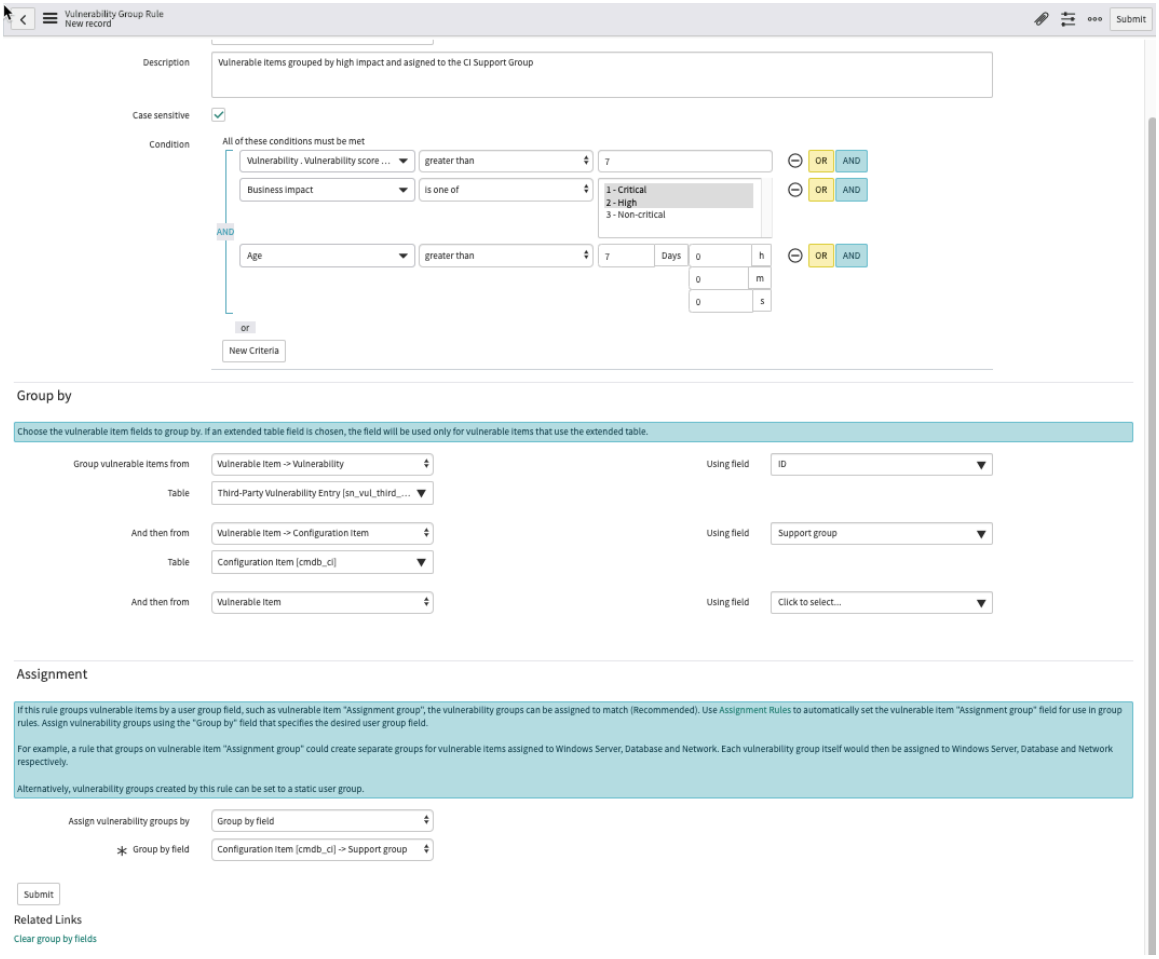
ヘッダーを右クリックして、[保存] を選択します。

影響度の高いすべての脆弱性一致アイテムを脆弱性および CI サポートグループに基づいてグループ化する修復タスクルール

この例は、影響度の高い脆弱性一致アイテムを CI サポートグループにアサインするグループルールのフォームフィールド設定を示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

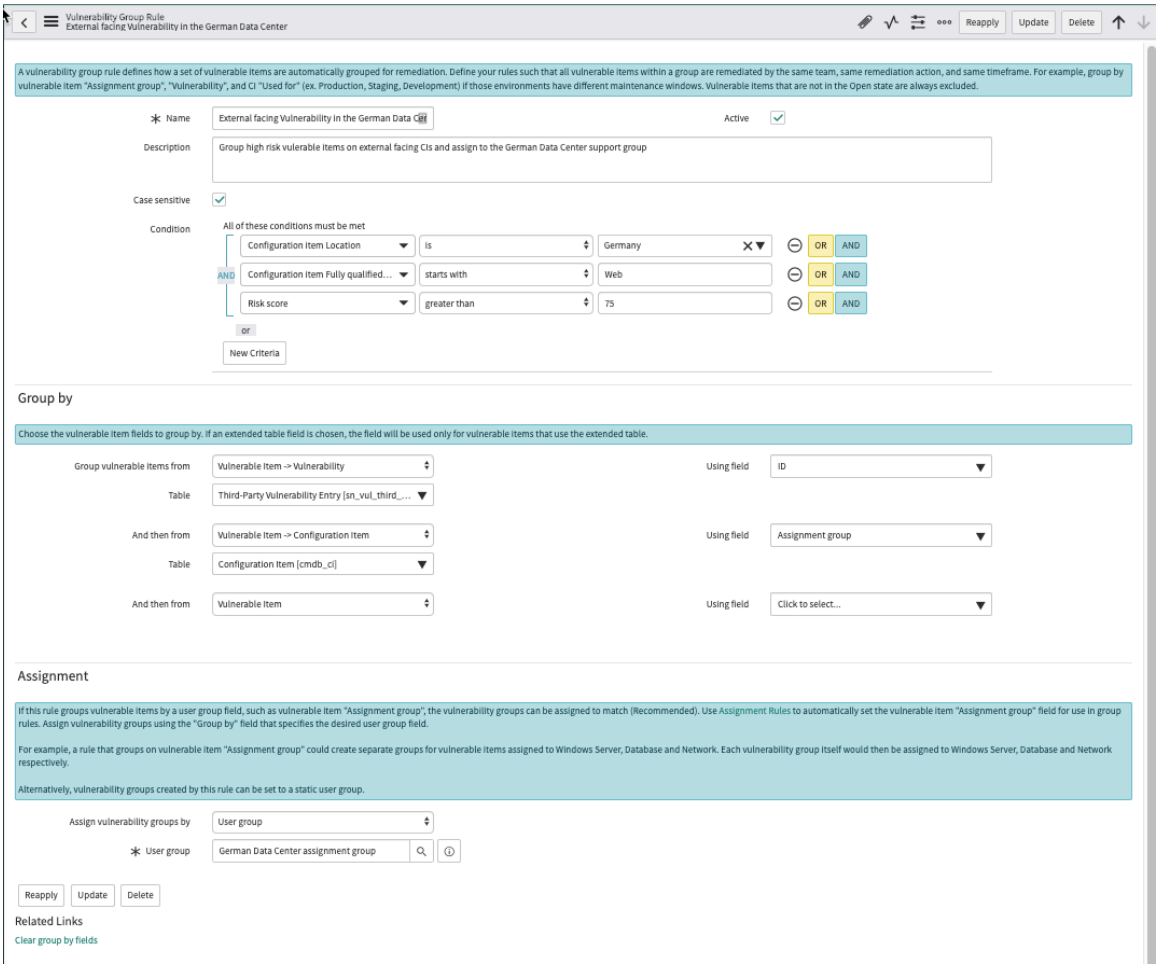


ドイツのデータセンターの外部向け **CI** に関する高リスクの脆弱性をすべてグループ化する修復タスクルール

この例は、ドイツのデータセンターの外部向け CI に関する高リスクの脆弱性のグループルールのフォームフィールド設定を示しています。これらは、ドイツのデータセンターのアサイン先グループにアサインされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



脆弱性対応 のリスクスコア算出の例

リスクスコア算出を決定し、組織に固有の脆弱性および資産データを使用するリスクスコアを生成できます。

リスクルール算出スコアを決定する例

次の例は、リスクルール算出のスコアを決定する方法を示しています。

リスクルール算出が、次の表のフィールドで構成されていると仮定します。

フィールド	重み付け	重み付けブレークダウン
脆弱性重大度	50	デフォルト：20 1 - 重大：100 2 - 高：80 3 - 中：60 4 - 低：40 5 - なし：20
脆弱性エクスプロイトが存在	50	デフォルト：50

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	重み付け	重み付けブレークダウン
		はい：100 いいえ：0

また、次の表に示されている脆弱性一致アイテムがシステムに存在すると仮定します。

ID	脆弱性重大度	脆弱性エクスプロイトが存在
VIT00001	1 - 重大	1 - はい
VIT00002	2 - 高	1 - はい
VIT00003	3：中	2 – いいえ
VIT00004	4：低	2 – いいえ
VIT00005	5：なし	2 – いいえ

脆弱性一致アイテムのリスクスコア算出は、次の式に基づいて計算されます。

`リスクスコア = (W(重大度) * FV (重大度) + W (エクスプロイト存在) * FV (エクスプロイト存在)) / 100`

ここで、**W** は重み付け、**FV** はフィールド値の重み付け割合です。

これらの脆弱性一致アイテムに対する計算後のリスクスコアは、次の表のとおりです。

ID	脆弱性重大度 **(50%)**	脆弱性エクスプロイトが存在 **(50%)**	結果のリスクスコア
VIT00001	1 - 重大 (50% x 100)	1 - はい (50% x 100)	100
VIT00002	2 - 高 (50% x 80)	1 - はい (50% x 100)	90
VIT00003	3 - 中 (50% x 60)	2 – いいえ (50% x 0)	30
VIT00004	4 - 低 (50% x 40)	2 – いいえ (50% x 0)	20
VIT00005	5 - なし (50% x 20)	2 – いいえ (50% x 0)	10

注:
VIT00005 の場合は、重大度の値が空であるため、デフォルトの重み付けが適用されます。

いずれかのフィールド値の重み付けのパーセンテージが変更された場合は、結果についてのこの表を参照してください。

フィールド	重み付け	重み付けブレークダウン
脆弱性重大度	50	• デフォルト：20 • 1 - 重大：100 • **2 -** 高：**70** * 改訂値

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	重み付け	重み付けブレークダウン
		• 3 - 中：60 • 4 - 低：40
脆弱性エクスプロイトが存在	50	• デフォルト：50 • はい：100 • いいえ：0

算出を再適用した後の脆弱性一致アイテムのリスクスコアを次の表に示します。

ID	脆弱性重大度 (50%)	脆弱性エクスプロイトが存在 (50%)	結果のリスクスコア
VIT00001	1 - 重大 (50% x 100)	1 - はい (50% x 100)	100
VIT00002	**2 - 高 (50% x 70)** * 改訂値	1 - はい (50% x 100)	**85** * 改訂値
VIT00003	3 - 中 (50% x 60)	2 – いいえ (50% x 0)	30
VIT00004	4 - 低 (50% x 40)	2 – いいえ (50% x 0)	20
VIT00005	5 - なし (50% x 20)	2 – いいえ (50% x 0)	10

検出のエラー処理

検出の作成中、あるいは脆弱性一致アイテムの作成中または更新中に、添付ファイルの処理エラーがログに記録されます。脆弱性統合プロセスが失敗した場合、[脆弱性統合ログ] タブにエラーが記録されます。

こうしたエラーは、次のいずれかのカテゴリでログに記録されます。

フィールド	説明
VI 作成	検出の作成中または更新中にエラーが発生しました。
検出	検出の作成中にエラーが発生しました。

脆弱性対応 のモバイルエクスペリエンス®

修復オーナーは、Now Platform インスタンス上の 脆弱性対応 (VR) アプリケーションに Android または iOS モバイルデバイスでアクセスできます。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性対応

脆弱性対応の概念とこの製品が組織にどのように役立つかを理解するには、「脆弱性対応について」を参照してください。

注:
Vulnerability Response Mobile アプリ モバイルをインストールする前に、 モバイルエージェント .

概要

修復オーナーロール (sn_vul.remediation_owner) を持つユーザーは、Vulnerability Response Mobile アプリ を使用して Now Platform インスタンスの脆弱性、修復タスク、およびアサインを Android または iOS モバイルデバイスから直接表示および検索できます。

修復タスク (RT) または VI が自分または自分のアサイン先グループにアサインされると、通知されます。このアプリを使用すると、修復オーナーはデスクトップに縛られることなく柔軟に再アサイン、フィールドの編集、修復の開始を行えます。

脆弱性、脆弱性一致アイテム、モジュール、およびすべてのソリューションにアクセスできます。モバイルデバイス上で以下のタスクを実行できます。

- 修復タスクを表示し、更新する。
- 変更要求を表示する。
- 修復タスクまたは脆弱性一致アイテムをアサイン先グループの別のメンバーに再アサインする。
- 重要な修復タスクが自分または自分のアサイン先グループにアサインされたときに通知を表示する。
- 修復タスクレコードのフィールドのサブセットを編集する。
- 特定の検索条件に一致する修復タスクを検索する。

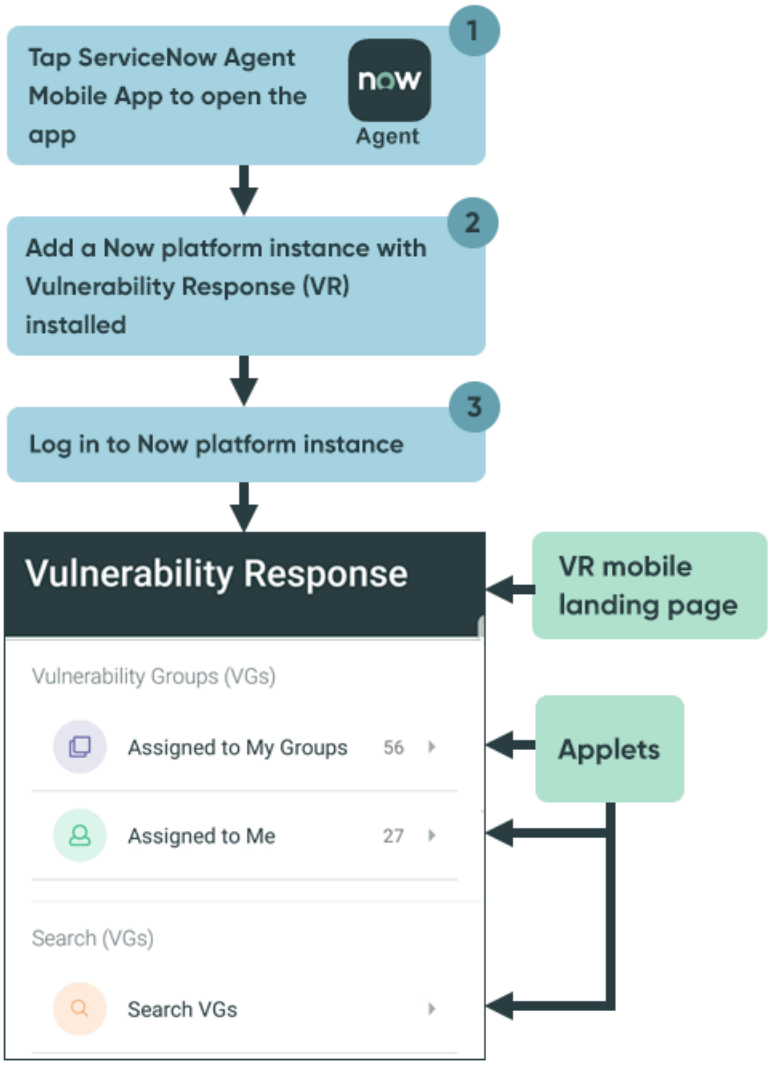
次の図は、モバイルデバイスから Now Platform インスタンスにログインする方法と、ログイン後に表示される Vulnerability Response Mobile アプリ のランディング画面を示しています。

Now Platform インスタンスを設定し、Vulnerability Response Mobile アプリ をインストールする方法の詳細な手順については、「Vulnerability Response Mobile アプリ のチェックリストをセットアップ」を参照してください。ログイン方法については、「Vulnerability Response Mobile アプリ へのログイン」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Vulnerability Response Mobile アプリ



アプリケーション

アプリケーションとは、Now Platform インスタンス内で特定の機能を提供する、セキュリティインシデントレスポンス (SIR)、脆弱性対応 (VR)、ガバナンス、リスク、コンプライアンス (GRC)、その他の ServiceNow 製品などの ServiceNow ソフトウェアコンポーネントです。Now Platform インスタンスにモバイルアプリを含むコアアプリケーションをインストールすると、これらのアプリケーションはモバイルデバイスの下部にアイコンとして表示されます。

モバイルデバイス上の脆弱性対応アイコン

フォルダー

各 ServiceNow® モバイル アプリケーションには、カテゴリ別にアプレットを分離するフォルダーが含まれています。前の画像では、修復タスクと Search (VG) が Vulnerability Response Mobile アプリ のフォルダーです。

アプレット

アプレットは、アプリケーション内のさまざまなオプションです。前の画像では、修復タスクの下のアイコンと Search (VG) が Vulnerability Response Mobile アプリ で使用可能なアプレットです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Vulnerability Response Mobile アプリ のアプレットの詳細については、次のトピックを参照してください。

Vulnerability Response Mobile アプリ のチェックリストをセットアップ

次のチェックリストには、Now Platform® インスタンスおよびモバイルデバイスで Vulnerability Response Mobile アプリを使用する前に完了する必要があるセットアップタスクが含まれています。

始める前に
右側の列の各ステップの後に詳細情報が表示されます。このタスクの完了までの推定時間：15 ～ 20 分。

必要なロール：admin、sn_vul.remediation_owner

Vulnerability Response Mobile アプリ用のモバイルデバイスが正常に設定されました。次のステップでは、Vulnerability Response Mobile アプリにログインして、Now Platform インスタンスをモバイルデバイスに追加します。

手順

1. オプションとして、このチェックリストを印刷して、Vulnerability Response Mobile アプリのインストールに必要なタスクを進めるために使用します。
2. Vulnerability Response Mobile アプリ にログインして Now Platform インスタンスを追加できるように、リストの各アイテムが完了していることを確認します。

モバイルチェックリスト

アイテム	説明
☐	admin ロールを持つユーザーは、脆弱性対応 コアアプリケーションが Now Platform インスタンスにインストールされていることを確認します。これは、モバイルデバイスで表示する Now Platform インスタンスです。 **注:** 脆弱性対応 コアアプリケーションと Now Platform インスタンスは、ファミリーリリースが同じである必要があります。 **a.** コアアプリケーションがインスタンスにインストールされていることを検証するには、[プラグイン] に移動して、脆弱性対応 を検索します。 **b.** 脆弱性対応 コアアプリケーションがまだインストールされていない場合は、[インストール] をクリックして、インストールします。 脆弱性対応 コアアプリケーションのインストールの詳細については、「脆弱性対応 のインストール」を参照してください。 ServiceNow Store での 脆弱性対応 コアアプリケーションの取得、エンタイトルメントの取得、コアアプリケーションのインストール、および依存関係のアクティブ化の詳細については、「セキュリティオペレーション および ServiceNow Store」を参照してください。
☐	admin ロールを持つユーザーは、モバイルデバイスで表示する Now Platform インスタンスに Vulnerability Response Mobile アプリ がインストールされていることを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アイテム	説明
	注: Vulnerability Response Mobile アプリ と Now Platform インスタンスは、ファミリーリリースが同じである必要があります。Vulnerability Response Mobile アプリ と 脆弱性対応 アプリケーションは互換性がある必要があります。脆弱性対応アプリケーションの互換性の詳細については、「脆弱性対応とコンフィギュレーションコンプライアンスの互換性マトリクス」を参照してください。 ServiceNow Store から Vulnerability Response Mobile アプリ をダウンロードして、Now Platform インスタンスにインストールします。 Vulnerability Response Mobile アプリ をインストールすると、その依存関係である com.glide.sg および com.glide.sg.agent_native_client もインストールされます。 これらの依存関係がインストールされていることを確認するには： **a.** 次のように移動する。 **All** (すべて) > プラグイン. **b.** プラグイン ID (com.glide.sg および com.glide.sg.agent_native_client) を検索します。 **c.** アクティブ化されていない場合は、これらのプラグインをアクティブ化します。これらのプラグインは Vulnerability Response Mobile アプリ に必要です。 ServiceNow Store での Vulnerability Response Mobile アプリアプリケーションの取得、エンタイトルメントの取得、アプリケーションのインストール、および依存関係のアクティブ化の詳細については、「セキュリティオペレーション および ServiceNow Store」を参照してください。
☐	admin ロールを持つユーザーは、Now Platform インスタンスで、モバイルユーザーに必要な Now Platform ロールをアサインしたことを確認します。 **a.** ユーザーにアサインされているロールを表示するには、次に移動します: **All** (すべて) > アドミニストレーション > ユーザー. **b.** ユーザー名、続いてロール関連リストを選択します。このユーザーにアサインされているすべてのロールが表示されます。 **c.** ユーザーがアサインされていることを確認するか、IT インフラストラクチャライブラリロール (itil) を持つユーザーをアサインします。itil ロールを持つユーザーは、変更要求と修復タスクを作成、オープン、更新、およびクローズできます。itil ロールを持つユーザーのみにタスクをアサインすることができます。 **d.** ユーザーがアサインされていることを確認するか、修復オーナーロール (sn_vul.remediation_owner) を持つユーザーをアサインします。sn_vul.remediation_owner ロールを持つユーザーは、脆弱性レコードとソリューションレコードを読み取ることができます。このロールは、itil ロールをアサインすると自動的に追加されます。 **e.** 必要なアサイン先グループを作成し、こうしたグループにモバイルユーザーをアサインしたことを確認します。 **注:** モバイルアプリケーションに多数のユーザーがいる場合は、sn_vul.remediation_owner ロールをグループにアサインすることもできます。グループに追加する各ユーザーは、このロールを継承します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アイテム	説明
	アサインルールおよびグループの詳細については、「脆弱性対応 アサインルールの概要」を参照してください。 ユーザーの詳細、およびユーザーとグループへのロールのアサインの詳細については、「ユーザー管理」を参照してください。
☐	修復オーナーロール (sn_vul.remediation_owner) を持つユーザーは、モバイルデバイスで最新の ServiceNow Agent アプリをダウンロードします。 最新の Agent アプリは、Apple iOS App Store と Google Play ストアで入手できます。
☐	sn_vul.remediation_owner ロールを持つユーザーとして、モバイルデバイスと Now Platform インスタンスで通知が有効になっていることを確認します。 重要な修復タスクが自分または自分のアサイン先グループにアサインされると、通知によって知らされます。タイムリーな修正を支援するには、通知を有効にした後、Vulnerability Response Mobile アプリ 内の通知をクリックしてレコードに直接移動します。 Now Platform インスタンスで通知を有効にしてモバイルデバイスに表示されるようにするには、次の手順を実行します。 **a.** Vulnerability Response Mobile アプリ を Now Platform インスタンスにダウンロードしてインストールしたことを確認します。 **b.** Now Platform インスタンスの [システムの設定] の [通知] で、**ServiceNow Mobile** アプリケーションが有効になっていることを確認します。 通知の設定の詳細については、「Setting notification preferences in Core UI」を参照してください。 Now Platform の通知は、モバイルデバイスのメッセージ画面にも表示されます。モバイルデバイスの設定でも通知が有効になっていることを確認します。

自動翻訳

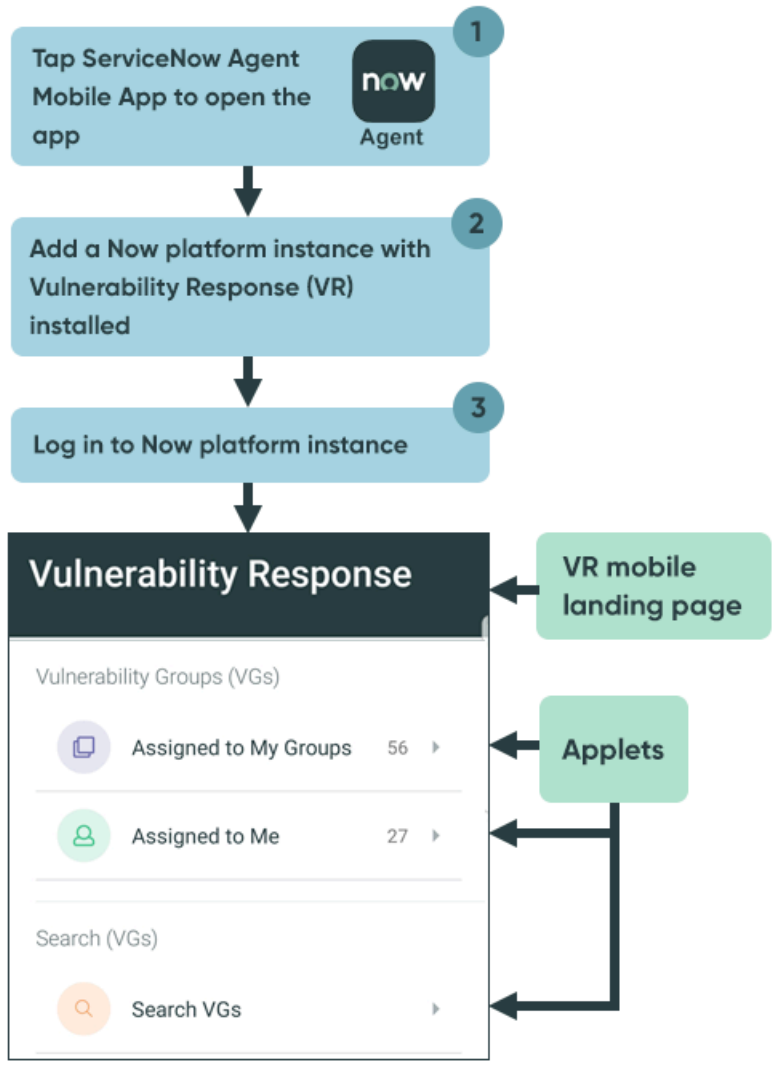
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Vulnerability Response Mobile アプリ へのログイン

脆弱性対応モバイルアプリを開き、脆弱性対応を使用する Now Platform インスタンスをモバイルデバイスに追加します。

始める前に
「Vulnerability Response Mobile アプリ のチェックリストをセットアップ」で説明されているセットアップ手順を完了していることを確認します。

Vulnerability Response Mobile アプリ

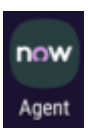


必要なロール：修復オーナー (sn_vul.remediation_owner)

このタスクについて
このタスクの完了にかかる時間：5 ～ 7 分。

手順

1. モバイルデバイスで、**ServiceNow** エージェントアプリをタップします。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Now Platform インスタンスにまだログインしていない場合は、 [インスタンス] 画面が表示されます。

2. 脆弱性対応 コアアプリケーションを含む Now Platform インスタンスがまだモバイルデバイスに追加されていない場合は、次の手順に従って追加します。

   a. 表示される [インスタンス] 画面で、プラスアイコン ( ) をタップします。
   Now Platform インスタンスのアドレスを入力して保存するように求める画面が表示されます。

   b. フィールドに入力します。

フィールド名	説明
インスタンスアドレスを入力するか、QR コードをスキャンしてください。	1 つ選択して続行します。 ▪ .service-now.com の前に、Now Platform インスタンスの名前 (例：vrmobilenewyorkagent) を入力します。 ▪ アドレスを入力します。これは、モバイルデバイスで表示する Now Platform インスタンスの URL のアドレスです。 ▪ QR コードをスキャンします。
(オプション) ニックネームを入力	このインスタンスのニックネームを入力します。デバイスに複数のインスタンスが存在する場合、ニックネームを使用することで、Now Platform インスタンスをすばやく見つけることができます。

   c. [保存してログイン] をタップします。

3. 表示される ServiceNow ログイン画面で、追加する Now Platform インスタンスの [ユーザー名] と [パスワード] を入力し、[ログイン] をタップします。
   [脆弱性対応] ランディング画面が表示されます。Vulnerability Response Mobile アプリ に正常にログインしました。

4. ログイン後、Vulnerability Response Mobile アプリ で通知が有効になっていることを確認します。

   a. 下部のランディング画面で、[通知] をタップします。

   b. [通知] 画面で、[通知を有効にします] をタップします。
   Now Platform からの通知は、Vulnerability Response Mobile アプリ の [通知] 画面に表示されます。

5. モバイルデバイスでインスタンスにログインすると、そのインスタンスがデバイスのデフォルトの Now Platform インスタンスになります。
   デバイス上の別の Now Platform を表示するには、デフォルトのインスタンスからログアウトする必要があります。ログアウトするには：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. [設定] アイコンをタップします。

b. [ログアウト] をタップします。
[インスタンス] 画面に、モバイルデバイスに追加した Now Platform インスタンスが表示されます。

c. オプション: 別のインスタンスをタップしてログインするか、前の手順に従って別のインスタンスを追加します。

タスクの結果

デバイスで **[ServiceNow** エージェント] アプリをタップした後に Vulnerability Response Mobile アプリ のインスタンス画面が表示されない場合は、デバイスで **[ServiceNow** エージェント] が信頼できるアプリとして許可されていることを確認してください。信頼できるアプリとしてのアクセスを許可するには、デバイスの [設定] および [一般的なデバイス管理] に移動し、オプション ([アプリを信頼 (Trust app)] など) をタップしてアクセスを許可します。

ログイン画面に認証情報を入力した後にエラーメッセージが表示された場合は、Now Platform インスタンスのユーザー名とパスワードが正しいことを確認してください。

ランディング画面の表示に問題がある場合は、ネットワーク接続を確認してください。

ServiceNow エージェントアプリをタップしても [インスタンス] 画面を表示できない場合は、デバイスからアンインストールしてください。Apple iOS App Store または Google Play ストアから最新バージョンのアプリを入手して、再インストールしてみてください。

Vulnerability Response Mobile アプリ での修復タスクの表示、アサイン、編集

グループにアサインされた修復タスク (RT) レコードのフィールドを表示、アサイン、または編集します。脆弱性、脆弱性一致アイテム、およびソリューションレコードと関連リスト内を移動して、対処するソリューション、展開メトリクス、およびアイテムを表示します。

始める前に

必要なロール：修復オーナー (sn_vul.remediation_owner)

このタスクについて

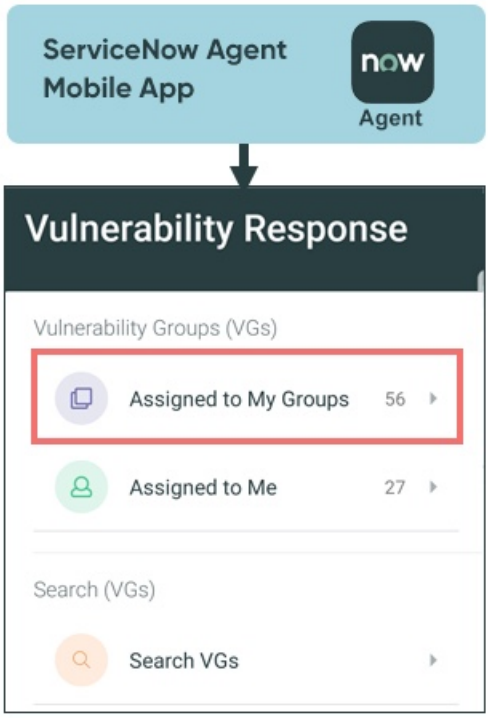
RT (VUL) レコードを自分にアサインするか、グループの別のメンバーに再アサインします。あるいは、編集、アサイン、または修正の前に、アクティブな修復タスクレコード、脆弱性一致アイテム (VI)、NVD 脆弱性、およびソリューションの詳細を表示します。このタスクの完了にかかる時間：5 ～ 10 分。

手順

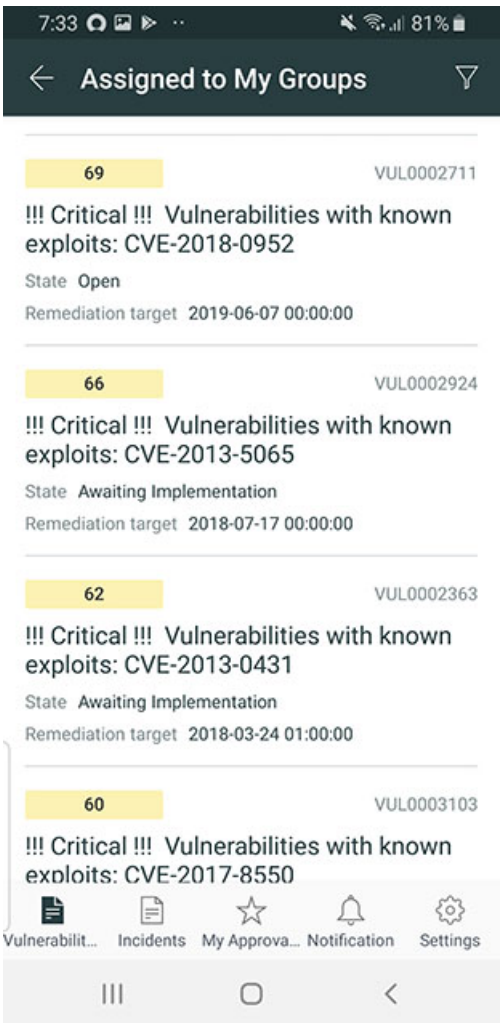
1. モバイルデバイスで Now Platform インスタンスにログインしていない場合、詳細については、「Vulnerability Response Mobile アプリ へのログイン」を参照してください。
2. [脆弱性対応] ランディング画面表示した状態で、[所属グループにアサイン済み] をタップします。
ログイン後に Vulnerability Response Mobile アプリ から移動した場合は、Now Agent アプリをタップすると、いつでも最後に表示していた画面に戻ります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳



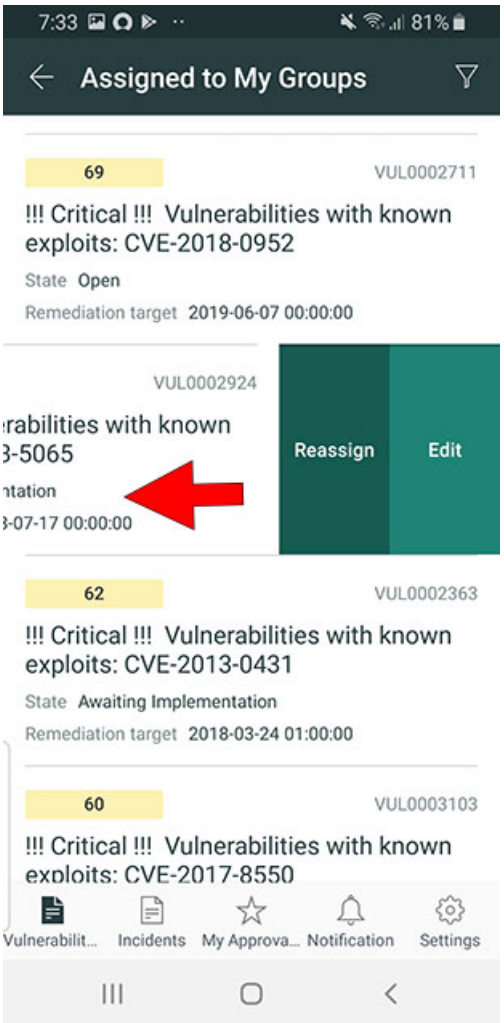
所属グループにアサイン済みのオープンレコードのリストが表示されます。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

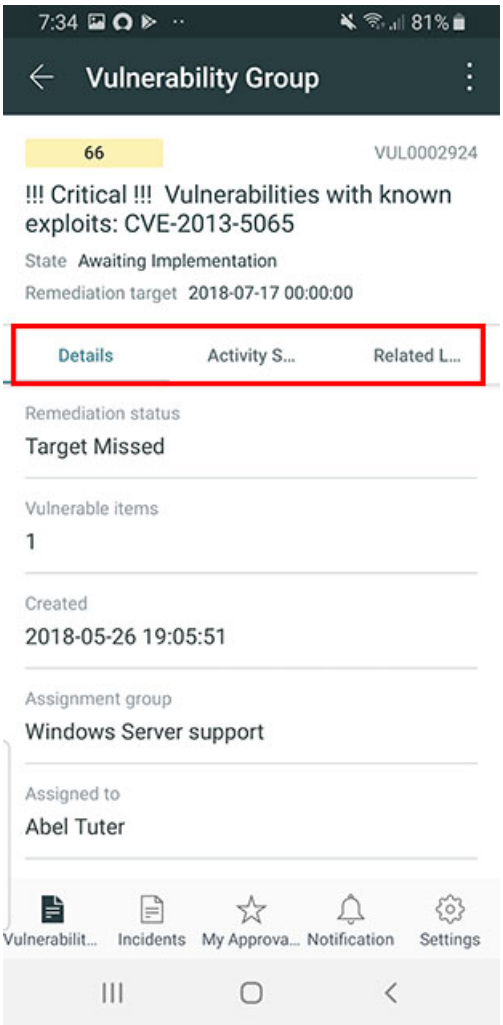
3. オプション: 特定の基準に一致するレコードを検索するには、「Vulnerability Response Mobile アプリでの修復タスクの検索」を参照してください。
4. または、表示されているフィルターアイコン ( ) を使用して、リストのレコード数を制限するフィルターを設定します。
   モバイルアプリの画面でのレコードのフィルタリングは、Now Platform で条件ビルダーを使用したフィルタリングと同様に機能します。
5. リストからレコードを直接再アサインまたは編集するには、オープンレコードのリストが表示された状態で、レコードを左にスワイプしてメニューを開きます。



6. 表示されるメニューでいずれかを選択して、続行します。
7. または、オープン脆弱性レコードの詳細を表示し、関連付けられたレコードと関連リストをさらに表示するには、[所属グループにアサイン済み] 画面を表示した状態で、リスト上のレコードをタップします。
8. 表示されるオープン修復タスクレコードで、次の表のいずれかのオプションを選択して、作業メモまたは関連リストを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



次の画像は、選択した脆弱性の修復タスクレコードから優先ソリューションレコードへのナビゲーションパスを示しています。レコードと関連リスト内を移動して、対処するソリューション、展開メトリクス、およびアイテムを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクからソリューションレコードまでのナビゲーションパス

9. レビュー、編集、または修正後、いずれかを選択して続行します。

Vulnerability Response Mobile アプリでアサインされた修復タスクの表示、再アサイン、編集

自分にアサインされた修復タスクレコードのフィールドを表示、アサイン、または編集します。レコードと関連リスト内を移動して、対処するソリューション、展開メトリクス、およびアイテムを表示します。

始める前に

必要なロール：修復オーナー (sn_vul.remediation_owner)

このタスクについて

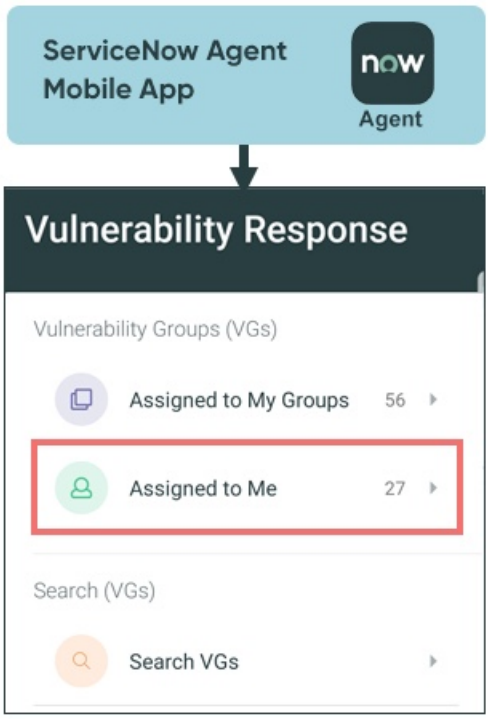
自分にアサインされたレコードを再アサインまたは編集します。編集、アサイン、または修正の前に、アクティブな修復タスクレコード、脆弱性一致アイテム (VI) レコード、脆弱性、およびソリューションの詳細を表示します。このタスクの完了にかかる時間：5 ～ 10 分。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

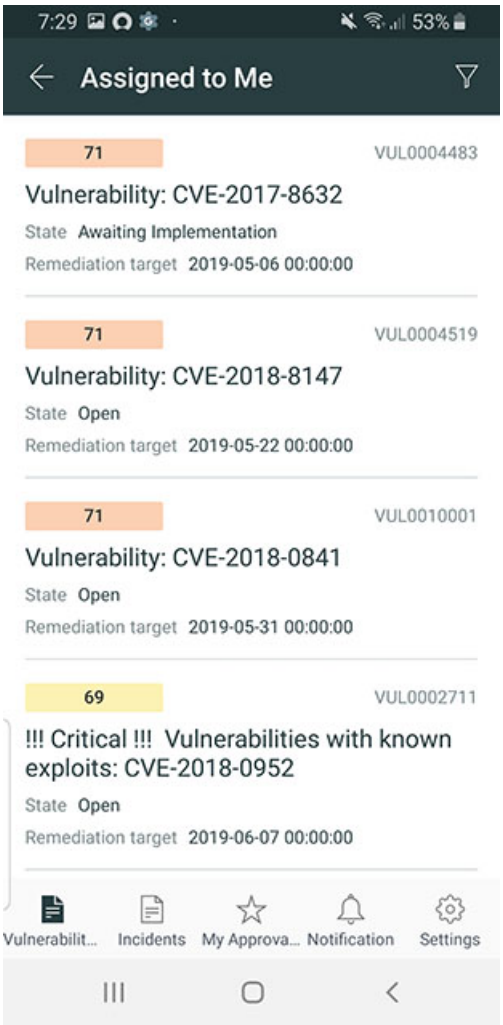
1. モバイルデバイスで Now Platform インスタンスにログインしていない場合、詳細については、「Vulnerability Response Mobile アプリ へのログイン」を参照してください。
2. [脆弱性対応] ランディング画面を表示した状態で、[自分にアサイン済み] をタップします。
   ログイン後に Vulnerability Response Mobile アプリ から移動した場合は、Now Agent アプリをタップすると、いつでも最後に表示していた画面に戻ります。



自分にアサインされている修復タスクレコードのリストが表示されます。

自動翻訳

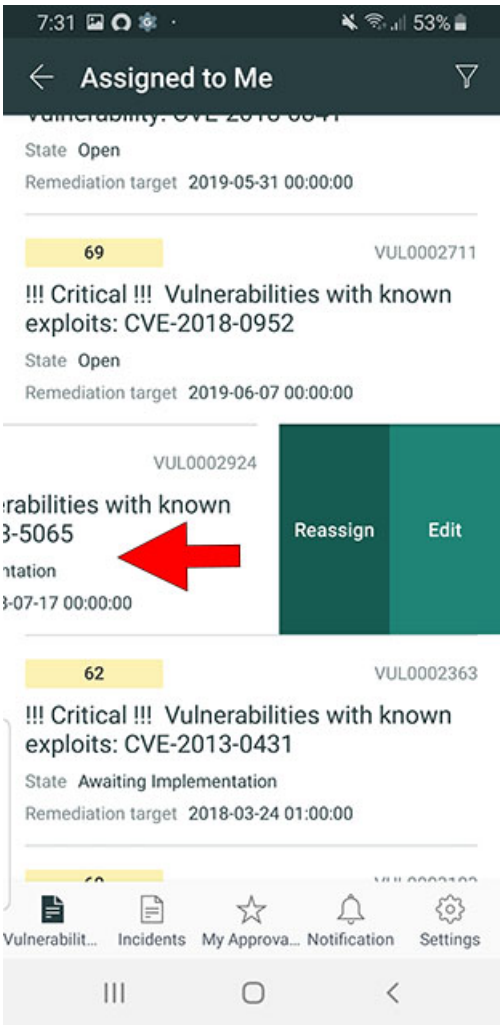
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. オプション: 特定の基準に一致するレコードを検索するには、「Vulnerability Response Mobile アプリでの修復タスクの検索」を参照してください。
4. または、表示されているフィルターアイコン ( ) を使用して、リストのレコード数を制限するフィルターを設定します。
   モバイルアプリの画面でのレコードのフィルタリングは、Now Platform で条件ビルダーを使用したフィルタリングと同様に機能します。
5. リストからレコードを直接再アサインまたは編集するには、[自分にアサイン済み] 画面を表示した状態で、レコードを左にスワイプしてメニューを開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

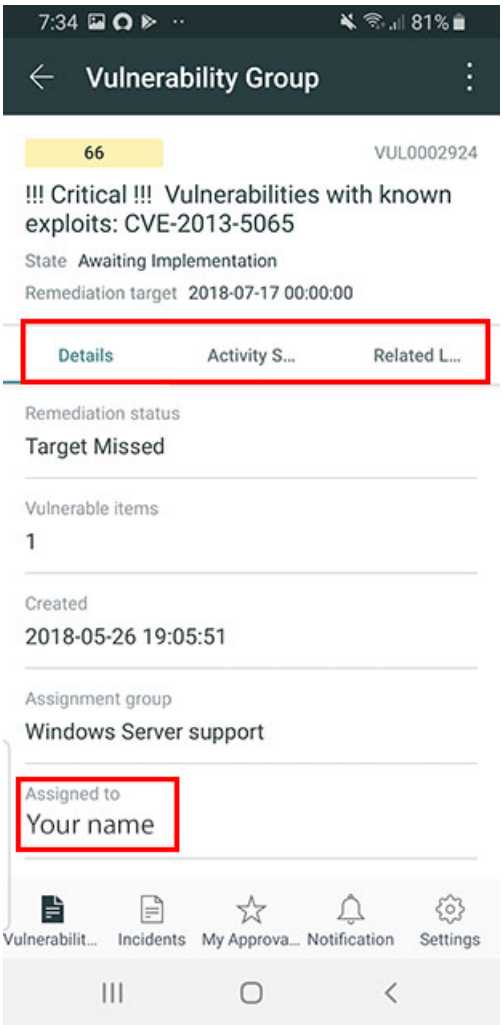


6. 1 つ選択して続行します。

7. または、オープンレコードの詳細を表示し、関連付けられたレコードと関連リストをさらに表示するには、[自分にアサイン済み] 画面を表示した状態で、リスト上のレコードをタップします。
8. 表示されるオープン修復タスクレコードで、次の表のいずれかのオプションを選択して、作業メモまたは関連リストを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



次の画像は、選択した脆弱性の修復タスクレコードから優先ソリューションレコードへのナビゲーションパスを示しています。レコードと関連リスト内を移動して、対処するソリューション、展開メトリクス、およびアイテムを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

RT からソリューションレコードまでのナビゲーションパス

9. 1 つ選択して続行します。

Vulnerability Response Mobile アプリでの修復タスクの検索

選択した特定の検索条件に一致する修復タスクを検索します。

始める前に
必要なロール：修復オーナー (sn_vul.remediation_owner)

このタスクについて
このタスクの完了にかかる時間：5 ～ 7 分。

手順

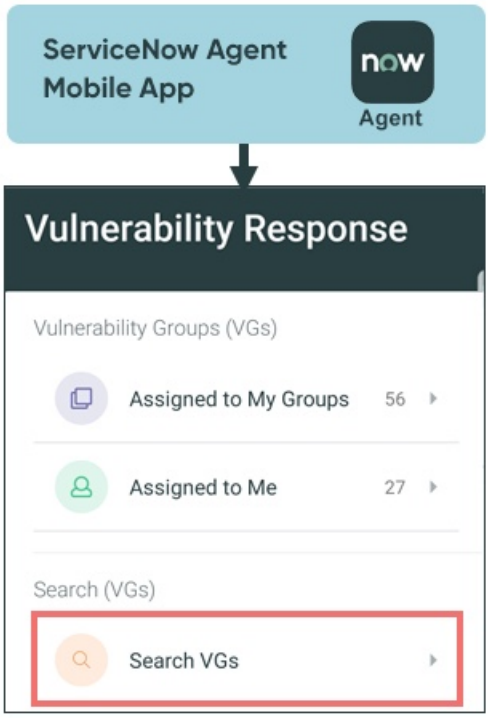
1. モバイルデバイスで Now Platform インスタンスにログインしていない場合、詳細については、「Vulnerability Response Mobile アプリ へのログイン」を参照してください。

2. [脆弱性対応] ランディング画面表示した状態で、**[RT を検索 (Search RT)]** をタップします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ログイン後に Vulnerability Response Mobile アプリ から移動した場合は、Now Agent アプリをタップすると、いつでも最後に表示していた画面に戻ります。



3. 表示される検索画面で、フィールドをタップし、目的の検索条件をフォームに入力します。

   表の後にある指示に従って、検索条件の編集、検索条件のクリア、または検索の送信を行います。

タップするフィールド	Android デバイスにエントリーを追加するには	iOS デバイスにエントリーを追加するには
数値	画面をタップし、RT 番号 (VUL0002372 など) を入力します。この番号は RT レコードの右上に表示されます。チェックマークアイコンをタップしてエントリーを追加し、[RT を検索 (Search RT)] 画面に戻ります。 閉じるアイコン (X) をタップすると入力がキャンセルされ、[RT を検索 (Search RT)] フィールドに戻ります。	RT 番号 (VUL0002372 など) を入力します。この番号は、RT レコードの右上に表示されます。[完了] をタップすると、[RT を検索 (Search RT)] 画面に戻ります。 展開されたフィールドで、[キャンセル] をタップしてエントリーをクリアし、[RT を検索 (Search RT)] 画面に戻ります。
リスク評価	後ろにチェックマークアイコンがある 1 つ以上のアイテムをタップしてエントリーを追加し、[RT を検索 (Search RT)] 画面に戻ります。 閉じるアイコン (X) をタップすると入力がキャンセルされ、[RT を検索 (Search RT)] フィールドに戻ります。	エントリーを追加するには、1 つ以上のアイテムをタップするか、検索アイコンをタップして検索フィールドにエントリーを入力します。[完了] をタップすると、[RT を検索 (Search RT)] 画面に戻ります。 展開されたフィールドで、[キャンセル] をタップしてエントリーをクリア

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タップするフィールド	Android デバイスにエントリーを追加するには	iOS デバイスにエントリーを追加するには
		し、[RT を検索 (Search RT)] 画面に戻ります。
修復ステータス	後ろにチェックマークアイコンがある 1 つ以上のアイテムをタップしてエントリーを追加し、[RT を検索 (Search RT)] 画面に戻ります。 閉じるアイコン (X) をタップすると入力がキャンセルされ、[RT を検索 (Search RT)] フィールドに戻ります。	エントリーを追加するには、1 つ以上のアイテムをタップするか、検索アイコンをタップして検索フィールドにエントリーを入力します。[完了] をタップすると、[RT を検索 (Search RT)] 画面に戻ります。 展開されたフィールドで、[キャンセル] をタップしてエントリーをクリアし、[RT を検索 (Search RT)] 画面に戻ります。
状態	後ろにチェックマークアイコンがある 1 つ以上のアイテムをタップしてエントリーを追加し、[RT を検索 (Search RT)] 画面に戻ります。 閉じるアイコン (X) をタップすると入力がキャンセルされ、[RT を検索 (Search RT)] フィールドに戻ります。	エントリーを追加するには、1 つ以上のアイテムをタップするか、検索アイコンをタップして検索フィールドにエントリーを入力します。[完了] をタップすると、[RT を検索 (Search RT)] 画面に戻ります。 展開されたフィールドで、[キャンセル] をタップしてエントリーをクリアし、[RT を検索 (Search RT)] 画面に戻ります。
理由	後ろにチェックマークアイコンがある 1 つ以上のアイテムをタップしてエントリーを追加し、[RT を検索 (Search RT)] 画面に戻ります。 閉じるアイコン (X) をタップすると入力がキャンセルされ、[RT を検索 (Search RT)] フィールドに戻ります。	エントリーを追加するには、1 つ以上のアイテムをタップするか、検索アイコンをタップして検索フィールドにエントリーを入力します。[完了] をタップすると、[RT を検索 (Search RT)] 画面に戻ります。 展開されたフィールドで、[キャンセル] をタップしてエントリーをクリアし、[RT を検索 (Search RT)] 画面に戻ります。
アサイン先グループ	リストから 1 つを選択するか、検索アイコンをタップして検索フィールドにエントリーを入力します。 エントリーなしの場合に、[アサイン先グループ] および [アサイン先] フィールドの値をクリアするには、[なし] を選択します。	リストから 1 つを選択するか、検索アイコンをタップして検索フィールドにエントリーを入力します。 エントリーなしの場合に、[アサイン先グループ] および [アサイン先] フィールドの値をクリアするには、[なし] を選択します。
アサイン先	リストから 1 つを選択するか、検索アイコンをタップして検索フィールドにエントリーを入力します。 エントリーなしの場合に、[アサイン先グループ] および [アサイン	リストから 1 つを選択するか、検索アイコンをタップして検索フィールドにエントリーを入力します。 エントリーなしの場合に、[アサイン先グループ] および [アサイン

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タップするフィールド	Android デバイスにエントリーを追加するには	iOS デバイスにエントリーを追加するには
	先] フィールドの値をクリアするには、[なし] を選択します。	先] フィールドの値をクリアするには、[なし] を選択します。
簡単な説明	画面をタップしてテキストを入力します。機能は、このフィールドのテキスト文字列と部分的なテキスト文字列を認識しますが、ワイルドカード (*) は使用できません。大文字は必須ではありません。チェックマークアイコンをタップしてエントリーを追加し、[RT を検索 (Search RT)] 画面に戻ります。	画面でテキストを入力します。機能は、このフィールドのテキスト文字列と部分的なテキスト文字列を認識しますが、ワイルドカード (*) は使用できません。大文字は必須ではありません。[完了] をタップすると、[RT を検索 (Search RT)] 画面に戻ります。 展開されたフィールドで、[キャンセル] をタップしてエントリーをクリアし、[RT を検索 (Search RT)] 画面に戻ります。
説明	画面をタップしてテキストを入力します。機能は、このフィールドのテキスト文字列と部分的なテキスト文字列を認識しますが、ワイルドカード (*) は使用できません。大文字は必須ではありません。チェックマークアイコンをタップしてエントリーを追加し、[RT を検索 (Search RT)] 画面に戻ります。	画面でテキストを入力します。機能は、このフィールドのテキスト文字列と部分的なテキスト文字列を認識しますが、ワイルドカード (*) は使用できません。大文字は必須ではありません。[完了] をタップすると、[RT を検索 (Search RT)] 画面に戻ります。 展開されたフィールドで、[キャンセル] をタップしてエントリーをクリアし、[RT を検索 (Search RT)] 画面に戻ります。

Android デバイスの場合、[RT を検索 (Search RT)] 画面が表示され、すべての条件が入力された状態で、いずれかを選択して続行します。

4. iOS デバイスの場合、[RT を検索 (Search RT)] 画面を表示した状態で、いずれかを選択して続行します。

5. オプション: 検索で複数のレコードが返される場合は、「Vulnerability Response Mobile アプリでのレコードのフィルタリング」により、検索結果を絞り込むことができます。

Vulnerability Response Mobile アプリ でのレコードのフィルタリング

追加のフィルターを設定して、画面に表示されるレコードの数を制限します。モバイルアプリでのレコードのフィルタリングは、Now Platform で条件ビルダーを使用したフィルタリングと同様に機能します。

始める前に
必要なロール：修復オーナー (sn_vul.remediation_owner)

このタスクについて
このタスクの所要時間：5 分

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 検索結果をさらに絞り込む場合、または表示されるレコードリストに追加のフィルター基準を入力する場合は、フィルターアイコン ( ) をタップします。
2. [フィルター] 画面を表示した状態で、フィールドをタップして展開します。
   修復タスクレコードの検索条件を入力する共通フィールドは、[ステータス] フィールドです。
3. 表示されるオプションから、チェックボックスをタップするか、フィルターのアイテムをタップします。
   フィルターの多くでは、複数のオプションを選択できます。
4. 戻るアイコン ( ) をタップするか、[完了] をタップして、フィールドに加えた変更を保存します。
   選択した条件が [フィルター] 画面に表示されます。基準と一致するレコードの数も画面の上部に表示されます。[リセット] をタップして、すべてのフィルターを削除し、デフォルト設定に戻します。
5. オプション: フィルター条件の設定を続行するには、[フィルター] 画面で手順 1 ～ 4 を繰り返します。
6. 交差アイコン ( ) をタップして、AND 条件を作成します。
7. または、交差アイコン ( ) をタップして、OR 条件を作成します。
8. 必要なすべての条件を追加したら、表示された [フィルター] 画面で [完了] をタップします。
   フィルター基準に一致するレコードのみが画面に表示されます。

関連情報

Vulnerability Response Mobile アプリでの修復タスクの検索

脆弱性対応オーケストレーション

脆弱性対応オーケストレーションのワークフローおよびアクティビティでは、ワークフローオーケストレーションを使用して、Windows または UNIX ベースのシステムおよび環境とやり取りし、データを取得できます。データを拡張することで、修正ライフサイクルを短縮できます。

ワークフローの編集またはカスタムワークフローの作成の詳細については、「Exploring flows」を参照してください。

脆弱性対応オーケストレーション のワークフローおよびアクティビティ

脆弱性対応オーケストレーション には多くのワークフローが付属しています。ワークフローとアクティビティにより、プロセスが自動化され、迅速化されます。ワークフローとアクティビティを使用して、スキャンレコードの作成、脆弱性一致アイテムのスキャンなどを行います。

脆弱性対応 - 脆弱性のスキャンワークフロー

単一または複数の脆弱性一致アイテムの脆弱性スキャンは、ベースシステムに含まれる [脆弱性対応] - [脆弱性のスキャン **(Scan Vulnerability)]** ワークフローアクティビティを使用して自動化できます。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

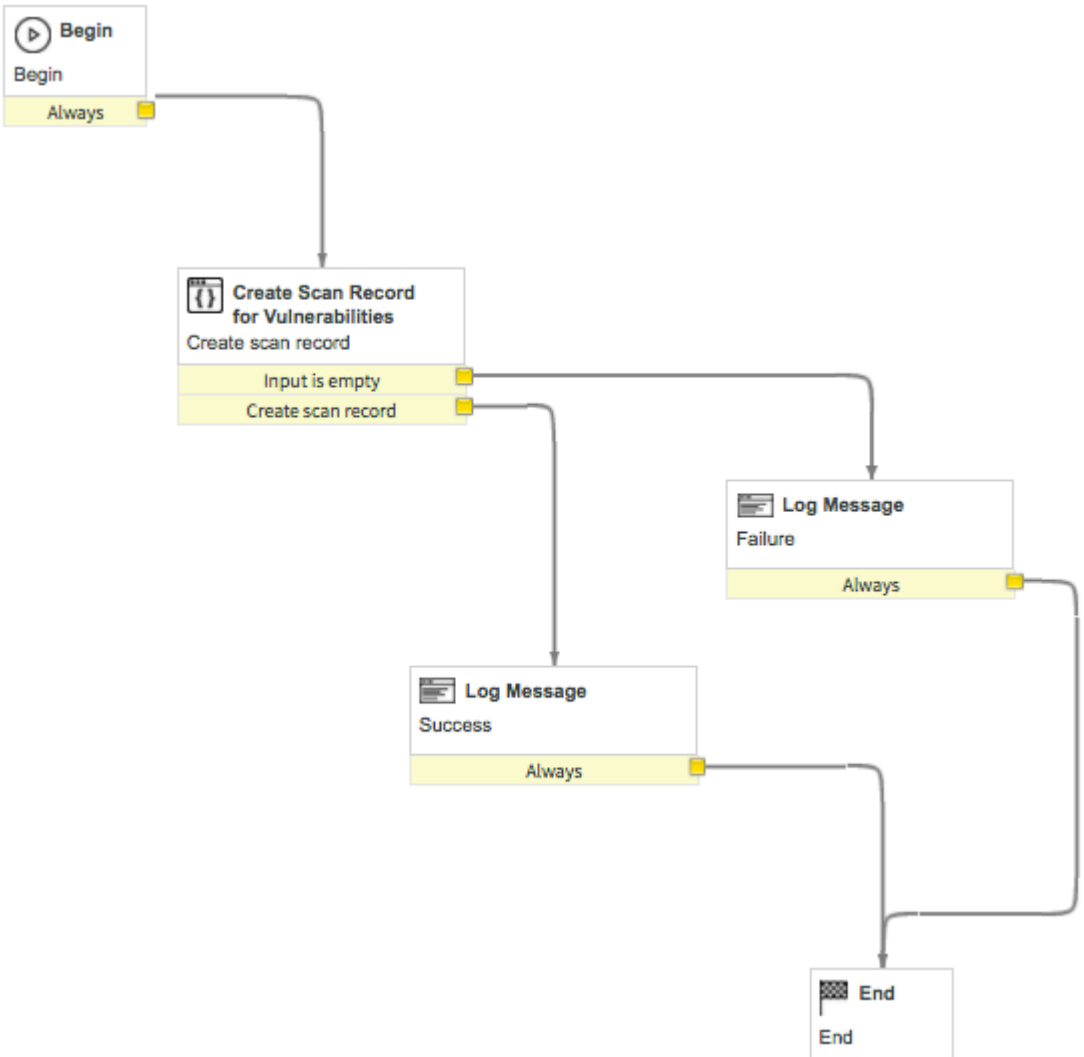
このタスクについて
[Vulnerability Response] - [脆弱性のスキャン **(Scan Vulnerability)]** ワークフローでは、呼び出し元の脆弱性または脆弱性のグループのスキャンレコードが作成されます。

注:

- 影響を受けるレコードに脆弱性パッチを適用した場合は、修正後に脆弱性または脆弱性一致アイテムを再スキャンすることをお勧めします。説明されている方法で再スキャンを実行することも、再スキャンを自動化することもできます。
- 脆弱性対応 v23.0 以降、[脆弱性対応 - 脆弱性のスキャン] ワークフローは廃止され、フローデザイナーの [脆弱性を再スキャン (Rescan Vulnerability)] フローに置き換わりました。

ワークフローアクティビティには、[脆弱性のスキャンレコードを作成] アクティビティの変数が含まれます

脆弱性対応 - 脆弱性のスキャンワークフロー



脆弱性のスキャンワークフロー

application 脆弱性対応 > 脆弱性をスキャン ワークフローは修復タスクを再スキャンします。

始める前に
必要なロール：なし

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

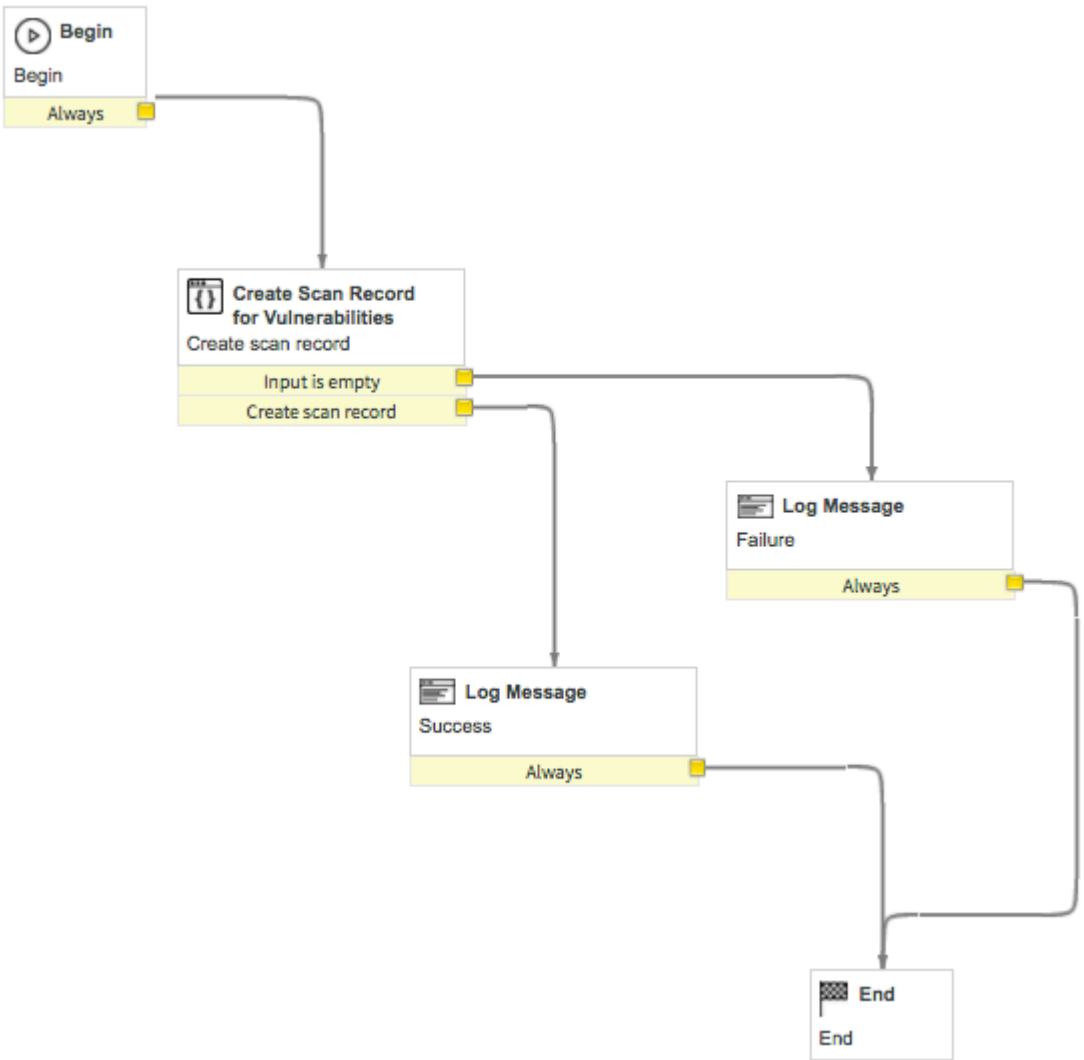
このタスクについて
このワークフローは、[クローズ/無視 **(Close/Ignore)]** アクション中に [脆弱性グループの再スキャン **(Rescan vulnerable group)]** によってトリガーされます。

ワークフロープロセスアクティビティには次のものが含まれます。

[脆弱性のスキャンレコードを作成] アクティビティの変数

ログメッセージ

脆弱性のスキャンワークフロー



手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 修復タスク.
2. タスクレコード (VUL) を開きます。
3. [クローズ] をクリックします。
4. [適切な状況] で [クローズ済み] を選択します。
5. [サブステータス] で [修正済み] を選択します。
6. [今すぐクローズしますか？] に対して [次のスキャンの確認を待機] を選択します。
   修復タスクと脆弱性一致アイテムについて、[ステータス] が [確認処理待ち] に、[サブステート] が [修正済み] に変わり、再スキャンが実行されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 - 脆弱性一致アイテムのスキャンワークフロー

単一または複数の脆弱性一致アイテムの脆弱性スキャンは、ベースシステムに含まれる 脆弱性対応 - 脆弱性一致アイテムのスキャンワークフローアクティビティを使用して自動化できます。

始める前に

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

このタスクについて

脆弱性対応 - 脆弱性一致アイテムのスキャンワークフローでは、呼び出し元の脆弱性一致アイテムまたはアイテムのグループのスキャンレコードが作成されます。

注:

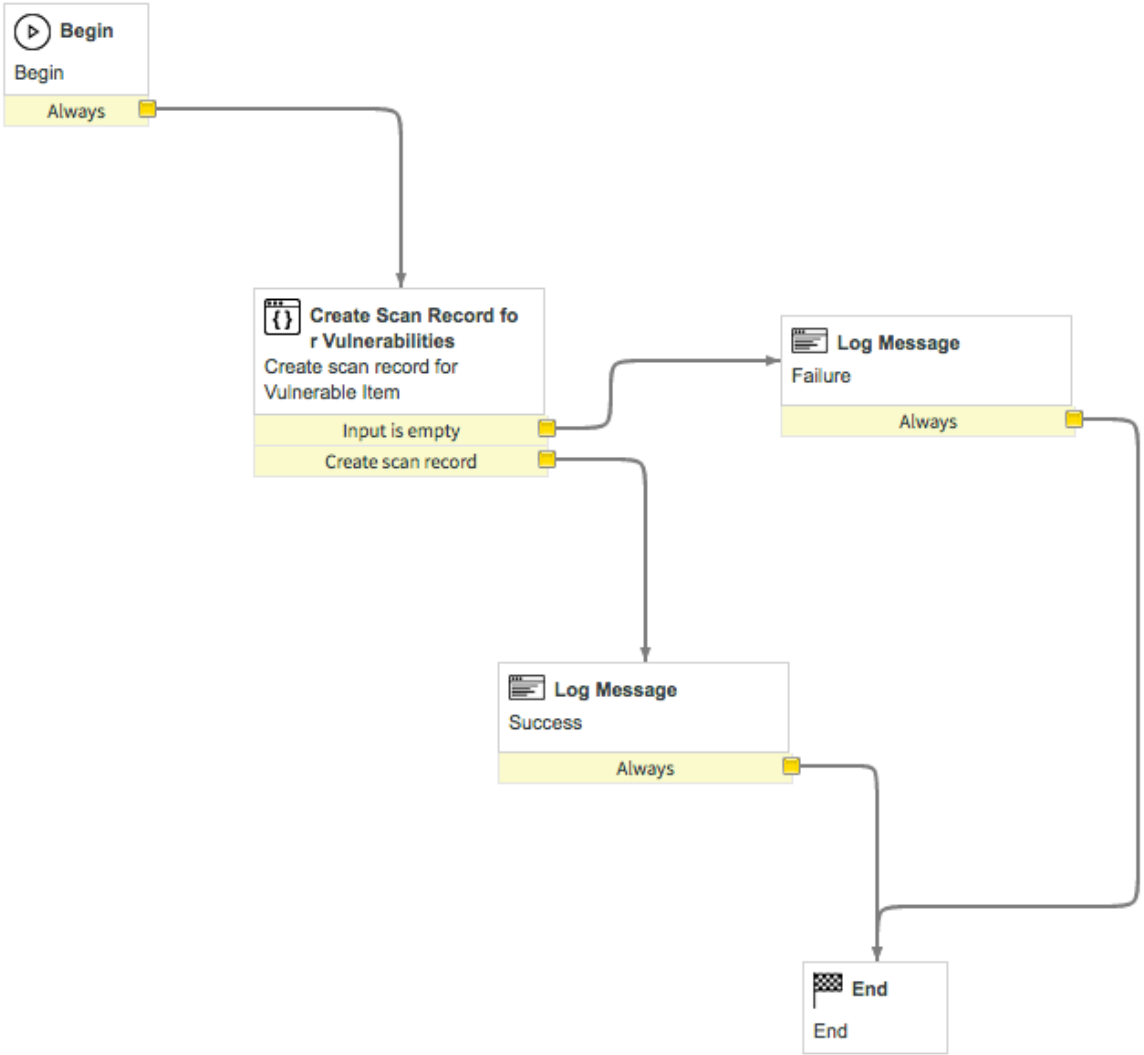
- 影響を受けるレコードに脆弱性パッチを適用した場合は、修正後に脆弱性または脆弱性一致アイテムを再スキャンすることをお勧めします。説明されている方法で再スキャンを実行することも、再スキャンを自動化することもできます。
- 脆弱性対応 v23.0 以降、[脆弱性対応 - 脆弱性一致アイテムのスキャン] ワークフローは廃止され、フローデザイナーの [脆弱性一致アイテムの再スキャン] フローに置き換わりました。

ワークフロープロセスアクティビティには、[脆弱性のスキャンレコードを作成] アクティビティの変数が含まれます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 - 脆弱性一致アイテムのスキャンワークフロー



脆弱性一致アイテムのスキャンワークフロー

application 脆弱性対応 > 脆弱性一致アイテムをスキャン ワークフローは脆弱性一致アイテムを再スキャンします。

始める前に

必要なロール：なし

このタスクについて

このワークフローは、[クローズ/無視 **(Close/Ignore)]** アクション中に [脆弱性を再スキャン] によってトリガーされます。

ワークフロープロセスアクティビティには次のものが含まれます。

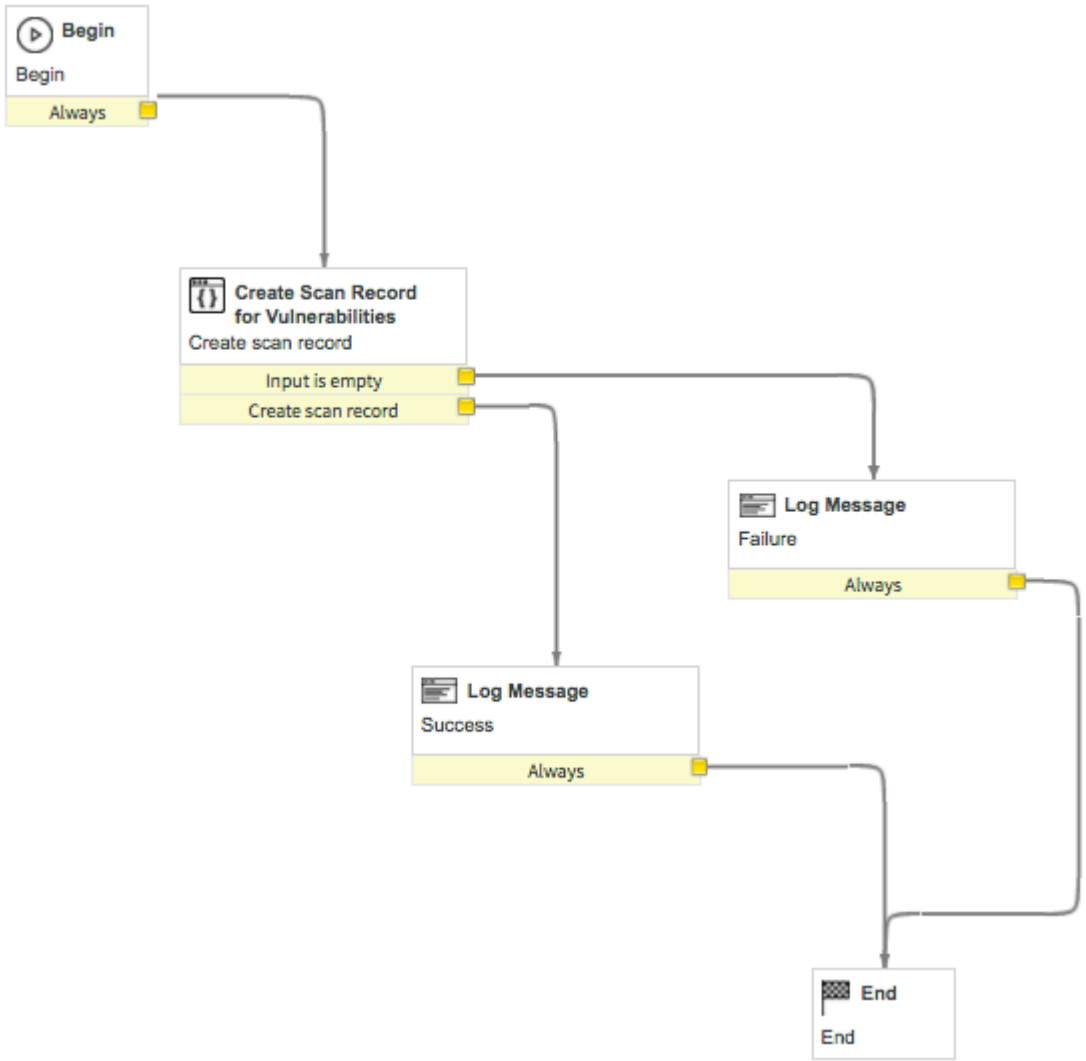
[脆弱性のスキャンレコードを作成] アクティビティの変数

ログメッセージ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性のスキャンワークフロー



自動翻訳

手順

1. 次のように移動する。 脆弱性 > 脆弱性 > 脆弱性一致アイテム.
2. 脆弱性一致アイテムを開きます。
3. [クローズ/無視 **(Close/Ignore)]** をクリックします。
4. [適切な状況] で [クローズ済み] を選択します。
5. [サブステータス] で [修正済み] を選択します。
   グループ変更の [ステータス] が [確認処理待ち] に、[サブステート] が [修正済み] に変わり、再スキャンが実行されます。

脆弱性対応オーケストレーションのワークフローアクティビティ

脆弱性対応オーケストレーションのアクティビティによって、ユーザーは、他のセキュリティインシデント、またはワークフローオーケストレーションを使用する他のシステムで過去に脆弱性が確認されたかどうかを判断できます。

[脆弱性のスキャンレコードを作成] アクティビティの変数

単一または複数の脆弱性一致アイテムの脆弱性スキャンは、ベースシステムに含まれる [脆弱性のスキャンレコードを作成] ワークフローアクティビティを使用して実行できます。入力がアクティビティに渡されると、スキャンレコードが作成されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

入力変数

変数	説明
taskids [文字列]	想定される入力を定義するカンマ区切りの sysIds の文字列。このフィールドは必須です。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
scanResult [ブーリアン]	入力が空でない場合は True を返します。taskIds のスキャンレコードが作成されます。

アプリケーション脆弱性対応

ServiceNow® 脆弱性対応アプリケーションのアプリケーション脆弱性対応 (AVR) 機能は、アプリケーション脆弱性一致アイテム (AVIT) をインポートし、ルールに従ってアプリケーションの脆弱性を修復できます。脆弱性対応は個別のサブスクリプションで利用できます。

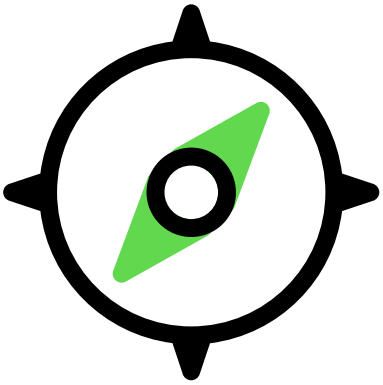
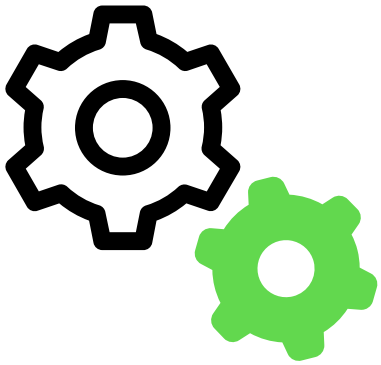
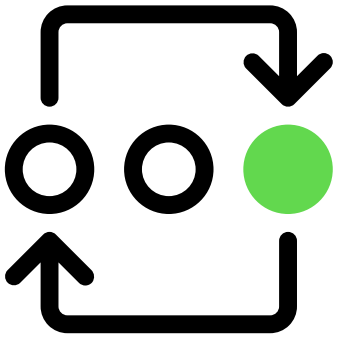
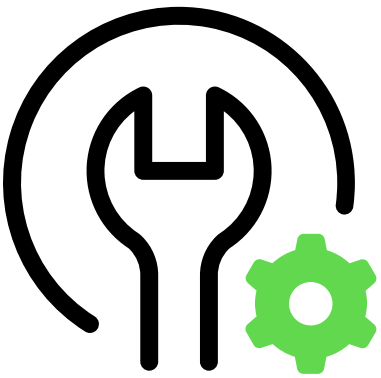
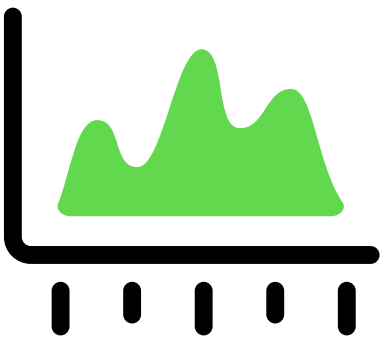
AVR v19.0 以降では、いくつかのキーテーブル名と列名が更新されています。その結果、ドキュメントには古い名前と新しい名前の両方への参照が表示されます。更新された用語の完全なリストについては、「アプリケーション脆弱性対応 製品ビュー」を参照してください。

脆弱性対応 の v19.0 以降では、ソフトウェアアプリケーションの脆弱性を特定するために、Software Composition Analysis (SCA) と Software Bill of Materials (SBOM) の脆弱性データを取り込むことができます。詳細については、「アプリケーション脆弱性対応 の詳細」と「Veracode 脆弱性統合」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション脆弱性対応

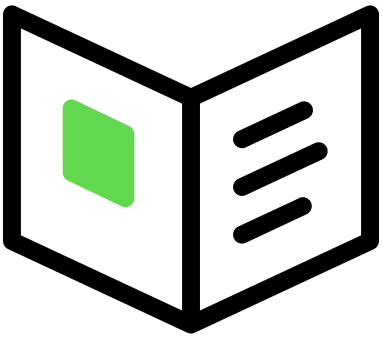
探索	構成	統合
		
Application Vulnerability Response の概念と機能について説明します。	Application Vulnerability Response を設定します。	他のアプリケーションと統合することで、Application Vulnerability Response を拡張します。
脆弱性対応ワークスペースの使用	修復	アナリティクスとレポート
		
脆弱性マネージャー、IT 修復、および脆弱性アセスメントのワークスペースで AVIT を監視、管理、および修復する方法について説明します。	アプリケーションの脆弱性を修復する方法について説明します。	Application Vulnerability Response 分析の表示

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション脆弱性対応 (続く)

Reference (参照)



フィールド、テーブル、プロパティなどのアプリケーション脆弱性対応コンポーネントの詳細を取得します。

トラブルシューティングとサポート

- セキュリティオペレーションリソースライブラリ
- セキュリティオペレーションコミュニティ
- 既知のエラーポータルで既知のエラー記事を検索する
- 連絡先 カスタマーサービス & サポート

アプリケーション脆弱性対応 の詳細

アプリケーションの脆弱性は、アプリケーションの開発ライフサイクル全体を通じてスキャンされるカスタムソフトウェアアプリケーションの脆弱性です。

アプリケーション脆弱性対応と利用可能なバージョン

アプリケーション脆弱性対応 (AVR) は、アプリケーションの脆弱性を処理する脆弱性対応アプリケーションの一部です。

利用可能バージョン

リリースバージョン	リリースノート
脆弱性対応 v23.0 脆弱性対応 v22.0 脆弱性対応 v21.0 脆弱性対応 v20.0	Application Vulnerability Response release notes 互換性情報については、「KB0856498 脆弱性対応互換性マトリクスおよびリ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

利用可能バージョン (続く)

リリースバージョン	リリースノート
脆弱性対応 v19.0 脆弱性対応 v18.2	リーススキーマの変更」を参照してください。

仕組み

脆弱性データは、共通脆弱性タイプ一覧 (CWE) やサードパーティの統合など、内部および外部のソースからインポートされます。データはインポート後に、構成管理データベース (CMDB) 内のアプリケーションデータと比較され、アプリケーション脆弱性対応 アプリケーションで処理されます。インポートされたアプリケーション脆弱性データと CMDB 内のデータが一致した場合、アプリケーション脆弱性一致アイテム (AVIT) が作成されます。

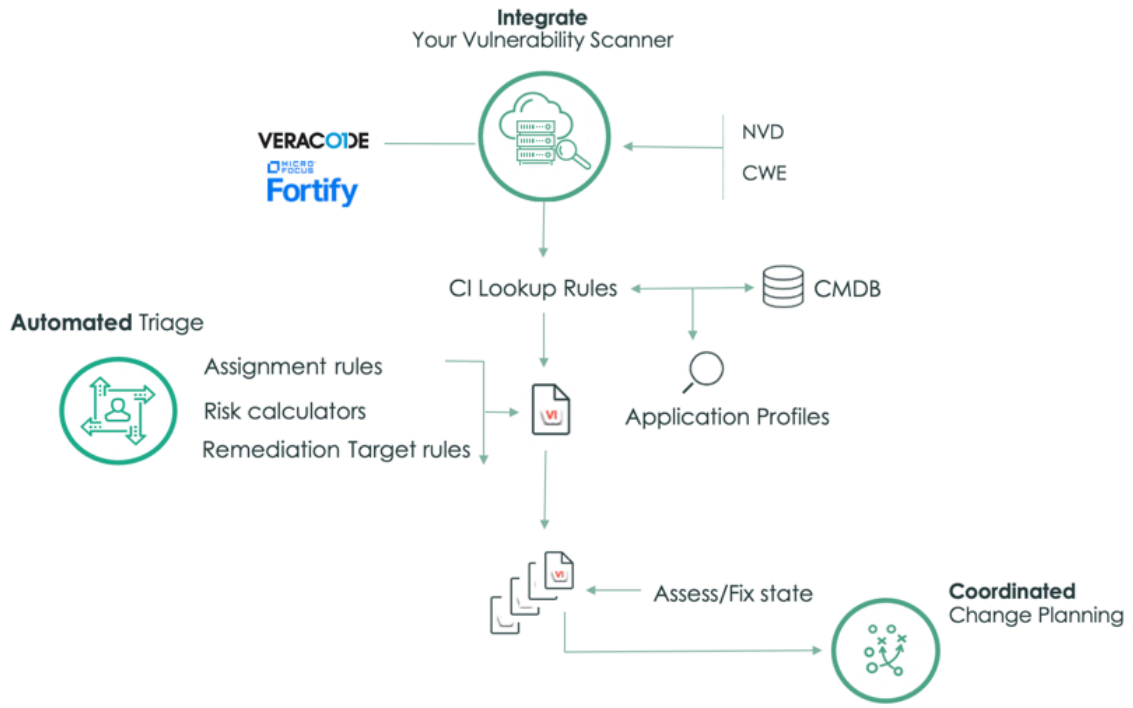
アプリケーション脆弱性対応 には、次の主要な機能が含まれています。

- サポートされているサードパーティのスキャナーと統合して、脆弱性データをインポートします。
- アプリケーション脆弱性関連データを比較して、アプリケーション内にアプリケーション脆弱性があるかが判断されます。
- アプリケーション脆弱性一致アイテム (AVIT) に優先順位を付け、修復し、管理します。各アプリケーション脆弱性は、CWE またはサードパーティライブラリ内の脆弱性エントリーを表します。
- 脆弱性対応のバージョン 18.0 以降では、Vulnerability Manager ワークスペース および IT 修復ワークスペースの AVIT をそれぞれ監視および修復できます。詳細については、「Vulnerability Manager ワークスペース」と「IT 修復ワークスペース」を参照してください。
- 計算ツールとライブラリを使用して アプリケーション脆弱性対応 データを関連付けると、次のタスクの実行に役立ちます。
  - **[CI** ルックアップルール] を使用してアプリケーション脆弱性一致アイテムを自動的に作成します。インポート時に、サードパーティの脆弱性が CWE に関連付けられ、AVIT が作成されます。
  - アサインルールを作成して、アプリケーション脆弱性一致アイテムのアサインを自動化します。
  - 計算ツールのグループを使用して、ビジネスインパクトを判断したり、フィルターを使用してさまざまな条件を指定したり、簡単な計算を適用したり、スクリプトを使用したりします。
  - 今後の修復アクティビティを監視できるように、アプリケーション脆弱性一致アイテムの修復予定期間を定義する修復ターゲットルールを作成します。
- 単一のサードパーティ脆弱性を複数の CWE エントリーに関連付け、リスクの判断に役立てるために脆弱性に関するプライマリ CWE を見つけます。[プライマリ **CWE]** の詳細については、「[アプリケーション脆弱性] フィールド」を参照してください。
- CWE データベースからダウンロードされた CWE レコード、またはサードパーティ統合からインポートされた CWE レコードを参照として使用して、脆弱性をエスカレートする必要があるかどうかを判断します。各 CWE レコードには、脆弱性を説明する関連するナレッジ記事も含まれています。

アプリケーション脆弱性対応 を使用して、統合から調査、解決までの情報のフローをたどります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



インポートされた脆弱性データのタイプ

アプリケーション脆弱性対応 は、次のタイプのインポートされたアプリケーション脆弱性データをサポートしています。

注:
v19.0 より前では、SAST、SCA、IAST、およびペネトレーションテストデータは取り込まれなかったため、Veracode、Fortify、Invicti 内に表示されるものとアプリケーション脆弱性対応に表示されるものとの間に違いが生じる場合がありました。

動的アプリケーションセキュリティテスト (DAST)

DAST スキャンは、アプリケーションに入力を送信し、実行中にその応答を監視することによって、脆弱性アプリケーションを検出します。このアプローチは、外部からの攻撃を模倣する可能性があります。動的スキャンでは、実行中のサービス (URL) の脆弱性がスキャンされます。脆弱性の結果には、検出された脆弱性の URL の場所が含まれています。

静的アプリケーションセキュリティテスト (SAST)

SAST スキャンは、保存中のアプリケーションのソースコードを確認し、コードの記述方法の脆弱性を見つけるのに役立ちます。SAST スキャンはコンパイルされていないソースコードに対して行われるため、アプリケーションサービスから独立して存在します。返される結果には、検出された脆弱性のファイルと行番号の場所が含まれます。

インタラクティブアプリケーションセキュリティテスト (IAST)

IAST スキャンは、プログラムの実行中にプログラムと対話することにより、ソフトウェアの脆弱性を検出します。人間による観察、自動テスト、およびセンサーを組み合わせて使用し、アプリケーションと対話して脆弱性を特定します。

ソフトウェア構成分析 (SCA)

脆弱性対応の v19.0 以降では、ソフトウェア構成分析 (SCA) の脆弱性を取り込むことができます。ソフトウェアアプリケーションで使用されているオープンソースソフトウェアの弱点を特定するのに役立つ SCA 脆弱性データ。

ペネトレーションテスト

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

アプリケーション脆弱性対応でペネトレーションテストアセスメント要求を構成すると、アプリケーションの弱点がどこにあり、その弱点を修正するために何ができるかを理解できるようになります。

ソフトウェア部品表

ソフトウェア部品表 (SBOM) データをアップロードして、オープンソースコンポーネントの脆弱性を特定します。詳細については、「ソフトウェア部品表 の詳細」を参照してください。

ユースケース

次のようないくつかの DAST ユースケースがサポートされています。

- スキャン結果の各脆弱性を何らかの cmdb_ci (子クラス) に関連付けます。
- ディスカバリー またはサードパーティ統合により CMDB にレコードが存在する場合、DAST スキャン結果を既存のアプリケーションに関連付けます。
- 新しいアプリケーションの識別や CMDB への格納が完了していない場合、DAST スキャン結果を新たに挿入されたスキャン済みアプリケーションに関連付けます。
- ServiceNow® 以外の製品でアプリケーションを管理する場合は、CMDB に対する DAST スキャン結果を保存します。
- 以前に他の目的でカスタマイズした場合は、CMDB に対する DAST スキャン結果を保存します。
- ソースコードリポジトリ用のアプリケーションを手動で作成します。

次のようないくつかの SAST ユースケースがサポートされています。

- スキャン結果の各脆弱性を何らかの cmdb_ci (子クラス) に関連付けます。
- ソースコードリポジトリ用の CI を手動で作成します。
- 関連するアプリケーションサービスのない SAST スキャン結果を保存します。

[store-future: BEGIN review]次のようないくつかの IAST ユースケースがサポートされています。[End]

[store-future: BEGIN review]次のようないくつかの SCA ユースケースがサポートされています。[End]

サードパーティ統合

アプリケーション脆弱性対応でサポートされているサードパーティ統合は、ServiceNow Store で個別のアプリケーションとして入手できます。詳細については、「他のアプリケーションとの アプリケーション脆弱性対応 の統合」を参照してください。

主な機能

- 共有 API は、DAST、SAST、IAST、SCA データ、および手動ペネトレーションテスト結果をインポートします。「ペネトレーションテスト」を参照してください。
- SBOM データのインポートには、別の API が使用されます。詳細については、「ソフトウェア部品表 の詳細」と「Veracode 脆弱性統合」を参照してください。

CI ルックアップルール

構成管理データベース (CMDB) で一致するアプリケーションデータを自動的に検索します。

アサインルール

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ユーザーグループ、ユーザーグループフィールド、およびスクリプトに基づいて、アプリケーションの脆弱性を自動的にアサインします。

リスク算出

条件フィルターを使用して、任意の条件に基づいて、算出を使用して AVIT の影響度を自動的に優先順位付けして評価します。

重大度マッピング

アプリケーション脆弱性一致アイテムのフィールドの初期値を自動的に計算します。脆弱性エントリーには、ソース重大度と正規化された重大度 (重大度マッピングに基づく) の両方があります。重大度は、 共通脆弱性タイプ一覧 (CWE) に関連付けられています。

修復ターゲットルール

アプリケーション脆弱性一致アイテムの修復予定期間を定義します。

レポート

セキュリティ体制、修復の傾向、最も重要な AVIT を含むアプリケーションまたは事業部門の上位 10 件を迅速に把握することができます。

両方のタイプのスキャンの共通点は、アプリケーションのリリースです。[名前] 文字列を定義するアプリケーションリリースは、スキャナー側でスキャンされた脆弱性結果をグループ化するための紐付けポイントになります。このようにして、AVR は、統合を通じてスキャン結果をインポートするときに、結果が属するアプリケーションリリースを認識します。

脆弱性対応 アプリケーションとスコープに、構成アイテム [cmdb_ci] 子テーブル、スキャン済みアプリケーション [sn_vul_app_scanned_application] が作成されました。このテーブルには、アプリケーションリリースの抽象化が保存され、CMDB 関係を通じてサービスのグラフ化が提供されます。これらは、 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > アプリケーション 移動しますスキャン済みアプリケーションのリストビューには、セットアップ中に追加された [部門] と [サポートグループ] が含まれています。

アプリケーション脆弱性一致アイテム (AVIT)

アプリケーション脆弱性の場合、AVR は脆弱性をアプリケーションに関連付けてアプリケーション脆弱性一致アイテム (AVIT) レコードを作成します。CMDB 内のアプリケーションの構成要素は複数定義されているため、アプリケーション脆弱性対応 ではアプリケーションをスキャン済みアプリケーションに限定しています。スキャン済みアプリケーションは、AVR によって [名前] および **[ID]** として識別された環境でスキャンされたアプリケーションです。スキャナーによって [修復済み **(Fixed)]** が確認されるまで、AVIT は最新のスキャンサマリーに基づいています。AVIT が見つからなくなった場合は、最後に確認されたスキャンサマリーに関連付けられたままになります。

アプリケーション脆弱性一致アイテムは、次から表示できます。 **All** (すべて) > アプリケーション脆弱性対応 > 脆弱性 > 脆弱性一致アイテム 移動します

アプリケーションが CMDB から削除されると、関連付けられている AVIT が閉じます。

AVIT フォームフィールドの詳細については、「[アプリケーション脆弱性一致アイテム] フィールド」を参照してください。

アプリケーション脆弱性対応 のユーザーグループとロール

多くの場合、チームは連携してアプリケーションの脆弱性を作成、管理、および監視します。チームの中には、戦略的ロールのメンバーと運用ロールのメンバーがいます。ほとんどの組織では、複数のロールに参加し、他者とユーザーロールを共有することもよくあります。アプリケーション脆弱性対応 では、詳細なロールを含む 3 つのユーザーグループ (App-Sec マネージャー、アプリケーションセキュリティチャンピオン、および開発者) を使用します。これらのグループとロールの詳細については、「アプリケーション脆弱性対応 のユーザーロールおよびロール」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

アプリケーション脆弱性対応 のステータス

アプリケーション脆弱性対応は、アプリケーション脆弱性一致アイテム (AVIT) の状態を示す状況モデルを提供し、AVIT をいつどのように修復するかを決定するのに役立ちます。

アプリケーション脆弱性一致アイテムはいくつかの状況を想定しています。詳細については、「アプリケーション脆弱性一致アイテム (AVI) の状況」を参照してください。

アプリケーション脆弱性対応 の構成

Now Platform インスタンスで アプリケーション脆弱性対応 を実行する場合は、事前に構成する必要があります。

アプリケーション脆弱性対応 の構成

確実に構成を実行できるように、構成の前に次のセットアップ手順を実行します。

始める前に

セットアップタスク	説明
脆弱性対応 アプリケーションがインストールされ、アクティブ化されていることを確認します。	アクティブ化されていることを確認するには、サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応 のインストール」を参照してください。
アプリケーション脆弱性対応 レポートを表示するために、脆弱性対応のパフォーマンスアナリティクス がインストールされ、アクティブ化されていることを確認します。	アクティブ化されていることを確認するには、サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応のパフォーマンスアナリティクス [PA] アプリケーションのインストールと構成」を参照してください。
Veracode 脆弱性統合 がインストールされ、アクティブ化され、設定されていることを確認します。(この時点では統合を実行しないでください。)	アクティブ化されていることを確認するには、サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「ServiceNow Vulnerability Response Integration with Veracode のインストール」を参照してください。
バージョン 14.0：Fortify 脆弱性統合 がインストールされ、アクティブ化され、設定されていることを確認します。(この時点では統合を実行しないでください。)	アクティブ化されていることを確認するには、サブスクリプション管理 > サブスクリプション

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「ServiceNow Vulnerability Response Integration with Fortify のインストール」と「Fortify 脆弱性統合 の構成」を参照してください。
脆弱性対応 で CWE 2000 統合が実行されていることを確認します。	統合を確認するには、「NVD レコードの更新を行うスケジュール済みジョブが実行されていることを確認する」を参照してください。
[オプション] 脆弱性対応 で NVD 統合が実行されていることを確認します。	確認するには、「CWE レコードの更新を行うスケジュール済みジョブが実行されていることを確認する」を参照してください。
インスタンスに必要な ServiceNow ロールがあることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。 • まだアサインされていない場合、admin ロールを持つユーザーはアプリケーションをインストールして、ユーザーをアプリセキュリティマネージャー、セキュリティチャンピオン、および開発者のユーザーグループにアサインします。グループロールの詳細については、「アプリケーション脆弱性対応 のユーザーロールおよびロール」を参照してください。 • アプリセキュリティマネージャーグループは構成を監督し、期待される結果を検証します。 **注:** アプリケーション脆弱性対応 構成は、脆弱性対応 のセットアップアシスタント機能からは利用できません。

必要なロール：アプリセキュリティマネージャーユーザーグループ

手順

1. 次のように移動する。 セキュリティオペレーション > **CMDB** > ルックアップルール.
   自分の環境に対する CI ルックアップルールを作成または変更するには、「CI ルックアップルールを作成する」を参照してください。
2. 次のように移動する。 アプリケーション脆弱性対応 > アドミニストレーション.
3. [アサインルール] を選択します。
   自分の環境に対するアプリケーションアサインルールを作成または変更するには、「アプリケーション脆弱性対応 アサインルールの作成または編集」を参照してください。
4. [脆弱性算出] を選択します。
   自分の環境に対するアプリケーション脆弱性算出を作成または変更するには、「アプリケーション脆弱性対応 のリスクを自動的に計算する」を参照してください。
5. [修復ターゲットルール] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自分の環境に対するアプリケーション修復ターゲットを作成または変更するには、「アプリケーション修復ターゲットルールの作成または編集」を参照してください。

6. [正規化された重大度マップ] を選択します。
自分の環境に対する重大度マップを作成または変更するには、「アプリケーション脆弱性一致アイテムの重大度を自動的にマッピングする」を参照してください。
7. 次のいずれかに移動します。 **Veracode** 脆弱性統合 > 統合 または **Fortify** 脆弱性統合 > 統合.
8. Veracode アプリケーションリスト統合または Fortify オンデマンドアプリケーションリスト統合を開きます。
9. まだ実行していない場合は、[今すぐ実行] を選択します。

   注:
   他の Veracode または Fortify 統合はデフォルトで非アクティブになっています。

   統合実行状況については、「Veracode アプリケーション脆弱性統合のインポート実行状況の表示」または「Fortify 脆弱性統合 インポート実行状況の表示」を参照してください。
10. Veracode または Fortify オンデマンドアプリケーションリスト統合の実行が完了したら、 アプリケーション脆弱性対応 > アドミニストレーション > アプリケーション.
11. アプリケーションごとに、[サポートグループ] (アサインルールで使用) と [部門] (レポートで使用) の値を入力します。
複数のエントリーを更新するには、「Edit multiple records in a list using the list editor (リストエディターを使用してリスト内の複数のレコードを編集)」を参照し、タスクを一括で完了します。

    注:
    自動更新された [事業部門] を表示するには、ページをリフレッシュします。[スキャン済みアプリケーション] フォームフィールドについては、「スキャン済みアプリケーションファイル」を参照してください。

12. 統合リストに戻り、他の Veracode または Fortify の統合をアクティブ化します。
デルタデータ統合インポートを設定するには、「アプリケーション脆弱性対応 統合のアクティブ化」を参照してください。

    Veracode および Fortify の統合は連結されており、アクティブ化すると連続して実行されます。
13. オプション: 次のように移動する。 アプリケーション脆弱性対応 > アドミニストレーション > アサインルール.

    a. オプション: 事前にアサインルールを作成または編集するときに、[ユーザーグループフィールド] で [構成アイテム：サポートグループ] を選択した場合、 [スキャン済みアプリケーション] リストビューに追加した値を使用できるようになります。
    アサインルールが編集されます。

    b. [更新] を選択します。

    c. [脆弱性アサインルール] リストビューで、[変更を適用 **(Apply Changes)]** を選択して AVI にアサインルールを再適用します。

タスクの結果
これで、アプリケーション脆弱性対応 構成が完了しました。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のタスク
次のように移動する。 アプリケーション脆弱性対応 > 概要 および アプリケーション脆弱性管理 (PA) ダッシュボード で全体的なセキュリティ体制に関する情報を確認してください。

CWE レコードの更新を行うスケジュール済みジョブが実行されていることを確認する

脆弱性をエスカレートする必要があるかどうかを決定するときは、共通脆弱性タイプ一覧 (CWE) データベースからダウンロードした CWE レコードを参照用に使用します。定期的に共通脆弱性タイプ一覧データベースから共通の脆弱性レコードを更新します。必要に応じて、デフォルトのスクリプトを更新するか、独自のスクリプトを作成することもできます。

始める前に
必要なロール：アプリセキュリティマネージャーグループ
各 CWE レコードには、脆弱性を説明する関連するナレッジ記事も含まれています。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > 統合.
2. **[CWE Comprehensive 2000** 統合 **(CWE Comprehensive 2000 Integration)]** スケジュール済みジョブを選択します。
3. [アクティブ] チェックボックスが選択されていることを確認します。

   注:
   このフォームの設定は 脆弱性対応 と アプリケーション脆弱性対応 で共有されます。統合の設定を変更するには、脆弱性対応 および ServiceNow との調整と専門知識が必要です。

4. ボックスが選択されている場合は、これで完了です。

   注:
   ボックスが選択されていない場合は、脆弱性対応 内でこの統合を設定する必要があります。詳細については、選択する前に「NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理」を参照してください。

   必要に応じて、脆弱性ライブラリの表示 を参照してインポートされたエントリーを確認します。

   [プライマリ **CWE]** フィールドには CWE エントリーが含まれています。脆弱性に関連付けられている CWE が複数ある場合、プライマリ CWE を決定する方法については「[アプリケーション脆弱性] フィールド」を参照してください。

NVD レコードの更新を行うスケジュール済みジョブが実行されていることを確認する

定期的に更新するリポジトリを識別します。スケジュール済みジョブを実行して、脆弱性情報データベース (NVD) レコードを夜間または毎週更新できます。まだ実行していない場合は、ジョブを有効にできます。

始める前に
必要なロール：アプリセキュリティマネージャーグループ

デフォルトでは、NVD 統合は毎週月曜日 00:00:00 にスケジュール済みジョブとして実行されます。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > 統合.
2. **[NIST National Vulnerability Database]** スケジュール済みジョブを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [アクティブ] チェックボックスが選択されていることを確認します。

   注:
   このフォームの設定は 脆弱性対応 と アプリケーション脆弱性対応 で共有されます。統合の設定を変更するには、脆弱性対応 および ServiceNow との調整と専門知識が必要です。

4. ボックスが選択されている場合は、これで完了です。

   注:
   ボックスが選択されていない場合は、脆弱性対応 内でこの統合を設定する必要があります。詳細については、選択する前に「NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理」を参照してください。

必要に応じて、脆弱性ライブラリの表示 を参照してインポートされたエントリーを確認します。

アプリケーション脆弱性対応 統合のアクティブ化

アプリケーション脆弱性対応 統合を有効にして、定期的な更新を実行します。

始める前に
必要なロール：アプリケーションセキュリティマネージャー

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > 統合.
2. 統合を選択します。
3. [アクティブ] チェックボックスをオンにします。
4. [更新] を選択します。
5. 必要に応じて、統合ごとに繰り返します。
   最初の実行後、統合を連結させて、後続の実行のためのデルタインポートを行います。

アプリケーション脆弱性対応 メール通知を定義する

メール通知を設定して、誤検出要求の承認や却下など、重要な更新やアクティビティに関する有用な情報を共有します。メール通知を作成するときに、送信時期、受信者、内容を指定できます。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > メールテンプレート.
2. **[New** (新規)] を選択します。

   メール通知を作成するための詳細な手順については、「Create an email notification」を参照してください。

タスクの結果
脆弱性対応 の v21.0 以降の場合、受信者がメール通知のリンクをクリックすると、そのロールに応じてレコードは Vulnerability Manager ワークスペース または IT 修復ワークスペース で開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- sn_vul.app_sec_manager のロールを持つユーザーのリンクは Vulnerability Manager ワークスペース で開きます。
- IT 修復ワークスペース で次のロールを持つユーザーに対してリンクが開きます：sn_vul.app_security_champion、または sn_vul.app_developer。

受信者に前述のいずれのロールもない場合は、メール通知のリンクがクラシック UI で開きます。

アプリケーション脆弱性対応で修復ターゲット通知を作成または編集する

脆弱性アドミニストレーターは、修復ターゲット通知を編集するか、新しい通知を追加して、通知の送信タイミング、通知の受信者、通知の内容を指定できます。

始める前に

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 通知.
2. 修復ターゲットの通知レコードを選択するか、[新規] を選択します。
3. 必要に応じて、フォームのフィールドに入力します。
   フォームフィールドの詳細については、「Create an email notification」を参照してください。
4. [通知をプレビュー] を選択してメッセージを表示します。

タスクの結果

脆弱性対応の v21.0 以降の場合、受信者がメール通知のリンクをクリックすると、そのロールに応じてレコードは Vulnerability Manager ワークスペース または IT 修復ワークスペースで開きます。

- sn_vul.app_sec_manager のロールを持つユーザーのリンクは Vulnerability Manager ワークスペース で開きます。
- IT 修復ワークスペース で次のロールを持つユーザーに対してリンクが開きます：sn_vul.app_security_champion、または sn_vul.app_developer。

受信者に前述のいずれのロールもない場合は、メール通知のリンクがクラシック UI で開きます。

アプリケーション脆弱性対応 の例外管理

組織が公開されている脆弱性管理またはセキュリティ方針、規格、指針に準拠できない場合、例外を要求できます。例外管理では、ポリシーに従って修復できないアプリケーション脆弱性一致アイテム (AVIT) に対する例外を要求、レビュー、承認、または却下します。

一部の脆弱性には、既存のパッチ、修正、またはソリューションがない可能性があります。例外が承認されるということは、脆弱性を修復しなかった場合の結果を認識し、同意していることになるため、リスクを受け入れているということでもあるのです。

注:

アプリケーション脆弱性対応 の v21.0 以降では、誤検出と例外を承認する期間を設定できます。また、設定した日数経過後の承認者と要求者の両方に対するメール通知も可能です。要求が発生すると、アプリケーション脆弱性一致アイテムが [レビュー中] ステータスに変わり、ステータス変更レコードが作成されます。構成された期間内に承認者が応答しない場合、アプリケーション脆弱性一致アイテムまたは修復タスクは [オープン] ステータスに戻ります。以前のステータスは **[backup_state]** フィールドに保存されます。詳細については、「例外管理の承認ルールの構成」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

例外のライフサイクル

例外の定義

例外は、AVI の修復を指定した期間保留することを要求するものです。たとえば、マシンにパッチが適用されない場合に、開発者が例外を要求できます。

例外の要求

開発者は、例外管理プロセスを使用して AVI の免除を要求できます。アプリケーションセキュリティアナリストがこの要求を承認すると、AVI は [保留] ステータスに移行します。

> **重要:**
> AVTI と RT の例外は、それぞれ脆弱性マネージャーワークスペースと IT 修復ワークスペースから要求できます。詳細については、「で修復タスクとレコードの例外を要求する Vulnerability Manager ワークスペース」と「IT 修復ワークスペースで例外を要求する」を参照してください。

例外ルール

v20 以降では、ルールの条件に一致する場合に、既存および新規のアプリケーション脆弱性一致アイテム (AVI) を特定の期間、自動的に保留する例外ルールを作成できます。例外ルールを使用して AVI を自動的に保留することで、サービスレベルアグリーメントの達成を逃すリスクを最小限に抑えることができます。ルールを使用すると手動での操作を省くことができるので、複数のアイテムを管理できるようになります。「例外ルールを作成する」を参照してください。

例外ルールの延長の要求

v20 以降、例外ルールの [保留期限] 日付の延長の要求を送信できます。修復タスクが新しい AVI の受け入れを停止する [保留期限] 日までに、ルールによって作成された多数のレコードが解決されないとわかった場合には、ルールの延長を要求できます。この延長によって例外ルールが更新されるため、既存のルールの保留日が自動的に延長されます。現在の日付から最大 1 年前までの日付を入力でき、延長の理由を含める必要があります。延長要求には、別々の承認グループからの 2 レベルの承認が必要です。

例外要求を承認する

すぐに修復できない AVIT は、アプリケーションセキュリティアナリストによってレビューされ、リスクが評価され、修復できるまでの保留が承認されます。例外要求の承認は 2 レベルフローにできます。第 1 レベルの承認者のみが存在する場合、例外を要求して承認できます。ただし、第 1 レベルの承認者がいない場合は、例外を要求できません。詳細については、「アプリケーション脆弱性対応 の例外承認者を追加する」を参照してください。

> **重要:**
> 脆弱性マネージャーワークスペースで例外要求を承認または却下できます。詳細については、「Vulnerability Manager ワークスペース で要求を承認または却下」を参照してください。

注:

AVIT の例外要求が承認されると、次のアクションを実行できます。

- 再オープン
- 詳細の取得

例外要求の追跡

例外が発生した後、AVIT の [ステータス変更承認] タブを使用してそのステータスを追跡できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

例外要求の有効期限と例外ルールの延長の要求

特定の AVI の例外要求が期限切れになると、影響を受ける AVI は [オープン] 状態に戻ります。

ただし、v20 以降では、例外ルールの [保留期限] の日付を延長する要求を送信できます。

アプリケーション脆弱性対応 の例外管理の設定

モジュールを使用して、要求された例外の期間を制限し、例外要求または誤検出要求にアンケートを追加します。デフォルトでは、 ServiceNow　アプリケーション脆弱性対応 モジュールを使用して例外が要求されます。GRC: ポリシーとコンプライアンス管理 の統合を使用して例外を要求することもできます。

始める前に

必要なロール：sn_vul.app_manage_exception_configuration

このタスクについて

脆弱性対応 が有効であれば、例外を要求できる期間を制限できます。同様に、GRC: ポリシーとコンプライアンス管理 モジュールがインストールされていれば、構成画面で GRC: ポリシーとコンプライアンス管理 を選択できます。このオプションを有効にすると、GRC からポリシーおよびコントロール目標を指定する例外を要求できます。

アンケートを追加すると、例外要求または誤検出要求を出しているユーザーにアンケートが送信されます。デフォルトのアンケートを使用することも、要件に基づいて作成することも可能です。

アンケートは、例外が要求されている理由を例外承認者が理解する際に役立ちます。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > 例外管理.
2. [例外管理構成] フォームで、[例外の管理に使用] リストからオプションを選択して、例外を管理する方法を選択します。

   注:
   脆弱性対応 バージョン 17.1 以降では、脆弱性対応 または GRC: ポリシーとコンプライアンス管理 のいずれかを選択できます。GRC: ポリシーとコンプライアンス管理 を使用して例外を要求するには、GRC プラグインをアクティブ化する必要があります。構成を変更しても、既存のデータには影響しません。

3. 選択したオプションに基づいて、フォームのフィールドに入力します。
   - 脆弱性対応 オプションを選択した場合は、フォームのフィールドに入力します。

VR 例外管理フォームの設定

フィールド	説明
期間	例外を要求できる期間。
単位	指定された期間の時間単位。
例外を要求するアンケートを有効化	上がっている例外要求にアンケートを追加するオプション。
例外を要求するアンケート	例外を要求するために自分が選択したアンケートを表示するオプション。デフォルトでは、[例外のアンケート] が表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
誤検出をマークするアンケートを有効化	上がっている誤検出要求にアンケートを追加するオプション。
誤検出をマークするアンケート	誤検出としてマークするために自分が選択したアンケートを表示するオプション。デフォルトでは、誤検出要求のアンケートが表示されます。

- GRC: ポリシーとコンプライアンス管理 オプションを選択した場合は、フォームのフィールドに入力します。

VR 例外管理フォームの設定

フィールド	説明
誤検出をマークするアンケートを有効化	上がっている誤検出要求にアンケートを追加するオプション。
誤検出をマークするアンケート	誤検出としてマークするために自分が選択したアンケートを表示するオプション。デフォルトでは、誤検出要求のアンケートが表示されます。

4. [保存] を選択します。

例外管理の承認ルールの構成

アプリケーション脆弱性対応 v15.0 以降では、フローデザイナーを使用して、例外管理、例外ルール、および誤検出管理の例外要求を承認します。アプリケーション脆弱性対応 (AVR) を初めて展開した場合、フローデザイナーはデフォルトで有効になっています。

始める前に
必要なロール：sn_vul.vulnerability_admin

このタスクについて
既存の VR ユーザーの場合、デフォルトのオプションはワークフローです。
アプリケーション脆弱性対応 v15.0 以降を展開した場合、システムプロパティ *sn_vul.flow_designer_activation* の値は true に設定されます。つまり、フローデザイナーはデフォルトで有効になっています。

v15.0 より前の アプリケーション脆弱性対応 を既に使用している場合、このシステムプロパティの値は false に設定されます。値を true に変更すると、フローデザイナーをアクティブ化できます。

注:
フローデザイナーをアクティブ化した後、 ワークフローの使用に戻すことはできません。ワークフローとフローデザイナーの詳細な比較については、「例外管理ワークフローとフローデザイナー」を参照してください。

フローデザイナーを使用するには、 承認ルールモジュールを使用してルールを作成します。このモジュールを使用すると、以下の各例外管理ワークフローの承認ルールを構成できます。

- 修復タスクの要求例外
- アプリケーション脆弱性一致アイテムの例外要求
- 例外ルール

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 修復タスクの誤検出
- アプリケーション脆弱性一致アイテムの誤検出

> **注:**
> ルール内に複数の承認レベルを含む条件を定義することもできます。フローデザイナーは、このモジュールで作成されたルールを自動的に継承し、一致する承認ワークフローを処理します。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > 承認ルール.
2. [承認ルール] ページで、承認ルールを設定するグループを選択します。
3. フォームのフィールドに入力します。

承認ルールフォーム

フィールド	説明
名前	承認構成名。
テーブル	ルールが適用されるテーブル。
アプリケーション	デフォルト値は脆弱性対応です。
ルールタイプ	ルールタイプを指定します。たとえば、例外管理、誤検出、例外ルールなどです。
有効	デフォルトで有効になっており、承認ルールが使用中であることを示します。
説明	承認ルールの簡単な説明。
承認の有効期限 (日数) アプリケーション脆弱性対応 の v21.0 以降	承認者が要求を承認できる期限。
承認者に通知 (日数) アプリケーション脆弱性対応 の v21.0 以降	承認者にアクションを実行するよう通知される日付。

4. [更新] を選択します。
   [承認構成] タブには、デフォルトで 2 つのレベルの承認者が設定されています。ルールを選択して、ルール内のさまざまなユースケースに基づいて条件を定義できます。

> **注:**
> 各構成ページで、複数の承認レベルを作成できます。

Example:
さまざまなユースケースに基づいて、異なる構成アイテムで見つかった同じ脆弱性に対して、異なる承認プロセスを定義できます。

アプリケーション脆弱性対応での修復の保留

v20.0 以降では、アプリケーション脆弱性一致アイテム (AVI) と修復タスクがライフサイクルを移動するときに選択できる [実装待ち] ステータスで修復を保留できます。レコードを手動でこのス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テータスに移行するには、AVI から [実装待ち] を選択し、[調査中] ステータスの修復タスクレコードを選択します。

ユースケース

修復スペシャリストは、レコードを [実装待ち] に移動して、タスクの調査と作業が完了したことをチームに知らせることができます。修正プログラムを実装する準備ができているものの、入手できないことがわかった場合は、この更新を選択できます。入手できない修正の例として、ソフトウェアパッチがあります。調査が完了したときにパッチのメンテナンス期間が利用できない場合は、パッチを展開できるようになるまでタスクを [実装待ち] に移動できます。

必須項目

[実装待ち] ステータスの AVI レコードと修復タスクレコードには、次の 2 つの必須の編集可能なフィールドがあります。

修復コミットメント日
: 修復予定日。

修復計画
: 修復のための修復計画の説明。このテキストはレコードのメモに表示されます。

フィールドとシステムプロパティ

レコードを [実装待ち] に移行すると表示されるモーダルに対してデフォルトで true に設定されている 2 つのシステムプロパティがあります。デフォルト設定のままにした場合：

sn_vul.remediation_fields
: [修復コミットメント日] フィールドと [修復計画] フィールドを必須フィールドとして設定します。false に設定した場合、これらのフィールドはオプションです。

sn_vul.awaiting_implementation
: レコードで [実装待ち] を選択した後、[修復コミットメント日] フィールドと [修復計画] フィールドを含むモーダルを表示します。false に設定すると、コミットメント日または計画の入力を求めるプロンプトを表示せずに、AVI のステータスを [実装待ち] に変更できます。

未達成修復コミットメント日モジュール

修復コミットメント日を過ぎた AVI を [未達成修復コミットメント日] モジュールで確認します。ナビゲート アプリケーション脆弱性対応 > 脆弱性一致アイテム > 未達成修復コミットメント日 をクリックしてリストを表示します。

修復タスクから **AVI** へのステータスロールダウン

レコードを [実装待ち] に移行する UI アクションボタンは、[調査中] ステータスのアプリケーション脆弱性一致アイテムおよび修復タスクレコードにのみ表示されます。ステータスロールダウンの場合、修復タスクで [実装待ち] を選択すると表示されるモーダルに、[既存の **AVI** を上書き] オプションがあります。

オプション	説明
[既存の **AVI** を上書き] を選択します。	既に [実装待ち] ステータスになっているタスク内の既存の AVI で、修復コミットメント日と修復計画を上書きするには、このオプションを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

オプション	説明
	選択すると、この機能は修復タスクの日付と計画データを AVI にロールダウンします。
[既存の **AVI** を上書き] は無効のままにします。	既に [実装待ち **]** ステータスになっているタスクの既存の AVI について日付と計画の値をそのまま維持するには、このオプションを非アクティブのままにします。 無効にすると、既に [実装待ち] にある AVI は既存の日付と計画データを保持し、ステータスロールダウンの影響を受けません。

ロールダウンの例

たとえば、修復タスクを [オープン] から [実装待ち] に移行して、ソフトウェアパッチメンテナンス期間のタスクのコミットメント日と計画情報を更新できるようにするとします。このタスクに [実装待ち] ステータスの AVI があり、修復タスクに一致するようにそのコミットメント日と計画情報を更新するとします。

修復タスクと一致するように AVI の日付と計画データを上書きするには、プロンプトが表示されたら [既存の **AVI** を上書き] チェックボックスをオンにします。AVI の日付と計画の値は、[実装待ち] を選択したときにプロンプトでタスクに入力する計画と日付の値になります。

この場合に上書きオプションを選択せず、[実装待ち]に AVI がある場合、AVI の元の日付と計画データはそのまま残ります。[実装待ち] を選択したときにプロンプトでタスクに入力した計画と日付の値は、タスクで既に [実装待ち] ステータスになっている AVI では使用されません。

タスクの AVI が [解決済み] または [クローズ済み **-** 修正済み **(Closed - fixed)]** で、タスクを [実装待ち] に移行した場合、[既存の **AVI** を上書き] を選択しても、ステータスの優先順位が高いため、[クローズ済み **-** 修正済み **(Closed - fixed)]** および [解決済み] から [実装待ち] に変更されることはありません。

タスクを [実装待ち] に移行するときに上書きが選択されておらず、既に [実装待ち] である AVI がある場合にには、タスクを [オープン] または [調査中] に戻すと、AVI は [実装待ち] のままになります。

アプリケーション脆弱性対応 の例外承認者を追加する

例外を要求できるように、ユーザーを承認者グループに追加します。

始める前に

必要なロール：sn_vul.app_exception_approver

このタスクについて

アプリケーション脆弱性一致アイテムの例外要求は、デフォルトの 2 レベルの承認フローを使用して承認されます。要求は、2 つのレベルの承認者によって承認されます。第 1 レベルのグループへのユーザーの追加は必須です。第 2 レベルにユーザーがいない場合、要求は第 1 レベルの承認後に承認されます。

手順

1. 次のように移動する。 **All** (すべて) > ユーザー管理 **(User Administration)** > グループ.
2. [名前] 列で [例外] を検索し、[アプリケーション例外承認者 **-** レベル **1 (Application Exception Approver - Level 1)]** をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

> **注:**
> アプリケーション脆弱性対応 の v12.8.1 以降では、システムプロパティ [sys_properties] テーブルのワークフローで、ベースシステムのシステムプロパティを使用して例外承認を行うことができます。このため、ワークフローで例外または誤検出要求が作成されると、この要求はシステムプロパティで定義されているグループ ID に承認のために送信されます。次のように移動する。 **All** (すべて) > システムプロパティ をクリックし、[*sn_vul.app_exception_approver_L1*]、[*sn_vul.app_exception_approver_L2*]、または [*sn_vul.app_false_positive_approver_group*] を選択して、プロパティ値を変更します。

3. [グループアプリケーション例外承認者 - レベル 1 (Group Application Exception Approver - Level 1)] フォームで、[グループメンバー] 関連リストをクリックします。
4. [新規] をクリックして、リストを作成します。
5. フォームのフィールドに入力します。

ユーザーフォーム

フィールド	説明
ユーザー ID	ユーザーの一意の識別子。
名	ユーザーの名。
姓	ユーザーの姓。
タイトル	ユーザーの役職。タイトルまたはジョブの説明を入力するか、リストから選択します。
部門	ユーザーの部門。
パスワード	ユーザーにアサインされたパスワード。このパスワードは、永続的または一時的なものにすることができます。
パスワードのリセットを強制	セキュリティを確保するためにユーザーがパスワードをリセットできるようにするオプション。
ロックアウト	ユーザーをインスタンスからロックアウトし、ユーザーのすべてのアクティブなセッションを終了するオプション。admin ロールを持つユーザーはロックアウトできません。
有効	このユーザーをアクティブにするオプション。次の領域では、自分だけが非アクティブなユーザーを見ることができます。 ○ ユーザーのリスト ○ 参照フィールドの選択リスト (虫眼鏡アイコン) ○ 参照フィールドに入力すると表示されるオートコンプリートリスト
Web サービスへのアクセスのみ	このユーザーを非インタラクティブユーザーとして指定するオプション。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
内部統合ユーザー	このユーザーを内部統合ユーザーとして指定するオプション。
メール	ユーザーのメールアドレス。
言語	ユーザーの優先言語。
カレンダー同期	ワークスケジュールの管理に使用されるカレンダー。たとえば、 Outlook です。
タイムゾーン	このユーザーがいる場所のタイムゾーン。
日付形式	ユーザーの優先日付形式。
電話 (勤務先)	ユーザーの勤務先電話。
携帯電話	ユーザーの携帯電話。
写真	[クリックして追加...] をクリックしてアップロードできる写真。

6. **[Submit]** をクリックします。
7. オプション: ステップ 1 ～ 5 を繰り返して、[アプリケーション例外承認者 - レベル 2 (Application Exception Approver - Level 2)] を作成します。
   承認者は、[アプリケーション脆弱性対応] > [自分の承認] に移動し、要求を承認する必要があります。

自動翻訳

アプリケーション脆弱性対応 での例外の要求と承認

アプリケーション脆弱性一致アイテムの修復または修復タスクを、指定した期間保留するように要求できます。

たとえば、マシンにパッチが適用されない場合に、開発者が例外を要求できます。アクセス権を持つ承認者は、他のユーザーからの要求を承認できます。

例外ルールを作成し、例外ルールの例外延長を要求することもできます。デフォルトでは、保留、例外ルール、および例外延長要求に対して 2 レベルの承認が必要です。

例外を要求または承認するには、次のページを参照して下さい。

- アプリケーション脆弱性一致アイテムの例外を要求する
- GRC: ポリシーとコンプライアンス管理 を使用したアプリケーション脆弱性の例外の要求
- アプリケーション脆弱性対応で例外ルールと例外ルール延長要求を承認する
- アプリケーション脆弱性対応 での例外ルールの延長の要求

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

例外管理の全ステージでメール通知が送信され、要求のステータスやその他の詳細情報が通知されます。たとえば、例外が要求されると、要求が発生したことを確認するメールが要求者に届きます。承認者にも、例外が要求されたことを示すメールが届きます。

アプリケーション脆弱性対応 の v21.0 以降では、誤検出と例外を承認する期間を設定できます。また、設定した日数経過後の承認者と要求者の両方に対するメール通知も可能です。要求が発生すると、アプリケーション脆弱性一致アイテムが [レビュー中] ステータスに変わり、ステータス変更レコードが作成されます。構成された期間内に承認者が応答しない場合、アプリケーション脆弱性一致アイテムまたは修復タスクは [オープン] ステータスに戻ります。以前のステータスは **[backup_state]** フィールドに保存されます。詳細については、「例外管理の承認ルールの構成」を参照してください。

アプリケーション脆弱性一致アイテムの例外を要求する

すぐに修復できないアプリケーション脆弱性一致アイテムの例外を要求します。たとえば、マシンにパッチが適用されない場合に、開発者が例外を要求できます。

重要:
脆弱性マネージャーワークスペースと IT 修復ワークスペースから、アプリケーション脆弱性一致アイテムと修復タスクの例外を要求できます。詳細については、「で修復タスクとレコードの例外を要求する Vulnerability Manager ワークスペース」と「IT 修復ワークスペースで例外を要求する」を参照してください。

始める前に
必要なロール：開発者グループ

手順

1. 次のように移動する。 アプリケーション脆弱性対応 > アプリケーション脆弱性一致アイテム > **All** (すべて) をクリックし、例外を要求するアイテムを選択します。
   選択したアイテムは、[オープン] または [調査中] ステータスである必要があります。

   注:

   アプリケーション脆弱性対応の v21.0 以降は、アプリケーション脆弱性一致アイテムの以前のステータスが **[backup_state]** フィールドに保存されます。

2. [アプリケーション脆弱性一致アイテム] フォームで、[例外の要求] をクリックします。

   注:
   で 脆弱性対応 が選択されているか、 GRC: ポリシーとコンプライアンス管理 されているかによって異なります アプリケーション脆弱性対応 > 例外管理 画面で、[例外の要求] フォームが変更されます。GRC: ポリシーとコンプライアンス管理 の場合は、「GRC: ポリシーとコンプライアンス管理 を使用したアプリケーション脆弱性の例外の要求」を参照してください。

3. [例外管理] 画面で 脆弱性対応 が選択されている場合は、[例外管理] フォームのフィールドに入力します。

   [例外の要求] フォーム

フィールド	説明
期限	例外要求の有効期限が切れる日付この日付は、次で選択した期間内である必要があります: **All**

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	(すべて) > アプリケーション脆弱性対応 > アドミニストレーション > 例外管理 スクリーン。 例外要求の有効期限が切れると、グループは [オープン] ステータスに戻ります。 **注:** アプリケーション脆弱性対応 (AVR) のバージョン 18.0 以降では、保留されたアプリケーション脆弱性一致アイテムをクローズして、スキャナーで再オープンできます。例外ウィンドウの有効期限が切れる前にアイテムが再オープンされた場合、AVIT のステータスはアクティブな例外ウィンドウに従って保留状態に戻ります。この機能を有効にするには、システムプロパティ sn_vul.auto_defer_avit_in_active_exception_window の値を true に設定します。また、保留期限は、AVIT がクローズした後や例外の有効期限が切れた後も保持されます。必要なロールは、読み取り、書き込みともに sn_vul.app_manage_exception_configuration です。
理由	[理由] を選択します。選択肢は次のとおりです。 ○ リスクの受容 ○ メンテナンス期間待ち ○ 修正が利用不可 ○ コントロールの緩和を実施 ○ その他 理由の新しい選択肢を追加する方法については、「ポリシー理由のマッピングの定義」を参照してください。
追加情報	この要求が行われている理由に関連する詳細情報。この必須フィールドは修復オーナーが更新します。

4. [承認要求] をクリックして例外要求を送信します。
   アプリケーション脆弱性一致アイテムのステータスが [レビュー中] に変わります。[ステータス変更承認] タブを使用して、例外要求のステータスを追跡します。

GRC: ポリシーとコンプライアンス管理 を使用したアプリケーション脆弱性の例外の要求

アプリケーション脆弱性対応 内の ポリシーとコンプライアンス管理 アプリケーションの GRC ポリシー例外管理機能を使用して、ポリシー例外を要求します。

始める前に

ポリシー例外統合を使用してポリシー例外を要求する前に、ServiceNow Store から GRC: ポリシーとコンプライアンス管理 アプリケーションをダウンロードする必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

必要なロール： sn_vul.remediation_owner

クラシック UI で例外を要求することもできます。手順は次のとおりです。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アプリケーション脆弱性一致アイテム (または [修復タスク]>[すべて] をクリックし、例外を要求するアイテムまたはグループを開きます。
   選択するアイテムまたはグループは、[オープン]、[調査中]、または [実装待ち] ステータスである必要があります。
2. 選択したフォームで、[例外の要求] をクリックします。
3. [例外管理] 画面で GRC: ポリシーとコンプライアンス管理 が選択されている場合は、[例外管理] フォームのフィールドに入力します。

[例外の要求] フォーム

フィールド	説明
ポリシー	例外を要求している脆弱性管理ポリシー。
コントロール目標	選択したポリシーに関連付けられているコントロール目標。ポリシーが選択されていない場合は、すべてのコントロール目標が一覧表示されます。
有効開始日	例外が開始される日付。デフォルト値は現在の日付です。過去の日付にすることはできません。
有効期限	ポリシー例外が期限切れになり、脆弱性一致アイテムまたはグループのステータスが [保留] から [オープン] に変更される日付。 **注:** ポリシー例外が有効である日数を、ポリシーとコンプライアンスでポリシーに設定した [最大例外期間 (日数)] を超える日数に設定することはできません。詳細については、「ポリシーの作成」を参照してください。
理由	例外を要求する理由。
理由	この要求が行われている理由に関連する詳細情報。この必須フィールドは修復オーナーが入力する必要があります。

   a. [承認要求] をクリックして例外要求を送信します。
   脆弱性一致アイテムのステータスが [レビュー中] に変わり、ポリシー例外が作成されます。[ステータス変更承認] タブを使用して、例外要求のステータスを追跡します。

   b. [ポリシー例外] 関連リストをクリックして、ポリシー例外を表示します。

   c. ポリシー例外番号をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

d. [承認者] フィールドで、承認者の名前を選択します。

e. [ソース] タブをクリックし、[コントロール目標] フィールドからコントロール目標を選択します。

f. [リスクアセスメント] タブをクリックし、[リスク評価] フィールドからリスク評価を選択します。

g. フォームを保存します。

h. [影響を受けるコントロール] タブをクリックし、 [追加] をクリックしてコントロールを追加します。

i. フォームを保存します。

> 注:
> [コンプライアンスレビューを要求] をクリックすると、コンプライアンスレビューを作成できます。

j. 承認フォームが承認者に送信されます。

k. 承認者は [承認] をクリックして要求を承認するか、[追加の承認を要求] をクリックして追加の承認を要求します。
レコードのステータスが [保留] に変わります。表示されている理由は、例外要求を出したときに選択したものです。[保留] タブにはレコードに関する追加のメモが表示されます。

> 注:
> 要求が却下された場合、レコードは前のステータスに移行します。

4. **[Submit]** をクリックします。
ポリシー例外統合および修復オーナーとコンプライアンスマネージャー間の引き渡しの詳細については、「ポリシーとコンプライアンス管理オプションのセットアップ」を参照してください。

アプリケーション修復タスクの例外を要求する

アプリケーション修復タスクをすぐに解決できない場合に、指定した期間修復タスクを保留する例外を要求します。

始める前に

例外は 脆弱性対応 のワークスペースから要求できます。「IT 修復ワークスペースで例外を要求する」を参照してください。

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

必要なロール：sn_vul.remediation_owner、sn_vul.app_security_champion、または sn_vul_container.remediation_owner

クラシック環境のアプリケーション修復タスクに対して例外を要求することもできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > 修復タスク > **All** (すべて).
2. 例外を要求するグループを選択します。
   選択するタスクは、[オープン]、[調査中]、または [実装待ち] ステータスである必要があります。
3. アプリケーション修復タスクレコードで、[例外の要求] を選択します。
4. フォームのフィールドに入力します。

[例外の要求] フォーム

フィールド	説明
期限	例外要求の有効期限が切れる日付。この日付は、構成で定義された例外期間内である必要があります。
理由	例外を要求する理由。
追加情報	この要求が行われている理由に関連する詳細情報。このフィールドは修復オーナーが更新します。

5. [承認要求] をクリックします。

アプリケーション脆弱性対応で例外ルールと例外ルール延長要求を承認する

すぐに修復できないアプリケーション脆弱性一致アイテムの例外要求を承認します。これらの要求のリスクを評価した上で、修復できるまで保留にすることを承認する必要があります。

始める前に

必要なロール：sn_vul.app_exception_approver

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > 自分の承認.
2. キューから要求を選択します。
3. 適切なコメントを添えて、要求を承認または却下します。

ポリシー理由のマッピングの定義

例外を要求するすべてのユーザーが使用可能な理由の選択肢を定義できます。

始める前に

GRC: Policy and Compliance Management アプリケーションがインストールされている必要があります。このアプリケーションは ServiceNow Store の個別のサブスクリプションで利用できます。

システム要件とファミリーの互換性の詳細については、ServiceNow Store Web サイトのアプリケーションリストを参照してください。

必要なロール：sn_vul.compliance.manager および sn_vul.vulnerability_admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > ポリシーとコンプライアンス > ポリシー例外 > 統合レジストリ.

   注:
   [理由の選択肢] テーブルで利用可能な理由の選択肢から選択する方法と、新しい理由を追加する方法があります。

2. アプリケーションの統合レジストリ ([アプリケーション脆弱性対応]、[脆弱性対応] など) をクリックします。
3. 既存の理由の選択肢を追加するには、次の手順を実行します。
   a. [理由の選択肢] リストで、[新規] をクリックします。
   b. 虫眼鏡アイコンをクリックし、理由を選択します。
4. [理由の選択肢] テーブルに新しい理由の選択肢を追加するには、次の手順を実行します。
   a. [理由の選択肢] リストで、[新規] をクリックします。
   b. 虫眼鏡アイコンをクリックします。
   c. [新規] をクリックします。
   d. フォームのフィールドに入力します。

   [理由の選択リスト] フォーム

フィールド	説明
ラベル	この選択肢の一意のラベル。
値	この選択肢の一意の値。 この値は、それぞれのアプリケーションの [ポリシー例外理由マッピング] テーブルでマッピングされます。このテーブルに移動するには、フィルターナビゲーターに「sn_vul_policy_reason_mapping.LIST」と入力します。
順序	この選択肢の順序。理由はこの番号に基づいて順序付けされます。
デフォルト	オンデマンドポリシー例外が要求されたときには常にこの理由の選択肢が利用可能であることを示すオプション。統合レジストリにアプリケーション固有の選択肢が入っていない場合は、[デフォルト] フィールドが選択されているすべての選択肢が使用可能になります。
有効	理由の選択肢のリストに選択肢を表示するオプション。

5. **[Submit]** をクリックします。

アプリケーション脆弱性対応 での例外ルールの延長の要求

保留された例外ルールがその保留された期限に達する前に、この例外ルールの延長を要求します。修復オーナーは、この要求を行うために保留期日まで待つ必要がなくなりました。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：アプリセキュリティマネージャー sn_vul.app_sec_manager、セキュリティチャンピオン sn_vul.app_security_champion。

このタスクについて
拡張ルールレコードでは、ルールが [承認済み] ステータスである場合にのみ、[保留期限] 日付の延長を要求できます。ルールによって作成された多数のレコードが、修復タスクが新しい AVI の受け入れを停止する日付である [保留期限] までに解決されていない場合に、ルールのこの延長を要求できます。この延長によって例外ルールが更新されるため、既存のルールの保留日が自動的に延長されます。

脆弱性対応 ワークスペースから延長を要求することもできます。詳細については、「脆弱性マネージャーのワークスペースでの保留された脆弱性一致アイテムの延長の要求」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > 例外ルール.
2. 承認済みの例外ルールを選択します。
3. [拡張を要求] を選択します。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
拡張期限	例外ルールを延長する必要がある期限の日付を選択します。
理由	例外ルールを保留する理由を入力します。 次の選択肢があります。 ○ リスクの受容 ○ メンテナンス期間待ち ○ 修正が利用不可 ○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

5. [要求承認] を選択します。
要求が承認されると、例外ルール、関連する修復タスク、およびアプリケーション脆弱性一致アイテムの [保留期限]、[理由]、および [補足情報 (Additional information)] フィールドが更新されます。要求が送信され、承認者によって後続のアクションが実行されると、メールがトリガーされます。

注:
- 要求は 2 段階の承認を経過します。
- [拡張を要求] ボタンは、例外ルールの一部として作成された修復タスクでは使用できません。
- 保留された例外ルールが再度延長されると、バックエンドで延長保留カウントが増加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション脆弱性対応 での保留された修復タスクの延長の要求

保留された例外ルールがその保留された期限に達する前に、保留された修復タスク (VUL) の延長を要求します。修復オーナーは、この要求を行うために保留期日まで待つ必要がなくなりました。

始める前に

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

このタスクについて

脆弱性対応 ワークスペースから延長を要求することもできます。詳細については、「脆弱性マネージャーのワークスペースでの保留された脆弱性一致アイテムの延長の要求」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > 修復タスク.
2. 保留された修復タスクを開きます。
3. [拡張を要求] を選択します。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
拡張期限	保留ステータスが期限切れになり、修復タスクが再アクティブ化される日付を選択します。
理由	問題を保留する理由を入力します。 次の選択肢があります。 ○ メンテナンス期間待ち ○ 修正が利用不可 ○ リスクの受容 ○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

5. [要求承認] を選択します。
   要求が承認されると、修復タスクに対する変更が、修復タスクの一部であるアプリケーション脆弱性一致アイテムにもロールダウンされます。ただし、アプリケーション脆弱性一致アイテムが保留ステータスであり、現在の期限日が更新期限日より前である必要があります。要求が送信され、承認者によって後続のアクションが実行されると、メールがトリガーされます。

   注:
   - 要求は 2 段階の承認を経過します。
   - [拡張を要求] ボタンは、例外ルールの一部として作成された修復タスクでは使用できません。
   - 保留された修復タスクが再度延長されると、バックエンドで延長保留カウントが増加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション脆弱性対応の保留されたアプリケーション脆弱性一致アイテムの延長の要求

保留されたアプリケーション脆弱性一致アイテムがその保留された期限に達する前に、このアプリケーション脆弱性一致アイテムの延長を要求します。修復オーナーは、この要求を行うために保留期日まで待つ必要がなくなりました。

始める前に

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

このタスクについて

脆弱性対応 ワークスペースから延長を要求することもできます。詳細については、「脆弱性マネージャーのワークスペースでの保留された脆弱性一致アイテムの延長の要求」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > 脆弱性一致アイテム.
2. 保留されたアプリケーション脆弱性一致アイテムを開きます。
3. [拡張を要求] を選択します。

   注:
   [拡張を要求 (Request Extension)] ボタンは、アプリケーション脆弱性一致アイテムのステータスが [保留] の場合にのみ表示されます。

4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
拡張期限	保留されたアプリケーション脆弱性一致アイテムを修復のために延長する必要がある期限を選択します。
理由	問題を保留する理由を入力します。 次の選択肢があります。 ○ メンテナンス期間待ち ○ 修正が利用不可 ○ リスクの受容 ○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

5. [要求承認] を選択します。
   要求が送信され、承認者によって後続のアクションが実行されると、メールがトリガーされます。

   注:
   - 要求は 2 段階の承認を経過します。
   - 保留された例外ルールが再度延長されると、バックエンドで延長保留カウントが増加します。

6. 要求が承認されると、[期限]、[理由]、および [保留メモ] が更新されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション脆弱性対応の例外ルールを作成、削除、およびキャンセルする

特定の条件を満たすアプリケーション脆弱性一致アイテム (AVI) に対する例外を自動的に要求するルールを作成します。

始める前に
たとえば、すぐに修正できないことがわかっている特定の既知の脆弱性または重大な脆弱性に基づく条件でルールを作成できます。このルールでは、新規および既存の AVI が承認済みルールの条件に一致する場合に、そうした AVI を自動的に保留にすることができます。

- ルールはルールレコードに入力した [有効期間開始日] から [有効期間終了日] まで適用されます。
- 修復タスク (AVUL) は、[保留] ステータスの一致する AVI に対してルールが承認された後に作成されます。
- この AVUL のグループ化方法は、例外ルールと呼ばれます。
- この AVUL をクローズ、再オープン、削除することはできません。新規および再オープンされた AVI は、この AVUL に追加され、「有効期間開始日」から「有効期限終了」の日付でグループが期限切れになるまで保留されます。

注:

メール通知は、例外ルールワークフローのすべてのステージで送信されます。こうしたメールには、要求のステータスとその他の詳細が記載されています。たとえば、例外ルールが要求されると、要求が送信されたことを確認するメールが要求者に届きます。

ルールが却下された場合は、[ドラフト] ステータスで再オープンして更新し、承認のために再送信できます。

必要なロール：アプリセキュリティマネージャー sn_vul.app_sec_manager およびセキュリティチャンピオン sn_vul.app_security_champion。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > 例外ルール.
2. 例外ルールの新規レコードページで、[新規] を選択します。
3. フィールドに入力します。

フィールド	説明
名前	例外ルールの名前。
状況	読み取り専用：ドラフト
有効期限開始	このルールがアクティブになり、AVI が保留される開始日付。
実行順序	各例外ルールの一意の順序。小さな値から大きな値の順です。
有効期限	修復タスクが新しい AVI の受け入れを停止する日付。
保留期限	修復タスクと AVI の保留期限の日付。この日付になると、AVUL がクローズされ、すべての AVI がタスクから移動して再オープンされます。グループルールがこうした AVI に再適用されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
理由	この例外ルールを作成する理由。
アサイン先グループ	保留された VI の追跡用に修復タスクがアサインされているグループ。
追加情報	要求者が承認者に提供する追加情報。この情報は、修復タスクの説明フィールドに入力されます。
条件	このルールに一致する AVI を指定するフィルター条件。
既存のデータで実行	このルールが初めて実行されるときに既存のデータでこのルールを実行できるようにするオプション。 このオプションを非アクティブのままにすると、ルールは新しいデータで始まるスケジュール済みジョブ *`Associate existing AVIs with Auto Exception Rule`* によって毎日実行されます。 [既存のデータで実行] オプションを有効にすると、スケジュール済みジョブは「有効期間開始日」に既存のデータに対して 1 回実行されます。

4. ルールの作成時にアサイン先グループを追加します。
5. いずれかを選択します。

   ルールが承認されると、[承認済み] ステータスに移行します。ルールは *`Associate existing AVIs with Auto Exception Rule scheduled`* ジョブで AVI を評価します。[既存のデータで実行] を選択した場合は、既存の AVI が評価されます。ルールに対して修復タスクが自動的に作成され、その条件を満たす一致する AVI がタスクに関連付けられます。

   スケジュール済みジョブは、既存のデータに対して例外ルールを 1 回実行します。AVI が見つからない場合でも、既存のデータに対してルールが再度実行されることはありません。ルールに一致した既存の AVI が既に保留されているため、新しいデータのみが評価されます。

6. ルールを削除するには、例外ルールレコードで [削除] を選択します。
   次のメッセージが表示されます。ルールを削除すると、関連する修復タスクが削除され、関連する脆弱性一致アイテムが再オープンされます (If you delete the rule, the associated remediation task will be deleted and the related vulnerable items will be reopened)。その後、修復タスクルールが個々の AVI に適用され、例外ルールが削除されます (The remediation task rules will then be applied to the individual AVIs and the exception rule is deleted)。
7. [ルールを保持] を選択して停止するかまたは [削除ルール] を選択して続行します。
8. ルールを非アクティブ化して [例外ルール] リストに残すには、[キャンセル] を選択します。
   次のメッセージが表示されます。このルールをキャンセルすると、関連する修復タスクが削除され、関連する脆弱性一致アイテムが再オープンされます (If you cancel this rule, the associated remediation task will be deleted and the related vulnerable items will be reopened)。その後、修復タスクルールが個々の脆弱性一致アイテムに適用され、例外ルールがドラフト状況に移行し

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ます (The remediation task rules will then be applied to the individual vulnerable items and the exception rule will be moved to the draft state)。

9. [ルールを保持] を選択して停止するか、[キャンセル] を選択してルールを [ドラフト] に移行して非アクティブ化します。

アプリケーション脆弱性対応 修復タスクとタスクルールの概要

修復タスク (AVUL) を設定すると、アナリストと修復スペシャリストがアプリケーション脆弱性一致アイテム (AVI) を整理して一括で分析できるようになります。修復タスクを形成する基準は、AVI が修復タスクに自動的にアサインされるように構成されます。修復タスクを使用すると、進捗状況を監視し、修復プロセスをより効率的に進めることができます。

アプリケーション脆弱性一致アイテムと修復タスクの保留数の追跡

脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、または修復タスクが保留された回数を追跡します。*`set deferral counts`* スケジュール済みジョブは毎日実行され、[保留数] 列で複数回保留されたレコード数が提示されます。レコードは、VR、AVR、および CVR の複数の保留モジュールに表示されます。

修復タスクルールについて

修復タスクルールを使用すると、アプリケーション脆弱性一致アイテムを自動的にグループ化してアサインする方法を定義できます。デフォルトのルール「脆弱性」は、脆弱性に基づいて AVI を収集するベースシステムに含まれています。ただし、AVI からアクセス可能な列では、その他の値セットでグループ化できます。こうした値には、構成アイテム (CI) や脆弱性エントリなどが含まれる場合があります。

アプリケーション脆弱性対応には、脆弱性対応アプリケーションをアクティブ化したときに使用可能な、そのアプリケーションに含まれているタスクルールがあります。

条件ビルダーを使用して複数の条件を作成できます。[グループ分け基準] セクションで、フィールドのペアを設定すると、別の行が表示されます。最大 6 つの [グループ分け基準] の選択を設定できます。グループのアサインを自動化することもできます。詳細については、「アプリケーション脆弱性対応 のアプリケーション脆弱性一致アイテムを自動的にアサインする」と「脆弱性対応 内のフィルタリング」を参照してください。

たとえば、アプリケーション脆弱性一致アイテムを、構成アイテム別または製品モデル別にグループ化できます。低重大度の脆弱性または低リスクの CI に対して、1 つのタスクルールを設定できます。重要なサーバーに対して、会社をより大きなリスクにさらす脆弱性に対しては、別のタスクルールを設定できます。利用可能なオプションの詳細については、「アプリケーション脆弱性対応修復タスクルールの作成、編集、または削除」を参照してください。

会社がより多くのリスクにさらされるアプリケーション脆弱性一致アイテムには、別のルールセットを使用できます。修復タスク名が修復タスクルールの [グループ分け基準] の値に追加され、新しいレコードの簡単な説明が作成されます。

新しいアプリケーション脆弱性一致アイテムが作成、インポート、またはクローズ後に再オープンされると、それに対してルールが評価されます。AVI は 1 回のみ自動的に評価されます。ただし、クローズ後に再オープンする場合や、ルールを手動で再適用する場合は除きます。

新規の AVI または再オープンされた AVI ごとに、以下の処理が行われます。

- 修復タスクルールごとに、AVI が修復タスクルールフィルターと比較されます。
- 修復タスクルール条件が一致するルールごとに、AVI の [グループ分け基準] の選択に基づいてデータがルールによってプルされます。グループ名とフィールドがビルドされます。この場合

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

は、高リスク：QID-32342：*QID-3242* のサマリー (名前：脆弱性 ID：脆弱性サマリー) となります。

> **注:**
> 簡単な説明フィールドは 160 文字に制限されています。これより長い脆弱性サマリーは切り捨てられます。

このルールでは、AVI と同じアサイン先グループにアサインされている、一致するオープン修復タスクがあるかどうかを確認します。

- タスクが見つかった場合、AVI は [オープン] ステータスの既存のタスクに追加されます。
- [オープン] ステータスのタスクが見つからない場合は、高リスク：**QID-32342** タスクが作成され、AVI と同じアサイン先グループにアサインされて、AVI が修復タスクに配置されます。

複数の修復タスクルールを定義すると、さまざまな種類の脆弱性をグループ化できます。各脆弱性は、修復タスクに配置される前に修復タスクルールの条件と比較されるため、ルールが多すぎるとパフォーマンスに影響を与える恐れがあります。重複する修復タスクを作成しない条件となるように、タスクルールを設定します。

デフォルトでは、修復タスクルールで、アイテムのグループ化の際に AVI のアサインルールによって設定されたアサイン先グループが使用され、AVI に一致するように修復タスクがアサインされます。

デフォルトのタスクルールの一部として、こうした修復タスクのアサインは [アサインルール] モジュールのルールによって制御されます。アサインルールについては、「脆弱性対応 アサインルールの概要」を参照してください。

タスクルールが削除されると、フォームまたはリストビューから、そのルールによって作成されたすべてのオープンタスクを削除できます。[オープン] ステータスでないタスクは除外されます。

修復タスクルールの再適用

修復タスクルールを変更する場合は、修復タスクルールページの [再適用] ボタンを使用して、そのルールによって作成されたすべてのアクティブなオープン修復タスクに対し、変更されたルールを再実行します。変更されたルールに基づいて、修復タスクが自動的に削除され、再作成されます。

[再適用] は、既存の修復タスクのみをチェックします。

[再適用] を選択すると、「この修復タスクルールを最適用すると、このルール用の修復タスクが削除されてから再作成されます (Reapplying this remediation task rule will delete and re-create the remediation tasks for this rule)」というメッセージが表示されます。[オープン] ステータスでない修復タスクは削除されません。

手動での修復タスクの作成と **AVI** の追加

別のアプリケーション修復タスクレコードからアプリケーション修復タスク (AVUL) を作成し、アプリケーション脆弱性一致アイテム (AVIT) を手動で追加します。詳細については、「アプリケーション脆弱性対応でアプリケーション修復タスクを手動で作成する」を参照してください。

修復タスクルールと **AVI** の作成と更新

スキャンの CI または製品モデルが既知の脆弱性に関連付けられている場合、AVI が作成されます。作成後、AVI は一致の修復タスクルールの条件に照らして評価されます。既存の修復タスクに一致するものがある場合は、AVI が追加されます。一致する修復タスクが見つからない場合は、新しい修復タスクが AVI に対して作成されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクのフィルタリング条件でキャプチャされたプロパティが AVI で更新または変更された場合、更新された AVI も一致の修復タスクルールに照らして評価されます。既存の修復タスクに一致するものがある場合は、AVI が追加されます。一致する修復タスクが見つからない場合は、新しい修復タスクが AVI に対して作成されます。

ステータスのロールアップとロールダウン

修復タスクを [オープン] に更新するか、[オープン] から [調査中] に更新すると、関連付けられているすべての AVI に対して新しいステータスがロールダウンされます。ステータスのロールダウンは、ステータスを変更した直後に発生します。

AVI から修復タスクへの状況のロールアップは、タスクのすべての AVI が [保留] または [クローズ済み - 修正済み **(Closed - Fixed)]** 状況である場合にのみ発生します。ロールアップは、15 分ごとに実行される *`Rollup application vulnerable item values to vulnerability and group`* スケジュール済みジョブによって行われます。ジョブが実行されるまでステータスはロールアップされません。AVI から修復タスクにステータスをロールアップするには、すべての AVI が同じステータスである必要があります。

アプリケーション脆弱性対応修復タスクルールの作成、編集、または削除

フィルター条件に基づいて、アプリケーション脆弱性一致アイテム (AVI) を修復タスク (AVUL) に自動的にグループ化するルールを作成できます。こうしたルールは、インポート時または手動作成時に AVI を自動的にグループ化します。

始める前に

新しいルールを作成しても、既存のデータには適用されません。送信すると、新しいインポートに対して実行されます。

必要なロール：アプリケーションセキュリティマネージャー

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > 修復タスクルール.
2. ルールを開くか、[新規] を選択します。
3. フォームのフィールドに入力するか、またはフィールドを編集します。

修復タスクルール

フィールド	説明
名前	タスクルールの名前。
有効	タスクがアクティブかどうかを示します。
説明	ルールの説明。
大文字と小文字を区別	条件が大文字と小文字を区別するかどうかを決定します。 **注:** デフォルト値は、大文字と小文字の区別なしです。
条件	ルールのオプションのフィルター条件。 デフォルト ([大文字と小文字を区別] チェックボックスが選択されていない) では、タスクルールのレコードとフォームで条件ビルダーに入力する検索テキストは、大文字と小文字が区別されません。選択によって、タスクのレコードとフォームで大文字と小文字を区別する検索を有効にできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	条件の例: 脆弱性 > 次の値に等しい > **VULNENT123451** (インポートされた既知の脆弱性)。この脆弱性があるすべての AVI がこの条件に一致します。
グループ (最大 **6** つの条件セットが利用可能)	
アプリケーション脆弱性一致アイテムのグループ化元 (Group application vulnerable items from)	ルールが AVI をグループ化するために使用するテーブル。 ツリーから要素を選択します。 ○ アプリケーション脆弱性一致アイテム [sn_vuln_vulnerable_item] ○ アプリケーション脆弱性一致アイテム - 構成アイテム [cmdb_ci] ○ アプリケーション脆弱性一致アイテム - アプリケーション脆弱性 [sn_vul_third_party_entry] ○ アプリケーション脆弱性一致アイテム - 製品モデル **注:** 拡張テーブルを選択した場合、[使用フィールド] はその拡張テーブルを使用するアプリケーション脆弱性一致アイテムにのみ適用されます。
使用フィールド	ルールが AVI をグループ化するために使用するテーブルのフィールド。ツリーから条件を選択します。 **注:** データを共有するすべての AVI が同じ修復タスクにアサインされてしまわないように、条件別のグループ化を作成できます。たとえば、[使用中 (Using)] フィールドとして [アサイン先グループ] と [IP アドレス (IP Address)] を選択し、複数の AVI が初期フィルター条件の [脆弱性] に一致する場合、[グループ分け基準] セクションで利用可能な多くのオプションを使用して、これらの AVI を修正のために個別のアサイン先グループにアサインできます。[グループ分け基準] 条件を使用すると、一部のデータを共有していても異なるグループにアサインできる個別の修復タスクを柔軟に作成できます。
アサイン	
修復タスクをアサインする基準	修復タスクを自動的にアサインする場合、[グループ] の選択肢に加えて [アサイン] の選択肢が、脆弱性一致アイテムをグループ化するために使用されます。必要に応じて新しいタスクが作成され、一致するアサイン先グループが設定されたタスクに各 AVI が配置されます。 このルールに基づいて作成されたタスクのアサインを自動化するには、利用可能なオプションのいずれかを選択します。 ○ [グループ分け基準] フィールド：[グループ分け基準] セクションの [使用フィールド **(Using field)]** からユーザーグループフィールドを選択すると、そのフィールドがドロップダウンメニューに表示されます。 ○ ユーザーグループ：ルックアップリストを使用して、静的ユーザーグループを選択します。

フォームまたはリストビューからルールを削除すると、そのルールによって作成されたすべてのオープン修復タスクを削除できるようになります。[オープン] ステータスでないグループは除外されます。

4. 新しいルールの [送信] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[送信] を選択すると、ルールが [修復タスクルール] リスト [sn_vul_grouping_rule] に表示されます。次の状況でルールが開始されます。

- 新しい AVI が作成されたとき。
- [再適用] を選択したとき。既存の修復タスクのみのタスクルールを評価するには、[再適用] を選択します。
- 自分またはシステムによって AVI が更新されたとき。

  AVI が更新されると、タスクルールが既存の修復タスクと一致するかどうかが評価されます。ルールチェックを開始する一般的な更新には次のようなものがあります。

  - ステータスが [クローズ済み] から [オープン] に、または [クローズ済み] から [調査中] に変わったとき。
  - 構成アイテム (CI) が変更されたとき。
  - 脆弱性が変更されたとき。

すべてのタスクルールで、更新された AVI との一致がチェックされます。ルールの条件が修復タスクの条件と一致する場合、一致する AVI がそのルールにアサインされます。

一致するものが見つからない場合は、新しい修復タスクが作成されます。

AVI から修復タスクへのステータスロールアップ、および修復タスクから AVI へのステータスロールダウンの詳細については、「アプリケーション脆弱性対応 修復タスクとタスクルールの概要」を参照してください。

修復タスクルールの例については、「アプリケーション脆弱性対応 修復タスクルールの例」を参照してください。

5. タスクルールを削除するには、[修復タスクルール] リストからルールを選択し、[削除] を選択します。
   次のメッセージが表示されます。選択した修復タスクルールによって n 個の修復タスクが作成されました (The selected remediation task rule created n remediation tasks)。その修復タスクのうち n 件が [オープン] ステータスです (Of the remediation tasks, n are in the Open state)。

オプション	説明
チェックボックスは無効です (デフォルト)。	ルールのみを削除します。[オープン] ステータスでないタスクは除外されます。
チェックボックスをオンにします。	この修復タスクルールを削除する際に、[オープン] ステータスの修復タスクの削除を含めます。[オープン] ステータスのルールと修復タスクを削除します。

6. いずれかのオプションを選択し、[削除] を選択します。

アプリケーション脆弱性対応でアプリケーション修復タスクを手動で作成する

別のアプリケーション修復タスクレコードからアプリケーション修復タスク (AVUL) を作成し、アプリケーション脆弱性一致アイテム (AVIT) を手動で追加します。

始める前に

必要なロール：sn_vul.app_sec_manager

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > 修復タスク > **All** (すべて).
2. ページの右上にある [新規] を選択します。
3. [グループ構成] タブの [グループ化の方法] で、[手動] を選択します。
4. [送信] を選択します。
5. アプリケーション修復タスク [sn_vul_app_vulnerability] テーブルで新しいタスクレコード (AVUL) を見つけます。
   レコードは [オープン] ステータスで作成されます。
6. レコードを開き、アプリケーション脆弱性一致アイテムの関連リストを使用して、新規または既存のアプリケーション脆弱性一致アイテムをこのグループに追加します ([編集] または [追加])。
7. [更新] を選択してレコードを保存するか、他の UI アクションを選択してレコードを別のステータスに移行します。

自動クローズルールを作成する

自動クローズルールを使用して、設定したフィルター条件に基づいて古い AVIT を自動的にクローズします。

始める前に
必要なロール：sn_vul.app_manage_auto_close_rules

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > 自動クローズルール.
   ベースシステムには次の自動クローズルールが提供されます。

   前回スキャンされたアプリケーション脆弱性：過去 90 日以内に報告されていない脆弱性は、[古い] ステータスに移行します。
2. [新規] を選択して、新しい自動クローズルールを作成します。
3. フォームのフィールドに入力します。

フィールド	値
名前	自動クローズルールの名前
アクティブ	ルールをアクティブ化するためのオプション有効にすると、フィルター基準に一致するすべての検出が自動的にクローズされます。
実行順序	自動クローズルールの実行に対する一意の値。この値によって実行順序が決まります。デフォルト値は 100 です。
統合タイプ	アプリケーション脆弱性統合
説明	自動クローズルールの説明。
条件	クローズする必要がある検出を識別するために使用されるフィルター条件。

4. [**Submit** (送信)] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動クローズルールプロセッサーのスケジュール済みジョブは、夜間に実行されます。指定された条件に基づいて AVIT を識別し、一致した AVIT を [古い] ステータスに移行します。ステータスが [クローズ済み] と [古い] の両方の AVIT がある場合、AVIT はサブステートが [修復済み **(Fixed)]** に設定されてクローズされます。

ペネトレーションテストの構成

ペネトレーションテストアセスメントのタイプごとにスプリント期間と工数概算を構成できます。これにより、アプリケーションオーナーに対するスケジュール機能が提供され、ペネトレーションテストアセスメント要求の暫定的な期間を決定することができます。

始める前に
必要なロール：倫理的なハッカー

このタスクについて
倫理的なハッキングチームに対してペネトレーションテストアセスメント設定を構成して、ペネトレーションテストのアセスメント要求を受け取るグループや連絡先を決定することもできます。

脆弱性対応 の v19.0 以降では、Veracode 脆弱性統合 を使用している場合は、Veracode 脆弱性統合 のペネトレーションアセスメントテストは Veracode からの手動検出結果になります。これらは、アプリケーション脆弱性対応 で構成したペネトレーションテストアセスメント要求にはリンクされません。Veracode からのペネトレーションテストアセスメントの詳細については、「Veracode 脆弱性統合」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > ペネトレーションテストの構成.
2. 最初のセクションを使用して、アサイン先グループを構成します。
3. フォームのフィールドに入力します。

[ペネトレーションテストの構成] フォーム

フィールド	説明
ペネトレーションテストチームのユーザーグループ	ペネトレーションテストアセスメント要求がアサインされるグループ。
ペネトレーションテストアセスメント要求のデフォルトのアサイニー	ペネトレーションテストアセスメント要求の連絡先。

4. [更新] を選択します。
5. 2 番目のセクションを使用して、スプリントを構成します。
   詳細については、「ペネトレーションテストのスプリントの構成」を参照してください。
6. 3 番目のセクションを使用して、アセスメントタイプを構成します。
   詳細については、「ペネトレーションテストのアセスメントタイプの構成」を参照してください。

ペネトレーションテストのスプリントの構成

倫理的ハッキングチームに対してスプリント期間とキャパシティを設定し、このチームがペネトレーションテストアセスメントのスプリントキャパシティを管理できるようにします。

始める前に
必要なロール：倫理的ハッキング

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > ペネトレーションテストの構成.
2. [スプリントを構成] の [構成] オプションを選択します。
3. フォームのフィールドに入力します。

[スプリント構成] フォーム

フィールド	説明
スプリント期間 (日数)	スプリントの日数。
開始日	スプリント期間の開始日。
スプリント数	スプリント範囲の開始日と終了日に基づいた、生成可能なスプリントの数。
終了日	スプリント期間の最終日。
スプリントキャパシティ	
スプリントキャパシティ (時間)	スプリントのキャパシティ (時間)。

4. [スプリントを生成] を選択します。
作成されたスプリントを表示するには、[スプリントを表示] を選択します。

> **注:**
> スプリントが生成されて進行した後、同じ期間に対して [スプリントを生成] を選択した場合、現在のスプリントは通常どおりに完了します。残りのスプリントは、更新されたスプリント構成に基づいて再計算されます。

ペネトレーションテストのアセスメントタイプの構成

ペネトレーションテストアセスメントのタイプごとに工数概算を構成します。これにより、各アセスメントタイプに必要な工数を見積もることで、各スプリントのキャパシティを管理できます。

始める前に
必要なロール：倫理的ハッキング

このタスクについて
各スプリントはペネトレーションテスト要求にアサインされます。アセスメントタイプの工数概算に基づいて、スプリントの残高 (時間数) を反映するように時間が調整されます。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > ペネトレーションテストの構成.
2. 脆弱性対応 の v19.0 以降では、[構成] を選択すると、アセスメントタイプ、アプリケーションサイズ、および工数概算が表示されます。
3. オプション: 必要に応じてアセスメントタイプのレコードを選択してフィールドを更新するか、新しいレコードを作成します。

   (Optional) [アプリケーションサイズ (Application size)] の値によって、テスト時間とテスト作業をより正確に見積もるためのオプションが増えます。これらのレコードの時間を編集するか、または [新規] を選択して独自の組み合わせを作成することができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

既存のペネトレーションテスト要求レコードの [アセスメントタイプ] と [アプリケーションサイズ (Application size)] の値を変更して、スプリントキャパシティに合わせてテストをスケジュールできます。たとえば、テスト要求を入力する場合、一部のスプリントがテストのために既に確保されていることから、構成したスプリントの数が表示されないことがあります。スプリントの工数概算の時間が、テストのタイプとサイズに必要な組み合わせと一致する場合、新しい要求には使用できません。

次の [ペネトレーションテストスプリント] リストのレコードで、テスト要求にアサインされたスプリントを確認できます。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > ペネトレーションテストの構成 > スプリントを構成. スプリントの構成の詳細については、「ペネトレーションテストのスプリントの構成」を参照してください。

[アセスメントタイプ]、[アプリケーションサイズ]、および [工数概算] の基準値は次のとおりです。

[ペネトレーションテストアセスメントタイプの構成] フォーム

アセスメントタイプ	アプリケーションサイズ	工数概算 (時間)
集中テスト	小	20
集中テスト	中	30
集中テスト	大	40
集中テスト	標準	40
再テスト	小	10
再テスト	中	15
再テスト	大	20
再テスト	標準	20
完全なペネトレーションテスト	小	60
完全なペネトレーションテスト	中	70
完全なペネトレーションテスト	大	80
完全なペネトレーションテスト	標準	80

4. 変更を保存する場合は [更新] を選択し、新しいレコードの場合は [送信] を選択します。
5. v19.0 より前では、[アセスメントタイプを構成] の [構成] オプションを選択します。
6. 必要に応じて、アセスメントタイプの値を更新します。
基準値は次のとおりです。

[ペネトレーションテストアセスメントタイプの構成] フォーム

アセスメントタイプ	工数概算 (時間)
集中テスト	40
再テスト	20

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アセスメントタイプ	工数概算 (時間)
完全なペネトレーションテスト	80

7. 変更内容を保存します。

他のアプリケーションとの アプリケーション脆弱性対応 の統合

脆弱性対応 には、サードパーティ統合のサポートが含まれています。

サードパーティ統合

アプリケーション脆弱性統合は、外部システムとベンダーからデータを取得することによって、インスタンスのアプリケーション脆弱性データを強化するのに役立ちます。サポートされる統合の詳細については、次の概要トピックを参照してください。

- Fortify 脆弱性統合
- GitHub アプリケーション脆弱性統合
- Invicti 脆弱性統合
- Veracode 脆弱性統合
- Atlassian Jira 統合

重要:
脆弱性マネージャーワークスペースでは、リストアクションとフォームアクションを使用してアジャイルの問題を手動で作成し、AVIT と RT の修復を追跡できます。

注:

アプリケーション脆弱性対応 ではマルチソース統合はサポートされていません。サードパーティ統合は個別に扱われます。環境で複数のサードパーティ統合アプリケーションが使用されている場合、統合全体でアプリケーション脆弱性一致アイテム (AVI) の重複排除は行われません。

統合に関するその他の注意事項

統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、 アプリケーション脆弱性対応のバージョン 18.2.4 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

アプリケーション脆弱性対応の脆弱性統合は、スケジュールに基づいて実行するように構成されます。ただし、必要に応じて手動で実行することもできます。

必要なロール:sn_vul.app_read_integrations

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > 統合.
2. 実行する統合のレコードを開きます。
3. **[Execute Now** (今すぐ実行する)] をクリックします。

Vulnerability Response Integration with Black Duck

Vulnerability Response Integration with Black Duck との 脆弱性対応 統合では、Black Duck Software Composition Analysis (SCA) ツールからインポートされたデータが使用されます。これにより、コードの欠陥による影響や優先度を判断できるようになります。

統合の概要

Vulnerability Response Integration with Black Duck を使用して、SCA を収集し、そのデータを Now Platform で使用できるようにすることができます。脆弱性対応 v22.0.5 以降、SCA 脆弱性データをインスタンスにインポートして、ソフトウェアアプリケーションの脆弱性を特定することができます。詳細については、「ソフトウェア部品表 の詳細」を参照してください。

共有 API が SCA データを取り込みます。

注:
統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は「VR System」です。この値は変更しないでください。

スケジュール済みジョブにより、リストされている順序で統合が毎日自動的に呼び出されます。スケジュール済みジョブを手動で実行することもできます。スケジュール済みジョブでは、インスタンスを他の脆弱性管理システムと同期させることで、脆弱性修復ライフサイクルを簡素化します。

利用可能バージョン

Black Duck Integration の利用可能なバージョン

リリースバージョン	リリースノート
Vulnerability Response Integration with Black Duck 1.0.5	Application Vulnerability Response release notes

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザーグループおよびロール

Vulnerability Response Integration with Black Duck は admin ロールのユーザーによってインストールされ、アプリセキュリティマネージャーグループのメンバーによって構成されます。詳細については、「アプリケーション脆弱性対応 のユーザーロールおよびロール」を参照してください。

統合実行のステータスについては、「Vulnerability Response Integration with Black Duck インポート実行ステータスの表示」を参照してください。

サードパーティの脆弱性データを表示する方法については、「脆弱性ライブラリの表示」を参照してください。

Vulnerability Response Integration with Black Duck の統合前のタスクの準備

統合を成功させるために、Vulnerability Response Integration with Black Duck の統合前のタスクを計画して実行します。Vulnerability Response Integration with Black Duck では、Black Duck Software Composition Analysis (SCA) アプリケーションと API に精通していることを前提としています。

始める前に

Vulnerability Response Integration with Black Duck をインストールして構成する前に、アプリケーション脆弱性対応でも使用されている Common Weakness Enumeration (CWE) 統合を実行してインストールする必要があります。CWE 統合は、デフォルトで脆弱性対応とともにインストールされます。

> **注:**
> NIST 脆弱性データベース (NVD) データは Black Duck アプリケーション脆弱性統合のインストールには必要ありませんが、あれば便利です。NVD の詳細については、「NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理」を参照してください。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は VR.System です。この値は変更しないでください。

必要なロール：アプリセキュリティマネージャーグループ

このタスクについて

> **注:**
> 統合を実行する前に、要件に基づいて必要な構成変更を行います。

インポートする予定のアプリケーション脆弱性一致アイテムの数に応じて、インスタンスのサイジングを検証します。インスタンスが小さすぎると、ロードに時間がかかることがあります。インスタンスのサイズがわからない場合は、カスタマーサービス & サポートにお問い合わせください。

Vulnerability Response Integration with Black Duck には API URL と API トークンが必要です。

手順

API トークンとキー認証情報を作成します。

a. Black Duck プラットフォームにログインします。

b. ユーザーアカウントメニューに移動し、**[API Credentials (API** 資格情報)] を選択します。

c. [Generate API Credentials (API 認証を生成)] を選択します。

d. 後で使用するために認証情報を記録します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ServiceNow Vulnerability Response Integration with Black Duck をインストールする

インスタンスで統合を実行する前に、Black Duck ソフトウェア構成分析 (SCA) ツールがアプリケーション脆弱性対応と適切に統合されるように、インストールと構成の手順を完了する必要があります。

始める前に

インストールの前に、次のセットアップチェックリストを完了します。Black Duck ソフトウェア構成分析 (SCA) ツールがアプリケーション脆弱性対応と適切に統合されるように、これらのセットアップタスクを実行する必要があります。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

セットアップタスク

セットアップタスク	説明
脆弱性対応 アプリケーションがインストールされ、アクティブ化されていることを確認します。	このアプリケーションがアクティブ化されていることを確認するには、次の場所に移動しますサブスクリプション管理 > サブスクリプションインスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応 のインストール」を参照してください。
インスタンスに必要な ServiceNow ロールがあることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。 • まだアサインされていない場合、admin ロールを持つユーザーはアプリケーションをインストールして、ユーザーをアプリセキュリティマネージャーグループにアサインします。グループロールの詳細については、「アプリケーション脆弱性対応 のユーザーロールおよびロール」を参照してください。 • アプリセキュリティマネージャーグループは構成を監督し、期待される結果を検証します。

必要なロール：admin

このタスクについて

この SCA ツールは別のサブスクリプションとして利用できます。

手順

1. Vulnerability Response Integration with Black Duck をインストールするインスタンスにログインします。
2. ServiceNow Store に移動します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. ServiceNow Store で、Black Duck アプリケーションとの脆弱性対応統合を検索します。
4. アプリケーションタイルを選択します。
   インストールしているアプリケーションに関する詳細が表示されます。

   注:
   該当する場合は、[他の要件] および [依存関係] セクションを読むことを検討してください。

5. [アプリを要求] を選択して、Now Support ログイン認証情報を入力します。
6. [取得] を選択します。
7. [インスタンス名] と [インスタンスの理由] を入力し、[インスタンスを検証 **(Validate Instance)**] を選択します。
8. [要求] を選択します。
   詳細なインストール手順が記載されたメールが届きます。
9. 次のように移動する。 システムアプリケーション > アプリケーション.
10. アプリケーションを見つけて選択し、[インストール] を選択します。
    アプリケーションはインスタンスへ自動的にインストールされます。

次のタスク
環境に Vulnerability Response Integration with Black Duck を構成します。「Vulnerability Response Integration with Black Duckの構成」を参照してください。

Vulnerability Response Integration with Black Duckの構成

インスタンスで Vulnerability Response Integration with Black Duck を実行する前に、Black Duck ソフトウェア構成分析 (SCA) ツールがアプリケーション脆弱性対応アプリケーションと適切に統合されるように、インストールと構成の手順を完了する必要があります。

始める前に
必要なロール：アプリセキュリティマネージャーユーザーグループ

このタスクについて
Vulnerability Response Integration with Black Duck は別のサブスクリプションとして利用できます。

手順

1. 次のように移動する。 **All** (すべて) > **Blackduck** 脆弱性統合 > 構成.
2. [ベーシック認証] タイプを選択します。
   ベーシック認証には、オンプレミスインスタンス用の MID サーバーが必要です。ベーシック認証に必要な API トークンは、Black Duck アカウントから生成できます。
3. フォームのフィールドに入力します。
   ベーシック認証

フィールド	説明
API URL	エンタープライズまたはオンプレミスのインスタンスの Black Duck API URL。オンプレミスインスタンスは、Black Duck エンドポイント URL です。
API トークン	Black Duck コンソールから生成したトークン。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
MID サーバー	ベーシック認証用のオンプレミスのインスタンスに必要な MID サーバー。
SCA を含める	デフォルトで含まれているソフトウェア構成分析 (SCA) スキャンからの脆弱性。SCA スキャンは、オープンソースコンポーネントの脆弱性を特定します。
ServiceNow で誤検出を管理するオプションを選択します。	誤検出を管理する ServiceNow のオプション。[ソース] ステータスが誤検出または潜在的な誤検出としてマークされている、インポートされたアプリケーションの脆弱性一致アイテム (AVI) をトリアージする場合は、このオプションを有効のままにします。 通常はインスタンスで [ソース] 状況にマッピングされる [クローズ済み] 状況を持つ AVI は、代わりに [オープン] にマッピングされます。 AVI レコードから誤検出を要求できます。 ○ スキャナーからインポートされた [ソース] ステータスを保持する場合は、いずれかまたは両方のオプションを非アクティブにします。 ○ 非アクティブにすると、例外の要求と誤検出のアクションは、AVI には表示されません。
統合インスタンス	データのインポートに使用しているインスタンス。

4. [認証情報を保存してテスト] を選択します。
5. 他の統合を実行する前に、**[Black Duck** プロジェクトリスト統合 **(Black Duck Project List Integration)]** を実行します。
   Black Duck アプリケーションリスト統合や Black Duck アプリケーション脆弱性一致アイテム統合など、その他の Black Duck 統合は、プロジェクトリスト統合からインポートした現在のプロジェクトおよびアプリケーションデータに依存します。

Vulnerability Response Integration with Black Duck インポート実行ステータスの表示

[脆弱性統合実行] 関連リストを表示して、統合実行の成功を確認し、問題を特定して、修復の決定を通知します。

始める前に
必要なロール：admin

手順
1. 次のように移動する。 **All** (すべて) > **Blackduck** 脆弱性統合 > 統合.
2. 統合を選択します。
3. [脆弱性統合実行] 関連リストを選択します。
4. すべてのインポートが成功したことを確認します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

トラブルシューティング：

実行が失敗した場合の一般的な原因は次のとおりです。

- ネットワークの中断。
- データ転送の問題による、変換中のデータ破損。

これらの条件のいずれかが発生した場合は、[今すぐ実行] を選択して統合を再実行します。

5. インポートされたリポジトリを表示するには、統合リストに移動し、Black Duck 統合レコードを選択します。
6. [脆弱性統合実行] 関連リストを選択し、レコードを開きます。

Vulnerability Response Integration with Black Duck のデータ変換

インポートするデータを特定すると、Vulnerability Response Integration with Black Duck からデータが取得され、一連のデータソースによって処理され、インスタンス内で変換されます。

Vulnerability Response Integration with Black Duck

API のデータは最初に Black Duck AppVul アイテムインポート [sn_vul_blackduck_appvul_item_import] テーブルにロードされ、Black Duck AppVul アイテム変換を使用してインポートされた情報が変換されます。

この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ をクリックし、「 **Black Duck AppVul Item Transform**」を検索します。次の表に、統合別の変換マップフィールドを示します。

Black Duck AppVul アイテム変換マップのフィールド

ソースフィールド	ターゲットフィールド	説明
app_id	source_app_id	アプリケーション ID
issueid	source_avit_id	AVIT ID
app_name	app_name	アプリケーション名。
version	app_version	アプリケーションのバージョン
build_id	source_scan_id	アプリケーションのビルド ID
account_id	account_id	アカウント ID
sandbox_id	sandbox_id	サンドボックス ID
last_update_time	last_scan_date	最終更新時間
app_name + last_scan_date	scan_summary_name	スキャンサマリー
life_cycle_stage	source_sdlc_status	ソース SDLC ステータス
level	source_severity	ソース重大度
category_name	category	カテゴリ
source_severity	source_severity	ソース重大度
category_id + " CWE-" + cweId	source_entry_id	ソースエントリー ID
source_vulnerability_summary	source_vulnerability_summary	ソース脆弱性のサマリー
source_recommendation	source_recommendation	ソースの推奨事項

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Black Duck AppVul アイテム変換マップのフィールド (続く)

ソースフィールド	ターゲットフィールド	説明
description	description	ソースの説明
description	source_vulnerability_explanation	ソース脆弱性の説明
mitigation_status_desc	source_mitigation_status	ソース緩和ステータス
remediation_status	source_remediation_status	ソース修復ステータス
line	line_number	欠陥が見つかった行
module	application_module	アプリケーションモジュール
sourcefile	source_notes	ソースメモ
affects_policy_compliance	complies_with_policy	値は、true または false のソース情報に基づいて [はい] または [いいえ] になります。
Sourcefilepath + sourcefile	場所	静的な欠陥の位置マッピング。
URL	場所	動的な欠陥の場所マッピング。
scope、type、exploitLevel	source_additional_info	静的な欠陥の場合にソースから値が入力される名前値フィールド。

次の表は、変換プロセス中に実行される変換スクリプトのリストです。

Black Duck 変換マップスクリプトのタイミングと目的

Black Duck 変換マップスクリプト

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を作成したとき)。	レコードを処理し、作成済み、更新済みまたは未変更のエンティティの数と、この統合の一部としてインポートされたエンティティの数を更新するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。
onBefore (インポートセットの変換が完了する前)。	無効で無視する必要があるレコードの動作を定義するために使用されるスクリプト。また、レコード処理のグローバルオブジェクトを定義するためにも使用されます。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

Black Duck 統合ステータスマッピング

Black Duck 脆弱性統合からのソースステータスと、インスタンス内のターゲットステータスを次の表に示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Black Duck ソースステータスとそれに対応する **Now Platform** ステータス

Black Duck ソースステータス	ソース状況の説明	**Now Platform** のターゲットステータス
新規	脆弱性はこのコンポーネントバージョンに影響します。	オープン
Needs Review (要レビュー)	脆弱性がこのコンポーネントバージョンに影響を与えるかどうかは判断できません。	オープン
修復が必要	このバージョンには修復が必要です。	オープン
修正が完了	この脆弱性の修復が完了しました。	クローズ済み
脅威緩和	脆弱性が緩和されました。	クローズ済み
パッチ済み	脆弱性にパッチが適用されました。	クローズ済み
無視	脆弱性は無視されました。	クローズ済み

Black Duck 統合インスタンスからのプロジェクト情報のインポート

Black Duck 統合インスタンスからプロジェクト情報をインポートして、脆弱性統合が順番に実行されるようにします。統合が成功すると、アプリケーション脆弱性一致アイテム (AVI) を特定して取り込むことができます。

始める前に

必要なロール：アプリセキュリティマネージャーグループ

このタスクについて

[sn_vul_blackduck_project] Black Duck プロジェクトテーブルの Vulnerability Response Integration with Black Duck からすべてのプロジェクト情報をインポートできます。プロジェクトの異なるバージョンをクエリするために必要なすべての必須属性 (プロジェクト GUID など) は、[sn_vul_blackduck_project] Black Duck プロジェクトテーブルにキャプチャされます。

手順

1. 次のように移動する。 **All** (すべて) > **Blackduck** 脆弱性統合 > 統合.
2. 統合を選択します。
   たとえば、**[Black Duck** プロジェクトリスト統合 **(Black Duck Project List Integration)]** を選択できます。
3. [今すぐ実行] をクリックします。

> **注:**
> 各 Vulnerability Response Integration with Black Duck は、最も完全なデータ検索を提供することを目的としています。これらの統合を順序どおりに実行しない場合、データが不完全になる可能性があり、ServiceNow およびアプリケーション脆弱性対応の専門知識が必要になります。

インポートが完了すると、[sn_vul_blackduck_project] Black Duck プロジェクトテーブルにプロジェクトの詳細が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. 統合実行状況については、「Vulnerability Response Integration with Black Duck インポート実行ステータスの表示」を参照してください。
5. オプション: 他の統合パラメーターを変更する場合は、統合インスタンスに移動する必要があります。

Vulnerability Response Integration with Black Duck プロジェクトバージョンを検出されたアプリケーションのテーブルにインポートする

Black Duck 脆弱性統合が順番に実行されるように、Vulnerability Response integration with Black Duck プロジェクトバージョンを検出されたアプリケーション [sn_vul_release] テーブルにインポートします。統合が成功すると、アプリケーション脆弱性一致アイテム (AVI) を特定して取り込むことができます。

始める前に
必要なロール：アプリセキュリティマネージャーグループ

このタスクについて
検出されたアプリケーション [sn_vul_release] テーブルの Vulnerability Response Integration with Black Duck から、インポートされたプロジェクトのすべての異なるバージョンを追加および表示できます (詳細は「Black Duck プロジェクト表」を参照)。

手順
1. 次のように移動する。 **All** (すべて) > **Blackduck** 脆弱性統合 > 統合 .
2. 統合を選択します。
   たとえば、**[Black Duck** アプリケーションリスト統合 **(Black Duck Application List Integration)]** を選択できます。
3. [今すぐ実行] をクリックします。

   注:
   統合のプロジェクトバージョンはそれぞれ、最も完全なデータ検索機能を提供することを目的としています。これらの統合を順序どおりに実行しない場合、データが不完全になる可能性があり、ServiceNow およびアプリケーション脆弱性対応の専門知識が必要になります。

   インポートが完了すると、検出されたアプリケーション [sn_vul_release] テーブルにプロジェクトのさまざまなバージョンが表示されます。CI ルックアップルールを使用している場合、これらの検出されたアプリケーションは構成アイテム [cmdb_ci] テーブルにリンクされます。
4. 統合実行のステータスを確認します。
   詳細については、「Vulnerability Response Integration with Black Duck インポート実行ステータスの表示」を参照してください。

Vulnerability Response Integration with Black Duck からアプリケーション脆弱性一致アイテムをインポートする

Vulnerability Response integration with Black Duck からアプリケーション脆弱性一致アイテム (AVI) をインポートして、統合が順番に実行されるようにします。統合が成功すると、AVI を特定して取り込むことが可能になります。

始める前に
必要なロール：アプリセキュリティマネージャーグループ

このタスクについて
Vulnerability Response Integration with Black Duck からスキャン結果を表示したり、インスタンスに AVI を挿入したり、サードパーティの脆弱性データを拡張させたりできます。デフォルトでは、スキャナーレコードがクローズ済みステータスの場合、AVI は作成されません。プロパティ sn_vul_create_closed を使用して、既存の AVI を制御できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 **All** (すべて) > **Black Duck** 脆弱性統合 > 統合.
2. 統合を選択します。
   たとえば、**[Black Duck** アプリケーション脆弱性一致アイテム統合 **(Black Duck Application Vulnerable Item Integration)]** を選択できます。
3. [今すぐ実行] をクリックします。

   注:
   この Vulnerability Response Integration with Black Duck は、最も完全なデータ検索を提供することを目的としています。これらの統合を順序どおりに実行しないと、不完全なデータになる可能性があります。ServiceNow および アプリケーション脆弱性対応 の専門知識が必要になります。

   Vulnerability Response Integration with Black Duck からすべての SCA 脆弱性をインポートすると、AVI とサードパーティ脆弱性データを表示できます。

Vulnerability Response Integration with Black Duck のインポート時間の設定

Vulnerability Response Integration with Black Duck インポートの開始時間を設定します。統合を前もって設定しておくと、パフォーマンスが向上し、インポートの実行が速くなります。

始める前に
必要なロール：アプリセキュリティマネージャーグループ

このタスクについて
最初のインポート後に、Black Duck 脆弱性統合の実行ごとに完全なインポートが実行されます。

手順

1. 次のように移動する。 **All** (すべて) > **Black Duck** 脆弱性統合 > 統合.
2. 統合を選択します。
3. 新しく [開始時間] を設定します。
   時間は現地時間で時間単位で計算されます。Black Duck アプリケーションリスト統合インポートのデフォルト時間は 00:00:00 です。他の統合はオンデマンドでチェーンされており、Black Duck アプリケーションリスト統合の後に実行されるシーケンスに従います。[開始時間] を変更するには、ServiceNow およびアプリケーション脆弱性管理の高度な専門知識が必要です。
4. [更新] を選択します。
   新しい時間は、次のスケジュール済みインポートに使用されます。

クローズ済み **Black Duck** アプリケーション脆弱性一致アイテムを含める

デフォルトでは、クローズ済みアプリケーション脆弱性一致アイテム (AVI) は統合インポート中に作成されないため、Black Duck 脆弱性一致アイテム統合インポート中にクローズされた AVI を含めます。作成する場合は、システムプロパティを変更する必要があります。

始める前に
Vulnerability Response Integration with Black Duck がインストールされ、実行されていることを確認します。

必要なロール：admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. ナビゲーションフィルターで、「sys_properties.list」と入力します。
2. リストの [名前] フィールドに、「sn_vul.create_closed」と入力します。
3. [値] フィールドをダブルクリックし、**[True]** に設定します。
4. 緑色のチェックマークアイコン ( ) を選択して保存します。
   次の Black Duck インポートで [クローズ済み] ステータスのレコードは、アプリケーション脆弱性対応に AVI として作成されます。

Fortify 脆弱性統合

Fortify 脆弱性統合 では、Fortify 製品からインポートしたデータを使用して、コードの欠陥の影響と優先度を判断できます。

Fortify 脆弱性統合

Fortify 製品はスキャナーデータを収集し、そのデータを Now Platform® で使用できるようにします。脆弱性対応 の ServiceNow アプリケーション脆弱性対応 機能と簡単に統合し、サードパーティ脆弱性をマッピングして、データをインスタンスに拡張します。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

スケジュール済みジョブにより、統合が毎日自動的に呼び出されます。すべての統合が有効になると、順番に実行されるように連結されます。スケジュール済みジョブを手動で実行することもできます。スケジュール済みジョブでは、インスタンスを他の脆弱性管理システムと同期させることで、脆弱性修復ライフサイクルを簡素化します。

利用可能バージョン

リリースバージョン	リリースノート
との脆弱性対応の統合 Fortify v2.4 Fortify v2.3 Fortify v2.2 Fortify v2.1	Application Vulnerability Response release notes 互換性情報については、「KB0856498 脆弱性対応 互換性マトリクスおよびリリーススキーマの変更」を参照してください。

Fortify 脆弱性統合

Fortify 脆弱性統合を表示するには、次に移動します: **Fortify** 脆弱性統合 > 統合.

ベースシステムには、次の統合が含まれています。デフォルトでは、これらの統合はすべて有効ではありません。

最初の実行後、毎日スケジュール済みジョブが連結され、統合が順番に自動的に実行されます。スケジュール済みジョブを手動で実行することもできます。スケジュール済みジョブでは、インスタンスを他の脆弱性管理システムと同期させることで、脆弱性修復ライフサイクルを簡素化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Fortify 脆弱性統合

統合	説明
Fortify オンデマンドアプリケーションリスト統合	Fortify アプリケーションスキャナーデータ (脆弱性、メタデータ) を取得し、サードパーティアプリケーションデータを拡張します。この統合は毎日 00:00:00 に実行するように設定されます。デフォルトでアクティブ化されます。
Fortify オンデマンドスキャンサマリー統合	Fortify からスキャンレコードを取得します。この統合が有効になると、Fortify オンデマンドアプリケーションリスト統合の後に実行されるように連結されます。これはデフォルトで非アクティブです。
Fortify オンデマンドアプリケーション脆弱性一致アイテム統合	Fortify からスキャン結果を取得し、AVIT を挿入して、サードパーティ脆弱性データを拡張します。スキャナーレコードが [クローズ済み] ステータスの場合、AVIT は作成されません。既存の AVIT は引き続き更新されます。 v2.3 以降では、アプリケーション脆弱性一致アイテム統合の合計処理時間、統合前後のプロセスの平均時間、統合実行レコードに関するレポートなどの詳細を表示できます。 この統合が有効になると、Fortify オンデマンドスキャンサマリー統合の後に実行されるように連結されます。これはデフォルトで非アクティブです。

統合実行状況については、「Fortify 脆弱性統合 インポート実行状況の表示」を参照してください。

サードパーティの脆弱性データを表示する方法については、「脆弱性ライブラリの表示」を参照してください。

Fortify 脆弱性統合 の準備

Fortify 脆弱性統合 を成功させるには、事前統合タスクを計画して慎重に実行する必要があります。これらのタスクを実行して、統合の準備をします。Fortify 脆弱性統合は、Fortify 製品と API に精通していることを前提としています。

始める前に

共通脆弱性タイプ一覧 (CWE) 統合は アプリケーション脆弱性対応 でも使用され、Fortify 脆弱性統合をインストールして構成する前に実行する必要があります。

注:
NIST 脆弱性データベース (NVD) データは Fortify 脆弱性統合 のインストールには必要ありませんが、拡張が提供されるので便利です。

NVD の詳細については、「NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理」を参照してください。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

必要なロール：アプリケーションセキュリティマネージャー

このタスクについて

注:
統合を実行する前に、要件に基づいて必要な構成変更を行います。

インポートする予定のアプリケーション脆弱性一致アイテムの数に基づいて、インスタンスのサイジングを検証します。インスタンスが小さすぎると、ロードに時間がかかることがあります。インスタンスのサイズがわからない場合は、カスタマーサービス & サポート にお問い合わせください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Fortify 脆弱性統合 には、 Fortify オンデマンドアカウントから利用可能な API キー、API シークレット、および API ルート URL が必要です。

手順

API シークレットキーを作成するには次のステップを実行します。

a. Fortify オンデマンドポータルにログインします。

b. 次のように移動する。 **All** (すべて) > アドミニストレーション > 設定 > **API**.

c. ServiceNow をアプリケーションとして追加します。

d. [新しいシークレット] をクリックして API シークレットを生成します。

e. 後で使用するために API シークレットを記録します。

ServiceNow® Vulnerability Response Integration with Fortify のインストール

インスタンスで統合を実行する前に、インストールと構成のステップを完了して、アプリケーション脆弱性対応 が Fortify 製品と適切に統合されるようにします。このアプリケーションは別のサブスクリプションとして利用できます。

始める前に

インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

セットアップタスク	説明
脆弱性対応 アプリケーションがインストールされ、アクティブ化されていることを確認します。	このアプリケーションがアクティブ化されていることを確認するには、次の場所に移動します サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応 のインストール」を参照してください。
インスタンスに必要な ServiceNow ロールがあることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。 • まだアサインされていない場合、システムアドミニストレーター [admin] はアプリケーションをインストールして、ユーザーをアプリケーションセキュリティマネージャーグループにアサインします。グループロールの詳細については、「アプリケーション脆弱性

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	対応 のユーザーロールおよびロール」を参照してください。 • アプリセキュリティマネージャーグループは構成を監督し、期待される結果を検証します。

必要なロール：アプリケーションセキュリティマネージャー

手順

1. Fortify 脆弱性統合 をインストールするインスタンスにログインします。
2. ServiceNow Store に移動します。
3. ServiceNow Store で、Vulnerability Response Integration with Fortify アプリケーションを検索します。
4. アプリケーションタイルをクリックします。
   インストールしているアプリケーションに関する詳細情報が表示されます。

   注:
   該当する場合は、[他の要件] および [依存関係] セクションを読むことを検討してください。

5. [アプリを要求] をクリックし、Now Support ログイン認証情報を入力します。
6. [取得] をクリックします。
7. [インスタンス名] と [インスタンスの理由] を入力し、[インスタンスを検証] をクリックします。
8. [要求] をクリックします。
   詳細なインストール手順が記載されたメールが届きます。
9. 次のように移動する。 システムアプリケーション > アプリケーション.
10. アプリケーションを見つけて選択し、[インストール] をクリックします。
    アプリケーションはインスタンスに自動でインストールされます。

次のタスク

環境に Fortify 脆弱性統合 を構成します。「Fortify 脆弱性統合 の構成」を参照してください。

Fortify 脆弱性統合 の構成

インスタンスで統合を実行する前に、インストールと構成のステップを完了して、脆弱性対応 の アプリケーション脆弱性対応 機能を Fortify 製品と適切に統合できるようにします。このアプリケーションは別のサブスクリプションとして利用できます。

始める前に

必要なロール：アプリケーションセキュリティマネージャー

インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
脆弱性対応 アプリケーションがインストールされ、アクティブ化されていることを確認します。	このアプリケーションがアクティブ化されていることを確認するには、次の場所に移動しますサブスクリプション管理 > サブスクリプションインスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応 のインストール」を参照してください。
脆弱性対応 Integration with Fortify アプリケーションがインストールされ、アクティブ化されていることを確認します。	このアプリケーションがアクティブ化されていることを確認するには、次の場所に移動しますサブスクリプション管理 > サブスクリプションインスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「ServiceNow Vulnerability Response Integration with Fortify のインストール」を参照してください。
インスタンスに必要な ServiceNow ロールがあることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。 • まだアサインされていない場合、システムアドミニストレーター [admin] はアプリをインストールして、ユーザーをアプリセキュリティマネージャーグループにアサインします。 • アプリセキュリティマネージャーは構成を監督し、期待される結果を検証します。
Fortify 脆弱性統合 の場合は、**API ID** と **API** キーを用意します。	Fortify に接続し、**API ID** と **API** キーを取得します。

手順

1. Fortify アプリケーション脆弱性統合をインストールするインスタンスにログインします
2. ServiceNow Store に移動します。
3. ServiceNow Store で、脆弱性対応 Integration with Fortify アプリケーションを検索します。
4. アプリケーションタイルをクリックします。
   インストールしているアプリケーションに関する詳細情報が表示されます。

   注:
   該当する場合は、[他の要件] および [依存関係] セクションを読むことを検討してください。

5. [アプリを要求] をクリックし、Now Support ログイン認証情報を入力します。
6. [取得] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

7. [インスタンス名] と [インスタンスの理由] を入力し、[インスタンスを検証] をクリックします。
8. [要求] をクリックします。
   詳細なインストール手順が記載されたメールが届きます。
9. 次のように移動する。 システムアプリケーション > アプリケーション.
10. アプリケーションを見つけて選択し、[インストール] をクリックします。
    アプリケーションはインスタンスへ自動的にインストールされます。
11. インストールが完了したら、次に移動します: **Fortify** 脆弱性統合 > **FoD** 構成.
12. フォームのフィールドに入力します。

Fortify オンデマンド構成フォーム

フィールド	説明
API ルート URL	ユーザーの Fortify インスタンス URL。
API キー	Fortify API に送信される一意の識別子。
API シークレット	Fortify で提供されるクライアントシークレット。
DAST を含める	DAST スキャンからの脆弱性を含めるオプション。DAST スキャンは、アプリケーション全体の動作から脆弱性を特定します。
SAST を含める	SAST スキャンからの脆弱性を含めるオプション。SAST スキャンはコードの脆弱性を特定します。
ServiceNow での例外と誤検出のトリアージ (脆弱性対応 v20.0 以降)	インポート時に自動的に ServiceNow ワークフローを使用して、AVI の例外管理と誤検出を管理するためのオプションを選択します。これらのオプションはデフォルトでアクティブ化されています。使用例については、「アプリケーション脆弱性対応での保留と誤検出のステータスマッピングの管理」を参照してください。 ServiceNow での例外の管理 [保留]ステータスとしてマークされたインポート済み AVI をトリアージする場合は、このオプションを有効のままにします。 通常はインスタンスで [保留] 状況にマッピングされる [ソース] 状況を持つ AVI は、代わりに [オープン] にマッピングされます。 AVI レコードから例外を要求します。 ServiceNow での誤検出の管理 インポートされた AVI を [ソース]状況が誤検出または潜在的な誤検出としてマークされている状態でトリアージする場合は、こ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	のオプションを有効のままにします。 通常はインスタンスで [ソース] 状況にマッピングされる [クローズ済み] 状況を持つ AVI は、代わりに [オープン] にマッピングされます。 AVI レコードから誤検出を要求します。 ○ スキャナーからインポートされた [ソース] ステータスが保持する場合は、いずれかまたは両方のチェックボックスをオフにします。 ○ これらの AVI は、インポート時に [ターゲットステータス] および [ターゲット理由 (Target reason)] ステータスにマッピングされますが、例外および誤検出ワークフローによってトリアージされません。例外の要求と誤検出アクションは、AVI には表示されません。
ServiceNow でのトリアージ (v20.0 より前の脆弱性対応の場合)	ServiceNow インスタンスでのアプリケーションの脆弱性トリアージを管理： ○ ServiceNow 内の AVI をトリアージするチェックボックスを選択します。このオプションを選択すると、AVI は [オープン] ステータスでインポートされます。その後、例外を要求するか、AVI を誤検出としてマークすることができます。 ○ ソースステータス、つまりスキャナーからインポートされたステータスを保持するには、このチェックボックスが選択されていないことを確認します。 **注:** [誤検出としてマーク] および [例外の要求] オプションは、ServiceNow 内でトリアージされる AVI でのみ使用できます。

13. [認証情報を保存してテスト] を選択します。

次のタスク
環境でドメインセパレーションインポートが必要な場合は、「統合のためのドメインセパレーションインポートの作成」を参照してください。

初期インストールの詳細については、「アプリケーション脆弱性対応 の構成」を参照してください。

初期インストール後の変更については、「Fortify 脆弱性統合 の変更とアクティビティ」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Fortify 脆弱性統合 インポート実行状況の表示

[脆弱性統合実行] 関連リストを使用して、統合実行の成功を確認し、問題を特定して、修復の決定を通知します。

始める前に

Fortify インポート実行状況を表示するには、次のステップを実行します。

- 脆弱性対応 と Fortify 脆弱性統合 アプリケーションをインストールして構成する必要があります。
- Fortify 脆弱性統合 インポートがスケジュールされ、実行されている必要があります。

必要なロール：アプリケーションセキュリティマネージャー

このタスクについて

統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、 アプリケーション脆弱性対応のバージョン 18.2.4 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

手順

1. 次のように移動する。 **All** (すべて) > **Fortify** 脆弱性統合 > 統合.
2. 統合を選択します。
3. [脆弱性統合実行] 関連リストをクリックします。
4. すべてのインポートが成功したことを確認します。
5. v2.3 以降では、アプリケーション脆弱性一致アイテム統合の合計処理時間、統合前後のプロセスの平均時間、統合実行レコードに関するレポートなどの詳細を表示できます。

Fortify 脆弱性統合 の変更とアクティビティ

Fortify 脆弱性統合 専用のオプションの変更を構成します。

注:
ここに記載されている以外の Fortify 脆弱性統合 の設定を変更するには、ServiceNow およびアプリケーション脆弱性対応 に関する高度な専門知識が必要であり、製品ドキュメントの範囲を超えています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手動 Fortify アプリケーション脆弱性インポートの実行

初期インポートに失敗した場合、またはスケジュールされた初期インポートを待ちたくない場合は、日次スケジュール済みジョブから独立して完全なデータインポートを実行できます。

始める前に
必要なロール：アプリケーションセキュリティマネージャー

手順

1. 次のように移動する。 **All** (すべて) > **Fortify** 脆弱性統合 > 統合.
2. Fortify アプリケーションリスト統合などの統合を選択します。
3. [今すぐ実行] を選択します。

> **注:**
> データを完全に取得するには、Fortify アプリケーションの脆弱性統合を順番に実行します。

Fortify 脆弱性統合 を使用したデータのインポート

Fortify スキャナーからデータをインポートしてアプリケーション脆弱性一致アイテム (AVI) をマッピングし、インスタンスのデータを拡張します。

始める前に
必要なロール：アプリケーションセキュリティマネージャー

このタスクについて
最初のインポート後、Fortify 脆弱性統合は実行するたびにデルタインポートを行い、最新のデータを取得します。完全インポートの詳細については、「手動 Fortify アプリケーション脆弱性インポートの実行」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > **Fortify** 脆弱性統合 > 統合.
2. 統合を選択します。
3. フォームのフィールドに入力します。

フィールド	説明
名前	統合実行の名前。
アクティブ	統合をアクティブ化するオプション。
実行	統合を実行する頻度。
時刻	
アプリケーション	このレコードを含んでいるアプリケーションです。
ソース統合	この統合のソース統合。
ソースインスタンス	この統合のソースインスタンス。
次の統合	シーケンス内の次の統合。現在の統合実行の後に実行します。
開始時間	前回成功した統合実行の開始日時。時間は現地時間で時間単位で計算されます。初期実行のデフォルト時間は 00:00:00 です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
統合の詳細	
統合スクリプト	統合の実行時に実行される *VulnerabilityIntegrationBase* を拡張するスクリプトインクルード。このスクリプトは、サードパーティシステムからデータを取得する方法を定義します。
統合ファクトリスクリプト	統合スクリプト用に選択されたスクリプトインクルードのビルド方法を定義するスクリプト。
プロセッサ戦略をレポート	統合の実行時に統合スクリプトによって返されたデータを処理するために使用する戦略。

4. [今すぐ実行] を選択して統合を実行します。

クローズ済み **Fortify** オンデマンドアプリケーション脆弱性一致アイテムを含める

デフォルトでは、[クローズ済み] アプリケーション脆弱性一致アイテム (AVIT) は、Fortify の脆弱性一致アイテム統合インポート中に作成されません。作成する場合は、システムプロパティを変更する必要があります。

始める前に
Fortify 脆弱性統合 がインストールされ、実行されている必要があります。

必要なロール：アプリケーションセキュリティマネージャー

手順

1. 左側のナビゲーションの [フィルターナビゲーター] テキストボックスに「sys_properties.list」と入力します。
2. リストの [名前] 検索ボックスに、「sn_vul.create_closed」と入力します。
3. [値] フィールドをダブルクリックし、**[True]** に設定します。
4. 緑色のチェックマークアイコン をクリックして保存します。
   次の Fortify インポートで [クローズ済み] ステータスのレコードは、アプリケーション脆弱性対応に AVIT として作成されます。

GitHub アプリケーション脆弱性統合

GitHub アプリケーション脆弱性統合 は、静的アプリケーションセキュリティテスト (SAST) およびソフトウェア構成分析 (SCA) データをインポートして、GitHub 環境のリポジトリで脆弱性アラートを表示するのに役立ちます。

GitHub アプリケーション脆弱性統合

GitHub アプリケーション脆弱性統合 はスキャナーデータを収集し、そのデータを Now Platform® で使用できるようにします。脆弱性対応のServiceNow® アプリケーション脆弱性対応機能と簡単に統合し、インスタンスのサードパーティ脆弱性と GitHub アラートをマッピングします。

GitHub 環境は複数の組織をサポートしています。これらの組織には、オンプレミスとエンタープライズの両方に、エンジニアリング、品質、ドキュメントなどのさまざまな部門が含まれている場合があります。また、各組織は複数のリポジトリをサポートできます。GitHub リポジトリ統合を使用してアプリケーションデータをインポートした後、これらのリポジトリから脆弱性とアラートのデータをインポートできます。インポートされたデータは、アプリケーション脆弱性対応アプリケーション

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

内でアプリケーションと同様に処理されます。スキャナーが脆弱性を検出し、リポジトリのアラートを生成すると、アプリケーション脆弱性対応に脆弱性が作成されます。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

利用可能バージョン

リリースバージョン	リリースノート
GitHub アプリケーション脆弱性統合 v1.2、v1.1、1.0	Application Vulnerability Response release notes 互換性情報については、「KB0856498 脆弱性対応互換性マトリクスおよびリリーススキーマの変更」を参照してください。

GitHub の統合

統合	説明
GitHub組織の統合	この統合により、GitHub の構成中にリストされた特定のエンタープライズに属する組織がインポートされます。すべての組織は、このリリースで導入された「sn_vul_discovered_org」(検出された組織) テーブルに入力されます。 この統合は、エンタープライズレベルの API をサポートしています。
GitHub リポジトリ統合	v1.1 以降では、GitHub オンプレミスアカウントとクラウド (エンタープライズ) アカウントのすべてのアプリケーションデータをインポートします。統合では、組織 (オンプレミス) またはエンタープライズ (クラウド) 環境に設定したリポジトリからアプリケーションがインポートされます。 他の GitHub 統合は、リポジトリ統合からインポートされた現在のアプリケーションデータに依存するため、実行する前にこの統合を実行します。
GitHub CodeScan 統合	GitHub リポジトリからセキュリティ脆弱性とコーディングエラーのコードスキャン脆弱性アラートを取得します。インポートされたデータは、インスタンスの SAST 結果にマッピングされます。
GitHub Dependabot 統合	既知の脆弱性がある依存関係の Dependabot アラートをリポジトリから取得します。インポートされたデータは、インスタンスの SCA 結果にマッピングされます。
GitHub シークレットスキャン	アプリケーションセキュリティテストの結果とともに、組織のコードからシークレットを取得します。データはインスタンスの SCA 結果にマッピングされます。
GitHub シークレットスキャンロケーション	組織のコード内のスキャンされたシークレットの場所と行番号を取得して、開発者の修復に役立てます。

GitHub リポジトリから Now Platform® への SBOMファイルのアップロード

CI/CD (継続的統合および継続的デリバリ/展開) パイプラインで生成された SBOM ファイルが、Now Platform　インスタンスで正常にキューに入れられているかどうかを確認します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- GitHub 環境から開始する GitHub アクションを使用して、ソフトウェア開発サイクル中に潜在的に有害なコンポーネントから環境を保護します。
- GitHub マーケットプレイスで SBOM アップロードに必要な GitHub アクションを取得します。

SBOM ファイルをアップロードするには、SBOM アプリケーションが必要です。詳細については、「ソフトウェア部品表 の詳細」を参照してください。

インポートされたデータの表示

GitHub リポジトリ統合からインポートされたアプリケーションデータは、検出されたアプリケーション [sn_vul_app_release] テーブルに表示されます。最初にこの統合を実行します。

リポジトリ統合は、[設定] メニューから GitHub アカウントのリポジトリに設定したタグとトピックをインポートします。カスタムプロパティは、リポジトリの下のメニューにあります。プロパティに設定した値は、キーと値のペアとしてインポートされます。インスタンス内でこの情報を表示する場所の詳細については、「GitHub アプリケーション脆弱性統合 インポートの実行ステータスとインポートされたリポジトリデータを表示する」を参照してください。

GitHub Dependabot 統合からインポートされたデータ (検出結果) は、次のテーブルに表示されます。

- 検出されたアプリケーション [sn_vul_app_release]
- アプリケーション脆弱性のスキャンサマリー [sn_vul_app_vul_scan_summary]
- アプリケーション脆弱性一致アイテム [sn_vul_app_vulnerable_item]
- パッケージ [sn_vul_app_package]

GitHub CodeScan 統合からインポートされたデータは、次のテーブルに表示されます。

- 検出されたアプリケーション [sn_vul_app_release]
- アプリケーション脆弱性のスキャンサマリー [sn_vul_app_vul_scan_summary]
- アプリケーション脆弱性エントリ [sn_vul_app_vul_entry]
- アプリケーション脆弱性一致アイテム [sn_vul_app_vulnerable_item]

GitHub アプリケーション脆弱性統合 の準備

これらのタスクを実行して、統合の準備をします。GitHub アプリケーション脆弱性統合は、GitHub 製品と API に精通していることを前提としています。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

必要なロール：

- アプリケーションのダウンロード、インストール、アクティブ化、およびロールのアサインを行うアドミン。
- GitHub コンソールで認証情報を取得してトークンを生成する GitHub アドミニストレーター。
- インスタンスで接続とエイリアスレコードを設定するアドミン。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク

セットアップタスク	説明
脆弱性対応 アプリケーションがインストールされ、アクティブ化されていることを確認します。	このアプリケーションがアクティブ化されていることを確認するには、次の場所に移動します サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応 のインストール」を参照してください。
GitHub アプリケーション脆弱性統合 がインストールされ、アクティブ化されていることを確認します。	このアプリケーションがアクティブ化されていることを確認するには、次の場所に移動します サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「ServiceNow GitHub アプリケーション脆弱性統合 をインストールする」を参照してください。
インスタンスに必要な ServiceNow ロールがあることを確認します。	期待される結果を構成および検証するには、次のロールが必要です。 • まだアサインされていない場合、システムアドミニストレーター [admin] はアプリをインストールして、ユーザーをアプリセキュリティマネージャーユーザーグループにアサインします。 • アプリセキュリティマネージャーは構成を監督し、期待される結果を検証します。 • sn_vul_github_config_integration は、アプリセキュリティマネージャーユーザーグループに継承されます。このロールには、connection_admin ロールと oauth_admin ロールが含まれています。
GitHub の認証情報とアカウント情報を取得します。	認証用に作成するレコードには、アカウント情報が必要です。OAuth 認証に必要な詳細と必要なレコードの設定については、「GitHub アプリの OAuth 2.0 認証情報の作成 - GitHub アプリケーション脆弱性統合 用の JWT」を参照してください。
共通脆弱性タイプ一覧 (CWE) データをインポートしていることを確認します。	共通脆弱性タイプ一覧 (CWE) 統合はアプリケーション脆弱性対応でも使用され、GitHub 脆弱性統合をインストールして構成する前に実行する必要があります。脆弱性対応 では、デフォルトでインストールされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク (続く)

セットアップタスク	説明
	注: NIST 脆弱性データベース (NVD) データは、GitHub 脆弱性統合のインストールには必要ありませんが、拡張が提供されるので便利です。NVD の詳細については、「NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理」を参照してください。

GitHub アプリの OAuth 2.0 認証情報の作成 - GitHub アプリケーション脆弱性統合 用の JWT

GitHub アプリケーション脆弱性統合 用の JWT ベアラートークンを使用して、GitHub アプリを統合するには、次の手順を実行します。

必要なロール：

- sn_vul.app_sec_manager および admin (Now Platform 内のレコード)。
- GitHub アカウントのタスクに必要なインスタンスロールはありません。
- このセットアップの手順のコンテキストの詳細については、「 OAuth 2.0 プロトコル 」を参照してください。

GitHub アプリケーション脆弱性統合 用の GitHub アプリの作成および構成

GitHub アカウントからカスタム GitHub アプリを作成し、インスタンスの GitHub アプリケーション脆弱性統合 で OAuth 2.0 認証をアクティブ化にします。

始める前に

必要なロール：インスタンスロールは不要

このタスクについて

GitHub アカウントから、次の手順を完了します。「」を参照してください。 建物 GitHub アプリ
カスタムアプリケーションを作成および構成する方法については、 GitHub Developer サイトのページを参照してください。

手順

1. GitHub アカウントから、次の場所に移動して GitHub アプリを作成します 開発者設定 > **GitHub** アプリ.
2. [ホームページ **URL (Homepage URL)**] フィールドに「https://<instance-name>.service-now.com」と入力します。
3. [ユーザー認証コールバック **URL (User authorization callback URL)**] フィールドに、「https://<instance-name>.service-now.com/oauth_redirect.do」と入力します。
4. [ユーザーの識別と認証 **(Identifying and authorizing users)**] セクションで、[ユーザー認証トークンの有効期限 **(Expire user authorization tokens)**] フィールドの選択を解除します。
5. **[Webhook]** セクションで、[アクティブ] フィールドを選択します。
6. **[Webhook URL]** フィールドに「https://<instance-name>.service-now.com/」と入力します。
7. 残りのフィールドは空のままにします (デフォルト)。
8. [リポジトリの権限 **(Repository permissions)**] セクションで、次の設定を構成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コードスキャン	読み込み専用
コンテンツ	読み込み専用
カスタムプロパティ	読み込み専用
Dependabot アラート	読み込み専用
メタデータ	読み取り専用
シークレットスキャンアラート	読み取り専用

注:
すでに GitHub アプリを使用していて、いずれかの権限を更新する場合は、GitHub アプリのそれらの権限を確認して受け入れる必要があります。アプリに移動して、[構成] > [レビュー要求] > [新しい権限を承認 **(Accept new permissions)**] を選択できます。

9. 残りの権限は [アクセスなし] (デフォルト) のままにします 。
10. [イベントのサブスクライブ **(Subscribe to events)**] セクションで、[展開保護ルール **(Deployment protection rule)**] オプションを選択します。
11. ヘッダーを右クリックして、変更を保存します。
12. 新しく作成した GitHub アプリを選択したアカウントにインストールします。

    a. GitHub アプリの設定ページからアプリを選択します。

    b. 左のサイドバーで、[アプリのインストール **(Install App)**] を選択します。

    c. 正しいリポジトリを含む組織または個人アカウントの横にある [インストール] を選択します。

    d. すべてのリポジトリまたは選択したリポジトリにアプリをインストールします。
    詳細については、「GitHub アプリのインストール」を参照してください。

13. インストール後、アプリの設定 (歯車アイコン) を選択し、次の情報を書き留めるかメモします。

    これらの詳細は、Now Platform インスタンスでアプリケーションレジストリを作成するときに必要です。

    - アプリ ID
    - クライアント ID
    - クライアントシークレット。
    - URL のトークンをメモします。これは、インスタンスのトークン URL に入力するトークン ID です。

14. ページを下にスクロールし、新しい秘密鍵を生成してマシンに保存します。

GitHub アプリケーション脆弱性統合 の JKS 証明書を生成する

GitHub アプリケーション脆弱性統合 の JWT 認証用に JKS 証明書を生成します。

始める前に
.jks ファイルの生成に使用するパスワード (KeyStore パスワード) を書き留めておく必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

必要なロール：sn_vul.app_sec_manager

手順

1. GitHub アプリの秘密鍵を使用して、CA 署名済み証明書を作成します。

```
openssl req -new -x509 -key <file-name>.pem -out <certificate-name>.pem -days 1095
```

2. 必要な詳細を入力します。
3. GitHub アプリの秘密鍵と CA 署名済み証明書を使用して、PKCS 12 ファイルを作成します。

```
openssl pkcs12 -export -in <certificate-name>.pem -inkey <file-name>.pem -certfile
 <certificate-name>.pem -out <PKCS-12-file-name>.p12
```

4. エクスポートパスワードを入力します。
5. JKS ファイルを作成します。

```
keytool -importkeystore -srckeystore <PKCS-12-file-name>.p12 -srcstoretype pkcs12
 -destkeystore <JKS-certificate-filename>.jks -deststoretype JKS
```

6. 宛先とソースのキーストアのパスワードを入力します。

GitHub アプリケーション脆弱性統合 のインスタンスに GitHub Java キーストア証明書を添付する

有効な GitHub Java KeyStore (JKS) 証明書をインスタンスに添付して、JWT ベアラー権限許可トークン認証をアクティブ化します。

始める前に
有効な Java キーストア証明書。

必要なロール：sn_vul.app_sec_manager

手順

1. 次のように移動する。 **All** (すべて) > システム定義 > 証明書.
2. **[New** (新規)] を選択します。
3. フォームのフィールドに入力します。

X.509 証明書フォームのフィールド

フィールド	説明
名前	レコードを一意に識別する名前。たとえば、My GitHub App Certificate for AVR などです。
有効期限切れを通知する	証明書の有効期限が切れたときに通知するユーザーを指定するオプション。
有効期限切れ前に警告	証明書の有効期限が切れる前に通知を送信する日数。
アクティブ	証明書を有効にするオプション。
タイプ	証明書のタイプを選択するオプション。**[Java** キーストア] を選択します。
数日中に期限切れ	証明書の有効期限が切れるまでの日数。
キーストアパスワード	証明書に関連付けられたパスワード (ヒント：以前に作成した宛先キーストアのパスワード)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
簡単な説明	証明書の概要です。

4. 添付ファイルのアイコンを選択し、JKS 証明書を添付します。
5. [ストア/証明書を検証] を選択します。
   有効な証明書ファイルに対して「有効な key_store」メッセージが表示されます。

GitHub アプリケーション脆弱性統合 の GitHub JKS 証明書の JWT 署名キーを作成する

GitHub Java KeyStore 証明書にアサインする JSON Web トークン (JWT) 署名キーを作成します。

始める前に
必要なロール：

- admin
- sn_vul.app_sec_manager

手順

1. 次のように移動する。 **All** (すべて) > システム **OAuth** > **JWT** キー.
2. **[New** (新規)] を選択します。
3. フォームのフィールドに入力します。

JWT キーフォームのフィールド

フィールド	説明
名前	JWT 署名キーを一意に識別する名前です。例：My GitHub App JWT Key for AVR。
署名キーストア	前のタスクで添付された有効な JKS 証明書を選択します。
キー ID	このフィールドは空白のままにします。
署名アルゴリズム	この値は RSA 256 のままにします。
署名キーパスワード	署名キーに関連付けられたパスワード。これは、JKS ファイルの生成に使用したパスワードです。
アクティブ	キーを有効にするオプション。

4. ページの灰色のヘッダー内の任意の場所を右クリックして、[保存] を選択します。

GitHub アプリケーション脆弱性統合 の GitHub 署名キーの JWT プロバイダーを作成する

GitHub の ServiceNow インスタンスに JSON Web トークン (JWT) プロバイダーを追加します。

始める前に
必要なロール：

- admin
- sn_vul.app_sec_manager

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > システム **OAuth** > **JWT** プロバイダー.
2. **[New** (新規)] を選択します。
3. フォームのフィールドに入力します。

JWT プロバイダーフォームのフィールド

フィールド	説明
名前	JWT プロバイダーを一意に識別する名前。例：My GitHub App JWT Provider for AVR。
有効期限の間隔 (秒)	JWT プロバイダートークンの有効期間を設定する秒数。この設定はデフォルトのままにしておくことができます。
署名構成	前の手順で作成した JWT キーを選択します。

4. フォームヘッダーを右クリックし、[保存] を選択します。
5. [標準要求] 関連リストに、**iss** 要求の値の GitHub アプリのアプリ **ID** を入力します。
   これは、前の手順で作成した GitHub コンソールの GitHub アプリのアプリ ID です。
6. **aud** と **sub** の値は空白のままにします (デフォルト)。
7. フォームヘッダーを右クリックし、[保存] を選択します。

GitHub を **GitHub** アプリケーション脆弱性統合 の **OAuth** プロバイダー **(JWT)** として登録する

GitHub アプリアカウントの構成中に生成された情報を使用し、GitHub を OAuth プロバイダーとして登録して、インスタンスが OAuth 2.0 トークンを要求できるようにします。

始める前に
必要なロール：

- admin
- sn_vul.app_sec_manager

手順

1. 次のように移動する。 **All** (すべて) > システム **OAuth** > アプリケーションレジストリー.
2. **[New** (新規)] を選択します。
   「**OAuth** アプリケーションの種類は？」というメッセージが表示されます。
3. [サードパーティ **OAuth** プロバイダーに接続します] を選択します。
4. フォームのフィールドに入力します。

アプリケーションレジストリフォームのフィールド

フィールド	説明
名前	レコードを一意に識別する名前。たとえば、My GitHub App Provider for AVR と入力します。
クライアント ID	GitHub アプリのクライアント ID です。クライアント ID は、前の手順で作成した GitHub コンソールの GitHub アプリケーションから取得されます。この ID は、GitHub の GitHub アプリ構成の [バージョン情報] セクションで利用できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

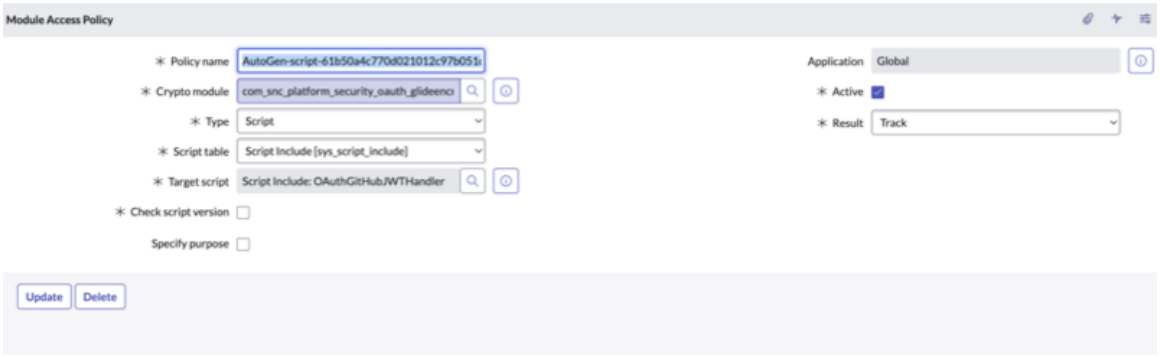
フィールド	説明
アクセス可能	この設定は現在の値のままにします。
クライアントシークレット	GitHub アプリのクライアントシークレットです。クライアントシークレットは、前の手順で作成した GitHub コンソールの GitHub アプリケーションから取得されます。この ID は、GitHub の GitHub アプリ構成の [バージョン情報] セクションで利用できます。
アクティブ	キーを有効にするオプション。これを選択したままにしておきます。
認証 URL	この URL は自動的に生成されます。
トークン URL	トークンを取得および更新するためにインスタンスが使用するトークンエンドポイントの場所。GitHub アプリの URL からトークンを入力します。これは、アプリが GitHub にインストールされた後に URL に表示されるトークンです。GitHub の GitHub アプリ構成の [アプリのインストール (Install App)] セクションから、歯車を選択します。トークンは Web ページの URL に表示されます。 ○ クラウドの場合：https://api.github.com/app/installations/49374672/access_tokens 。インストール ID：9374672。 ○ オンプレミスの場合：https://github-372.secops-eng.com/api/v3/app/installations/7/access_tokens/api/v3 。
OAuth API スクリプト	修正済み OAuthUtil スクリプトインクルードを参照できるようにするオプション。**[OAuthGitHubJWTHandler]** を選択します。
デフォルトの権限許可タイプ	アプリケーションレジストリに関連付けられた権限許可のタイプ。**[JWT** ベアラー] を選択します。

5. フォームの残りのフィールドはデフォルトのままにします。
6. フォームヘッダーを右クリックし、[保存] を選択します。
7. **[OAuth** エンティティプロファイル] 関連リストまでスクロールして選択し、リストに作成されたデフォルトプロファイルを開きます。
8. 以前に作成した JWT プロバイダーを **[JWT** プロバイダー] フィールドに入力し、フォームを保存します。
9. アプリケーションレジストリファイルに戻り、保存します。
10. 次のように移動する。 キー管理 > モジュールアクセスポリシー > **All** (すべて).
11. ポリシーを選択して、[com_snc_platform_security_oauth_glideencrypter] が [暗号化モジュール] フィールド値として表示され、[OAuthGitHubJWTHandler] が [ターゲットスクリプト] フィールドの [スクリプトインクルード] になるようにします。

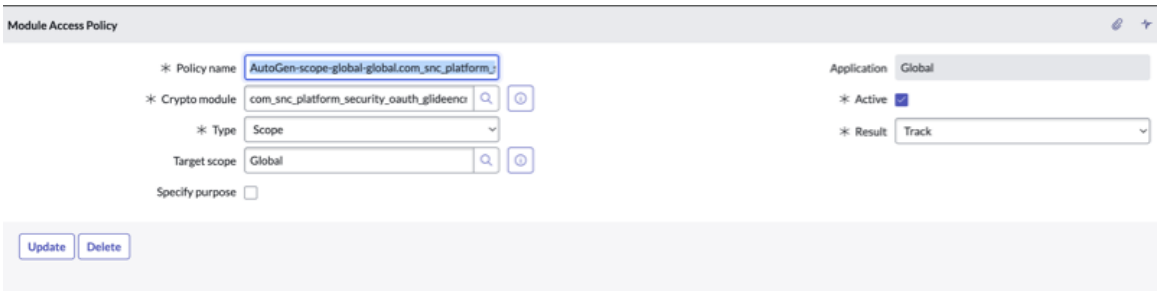
    次の画像では、[暗号化モジュール] フィールドの値としてcom_snc_platform_security_oauth_glideencrypterが選択されています。[スクリプトテーブル] フィールドに はスクリプトインクルード [sys_script_include] テーブルが表示され、[ターゲットスクリプト] フィールド値は OAuthGitHubJWTHandler です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳



12. [**Update** (更新)] を選択します。



前の画像に示すように、[ポリシー名] フィールドの値が変更され、[スクリプトテーブル] フィールドと [ターゲットスクリプト] フィールドが表示されなくなります。

13. [結果] フィールドが [追跡] に設定されていることを確認し、変更を保存します。

GitHub アプリケーション脆弱性統合 の認証情報と接続を作成する

アクションを許可するために、以前に作成した GitHub アプリプロバイダーに認証情報レコードを作成します。

始める前に

必要なロール：

- admin
- sn_vul.app_sec_manager

手順

1. 次のように移動する。 資格情報と接続 > 認証情報.
2. **[New** (新規)] を選択します。
3. **[OAuth 2.0** 認証情報] を選択します。
4. [新規] を選択し、フィールドに入力します。
5. ページのヘッダー内の任意の場所を右クリックして、[保存] を選択します。
   [認証情報] リストが表示されます。
6. 作成したレコードを開き、**[OAuth** トークンの取得] 関連リンクを選択します。
   OAuth トークンが正常にインポートされた旨の確認メッセージが表示されます。
7. 次のように移動する。 資格情報と接続 > 接続.
8. **[New** (新規)] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

9. **[HTTP(s)** 接続] を選択します。
10. [新規] を選択し、フィールドに入力します。
11. [送信] を選択します。
    [接続および資格情報エイリアス] リストが表示されます。
12. レコードを開き、[接続] 関連リストタブで [新規] を選択し、HTTP 接続レコードのフィールドに入力します。
13. [送信] を選択します。
    [接続および資格情報エイリアス] リストが表示されます。これで、「GitHub アプリケーション脆弱性統合 の構成」の手順を完了する準備ができました。[接続] フィールドに、前の手順で作成した認証情報を入力します。

ServiceNow® GitHub アプリケーション脆弱性統合 をインストールする

インスタンスで統合を実行する前に、インストールと構成のステップを完了して、GitHub アプリケーション脆弱性統合 が アプリケーション脆弱性対応 と適切に統合されるようにします。このアプリケーションは別のサブスクリプションとして利用できます。

始める前に
必要なロール：admin

手順

1. GitHub アプリケーション脆弱性統合 をインストールするインスタンスにログインします。
2. ServiceNow Store に移動します。
3. ServiceNow Store で、GitHub アプリケーション脆弱性統合 アプリケーションを検索します。
4. アプリケーションタイルを選択します。
   インストールしているアプリケーションに関する詳細情報が表示されます。

   注:
   該当する場合は、[他の要件] および [依存関係] セクションを読むことを検討してください。

5. [アプリを要求] を選択して、Now Support ログイン認証情報を入力します。
6. [取得] を選択します。
7. [インスタンス名] と [インスタンスの理由] を入力し、[インスタンスを検証] を選択します。
8. [要求] を選択します。
   詳細なインストール手順が記載されたメールが届きます。
9. 次のように移動する。 システムアプリケーション > アプリケーション.
10. アプリケーションを見つけて選択し、[インストール] を選択します。
    アプリケーションはインスタンスに自動でインストールされます。

GitHub アプリケーション脆弱性統合 の構成

インスタンスで統合を実行する前に、インストールと構成のステップを完了して、アプリケーション脆弱性対応が GitHub 製品と適切に統合されるようにします。このアプリケーションは別のサブスクリプションとして利用できます。

始める前に
必要なロール：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- アプリセキュリティマネージャーグループ
- OAuth の設定に必要な sn_vul.app_sec_manager

手順

1. 次のように移動する。 **All** (すべて) > **GitHub** 脆弱性統合 > 構成.
2. 認証タイプで [ベーシック認証] または **[OAuth]** を選択します。
   - ベーシック認証には、オンプレミスインスタンス用の MID サーバーが必要です。GitHub アカウントからベーシック認証に必要な API トークンを生成します。
   - OAuth には、「GitHub アプリの OAuth 2.0 認証情報の作成 - GitHub アプリケーション脆弱性統合 用の JWT」で説明されている OAuth アプリ、認証情報、接続の設定が必要です。
3. 選択したタイプに基づいてフィールドに入力します。
   ベーシック認証

フィールド	説明
API URL	Enterprise またはオンプレミスの適切な GitHub API URL。デフォルトの URL は https://api.github.com です。オンプレミスは GitHub エンドポイント URL です。
API トークン	GitHub コンソールから生成したトークン。
API タイプ	1 つ選択： 組織 特定の組織のデータを名前でインポートする場合は、このオプションを選択します。GitHub 環境は複数の組織をサポートしています。各組織は複数のリポジトリをサポートできます。組織を入力すると、その組織のデータのみがインポートされます。 Enterprise Enterprise 環境は複数の組織をサポートしています。Enterprise (クラウド) 環境内のすべての組織から脆弱性データをインポートする場合は、このオプションを選択します。
組織名	GitHub リポジトリの名前。入力した組織のデータのみがインポートされます。
MID サーバー	ベーシック認証のオンプレミスインスタンス用の MID サーバーが必要です。
例外管理と誤検出を管理するには、オプションを選択します。	インポート時に自動的に ServiceNow ワークフローを使用して、アプリケーション脆弱性一致アイテム (AVI) の例外管理と誤検出を管理するためのオプションを選択します。 ServiceNow での例外の管理

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	[保留]ステータスとしてマークされたインポート済み AVI をトリアージする場合は、このオプションを有効のままにします。 通常はインスタンスで [保留] 状況にマッピングされる [ソース] 状況を持つ AVI は、代わりに [オープン] にマッピングされます。 AVI レコードから例外を要求します。 ServiceNow での誤検出の管理 インポートされた AVI を [ソース]状況が誤検出または潜在的な誤検出としてマークされている状態でトリアージする場合は、このオプションを有効のままにします。 通常はインスタンスで [ソース] 状況にマッピングされる [クローズ済み] 状況を持つ AVI は、代わりに [オープン] にマッピングされます。 AVI レコードから誤検出を要求します。 ○ スキャナーからインポートされた [ソース] ステータスを保持する場合は、いずれかまたは両方のチェックボックスをオフにします。 ○ 非アクティブにすると、例外の要求と誤検出アクションは、AVI には表示されません。
統合インスタンス	データをインポートするインスタンス。

OAuth

フィールド	説明
API URL	Enterprise またはオンプレミスの適切な GitHub API URL。デフォルトの URL は https://api.github.com です。オンプレミスは GitHub エンドポイント URL です。
接続	作成した接続は「GitHub アプリの OAuth 2.0 認証情報の作成 - GitHub アプリケーション脆弱性統合 用の JWT」に記載されています。
API タイプ	1 つ選択： 組織

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	特定の組織のデータを名前でインポートする場合は、このオプションを選択します。GitHub 環境は複数の組織をサポートしています。各組織は複数のリポジトリをサポートできます。組織を入力すると、その組織のデータのみがインポートされます。 Enterprise Enterprise 環境は複数の組織をサポートしています。Enterprise (クラウド) 環境内のすべての組織から脆弱性データをインポートする場合は、このオプションを選択します。 注: GitHub アプリはエンタープライズレベルの API をサポートしていません。
組織名	GitHub リポジトリの組織名。入力した組織内のリポジトリからのデータのみがインポートされます。
例外管理と誤検出を管理するには、オプションを選択します。	インポート時に自動的に ServiceNow ワークフローを使用して、アプリケーション脆弱性一致アイテム (AVI) の例外管理と誤検出を管理するためのオプションを選択します。 ServiceNow での例外の管理 [保留]ステータスとしてマークされたインポート済み AVI をトリアージする場合は、このオプションを有効のままにします。 通常はインスタンスで [保留] 状況にマッピングされる [ソース] 状況を持つ AVI は、代わりに [オープン] にマッピングされます。 AVI レコードから例外を要求します。 ServiceNow での誤検出の管理 インポートされた AVI を [ソース]状況が誤検出または潜在的な誤検出としてマークされている状態でトリアージする場合は、このオプションを有効のままにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	通常はインスタンスで [ソース] 状況にマッピングされる [クローズ済み] 状況を持つ AVI は、代わりに [オープン] にマッピングされます。 AVI レコードから誤検出を要求します。 ○ スキャナーからインポートされた [ソース] ステータスを保持する場合は、いずれかまたは両方のチェックボックスをオフにします。 ○ 非アクティブにすると、例外の要求と誤検出アクションは、AVI には表示されません。

4. [認証情報を保存してテスト] を選択します。
5. 他の統合を実行する前に、GitHub リポジトリ統合を実行します。
   他の GitHub 統合は、リポジトリ統合からインポートされた現在のアプリケーションデータに依存します。リポジトリ統合からのデータは、検出されたアプリケーション [sn_vul_app_release] テーブルに保存されます。詳細については、「GitHub アプリケーション脆弱性統合 インポートの実行ステータスとインポートされたリポジトリデータを表示する」を参照してください。

GitHub アプリケーション脆弱性統合 インポートの実行ステータスとインポートされたリポジトリデータを表示する

[脆弱性統合実行] 関連リストを使用して、統合実行の成功を確認し、問題を特定して、修復の決定を通知します。

始める前に
必要なロール：sn_vul.app_sec_manager

手順
1. 次のように移動する。 **All** (すべて) > **GitHub** 脆弱性統合 > 統合.
2. 統合を選択します。
3. [脆弱性統合実行] 関連リストを選択します。
4. すべてのインポートが成功したことを確認します。

   Trouble?

   実行が失敗した場合の一般的な原因は次のとおりです。
   - ネットワークの中断。
   - データ転送の問題による、変換中のデータ破損。

   これらの条件のいずれかが発生した場合は、[今すぐ実行] を選択して統合を再実行します。
5. インポートされたリポジトリを表示するには、統合リストに戻り、GitHub リポジトリ統合レコードを選択します。
6. [脆弱性統合実行] 関連リストを選択し、レコードを開きます。
   統合実行でインポートしたリポジトリの数は、[インポートされたアイテム] 列に表示されます。

   [設定] メニューから GitHub アカウントのリポジトリに設定したタグとトピックがインポートされます。インポートされたカスタムプロパティは、[リポジトリ] の下のメニューにあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タグ、トピック、およびカスタムプロパティは、GitHub アカウントで構成されている場合にのみインスタンスにインポートされます。

インポートされた場合、この GitHub 情報は、検出されたアプリケーション [sn_vul_app_release] テーブルの [ソースの追加情報] 列と、検出されたアプリケーションレコードの [ソース追加情報] セクションのインスタンスに表示されます。カスタムプロパティはキーと値のペアとして表示され、タグとトピックはアレイに表示されます。

GitHub アプリケーション脆弱性統合 インポートセットを表示

GitHub アプリケーション脆弱性統合のインポート情報の詳細を表示します。

始める前に
必要なロール：sn_vul.app_sec_manager

手順

1. に移動します **GitHub** 脆弱性統合 > インポートセットテーブル.
2. 統合のレコードを選択します。
3. 関連リンクを選択すると、次の情報が表示されます。
   - インポートセット
   - 変換マップ
   - 変換履歴

Invicti 脆弱性統合

Invicti 脆弱性統合 では、Invicti 製品からインポートしたアプリケーションデータを使用して、コードの欠陥の影響と優先度を判断できます。

Invicti 脆弱性統合

Invicti 脆弱性統合 はスキャナーデータを収集し、そのデータを Now Platform® で使用できるようにします。脆弱性対応の ServiceNow® アプリケーション脆弱性対応機能と簡単に統合し、インポートされたサードパーティアプリケーション脆弱性情報をインスタンスにマッピングします。

統合では、次のタイプのスキャンデータがインポートされます。

- 動的アプリケーションセキュリティテスト (DAST)
- インタラクティブアプリケーションセキュリティテスト (IAST)

DAST および IAST の詳細については、「アプリケーション脆弱性対応 の詳細」を参照してください。

利用可能バージョン

リリースバージョン	リリースノート
Invicti 脆弱性統合 v1.1 Invicti 脆弱性統合 v1.0	Application Vulnerability Response release notes 互換性情報については、「KB0856498 脆弱性対応互換性マトリクスおよびリリーススキーマの変更」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統合

ベースシステムには、次の統合が含まれています。統合は連結されているため、1 つの統合が正常に完了すると、次の統合が開始されます。統合は、次のテーブルに示す順序で実行されます。

最初の実行後、毎日スケジュール済みジョブが連結され、これらの統合が順番に自動的に実行されます。スケジュール済みジョブを手動で実行することもできます。スケジュール済みジョブでは、インスタンスを他の脆弱性管理システムと同期させることで、脆弱性修復ライフサイクルを簡素化します。

Invicti アプリケーション脆弱性統合

統合	説明
Invicti アプリケーションリストアプリケーション	CI ルックアップルールレコードの *sn_vul.use_product_model* システムプロパティの設定方法に基づいて、Invicti によってスキャンされたアプリケーションを検出されたアプリケーション [sn_vul_app_release] テーブルまたはスキャン済みアプリケーション [sn_vul_app_scanned_application] テーブルにインポートします。 • 製品モデルプロパティが true に設定されている場合、アプリケーションは [検出されたアプリケーション] リリーステーブルに挿入されます。 • 製品モデルプロパティが false に設定されている場合、アプリケーションは [スキャン済みアプリケーション] テーブルに挿入されます。 システムプロパティを変更することで、構成アイテム (CI) をルックアップターゲットとするルックアップルールを有効にすることができます。変更する場合は、ルックアップターゲットに一致するように CI ルックアップルールも有効にする必要があります。詳細については、以下を参照してください。 • Invicti 脆弱性統合 の構成 • CI ルックアップルールを作成する • アプリケーション脆弱性対応での CI ルックアップルールの再適用
Invicti スキャンリスト統合	この統合は、アプリケーションリスト統合が正常に完了した後に開始されます。この統合により、スキャンが実行された日時に関するデータがインポートされます。
Invicti アプリケーション脆弱性一致アイテム統合	この統合は、スキャンリスト統合が正常に完了した後に開始されます。 v1.1 以降では、アプリケーション脆弱性一致アイテム統合の合計処理時間、統合前後のプロセスの平均時間、統合実行レコードに関するレポートなどの詳細を表示できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Invicti アプリケーション脆弱性統合 (続く)

統合	説明
	Invicti の各脆弱性には、**DirectoryListing** などの「タイプ」があります。このタイプは、一意の ID としてインスタンスにマッピングされ、アプリケーション脆弱性一致アイテム (AVI) レコード **Invicti-DirectoryListing** の [脆弱性] フィールドの値の一部として表示されます。 マッピングの詳細については、「Invicti 脆弱性統合 ステータスマッピング」を参照してください。

3 つすべての統合ページあたりのアイテム数の上限は 200 です。

Invicti 脆弱性統合 の準備

統合を成功させるには、統合前のタスクを計画して実行する必要があります。これらのタスクを実行して、統合の準備をします。Invicti 脆弱性統合 は、Invicti 製品と API に精通していることを前提としています。

共通脆弱性タイプ一覧 (CWE) 統合はアプリケーション脆弱性対応でも使用され、Invicti 脆弱性統合をインストールして構成する前に実行する必要があります。

注:
NIST 脆弱性データベース (NVD) データは統合のインストールには必要ありませんが、脆弱性拡張が提供されるので便利です。

NVD の詳細については、「NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理」を参照してください。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

注:
統合を実行する前に、要件に基づいて必要な構成変更を行います。

インポートする予定のアプリケーション脆弱性一致アイテムの数に基づいて、インスタンスのサイジングを検証します。インスタンスが小さすぎると、ロードに時間がかかることがあります。インスタンスのサイズがわからない場合は、カスタマーサービス & サポート にお問い合わせください。Now Platform インスタンスにアプリケーションをインストールして構成するには、アドミンロールが必要です。

Invicti コンソールで API 認証情報と API トークンを取得します。API の概要 の Invicti 製品の Web サイトで入手できる情報を確認します。

Invicti との **ServiceNow®** 脆弱性対応統合のインストール

インスタンスで統合を実行する前に、インストールと構成のステップを完了して、Invicti 脆弱性統合 アプリケーションが アプリケーション脆弱性対応 と適切に統合されるようにします。このアプリケーションは別のサブスクリプションとして利用できます。

始める前に
必要なロール：admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. Invicti 脆弱性統合 をインストールするインスタンスにログインします。
2. ServiceNow Store に移動します。
3. ServiceNow Storeで、Invicti 脆弱性統合 アプリケーションを検索します。
4. アプリケーションタイルを選択します。
   インストールしているアプリケーションに関する詳細情報が表示されます。

   注:
   該当する場合は、[他の要件] および [依存関係] セクションを読むことを検討してください。

5. [アプリを要求] を選択して、Now Support ログイン認証情報を入力します。
6. [取得] を選択します。
7. [インスタンス名] と [インスタンスの理由] を入力し、[インスタンスを検証] を選択します。
8. [要求] を選択します。
   詳細なインストール手順が記載されたメールが届きます。
9. 次のように移動する。 **All** (すべて) > システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて).
10. アプリケーションを見つけて選択し、[インストール] を選択してアクティブ化します。
    アプリケーションはインスタンスに自動でインストールされます。

Invicti 脆弱性統合 の構成

インスタンスで統合を実行する前に、インストールと構成のステップを完了して、脆弱性対応 の アプリケーション脆弱性対応 機能を Invicti 脆弱性統合 と適切に機能できるようにします。

始める前に
必要なロール：

- アプリケーションのインストールおよびアクティブ化を行うには admin
- 統合を構成するには、アプリセキュリティマネージャーユーザーグループ

インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

脆弱性対応 アプリケーションがインストールされ、アクティブ化されていることを確認します。	このアプリケーションがアクティブ化されていることを確認するには、次の場所に移動します サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応 のインストール」を参照してください。
Invicti 脆弱性統合 がインストールされ、アクティブ化されていることを確認します。	このアプリケーションがアクティブ化されていることを確認するには、次の場所に移動します サブスクリプション管理 > サブスクリプション

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

	インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「Invicti との ServiceNow 脆弱性対応統合のインストール」を参照してください。
インスタンスに必要な ServiceNow ロールがあることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。 • まだアサインされていない場合、システムアドミニストレーター [admin] はアプリをインストールして、ユーザーをアプリセキュリティマネージャーグループにアサインします。 • アプリセキュリティマネージャーは構成を監督し、期待される結果を検証します。
Invicti 脆弱性統合の場合は、[ユーザー**ID**] と **[API** トークン] を用意してください。	[ユーザー **ID**] と **[API** トークン] がわからない場合は、Invicti アドミニストレーターに連絡して取得してください。 詳細については、「API の概要」で Invicti 製品の Web サイトを参照してください。

手順

1. 次のように移動する。 **All** (すべて) > **Invicti** > **Invicti** 構成.
2. フィールドに入力します。

フィールド	説明
API URL	ユーザーの Invicti のインスタンス URL。これは、「Invicti 脆弱性統合 の準備」から取得した情報です。
ユーザー ID	一意のユーザー ID。
API トークン	Invicti コンソールから生成した API トークン。これは、「Invicti 脆弱性統合 の準備」から取得した情報です。
スキャンタイプを選択します。少なくとも 1 つ選択する必要があります。	
DAST のインポート	DAST スキャンからの脆弱性を含めるオプション。DAST スキャンは、アプリケーションの実行中にアプリケーションの脆弱性を動的に検出します。このアプローチは、外部からの攻撃を模倣する可能性があります。
IAST のインポート	IAST スキャンからの脆弱性を含めるオプション。IAST スキャンは、プログラムの実行中にプログラムと対話することにより、ソフトウェアの脆弱性を検出します。人間による観察、自動テスト、およびセンサーを組み合わせて使用

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	し、アプリケーションと対話して脆弱性を特定します。
日付形式	開始時間を、Invicti アプリケーション脆弱性一致アイテム統合で使用される Invicti API でサポートされている形式に変換するパラメーター。 このパラメーターは、Invicti アカウントで定義または選択した形式と一致します (例：**dd/MM/yyyy**)。Invicti コンソールの日付と時刻の形式が、Now Platform インスタンスの日付形式に入力したものと一致することを確認します。 Invicti コンソールでこの形式を変更するには： **a.** [Invicti サインイン] でログインします。 **b.** 右上の **[** ユーザー名] を選択します。 **c.** 次のように移動する。 ユーザー設定 > 日時形式. **注:** Now Platform インスタンスに無効な日付形式を入力すると、インポートに失敗する可能性があります。 Invicti コンソールの日付形式とは異なる有効な形式をインスタンスに入力すると、Invicti は空のペイロードを返します。
ServiceNow での例外の管理	1 つ選択： 有効 (選択済み) インスタンスで保留される可能性がある [存在] や **[AcceptedRisk]** などの状況を持つ Invicti のアプリケーション脆弱性一致アイテム (AVIT) は、代わりに自動的に [オープン] にマッピングされます。 有効 (選択されていない) Invicti からインポートされたアプリケーション脆弱性一致アイテム (AVIT) のソースステータスは保持されます。AVIT レコードからこれらの AVIT の例外を管理 (保留) する必要があります。 Invicti ソースの状態とターゲットフィールドの詳細については、「Invicti 脆弱性統合 ステータスマッピング」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ServiceNow での誤検出の管理	1 つ選択： 有効 (選択済み) インスタンスで [クローズ済み] に移行する可能性がある [存在] や [誤検出] などの状況を持つ AVIT は、代わりに自動的に [オープン] にマッピングされます。 有効 (選択されていない) Invicti からインポートされた AVIT ステータスは保持されます。AVIT レコードから、これらの AVIT の誤検出または潜在的な誤検出を管理する必要があります。

3. [認証情報を保存してテスト] を選択します。
4. オプション: 構成アイテムに基づくようにルックアップルールを変更します。

   (Optional) デフォルトでは、製品モデルに基づいて [sn_sec_cmn_ci_lookup_rule] テーブルにリストされているルックアップルールに対して **[sn_vul.use_product_model]** システムプロパティがアクティブ化 (true に設定) されています。このルールを有効にすると、次のようになります。

   - このルールは、製品モデルに基づいて、インポートされたデータとユーザーの構成管理データベース (CMDB) のデータとの一致を識別します。
   - 検出されたアプリケーション [sn_vul_app_release] テーブルでレコードが作成または更新されます。
   - Invicti のルックアップルールを作成または編集すると、ルールフォームの [ルックアップターゲット] フィールドに [製品モデル] が表示されます。

   構成アイテムに基づくようにルールを変更するには、**[sn_vul.use_product_model]** システムプロパティを手動で非アクティブ化 (false に設定) する必要があります。

   a. 次のように移動する。 **All** (すべて) > システムプロパティ をクリックし、**sn_vul.use_product_model** レコードを見つけて、値を false に設定します。

   b. [**Update** (更新)] を選択します。

   c. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > **CMDB** > ルックアップルール.

   d. ルックアップターゲットが [構成アイテム] であるアプリケーション名とソースアプリケーション ID のルールを見つけます。

   e. これらのルールに [有効] チェックボックスをオンにします。

   f. [更新] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Invicti のルックアップルールを作成または編集すると、ルールフォームの [ルックアップターゲット] フィールドに [構成アイテム] が表示されることに注意してください。スキャンされたアプリケーション [sn_vul_app_scanned_application] テーブルでレコードが作成または更新されます。

Invicti 脆弱性統合 インポートの実行状況とレコードの表示

[脆弱性統合実行] 関連リストを使用して、統合実行の成功を確認し、問題を特定して、修復の決定を通知します。

インポートステータス、インポートセット、およびレコードの表示

インポートのステータスを表示するには、アプリセキュリティマネージャーユーザーグループのユーザーとして、 **All** (すべて) > **Invicti** 脆弱性統合 > 統合 をクリックし、統合レコードを選択します。[脆弱性統合実行] 関連リストを選択します。

v1.1 以降では、アプリケーション脆弱性一致アイテム統合の合計処理時間、統合前後のプロセスの平均時間、統合実行レコードに関するレポートなどの詳細を表示できます。

インポートセットを表示するには、次に移動します: **All** (すべて) > **Invicti** 脆弱性統合 > 統合 > インポートセットテーブル をクリックし、統合を選択します。

アプリケーションリスト統合は、ルックアップターゲットに基づいてレコードを作成または更新します。

- 製品モデル：検出されたアプリケーション [sn_vul_app_release] テーブル
- 構成アイテム：スキャン済みアプリケーション [sn_vul_app_scanned_application] テーブル

スキャンリスト統合は、スキャン済みアプリケーション [sn_vul_app_scan_summary] テーブルのレコードを作成または更新します。

アプリケーション脆弱性一致アイテム統合は、アプリケーション脆弱性一致アイテム [sn_vul_app_vulnerable_item] および CWE [sn_vul_cwe] テーブルのレコードを作成または更新します。

注:
Invicti の各脆弱性には、ProductDirectoryListing などの「タイプ」があります。このタイプは、一意の ID としてインスタンスにインポート、マッピングされ、アプリケーション脆弱性一致アイテム (AVIT) レコードの [脆弱性] フィールドの値の一部として表示されます。この例では、値は Invicti-ProductDirectoryListing であり、この値はアプリケーション脆弱性エントリレコードの一意の ID としても表示されます。Invicti AVIT は複数の共通脆弱性タイプ一覧 (CWE) エントリをサポートしているため、CWE は一意の ID として使用されません。CWE は AVIT レコードにも表示されます。

Invicti AVIT の場合、Invicti の脆弱性に対して重複するタイプがある場合、「custom」という単語が値に挿入されます (例：Invicti-custom-ProductDirectoryListing)。脆弱性のカスタムタイプを作成する場合、脆弱性 ID は Invicti-Custom-<title of vulnerability> である可能性があります。

新しいフィールド：スキャンタイプ = Invicti の場合、[影響を受けるパラメーター] フィールドと [カスタム] フィールドには、脆弱性の理解と修復に役立つデータが含まれている場合があります。データがない場合、これらのフィールドは AVIT に表示されません。

Invicti 脆弱性統合 ステータスマッピング

Invicti 脆弱性統合 からの次のソースステータスと、インスタンス内のそれらのターゲットステータスを次の表に示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Invicti ソースステータスとそれに対応する **Now Platform** ステータス

Invicti ソースステータス	ソース状況の説明	**Now Platform** のターゲットステータス
存在 (Present)	問題が識別されます。	オープン
存在、AcceptedRisk、回復済み	問題が検討され、低リスクの脆弱性としてマークされています。	保留
存在、誤検出	問題が検討され、本物の脆弱性ではないとしてマークされています。	クローズ
FixedUnconfirmed、修正済み未確認	この問題は修正されましたが、Invicti Enterprise によって確認されていません。	解決済み
修正済み (確認済み)、FixedConfirmed、FixedConfirmed、AcceptedRisk、FixedConfirmed、誤検出	この問題は Invicti Enterprise によって修正および確認されており、これ以上のアクションは必要ありません。	クローズ
修正済み (再テストできません)	問題は特定されましたが、Invicti は問題が修正されたかどうかを確認するために再テストできません。	解決済み
回復済み	この問題は以前のスキャンで修正されましたが、再度検出されました。	オープン
保留、無視	問題はユーザーによって無視されました。Invicti Enterprise では、問題を無視するために、ユーザーはそのステータスを「受け入れられたリスク」に更新します。	リスク受容

アプリケーションリリースマッピング

ソースフィールド	Now Platform のターゲットフィールド
ID	source_app_id
CreatedAt	app_creation_date
UpdatedAt	app_updation_date
名前	app_name
RootUrl	Source_additional_info
説明	説明
タグ	タグ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性マッピング

ソースフィールド	Now Platform のターゲットフィールド
タイプ	カテゴリ名
脆弱性の詳細	サマリー
影響	脅威
ソース参照	Web 参照
ソースの推奨事項	ソリューション
タイプ	source_entry_id/ID
重大度	source_severity
分類[“Cwe”]	CWE リスト
CvssVectorString	CVVS v3 フィールド

スキャンサマリーマッピング

ソースフィールド	ターゲット フィールド
ソース	ソース
TotalVulnerabilityCount	Detected_flaw_count
開始日	動的スキャン日
ID	source_scan_id

アプリケーション脆弱性一致アイテム **(AVIT)** マッピング

ソースフィールド	Now Platform のターゲットフィールド
タイプ	スキャンタイプ
Web サイト ID	ソースアプリ ID
ID	ソース AVIT ID
最終確認日	前回検出
初回確認日	初回検出
最終更新日	前回スキャン日
parameters	影響を受けるパラメーター
URL	影響を受ける URL
重大度	ソース重大度
URL	ソースリンク
脆弱性の詳細	ソース脆弱性のサマリー
外部参照	ソース参照
修復策 + 修復策の参照	ソースの推奨事項
状況	ソース修復ステータス

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

影響	ソース脆弱性の説明

Veracode 脆弱性統合

脆弱性対応 Integration with Veracode アプリケーションでは、Veracode 製品からインポートしたデータを使用して、コードの欠陥の影響と優先度を判断できます。

Veracode 脆弱性統合

Veracode 製品は、ダイナミックアプリケーションセキュリティテスト (DAST)、スタティックアプリケーションセキュリティテスト (SAST)、および手動スキャナーデータを収集し、そのデータを Now Platform で利用できるようにします。脆弱性対応 の アプリケーション脆弱性対応 機能と簡単に統合し、サードパーティ脆弱性をマッピングして、データをインスタンスに拡張します。

脆弱性対応 の v19.0 以降では、ソフトウェアアプリケーションの脆弱性を特定するために、Software Composition Analysis (SCA) と ソフトウェア部品表 (SBOM) の脆弱性データをインポートすることができます。詳細については、「ソフトウェア部品表 の詳細」を参照してください。

共有 API は、DAST、SAST、SCA データ、および手動ペネトレーションテスト結果を取り込みます。

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

スケジュール済みジョブにより、統合がリストされている順序で毎日自動的に呼び出されます。スケジュール済みジョブを手動で実行することもできます。スケジュール済みジョブでは、インスタンスを他の脆弱性管理システムと同期させることで、脆弱性修復ライフサイクルを簡素化します。

Veracode から詳細を取得

v4.2 以降において次の Veracodeデータを表示する場合、[アプリケーション脆弱性一致アイテム] [sn_vul_app_vulnerable_item] テーブルまたは [脆弱性対応ワークスペース] のリストビューより、ソースとして Veracode を有するアプリケーション脆弱性一致アイテム (AVIT) の [詳細情報を取得] を選択します。

- 動的アプリケーションセキュリティテスト (DAST) スキャンに関する HTTP ソース要求およびソース応答の詳細が、HTTP 要求/応答の関連リストに表示されます。
- Veracode からのソリューション推奨事項が [検索結果] 関連リストに表示されます。
- HTTP ソース要求、ソース応答、および推奨事項は、脆弱性対応 脆弱性対応 ワークスペースの [詳細] タブに表示されます。
- [説明] 列は、アプリケーション脆弱性一致アイテム [sn_vul_app_vulnerable_item] テーブルでサポートされています。

利用可能バージョン

リリースバージョン	リリースノート
Veracode v4.3 Veracode v4.2 Veracode v4.1	Application Vulnerability Response release notes 互換性情報については、「KB0856498 脆弱性対応 互換性マトリクスおよびリ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

リリースバージョン	リリースノート
	リースススキーマの変更」を参照してください。

ユーザーグループおよびロール

Veracode 脆弱性統合 はシステムアドミニストレーター [admin] によってインストールされ、アプリセキュリティマネージャーグループのメンバーによって構成されます。詳細については、「アプリケーション脆弱性対応 のユーザーロールおよびロール」を参照してください。

Veracode 脆弱性統合

Veracode脆弱性統合を表示するには、次に移動します: **All** (すべて) > **Veracode** 脆弱性統合 > 統合.

ベースシステムには、次の統合が含まれています。

Veracode 脆弱性統合

統合	説明
v4.1 以降：Veracode プロジェクトのリンク統合	統合はデフォルトで有効化されています。アプリケーションごとに、関連するすべてのプロジェクトを Veracode から取得します。 アプリケーションは、Veracode アプリケーション内に複数のプロジェクトを含めることができます。この統合からインポートされたデータが次のレコードに表示されます。 • 前回の **SCA** スキャン日、アプリの作成日、 およびアプリの更新日は、[検出されたアプリケーション] のレコードに一覧表示されます。 • アプリケーション脆弱性のスキャンサマリーレコードとアプリケーション脆弱性一致アイテム (AVIT) に、 ソース **SDLC** ステータス (ソフトウェア開発ライフサイクル) が表示されます。 • ソースの利用性は、アプリケーション脆弱性一致アイテム (AVI) レコードに表示されます。
Veracode アプリケーションリスト統合 (JSON)	この統合は、デフォルトでは非アクティブです。Veracode アプリケーションスキャナーデータ (脆弱性、メタデータ) を取得し、アプリケーションデータを拡張します。 JSON ベースの API を介して Veracode からスキャンレコードを取得します。
Veracode アプリケーションリスト統合 (XML)	この統合は、デフォルトでは非アクティブです。この統合の XML ベースバージョンは非アクティブ化 (廃止) されました。Veracode アプリケーションスキャナーデータ (脆弱性、メタデータ) を取得し、アプリケーションデータを拡張します。この統合は毎日 00:00:00 に実行するように設定されます。 **注:** Veracode 以降、アプリケーションのリストを取得するために JSON ベースの API が使用されています。この API は、これらのアプリケーションの「前回のポリシーコンプライアンスチェック日」をインポートし、これらのアプリケーションが Veracodeによって最後にスキャンされた日時を示します。
Veracode ソフトウェア部品表	Veracode 脆弱性統合 のバージョン 4.3 では、Veracode SBOM ファイルで以下の機能拡張が行われています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Veracode 脆弱性統合 (続く)

統合	説明
(SBOM) 統合	• SBOM Response がインストールされている場合、アップロードする SBOM ファイルに Veracode で検出された脆弱性を含めることができます。 • Veracode は、Veracode SBOM ファイルの部品表 [sn_sbom_doc] テーブルにあるレコードの [ソース] フィールドにマッピングされます。 統合はデフォルトで有効化されています。v4.2 以降、Veracode で生成された CycloneDX および SPDX 形式の ソフトウェア部品表 ファイルをインポートし、インスタンスで解析できるようキューに格納します。このデータをインポートして表示するには、ソフトウェア部品表 アプリケーションがインストールされている必要があります。
Veracode スキャンサマリー統合 (JSON)	この統合は、デフォルトでは非アクティブです。JSON ベースの API を介して Veracode からスキャンレコードを取得します。この統合は、XML ベースの API 統合に代わるものです。これは、連結され Veracode アプリケーションリスト統合に従います (有効な場合)。
Veracode スキャンサマリー (XML)	この統合は、デフォルトでは非アクティブです。この統合の XML ベースバージョンは非アクティブ化 (廃止) されました。Veracode からスキャンレコードを取得します。この統合は、連結され Veracode アプリケーションリスト統合に従います (有効な場合)。 **注:** 自動的に Veracode アプリケーションリスト統合に従います (有効な場合)。Veracode からのアプリケーションの「前回のポリシーコンプライアンスチェック日」を使用すると、この統合では、この統合の「delta_start_time」の後にスキャンされたアプリケーションのデータのみが取得されます。
Veracode アプリケーション脆弱性一致アイテムの JSON 統合	v4.2 以降では、合計処理時間や統合前後でのプロセスの平均実行時間などの詳細情報を表示したり、アプリケーション脆弱性一致アイテムの統合での統合実行レコードに関するレポートを作成したりすることができます。 この統合は、デフォルトでは非アクティブです。Veracode から、XML ベースの統合よりも多くの脆弱性データを含むスキャン結果を取得します。AVI を挿入してサードパーティ脆弱性データを強化します。
Veracode アプリケーション脆弱性一致アイテム統合 (XML)	v4.2 以降では、合計処理時間や統合前後でのプロセスの平均実行時間などの詳細情報を表示したり、アプリケーション脆弱性一致アイテムの統合での統合実行レコードに関するレポートを作成したりすることができます。 この統合は、デフォルトでは非アクティブです。Veracode からスキャン結果を取得し、アプリケーション脆弱性アイテム (AVIT) を挿入して、サードパーティ脆弱性データを拡張します。デフォルトでは、スキャナーレコードが [クローズ済み] ステータスの場合、AVIT は作成されません。既存の AVIT は引き続き更新されます。 この統合は連結され、Veracode スキャンサマリー統合に従います (有効な場合)。Veracode スキャンサマリー JSON 統合の XML ベースの API は廃止されました。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Veracode 脆弱性統合 (続く)

統合	説明
	注: Veracode スキャンサマリー統合に自動的に従います。Veracode からのアプリケーションの「前回のポリシーコンプライアンスチェック日」を使用すると、この統合では、この統合の「delta_start_time」の後にスキャンされたアプリケーションのデータのみが取得されます。
Veracode カテゴリ統合	この統合は、デフォルトでは非アクティブです。Veracode から拡張カテゴリデータを取得します。
Veracode CWE 統合	統合はデフォルトで有効化されています。脅威情報と修復推奨事項のために、Veracode 固有の共通脆弱性タイプ一覧 (CWE) データを取得します。これらのデータは、アプリケーション脆弱性エントリレコードで入力および更新されます。 この CWE 統合は、脆弱性対応 アプリケーションに対してアクティブ化する CWE Comprehensive 2000 統合 (CWE Comprehensive 2000 Integration) スケジュール済みジョブから独立して動作します。 Veracode CWE 統合 (Veracode CWE Integration) と CWE Comprehensive 2000 統合 (CWE Comprehensive 2000 Integration) が有効になっている場合、データは複製されません。
Veracode DevOps 統合	この統合は、デフォルトでは非アクティブです。この統合は、アプリケーション脆弱性対応 の [アプリケーション脆弱性統合] リストに表示されます。DevOps チェンジベロシティライセンスをお持ちの場合、この機能は、DevOps ユーザーがサードパーティの脆弱性スキャンのサマリー詳細を表示するために SecOps ライセンスを必要としない構造になっています。アプリケーション脆弱性対応 への影響や変更はありません。

統合実行状況については、「Veracode アプリケーション脆弱性統合のインポート実行状況の表示」を参照してください。

サードパーティの脆弱性データを表示する方法については、「脆弱性ライブラリの表示」を参照してください。

Veracode 脆弱性統合 の準備

Veracode 脆弱性統合 を成功させるには、事前統合タスクを計画して慎重に実行する必要があります。これらのタスクを実行して、統合の準備をします。Veracode 脆弱性統合は、Veracode 製品と API に精通していることを前提としています。

始める前に

共通脆弱性タイプ一覧 (CWE) 統合は アプリケーション脆弱性対応 でも使用され、Veracode 脆弱性統合をインストールして構成する前に実行する必要があります。脆弱性対応 では、デフォルトでインストールされます。

注:
NIST 脆弱性データベース (NVD) データは Veracode アプリケーション脆弱性統合のインストールには必要ありませんが、VVD では拡張が提供されるので便利です。NVD の詳細については、「NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

統合レコードごとに run-as ユーザーが構成されています。このユーザーのデフォルト値は **VR.System** です。この値は変更しないでください。

必要なロール：アプリセキュリティマネージャーグループ

このタスクについて

注:
統合を実行する前に、要件に基づいて必要な構成変更を行います。

インポートする予定のアプリケーション脆弱性一致アイテムの数に基づいて、インスタンスのサイジングを検証します。インスタンスが小さすぎると、ロードに時間がかかることがあります。インスタンスのサイズがわからない場合は、カスタマーサービス & サポート にお問い合わせください。

Veracode 脆弱性統合には API ID と API キーが必要です。

手順

API ID とキー認証情報を作成するには、次の手順を実行します。

a. Veracode プラットフォームにログインします。

b. ユーザーアカウントメニューに移動し、**[API** 認証情報] を選択します。

c. [API 認証情報を生成 **(Generate API Credentials)]** をクリックします。

d. 後で使用するために認証情報を記録します。

ServiceNow® Vulnerability Response Integration with Veracode のインストール

インスタンスで統合を実行する前に、インストールと構成のステップを完了して、アプリケーション脆弱性対応 が Veracode 製品と適切に統合されるようにします。このアプリケーションは別のサブスクリプションとして利用できます。

始める前に

インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

セットアップタスク	説明
脆弱性対応 アプリケーションがインストールされ、アクティブ化されていることを確認します。	このアプリケーションがアクティブ化されていることを確認するには、次の場所に移動しますサブスクリプション管理 > サブスクリプションインスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応 のインストール」を参照してください。
インスタンスに必要な ServiceNow ロールがあることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	• まだアサインされていない場合、システムアドミニストレーター [admin] はアプリケーションをインストールして、ユーザーをアプリケーションセキュリティマネージャーグループにアサインします。グループロールの詳細については、「アプリケーション脆弱性対応 のユーザーロールおよびロール」を参照してください。 • アプリセキュリティマネージャーグループは構成を監督し、期待される結果を検証します。

必要なロール：admin

手順

1. Veracode 脆弱性統合 をインストールするインスタンスにログインします。
2. ServiceNow Store に移動します。
3. ServiceNow Store で、Vulnerability Response Integration with Veracode アプリケーションを検索します。
4. アプリケーションタイルをクリックします。
   インストールしているアプリケーションに関する詳細情報が表示されます。

   注:
   該当する場合は、[他の要件] および [依存関係] セクションを読むことを検討してください。

5. [アプリを要求] をクリックし、Now Support ログイン認証情報を入力します。
6. [取得] をクリックします。
7. [インスタンス名] と [インスタンスの理由] を入力し、[インスタンスを検証] をクリックします。
8. [要求] をクリックします。
   詳細なインストール手順が記載されたメールが届きます。
9. 次のように移動する。 システムアプリケーション > アプリケーション.
10. アプリケーションを見つけて選択し、[インストール] をクリックします。
    アプリケーションはインスタンスに自動でインストールされます。

次のタスク
環境に Veracode 脆弱性統合 を構成します。「Veracode 脆弱性統合 の構成」を参照してください。

Veracode 脆弱性統合 の構成

インスタンスで統合を実行する前に、インストールと構成のステップを完了して、アプリケーション脆弱性対応 が Veracode 製品と適切に統合されるようにします。このアプリケーションは別のサブスクリプションとして利用できます。

始める前に
インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

セットアップタスク	説明
脆弱性対応 アプリケーションがインストールされ、アクティブ化されていることを確認します。	このアプリケーションがアクティブ化されていることを確認するには、次の場所に移動しますサブスクリプション管理 > サブスクリプションインスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「脆弱性対応 のインストール」を参照してください。
脆弱性対応 Integration with Veracode アプリケーションがインストールされ、アクティブ化されていることを確認します。	このアプリケーションがアクティブ化されていることを確認するには、次の場所に移動しますサブスクリプション管理 > サブスクリプションインスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールもアクティブ化もされていない場合は、「ServiceNow Vulnerability Response Integration with Veracode のインストール」を参照してください。
インスタンスに必要な ServiceNow ロールがあることを確認します。	期待される結果を構成および検証するには、次のロールが必要です。 • まだアサインされていない場合、システムアドミニストレーター [admin] はアプリをインストールして、ユーザーをアプリセキュリティマネージャーユーザーグループにアサインします。 • アプリセキュリティマネージャーは構成を監督し、期待される結果を検証します。
Veracode アプリケーション脆弱性統合の場合は、**API ID** と **API** キーを用意してください。	Veracode に問い合わせ、**[API ID]** と **[API** キー] を取得してください。「Veracode 脆弱性統合 の準備」を参照してください。 バージョン 4.0 以降では、Veracode 脆弱性統合 を使用している場合は、Veracode 脆弱性統合 のペネトレーションアセスメントテストは Veracode からの手動検出結果になります。これらの検出結果は、アプリケーション脆弱性対応 で構成したペネトレーションテストアセスメント要求にはリンクされません。アプリケーション脆弱性対応 でのペネトレーションテスト

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	要求の詳細については、「ペネトレーションテストの構成」を参照してください。

必要なロール：アプリセキュリティマネージャーユーザーグループ

手順

1. 次のように移動する。 **All** (すべて) > **Veracode** 脆弱性統合 > 構成.
2. **[API ID]** フィールドと **[API** キー] フィールドに入力します。
3. テスト結果を選択します。

オプション	説明
バージョン 4.0：	**a.** インポートに含める **[DAST]** または **[SAST]** データタイプを選択します。 注: いずれか、または両方を選択できますが、少なくとも 1 つを選択する必要があります。 **b.** Software Composition Analysis (SCA) 脆弱性をインポートするには、**[SCA]** を選択します。 **c.** Veracode から手動ペネトレーションテストの結果をインポートするには、[手動を含める **(Include Manual)]** を選択します。これらの結果に対して AVIT が作成されます。
バージョン 3.0	インポートに含める **[DAST]** または **[SAST]** データタイプを選択します。 注: いずれか、または両方を選択できますが、少なくとも 1 つを選択する必要があります。
バージョン 1.0：	デフォルトでは、ダイナミックアプリケーションセキュリティのテスト結果が選択されています。

4. インポートされたデータをフィルタリングするためのVeracode 重大度レベルを追加します。この値は Veracode からインポートされます。フィールドには複数の値を追加できます。入力されている場合、インポートでは、追加した重大度レベルに一致するデータのみが収集されます。
5. 選択内容を保存して検証します。

オプション	説明
バージョン 3.0：	[認証情報を保存してテスト] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

オプション	説明
	注: エラーメッセージが表示されない限り、構成は正常に完了しています。構成中にエラーメッセージが表示される場合は、データを再入力します。
バージョン 1.0：	[保存] をクリックします。 [認証情報をテスト] をクリックして、構成が正常であることを確認します。 注: エラーメッセージが表示されない限り、構成は正常に完了しています。構成中にエラーメッセージが表示される場合は、データを再入力します。

6. インポート時に AVIT の例外と誤検出を管理する方法を選択します。
ServiceNow 例外管理と誤検出ワークフローがデフォルトでアクティブにされた状態で、インポート時に AVIT を管理するためのオプション。ワークフローは、AVIT の [ソース] ステータスがインスタンスでどのようにマッピングされているかに基づいてトリガーされます。使用例については、「アプリケーション脆弱性対応での保留と誤検出のステータスマッピングの管理」を参照してください。

7. v4.3 以降では、次のパラメーターの設定を選択または検証します。

8. [認証情報を保存してテスト] を選択します。

次のタスク
環境でドメインセパレーションインポートが必要な場合は、「統合のためのドメインセパレーションインポートの作成」を参照してください。

初期インストールの手順の詳細については、「アプリケーション脆弱性対応 の構成」を参照してください。

初期インストール後の変更については、「Veracode 脆弱性統合 の変更とアクティビティ」を参照してください。

Veracode アプリケーション脆弱性統合のインポート実行状況の表示

[脆弱性統合実行] 関連リストを使用して、統合実行の成功を確認し、問題を特定して、修復の決定を通知します。

始める前に
Veracode 脆弱性統合 インポート実行状況を表示するには、次のステップを実行します。

- アプリケーション脆弱性対応 および Veracode 脆弱性統合をインストールして構成する必要があります。
- Veracode 脆弱性統合インポートがスケジュールされ、実行されている必要があります。

必要なロール：アプリセキュリティマネージャーグループ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて

統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、 アプリケーション脆弱性対応のバージョン 18.2.4 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

手順

1. [store-future: BEGIN review]Veracode 統合実行状況チャートを使用していない場合は、 [End] 次のように移動する。 **All** (すべて) > **Veracode** 脆弱性統合 > 統合.
2. 統合を選択します。
3. [脆弱性統合実行] 関連リストをクリックします。
4. すべてのインポートが成功したことを確認します。

   Trouble?

   実行が失敗した場合の一般的な原因は次のとおりです。

   ○ ネットワークの中断。

   ○ データ転送の問題による、変換中のデータ破損。
   これらの条件のいずれかが発生した場合は、[今すぐ実行] をクリックして統合を再実行します。
5. v4.2 以降では、合計処理時間や統合前後でのプロセスの平均実行時間などの詳細情報を表示したり、アプリケーション脆弱性一致アイテムの統合での統合実行レコードに関するレポートを作成したりすることができます。
   Veracode でインポートされた新たな詳細情報の表示について、詳しくは Veracode 脆弱性統合の「詳細の取得」を参照してください。

Veracode スキャンサマリーの表示

Veracode 脆弱性統合のスキャンサマリー情報の詳細を表示します。

始める前に

必要なロール：アプリセキュリティマネージャーグループ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. アプリケーション脆弱性のスキャンサマリー [sn_vul_app_vul_scan_summary_list] テーブルに移動します。
2. Veracode スキャンのレコードを選択します。
3. 脆弱性対応 の v19.0 および Veracode 脆弱性統合 v4.0 以降では、次の列を表示するにはリストのカスタマイズアイコン (歯車アイコン) を使用します。
   - 静的スキャンサイズ
   - サードパーティライブラリの数
   - 脆弱なサードパーティライブラリの数
   - 重大度別のサードパーティ欠陥の数
   - サードパーティライブラリの問題の数
   - サードパーティライセンスの問題の数
   - 修正された欠陥数 (Fixed Flaw count)
   - 軽減された欠陥数 (Mitigated Flaw count)
   - 軽減されていない欠陥数 (Unmitigated Flaw count)
   - 重大度別の静的な欠陥数
   - 重大度別の新しい欠陥数
   - 重大度別の軽減されていない欠陥数 (unmitigated flaw count by severity)
   - 重大度別の欠陥の合計数
   - 前回の SCA スキャン評価
   - 前回の SCA スキャン日
   - スキャンの公開日
   - Tags

Veracode 脆弱性統合のデータ変換

インポートするデータを特定すると、Veracode アプリケーションからデータが取得され、一連のデータソースによって処理され、インスタンス内で変換されます。

Veracode アプリケーション脆弱性一致アイテム統合

API のデータは最初に Veracode AppVul アイテムインポート [sn_vul_veracode_appvul_item_import] テーブルにロードされ、Veracode AppVul アイテム変換を使用してインポートされた情報が変換されます。

この変換マップにアクセスするには、*System Import Sets > Transform Maps*に移動し、Veracode AppVul アイテム変換を検索します。次の表に、統合別の変換マップフィールドを示します。

Veracode AppVul アイテム変換マップのフィールド

ソースフィールド	ターゲットフィールド	説明
app_id	source_app_id	アプリケーション ID
issueid	source_avit_id	AVIT ID

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Veracode AppVul アイテム変換マップのフィールド (続く)

ソースフィールド	ターゲットフィールド	説明
app_name	app_name	アプリケーション名。
version	app_version	アプリケーションのバージョン
build_id	source_scan_id	アプリケーションのビルド ID
account_id	account_id	アカウント ID
sandbox_id	sandbox_id	サンドボックス ID
last_update_time	last_scan_date	最終更新時間
app_name + last_scan_date	scan_summary_name	スキャンサマリー
life_cycle_stage	source_sdlc_status	ソース SDLC ステータス
level	source_severity	ソース重大度
category_name	category	カテゴリ
source_severity	source_severity	ソース重大度
category_id + " CWE-" + cweId	source_entry_id	ソースエントリー ID
source_vulnerability_summary	source_vulnerability_summary	ソース脆弱性のサマリー
source_recommendation	source_recommendation	ソースの推奨事項
description	description	ソースの説明
description	source_vulnerability_explanation	ソース脆弱性の説明
mitigation_status_desc	source_mitigation_status	ソース緩和ステータス
remediation_status	source_remediation_status	ソース修復ステータス
line	line_number	欠陥が見つかった行
module	application_module	アプリケーションモジュール
sourcefile	source_notes	ソースメモ
affects_policy_compliance	complies_with_policy	値は、true または false のソース情報に基づいて [はい] または [いいえ] になります。
Sourcefilepath + sourcefile	location	*static* 欠陥の場合の場所マッピング
url	location	*dynamic* 欠陥の場合の場所マッピング
scope、type、exploitLevel	source_additional_info	静的な欠陥の場合にソースから値が入力される名前値フィールド

変換プロセス中に、次の変換スクリプトが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Veracode 変換マップスクリプトのタイミングと目的

スクリプトが実行されるタイミング	目的
onComplete (インポートセットが変換を完了したとき)	データソースを処理し、作成済み、更新済みまたは未変更の AVIT、この統合の一部として Veracode からインポートされた AVIT の数を更新するために使用されるスクリプト。このスクリプトは内部使用のためのものであり、変更または削除しないでください。

Veracode 脆弱性統合 の変更とアクティビティ

Veracode 脆弱性統合専用のオプションの変更を構成します。

Veracode 脆弱性統合 によってインポートされた追加データの表示

注:
ここに記載されている以外の Veracode 脆弱性統合 の設定を変更するには、ServiceNow および アプリケーション脆弱性対応 に関する高度な専門知識が必要であり、製品ドキュメントの範囲を超えています。

Veracode から詳細を取得

v4.2 以降において次の Veracodeデータを表示する場合、[アプリケーション脆弱性一致アイテム] [sn_vul_app_vulnerable_item] テーブルまたは [脆弱性対応ワークスペース] のリストビューより、ソースとして Veracode を有するアプリケーション脆弱性一致アイテム (AVIT) の [詳細情報を取得] を選択します。

- 動的アプリケーションセキュリティテスト (DAST) スキャンに関する HTTP ソース要求およびソース応答の詳細が、HTTP 要求/応答の関連リストに表示されます。
- Veracode からのソリューション推奨事項が [検索結果] 関連リストに表示されます。
- HTTP ソース要求、ソース応答、および推奨事項は、脆弱性対応 脆弱性対応 ワークスペースの [詳細] タブに表示されます。
- [説明] 列は、アプリケーション脆弱性一致アイテム [sn_vul_app_vulnerable_item] テーブルでサポートされています。

Veracode 統合インスタンスパラメーターの変更

初期インストール後に Veracode 統合インスタンスで Veracode 統合のパラメーターを変更できます。

始める前に
必要なロール：アプリセキュリティマネージャーグループ

このタスクについて
統合のインスタンスから統合のパラメーターを変更して、取り込むデータのタイプを決定できます。これらの設定の一部では、統合の設定ページからこれらのパラメーターを変更することもできます。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > 統合.
2. 変更する Veracode 統合の [ソースインスタンス] 列で **[Veracode** アプリケーション脆弱性 **(Veracode Application Vulnerability)]** を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. [統合インスタンスパラメーター] タブを選択し、[値] 列のフィールドをダブルクリックして値を変更します。

   脆弱性対応 の v19.0 および Veracode 脆弱性統合 の v4.0 以降では、Veracode 統合の次のパラメーターを構成できます。

   import manual

   Veracode から手動ペネトレーションテストの結果をインポートするには、true を入力します。この値は、統合設定ページから変更することもできます。

   Veracode 脆弱性統合 のペネトレーションアセスメントテストは Veracode からの手動検出結果になります。これらの検出結果は、アプリケーション脆弱性対応 で構成したペネトレーションテストアセスメント要求にはリンクされません。アプリケーション脆弱性対応 でのペネトレーションテスト要求の詳細については、「ペネトレーションテストの構成」を参照してください。

   import_sca

   Software Composition Analysis (SCA) 脆弱性をインポートするには、true と入力します。この値は、統合設定ページから変更することもできます。

   status

   「Open」または「Closed」と入力して、必要なステータスの検出結果をインポートします。このフィールドを空のままにすると、統合は [オープン] ステータスと [クローズ済み] ステータスの両方の検索結果をインポートします。

   policy_sandbox

   「policy」または「sandbox」と入力して、ポリシーまたはサンドボックスに対応するレコードをインポートします。これらのレコードは、環境でのアプリケーションのテスト方法に関連している可能性があります。

   policy_rule_passed

   「true」または「false」と入力して、ポリシールールに合格したレコードをインポートします。これらのレコードは、環境でのアプリケーションのテスト方法に関連している可能性があります。

4. [更新] を選択して、変更を保存します。

手動 **Veracode** アプリケーション脆弱性インポートの実行

初期インポートに失敗した場合、またはスケジュールされた初期インポートを待ちたくない場合は、日次スケジュール済みジョブから独立して完全なデータインポートを実行できます。

始める前に

必要なロール：アプリセキュリティマネージャーグループ

手順

1. 次のように移動する。 **All** (すべて) > **Veracode** 脆弱性統合 > 統合.
2. 統合を選択します (Veracode アプリケーションリスト統合など)。
3. [今すぐ実行] をクリックします。

   注:
   Veracode アプリケーション脆弱性統合はそれぞれ、最も完全なデータ検索機能を提供することを目的としています。順序どおりに実行しないと、不完全なデータになる可能性があります。ServiceNow および アプリケーション脆弱性対応 の専門知識が必要になります。

インポートが完了すると、スケジュール設定されたインポートが再開します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

4. 統合実行状況については、「Veracode アプリケーション脆弱性統合のインポート実行状況の表示」を参照してください。
5. 他の統合パラメーターを変更する場合は、統合インスタンスに移動する必要があります。

Veracode 脆弱性統合のインポート時間の設定

必要に応じて Veracode 脆弱性統合 の開始時間をリセットできます。

始める前に
必要なロール：アプリセキュリティマネージャーグループ

このタスクについて
最初のインポート後に、Veracode 脆弱性統合の実行ごとに完全インポートが実行されます。インポートの実行の詳細については、「手動 Veracode アプリケーション脆弱性インポートの実行」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > **Veracode** 脆弱性統合 > 統合.
2. 統合を選択します。
3. 新しく [開始時間] を設定します。
   時間は現地時間で時間単位で計算されます。Veracode アプリケーションリスト統合インポートのデフォルト時間は 00:00:00 です。他の統合は [オンデマンド] であり、Veracode アプリケーションリスト統合の後に実行されるようにチェーンされます。これらのいずれかの [開始時間] を変更するには、ServiceNow および アプリケーション脆弱性管理 の高度な専門知識が必要です。
4. [更新] をクリックします。
   新しい時間は、次のスケジュール済みインポートに使用されます。

クローズされた Veracode アプリケーション脆弱性一致アイテムを含める

デフォルトでは、[クローズ済み] アプリケーション脆弱性一致アイテム (AVI) は、Veracode の脆弱性一致アイテム統合インポート中に作成されません。作成する場合は、システムプロパティを変更する必要があります。

始める前に
Veracode 脆弱性統合 がインストールされ、実行されている必要があります。

必要なロール：admin

手順

1. 左側のナビゲーションの [フィルターナビゲーター] テキストボックスに「sys_properties.list」と入力します。
2. リストの [名前] 検索ボックスに、「sn_vul.create_closed」と入力します。
3. [値] フィールドをダブルクリックし、**[True]** に設定します。
4. 緑色のチェックマークアイコン をクリックして保存します。
   次の Veracode インポートで [クローズ済み] ステータスのレコードは、アプリケーション脆弱性対応 に AVI として作成されます。

アプリケーション脆弱性対応 の脆弱性を修復する

修復の監視は、ステータスの確認で始まり、アプリケーション脆弱性一致アイテム (AVIT) のクロージングで終わるプロセスです。アプリケーション脆弱性対応は、そのプロセスをより生産的かつ効率的に行うたのツールと手順を提供します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

アプリケーション脆弱性対応 修復プロセス

アプリケーション脆弱性一致アイテムの修復は手動で行われます。

プロセスの概要：

- アプリケーション脆弱性対応 インスタンスにログインします。
- アプリケーション脆弱性一致アイテムのルール (CI ルックアップ、アサイン) が期待どおりに機能していることを検証します。CI ルックアップルールの変更については、「アプリケーション脆弱性対応 でアプリケーションを自動的に識別する」を参照してください。アサインルールについては、「アプリケーション脆弱性対応 のアプリケーション脆弱性一致アイテムを自動的にアサインする」を参照してください。
- 修復ターゲットが正しいことを検証します。修復ターゲットルールの仕組みと修復方法については、「アプリケーション脆弱性対応 で修復ターゲットトラッキングを自動化する」を参照してください。アプリケーション脆弱性一致アイテムの修復ターゲットのステータスを表示する。

  注:
  修復ターゲットルールは AVIT に属します。これらのルールは、AVIT のインポート時に実行されます。

- ダッシュボードまたはレポートを確認します。たとえば、状況別に AVIT の経過時間を示すダッシュボードを表示します。

  注:

  脆弱性対応のパフォーマンスアナリティクス アプリケーション (com.snc.vulnerability.analytics) がアクティブ化されている場合、特定のロールを持つユーザーは、アプリセキュリティマネージャーおよびセキュリティチャンピオンの各グループのメンバーが関心のあるデータを表示できます。

  アプリセキュリティマネージャーの場合、脆弱性対応のパフォーマンスアナリティクス にはアプリケーション脆弱性対応 の概要が含まれており、関心のある領域を監視するのに役立ちます。「アプリケーション脆弱性対応のアナリティクスおよびレポートのソリューション」および「アプリケーションの脆弱性管理 (PA) ダッシュボード」を参照してください。

  脆弱性対応 アプリケーションのバージョン 13.0 以降：セキュリティチャンピオンの場合、脆弱性対応のパフォーマンスアナリティクス に [自分のアプリケーションの脆弱性] ダッシュボードが含まれており、関心のある領域を監視するのに役立ちます。「自分のアプリケーションの脆弱性ダッシュボード」を参照してください。

  脆弱性対応 アプリケーションのバージョン 13.0 以降：レポートまたは関連リストに対してコレクションされるデータの量を制限するには、「脆弱性対応 レポートおよび関連リストのサービス分類の定義」を参照してください。

- AVIT のステータスを優先度順に確認し、変更内容を検索します。
- 必要に応じて、AVIT のリスクを変更します。詳細については、「アプリケーション脆弱性算出を作成する」を参照してください。
- 必要に応じて、修復のために AVIT をアサイン先グループに再アサインします。
- 再スキャンは、サードパーティのスケジュール済みインポートによって自動的にトリガーされます。
- スキャン後、ステータスが [修復済み **(Fixed)]** の場合、インポート時に AVIT が自動的にクローズされます。
- スキャン後、ステータスが [修復済み **(Fixed)]** ではない場合、AVIT が再オープンされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Veracode から詳細を取得

次の Veracode データを表示する場合、アプリケーション脆弱性一致アイテム [sn_vul_app_vulnerable_item] テーブルまたは脆弱性対応ワークスペースのリストビューから、ソースとして Veracode を有するアプリケーション脆弱性一致アイテム (AVIT) の [詳細を取得 **(Get More Details)]** を選択します。

- 動的アプリケーションセキュリティテスト (DAST) スキャンに関する HTTP ソース要求およびソース応答の詳細が、HTTP 要求/応答の関連リストに表示されます。
- Veracode からのソリューション推奨事項が [検索結果] 関連リストに表示されます。
- HTTP ソース要求、ソース応答、および推奨事項は、脆弱性対応 脆弱性対応 ワークスペースの [詳細] タブに表示されます。
- [説明] 列は、アプリケーション脆弱性一致アイテム [sn_vul_app_vulnerable_item] テーブルでサポートされています。

脆弱性ライブラリの表示

脆弱性情報データベース (NVD)、共通脆弱性タイプ一覧 (CWE)、またはサードパーティからインポートされた脆弱性データを表示して、修復タスクをエスカレートするかどうかを決定できます。

始める前に
必要なロール：アプリセキュリティマネージャーグループ

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > ライブラリ用。

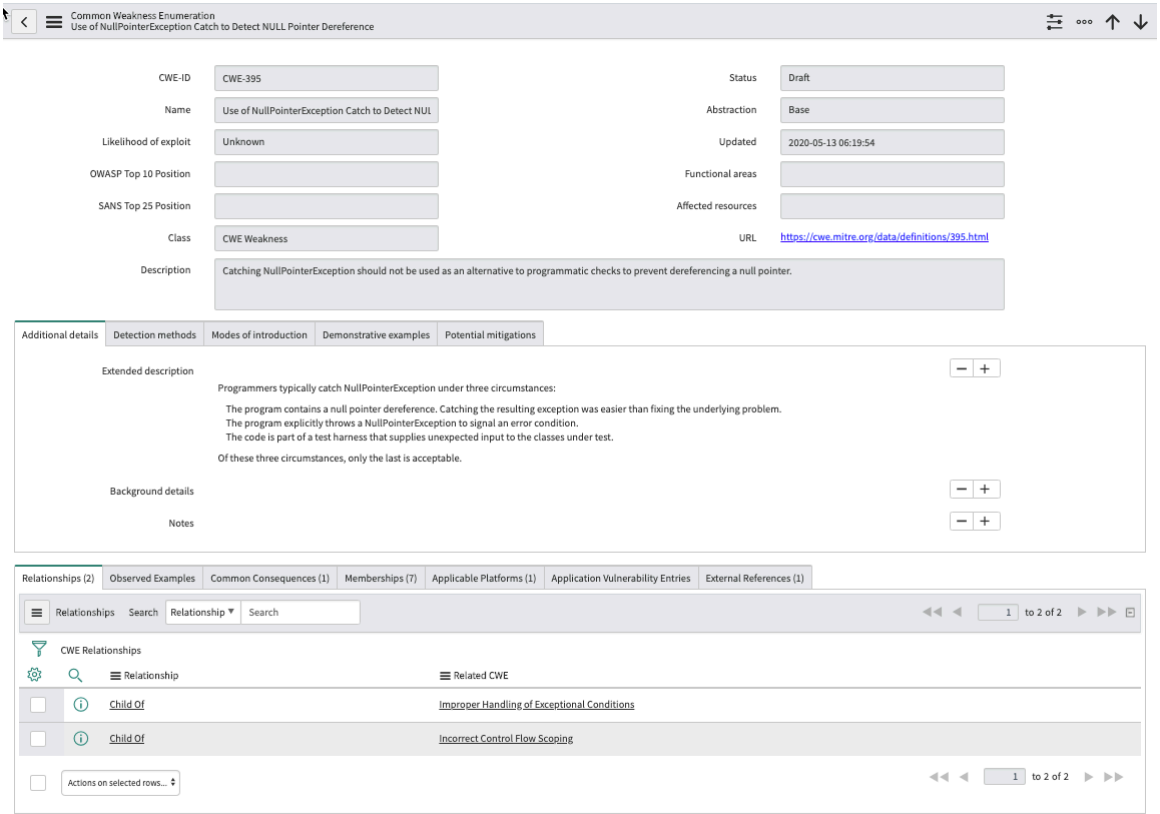
   次のライブラリが利用可能です。

ライブラリ	説明
NVD	NVD によって検出された脆弱性のリストで、セキュリティチェックリスト、セキュリティ関連のソフトウェアの欠陥、不適切な構成、製品名、およびエクスプロイトを含む影響度メトリクスが含まれています。
CWE	コミュニティで開発されたソフトウェアの脆弱性タイプのリスト。 各 CWE レコードには、脆弱性を説明する関連するナレッジ記事も含まれています。[共通脆弱性タイプ一覧] 画面から脆弱性をエスカレートすることはできません。これは参照用です。
サードパーティ	インスタンスにインポートされたサードパーティ脆弱性のリスト。関連する参照、脆弱性一致アイテム、エクスプロイト、CWE、および CVE のリストが含まれています。

2. ライブラリを選択して、脆弱性を表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



特定のフィールドの詳細については、「[アプリケーション脆弱性] フィールド」を参照してください。

[アプリケーション脆弱性] フィールド

脆弱性は、脆弱性情報データベース (NVD)、共通脆弱性タイプ一覧 (CWE)、またはサードパーティ統合からレコードがダウンロードされると自動的に作成されます。NVD と CWE は、脆弱性対応 の [ライブラリ] または アプリケーション脆弱性対応 の [脆弱性] の下に格納されます。

CWE 脆弱性エントリーフィールド

次の表のフィールドは読み取り専用です。

フィールド	説明
CWE ID	この脆弱性エントリーの識別子。この識別子はカテゴリと脆弱性の両方に使用され、2 つのデータセット間で一意です。
名前	この CWE-ID にアサインされた記述名。
エクスプロイトの可能性	定性的スケールで脆弱性が利用される可能性。次のいずれかになります。 • 低 • 中程度 • 高
OWASP 上位 10 位	OWASP 上位 10 リストにおけるこの脆弱性の数値的な位置。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
SANS 上位 25 位	SAN 上位 25 リストにおけるこの脆弱性の数値的な位置。
クラス	脆弱性のタイプ
ステータス	次のいずれかになります。 • 未完了 • ドラフト • 安定 • 不使用 • 廃止 • 不安定
抽象化	次のいずれかになります。 • バリアント • クラス • ベース • 複合
更新日時	最後にインスタンスでレコードが更新された日時。
機能エリア	影響を受ける機能エリアのリスト。たとえば、[ファイル処理 **(File Processing)]**。24/862 の脆弱性についてのみ設定されます。
影響を受けるリソース	影響を受けるリソースのリスト。たとえば、[ファイル] または [ディレクトリ]。51/863 の脆弱性についてのみ設定されます。
URL	この脆弱性に関連付けられたナレッジベース記事。
説明	脆弱性の説明。
統合実行	この CWE がインポートされた統合実行。
セクション	
その他の詳細	脆弱性をさらに説明するソフトウェアの概念の説明。含まれる内容： • 詳細な説明 • バックグラウンドの詳細 • メモ
ディスカバリー方法	アプリケーションにおけるこの脆弱性を検出する方法の詳細。
導入モード	脆弱性が導入されるフェーズ ([実装 **(Implementation)]**、[アーキテクチャと設計 **(Architecture and Design)]** など)。
デモ例	脆弱性のコード例と説明。
緩和の可能性	アプリケーションライフサイクルのどのフェーズで発生するか、緩和の有効性など、脆弱性を防止する方法の詳細。
関連リスト	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
関係	この脆弱性に関連付けられた CWE。この CWE とその他との関係を一覧表示します。parent/child、follows/precedes、requiredby/requires (複合的な脆弱性の場合)、CanAlsoBe、PeerOf、MemberOf を含めることができます。
観測された例	この脆弱性を表す CVE。
一般的な結果	悪用に成功した場合の結果、その範囲と影響。たとえば、 範囲：機密性 影響：アプリケーションデータの読み取り
メンバーシップ	この脆弱性を含む CWE メンバーシップ。
適用プラットフォーム	この脆弱性に関連付けられたプラットフォーム。
アプリケーション脆弱性エントリー	1 つに関連付けられた他のアプリケーション脆弱性エントリー。
外部参照	外部ソースからの脆弱性に関する情報。

アプリケーション脆弱性エントリーのフィールド

次の表のフィールドは読み取り専用です。

フィールド	説明
ID	この脆弱性エントリーの識別子。
ソース	脆弱性の発生元 - スキャナーまたは物理テスト。
重大度	この脆弱性の重大度を正規化したもの。重大度マップは、NVD および ServiceNow サードパーティ統合に提供されます。重大度マップの作成や調整の詳細については、「アプリケーション脆弱性一致アイテムの重大度を自動的にマッピングする」を参照してください。
バージョン 13.0：プライマリ CWE バージョン 12.1：CWE エントリー	この脆弱性が最も適合する共通脆弱性タイプ一覧要素への参照。 脆弱性に複数の CWE が関連付けられている場合、プライマリ CWE は次のように決定されます。 • CWE が OWASP 上位 10 位にマッピングされていますか。該当する場合は、この CWE を使用します。該当しない場合は、続行します。 • SANS 上位 25 位にマッピングされていますか？該当する場合は、この CWE を使用します。該当しない場合は、続行します。 • CWE の重大度は最高ですか？該当する場合は、この CWE を使用します。該当しない場合は、続行します。 • すべての CWE のうち最新のものを選択します。最新の CWE は、CWE レコードの内、最新の [更新済み **(Updated)]** フィールド値を含むものです。
カテゴリ名	サードパーティ統合によって提供される分類。アサインを支援します。
脆弱性の詳細	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
脅威	この脆弱性に由来する脅威の説明。
緩和の説明	この脆弱性を緩和するために実行できる手順の説明。
関連リスト	
バージョン 13.0： CWE	この脆弱性に関連する CWE のリスト。Veracode 脆弱性統合 には適用されません。

NVD エントリーのフィールド

次の表のインポートされたフィールドは読み取り専用です。

注:

NVD データは アプリケーション脆弱性対応 では使用されず、エントリーは 脆弱性対応 データのみを表します。

アプリケーション脆弱性対応 で使用される CWE は、脆弱性の例として NVD エントリーを指すことができ、ここでは情報提供のみを目的としています。

フィールド	説明
ID	この脆弱性エントリーの識別子。
リスク評価	(脆弱性に関連付けられている 脆弱性対応 脆弱性一致アイテム (VI) がない場合は非表示) VI を [重大]、[高]、[中]、[低]、および [なし] に分類する数値化された [リスクスコア]。
リスクスコア	(脆弱性に関連付けられている VI がない場合は非表示) 脆弱性一致アイテムが環境にもたらすリスク量を算出したもの。
重大度	脆弱性対応 におけるこの脆弱性の重大度を正規化したもの。重大度マップは、NVD および ServiceNow サードパーティ統合に提供されます。アプリケーション脆弱性対応 [重大度] は、NVD ではなく、インポートされた [ソース重大度] から導出されます。アプリケーション脆弱性対応 の重大度マッピングについては、「アプリケーション脆弱性一致アイテムの重大度を自動的にマッピングする」を参照してください。
エクスプロイト有無	少なくとも 1 つのエクスプロイトがこの脆弱性に関連付けられている場合は、有り。
エクスプロイトスキルレベル	この脆弱性を利用するために必要な最低スキルレベル。
エクスプロイト攻撃ベクトル	この脆弱性のエクスプロイトの最も脆弱な攻撃ベクトル。
アクティブな VI	(脆弱性に関連付けられている VI がない場合は非表示)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	[クローズ済み] ステータスではない、この脆弱性に関連付けられた脆弱性一致アイテムの数。この脆弱性にアクティブな AVI がない場合、[リスク評価] と [リスクスコア] は表示されません。
CWE エントリー	NVD に従った、この脆弱性が最も適合する共通脆弱性タイプ一覧要素への参照。
公開日	この脆弱性が公開された日付。
最終変更日	この脆弱性が前回変更された日付。
まとめ	脆弱性の説明。
脆弱性の詳細	
CVSS v2	インポートされた CVSS v2 データ
CVSS v3	インポートされた CVSS v3 データ。2015 年より前は利用できません。
優先ソリューション	(脆弱性に関連付けられている VI がない場合は非表示) この脆弱性で参照されたソリューションから導出された、チェーン内で最も優先度が高いソリューション。連結内に複数の最高優先度が存在する場合、値は設定されません。手動で設定した値は、後続のインポートで上書きできます。この値の手動設定は、脆弱性一致アイテムで行う必要があります。
修復ステータス (脆弱性に関連付けられている VI がない場合は非表示)	
保留を除外する	
脆弱性一致アイテム	この脆弱性があるアクティブなアプリケーション脆弱性一致アイテムの数。この数には、保留された脆弱性一致アイテムは含まれません。
合計 VI	この脆弱性がある脆弱性一致アイテムの合計数。この数には、保留された脆弱性一致アイテムは含まれません。
修復された VI の割合	この脆弱性がある脆弱性一致アイテムの修復の完了率。この数には、保留された脆弱性一致アイテムは含まれません。
保留を含める	
脆弱性一致アイテム	この脆弱性があるアクティブな脆弱性一致アイテムの数。
合計 VI	この脆弱性がある脆弱性一致アイテムの合計数。
修復された VI の割合	この脆弱性がある脆弱性一致アイテムの修復の完了率。
関連リンク	
v13.0 より前：ソフトウェア脆弱性のインポートを強制 注: v13.0 で削除	(使用廃止) NVD からの情報に基づいて、ITSM ソフトウェア資産管理 を使用して製品マッピングを再計算します。脆弱なソフトウェアライブラリを更新します。
ステータスを更新	前回の更新日時を表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	以下を更新します。 • 修復タスクステータス • リスクスコアと評価 • [修復ステータス] セクションのアクティブな VI、合計 VI などのメトリクス
関連リスト	
脆弱性一致アイテム	(脆弱性に関連付けられている VI がない場合は非表示) この脆弱性に関連付けられた脆弱性一致アイテム。
脆弱性参照	NVD によって引用された、外部ソースからの脆弱性に関する情報。
エクスプロイト	この脆弱性に関連付けられているエクスプロイト。
ソリューション	(脆弱性に関連付けられている VI がない場合は非表示) この脆弱性に関連付けられているすべての 脆弱性ソリューション管理 統合ソリューション。
バージョン 13.0：弱点	一般的な脆弱性とエクスポージャー (CVE) に関連付けられたインポートされた CWE 脆弱性データ。
バージョン 13.0：脆弱なソフトウェア	(脆弱性に関連付けられている VI がない場合は非表示) 脆弱性に関連するインポートされた共通プラットフォーム一覧 (CPE) データ。

自動翻訳

アプリケーション脆弱性対応 でアプリケーションを自動的に識別する

サードパーティ統合からデータをインポートすると、アプリケーション脆弱性対応 は自動的にアプリケーションデータを使用して、構成管理データベース (CMDB) 内で一致するものを検索します。その際に **CI** ルックアップルールを使用します。これらのルールは、アプリケーション脆弱性一致アイテム (AVI) レコードのアプリケーションを識別し、修復に役立ちます。

アプリケーションがインポートされると、source_app_id と app_name を使用して、スキャン済みアプリケーション [sn_vul_app_scanned _application] テーブルでルックアップが実行され、以前のインポートからのアプリケーションとの一致を検索します。アプリケーション ID の一致が見つかると、その値がアプリケーション脆弱性一致アイテムレコードの [アプリケーション] および [アプリリース] フィールドで使用されます。

一致が見つからなかった場合、またはアプリケーション ID フィールドが空の場合、ルールは他のアプリケーション情報を使用して、アプリケーションを正しく識別しようと試みます。それでも一致するものが見つからない場合は、[アプリケーション名] フィールドと [アプリケーション **ID]** フィールドのみを含むプレースホルダーのスキャン済みアプリケーションレコードが作成されます。

[ソースアプリケーション **ID]** と [アプリケーション名] のルックアップルールは、デフォルトで Veracode 脆弱性統合 が付属された状態で出荷されます。

注:
アプリケーション脆弱性対応 のデフォルトの CI ルックアップルールは、Veracode 脆弱性統合でのみ使用できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

一致を試行する場合、ルックアップルールは、最も低い [順番 **(Order)**] 値から順に評価されます。ルールが単一の CI を一致として返すと停止します。

> **注:**
> 複数の CI を返すようにルールが作成されている場合は、最初に一致したもののみが使用されます。

一致する問題を見つけやすくするため、一致が見つかると、その問題を見つけるために使用された CI ルックアップルールが、スキャン済みアプリケーションの **[CI** 一致ルール] フィールドに追加されます。[スキャン済みアプリケーション] リストビューの上部にある [カスタマイズリストの更新] ギア アイコンをクリックして、ビューに追加します。

> **注:**
> ルールは、一度削除すると元に戻せません。新しいルールを作成する場合は、既存のルールを削除せずに非アクティブ化します。

CI ルックアップルールはドメインセパレーションすることができ、ソース固有です。サポートされている場合、各ソースは複数の展開を持つことができます。たとえば、Veracode 脆弱性統合の場合、Veracode 脆弱性統合を複数展開することができます。各展開には、独自の CI ルックアップルールのセットがあります。

> **注:**
> CI ルックアップルールは、脆弱性統合のすべての展開で共有されます。ルールが削除または変更された場合、その削除または変更は脆弱性統合のすべての展開に影響します。

脆弱性データのインポートはインスタンスに負荷をかける可能性があり、慎重にルールをビルドしないと、リソースのパフォーマンス問題が発生する可能性があります。 CMDB 内で反復して照合を実行するために使用されるロジックでは、処理時間が長くなる可能性があります。リソースの潜在的なデグレードやパフォーマンスの複雑化を回避するために、カスタム作成された CI ルックアップルールまたは事前定義された **CI** ルックアップルールの変更をテストします。孤立レコードの重複防止、データの削除、およびデータのクリーンアップの詳細については、「アプリケーション脆弱性対応 CI ルックアップルール実行後の重複レコードまたは孤立レコードの防止」を参照してください。

自動翻訳

関連情報

構成管理と CMDB

CI ルックアップルールを作成する

[CI ルックアップルール] モジュールには、構成管理データベース (CMDB) のどのフィールドに一致するデータがあるかを定義するルールが含まれています。これらのルールは、アプリケーションやアプリケーションリリースを識別し、アプリケーション脆弱性一致アイテム (AVI) に追加して修復に役立てるために使用されます。

始める前に

必要なロール：アプリセキュリティマネージャーグループ

このタスクについて

CI ルックアップルールを作成するには、ServiceNow および アプリケーション脆弱性管理 の高度な専門知識が必要です。既存のルックアップルールのいずれかを修復するのではなく、それをコピーしてコピーを修復することを検討してください。新しいルールで問題がなければ、元のルールを非アクティブ化します。

> **注:**
> ルールは、一度削除すると元に戻せません。新しいルールを作成する場合は、既存のルールを削除せずに非アクティブ化します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > **CMDB** > **CI** ルックアップルール.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

CI ルックアップルールフォーム

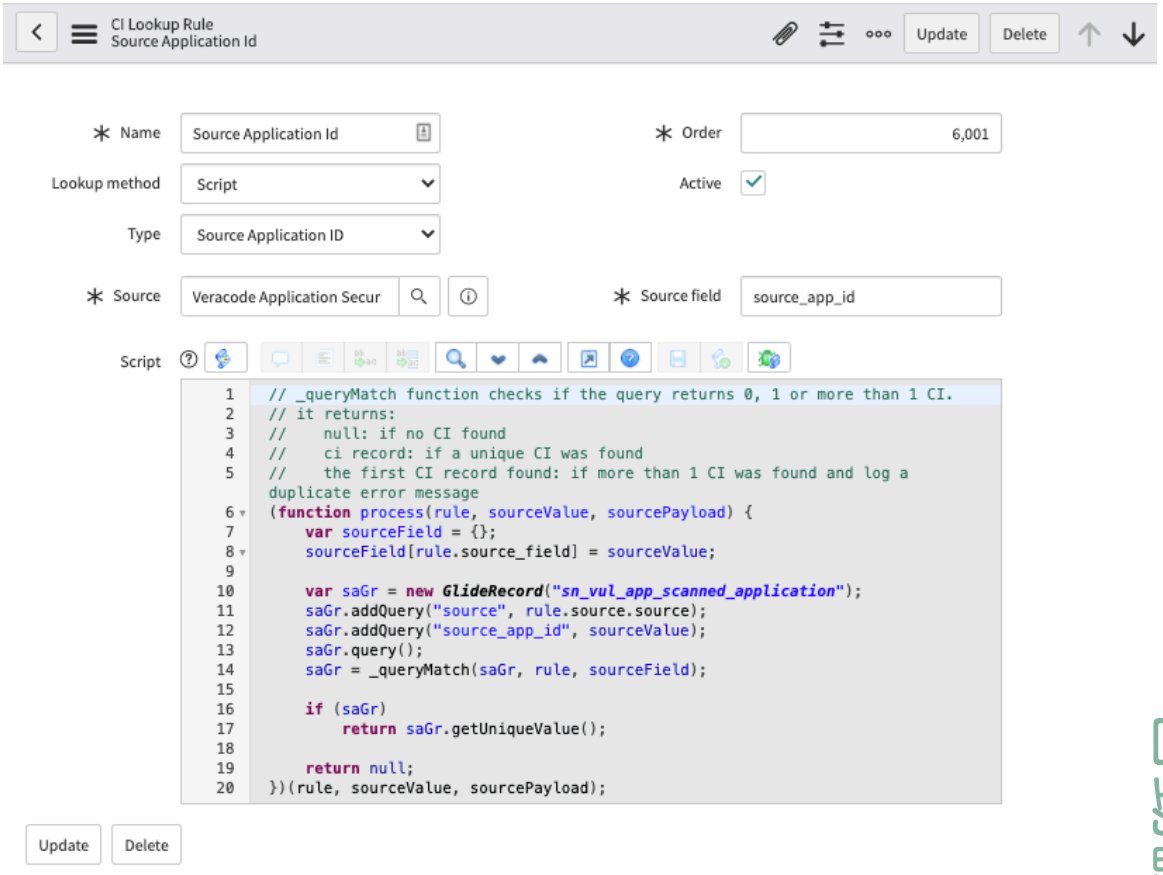
フィールド	説明
名前	ルールの名前。
ルックアップメソッド	照合に使用される方法。選択肢は次のとおりです。 ○ [スクリプト]：ビルド済みスクリプトまたはカスタムスクリプト。 ○ [一致するフィールド **(Field matching)]**：CMDB 内のテーブルまたはフィールドを検索します。
タイプ	スクリプト [ルックアップメソッド] で使用するタイプ。
順序	ルールの優先順位。順位が低い一致から順に評価されます。
有効	ルールがアクティブか無効かを示すチェックボックス。
ソース	このルールへの入力として使用されるソース。選択すると、条件フィルターが表示されます。
ソースフィールド	このルールへの入力として使用されるソースフィールド。フィールドは文字列または数値である必要があります。
説明	ルールを説明するテキスト。
V19.0：ルックアップターゲット	従うルックアップアプローチ。次から選択します。 ○ 構成アイテム ○ 製品モデル
スクリプト	[タイプ] に基づく編集可能なサンプルスクリプトが表示されます。デフォルト関数のテンプレートに含まれるコメントに従って、カスタムスクリプトを実装します。 **注:** process 関数には、*rule*、*sourceValue*、および *sourcePayload* の 3 つのパラメーターがあります。
CI テーブルで検索	CMDB 内を検索するテーブル。[ルックアップ方法] に一致するフィールドとともに使用されます。
V19.0：製品テーブルで検索	製品モデルの [ルックアップターゲット] を選択した場合、デフォルト値は [アプリケーションモデル] です。
CI フィールドで検索	CI を見つけるために使用できる情報を含むフィールド。[ルックアップ方法] に一致するフィールドとともに使用されます。このフィールドは、CI レコード、またはネットワークアダプタなどの関連レコードにあります。
V19.0：製品モデルフィールドで検索	製品モデルの [ルックアップターゲット **]** を選択した場合、デフォルト値は [名前] です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [送信] をクリックします。

スクリプトを使用した **CI** ルックアップルールの例



関連情報

[アプリケーション脆弱性一致アイテム] フィールド

アプリケーション脆弱性対応での **CI** ルックアップルールの再適用

構成アイテム (CI) ルックアップルールを再適用して、検出されたアプリケーションレコードの (スキャンされたアプリケーションおよび製品モデルの) 既存の CI を更新できます。

ルックアップルールの再適用

CI ルックアップルールを再適用すると、アクティブ化されたすべてのルールが既存の検出されたアプリケーションに適用されます。検出されたアプリケーションレコードの更新には時間がかかる場合があります。

検出された既存のアプリケーションにルールを再適用するには、次に移動します: **All** (すべて) > セキュリティオペレーション > **CMDB** > ルックアップルール をクリックし、[変更を適用] を選択します。

注:
アプリケーション脆弱性対応 の v25.0.3 以降、廃止された CI に関連する脆弱性一致アイテムと検出をクローズするために、新しい自動クローズルール「CI 廃止」が導入されました。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ルックアップターゲットの設定

デフォルトで、*sn_vul.use_product_model* システムプロパティはアクティブ化されています (**[true]** に設定されています)。CI ルックアップルールレコードのシステムプロパティの設定に応じて、検出されたアプリケーションレコードは次の方法で更新されます。

- [値] フィールドが **true** に設定されている場合、製品モデルは CI ルックアップルールのルックアップターゲットであり、検出されたアプリケーションは製品モデルで更新されます。
- [値] フィールドが **false** に設定されている場合、構成アイテム (スキャン済みアプリ) がルックアップターゲットになり、検出されたアプリケーションは構成アイテム (スキャン済みアプリケーション) で更新されます。

構成アイテムがターゲットとして使用されるように *sn_vul.use_product_model* システムプロパティを変更するには：

1. sn_vul.app_sec_manager ロールを持つユーザーとして、次の場所に移動します **All** (すべて) > システムプロパティ > **All** (すべて)
2. *sn_vul.use_product_model* を見つけます。
3. レコードを開きます。
4. [タイプ (Type)] フィールドを **false** に設定します。
5. [更新] を選択します。

このシステムプロパティをリセットする場合は、ルックアップターゲットがシステムプロパティ設定と一致するようにルールを変更する必要があります。たとえば、構成アイテムをターゲットとして使用するようにシステムプロパティをリセットした場合は、ルックアップターゲットを構成アイテムとして持つルールを見つけます。

1. これらのルールの [有効] チェックボックスをオンにし、[更新] を選択します。
2. 製品モデルをターゲットとして使用するルールを見つけ、[アクティブ] チェックボックスをオフにし、[更新] を選択して無効にします。

新しいルックアップルールを作成する場合は、ルールフォームでルールのルックアップターゲットを設定します。詳細については、「CI ルックアップルールを作成する」を参照してください。

アプリケーション脆弱性対応 **CI** ルックアップルール実行後の重複レコードまたは孤立レコードの防止

CMDB 内の構成アイテム (CI) の一致から生じる重複または孤立レコードを防ぐための措置を講じます。

脆弱性データのインポートはインスタンスに負荷をかける可能性があり、慎重にルールをビルドしないと、リソースのパフォーマンス問題が発生する可能性があります。CMDB 内で反復して照合を実行するために使用されるロジックでは、処理時間が長くなる可能性があります。ルール内の処理スクリプトを徹底的にテストしてデバッグすることで、プロセスの後半で発生する可能性のある問題を軽減できます。

重複レコードまたは孤立レコードの防止

- テストする CI ルックアップルールに固有の、小さいデータのサブセットを使用します。
  - テスト対象を除いて、すべての **[CI** ルックアップルール] を [非アクティブ] に設定します。
  - インポートされたアプリケーションと構成アイテム (CI) を分析し、想定される動作を観測していること、照合が適切に行われていることを確認します。
- [廃止] などの CI ステータスを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- テストデータを削除します。CI の照合で正しい動作または予想される動作を観察し始めたら、最初からやり直します。これは次の方法で実行できます。
  - テストに使用するデータの削除 ([テーブルからのデータの削除 **(Deleting data from tables)]** セクションを参照)
    - スキャン済みアプリケーション
    - アプリケーション脆弱性一致アイテム (AVI)
  - 手動で統合を再実行します。

。

テーブルからのデータの削除

データをインポートしたときに、問題があることに気付くことがあります。開発環境やパフォーマンス環境で発生した場合、より良い環境から再クローンできますが、そうでない場合もあります。

注:
これらのアクションを実行するには、ServiceNow の高度な専門知識が必要です。

テーブルからデータを削除するには、次の 4 つのオプションがあります。

- [テーブル構成] で [すべてのレコードを削除] を使用する。
- [自動フラッシュ] (sys_auto_flush.list) に移動し、新しい [自動フラッシュ] レコードを作成して、[テーブルクリーナー] を設定します。
- バックグラウンドスクリプトを使用して gs.truncateTable を切り捨てます。

  注:
  本番環境では *`truncateTable`* を使用しないでください。本番環境や共有環境で大規模な削除を実行する場合は、事前にサポート担当者にご相談ください。

- HI でデータを削除する要求を作成します。

アプリケーション脆弱性対応 のアプリケーション脆弱性一致アイテムを自動的にアサインする

アプリケーションタグ、または構成アイテム [cmdb_ci] 内のアサイン先グループやプラットフォームアサイン先グループに基づいて、アプリケーションの脆弱性を自動的にアサインし、アサインまでの平均時間を短縮します。

アプリケーション脆弱性一致アイテムを自動的にアサインする

[次を使用してアサイン] を使用して AVI をアサインするには、3 つの異なる方法があります。

注:
脆弱性対応 のアサインの推奨機能は アプリケーション脆弱性対応では利用できません。

- ユーザーグループ：このオプションを使用すると、既存の Now Platform® ユーザーグループを選択できます。
- ユーザーグループフィールド：このオプションを使用すると、cmdb_ci テーブルを使用して利用可能なアサイン先グループフィールドを選択できます。デフォルトでは、[ユーザーグループフィールド] の下のリストメニューに次の 3 つのグループフィールドが表示されます。
  - なし：この必須フィールドにデフォルト値がないことを示します
  - 構成アイテム：承認グループ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 構成アイテム：アサイン先グループ
- 構成アイテム：サポートグループ

- スクリプト：このオプションを使用すると、スクリプトを使用して条件を定義できます。このオプションには、コーディングまたは高度な ServiceNow の専門知識が必要です。

最優先のルール (リスクが重大な場合、または AVI は規制対応によって取り扱うべき場合など、特別な処理が必要なアイテム) を最初に実行します。次に、一般的なルールを実行します。この場合、特別な処理は必要なく、誰が責任を負うべきかがわかっています。最後に、AVI が属するべきアサイン先グループを決定するグループに、AVI をアサインするためのデフォルトルールを作成します。このグループは、決定を対象に別のルールを追加できます。このデフォルトルールは最後に実行されます。

アサインルールの評価プロセス

新しい AVI が作成、インポート、またはクローズされてから再度オープンされると、その AVI に対してアサインルールが評価されます。AVI は、クローズ後に再オープンされない限り、1 回しか評価されません。変更後にルールを手動で再適用することができます。

新規、更新、または再オープンされた AVI ごとに、次の処理が使用されます。

- 脆弱性アサインルールごとに、AVI がアサインフィルター (順序が最下位のアサインルールが優先) と比較されます。
- 条件に一致すると、AVI にアサイン先グループがアサインされます。ルックアップは停止します。
- 他のすべてのルールの中で条件が一致しない場合、デフォルトルールが存在すれば、AVI はデフォルトのアサイン先グループにアサインされます。

> **注:**
> デフォルトルールがない場合、AVI は未アサインの状態のままになります。

[手動] または [ルール] の [アサインタイプ]、および [アサインルール] は、アプリケーション脆弱性一致アイテム (AVI) フォームのフォームレイアウトスラッシュバケットから利用可能です。最初にルールによってアサインされたが、後で手動で再アサインされた AVI には、元のルールへの参照が含まれています。[アサインルール] と [アサインタイプ] 情報を使用して、アサインルールが意図した受信者に対して適切なマッチングを見つけられなかったケースを特定しますまたは、どのルールの再アサインが最も多いかを確認します。

> **注:**
> アサインルールは、手動作成されたアサインは再評価しません。

アサインルールを再適用する

アサインルールを変更する場合は、[アサインルール] リストビューの [変更を適用] ボタンを使用して、すべてのアクティブなオープン AVI で変更されたルールを再実行します (手動でアサインされたルールを除く)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

最初に [変更を適用] を使用する前に *Reapply all vulnerability assignment rules* のスケジュール済みジョブが実行されていない場合は、手動でアサインされた AVI を除くすべてのオープン AVI に対して、すべてのアサインルールが実行されます。その後、[変更を適用] を使用すると、変更されたルールと依存ルールのみが再実行されます。あるルールを変更すると、変更されていない別のルールに AVI が一致することがあります。[store-future: BEGIN review]アサインルールを再適用しても、脆弱性一致アイテムは再グループ化されません。[End]

スケジュール済みジョブ [*Reapply all assignment rules*] は、デフォルトでは非アクティブです。アクティブ化すると、手動でアサインされたものを除くすべてのオープン AVI に対して、すべてのルールが適用されます。[日次]、[週次]、[月次]、[定期的]、**[1** 回]、または [オンデマンド] で実行できます。環境内のアクティブな AVI の数に応じて、最初の実行後に [実行] フィールドを適切に設定して、パフォーマンスに影響がないようにすることを忘れないでください。

アプリケーション脆弱性対応 アサインルールの作成または編集

フィルター条件に基づいて、アプリケーション脆弱性一致アイテム (AVI) を自動的にアサインするルールを作成できます。これらのルールは、インポートまたは手動作成時に AVI をアサインします。

始める前に

必要なロール：アプリセキュリティマネージャーグループ

このタスクについて

アサインルールでは、アサインの条件と実行順序を定義します。AVI がルール条件に一致すると、アサインルックアップは停止します。詳細については、「アプリケーション脆弱性管理 内のフィルタリング」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > アサインルール.
2. [**New**] をクリックします。
3. [新規] の場合、必要に応じて、フォームのフィールドに入力します。

アプリケーションの脆弱性アサインルール

フィールド	説明
名前	グループルールの名前。
有効	アサインルールがアクティブかどうかを示します。
実行順序	このルールが評価される順番。 最優先のルール (リスクが重要な特別な処理が必要なアイテム、または規制コンプライアンスによる AVI の処理が必要なアイテム) が最初に実行されます。次に、一般的なルールを実行します。この場合、特別な処理は必要なく、誰が責任を負うべきかがわかっています。最後に、AVI が属するべきアサイン先グループを決定するグループに、AVI をアサインするためのデフォルトルールを作成します。このグループは、決定を対象に別のルールを追加できます。このデフォルトルールは最後に実行されます。
説明	アサインルールの説明。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
条件	
条件フィールド	満たす必要がある条件。
新しい基準	選択する条件フィルターフィールドを追加します。
次を使用してアサイン	このルールに基づいて作成されたグループのアサインを自動化するには、利用可能なオプションの 1 つを選択します。 ○ ユーザーグループ：ルックアップテーブルからユーザーグループを選択します。 ○ ユーザーグループフィールド：リストメニューからユーザーグループフィールドを選択します。 ○ スクリプト：スクリプトを作成または編集します。 **注:** スクリプトの作成または編集には ServiceNow の専門知識が必要です。

4. **[Submit]** をクリックします。
   次のインポートで新しいルールまたは更新されたルールが評価されます。

アプリケーション脆弱性対応 のリスクを自動的に計算する

アプリケーション脆弱性算出は、アプリケーション脆弱性一致アイテム (AVI) のフィールドの初期リスク値の計算を自動化します。リスク計算により、修復の優先順位を決めるインサイトが得られます。各算出の条件が順番に評価され、最初に一致した算出が使用されます。

アプリケーション脆弱性算出

アプリケーション脆弱性対応 ベースシステムには、アプリケーション脆弱性一致アイテムのベース [リスクスコア] を設定する 2 つの脆弱性算出が含まれています。

- 基本的なリスク算出
- 高度なリスク算出

アプリケーション脆弱性算出は、条件フィルターを使用することにより、任意の条件に基づいて AVI の影響度を優先順位付けして評価するようにビルドすることができます。脆弱性のビジネスインパクト、構成アイテム (CI) のクラス、または AVI の経過時間など、追加の脆弱性算出を作成して AVI に他のフィールドを設定できます。または、既存の脆弱性算出機能をカスタマイズすることも可能です。算出は、どのような優先順位でも反映できるように記述できます。詳細については、「アプリケーション脆弱性管理 内のフィルタリング」を参照してください。

AVI には、リスク算出から導出された [リスクスコア] 値が含まれています。

注: AVI は [ソース重大度] を表示しますが、正規化された重大度は表示しません。正規化された重大度は、[リスクスコア] 値を取得するための算出によって使用されますが、AVI には表示されません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

各算出機能には、算出ルールのリストが含まれ、その条件によりどのような場合に適用するのかが決定されます。算出が実行されると、各算出ルールの条件が順番に評価され、最初に一致した算出ルールが使用されます。

有効なすべての脆弱性算出は、AVI が作成されるたびに、関連付けられた CI または脆弱性が変更された場合に、選択したフィールドを設定します。

正規化された脆弱性重大度を使用して、[基本的なリスク] 算出が AVI の [リスクスコア] を計算します。

注:
一度にアクティブにできる算出は、ターゲットフィールド ([リスクスコア]) ごとに 1 つのみです。

[基本的なリスク] はデフォルトで有効になっています。**[Advanced Risk** 計算機] はデフォルトで非アクティブになっています。

アプリケーション脆弱性算出ルール

ベースシステムの [基本的なリスク算出] の計算には、重大度 (なし～重大) ごとに、重大度に基づいて [リスクスコア] の値 (0 ～ 100) をアサインする算出ルールが含まれています。[不明な重大度] には、リスクスコア 100 が自動的にアサインされます。これらの値は調整可能で、[高度なリスク算出] のように、新しい算出ルールやリスクルールを作成できます。

注:
アプリケーション脆弱性対応の v23.0 以降では、AVIT でリスクスコアが更新されるたびに、[メモ] セクションが次の詳細で更新されます。

- 算出グループ名
- 算出名：算出ルールがテンプレートとスクリプトのどちらに基づいているかに応じて、名前に括弧で囲まれた詳細が追加されます。算出ルールの基準を変更または表示するには、任意のルールを選択し、[詳細表示] チェックボックスをオンにします。[値のタイプ **(Value type)]** ドロップダウンボックスから、必要なオプションを選択します。[テンプレート] を選択した場合、リスクスコアはルールで指定された条件に従って更新されます。[スクリプト] を選択した場合、既存のスクリプトを追加または更新できます。システムプロパティ *sn_sec_cmn.risk_score_changes_add_worknotes* は、[作業メモ] セクションへの入力に役立ちます。アプリケーション脆弱性対応 v25.0.3 以降、システムプロパティ*sn_sec_cmn.risk_score_changes_add_worknotes*はデフォルトで無効になっています。これを有効にした場合にのみ、アプリケーション脆弱性一致アイテムのリスクスコアに関連するすべての変更を [作業メモ] セクションで確認できます。また、作業メモは、リスクスコアに変更がある場合にのみ更新されます。

ベースシステムの [高度なリスク算出] には、[デフォルトのリスクルール]と呼ばれる特殊な脆弱性算出ルールが含まれています。複数の値に基づいて、[リスクスコア] が計算されます。

- 脆弱性重大度
- OWASP 上位 10 件
- SANS 上位 25 位

デフォルトのリスクルールの基準をカスタマイズできます。詳細については、「リスクルールのフィールドと重み付けを定義する」を参照してください。

[デフォルトのリスクルール] で使用する値と、これらの各値の重み付けを調整できます。重み付けは、[リスクスコア] を設定するときに各要素をどの程度考慮するかを調整するために使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

各ルールには [順序] 設定がありますが、条件に一致する最初のルールによって AVI の [リスクスコア] フィールドが更新されます。通常、スクリプト化されていない算出ルールは、スクリプト化された算出ルールよりもパフォーマンスへの影響が少なくなります。

脆弱性のリスクスコアの重み付け

すべての脆弱性には、重大度、重要度、エクスプロイト情報などの要素に基づいてリスクスコアと評価がアサインされます。このリスク評価の算出を担当するのが、脆弱性一致アイテムのテーブルのビジネスルール *`Update Risk Rating from Risk Score`* です。リスクスコアが変更されるたびに、脆弱性一致アイテムのリスク評価が算出されて入力されます。脆弱性対応 (VR) アプリケーションのバージョン 17.1 より前では、次のリスク評価がスクリプトインクルード VulnerabilityUtils の一部として提供され、ハードコードされていました。

値 (リスク評価)	重み付け (リスクスコア)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

脆弱性対応 のバージョン 18.0 以降では、

- 出荷時のリスク評価タイプはベーステーブルで avr_risk_rating となっています。リスク評価タイプは、リスク評価が計算される各テーブルのビジネスルールの一部として渡されます。
- リスク評価の算出の対象となる [リスクスコアの重み付け] テーブルの値をクエリできるように、スクリプトが変更されます。
- 既存のタイプにエントリを追加するか、新しいタイプを作成します。新しいタイプを作成するときは、新しいリスク評価のラベルを追加し、関連するスクリプトとビジネスルールも変更してください。新しいリスクスコアのスタイルも新たに追加する必要があります。
- ベーステーブルのレコードをクエリするようにスクリプトを変更します。

[リスクスコアの重み付け] テーブルにアクセスするには、フィルターナビゲーターに「sn_sec_cmn_risk_score_weight」と入力します。

さらに、次のシナリオではリスクスコアが自動的に再計算されます。

- 構成アイテム (CI) が非インターネットフェーシングからインターネットフェーシングに変更されたとき。
- 脆弱性一致アイテム (VI) の関連する一般的な脆弱性とエクスポージャー (CVE) またはサードパーティエントリー (TPE) が、CVE の既知の悪用された脆弱性 (KEV) にリンクされている場合。

リスクルールのフィールドと重み付けを定義する

組織に固有の脆弱性や資産データを利用したリスクスコアを生成できるように、リスクルールのパラメーターと重み付けをカスタマイズします。リスクルールに含まれるフィールドを選択することで、効果的なリスクスコアリングフレームワークを定義できます。

始める前に

必要なロール：sn_vul.app_manage_risk_score_configuration

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > 脆弱性の算出.
2. [脆弱性算出] ページで、[高度なリスク算出] をクリックします。
3. 次のように移動する。 [脆弱性算出] ページ > [脆弱性算出ルール] タブ > デフォルトのリスクルール.
4. オプション: [脆弱性リスクルール] ページの [リスク算出基準] セクションで、全体的なリスクスコアの計算における重要性に従って、各基準の重み付けを設定します。
5. ルールを非アクティブ化するには、[アクティブ] チェックボックスをオフにします。
6. リスク算出基準にリスクルールフィールドを追加するには、[基準を追加] をクリックします。
7. フォームのフィールドに入力します。

リスクルールのフィールドフォーム

フィールド	説明
参照テーブルを選択	リスクスコアの重み付けの定義に使用するテーブル。次のオプションのいずれかを選択できます。 ○ [アプリケーション脆弱性一致アイテム]：脆弱性一致アイテム (VI) から直接ドット連結可能なフィールドを追加します。 ○ [アプリケーション脆弱性一致アイテム - 構成アイテム]：ハードウェアテーブルなど、ベーステーブルの拡張の一部であるドット連結可能なフィールドを追加します。これらのフィールドはベーステーブル (cmdb_ci) に含まれていません。 ○ [アプリケーション脆弱性一致アイテム - 脆弱性]：サードパーティエントリーなど、ベーステーブルを拡張するテーブルに含まれるドット連結可能なフィールドを追加します。これらのフィールドは、脆弱性エントリーベーステーブルの一部ではありません。 ○ [アプリケーション脆弱性一致アイテム参照テーブル **(Application Vulnerable Item Reference Table)]**：関連テーブル (m2m) に含まれるフィールド、または脆弱性一致アイテムへの参照を持つテーブルを追加します。これらのフィールドは、VI から直接ドット連結することはできません。 ○ [構成アイテム参照テーブル]：関連テーブル (m2m) に含まれるフィールド、または cmdb_ci への参照を持つテーブルを追加します。これらのフィールドは、VI から直接ドット連結することはできません。 ○ [脆弱性参照テーブル]：関連テーブル (m2m) に含まれるフィールド、または sn_vul_entry への参照を持つテーブルを追

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	加します。これらのフィールドは、VI から直接ドット連結することはできません。 ○ [カスタム条件]：条件を評価することでルールに重み付けをアサインするには、このオプションを使用します。たとえば、インターネット向けフィルターは、構成アイテム (CI) が外部か内部かを判断します。
テーブル	[参照テーブルを選択] から次のいずれかのオプションが選択されている場合にのみ表示されるフィールド。 ○ [アプリケーション脆弱性一致アイテム] -> [構成アイテム] ○ [アプリケーション脆弱性一致アイテム] -> [脆弱性] ○ アプリケーション脆弱性一致アイテム参照テーブル ○ 構成アイテム参照テーブル ○ 脆弱性参照テーブル
フィールド	このルールのリスクスコア算出に使用するフィールド。
集計	[参照テーブルを選択] から参照テーブルが選択されている場合にのみ表示されるフィールド。関連テーブル (m2m) から [フィールド] が選択されている場合に、算出で考慮する最小値または最大値を選択します。
重み付け	リスクルール内でのこのフィールドの重み付け。値は 0 ～ 100 の整数である必要があります。
値の重み付けを定義	各フィールド値に重み付けをアサインするコンポーネント。数値フィールドの場合、フィールド値は範囲 (1 ～ 5 など) として定義できます。重み付けは 0 ～ 100 の整数でなければなりません。 **注:** [カスタム条件] オプションが [参照テーブルを選択] で選択されている場合、このフィールドは表示されません。
条件テーブル	[参照テーブルを選択] からカスタム条件が選択されている場合にのみ表示されるフィールド。条件をリストから選択します。
フィールド名	[参照テーブルを選択] からカスタム条件が選択されている場合にのみ表示されるフィールド。リスク基準の名前を入力します。
条件	[参照テーブルを選択] からカスタム条件が選択されている場合にのみ表示されるフィールド。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	定義された条件に一致するこのテーブルのアイテムをプレビューします。

8. **[Submit]** をクリックします。
9. [ルール] ページで、ルールをアクティブ化して再適用し、アクティブな脆弱性一致アイテムのリスクスコアを再評価します。

Example:
ソース重大度をリスクルールの基準として追加します。

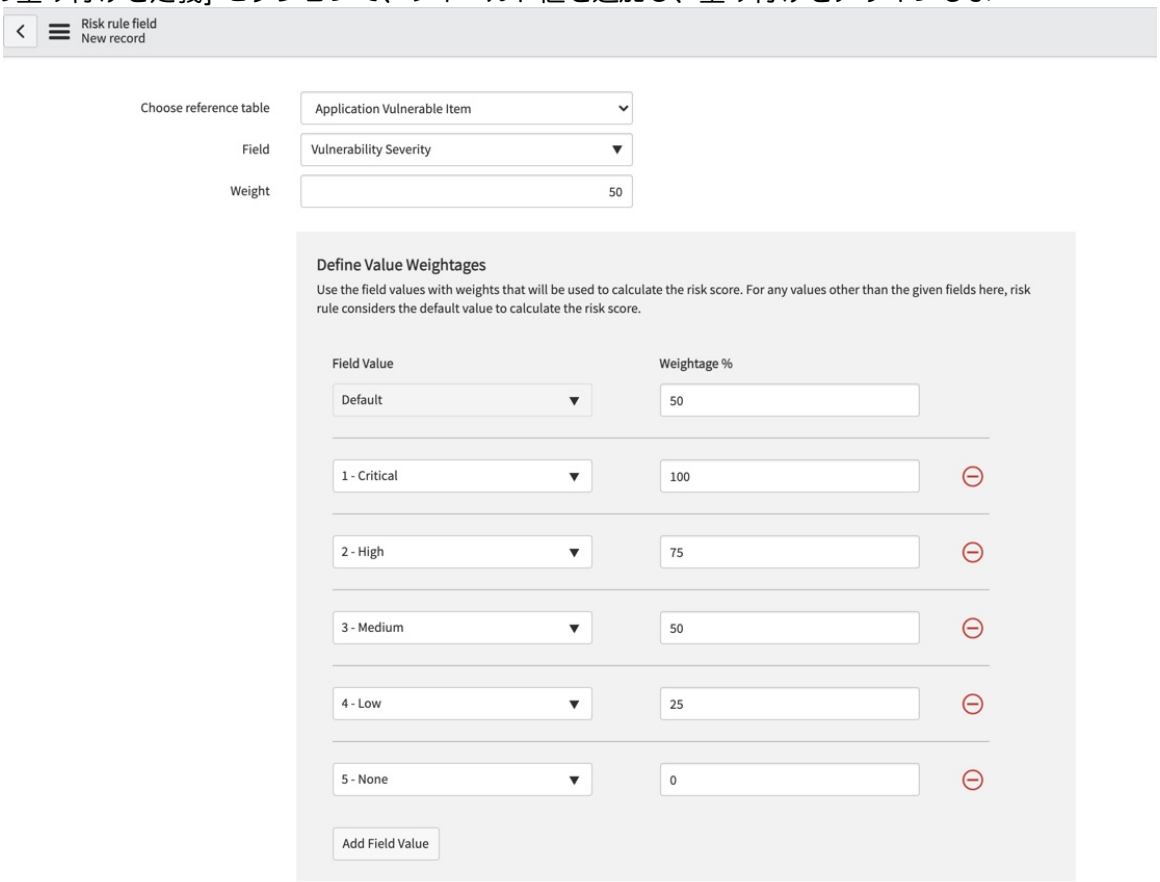
ユースケース：Qualys や Tenable などのサードパーティベンダーが独自のスコアを提供します。これらのスコアは、sn_vul_entry テーブルの [ソース重大度] フィールドに入力されます。このフィールドはリスクスコアの算出に使用します。このスコアを使用してリスクスコアを算出するには、次の操作を行います。

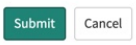
1. [リスクルール] ページに移動します。
2. ルールを非アクティブ化するには、[アクティブ] チェックボックスをオフにします。
3. リスク算出基準にリスクルールフィールドを追加するには、[基準を追加] をクリックします。
4. [参照テーブルを選択] リストから、[アプリケーション脆弱性一致アイテム] を選択します。
5. フィールドリストから、**[Vulnerability.Severity]** を選択します。
6. [重み付け] フィールドで、リスクルール内でのこのフィールドの相対的な重要度を入力します。値は 0 ～ 100 の整数である必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. [値の重み付けを定義] セクションで、フィールド値を追加し、重み付けをアサインしま



す。 

8. [送信] をクリックします。

関連情報

Vulnerability Response 算出および脆弱性算出ルール

アプリケーション脆弱性算出を作成する

アプリケーション脆弱性算出は、特定の基準が満たされたときにターゲットフィールドを計算するために事前定義された式です。アプリケーション脆弱性一致アイテム (AVI) の [リスクスコア] を計算する算出には、[リスクルール] を含めることができます。リスク計算により、修復の優先順位を決めるヒントが得られます。

始める前に

必要なロール：アプリセキュリティマネージャーグループ

注:
スクリプトを含むアプリケーション脆弱性算出を実行すると、パフォーマンスの低下を感じることがあります。

最も単純なルールが最初に実行されるようにルールを並べ替えてください。条件とテンプレート値またはリスクルールで処理できないアイテムに対してのみ、スクリプトを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > 脆弱性の算出.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

脆弱性算出フォーム

フィールド	説明
名前	アプリケーション脆弱性算出の名前。
テーブル	AVI テーブルの名前が自動入力されます。
アプリケーション	脆弱性対応 が自動入力されます。
ターゲットフィールド	計算するためのフィールド。
説明	算出のテキスト説明。
有効	算出をオンまたはオフにします。

4. ヘッダーを右クリックして、[保存] を選択します。
[脆弱性算出ルール] セクションが表示されます。
5. [新規] をクリックして、算出ルールを作成します。

> **注:**
> [新しいリスクルール] フォーム ([ターゲットフィールド] が [リスクスコア] の場合にのみ使用可能) については、ステップ 10 を参照してください。

6. 必要に応じてフィールドに入力します。

[脆弱性算出ルール] フォーム

フィールド	説明
名前	算出ルールの名前。
順序	脆弱性算出を実行する順序。順序エントリーが 100 の算出は、順序エントリーが 200 の算出の前に実行されます。
算出	算出の親が自動入力されます。
有効	デフォルトでは、[アクティブ] チェックボックスがオンになっています。これは、算出ルールがアクティブであることを意味します。このチェックボックスをオフにすると、システムに作成された新しい脆弱性一致アイテムにこのルールは適用されません。
詳細表示	選択すると、[条件タイプ] と [値タイプ] から、スクリプト化された条件とスクリプト値を選択できます。

7. 必要に応じて、[この条件を満たしている場合] タブのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[この条件を満たしている場合] タブ

フィールド	説明
条件タイプ	[詳細ビュー **(Advanced view)**] を選択すると使用できます。次の選択肢があります。 ○ フィルター：フィルター条件を使用します。 ○ フィルターグループ：「フィルターグループの作成と定義 (create and define filter groups)」を参照して、算出基準を定義します。 ○ スクリプト：この算出を適用するタイミングを決定するために使用されるスクリプト条件。 **注:** 算出を適用するタイミングを決定するスクリプトを記述する前に、[アプリケーション脆弱性算出] リストに戻ります。ベースシステムに付属している脆弱性算出レコードを確認します。
条件	算出を使用するかどうかを決めるための基本的なフィルター条件を定義します。 [フィルターグループ] または [スクリプト] の条件タイプのいずれかを選択すると、このフィールドは非表示になります。

8. [これらの値を設定 **(Set these values)**] タブをクリックし、必要に応じて、フォームのフィールドに入力します。

[これらのフィールドを設定 **(Set these fields tab)**] タブ

フィールド	説明
値のタイプ	[詳細ビュー **(Advanced view)**] を選択すると使用できます。次の選択肢があります。 ○ テンプレート：各フィールドに設定する値を定義します。 ○ スクリプト：各フィールドの値を設定するために使用します。
スクリプト値	[スクリプト] の値タイプを選択した場合に使用できます。 計算を適用する値を定義します。
テンプレート	算出に使用するフィールドと値を選択します。 [スクリプト] 値タイプのいずれかを選択すると、このフィールドは非表示になります。

9. すべての入力が完了したら、[送信] をクリックします。

注: 既存の算出を編集し、既存のすべてのスコアを更新する場合は、 [算出を再適用] ボタンを使用できます。すべてのアクティブな AVI を処理し、その算出を使用して値を設定する場合は、それらの AVI の値を再計算します。算出の再適用には時間がかかるため、スケジュール済みジョブで処理されます。

10. 必要に応じて、[新しいリスクルール] フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

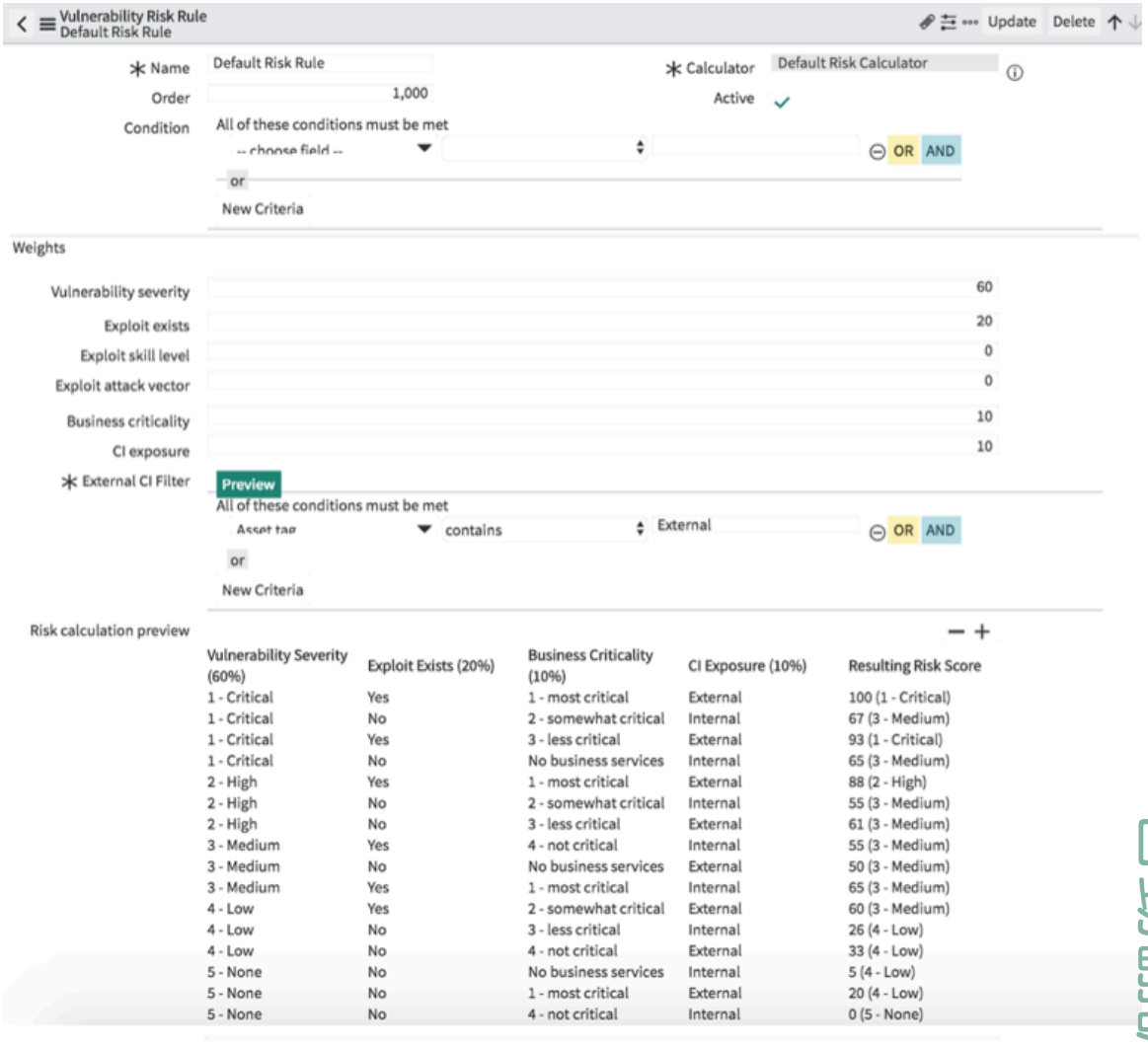
自動翻訳

その値から取得されるべき結果の割合に従って、各重み付けを設定します。スキャナーで提供されないデータ、またはリスクスコアに含めるべきでないデータについては、重み付けをゼロに設定します。

重み付けを更新すると、残りの重み付けと想定される [リスクスコア] の結果がシナリオに表示されます。

フィールド	説明
名前	算出ルールの名前。
順序	算出を実行する順序。順序エントリーが 100 の算出は、順序エントリーが 200 の算出の前に実行されます。
算出	算出の親が自動入力されます。
有効	デフォルトでは、[アクティブ] チェックボックスがオンになっています。これは、算出ルールがアクティブであることを意味します。このチェックボックスをオフにすると、システムに作成された新しい脆弱性一致アイテムにこのルールは適用されません。
条件	算出を使用するかどうかを決めるための基本的なフィルター条件を定義します。 [フィルターグループ] または [スクリプト] の条件タイプのいずれかを選択すると、このフィールドは非表示になります。
重み付け	
脆弱性重大度	重大度に基づく結果の割合。
OWASP 上位 10 件	OWASP 上位 10 件のリストに脆弱性が存在することに起因する結果の割合。この情報が脆弱性に存在しない場合は、重み付けをゼロに設定します。
SANS 上位 25 位	SANS 上位 25 位のリストに脆弱性が存在することに起因する結果の割合。この情報が脆弱性に存在しない場合は、重み付けをゼロに設定します。
現在までの累計	自動計算された割合の合計。この値が 100 に達すると、シナリオのプレビューにさまざまなシナリオのサンプルリスクスコアが表示されます。
サンプルシナリオ	すべての重み付けの合計が 100% になると、リスクスコアのシナリオが表示され、考えられる一部のシナリオでリスクスコアのプレビューが示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

11. [送信] をクリックします。

アプリケーション脆弱性一致アイテムの重大度を自動的にマッピングする

アプリケーション脆弱性対応 重大度マッピングは、サードパーティソースの重大度フィールドを 脆弱性対応 内で認識可能なフィールドに変換します。

始める前に

必要なロール：アプリセキュリティマネージャーグループ

このタスクについて

Veracode 脆弱性統合 などの アプリケーション脆弱性対応 サードパーティ統合は、インストール時に重大度マッピングを提供します。これらのマップは、既存のマップのフィールドを変更することで調整できます。

重大度マップの作成または編集は、自分の環境におけるカスタマイズされたまたは非標準のサードパーティマッピングのみを対象としており、アプリケーション脆弱性対応 および ServiceNow の専門知識が必要です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > 正規化された重大度マッピング.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

フィールドマッピング

フィールド	説明
ソース	重大度マッピングのソースの名前。
ソース値	ソース重大度の値。
ターゲット値	ターゲットの重大度の値。選択肢は次のとおりです。 ○ 1- 重大 ○ 2 - 高 ○ 3：中 ○ 4：低 ○ 5：なし

4. ソース重大度レベルごとにステップ 3 を繰り返します。
5. **[Submit]** をクリックします。

アプリケーション脆弱性管理 内のフィルタリング

算出とアサインルールは、[条件ビルダー] を使用して作成されたインポート時の条件を使用します。各レコードはこうしたフィルターを使用して評価されるため、基準を変更するとパフォーマンスに影響する場合があります。

ベースシステムに含まれるルールと算出は、パフォーマンスが最適化されています。ルールや算出の編集または作成には注意が必要であり、ServiceNow と アプリケーション脆弱性対応 の両方の専門知識が必要になる場合があります。そのため、いくつかのガイダンスが利用可能です。

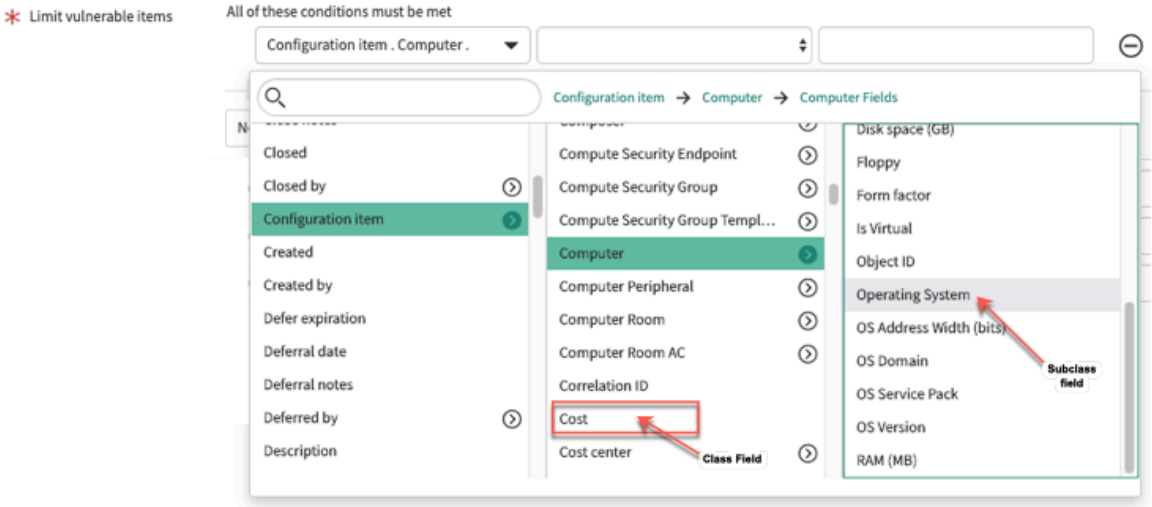
サブクラスフィールドに基づくフィルタリングの回避

一部のテーブルは拡張をサポートしています。CMDB CI [cmdb_ci] テーブルはその一部です。cmdb_ci_hardware や cmdb_ci_computer などのテーブルは、このテーブルを拡張します。親テーブルにないフィールドに基づいてフィルタリングを行う場合、そのフィルターのビルドと評価に費用を要する場合があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

条件フィルタードロップダウンメニュー



たとえば、 構成アイテム > コスト コストは構成アイテムのクラスフィールドであり、サブクラスフィールドではないため、パフォーマンスに悪影響を与えることはありません。

構成アイテム > コンピューターただし、別のフィールド (この場合は **Operating System**) へのドット連結を必要とするサブクラスです。このプロセスには何ミリ秒もかかる場合があり、何百万のもの脆弱性一致アイテムをインポートする場合、すぐに累積してしまい、パフォーマンスに影響を与えます。

注:
[contains] 条件の使用はワイルドカード検索に似ており、パフォーマンスに影響を与える可能性があります。可能な場合は [次の値に等しい] を使用する方が効率的です。

アプリケーション脆弱性対応 で修復ターゲットトラッキングを自動化する

アプリケーション修復ターゲットルールは、アプリケーション脆弱性一致アイテム (AVI) を修復するための予想期間を定義し、脆弱性そのものを修復するための期間を提供します。たとえば、アプリケーション脆弱性一致アイテムに重大なリスク評価が含まれている場合、そのアイテムの脆弱性を 15 日以内に修正する必要があります。

アプリセキュリティマネージャーは、以下を定義することによってアプリケーション修復ターゲットルールを作成できます。

- 修復ターゲット
- リマインダーターゲット
- [store-future: BEGIN review]リマインダーおよび通知の受信者：AVI がリマインダーまたは修復ターゲット日を過ぎ、修復されていない場合に通知する必要があるユーザー。[End]

アプリセキュリティマネージャーは、AVI フォームおよびリストビューで修復ターゲット日を表示できますが、[保留]、[解決済み]、または [クローズ済み] ステータスの AVI の日付は更新されません。

[修復ターゲット日] は、次のように AVI リストビューでは色付きのドットで表示されます。

- 通知日に達していない AVI は緑色で示されます。
- 修復ターゲット日が近づいている AVI はオレンジ色で示されます。
- 修復ターゲット日が過ぎた AVI は赤色で示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[store-future: BEGIN review]1 つ以上の AVI について、修復ターゲット日に近づいているか、修復ターゲット日が過ぎていると、アプリケーション修復ターゲットルールごとに概要メールが送信されます。[End]

デフォルトのルール

アプリケーション脆弱性対応 は、デフォルトで非アクティブになっている 3 つのデフォルトルールが付属した状態で出荷されます。

- 重大なリスク評価ルール：リスク評価が **[1 - 重大 (1-Critical)]**、修復ターゲットが 15 日、リマインダーがターゲット日の **[7]** 日前である修復ターゲット。
- 中から高のリスク評価ルール：リスク評価が **[1 - 高 (2-High)]** または **[3 - 中 (3-Medium)]**、修復ターゲットが 30 日、リマインダーがターゲット日の **[7]** 日前である修復ターゲット。
- 重大度の低いリスク評価ルール：リスク評価が **[4 - 低 (4-Low)]**、修復ターゲットが 45 日、リマインダーがターゲット日の **[7]** 日前である修復ターゲット。

修復ターゲットルールは非アクティブ化または削除が可能

ルールが非アクティブ化されると、ルールが適用された AVI の現在の修復ターゲット日がクリアされます。AVI がアクティブなルールを満たしている場合はそのルールが適用され、そうでない場合は、ルールもターゲット日もなく、ステータスは [ターゲットなし] になります。

ルールが削除されると、クローズされた AVI の [修復ターゲット] 日と関連フィールドは保持されます。クローズされていない AVI の [修復ターゲット] 日と関連フィールドはクリアされ、依存ルールが再適用されます。

修復ルールのシナリオ

複数の修復ターゲットルールが同じ AVI に適用される場合は、最も制限の厳しいルールが適用されます。

たとえば、AVI が 2 つのアプリケーション修復ターゲットルールの条件を満たす場合、

シナリオ：AVI の最終オープン日時は 2018 年 3 月 1 日 10:00:00。

- アプリケーション修復ターゲットルール 1：最終オープン日時は 2018 年 3 月 7 日、修復ターゲットは最終オープンから 15 日、算出された修復ターゲット日は 2018 年 3 月 16 日 10:00:00。
- アプリケーション修復ターゲットルール 2：最後オープン日時は 2018 年 3 月 10 日、修復ターゲットは最終オープンから 10 日、算出された修復ターゲット日は 2018 年 3 月 11 日 10:00:00。

このシナリオでは、 より厳しい日付制限のアプリケーション修復ターゲットルール 2 が AVI に適用されます。(AVI の最初の識別日時から 10 日、15 日。)

注:
アプリケーション修復ターゲットは、[最終オープン日] の日付に日数 (24 時間単位で測定) を加えて算出されます。このフィールドは、フォームレイアウトのスラッシュバケットから AVI フォームに追加できます。これは、インスタンスで AVI が最後にオープンされた日付です。

V17.1 以降では、修復ターゲットは [ターゲット開始 (日付)] から算出されます。デフォルト値は [最終オープン日] のままです。

注:
アプリケーション修復ターゲットルールが定義されると、[修復ターゲットルール] リストビューの *Evaluate remediation targets* スケジュール済みジョブまたは [変更を適用] ボタンによって修復ターゲット日が算出されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

修復ターゲットのスケジュール済みジョブの評価について

Evaluate remediation targets は、毎日 4:00:00 に 1 回実行されます。

Evaluate remediation targets は、修復ターゲット日が最も早いルールから順に、アクティブなすべての脆弱性ルールを反復処理します。次のようなすべての AVI を対象とします。

- [クローズ済み]、[保留]、または [解決済み] のいずれのステータスでもない。
- 修復ターゲット日がない。
- アプリケーション修復ターゲットルールの日付より後の修復ターゲット日がある。

Evaluate remediation targets は、修復ターゲット日が存在しない場合は追加し、このルールにレコード内の日付よりも前の日付が含まれている場合は、既存のターゲット日を更新します。最後に、AVI フォームの [修復ターゲット日] フィールドと [修復ステータス] フィールドが更新されます。非アクティブルールの場合、[修復ターゲットを評価 **(Evaluate remediation targets)]** は AVI の修復フィールドをクリアします。

修復ターゲットルールを再適用する

修復ターゲットルールを変更する場合、[修復ターゲットルール] リストページの [変更を適用] ボタンを使用して、[クローズ済み]、[保留]、または [解決済み] ステータスのルールを除き、すべてのアクティブなオープン AVI で変更されたすべてのルールを再実行します。

注:

スケジュール済みジョブ *Evaluate remediation targets* が実行されている場合、再適用プロセスを開始することはできません。ただし、再適用プロセスが既に実行されていて、スケジュール済みジョブがトリガーされると、それらは並行して実行されます。

脆弱性対応 および アプリケーション脆弱性対応 の再適用プロセスは独立しており、並行して実行できます。

アプリケーション修復ターゲットルールの作成または編集

アプリケーション脆弱性一致アイテム (AVI) レベルで修復ターゲットルールを設定することで、リスクの高い脆弱性の修復をタイムリーに促進します。

始める前に
必要なロール：アプリセキュリティマネージャーグループ

注:
ベースシステムには、 3 つの修復ターゲットルールが含まれています。

- 重大なリスク評価ルール
- 重大度の低いリスク評価ルール
- 中から高のリスク評価ルール

これらのルールは、デフォルトでは非アクティブです。新しいものを作成するのではなく編集する場合は、保存する前に [アクティブ] ボックスをオンにすることを忘れないでください。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アドミニストレーション > 修復ターゲットルール.
2. [**New**] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
名前	ルールの名前。
ターゲット (日数)	最後に開いてから AVI を修復するまでの日数を指定します。
V17.1：ターゲット開始日 (日付)	ターゲット SLA が算出される日付。日付タイプまたは日付と時刻タイプのフィールドのみを指定できます。デフォルト値は [最終オープン日] です。このフィールドの値をカスタマイズするには、「KB1642413」を参照してください。
アクティブ	デフォルトでは、[アクティブ] チェックボックスがオンになっています。これは、修復ターゲットルールがアクティブであることを意味します。このチェックボックスをオフにすると、システムに作成された新しい AV にこのルールは適用されません。
通知 (期限前の日数)	リマインダーを設定するターゲット修復時間までの日数。この値を使用して計算された通知日は、修復ステータスを表示するために使用され、色分けされています。日付が通知日より前の場合、修復ステータスは「実行中」になります。通知日を過ぎており、修復ターゲット日より前の場合、ステータスはターゲット間近として表示されます。 **注:** このフィールドが 0 に設定されている場合、[ターゲット経過] 通知のみが設定されます。
ルールの適用先	条件フィルターを使用して、ルールを AVI に適用するための基準を選択します。パフォーマンスへの影響を防ぐには、完全な本番環境で条件をテストしてください。テストにより、構成管理データベース (CMDB) の条件とサイズを指定して、[修復ターゲットの評価]ジョブの実行にかかる時間を判断できます。
更新履歴	
アクティビティ	ルールの初期作成には使用されません。その後、システム作業メモがここに記録されます。

4. **[Submit]** をクリックします。
このルールは、スケジュール済みジョブ [*Evaluate remediation targets*] の次の実行時に有効になります。既存のルールが更新された場合、または [修復ターゲットルール] リストビューの [変更を適用] ボタンを使用する場合も同様です。既存のルールが更新された場合も同様です。スケジュール済みジョブと [変更を適用] の詳細については、「アプリケーション脆弱性対応 で修復ターゲットトラッキングを自動化する」を参照してください。

アプリケーション脆弱性一致アイテムの修復ターゲットのステータスを表示する

修復ターゲットルールで定義されているように、アプリケーション脆弱性一致アイテム (AVI) が修復ターゲット日にほぼ近づいた (または過ぎている) と、AVI レコードはステータスで更新されます。この情報は、今後の修復アクティビティを積極的に監視するのに役立ちます。

始める前に
必要なロール：アプリセキュリティマネージャーグループ

このタスクについて
[修復ターゲットを評価 **(Evaluate remediation targets)]** スケジュール済みジョブは、現在の日付を関連する修復ターゲットルールで指定された脆弱性一致アイテムの修復日と比較するために、 1 日

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

に 1 回実行されます。現在の日付が修復期限切れまでの日数内にある場合、修復ステータスが脆弱性一致アイテムレコードに追加されます。

手順

次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > 脆弱性一致アイテム.
AVI の修復日が修復ターゲットルールで設定された条件の範囲内にある場合は、[脆弱性一致アイテム] リストビューに表示される [修復ターゲットステータス] 列を確認します。AVI の修復ターゲット日が過ぎている場合、AVI フォームに注釈が表示されます。

注:
[ターゲット間近]、[ターゲット内]、および [過去のターゲット] である AVI の数を表示するには、「Application Vulnerability Management [PA] dashboard (アプリケーションの脆弱性管理 (PA) ダッシュボード)」を参照してください。

関連情報

アプリケーション修復ターゲットルールの作成または編集

修復タスクをクローズ

アプリケーション修復タスクに関連する問題をそれ以上分析することなくすぐにクローズできると判断した場合は、[クローズ] 機能を使用できます。脆弱性対応の v23.0 以降では、アプリケーション修復タスクの [クローズ] ボタンが削除されました。

始める前に
必要なロール：admin

このタスクについて
脆弱性対応 ワークスペースでは、修復タスクは、以前のバージョンの 脆弱性対応 での修復タスクと同じ状況に移行します。ある修復タスクのすべての脆弱性一致アイテム (VIT) がクローズされると、その修復タスクは [非アクティブ] ステータスに移行します。

重要:
状況同期を有効にした状態で、それぞれのレコードのライフサイクルの状況を介して変更要求と修復タスクを手動で移行することはできますが、CHG の状況が変化したことをシステムが登録したり、各自が CHG を追加したり、修復タスクから CHG を削除したりすると、状況同期によって手動による介入が無効になる可能性があります。ただし、変更要求の状況により、修復タスクのステータスが [クローズ済み] または [保留] 状況から自動的に移行されることはありません。

手順

1. レビューを要求するレコードを開きます。
2. [クローズ] ボタンをクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
ステータス	ステータスとして [クローズ済み] を選択します。
理由	問題をクローズする理由を入力します。
追加情報	その他の関連情報を入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [送信] を選択します。
   修復タスクは [クローズ済み] とマークされます。

アプリケーション脆弱性対応の変更管理

アプリケーション脆弱性対応アプリケーションの修復タスクから変更要求を作成し、手動での介入が必要なアプリケーション脆弱性 (AVIT) の調査を迅速化します。

構成アイテム (CI) として分類されるスキャン済みアプリケーションについて事前入力された情報を使用して変更要求を作成し、手動での介入が必要なアプリケーション脆弱性 (AVIT) の調査を迅速化します。

- アプリケーション脆弱性対応の変更要求ワークフローは、脆弱性対応でサポートされているワークフローと似ています。
- 脆弱性対応変更要求ワークフローの詳細については、「脆弱性対応 の変更管理」を参照してください。

アプリケーション修復タスクの変更要求の作成

アプリセキュリティマネージャーまたはセキュリティチャンピオンは、アプリケーション脆弱性対応アプリケーションの修復タスクから変更要求を作成できます。

始める前に
必要なロール：

脆弱性マネージャーマネージャーワークスペースから:sn_vul.app_sec_manager。

ITRem オーナーワークスペースから:sn_vul.app_sec_champion または sn_vul.app_developer、および itil ロール。

このタスクについて
クラシック環境から変更要求を作成するには、以下の手順に従います。

修復タスクから、変更要求を直接作成、承認、実装、レビュー、およびクローズすることができます。修復タスクから事前入力された情報を使用して、次の 3 つのタイプの変更要求を作成できます。

- 標準。事前に承認された、リスクの低い、比較的一般的な変更を指し、指定された手順または作業指示書に従って行います。
- 通常。通常の変更要求は、実装、レビュー、およびクローズする前に 2 レベルの承認が必要な規範的なプロセスに従います。
- 緊急。重大なインシデントを解決するための変更。

> **注:**
> アプリケーション脆弱性対応の変更要求は、検出されたアプリケーションが構成アイテム (CI) に関連付けられている場合にのみサポートされます。これは、製品モデル [sn_vul.use_product_model] システムプロパティで [製品モデル] を [False] に設定した場合にのみ発生します。

手順

1. 既存の修復タスクレコードから完全な変更要求を作成するには、次に移動します: **All** (すべて) > アプリケーション脆弱性対応 > 修復タスク > 所属グループにアサイン済み.
   自分のアサイン先グループにアサインされている修復タスクレコードのリストが表示されます。
2. オプション: 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > 修復の概要 修復の概要ダッシュボードを表示し、自分または自分のアサイン先グループにアサインされた VUL を見つけます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. または、[番号] 列で修復タスクをクリックしてレコードを開き、詳細を表示します。
   レコードが表示されます。
4. 変更要求を作成する APP-VUL レコードを表示した状態で、レコードの右上にある [変更を作成] をクリックします。
   [変更要求の作成] フォームが表示されます。
5. フィールドに入力します。

   a. [適用先] フィールドの選択リストから、いずれかを選択して続行します。

オプション	説明
このグループ内のすべてのアクティブなアプリケーション脆弱性一致アイテム	選択すると、[変更を作成] をクリックした後に、ステータスが [クローズ済み] 以外のこの修復タスクのすべてのアクティブなアプリケーション脆弱性一致アイテムが変更要求に自動的に追加されます。
一連の条件に一致する、このグループ内のすべてのアプリケーション脆弱性一致アイテム	選択すると、下の 2 番目の図に示すように条件ビルダーが表示されます。新しい変更要求に必要な脆弱性一致アイテムを特定するためのフィルター基準を入力します。 フィルターの例には、「特定の検索条件に一致する脆弱性一致アイテムのみ」などがあります。 [ステータス] [次の値に等しい] [オープン] かつ [リスクスコア] [次の値を超える] **[75]**。 条件を入力すると、条件に一致する AVIT の数 (10) を示すメッセージが表示されます。一致するアイテムをプレビューするためのリンク ([一致するアイテムをプレビュー **(Preview matching items)]**) が表示されます。 フィルター条件に一致するアイテムがない場合は、フィルターを調整するように指示するメッセージが条件ビルダーの下に表示されます。 [変更を作成] をクリックすると、この条件フィルターに一致するすべてのアプリケーション脆弱性一致アイテムが新しい修復タスクに移動されます。この変更要求が修復タスクに関連付けられます。

   一連の条件に一致するタスク内のアプリケーション脆弱性一致アイテムの変更要求フォームを作成します

   b. オプション: フォームに表示されている場合は、[一致アイテムのプレビュー] リンクをクリックして、フィルター基準に一致する AVIT のリストを表示します。
   修復タスクリストのプレビューが表示されます。このプレビューリストでアイテムを選択して UI アクションを実行できますが、これらのアクションは APP-VUL でも実行されます。たとえば、プレビューリストから VI を削除すると、その AVIT は APP-VUL からも削除されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

c. プレビューが完了したら、ブラウザーウィンドウを閉じて変更要求フォームに戻ります。

d. [CR に CI を追加] チェックボックスで、1 つを選択して続行します。

オプション	説明
[CR に CI を追加] チェックボックスをオン	デフォルトはオンです。チェックボックスをオンにすると、この修復タスクのアクティブな脆弱性一致アイテムに属する構成アイテム (CI) がこの変更要求に追加されます。APP-VUL は自動的に [実装待ち] ステータスに移行します。
[CR に CI を追加] チェックボックスをオフ	この修復タスクのアクティブなアプリケーション脆弱性一致アイテムの CI を新しい変更要求に追加しない場合は、このチェックボックスをオフにします。 無効にすると、変更要求状況は APP-VUL に同期されず、APP-VUL は現在のステータスのままになります。

e. [変更タイプ] フィールドの選択リストから、いずれかを選択して続行します。

変更タイプ	説明
緊急	重大なインシデントを解決するための変更。
通常	標準的な変更でも緊急の変更でもないサービスへの変更を実施するために使用される変更タイプ。
標準	事前に承認された低リスクの変更要求で、頻繁に実施されます。承認済みの標準変更要求をテンプレートのカタログで事前定義して、標準変更へのアクセスと要求をより効率的にすることができます。選択すると、2 つのフィールドが表示されます。各選択リストからいずれかを選択して、次のフィールドに入力します。 ▪ 変更カテゴリ：既存のカタログから変更のカテゴリを選択します。たとえば、[ハードウェア]、[サーバーの標準的な変更]、[ソフトウェア] などです。この例では、[標準的な変更のパッチ適用 (Patching Standard Changes)] が選択されています。 ▪ 変更テンプレート：事前定義されたサポートタスクを使用して、変更要求に利用可能なテンプレートをカタログから 1 つ選択します。この例では、[Microsoft 月次パッチ適用サイクル (Microsoft Monthly Patching Cycle)] テンプレートが選択されています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

変更タイプ	説明
	ITSM の変更要求のカテゴリ、テンプレート、および変更タイプの詳細については、「変更タイプ」を参照してください。

この機能は、ITSM 変更管理のカタログで設定した変更要求のタイプを自動的に読み取ります。たとえば、ITSM の標準的な変更の要求の名前を「標準」から「事前承認済み」に変更すると、次の図に示すとおり、[変更要求の作成] フォームの [変更タイプ] 選択リストに新しい名前が自動的に表示されます。

フォームの [変更要求プレビュー] セクションのフィールドには、APP-VUL からの情報が事前に入力されています。これらのフィールド値は必要に応じて編集できます。たとえば、この後の図のフィールドの値を確認します。

終了予定日

この日付 (2019-10-10) は、APP-VUL の [修復ターゲット日] フィールドに表示される値と同じです。この値は、APP-VUL に属するアプリケーション脆弱性一致アイテムの最も早い修復ターゲット日から導出されます。修正日をさらに早める必要がある重大な問題の変更要求を作成している場合は、この値と [優先度] フィールドの値を編集することをお勧めします。

理由

このフィールドには、CHG に追加された CI の数が表示されます。追加情報が必要な場合は、このテキストを編集することをお勧めします。たとえば、新しい APP-VUL の作成に使用したフィルターに関するメモ (リスクスコアが 75 より大きいなど) をこのフィールドに追加することもできます。このテキストは、新しい変更要求と修復タスクを見つけるのに役立ちます。

実装計画

このフィールドには、脆弱性の優先ソリューションが表示されます。

アサイン先グループとアサイン先

これらのフィールドを編集して、アサイン先グループを変更するか、いずれかのアサイン先グループのユーザーにこの変更要求を再アサインします。

6. 必要に応じてフィールドのプレビューと編集を続行します。
7. 変更を保存してこのページに留まるには、フォームの上部にあるグレーのバナーを右クリックして、[挿入と維持] を選択します。
8. 編集が完了したら、いずれかを選択して続行します。

注:

[アサイン先グループ] および [アサイン先] のフィールドが未アサイン (空) の [オープン] ステータスの修復タスクの場合、[変更を作成] をクリックすると、現在のログオンユーザーが自動的にタスクにアサインされます。さらに、 [CI を CR に追加] チェックボックスをオンにする必要があります。VUL の上部に、このアサインを示す青色の確認メッセージが表示されます。

次のタスク

変更要求と変更タスクを監視して、それらが完了し、変更要求が実装されていることを確認します。この CHG が実装され、[レビュー] ステータスに移行した後、ステータス同期が有効になっている場合、APP-VUL は自動的に [解決済み] に移行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

既存の変更要求への修復タスクの関連付け

Appsec マネージャーまたはセキュリティチャンピオンは、修復タスク (APP-VUL) をインスタンスで既に利用可能な変更要求に関連付けることで、修復タスクの解決に取り組むときに重複した変更要求 (CHG) を作成しないようにします。

始める前に

必要なロール：

脆弱性マネージャーマネージャーワークスペースから:sn_vul.app_sec_manager。

ITRem オーナーワークスペースから:sn_vul.app_sec_champion または sn_vul.app_developer、および itil ロール。

このタスクについて

修復オーナーは、自分または自分のアサイン先グループにアサインされた修復タスクを、修復タスクレコードから直接、既存の変更要求に関連付けることができます。次の図は、変更要求を既存の APP-VUL (VG) に関連付ける基本的なフローを示しています。

注:
既存の変更要求を任意のステータス ([オープン]、[調査中]、[実装待ち]、[クローズ済み]、および [保留]) の APP-VUL に関連付けることができます。変更要求を既存の VUL に関連付けると、アクティブな VI のみが変更要求に追加されます。

開始する前に、重複する変更要求を作成しないように、APP-VUL に既に関連付けられている既存の変更要求を表示することをお勧めします。特定の APP-VUL に関連する変更要求の数を簡単に追跡するには、[修復タスク] リストの [CR 数] 列を参照します。表示されていない場合は、右上の設定アイコン () をクリックします。[CR 数] 列を [利用可能] から [選択済み] に移動して、**[OK]** をクリックします。

このテーブルに既存のデータがあるお客様に対して新しい列を自動的に入力するには、スケジュール済みジョブ [新しい CR カウント列を入力 (Populate new CR Count Column)] を実行します。

手順

1. 修復タスクを既存の変更要求に関連付けるには、次に移動します: **All** (すべて) > アプリケーション脆弱性対応 > 修復タスク.
2. 作業する修復タスクを見つけます。
3. オプション: 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > 修復の概要 修復の概要ダッシュボードを表示し、自分または自分のアサイン先グループにアサインされた APP-VUL を見つけます。
4. [番号] 列で、APP-VUL レコードをクリックして開きます。
   APP-VUL レコードが表示されます。
5. 表示されていない場合は、開かれているレコードを表示した状態で、[変更要求] 関連リストまでスクロールして選択します。
   APP-VUL に関連付けられている変更要求が [追加] ボタンとともに表示されます。次の図では、この APP-VUL に既に関連付けられている変更要求はありません。
6. APP-VUL を既存の CHG に関連付けるには、[追加] をクリックします。
   [既存の変更要求を修復タスクに追加] フォームが表示されます。
7. フォームで、検索アイコンをクリックします。
   次の図に示すように、既存の変更要求のリストビューが新しいウィンドウに表示されます。
8. 表示されたリストからアイテムを選択するか、フィルター () をクリックして条件を入力し、検索結果を制限します。
9. [CR に CI を追加] チェックボックスで、1 つを選択して続行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
このチェックボックスは、[新規] ステータスの既存の変更要求に対してのみ表示されます。

オプション	説明
[CR に CI を追加] チェックボックスをオン	デフォルトはオンです。チェックボックスをオンにすると、この修復タスクのアクティブな脆弱性一致アイテムに属する構成アイテム (CI) がこの変更要求に追加されます。 選択すると、変更要求のステータスが APP-VUL に同期されます。詳細については、「変更要求と修復タスク間のステータスの同期」を参照してください。
[CR に CI を追加] チェックボックスをオフ	この修復タスクのアクティブな脆弱性一致アイテムの CI を新しい変更要求に追加しない場合は、このチェックボックスをオフにします。 無効にすると、変更要求状況は APP-VUL に同期されず、APP-VUL は現在のステータスのままになります。

10. [変更の要求の検索] フィールドに、適切な変更要求番号を表示した状態で、[送信] をクリックします。
APP-VUL が表示されます。レコードの上部に、選択した変更要求が APP-VUL に正常に関連付けられたことを示す青色の確認メッセージが表示されます。

注:
[オープン] ステータスで、[アサイン先グループ] および [アサイン先] フィールドが未アサイン (空) の APP-VUL の場合、[追加] をクリックすると、現在ログオンしているユーザーが自動的に APP-VUL にアサインされます。さらに、 [CI を CR に追加] チェックボックスをオンにする必要があります。APP-VUL の上部に、現在のユーザーがアサインされていることを示す青色の確認メッセージが表示されます。

次のタスク
APP-VUL レコードを確認します。[変更要求] 関連リストの [変更要求] 列で、新しい CHG のリンクをクリックして CR レコードを表示します。開かれている CHG レコードで、変更要求状況を監視できます。影響を受ける構成アイテム (CI) と修復タスクが、[影響を受ける CI (Affected CIs)] および修復タスクの関連リストに表示されます。

ペネトレーションテスト

アプリケーション脆弱性対応 のペネトレーションテストにより、アプリケーションオーナーはアプリケーションのセキュリティ体制を評価できます。これは、倫理的なハッキングチームによるアプリケーションの手動テストです。

必要なロール

ペネトレーションテストには次のロールが必要です。

[アプリセキュリティマネージャー]：ペネトレーションテストアセスメント要求を管理するセキュリティマネージャーとアプリケーションオーナーが含まれます。次の詳細なロールが含まれています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- sn_vul.app_manage_pen_test_request
- sn_vul.app_read_all
- cmdb_read

[倫理的なハッカー]：アプリケーションのペネトレーションテストを実行する倫理的なハッキングチームのメンバーが含まれます。次の詳細なロールが含まれています。

- sn_vul.app_update_assignment_group
- sn_vul.app_update_assigned_to
- sn_vul.app_manage_manual_avits
- sn_vul.app_manage_pen_test_request_config
- itil
- sn_vul.app_read_all
- sn_vul.app_manage_pen_test_request
- sn_vul.app_update_state

各ロールの詳細については、「アプリケーション脆弱性対応 のユーザーロールおよびロール」を参照してください。

脆弱性対応 の v19.0 以降では、Veracode 脆弱性統合 を使用している場合は、Veracode 脆弱性統合 のペネトレーションアセスメントテストは Veracode からの手動検出結果になります。これらは、アプリケーション脆弱性対応 で構成したペネトレーションテストアセスメント要求にはリンクされません。Veracode からのペネトレーションテストアセスメントの詳細については、「Veracode 脆弱性統合」を参照してください。

自動翻訳

ペネトレーションテストのライフサイクル

アプリケーションオーナーは、倫理的なハッキングチームにアプリケーションのペネトレーションテストアセスメントを要求できます。倫理的なハッキングチームはこの要求に基づいて行動し、ペネトレーションテストの結果を作成します。これらの結果は、手動で作成されたアプリケーション脆弱性一致アイテム (AVI) です。

ペネトレーションテストワークフローは、テスト要求を上げるところから倫理的なハッキングチームの検出結果の解決までのペネトレーションテストのライフサイクルをカバーしています。

ペネトレーションテストアセスメントを要求する

v19.0 以降では、次の場所で新しい要求を作成したり、既存の要求をコピーしたりできます。 **All** (すべて) > ペネトレーションテストアセスメント要求 > **All** (すべて).

v19.0 より前では、アプリケーションオーナーは、 ITSM サービスカタログを使用して、アプリケーションのペネトレーションテストアセスメントを要求できました。

ペネトレーションテストアセスメント要求をレビューする

倫理的なハッキングチームは、アプリケーションとペネトレーションテストアセスメント要求の範囲をレビューして評価し、既存のバックログに追加します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

環境準備

その後、倫理的なハッキングチームは、アプリケーションオーナーにテストを開始するための環境を提供するように要求を送信します。環境の準備ができたら、アプリケーションオーナーは倫理的なハッキングチームに通知します。

テスト要求の設定の詳細については、「ペネトレーションテストの構成」を参照してください。

ペネトレーションテスト結果のテストと報告

倫理的なハッキングチームはアプリケーションをテストし、結果をアプリケーションオーナーに報告します。倫理的なハッキングチームは、修復ターゲット日を使用して、ペネトレーションテスト結果の Service Level Agreement (SLA) も定義します。これらの結果は手動で作成された AVI です。アプリケーションオーナーは、倫理的なハッキングチームによって作成された AVI を順次レビューします。修正を計画し、アプリケーションチームにアサインします。

注:
修復ターゲットルールはペネトレーションテスト結果に適用されません。

倫理的なハッキングチームは、アプリケーション脆弱性エントリー (AVE) のライブラリを作成し、AVI をレポートする際にそれらを再利用できます。ペネトレーションテスト結果のステータスを追跡することもできます。

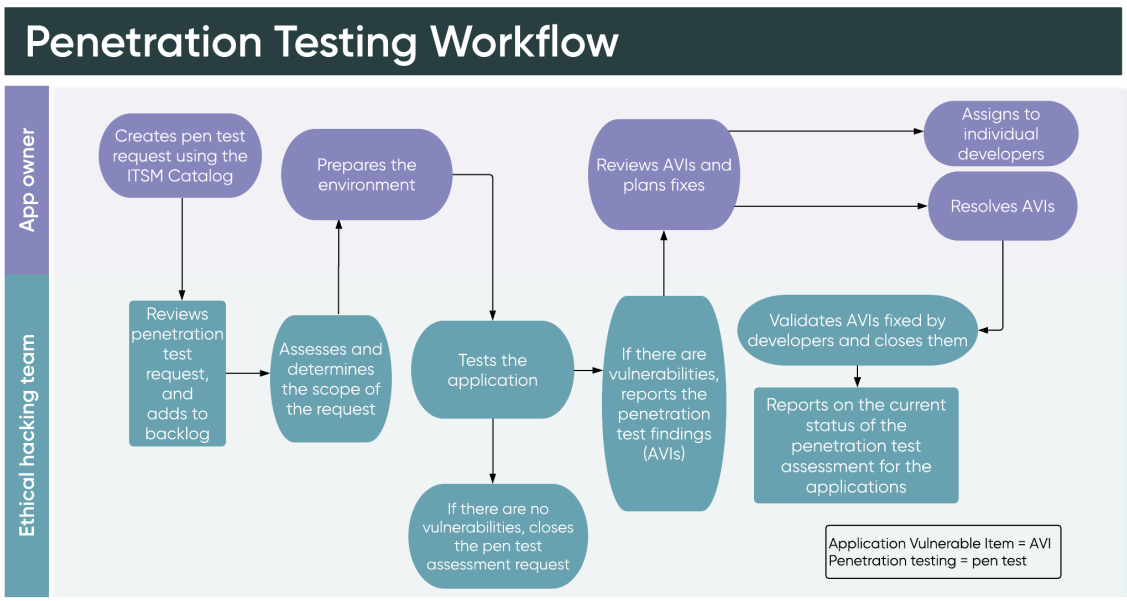
ペネトレーションテスト結果の修正と検証

ペネトレーションテスト結果がアプリケーションチームによって修復、解決された後、修正は倫理的なハッキングチームによって手動で検証され、クローズされます。

アプリケーション脆弱性管理 レポート

アプリケーション脆弱性管理 PA ダッシュボードで利用可能なレポートを使用して、ペネトレーションテスト結果を追跡します。

ペネトレーションテストのライフサイクル



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

既存の要求からのペネトレーションテストアセスメント要求の作成 (v19.0 より前)

v19.0 以降では、既存の要求のリストから直接ペネトレーションテストアセスメント要求を作成します。このリストで [クローズ済み] ステータスの既存の要求をコピーして、要求を作成することもできます。

始める前に

必要なロール：アプリケーションセキュリティマネージャー

このタスクについて

脆弱性対応 の v19.0 以降では、Veracode 脆弱性統合 を使用している場合は、Veracode 脆弱性統合 のペネトレーションアセスメントテストは Veracode からの手動検出結果になります。これらは、アプリケーション脆弱性対応 で構成したペネトレーションテストアセスメント要求にはリンクされません。Veracode からのペネトレーションテストアセスメントの詳細については、「Veracode 脆弱性統合」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > ペネトレーションテストアセスメント要求 > **All** (すべて).
2. オプション: または、クローズ済みの要求を複製することで、要求を作成することもできます。元の要求のすべての値が新しいフォームで保持されます。アクティブなアプリケーション脆弱性一致アイテム (AVI) が新しい要求に自動的にコピーされます。[クローズ済み] ステータスのレコードから [要求のコピーと作成] を選択します。
3. [新規] を選択し、フィールドに入力します。

[ペネトレーションテストアセスメント要求] フォーム

フィールド	説明
数値	ペネトレーションテストアセスメント要求に対して生成された一意の識別子。
状況	要求のステータスに基づいて値を選択します。
要求者	アプリケーションのアセスメントを要求しているユーザー。
アサイン先グループ	ペネトレーションテスト結果で作業するために選択されたグループ。アプリセキュリティマネージャーが手動で追加または編集できます。 グループを設定するには、「ペネトレーションテストの構成」を参照してください。
アプリケーション	検索オプションを使用してアプリケーションを選択します。
アサイン先	このペネトレーションテスト結果で作業するように選択されたアサイン先グループの個人。アプリセキュリティマネージャーが手動で追加または編集できます。
アプリケーションタイプ	以下のいずれかのオプションを選択します。 ○ Web サービス (v16.1 より前は API) ○ Web アプリケーション

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ 親密なクライアント ○ モバイル ([モバイル] を選択すると、フォームの下部に [モバイル] タブが追加フィールドとともに表示されます)
スプリント	選択した [アセスメントタイプ] フィールドに基づいて、アセスメント要求に対応できる帯域幅のスプリントを表示します。 スプリントキャパシティとテストスコープの変更の詳細については、「ペネトレーションテストのスプリントの構成」および「ペネトレーションテストのアセスメントタイプの構成」を参照してください。
v19.0：アプリケーションサイズ	テストするアプリケーションのサイズを選択します。 ○ 小 ○ 中 ○ 大 ○ 標準 (サイズが不明な場合はこのオプションを選択します) アプリケーションサイズとスプリントキャパシティを使用したスプリントキャパシティとテストスコープの変更の詳細については、「ペネトレーションテストの構成」を参照してください。
作成済み	要求が作成された日時。
アセスメントタイプ	次からアセスメントタイプを選択します。 ○ 完全なペネトレーションテスト ○ 集中テスト ○ 再テスト テストの組み合わせとテストスコープの詳細については、「ペネトレーションテストのアセスメントタイプの構成」を参照してください。
更新日時	要求が最後に更新された日時。
デモの日付	このアプリケーションのデモが可能な日付。
本番展開の予定日	このアプリケーションを本番環境に展開する予定日。
展開予定のアプリケーションのバージョン / リリース	本番展開が計画されているアプリケーションのバージョン。
v19.0：[サードパーティベンダーまたは合弁会社が所有するアプリケーション (Application owned by third-party vendor or a joint venture)] タブ このフィールドで [はい] を選択すると、[ベンダー/合弁会社情報 (Vendor / Joint Venture Information)] タブが表示されます。追加のフィールドに入力します。	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ペネトレーションテストの実行を許可する条項は存在しますか？(Clause exists that enables us to perform pen testing?)	「条項」という用語は、追加する 2 人以上の関係者間に存在する契約を含むテストの標準を指すことがあります。[はい]を選択した場合は、条項を追加します。
ペネトレーションテストの実行権限に言及している条項 (The clause citing the permission to perform pen testing)	
ベンダーの完全な登録名と住所	
侵入検知システム	
ベンダーからの技術に関する連絡	
ログの情報を調べて悪意のあるアクティビティがあるかどうかを確認しましたか？(Has the logged information been reviewed form malicious activity?)	
アプリケーションは別のサードパーティベンダーによってホストされていますか？	
ペンテストを承認するベンダーからの連絡	
[アプリケーションの詳細] タブ	
アプリケーションの目的	アプリケーションの機能の説明。
テクノロジースタック詳細	フロントエンドからバックエンドまで、データベース、および他の重要なテクノロジーに至る完全なテクノロジースタック。
サードパーティのアプリケーションですか？	このアプリケーションがサードパーティベンダーによって所有されているかどうかを確認します。
アプリケーションからアクセスできる機密データの種類を一覧表示	アプリケーションからアクセスできる機密データの種類を分類します。たとえば、PII データ、PHI データ、およびクレジットカード番号などの財務データです。
認証タイプ	このアプリケーションが LDAP 認証、独自のネイティブ認証、または他の形式の認証を使用するかどうかを指定します。
アプリケーションはコンプライアンスプログラムの対象ですか？	このアプリケーションが PCI などのコンプライアンスプログラムに影響を与えるかどうかを指定します。
アプリケーションチームの連絡先	倫理的なハッキングチームからの問い合わせの際に連絡先となるアプリケーションチームのメンバー。
コンプライアンスプログラムのリスト	
関連するサードパーティインターフェイスまたはアプリケーション	
IP アドレス	
本番環境のユーザーの概数は？(Approximate number of users in production?)	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
自動スクリプトは存在しますか？	
このアプリの本番バージョンは外部向けですか？(Production version of this app is external-facing?)	
v 19.0：ビジネスインパクト	
経済的損害	リストから 1 つ選択します。
非準拠	リストから 1 つ選択します。
風評被害	リストから 1 つ選択します。
プライバシー違反	リストから 1 つ選択します。
[テストの詳細] タブ	
テストする URL	ペネトレーションテストに含める必要がある URL。
除外する URL	ペネトレーションテストから除外する必要がある URL。
このアプリケーションは以前にテストしましたか？	このアプリケーションのペネトレーションテストは実行済みであるかどうかを指定します。
再テストの理由	アプリケーションのテストが以前に実行済みである場合にペネトレーションテストの再アセスメントを要求する理由。
アプリケーションをテストしたのはいつですか？	アプリケーションのペネトレーションテストの実施期間。
テストアカウントの詳細	倫理的なハッキングチームがペネトレーションテストに使用できるテストアカウントの詳細。
アプリケーションロール	アプリケーションがサポートするのユーザーのロール。
最も使用されるロール	アプリケーションで最も一般的に使用されるロール。
[追加コメント] タブ	
作業メモ	

4. [保存] を選択して編集を保存するか、[送信] を選択して要求を開始します。

ペネトレーションテストアセスメント要求の作成 **(v19.0** より前)

Web アプリケーションまたは API のペネトレーションテストアセスメント要求を開始します。これらの要求は倫理的なハッキングチームに送信され、アプリケーションのテストが続行され、ペネトレーションテスト結果が手動で報告されます。

始める前に

必要なロール：アプリケーションセキュリティマネージャー

このタスクについて

アプリケーションオーナーは、アプリケーションまたは API を手動でスキャンするために、ペネトレーションテストアセスメント要求を挙げます。倫理的なハッキングチームがアプリケーションをテ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ストし、手動でペネトレーションテスト結果を作成します。これらの結果は、手動で作成されたアプリケーション脆弱性一致アイテム (AVI) です。

ペネトレーションテスト結果のデフォルトのアサイン先グループは、関連するペネトレーションテストアセスメント要求の [アプリケーションチーム] フィールドで設定されたグループです。ペネトレーションテスト結果のアサインタイプは [手動] です。アサインルールは、これらのペネトレーションテスト結果のアサインを上書きすることはできません。

v19.0 以降では、ペネトレーションテストアセスメント要求 [sn_vul_pen_test_assessment_request_list] テーブルからペネトレーションテストアセスメント要求を直接作成できます。詳細については、「既存の要求からのペネトレーションテストアセスメント要求の作成 (v19.0 より前)」を参照してください。

手順

1. v19.0 より前では、移動先: **All** (すべて) > セルフサービス > **Service Catalog** > サービス > ペネトレーションテストアセスメント要求.
2. オプション: または、クローズ済みの要求を複製することで、要求を作成することもできます。元の要求のすべての値が保持されます。アクティブなアプリケーション脆弱性一致アイテム (AVI) が新しい要求に自動的にコピーされます。
3. フォームのフィールドに入力します。

[ペネトレーションテストアセスメント要求] フォーム

フィールド	説明
数値	ペネトレーションテストアセスメント要求に対して生成された一意の識別子。
要求者	アプリケーションのアセスメントを要求しているユーザー。
親アセスメント要求	子要求の作成に使用された元のペネトレーションテストアセスメント要求。クローズ済みアセスメント要求を使用して作成されます。子アセスメント要求フォームでのみ表示されます。
アプリケーション	検索オプションを使用してアプリケーションを選択します。
アプリケーションタイプ	以下のいずれかのオプションを選択します。 ○ Web サービス (v16.1 より前は API) ○ Web アプリケーション ○ 親密なクライアント ○ モバイル ([モバイル] を選択すると、フォームの下部に [モバイル] タブが追加フィールドとともに表示されます)
v19.0：アプリケーションサイズ	テストするアプリケーションのサイズを選択します。 ○ 小 ○ 中

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ 大 ○ 標準 (サイズが不明な場合はこのオプションを選択します)
アセスメントタイプ	次からアセスメントタイプを選択します。 ○ 完全なペネトレーションテスト ○ 集中テスト ○ 再テスト 詳細については、「ペネトレーションテストのアセスメントタイプの構成」を参照してください。
アプリケーションの目的	アプリケーションの機能の説明。
テクノロジースタック詳細	フロントエンドからバックエンドまで、データベース、および他の重要なテクノロジーに至る完全なテクノロジースタック。
サードパーティのアプリケーションですか？	このアプリケーションがサードパーティベンダーによって所有されているかどうかを確認します。
アプリケーションからアクセスできる機密データの種類を一覧表示	アプリケーションからアクセスできる機密データの種類を分類します。たとえば、PII データ、PHI データ、およびクレジットカード番号などの財務データです。
認証タイプ	このアプリケーションが LDAP 認証、独自のネイティブ認証、または他の形式の認証を使用するかどうかを指定します。
アプリケーションはコンプライアンスプログラムの対象ですか？	このアプリケーションが PCI などのコンプライアンスプログラムに影響を与えるかどうかを指定します。
アプリケーションチームの連絡先	倫理的なハッキングチームからの問い合わせの際に連絡先となるアプリケーションチームのメンバー。
デモの日付	このアプリケーションのデモが可能な日付。
本番展開の予定日	このアプリケーションを本番環境に展開する予定日。
展開予定のアプリケーションのバージョン / リリース	本番展開が計画されているアプリケーションのバージョン。
v19.0：サードパーティベンダーまたは合弁会社が所有するアプリケーション (Application owned by third-party vendor or a joint venture)	このフィールドで [はい] を選択すると、[ベンダー/合弁会社情報 (Vendor / Joint Venture Information)] タブが表示され、追加のフィールドが表示されます。 「条項」という用語は、2 人以上の関係者間に存在する契約を含むテストの標準を指すことがあります。
状況	要求のステータスに基づいて値を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
アサイン先グループ	ペネトレーションテスト結果で作業するために選択されたグループ。アプリセキュリティマネージャーが手動で追加または編集できます。
アサイン先	このペネトレーションテスト結果で作業するように選択されたアサイン先グループの個人。アプリセキュリティマネージャーが手動で追加または編集できます。
スプリント	選択した [アセスメントタイプ] フィールドに基づいて、アセスメント要求に対応できる帯域幅のスプリントを表示します。
作成済み	要求が作成された日時。
テスト開始日	テストが開始される日時。
更新日時	要求が最後に更新された日時。
テストの詳細	
テストする URL	ペネトレーションテストに含める必要がある URL。
除外する URL	ペネトレーションテストから除外する必要がある URL。
このアプリケーションは以前にテストしましたか？	このアプリケーションのペネトレーションテストは実行済みであるかどうかを指定します。
再テストの理由	アプリケーションのテストが以前に実行済みである場合にペネトレーションテストの再アセスメントを要求する理由。
アプリケーションをテストしたのはいつですか？	アプリケーションのペネトレーションテストの実施期間。
テストアカウントの詳細	倫理的なハッキングチームがペネトレーションテストに使用できるテストアカウントの詳細。
アプリケーションロール	アプリケーションがサポートするのユーザーのロール。
最も使用されるロール	アプリケーションで最も一般的に使用されるロール。

4. [送信] を選択します。
   関連するアプリケーションに対して要求が作成されたというメール通知が、倫理的なハッキングチームに送信されます。

[クローズ済み] ステータスのペネトレーションテスト要求の複製

[クローズ済み] ステータスの要求を複製してペネトレーションテストアセスメント要求を作成します。アクティブなアプリケーション脆弱性一致アイテム (AVI) が新しい要求にコピーされます。

始める前に
必要なロール：アプリケーションチーム

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > ペネトレーションテストアセスメント要求 > **All** (すべて).
2. [クローズ済み] ステータスの要求を選択します。
3. [要求をコピーして作成] を選択します。
   新しい要求が作成され、アクティブな AVI が更新されたデータとともにこの要求にコピーされます。親要求から AVI の元のステータスを表示するには、[ペネトレーションテスト結果のスナップショット] タブに移動します。

アセスメント要求に基づくペネトレーションテスト結果の作成 (v19.0 より前)

ペネトレーションテストアセスメント要求に基づくペネトレーションテスト結果を作成します。これらの結果は、手動で作成されたアプリケーション脆弱性一致アイテム (AVI) です。

始める前に
必要なロール：倫理的なハッカー

手順

1. 次のように移動する。 **All** (すべて) > セルフサービス > **Service Catalog** > サービス > ペネトレーションテストアセスメント要求.
2. ペネトレーションテストアセスメント要求の AVI を作成するには、関連する要求を選択します。
3. [アプリケーション脆弱性一致アイテム] セクションで、[新規] を選択します。
4. フォームのフィールドに入力します。

[アプリケーション脆弱性一致アイテム] フォーム (ペネトレーションテスト表示)

フィールド	説明
数値	このレコードに対して自動的に生成された AVI 識別子。
アセスメント要求	この AVI が関連付けられているペネトレーションテストアセスメント要求。
脆弱性	検索オプションを使用して、脆弱性エントリーテーブルから選択された脆弱性。
リスク評価	脆弱性一致アイテムを [重大]、[高]、[中]、[低]、および [なし] に分類する数値化された [リスクスコア] 。リスク評価の詳細については、「アプリケーション脆弱性対応 のリスクを自動的に計算する」を参照してください。 V16.1 以降では、デフォルトで、値は脆弱性の重大度と同じになります。
コンプライアンスプログラムに影響？	コンプライアンスプログラムに影響があるかどうかを確認します。選択肢は [はい] および [いいえ] です。
影響を受けるコンプライアンスプログラムのリスト	このフィールドは、[コンプライアンスプログラムに影響] フィールドの値が *Yes* に設定されている場合に表示されます。影響を受けるコンプライアンスプログラムを一覧表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
予定されているリリース/修正バージョン	ペネトレーションテスト結果をいつまでに解決する必要があるかを公表しています。
状況	AVI 作成時のデフォルト値は [オープン] です。状況のマッピング方法の詳細については、「アプリケーション脆弱性一致アイテム (AVI) の状況」を参照してください。
アサイン先グループ	この AVI で作業するように選択されたグループ。アプリセキュリティマネージャーが手動で追加または編集できます。
アサイン先	この AVI で作業する、選択されたアサイン先グループの個人。アプリセキュリティマネージャーが手動で追加または編集できます。
修復ターゲット	AVI が最初に識別されてから、修復されるべき日付。このフィールドは、該当する場合にのみ表示されます。 修復ターゲットの詳細については、「アプリケーション脆弱性対応 で修復ターゲットトラッキングを自動化する」を参照してください。
作成済み	アプリケーション脆弱性一致アイテム (AVI) が作成された時点のタイムスタンプ。
更新日時	アプリケーション脆弱性一致アイテム (AVI) が更新された時点のタイムスタンプ。
開始者	このペネトレーションテスト結果を作成したユーザー。
セキュリティチームの連絡先	倫理的なハッキングチームの連絡先。
簡単な説明	ペネトレーションテスト結果の簡単な説明。
詳細	
技術的な詳細	ペネトレーションテスト結果の技術的な詳細。
影響	ペネトレーションテスト結果の影響のアセスメント。
再現手順	ペネトレーションテスト結果を再現して確認する手順を文書化しています。
推奨事項	推奨アクションをこのフィールドに記録しています。
メモ	
作業メモ	メモを追加して、状況移行および他のフィールド更新に関する情報を伝達します。
V16.1：影響を受ける URL	影響を受ける URL に関連する詳細情報。
V16.1：影響を受けるパラメーター	影響を受けるパラメーターに関連する詳細情報。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
V16.1：影響を受ける機能	影響を受ける機能に関連する詳細情報。

5. フォームを保存するには、[送信] を選択します。

アプリケーション脆弱性エントリーを作成する

ペネトレーションテスト結果で指定された脆弱性のアプリケーション脆弱性エントリーを作成します。アプリケーション脆弱性は、カスタムソフトウェアアプリケーションの脆弱性です。

始める前に
必要なロール：倫理的なハッカー

このタスクについて
アプリケーション脆弱性対応 はアプリケーションに脆弱性を関連付け、ペネトレーションテスト結果を作成します。これらの結果は、手動で作成されたアプリケーション脆弱性一致アイテム (AVI) です。ペネトレーションテスト時は、既存エントリーを再利用するか、脆弱性ごとに手動で作成することができます。

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > ライブラリー > サードパーティ.
2. [アプリケーション脆弱性エントリー] ページで、[新規] を選択します。
3. フォームのフィールドに入力します。

[アプリケーション脆弱性エントリー] フォーム (ペネトレーションテスト表示)

フィールド	説明
ID	この脆弱性エントリーの識別子。
重大度	この脆弱性の重大度を正規化したもの。重大度マップは、NVD および ServiceNow サードパーティ統合に提供されます。重大度マップの作成や調整の詳細については、「アプリケーション脆弱性一致アイテムの重大度を自動的にマッピングする」を参照してください。
プライマリ CVE	この脆弱性が最も適合する共通脆弱性タイプ一覧要素への参照。
カテゴリ名	サードパーティ統合によって提供される分類。アサインを支援します。
脆弱性の詳細	
攻撃ベクトル	この脆弱性に対する最も脆弱な攻撃ベクトル。
攻撃の複雑さ	攻撃者がコントロールできない、脆弱性の悪用に必須の条件について説明しているメトリクス。
スコープ	ソフトウェアの脆弱性が、手段を超えてリソースに影響与える能力を測定するためのメトリクス。
完全性	脆弱性が利用された場合に完全性に及ぼす影響度を測定するためのメトリクス。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
CVSS ベクトル	ソフトウェアの脆弱性の特性と重大度をキャプチャするためのオープンフレームワーク。
必要な権限	攻撃者が脆弱性を悪用する前に保有する必要がある権限のレベル。
ユーザーのインタラクション	脆弱性を利用するための人間による操作の要件。
機密性	脆弱性が利用されたことによる情報リソースの機密性への影響。これらのリソースはソフトウェア コンポーネントによって管理されます。
Availability	脆弱性が利用された場合に影響を受けるコンポーネントの可用性への影響。
CVSS 基本スコア	アプリケーション脆弱性エントリーの重大度を示す数値 (0 ～ 10)。
脅威	この脆弱性に由来する脅威の説明。
緩和の説明	脆弱性を緩和する手順の説明。

4. フォームを保存するには、[送信] を選択します。

> **注:**
> AVE はアプリケーション脆弱性エントリー (sn_vul_app_vul_entry) テーブルに作成されます。アプリケーション脆弱性エントリーテーブルは、脆弱性エントリー (*sn_vul_entry*) テーブルの子です。したがって、作成された AVE は脆弱性エントリーテーブルにも追加されます。

ペネトレーションテストワークスペース

アプリケーション脆弱性対応のペネトレーションテストワークスペースは、顧客がペネトレーションテストアセスメント要求を要求し、ワークフローを使用して追跡するのに役立ちます。これにより、アプリケーションオーナーはアプリケーションのセキュリティ体制を評価できます。これは、倫理的なハッキングチームによるアプリケーションの手動テストです。

必要なロール

ペネトレーションテストには次のロールが必要です。

sn_vul.app_pen_tester: アプリケーションのペネトレーションテストの一環としてペネトレーションテスト結果を作成するペネトレーションテスターを表します。

sn_vul.app_pen_test_requester: アクション:sn_vul.app_pen_test_requester のレコードを選択します。

ペネトレーションテストのライフサイクル

アプリケーションオーナーは、倫理的なハッキングチームにアプリケーションのペネトレーションテストアセスメントを要求できます。倫理的なハッキングチームはこの要求に基づいて行動し、ペネトレーションテストの結果を作成します。これらの結果は、手動で作成されたアプリケーション脆弱性一致アイテム (AVI) です。

ペネトレーションテストワークフローは、テスト要求を上げるところから倫理的なハッキングチームの検出結果の解決までのペネトレーションテストのライフサイクルをカバーしています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

新しいペネトレーションテストアセスメント要求を作成します

Web アプリケーション、モバイルアプリケーション、または API のペネトレーションテストアセスメント要求を開始します。これらの要求は倫理的なハッキングチームに送信され、アプリケーションのテストが続行され、ペネトレーションテスト結果が手動で報告されます。

始める前に
必要なロール：アプリケーションセキュリティマネージャー

手順

1. 次のように移動する。 ペネトレーションテストワークスペース.
2. [ペネトレーションテストアセスメント要求] フォームのフィールドに入力します。
3. [**Submit** (送信)] を選択します。
   関連するアプリケーションに対して要求が作成されたというメール通知が、倫理的なハッキングチームに送信されます。
4. フォームが送信されると、倫理的なハッキングチームは スコーピングを開始できます。
5. スコーピング後、アプリケーションオーナーはテスト環境を準備し、倫理的なハッキングチームはテストを開始できます。
6. 要求元の詳細を確認する必要がある場合は、[保留] ボタンを選択してテストフェーズを保留中としてマークできます。
7. テストが完了すると、[ペネトレーションテストテスト結果] タブで AVIT を表示できます。

> **注:**
> 既存の要求から要求を複製することができます。複製されると、親要求に添付されている AVIT が複製された要求に移動されます (コピーされません)。

アセスメントアンケートに基づくペネトレーションテスト結果の作成

MASVS アンケートの認定基準に準拠したテストをペネトレーションテストワークフローに組み込んだペネトレーションテスト結果を作成します。これらの結果は、手動で作成されたアプリケーション脆弱性一致アイテム (AVI) です。

始める前に
必要なロール:アプリケーションセキュリティマネージャー

手順

1. 次のように移動する。 ペネトレーションテスト結果 学習します。
2. アプリケーションに基づいて公開されたアンケートを選択します。
3. テストをレビューし、テストフェーズを完了としてマークします。
4. 上記のステップが完了したら、要求をクローズします。

> **注:**
> 上記の手順は、倫理的ハッキングチームのメンバーが実行できます。

アセスメントアンケートを公開する

モバイルアプリケーションをテストするために、テスターが製品のバグを特定するのに役立つように、OASコミュニティによって開発された特定の標準があります。アセスメントワークスペースに移動して、任意のアンケートを作成します。公開して、アセスメント要求フォームで表示できるようにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール:sn_vul.app_pen_test_requester

ペネトレーションテストの要求者とテスターに必要なロール:

sn_vul.app_manage_pen_test_request:

包含:sn_smart_asmt.assessment_reader sn_smart_asmt:assessment_admin sn_smart_asmt.actor。

sn_vul.app_pen_tester

次を含む:sn_smart_asmt.assessment_reader sn_smart_asmt:actor。

> **注:**
> スマートアセスメントエンジン機能の一環として、上記のロールが追加されました。これらのロールは、ペネトレーションテストの要求者とテスターがアンケートを表示して送信するために不可欠です。

手順

1. 次のように移動する。 アセスメントワークスペース.
2. 各アンケート内にガイドラインがあります。アンケートを確認し、必要に応じて組織のテストニーズを満たすように変更し、その後テストを完了できます。
   アンケートはデフォルトで MASVS 標準に準拠しています。詳細については、以下をご覧ください。
3. アンケートを公開し、ペネトレーションテストアセスメント要求フォームのテストの詳細セクションにあるリストから公開されたアンケートを選択します。

   > **注:**
   > アンケートを公開して、ペネトレーションテスト要求アセスメント要求フォームで表示できるようにします。

4. テストを実行するペルソナは、ペネトレーションテスト要求フォームの [アセスメント] タブで、テストを合格、不合格、または該当なしとしてマークできます。

アセスメントアンケートの使用

アセスメントアンケートの作成後、これらのアンケートをテスト目的で使用できます。

始める前に
必要なロール:sn_vul.app_pen_tester

手順

1. 次のように移動する。 ペネトレーションテスト要求 進みます。
2. フォームに記載されているガイドラインに従ってください。
3. ペネトレーションテスト要求を選択します。
4. [アセスメント] タブに移動します。
5. タブを開き、アンケートに回答して 送信します。

   > **注:**
   > ペネトレーションテスト要求にアサインされたペルソナは、要求を送信できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ペネトレーションテストダッシュボード

個人のペネトレーションテストダッシュボードで、ペネトレーションテスト要求と手動検出結果の概要を確認します。チームの進捗状況は、ペネトレーションテストワークスペースで確認できます。ダッシュボードには、ペネトレーションテスト結果の概要が表示され、注意が必要なテストの表示と優先順位付け、テスト結果の追跡、アサインの表示ができます。

ペネトレーションテストマネージャー/倫理的ハッキングチームのリードは、ペネトレーションテスト要求の監視などの主要なメトリクスを特定および分析し、ペネトレーションテストワークスペースでチームの全体的な進捗状況を表示できます。ペネトレーションテストマネージャー/倫理的ハッキングチームのリードは、次のインサイトも表示できます。

- 戦略的な意思決定に役立つ情報を提供するために、ステータスとアセスメントタイプ別に分類された手動検出結果の概要。
- キャパシティ計画立案を改善するために、アサインされたペネトレーションテストを個人に配布
- 進捗状況に基づいて期限切れの検出結果に優先順位を付け、解決効率を高めます。
- 臨界分布に基づいてペネトレーションテストの結果の状況を理解します。

ペネトレーションダッシュボードコンポーネント

パーソナルダッシュボードのコンポーネントを活用して、チームの進捗状況とデータを視覚的に分析し、ビジネスの成果を推進します。

重要アイテムインジケーター

未アサインの緊急リリース、概要日付を過ぎたテスト、未アサインのテスト、および処理待ちの重要な検証を表示します。

- 未アサインの緊急リリース:アセスメントタイプ「緊急リリース」の未アサインのペネトレーションテスト要求の合計数を示します。
- 期限切れのテスト:期日を過ぎたテストの合計数を示します。
- 未アサインのテスト: チームにアサインされていないテストの合計数を示します。
- 重大 検証処理待ち:「検証処理待ち」ステータスのすべての要求の AVIT の合計数を示します。

注:
各タイルを選択してアイテムのリストを表示し、必要なタスクを実行します。

ペネトレーションテスト要求

ステータス別のテスト要求、期限切れのテスト、およびリリース承認別のテストを表示します。

- ステータス別のテスト要求:ペネトレーションテストサイクルのこれらの異なる状況でのテスト要求の数を示します。色付きの各タイルをクリックすると、さまざまな状況のテスト要求のリストを表示して移動できます。タブの右上のセクションにあるフィルタードロップダウンから月を選択して、次の 6 か月間のこれらのテストのステータスを表示することもできます。テスト要求のさまざまな状況は次のとおりです。
  - オープン:オープンなテスト要求の数。
  - スコーピング中:
  - スコーピングが完了しました:
  - 環境準備:
  - テスト環境の準備完了:
  - テスト中:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 完全なペネトレーションテスト:
- バグ報奨金プログラム:倫理的なハッカーに対して、セキュリティの脆弱性を見つけて報告するための報酬を提供します。
- 集中テスト:
- エグゼクティブの関心:組織内の重要なプロジェクトに対する上級管理職の関与とサポートに関するレポート。
- ワンオフレビュー:通常の開発サイクルとリリースサイクル以外の特定のプロジェクトを評価して、パフォーマンスを評価し、改善を実装します。
- 緊急リリース:セキュリティの脆弱性などの重大な問題に対処するための迅速なソフトウェア更新に必要な緊急リリースをサポートします。

- 期限切れのテスト:特定の期間から保留中のテストを示します。期限のテストを表示するタイムラインを選択できます。ドロップダウンオプションは、[昨日が期限]、[今週が期限]、[先週が期限]、[先月が期限]、および [先月より前が期限] です。
- リリース承認別のテスト:リリース準備完了テストの承認ステータスを示します。また、新しいソフトウェアを展開する前に、必要なすべてのチェックが完了していることを確認します。タブの右上のセクションにあるフィルタードロップダウンから月を選択して、次の 6 か月間のこれらのテストのステータスを表示することもできます。

実行内容の詳細

検証処理待ちの AVIT の数とともに報告されたオープンペネトレーションテスト結果 (AVIT) の数を示します。色付きの各タイルを選択して、さまざまな状況の検出結果のリストを表示して移動できます。このセクションで次のデータを表示できます。

- リスク評価別の未解決の結果 **(AVIT)**
- 検出結果の検証処理待ち **(AVIT)**

チームの概要

次の 6 か月間にチームメンバーにアサインされたテストを示します。状況は次のとおりです。

- スコーピング中
- オープン
- スコーピング完了
- テスト環境の準備完了
- テスト中
- 環境準備

アプリケーション脆弱性対応 向け プラットフォームアナリティクスソリューション

プラットフォームアナリティクスソリューション には、他の Now Platform 製品とともに使用するために、パッケージ化された プラットフォームアナリティクス のコンテンツが含まれています。このプラットフォームアナリティクスソリューションからは、アプリケーションの脆弱性管理プロセスを分析するための重要なメトリクスが示されます。

概要

脆弱性対応のパフォーマンスアナリティクスコンテンツパックは、ServiceNow® Store で別個のサブスクリプションとして入手できます。アプリケーションは、脆弱性対応アプリケーションとともに

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

自動的にインストールされます。アプリケーション脆弱性対応コンテンツパックは、脆弱性対応のパフォーマンスアナリティクスコンテンツパックの一部です。

設定の詳細については、「脆弱性対応のパフォーマンスアナリティクス [PA] アプリケーションのインストールと設定)」を参照してください。

主要な用語

パフォーマンスアナリティクス (PA)

管理ダッシュボードを作成し、KPI とメトリクスに関するレポートを作成し、重要なビジネス上の質問に回答することで、品質向上とコスト削減に役立つソリューション。

アプリケーション脆弱性一致アイテム

構成アイテム (CI) に存在する、サードパーティの脆弱性スキャナーによって報告されたアプリケーションの脆弱性。

PA インジケーター

アクティビティや組織の作業の定期的な間隔で実行されるパフォーマンス測定値 ([最重要アプリケーション脆弱性一致アイテム (AVI) の上位 10 個のアプリケーション] など) を定義します。

PA インジケーターソース

1 つのテーブルまたはデータベースのビューからレコードをフィルタリングするデータセット (AVI アクティブなど)。

- 自分のアプリケーションの脆弱性ダッシュボードでは、アプリケーションの脆弱性のボリューム、パフォーマンス、および初期分析と検出から封じ込めや修復までの進捗状況を追跡します。
- 修復ターゲットの達成率を確認し、組織に最も大きなリスクをもたらすアプリケーション脆弱性一致アイテム (AVI) を効率的に判断します。

必要なロール

このソリューションには、次のロールとタスクが関連付けられています。

- Now Platform 管理者 (admin)：この分析およびレポートのソリューションをインストールしてアクティブ化し、システムプロパティに必要な変更を加えます。
- パフォーマンスアナリティクス アドミン (pa_admin)：インジケーター、ブレークダウン、ウィジェット、およびダッシュボードを確認します。データ収集を設定して開始します。適切なステークホルダーとダッシュボードを共有します。

以下のダッシュボードでは AVI のアクティビティがグラフィックで表示されるため、修復計画とステータスの進捗状況の判断に役立ちます。そのため、影響を受ける重要なアプリケーションや目立った脆弱性に関連する KPI に注目できます。

- アプリケーションの脆弱性管理ダッシュボードでは、脆弱性のリスクとそのまん延、影響を受けるアプリケーション、修復の傾向、および修復の進捗状況を確認できます。傾向のデフォルトは 3 か月ですが、7 日間、1 か月、3 か月、6 か月、YTD、1 年、または [すべて] に変更できます。
- 自分のアプリケーションの脆弱性ダッシュボードでは、アプリケーションの脆弱性のボリューム、パフォーマンス、および初期分析と検出から封じ込めや修復までの進捗状況を追跡します。

> **注:**
> 自分のアプリケーションの脆弱性ダッシュボードは概要ダッシュボードのサブセットであり、セキュリティチャンピオンユーザーグループのメンバーがインスタンスにログインした場合にのみ使用できます。自分のアプリケーションの脆弱性ダッシュボードの詳細については、「自分のアプリケーションの脆弱性ダッシュボード」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション脆弱性管理 **(PA)** ダッシュボード

アプリケーションの脆弱性のボリューム、パフォーマンス、および初期分析と検出から封じ込めや修復までの進捗状況を追跡します。

ユースケース

ユーザー	ダッシュボードの使用法
脆弱性マネージャー	アプリケーション脆弱性管理 ダッシュボードを使用することで、組織に最も大きなリスクをもたらすアプリケーション脆弱性一致アイテム (AVI) を脆弱性管理で判断できます。 これらのダッシュボードでは AVI のアクティビティがグラフィックで表示されるため、修復計画とステータスの進捗状況の判断に役立ちます。影響を受ける重要なアプリケーションや目立った脆弱性に関連する KPI に注目します。

必要な **Now Platform** ロール、セットアップ、およびダッシュボードのタブ

アプリケーションの脆弱性管理 (PA) ダッシュボードは、脆弱性対応のパフォーマンスアナリティクスコンテンツパックの一部です。脆弱性対応のパフォーマンスアナリティクスコンテンツパックは、脆弱性対応 アプリケーションとともに自動的にインストールされます。ServiceNow Store で、別のサブスクリプションとして利用できます。

設定の詳細については、「脆弱性対応のパフォーマンスアナリティクス [PA] アプリケーションのインストールと設定)」を参照してください。

セキュリティチャンピオン、アプリセキュリティマネージャー、または開発者ユーザーグループにアサインされたユーザーとしてダッシュボードを表示するには、 アプリケーション脆弱性対応 > 概要.

> **注:**
> 自分のアプリケーションの脆弱性ダッシュボードは概要ダッシュボードのサブセットであり、セキュリティチャンピオンユーザーグループのメンバーがインスタンスにログインした場合にのみ使用できます。自分のアプリケーションの脆弱性ダッシュボードの詳細については、「自分のアプリケーションの脆弱性ダッシュボード」を参照してください。

アプリケーション脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で表示することもできます。新しい UI でダッシュボードを表示するには、次に移動します: ワークスペース > 脆弱性マネージャーワークスペース をクリックし、[ダッシュボード] アイコンをクリックします。ロールに応じてデフォルトのダッシュボードが表示されます。他のダッシュボードを表示するには、ダッシュボード名の横にあるドロップダウンをクリックします。詳細については、「の [ダッシュボード] ページ Vulnerability Manager ワークスペース」と「の [ダッシュボード] ページ IT 修復ワークスペース」を参照してください。

概要ダッシュボードでは、脆弱性のリスクとそのまん延、影響を受けるアプリケーション、修復の傾向、および修復の進捗状況を確認できます。傾向のデフォルトは 3 か月ですが、7 日間、1 か月、3 か月、6 か月、YTD、1 年、または [すべて] に変更できます。

アプリケーション脆弱性管理 ダッシュボードのデータを [スキャンタイプ]、[アプリケーション]、または [事業部門] 別に分類します。これらの選択肢にはそれぞれ、選択を絞り込むための [要素を選択] という追加フィルターがあります。アプリケーション脆弱性対応 v15.0 以降では、ビジネスアプリケーションと CI アプリケーションが [アプリケーション] フィルターの選択肢に追加されています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

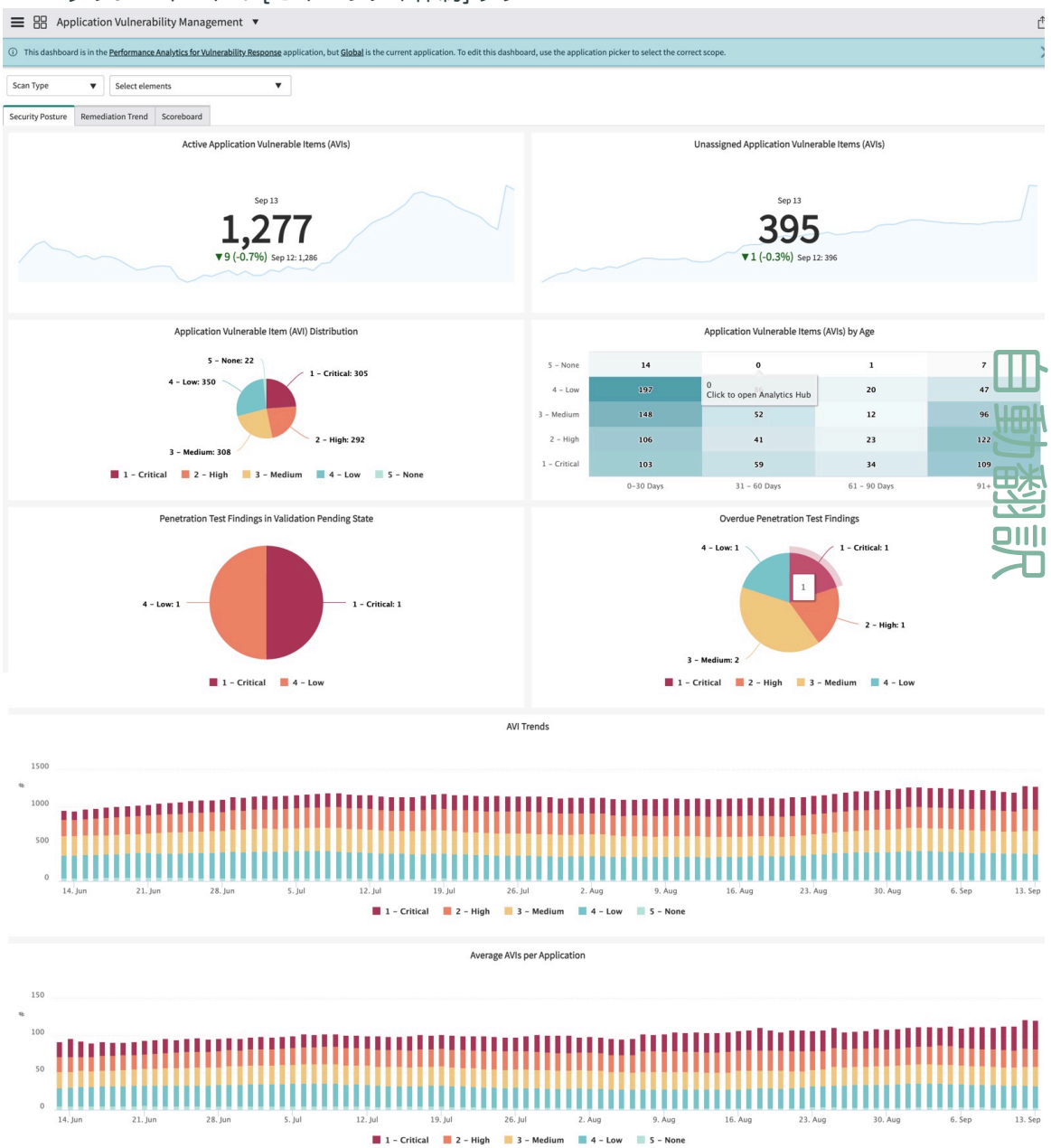
[セキュリティ体制] タブ

[セキュリティ体制] タブで、セキュリティ体制および、修復アクションの進捗状況を把握することができます。

アプリケーション脆弱性対応 v15.0 以降では、ペネトレーションテストの結果レポートを確認できます。ペネトレーションテストの結果は、ペネトレーションテストアセスメント要求に基づいて手動で作成されたアプリケーション脆弱性一致アイテム (AVI) です。

注:
これらのウィジェットの [スキャンタイプ] は [手動] です。

AVM ダッシュボードの [セキュリティ体制] タブ



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

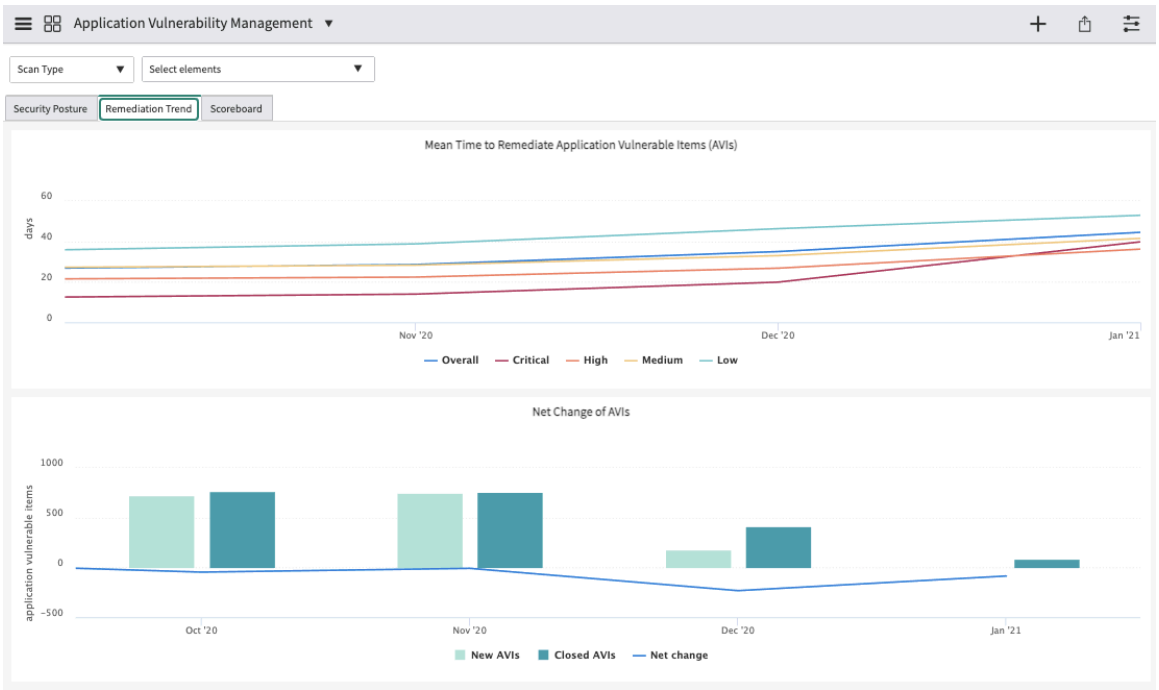
[例外] タブ

このダッシュボードは、過度の保留の可能性があるために組織がリスクを負っている場所を把握し、修復オプションを再検討するのに役立ちます。

理由別の保留アプリケーション脆弱性一致アイテム、AVI の期限切れ間近の保留要求、アサイン先グループ別の重大なアプリケーション脆弱性一致アイテムの例外、要求者別の AVI 例外要求を表示できます。

[修復の傾向] タブ

[修復の傾向] タブを見ると、修復アクションの進捗状況を把握できます。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

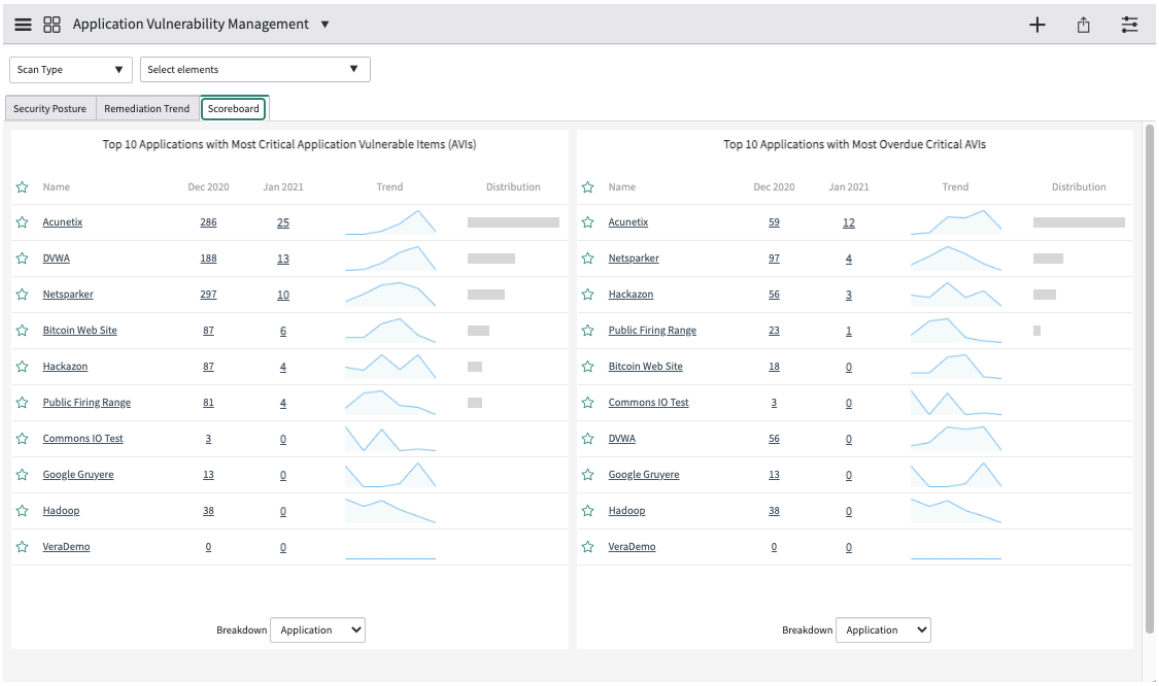
[スコアボード] タブ

[スコアボード] タブを見ると、修復アクションの進捗状況と、その完了に最も支援が必要な AVI を把握できます。

スキャンタイプの要素は次のとおりです。

- 動的：動的データインポートからのメトリクスのみを使用
- 静的：静的データインポートからのメトリクスのみを使用

いずれか一方、または両方を選択できます。



インジケーター

低い AVI の平均修復時間

[[クローズ済みアプリケーション脆弱性一致アイテムの合計期間 > リスク評価 = 4 - 低]] / [[クローズ済みアプリケーション脆弱性一致アイテム > リスク評価 = 4 - 低]]。目標は最小化することです。

アプリケーションリリース

テーブル sn_vul_app_vulnerable_item を使用している AVI.Active のアプリケーションの個別のカウント。目標は最小化することです。

アプリケーション脆弱性一致アイテム

テーブル sn_vul_app_vulnerable_item を使用している AVI.Active アプリ vul アイテム のカウント。目標は最小化することです。

アプリケーションごとの平均 AVI

[アクティブなアプリケーション脆弱アイテム]] / [[アプリケーションリリース]]。目標は最小化することです。

未アサインの VI

これはインジケーターソース AVI.Active のカウントで、テーブル sn_vul_app_vulnerable_item を使用しています。目標は最小化することです。

AVI の平均修復時間

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[[クローズ済みアプリケーション脆弱性一致アイテムの合計期間]] / [[クローズ済みアプリケーション脆弱性一致アイテム]]。目標は最小化することです。

高い AVI の平均修復時間

[[クローズ済みアプリケーション脆弱性一致アイテムの合計期間 > リスク評価 = 2 - 高]] / [[クローズ済みアプリケーション脆弱性一致アイテム > リスク評価 = 2 - High]]。目標は最小化することです。

クローズされたアプリケーション脆弱性一致アイテム

これはインジケーターソース AVI.Closed のカウントで、テーブル sn_vul_app_vulnerable_item を使用しています。目標は最大化することです。

重要な AVI の平均修復時間

[[クローズ済みアプリケーション脆弱性一致アイテムの合計期間 > リスク評価 = 1 - 重大]] / [[クローズ済みアプリケーション脆弱性一致アイテム > リスク評価 = 1 - 重大]]。目標は最小化することです。

新しいアプリケーション脆弱性一致アイテム

これはインジケーターソース AVI.New のカウントで、テーブル sn_vul_app_vulnerable_item を使用しています。目標は最小化することです。

中程度の AVI の平均修復時間

[[クローズ済みアプリケーション脆弱性一致アイテムの合計期間 > リスク評価 = 3 - 中程度]] / [[クローズ済みアプリケーション脆弱性一致アイテム > リスク評価 = 3 - 中程度]]。目標は最小化することです。

VI の正味増減

[[新規アプリケーション脆弱性一致アイテム]] - [[クローズ済みアプリケーション脆弱性一致アイテム]] 目標は最小化することです。

クローズされたアプリケーション脆弱性一致アイテムの合計期間

これはインジケーターソース AVI.Closed のカウントで、テーブル sn_vul_app_vulnerable_item を使用しています。目標は最小化することです。

重大な期限切れのアプリケーション脆弱性一致アイテム

テーブル sn_vul_app_vulnerable_item を使用している AVI.Active というデータソースのカウント。目標は最小化することです。

重大なアプリケーション脆弱性一致アイテム

これは、テーブル sn_vul_analytics_app_ci_dept_bu を使用する、AVI がアクティブなアプリケーションインジケーターソースのカウントです。目標は最小化することです。

ブレークダウン

- 経過時間
- クローズした経過時間
- アプリケーション
- 事業部門
- リスク評価
- スキャンタイプ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
アプリケーション脆弱性一致アイテム (AVI) の経過時間とクローズ所要時間の計算をカスタマイズすると、これらのメトリクスを含むパフォーマンスアナリティクス (PA) レポートが急激に増減する可能性があります。AVI の経過時間およびクローズ所要時間の計算をカスタマイズする方法の詳細については、 KB1703270 KB 記事を参照してください。

データの可視化

セキュリティ体制

名前	タイプ	説明
V15.0：検証処理待ちステータスのペネトレーションテスト結果	円グラフ	[解決済み] ステータスだが検証処理待ちのペネトレーションテストの結果。リスク評価別にグループ化されています。
V15.0：期限切れのペネトレーションテスト結果	円グラフ	修復ターゲット日を過ぎた重大なペネトレーションテスト結果。リスク評価別にグループ化されています。
アクティブなアプリケーション脆弱性一致アイテム (AVI)	単一スコア	アクティブな (クローズされていない) アプリケーション脆弱性一致アイテム (AVI) の数。
未アサインのアプリケーション脆弱性一致アイテム (AVI)	単一スコア	アサイン先グループのないアクティブなアプリケーション脆弱性一致アイテム (AVI) の数。
アプリケーション脆弱性一致アイテム (AVI) の分布	円グラフ	リスク評価によってグループ化されたすべてのアクティブなアプリケーション脆弱性一致アイテム (AVI) の分布。
経過時間ごとのアプリケーション脆弱性一致アイテム	ヒートマップ	リスク評価および経過時間 (日)でグループ化された、アクティブなアプリケーション脆弱性一致アイテム (AVI) の数。 **注:** アプリケーション脆弱性一致アイテム (AVI) の経過時間とクローズ所要時間の計算をカスタマイズすると、これらのメトリクスを含むパフォーマンスアナリティクス (PA) レポートが急激に増減する可能性があります。AVI の経過時間およびクローズ所要時間の計算をカスタマイズする方法の詳細については、 KB1703270 KB 記事を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティ体制 (続く)

名前	タイプ	説明
AVI の傾向	傾向	リスク評価によってグループ化されたアクティブなアプリケーション脆弱性一致アイテム (AVI) の傾向。
アプリケーションごとの平均 AVI	傾向	アプリケーションごとの平均アプリケーション脆弱性一致アイテム (AVI) の傾向 (リスク評価別)。

修復の傾向

名前	タイプ	説明
アプリケーション脆弱性一致アイテム (AVI) の平均修復時間	線グラフ	リスク評価別のアプリケーション脆弱性一致アイテム (AVI) の平均修復時間の傾向。
AVI の正味増減	傾向	検出された新しいアプリケーション脆弱性一致アイテム (AVI) とクローズ済みの傾向 (月別)。

スコアボード

名前	タイプ	説明
最重要アプリケーション脆弱性一致アイテム (AVI) の上位 10 個のアプリケーション	スコアカードと分布棒	重大なアプリケーション脆弱性一致アイテム (AVI) の数が最も多いアプリケーション。
期限切れの最重要 AVI の上位 10 個のアプリケーション	スコアカードと分布棒	修復ターゲット日を過ぎたアクティブなアプリケーション脆弱性一致アイテム (AVI) の数が最も多いアプリケーション。

自分のアプリケーションの脆弱性ダッシュボード

このダッシュボードには、修復ターゲット達成率の表示など、アプリケーションの脆弱性管理プロセスを分析するための重要なメトリクスが表示されます。

必要な **Now Platform** のロールとダッシュボードの表示

注:

- このダッシュボードは、アプリケーション脆弱性対応コンテンツパックの一部です。アプリケーション脆弱性対応コンテンツパックは、脆弱性対応のパフォーマンスアナリティクスコンテンツパックの一部です。
- 脆弱性対応のパフォーマンスアナリティクスコンテンツパックは、ServiceNow® Store で別個のサブスクリプションとして入手できます。
- 脆弱性対応のパフォーマンスアナリティクスコンテンツパックは、脆弱性対応アプリケーションとともに自動的にインストールされます。

自分のアプリケーションの脆弱性ダッシュボードは、セキュリティチャンピオンユーザーグループのメンバーがインスタンスにログインした場合にのみ使用できます。概要ダッシュボードの詳細については、「アプリケーションの脆弱性管理 (PA) ダッシュボード」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ダッシュボードを表示するには、次に移動します: アプリケーション脆弱性対応 > 自分のアプリケーションの脆弱性.

アプリケーション脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で表示することもできます。新しい UI でダッシュボードを表示するには、次に移動します: ワークスペース > 脆弱性マネージャーワークスペース をクリックし、[ダッシュボード] アイコンをクリックします。ロールに応じてデフォルトのダッシュボードが表示されます。他のダッシュボードを表示するには、ダッシュボード名の横にあるドロップダウンをクリックします。詳細については、「の [ダッシュボード] ページ Vulnerability Manager ワークスペース」と「の [ダッシュボード] ページ IT 修復ワークスペース」を参照してください。

経時的な傾向データを示すレポートが表示されます。重要なメトリクスの傾向を定期的に確認してビジネスプロセス全体を分析し、改善が必要な領域を特定します。

自分のアプリケーションの脆弱性ダッシュボードは、脆弱性対応のパフォーマンスアナリティクスコンテンツパックに付属しています。脆弱性対応のパフォーマンスアナリティクスコンテンツパックは、脆弱性対応 アプリケーションとともに自動的にインストールされます。ServiceNow Store で、別のサブスクリプションとして利用できます。

ユースケース

ユーザー	ダッシュボードの使用法
自分または所属するグループにアサインされた脆弱性を修正する IT スペシャリスト、修復オーナー、またはアナリスト。	セキュリティチャンピオンは、自分のアプリケーションの脆弱性ダッシュボードを使用して、アプリケーションの脆弱性のボリューム、パフォーマンス、および修復の進捗状況を追跡します。 組織に最も大きなリスクをもたらすアプリケーション脆弱性一致アイテム (AVI) を効率的に判断します。 これらのダッシュボードでは AVI のアクティビティがグラフィックで表示されるため、修復計画とステータスの進捗状況の判断に役立ちます。そのため、影響を受ける重要なアプリケーションや目立った脆弱性に関連する KPI に注目できます。 脆弱性への感染とセキュリティ体制に関するインサイトを迅速に得ることができます。初期分析と検出から封じ込めや修復までの進捗状況を追跡します。

自分のアプリケーションの脆弱性 **(PA)** ダッシュボードのタブ

自分のアプリケーションの脆弱性管理ダッシュボードでは、脆弱性のリスクとそのまん延、影響を受けるアプリケーション、修復の傾向、および修復の進捗状況を確認できます。傾向のデフォルトは 3 か月ですが、7 日間、1 か月、3 か月、6 か月、YTD、1 年、または [すべて] に変更できます。

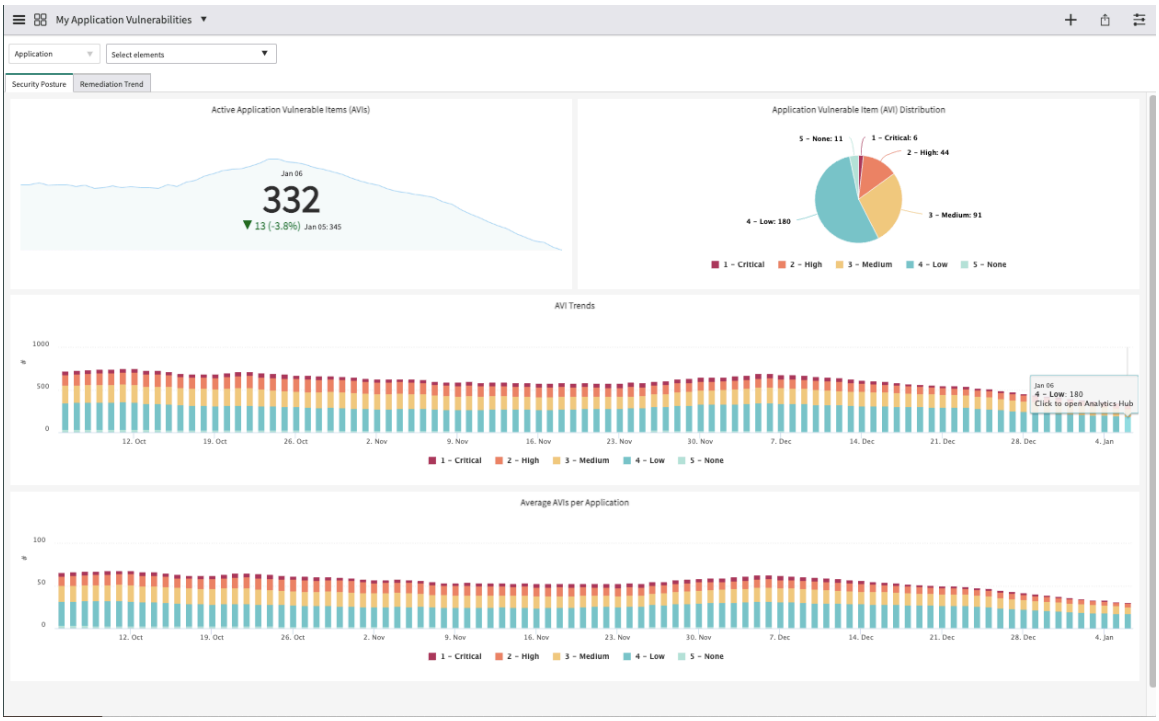
データは [アプリケーション] 別にダッシュボードに分類されます。[要素を選択] リストを使用して選択を絞り込みます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

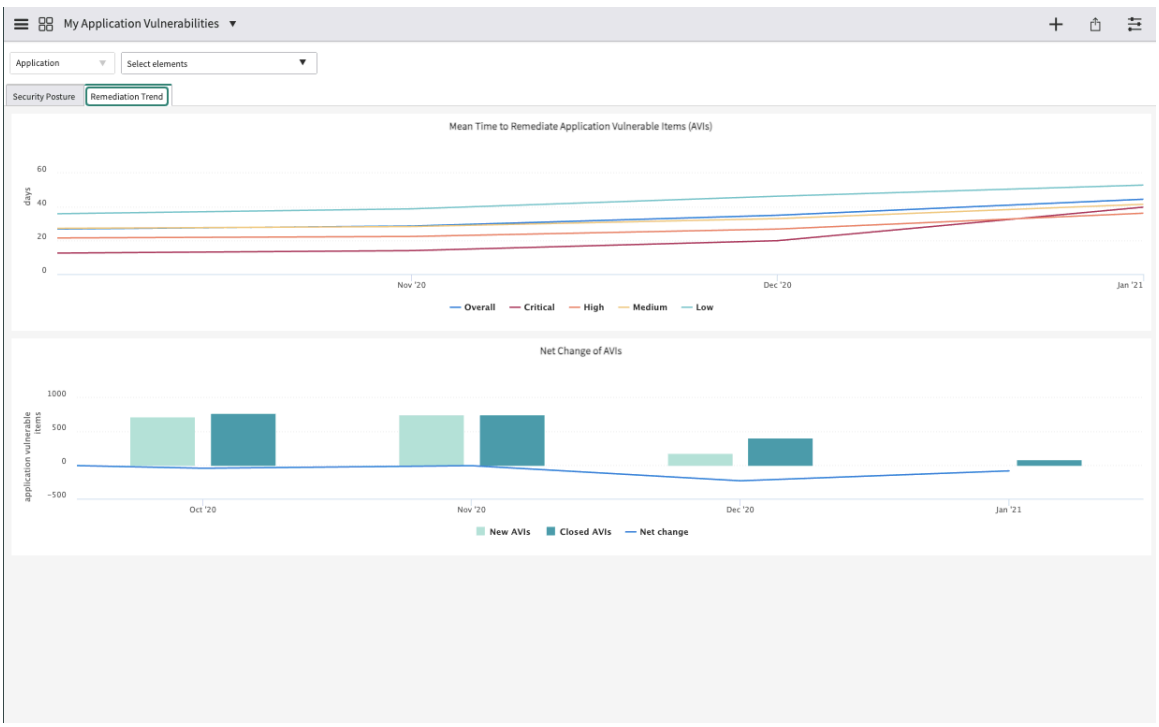
[セキュリティ体制] タブ

[セキュリティ体制] タブで、セキュリティ体制および、修復アクションの進捗状況を把握することができます。アプリケーションの脆弱性管理ダッシュボードのデータを、[スキャンタイプ]、[アプリケーション]、または [事業部門] 別に分類します。これらの選択肢にはそれぞれ、選択を絞り込むための [要素を選択] という追加フィルターがあります。



[修復の傾向] タブ

[修復の傾向] タブを見ると、修復アクションの進捗状況を把握できます。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インジケーター

低い AVI の平均修復時間

[[クローズ済みアプリケーション脆弱性一致アイテムの合計期間 > リスク評価 = 4 - 低]] / [[クローズ済みアプリケーション脆弱性一致アイテム > リスク評価 = 4 - 低]]。目標は最小化することです。

アプリケーションリリース

テーブル sn_vul_app_vulnerable_item を使用している AVI.Active のアプリケーションの個別のカウント。目標は最小化することです。

アプリケーション脆弱性一致アイテム

テーブル sn_vul_app_vulnerable_item を使用している AVI.Active アプリ vul アイテム のカウント。目標は最小化することです。

アプリケーションごとの平均 AVI

[アクティブなアプリケーション脆弱アイテム]] / [[アプリケーションリリース]]。目標は最小化することです。

未アサインの VI

これはインジケーターソース AVI.Active のカウントで、テーブル sn_vul_app_vulnerable_item を使用しています。目標は最小化することです。

AVI の平均修復時間

[[クローズ済みアプリケーション脆弱性一致アイテムの合計期間]] / [[クローズ済みアプリケーション脆弱性一致アイテム]]。目標は最小化することです。

高い AVI の平均修復時間

[[クローズ済みアプリケーション脆弱性一致アイテムの合計期間 > リスク評価 = 2 - 高]] / [[クローズ済みアプリケーション脆弱性一致アイテム > リスク評価 = 2 - High]]。目標は最小化することです。

クローズされたアプリケーション脆弱性一致アイテム

これはインジケーターソース AVI.Closed のカウントで、テーブル sn_vul_app_vulnerable_item を使用しています。目標は最大化することです。

重要な AVI の平均修復時間

[[クローズ済みアプリケーション脆弱性一致アイテムの合計期間 > リスク評価 = 1 - 重大]] / [[クローズ済みアプリケーション脆弱性一致アイテム > リスク評価 = 1 - 重大]]。目標は最小化することです。

新しいアプリケーション脆弱性一致アイテム

これはインジケーターソース AVI.New のカウントで、テーブル sn_vul_app_vulnerable_item を使用しています。目標は最小化することです。

中程度の AVI の平均修復時間

[[クローズ済みアプリケーション脆弱性一致アイテムの合計期間 > リスク評価 = 3 - 中程度]] / [[クローズ済みアプリケーション脆弱性一致アイテム > リスク評価 = 3 - 中程度]]。目標は最小化することです。

VI の正味増減

[[新規アプリケーション脆弱性一致アイテム]] - [[クローズ済みアプリケーション脆弱性一致アイテム]] 目標は最小化することです。

クローズされたアプリケーション脆弱性一致アイテムの合計期間

これはインジケーターソース AVI.Closed のカウントで、テーブル sn_vul_app_vulnerable_item を使用しています。目標は最小化することです。

重大な期限切れのアプリケーション脆弱性一致アイテム

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

テーブル sn_vul_app_vulnerable_item を使用している AVI.Active というデータソースのカウント。目標は最小化することです。

重大なアプリケーション脆弱性一致アイテム

これは、テーブル sn_vul_analytics_app_ci_dept_bu を使用する、AVI がアクティブなアプリケーションインジケーターソースのカウントです。目標は最小化することです。

ブレークダウン

- 経過時間
- クローズした経過時間
- アプリケーション
- 事業部門
- リスク評価
- スキャンタイプ

注:
アプリケーション脆弱性一致アイテム (AVI) の経過時間とクローズ所要時間の計算をカスタマイズすると、これらのメトリクスを含むパフォーマンスアナリティクス (PA) レポートが急激に増減する可能性があります。AVI の経過時間およびクローズ所要時間の計算をカスタマイズする方法の詳細については、 KB1703270 KB 記事を参照してください。

データの可視化

セキュリティ体制

名前	タイプ	説明
アクティブなアプリケーション脆弱性一致アイテム (AVI)	単一スコア	アクティブな (クローズされていない) アプリケーション脆弱性一致アイテム (AVI) の数。
アプリケーション脆弱性一致アイテム (AVI) の分布	円グラフ	リスク評価によってグループ化されたすべてのアクティブなアプリケーション脆弱性一致アイテム (AVI) の分布。
AVI の傾向	傾向	リスク評価によってグループ化されたアクティブなアプリケーション脆弱性一致アイテム (AVI) の傾向。
アプリケーションごとの平均 AVI	傾向	アプリケーションごとの平均アプリケーション脆弱性一致アイテム (AVI) の傾向 (リスク評価別)。

修復の傾向

名前	タイプ	説明
アプリケーション脆弱性一致アイテム (AVI) の平均修復時間	折れ線グラフ	リスク評価別のアプリケーション脆弱性一致アイテム (AVI) の平均修復時間の傾向。
AVI の正味増減	傾向	検出された新しいアプリケーション脆弱性一致アイテム (AVI) とクローズ済みの傾向 (月別)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

の集計レポートフレームワーク アプリケーション脆弱性対応

集計レポートフレームワークを使用すると、複雑で長時間実行されるオンザフライクエリを含むデータのレポートを作成して、パフォーマンスを向上させることができます。

集計されたレポートフレームワークは、次の方法でパフォーマンスを向上させます。

- より少ないリソース使用量で、迅速にレポートをレンダリングする
- データを集計し、集計とブレークダウン ([グループ分け基準]) を再利用する
- データベースへの照会を減らす

100 万を超えるアプリケーション脆弱性一致アイテム (AVIT) がある場合は、標準レポートと一緒に集計レポートフレームワークを使用します。

必要なロール

このソリューションには、次のロールとタスクが関連付けられています。

- Now Platform アドミン (admin)：この プラットフォームアナリティクスソリューション をインストールしてアクティブ化し、システムのプロパティに必要な変更を加えます。
- パフォーマンスアナリティクス アドミン (pa_admin)：集計、ウィジェット、およびダッシュボードを確認します。データ収集を設定して開始します。適切なステークホルダーとダッシュボードを共有します。
- アドミン (sn_vul_cmn.admin)：集計を作成します。
- VR 書き込み (sn_vul_cmn.write)：集計および集計結果のデータを編集します。
- VR 読み取り (sn_vul_cmn.read)：集計および集計結果のデータを確認します。
- 脆弱性アナリスト [sn_vul.vulnerability_analyst]：集計結果を確認します。

関連情報

ソースデータの集計を構成する

複数の集計を同時に実行する

同時に実行できる集計の数を構成する

集計を使用してレポートを作成する

アプリケーション脆弱性対応 参照

アプリケーション脆弱性対応 アプリケーションとともにインストールされるテーブル、ロール、およびプロパティに関する情報を含む参照トピック。

詳細については、以下を参照してください。

- アプリケーション脆弱性対応 のユーザーロールおよびロール
- アプリケーション脆弱性対応 とともにインストールされるコンポーネント
- アプリケーション脆弱性一致アイテム (AVI) の状況
- スキャン済みアプリケーションファイル
- [アプリケーション脆弱性一致アイテム] フィールド
- [アプリケーション脆弱性] フィールド
- ペネトレーションテストのステータス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション脆弱性対応 のユーザーロールおよびロール

アプリケーション脆弱性対応 (AVR) で脆弱性の修復を正常に行う場合は、事前にユーザーをユーザーグループにアサインする必要があります。

ロールは、アプリケーション脆弱性対応、脆弱性対応のパフォーマンスアナリティクス、および アプリケーション脆弱性対応 とのサードパーティ統合において、自分とそのグループが表示および実行できる内容を定義します。

ユーザーグループ

アプリケーション脆弱性対応 をサポートするデフォルトのユーザーグループ は次のとおりです。

- アプリセキュリティマネージャー：セキュリティマネージャーが含まれています。アプリケーション脆弱性対応 v15.0 以降では、ペネトレーションテストアセスメント要求を管理するアプリケーションオーナーも含まれます。
- セキュリティチャンピオン：開発グループとセキュリティマネージャー間の連絡係が含まれます。
- 開発者：個々の一般社員が含まれます。
- 倫理的なハッカー (V15.0)：アプリケーションのペネトレーションテストを実行する倫理的なハッキングチームのメンバーが含まれています。

ユーザー管理モジュールを使用して、アプリケーション脆弱性対応 のデフォルトユーザーグループにユーザーをアサインするには、システムアドミニストレーター [admin] ロールが必要です。

注:

アプリケーション脆弱性対応 の アプリケーション脆弱性対応 ユーザーグループに AVR ユーザーをアサインすることは、脆弱性対応 セットアップアシスタント機能では利用できません。そこには、脆弱性対応 ロールのみがアサインされます。

次の表は、利用可能な アプリケーション脆弱性対応 ユーザーグループとそれらに関連付けられたロールを示しています。この表を使用して、どのユーザーにどのグループをアサインするかを決定します。

ユーザーグループ	このグループでのロール
セキュリティチャンピオン このグループのメンバーは次のことができます。 • 自分にアサインされたアプリケーション脆弱性一致アイテム (AVI) の読み取りおよび書き込み。 • 自分にアサインされている AVI を別の個人またはグループにアサインする。 • V20.0：例外ルールを作成、更新、削除、およびキャンセル (非アクティブ化) します。	• sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_manage_auto_exception_rule
アプリセキュリティマネージャー このグループのメンバーは次のことができます。	• sn_vul.app_manage_auto_exception_rule • sn_vul.app_manage_group_rules • sn_vul.app_read_all • sn_vul.app_write_all

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザーグループ	このグループでのロール
• V20.0：例外ルールを作成、更新、削除、およびキャンセル (非アクティブ化) します。 • アプリケーション修復タスクルールに対する読み取り、書き込み、削除、およびすべての操作。 • すべての AVI の読み取りと書き込み。 • ルール、算出、および重大度マップを作成および管理して、AVR を設定する。 • 統合の設定。 • AVI の削除。 • 個人またはグループへの AVI のアサイン。 • アプリケーションの管理。 • アプリケーションモジュールへのアクセスの許可。 • 統合のスケジュール、構成、実行。 • 統合の読み取りと実行。 • AVR パフォーマンスアナリティクス ダッシュボードとレポートの表示。 • V15.0：ペネトレーションテストアセスメント要求の管理。	• sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_configure_integrations **注:** デフォルトでは、このロールにはサードパーティ統合構成の詳細なロールが含まれています。単一または特定の統合によってアプリセキュリティマネージャーのユーザーグループを定義または編集するには、「脆弱性対応 のペルソナと詳細なロール」を参照してください。 • sn_vul.app_manage_assignment_rules • sn_vul.app_manage_remediation_target_rules • sn_vul.app_manage_risk_score_configurations • sn_vul.app_manage_applications • sn_vul.app_manage_app_vul_permissions • sn_vul.app_manage_normalized_severity • バージョン 13.0：sn_vul.app_manage_app_sc • バージョン 12.0 のみ：sn_vul.app_read_application_release [v12.1 で削除。使用不可] • sn_sec_int.admin • バージョン 13.0：pa_power_user • pa_viewer **注:** 脆弱性対応 v13.0 以降では、pa_viewer は pa_power_user に含まれ、それ自体は不要です。 • V15.0：sn_vul.app_manage_pen_test_request • V15.0：sn_vul.app_update_state • V15.0：cmdb_read
開発者 このグループのメンバーは次のことができます。	• sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザーグループ	このグループでのロール
• 自分にアサインされた AVR レコードの読み取りと書き込み。 • 自分にアサインされている AVI を別の個人またはグループにアサインする。	• sn_vul.app_update_assigned_to • sn_vul.app_pa_sc_view
V15.0：倫理的なハッカー このグループのメンバーは次のことができます。 • ペネトレーションテストアセスメント要求のデフォルトのアサイン先グループとアサイニーの設定。 • ペネトレーションテスト結果の管理。 • ペネトレーションテストアセスメント要求の管理。 • アプリケーション脆弱性一致アイテムの表示。 • アプリケーション脆弱性一致アイテムのアサインの更新。	• V15.0：sn_vul.app_update_state • V15.0：sn_vul.app_manage_pen_test_request • V15.0：itil • V15.0：sn_vul.app_read_all • V15.0：sn_vul.app_manage_pen_test_request_config • V15.0：sn_vul.app_manage_manual_avits • V15.0：sn_vul.app_update_assigned_to • V15.0：sn_vul.app_update_assignment_group

ユーザーを アプリケーション脆弱性対応 のユーザーグループにアサインする

インスタンスのユーザー管理モジュールを使用して、ユーザーをグループにアサインします。

始める前に
必要なロール：admin

手順

ユーザーをグループにアサインする、またはグループから削除するには

a. 次のように移動する。 アドミニストレーション > グループ.

b. 適切なグループ ([アプリセキュリティマネージャー]など) を見つけて開きます。
グループレコードが表示されます。

c. [グループメンバー] タブを選択します。
グループの現在のメンバーが表示されます。

d. [編集] をクリックします。
[メンバーの編集] フォームが表示されます。

e. [コレクション] リストから、グループに追加する、またはグループから削除するユーザーを選択します。

f. すべてのユーザーが [グループメンバー] リストに追加されたか、または削除されたら、[保存] をクリックします。
[グループメンバー] タブに戻ります。

g. [更新] をクリックして変更を保存し、[グループ] リストに戻ります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連情報

アプリケーション脆弱性対応 とともにインストールされるコンポーネント

アプリケーション脆弱性対応 とともにインストールされるコンポーネント

アプリケーション脆弱性対応 機能がアクティブ化されると、いくつかのタイプのコンポーネント (テーブル、ユーザーロール、スケジュール済みジョブなど) がインストールされます。

アプリケーション脆弱性対応 の v24.0.6 以降、最も頻繁に使用されるシステムプロパティに アプリケーション脆弱性対応 アプリケーション内でアクセスできるようになりました。これらのシステムプロパティを表示するには、次に移動します: **All** (すべて)アプリケーション脆弱性対応プロパティ.

注:
アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「アプリケーションとともにインストールされているコンポーネントの検索」を参照してください。

この機能ではデモデータを利用できます。

インストールされるロール

アプリケーション脆弱性対応 の詳細なロールは、デフォルトで特定のユーザーグループにアサインされます。

注:
これらのユーザーグループ以外の詳細なロールを使用するには、コーディングと高度な アプリケーション脆弱性対応 または ServiceNow の専門知識が必要です。

ロールタイトル [名前]	説明	含んでいるロール
V20.0 : sn_vul.app_manage_auto_exception_rule	例外ルールを作成、更新、削除、およびキャンセル (非アクティブ化) します。	sn_vul.app_read_auto_
sn_vul.app_manage_group_rules	アプリケーション修復タスクルールに対する読み取り、書き込み、削除、およびすべての操作。	• sn_vul.app_read_all • sn_vul.app_read_gro
V20.0 : sn_vul.app_exception_approver	例外ルールと例外ルール延長要求を承認します。 v20.0 以降、このロールの詳細ロール sn_vul.app_read_all が削除され、すべてのアプリケーション脆弱性一致アイテムと修復タスクではなく、自分と自分のグループに割り当てられたアプリケーション脆弱性一致アイテムと修復タスクにアクセスできるようになりました。	• sn_vul.app_read_aut • sn_vul.view_manager
sn_vul.app_false_positive_approver	誤検出要求を承認または却下します。	sn_vul.view_manager_v
sn_vul.app_read_assigned	自分にアサインされたアプリケーション脆弱性一致アイテム (AVI) を、クラシック UI と IT 修復ワークスペースの両方で表示します。	sn_vul.view_rem_works

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロールタイトル [名前]	説明	含んでいるロール
	重要: 脆弱性対応 の v24.0 以降、sn_vul.app_read_assigned ロールにはIT 修復ワークスペースにアクセスする権限があります。	
sn_vul.app_read_all	すべての AVI と関連情報をクラシック UI または Vulnerability Manager ワークスペースで表示します。 **重要:** 脆弱性対応 v24.0 以降、sn_vul.app_read_all ロールにはVulnerability Manager ワークスペースにアクセスする権限があります。	sn_vul.view_manager_v
sn_vul.app_write_assigned	自分にアサインされた AVI を更新します。	
sn_vul.app_write_all	すべての AVI と関連情報を更新します。	
sn_vul.app_update_assignment_group	アサイン先グループを更新します。	**注:** デフォルトのユーザ る場合は、sn_vul.ap sn_vul.app_write_a
sn_vul.app_update_assigned_to	AV アサイニーを更新します。	**注:** デフォルトのユーザ る場合は、sn_vul.ap sn_vul.app_write_a
sn_vul.app_configure_integrations	サードパーティ統合を設定します。	sn_vul.app_read_all sn_vul.app_read_integr sn_sec_int.admin sn_vul_veracode.config sn_vul.configure_nvd_a [store-future: BEGIN review]sn_vul_fortify.c **注:** 単一または特定の統 リティマネージャー または編集するには ナと詳細なロール」

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロールタイトル [名前]	説明	含んでいるロール
sn_vul.app_read_integrations	すべてのサードパーティ統合を表示します。	
sn_vul_veracode.configure_integration	Veracode 統合を定義、更新、削除します。	
sn_vul.app_manage_assignment_rules	AVI アサインルールを定義、更新、削除します。	sn_vul.app_read_all sn_vul.app_read_assig
sn_vul.app_read_assignment_rules	アサインルールを表示します。	
sn_vul.app_manage_remediation_target_rules	AVI 修復ターゲットルールを定義、更新、削除します。	sn_vul.app_read_all sn_vul.app_read_remed
sn_vul.app_manage_risk_score_configurations	AVR 算出とリスクルールを定義、更新、削除します。	sn_vul.app_read_all sn_vul.app_read_risk_s sn_sec_cmn.calc.write
sn_vul.app_read_risk_score_configuration	AVR 算出とリスクルールを表示します。	
sn_vul.app_manage_applications	アプリケーションレコードを表示、更新、削除します。	
sn_vul.app_manage_app_sc	[スキャン済みアプリケーション] 関連リストで自分を追加または削除する機能をセキュリティチャンピオンに提供します。	
sn_vul.app_pa_sc_view	特定のセキュリティチャンピオンに関連するビューを提供します。	
sn_vul.app_manage_app_vul_permissions	[内部] sn_vul.app_manage_applications で使用します。	
sn_vul.app_manage_normalized_severity	正規化された重大度へのマッピングを更新します。	sn_vul.app_read_norma
sn_vul.app_read_normalized_severity [v12.1 で削除。使用不可]	正規化された重大度レコードを表示します。	
sn_vul.app_read_application_release	アプリケーションリリースレコードを表示します。	
sn_sec_int.admin	統合へのアクセスを提供します。	
pa_power_user	レポートへのアクセスを提供します。	pa_viewer
sn_vul.app_sec_manager	アプリケーション脆弱性一致アイテムに優先順位を付け、管理します。	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロールタイトル [名前]	説明	含んでいるロール
sn_vul.app_developer	アプリケーション脆弱性の修正を担当する開発者。	
sn_vul.app_create_watch_topic	アプリケーション脆弱性の監視トピックを作成します。	
sn_vul.app_read_watch_topic	アプリケーション脆弱性の監視トピックを読み取ります。	
sn_vul.app_edit_watch_topic	アプリケーション脆弱性の監視トピックを編集します。	
sn_vul_blackduck.configure_integration	サードパーティ統合を設定します。	sn_vul_blackduck.confi

インストールされるスケジュール済みジョブ

脆弱性対応 共有のスケジュール済みジョブについては、「脆弱性対応 とともにインストールされるコンポーネント」を参照してください。

スケジュール済みジョブ	説明
既存の AVI を自動例外ルールに関連付ける	アプリケーション脆弱性一致アイテムの例外ルールへの一致について評価します。
エントリーと CVE M2M の入力	既存のレコードを複数の CWE レコードと整合させます。更新後に 1 回実行し、入力した後、無効にします。
プライマリ CWE を再同期	カスタマイズされたプライマリ CWE 算出用。更新後に 1 回実行し、再同期した後、無効にします。
アプリケーション脆弱性一致アイテムの値を脆弱性とグループにロールアップする	アプリケーション脆弱性一致アイテムの脆弱性とグループのロールアップを算出します。 **注:** アプリケーション脆弱性対応の v23.0 以降では、スケジュール済みジョブが拡張され、マルチスレッド機能を備えたバックグラウンドジョブが作成されます。このアップグレードでは、ジョブをいくつかの小さな子ジョブに分割し、並列または同時に実行します。この変更により、複数のレコードを同時に処理できるようになり、タスク全体の速度が大幅に向上します。
Black Duck プロジェクトリスト統合	Black Duck プロジェクトテーブルにデータを取得して取り込みます。
Black Duck アプリケーションリスト統合	プロジェクトテーブルの Black Duck 統合で、利用可能なすべてのプロジェクトバージョンのアプリケーションを検出されたアプリケーションテーブルにインポートします。
Black Duck アプリケーション脆弱性一致アイテム統合	システム内で検出されたすべてのアプリケーションについて、スキャナーによって検出された脆弱性に基づいて、脆弱性一致アイテムを ServiceNow アプリケーションに取り込みます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インストールされるテーブル

テーブル	説明
アプリケーションリリース [sn_vul_app_release]	アプリケーションのバージョン情報が含まれています。
バージョン 13.0： アプリケーションセキュリティチャンピオン [sn_vul_app_m2m_app_sc]	アプリケーション脆弱性対応 セキュリティチャンピオングループレコードが含まれています。
アプリケーション脆弱性エントリー [sn_vul_app_vul_entry]	アプリケーション脆弱性エントリーが含まれています。
アプリケーション脆弱性統合 [sn_vul_app_integration]	アプリケーション脆弱性対応 統合レコードが含まれています。
アプリケーション脆弱性のスキャン場所 [sn_vul_app_vul_scan_location]	サードパーティスキャンの場所情報が含まれています。
アプリケーション脆弱性のスキャンサマリー [sn_vul_app_vul_scan_summary]	サードパーティスキャンのサマリー情報が含まれています。
アプリケーション脆弱性一致アイテム [sn_vul_app_vulnerable_item]	AVI レコードが含まれています。 v19.0 以降、ソフトウェア部品表に次の列が追加されています。 • sn_sbm_config_rule • sn_sbom_component • vex_justification • vex_detail • vex_response • vex_state • sca_type (SBOM-SCA)
スキャン済みアプリケーション [sn_vul_app_scanned_application]	アプリケーション情報が含まれています。
ステータスマップ [sn_vul_app_state_map]	サードパーティ統合からアプリケーション脆弱性一致アイテム (AVI) 状況への状況マッピングが含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
脆弱性 CWE [sn_vul_m2m_entry_cwe]	CVE データをアプリケーション脆弱性エントリーにリンクします。
アプリケーション修復タスクマニフェスト sn_vul_app_rt_manifest	修復タスクの更新は、スケジュール済みジョブがこのマニフェストテーブルを使用することで行われます。
アプリケーション修復タスク sn_vul_app_vulnerability	アプリケーション修復タスクが含まれています。
アプリケーション修復タスクアイテム sn_vul_app_m2m_vul_group_item	AVI とアプリケーション修復タスク間の M2M テーブル。
バージョン 21.0： アプリケーション脆弱性一致アイテム sn_vul_app_vulnerable_item	AVI レコードが含まれています。
バージョン 21.0： パッケージ [sn_vul_app_package]	アプリケーションパッケージの詳細が含まれています。
バージョン 21.0： ライセンス sn_vul_app_license	アプリケーションライセンスが含まれています。
バージョン 21.0： アプリケーション修復タスク sn_vul_app_vulnerability	アプリケーション修復タスクが含まれています。
sn_vul_blackduck_config	Black Duck 統合構成の詳細が含まれています。
sn_vul_blackduck_project	Black Duck からのプロジェクトの詳細が含まれています。
sn_vul_blackduck_project_import	Black Duck プロジェクトの取り込み用のインポートセットテーブル。
sn_vul_blackduck_app_import	Black Duck アプリケーションの取り込み用のインポートセットテーブル。
sn_vul_blackduck_avit_import	Black Duck AVIT 取り込み用のインポートセットテーブル。

アプリケーション脆弱性一致アイテム **(AVI)** の状況

アプリケーション脆弱性対応 は、任意の時点でのアプリケーション脆弱性一致アイテム (AVI) の状態を示す状況モデルを提供します。各ステータスが互いにどのように関連し、影響を与えているかを知ることで、AVI をいつどのように修復すればよいかを判断できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

アプリケーション脆弱性一致アイテムの状況

状況がどのように機能するかを理解すると、アプリケーション脆弱性一致アイテム (AVI) ルールの作成または編集に役立ちます。AVI には、サードパーティ統合からインポートされた修復ステータスからマッピングされるいくつかの想定される状況があります。AVI の では、[ステータス] フィールドは読み取り専用です。

アプリケーション脆弱性対応状況フロー図

状況	説明
オープン	作成時のステータス。このステータスから、次のことができます。 V16：詳細を取得 Fortify からインポートされた AVI に関する次の情報を取得します。 • 脆弱性のサマリー • 脆弱性の説明 • 推奨事項 • 参照 • 要求 • 応答 V16：誤検出としてマーク スキャナーがシステムに脆弱性が存在することを報告したが、実際には脆弱性が存在しない場合、アイテムを誤検出としてマークします。 V16：例外を要求 例外、再オープン (まで) の日付、理由を要求し、オプションで追加情報を入力します。例外が要求された日付までアイテムの修復を保留します。 V15：クローズ [クローズ済み] ステータス ([脆弱性一致アイテム] ダイアログボックスからの理由) を選択し、追加情報を入力します。AVI を閉じます。 V15：解決 オープン AVI を解決済みとしてマークし、解決済みステータスに移行します。[アプリケーション脆弱性一致アイテムを解決] ダイアログボックスに解決メモを追加する必要があります。
保留	**[V15]**：これは [例外の要求 **(Request Exception)]** オプションによってトリガーされ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション脆弱性対応状況フロー図 (続く)

状況	説明
	ます。承認ワークフローの一部として、保留ステータスは [レビュー中 (In Review)] であり、承認されるまでクローズできません。 このステータスから、次のことができます。 V16：詳細を取得 Fortify からインポートされた AVI に関する次の情報を取得します。 • 脆弱性のサマリー • 脆弱性の説明 • 推奨事項 • 参照 • 要求 • 応答 再オープン クローズ済みまたは解決済みの AVI を [オープン] ステータスに戻します。 クローズ [クローズ済み] ステータス (理由) を選択し、追加情報を入力します。AVI を閉じます。
調査中	[ステータス] リストからこのオプションを選択します。このステータスから、次のことができます。 V20.0 修復タスクまたは AVI レコードを手動で [実装待ち] に移行します。 V16：詳細を取得 Fortify からインポートされた AVI に関する次の情報を取得します。 • 脆弱性のサマリー • 脆弱性の説明 • 推奨事項 • 参照 • 要求 • 応答 V16：誤検出としてマーク スキャナーがシステムに脆弱性が存在することを報告したが、実際

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション脆弱性対応状況フロー図 (続く)

状況	説明
	には脆弱性が存在しない場合、アイテムを誤検出としてマークします。 V16：例外を要求 例外、再オープン (まで) の日付、理由を要求し、オプションで追加情報を入力します。例外が要求された日付までアイテムの修復を保留します。 V15：クローズ [クローズ済み] ステータス ([脆弱性一致アイテム] ダイアログボックスからの理由) を選択し、追加情報を入力します。AVI を閉じます。 V15：解決 オープン AVI を解決済みとしてマークし、解決済みステータスに移行します。[アプリケーション脆弱性一致アイテムを解決] ダイアログボックスに解決メモを追加する必要があります。
実装待ち	レコードを手動でこのステータスに移行するには、AVI から [実装待ち] を選択し、[調査中] ステータスの修復タスクレコードを選択します。このステータスから、次のことができます。 オープン AVI を [オープン] ステータスに戻します。 調査中 解決に関する詳細情報を取得します。[調査中] に移行します。 解決 オープン AVI を解決済みとしてマークし、解決済みステータスに移行します。[アプリケーション脆弱性一致アイテムを解決] ダイアログボックスに解決メモを追加する必要があります。 クローズ [クローズ済み] ステータス ([脆弱性一致アイテム] ダイアログボックスからの理由) を選択し、追加情報を入力します。AVI を閉じます。 このステータスでは、タスクの調査と作業が完了し、修正を実装する準備ができていてもまだ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション脆弱性対応状況フロー図 (続く)

状況	説明
	利用できない場合に、レコードを [実装待ち] に移行します。 [修復コミットメント日] フィールドと [修復計画] フィールドを設定します。 実装後、レコードを解決するかクローズします。
解決済み	[解決 (Resolve)] ボタンからトリガーされます。このステータスから、次のことができます。 V16：詳細を取得 Fortify からインポートされた AVI に関する次の情報を取得します。 • 脆弱性のサマリー • 脆弱性の説明 • 推奨事項 • 参照 • 要求 • 応答 再オープン [オープン] ステータスに戻します。 クローズ [クローズ済み] ステータス (理由) を選択し、追加情報を入力します。グループをクローズします。 メモおよび解決情報が [メモ] タブに表示されます。
クローズ済み	[クローズ (Close)] ボタンからトリガーされます。このステータスから、次のことができます。 再オープン：[オープン] ステータスに戻します。

注:
AVI のソースとなったさまざまな統合については、「 アプリケーション脆弱性対応 と他のアプリケーションとの統合」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション修復タスクのステータス

アプリケーション修復タスクは、作成からクローズまで、修復プロセス全体でさまざまなステータスに移行します。

ステータスの優先順位は次のとおりです。

[保留] > [解決済み] > [実装待ち] > [調査中] > [オープン]

状況移行は、保留、オープン、クローズなどのさまざまなアクションを実行するときに発生します。

特定の状況でアプリケーション修復タスクに対して実行できるアクションは、ホスト修復タスクのアクションと似ています。したがって、詳細については、脆弱性対応ドキュメントの「脆弱性対応 修復タスクステータス」を参照してください。

注:
脆弱性対応の v23.0 以降では、修復タスクのクローズがスキャナーによって行われるように、[クローズ] ボタンが削除されました。

アプリケーション脆弱性対応 修復タスクルールの例

条件ビルダーを使用した修復タスクルールの例。

脆弱性、製品モデル、IP アドレス、およびアサイン先グループを使用した修復タスクルール

1. 新しいレコードの条件ビルダーで、条件を次のように設定します 脆弱性 > 次の値に等しい 既知の脆弱性を入力します。

   脆弱性は、「アプリケーション脆弱性対応 の構成」で説明されているように、国家脆弱性データベース (NVD) と共通脆弱性タイプ (CWE) の統合からインポートされます。

2. [グループ分け基準] セクションで、[アプリケーション脆弱性一致アイテムのグループ化元 **(Group application vulnerable items from)]** フィールドで [アプリケーション脆弱性一致アイテム] を選択します。
3. [使用中 (Using)] フィールドで、[アサイン先グループ] を選択します。

   アサインルールを使用して、修復タスクルールで使用する [アサイン先グループ] フィールドを自動的に設定します。アプリケーションに用意されているルールを使用することも、独自のアサインルールを設定することもできます。詳細については、「アプリケーション脆弱性対応 のアプリケーション脆弱性一致アイテムを自動的にアサインする」を参照してください。

4. 別の条件、たとえば [アプリケーション脆弱性一致アイテムのグループ化元 **(Group application vulnerable item from)]** フィールドで [アプリケーション脆弱性一致アイテム] 構成アイテム、[使用中 **(Using)]** フィールドで IP アドレスまたは製品モデルを選択します。
5. [アサイン] セクションの [修復タスクフィールドをアサインする基準 (Assign remediation task field by)] フィールドで、[フィールド別にグループ化 **(Group by field)]** を選択します。
6. [グループ分け基準] フィールドで、[アサイン先グループ]を選択します。

   このセクションで説明したように、この選択では、[グループ分け基準] セクションで設定した条件に基づいて、脆弱性一致アイテムがさまざまなグループにアサインされます。AVI は脆弱性を共有していますが、CI 製品モデルに基づいてまたは IP アドレス別にさまざまなグループにアサインされます。

7. [送信] を選択してルールを保存します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スキャン済みアプリケーションファイル

アプリケーションは、インポート時に次の場所に保存されます アドミニストレーション > 検出されたアプリケーション in アプリケーション脆弱性対応.

スキャン済みアプリケーションファイル

この表のインポートされたフィールドは、特に指定しない限り読み取り専用です。[部門] と [サポートグループ] のエントリーは、アプリセキュリティマネージャーが手動で追加または編集できます。

フィールド	説明
名前	インポートされたアプリケーションの名前。
バージョン	インポートされたアプリケーションのバージョン (該当する場合)。
運用ステータス	インポートされたアプリケーションの運用ステータス。
部門	インポートされたアプリケーションが属する部門。空の場合は手動で追加できます。
事業部門	インポートされた部門が属する事業部門。[部門] フィールドが入力されると、このフィールドにはその部門が属する事業部門が自動入力されます。それ以外の場合は、空のままで読み取り専用になります。
サポートグループ	インポートされたアプリケーションが属するサポートグループ。空の場合は手動で追加できます。
説明	インポートされたアプリケーションの説明。
前回のポリシーコンプライアンスチェック日	ポリシーコンプライアンスのためにアプリケーションが Veracode によって最後にスキャンされた日付。アプリケーションリスト統合の連結済み統合で、アプリケーションのデルタ取り込みに対応している場合、この日付をそれぞれの統合のデルタ開始時間と比較することで使用されます。 **注:** データは、「前回のポリシーコンプライアンスチェック日」の値が連結済み統合の「開始時間」(delta_start_time) 以上である Veracode からプルされるアプリケーションについて取得されます。
[関連リスト (アプリセキュリティマネージャーまたはセキュリティチャンピオンのみに表示)]	
セキュリティチャンピオン	セキュリティチャンピオンに関連付けられているアプリケーションを一覧表示します。アプリセキュリティマネージャーは、リストのメンバーを追加または削除できます。

[アプリケーション脆弱性一致アイテム] フィールド

アプリケーション脆弱性一致アイテム (AVIT) は、サードパーティの脆弱性統合のインポート中に自動的に作成されます。

[アプリケーション脆弱性一致アイテム] フィールド

[アサイン先グループ]、[アサイン先] フィールド、 および [メモ] を除き、AVIT の他のすべてのフィールドは読み取り専用です。

フィールド	説明
番号	このレコードに対して自動的に生成された AVIT 識別子。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
スキャンタイプ	この AVIT を検出したスキャナーのタイプ。 選択肢は次のとおりです。 • ダイナミック • 静的 • SCA
リスク評価	脆弱性一致アイテムを [重大]、[高]、[中]、[低]、および [なし] に分類する数値化された [リスクスコア] 。リスク評価の詳細については、「アプリケーション脆弱性対応 のリスクを自動的に計算する」を参照してください。
リスクスコア	AVI が環境にもたらすリスクの量を算出したもの。 詳細については、「アプリケーション脆弱性対応 のリスクを自動的に計算する」を参照してください。
修復コミットメント日	AVIT が [調査中] に移行した後に修復する必要がある日付。このフィールドは、AVIT が [調査中] の場合にのみ表示されます。
修復ターゲット	AVIT が最初に識別されてから、修復されるべき日付。該当する場合にのみ表示されます。 修復ターゲットの詳細については、「アプリケーション脆弱性対応 で修復ターゲットトラッキングを自動化する」を参照してください。
修復ステータス	AVIT の修復のステータス。該当する場合は、最も近い期日の AVIT によって決定されます。 状況は次のとおりです。 • 実行中 • 該当 CI 確認中 • 過去のターゲット
カテゴリ名	脆弱性カテゴリの名前
脆弱性	このアプリケーション脆弱性一致アイテムに関連付けられた脆弱性の ID。
アプリケーションリリース	アプリケーションのバージョン。
アプリケーションモジュール	DAST スキャンで影響を受けるアプリケーション。SAST スキャンでは非表示
場所 バージョン 14.0 : SAST	DAST： アプリケーション内の脆弱性の URL の場所。 SAST：アプリケーション内の脆弱性のファイルパスと行番号。
状況	このフィールドは、作成時のデフォルトで [オープン] になっています。状況のマッピング方法の詳細については、「アプリケーション脆弱性一致アイテム (AVI) の状況」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
理由	[AIV が [クローズ済み] ステータスの場合にのみ表示されます。] ステータスの説明。
アサイン先グループ	この AVIT で作業するように選択されたグループ。アプリセキュリティマネージャーが手動で追加または編集できます。
アサイン先	この AVI で作業する、選択されたアサイン先グループの個人。アプリセキュリティマネージャーが手動で追加または編集できます。
初回検出	サードパーティソースがアプリケーション脆弱性一致アイテムを最初に検出した日付。
前回検出	サードパーティソースがアプリケーション脆弱性一致アイテムを最後に検出した日付。
クローズ済み	[AVIT が [クローズ済み] ステータスの場合にのみ表示されます。]AVI がクローズされた日付。
クローズ担当者	[AVIT が [クローズ済み] ステータスの場合にのみ表示されます。]AVIT をクローズしたエンティティ。
サマリー	インポートされた脆弱性の説明。
結果 サードパーティ統合からインポートされた読み取り専用データ。	
ソース AVIT ID	インポートされたソース AVIT の識別子。
ソース重大度	インポートされたソースアプリケーションからの重大度。
ソースターゲット修正日	インポートされたソースが予定している AVIT の修復日。
ソース緩和ステータス	インポートされたソースアプリケーションからの緩和ステータス。
ソース修復ステータス	インポートされたソースアプリケーションからの修復ステータス。
ソース検索ステータス	[設定されている場合のみ表示] インポートされたソースアプリケーションからの問題のステータス。
SDLC ステータス	インポートされたソフトウェア開発ライフサイクルのステータス。
ポリシーに準拠	インポートされたコンプライアンスのステータスステータスがない場合、このフィールドは [適用外 **(Not Applicable)]** に設定されます。
ソースリンク	ソース AVIT への URL。
ソースメモ	インポートされたソースからのメモ。
脆弱性のサマリー	インポートされたソースからのサマリー。
脆弱性の説明	インポートされたソースからの説明。
推奨事項	インポートされたソースからの推奨事項。
参照	インポートされたソースからの参照。
[HTTP 要求/応答 **(DAST** スキャンの場合のみ表示) **(HTTP Request/Response (only visible for DAST scans))]**	
ソース要求	HTTP 要求

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ソース応答	HTTP 応答
Notes	
修復計画	AVIT の修復方法の詳細。計画は、修復コミットメント日までに実装する必要があります。このフィールドは、AVIT が [調査中] の場合にのみ表示されます。
追加コメント / 作業メモ	関連情報。作業メモのテキストボックスを選択して情報を追加します。 脆弱性対応 v20.0 以降では、保留されたアプリケーション脆弱性一致アイテムの [メモ (Notes)] セクションに作業メモを追加できます。

AVIT の経過時間の計算:

- AVIT リストの [経過時間] 列には、AVIT がアクティブである期間 (日数 HH:MM:SS 形式) が表示されます。クローズ済み AVIT の経過時間の値はゼロです。
- AVIT リストの [クローズ所要時間] 列には、AVI がクローズされるまでアクティブである期間 (形式:日数 HH:MM:SS) が表示されます。クローズ済みステータス以外の AVIT の場合、[クローズ所要時間] の値はゼロです。

経過時間およびクローズ所要時間の計算をカスタマイズする方法の詳細については、KB1703270 記事を参照してください。

ペネトレーションテストのステータス

アプリケーションオーナーは、アプリケーションのペネトレーションテストアセスメントを要求し、要求が解決されるまで倫理的なハッキングチームの進捗状況を監視できます。

ペネトレーションテストアセスメント要求は、解決されるまで次の移行状況をたどります。

ペネトレーションテストアセスメント要求のステージ

フィールド	説明
ペネトレーションテストの状況	
オープン	アプリケーションオーナーによってアセスメント要求が作成されたときの状態。
スコーピング	倫理的なハッキングチームは、要求とアプリケーションの範囲を評価します。
環境準備	アプリケーションオーナーは、ロールやその他の情報を含む環境を作成し、テストのために倫理的なハッキングチームに提供します。
テスト	倫理的なハッキングチームがアプリケーションを手動でテストして、ペネトレーションテストの結果を識別します。
V16.1：テスト中	倫理的なハッキングチームは、現在テストが進行中であることを示しています。このステータスが選択されている場合、[保留中のテスト] オプションがフォームで使用可能になります。
V16.1：保留中のテスト	このフィールドは、[テスト中] ステータスが選択されている場合にのみ表示されます。倫理的なハッキングチームは、必要に応じてこの

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ペネトレーションテストアセスメント要求のステージ (続く)

フィールド	説明
	ステータスを選択することで、ペネトレーションテストアセスメント要求の Service Level Agreement (SLA) を制御します。これにより、正確な SLA が報告されます。
V16.1：テストをレビュー中	倫理的なハッキングチームは、テストが完了し、該当分野の専門家によってレビュー中であることを示しています。
クローズ済み	倫理的なハッキングチームは、ペネトレーションテスト結果が報告された後、ペネトレーションテストアセスメント要求をクローズします。 **注:** V16.1 以降では、フォームの [要求をコピーして作成 **(Copy and Create Request)**] オプションを使用して、[クローズ済み] ステータスの要求を複製し、新しい要求を作成できます。詳細については、「[クローズ済み] ステータスのペネトレーションテスト要求の複製」を参照してください。
V16.1：キャンセル	アプリケーションオーナーがペネトレーションテストアセスメント要求をキャンセルします。
V16.1：ドラフト	アプリケーションオーナーは要求を作成し、その要求を送信する前にドラフトとして保存します。
アプリケーション脆弱性一致アイテムの状況	
オープン	倫理的なハッキングチームがペネトレーションテスト結果を識別して作成すると、そのステータスは [オープン] になります。
解決済み	アプリケーションチームがペネトレーションテスト結果を解決すると、ステータスが [解決済み] に変わります。 **注:** ペネトレーションテスト結果が解決されたが、倫理的なハッキングチームによってまだ検証されていない場合、サブステートは *`Validation Pending`* になります。
クローズ済み	倫理的なハッキングチームは、ペネトレーションテスト結果が解決されたことを検証し、ステータスを [クローズ済み] に変えます。

アプリケーション脆弱性対応での保留と誤検出のステータスマッピングの管理

Veracode 脆弱性統合と Fortify 脆弱性統合によってインポートされ、インポート後にインスタンスにマッピングされるアプリケーション脆弱性一致アイテム (AVI) のソースステータスを管理できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性対応の v20.0 以降、ServiceNow ワークフローを使用してインポートされた AVI をトリアージするためのオプションが増えました。

Fortify 脆弱性統合 の構成または Veracode 脆弱性統合 の構成する場合、統合構成ページには、インスタンスの例外と誤検出の管理に役立つ 2 つのオプションがあります。

- ServiceNow での例外の管理
- ServiceNow での誤検出の管理

必要なロール：アプリケーションセキュリティマネージャー

例外管理のためのユースケース

AVI は、ソース ステータスとのこれらの統合からインポートされます。インポート時に、これらのステータスはインスタンスの [ターゲット] および [ターゲット理由 **(Target reason)]** のステータスにマッピングされます。スキャナーのソースステータスとインスタンスで使用されるステータスが完全に一致しない場合があるためです。

たとえば、Fortify 脆弱性統合からの [修正されない]、[修正の保留 **(Remediation Deferred)]**、[リスク受容]、[リスクの軽減 **(Risk Mitigated)]** などのソースステータスは、インスタンスで [リスク受容] または [コントロールの緩和を実施] のサブステートを持つ [保留] ステータスにマッピングされます。

これらの統合の設定ページには、次のオプションがあります。

オプション	チェックボックスをオン	説明
ServiceNow での例外の管理	Y (デフォルト)	このオプションを選択したままにする場合は、AVI レコードから例外を要求する必要があります。 [保留] ステータスのマークが付けられているインポートされた AVI は、ServiceNow 例外管理ワークフローでトリアージされます。 通常は [保留] ステータスにマッピングされる [ソース] ステータスを持つ AVI は、[オープン] ステータスの [ターゲットトリアージステータス] にマッピングされます。
	N	チェックボックスをオフにすると、スキャナーからインポートされた [ソース] ステータスが保持されます。 これらの AVI は、インスタンスの [ターゲット] ステータスに [保留] として、および [ターゲット理由 **(Target reason)]** ステータスにマッピングされ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	チェックボックスをオン	説明
		ます。[ターゲットトリアージ] ステータスおよび [ターゲットトリアージ理由] ステータスにマッピングされていないため、例外ワークフローによってトリアージされません。 レコードが既に [保留] ターゲットステータスになっているため、[例外の要求] UI アクションは AVI レコードでは使用できません。

誤検出のユースケース

たとえば、Veracode 脆弱性統合からの誤検出の場合、[誤検出] や [潜在的な誤検出] などのソースステータスは、サブステートが [誤検出] の [クローズ済み] [ターゲット状況] にマッピングされます。

オプション	チェックボックスをオン	説明
ServiceNow での誤検出の管理	Y (デフォルト)	このオプションを選択したままにする場合は、AVI レコードから [誤検出] を要求する必要があります。 [誤検出] や [潜在的な誤検出] のマークが付けられているインポートされた AVI は、ServiceNow 例外管理ワークフローでトリアージされます。 通常は [クローズ済み] [ターゲットステータス] にマッピングされる [ソース] ステータスを持つ AVI は、[オープン] の [ターゲットトリアージ] ステータスにマッピングされます。 [誤検出] UI アクションは AVI レコードで使用できます。
	N	チェックボックスをオフにすると、スキャナーからインポートされた [ソース] ステータスが保持されます。 これらの AVI は、インスタンスの [誤検出]で [ターゲットステータス] に [クローズ済み] として、および [ターゲット理由

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	チェックボックスをオン	説明
		(Target reason)] ステータスにマッピングされます。これらは誤検出ワークフローによってトリアージされません。 レコードが既に [クローズ済み] ターゲットステータスになっているため、[誤検出] UI アクションは AVI レコードでは使用できません。

アプリケーション脆弱性対応 参照

アプリケーション脆弱性対応 では次の用語が使用されます。

アプリケーション脆弱性一致アイテム (AVI)

脆弱性エントリーと自社環境における潜在的な脆弱性アプリケーションのペアリング。

アサインルール

定義された基準に基づいて AVI をアサインするために使用されるルール。

共通プラットフォーム一覧 (CPE)

情報技術システム、ソフトウェア、およびパッケージのための NIST NVD 構造化命名スキーム。

一般的な脆弱性とエクスポージャー (CVE)

情報セキュリティの脆弱性とエクスポージャーに関する公知の辞書。

共通脆弱性タイプ一覧 (CWE)

コミュニティで開発されたソフトウェアの脆弱性タイプのリスト。

統合

CWE またはサードパーティシステム (Veracode など) からレポートデータをプルして、脆弱性データを取得するスケジュール済みジョブ。

> **注:**
> 脆弱性対応 の NIST National Vulnerability Database 統合がアクティブ化されて設定されている場合、CVE 拡張は CWE で使用できますが、必須ではありません。NIST National Vulnerability Database 統合の詳細については、「NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理」を参照してください。

脆弱性情報データベース (NVD)

セキュリティ設定共通化手順 (SCAP) を使用して表される、標準ベースの脆弱性管理データの米国政府リポジトリ。

修復ターゲットルール

定義された基準に基づいて、AVI に修復の目標期日をアサインするために使用されるルール。

脆弱性算出

定義された基準に基づいて、アプリケーションの脆弱性に優先順位を付けて分類するために使用される算出。

アプリケーション脆弱性対応の例外ルールフォーム

例外ルールの既知の脆弱性に基づくルールの例。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
名前	目的を識別してルールを簡単に見つける助けとなる一意の名前 (Veracode-1 cwe-22 exception など)。
状況	読み取り専用：ドラフト
有効期限開始	このルールがアクティブになり、VI が保留される日付。
実行順序	各例外ルールの一意の順序。小さな値から大きな値の順です。
有効期限	修復タスクが新しい VI の受け入れを停止する日付。
保留期限	修復タスクと AVI の保留期限の日付。この日付になると、AVUL がクローズされ、すべての AVI がタスクから移動して再オープンされます。グループルールがこうした AVI に再適用されます。
理由	この例外ルールを作成する理由。リストから 1 つを選択します ([修正不可] など)。
アサイン先グループ	保留された VI を追跡するためにアサインされたグループ (アプリセキュリティマネージャーなど)。
追加情報	要求者が承認者に提供する追加情報。この情報は、修復タスクの説明フィールドに入力されます。この例では、Defer AVIs with the vulnerability – Veracode-1-22 です。
条件	このルールに一致する AVI を指定するフィルター条件。この例では、Vulnerability is Veracode-1-22 です。
既存のデータで実行	このルールが初めて実行されるときに既存のデータでこのルールを実行できるようにするオプション。 このオプションを非アクティブのままにすると、ルールは新しいデータで始まるスケジュール済みジョブ *`Associate existing AVIs with Auto Exception Rule`* によって毎日実行されます。 [既存のデータで実行] オプションを有効にすると、スケジュール済みジョブは「有効期間開始日」に既存のデータに対して 1 回実行されます。

アプリケーション脆弱性対応 製品ビュー

アプリケーション脆弱性対応 (AVR) 製品は、アプリケーションセキュリティテストツールによって検出された弱点と脆弱性を取り込み、環境内のすべてのアプリケーションのセキュリティ体制を一括管理画面で把握できるようにします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

AVR を使用すると、修正ワークフローのリスクを軽減できます。この製品ビューは、AVR の主要エンティティが CSDM コアフレームワークでどのように機能するかを理解するのに役立ちます。

更新された用語

AVR v19.0 以降では、次のキーテーブル名と列名が更新されています。その結果、ドキュメントには古い名前と新しい名前の両方への参照が表示されます。

更新された **AVR** の用語、テーブル、およびフィールド名のリスト

AVR v19.0 より前	**AVR v19.0** 以降
CI ルックアップルール	ルックアップルール
CI ルックアップルールフォーム	ルックアップルールフォーム
CI 一致ルール	一致ルール
検索するテーブル	CI テーブルで検索
検索対象フィールド	CI フィールドで検索
アプリケーションリリース	検出されたアプリケーション
アプリケーションリリーステーブル	検出されたアプリケーションテーブル
事業上の重要度	ソース事業上の重要度

必須条件

次のアプリケーションの最新バージョンをインストールします。

- Security Support Common
- 脆弱性対応
- Security Integration Framework
- セキュリティサポートオーケストレーション
- Veracode や Fortify などのスキャナー統合

AVR と CSDM 4.0

AVR v19.0 より前では、アプリケーションの脆弱性が取り込まれると、脆弱性が取り込まれたアプリケーションは、ルックアップの対象となっていました。その際に、スキャン済みアプリケーション (sn_vul_app_scanned_application) に対して CI ルックアップルールが使用されました。アプリケーション名レコードが存在しない場合は、エントリが作成されていました。

AVR v19.0 以降では、CSDM 4.0 フレームワークに合わせるために、スキャン済みアプリケーションテーブルの代わりに製品モデルテーブルが使用されます。アプリケーションにバージョンがある場合、ルックアップはソフトウェアモデルテーブルに対して行われます。アプリケーションにバージョンが存在しない場合、ルックアップはアプリケーションモデルテーブルに対して行われます。アプリケーションモデルとソフトウェアモデルはどちらも製品モデルテーブルの子テーブル、つまり CMDB の基盤テーブルです。次のスクリーンショットでは、製品モデルを説明しています。

システムプロパティ

CSDM 4.0 製品モデルベースのルックアッププロセスを使用するには、システムプロパティ *sn_vul.use_product_model* を *true*に設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システムプロパティの考慮事項

システムプロパティ名	システムプロパティ値	ルックアップターゲット値	考慮事項
sn_vul.use_product_model	true	[製品モデル] 値の選択	新規ユーザーは、CSDM 4.0 フレームワークの製品モデルルックアップルールを使用するために、[製品モデル] 値を選択する必要があります。
	false	[構成アイテム] 値の選択	既存のユーザーは、CI ルックアッププロセスと既存の **CI** ルックアップルールを引き続き使用できます。

注:
ルックアップターゲット値を設定するには、[ルックアップルール **(Lookup Rule)]** ページ > **[AVR** 統合ルックアップルール **(AVR integration lookup rule)]** > [ルックアップターゲット **(Lookup target)]** フィールドに移動します。

AVR のルックアップルール

CSDM 4.0 フレームワークでは、CI ルックアップルールの代わりに製品モデルベースのルックアップルールを使用して、それぞれの製品モデルクラスにエントリを作成します。スクリプトの場合も同様に、CSDM 4.0 モデルのフレームワーク内でルックアップルールを定義できます。

AVR v19.0 以降では、ルックアップルールを作成するときに、[ルックアップターゲット **(Lookup target)]** フィールドを使用して、構成アイテムアプローチと製品モデルアプローチのどちらを使用するかを定義する必要があります。詳細については、「CI ルックアップルールを作成する」を参照してください。

検出されたアプリケーション

次のように移動する。 **All** (すべて) > 検出されたアプリケーション. [検出されたアプリケーション (Discovered Applications)] テーブルには、スキャナーから取り込まれたアプリケーションが表示されます。システムプロパティ *`sn_vul.use_product_model`* が *`true`* に設定されている場合は、アプリケーションに対応する製品モデルを表示できます。

AVR の考慮事項

重複する **CI** または製品モデルレコードの存在

システムプロパティ *`sn_vul.use_product_model`* がルックアッププロセスに対して正しく構成されていることを確認します。ルックアップルールフォームを構成するときは、構成アイテムまたは製品モデルのいずれかを必ずルックアップターゲットとして選択してください。

コンテナ脆弱性対応

ServiceNow® コンテナ脆弱性対応 アプリケーションはコンテナ脆弱性一致アイテム (CVIT) をインポートし、ルールに従ってコンテナ脆弱性を修復できるようにします。脆弱性データは、脆弱性情報データベース (NVD) 統合やサードパーティの統合などの内部および外部のソースから取得されます。

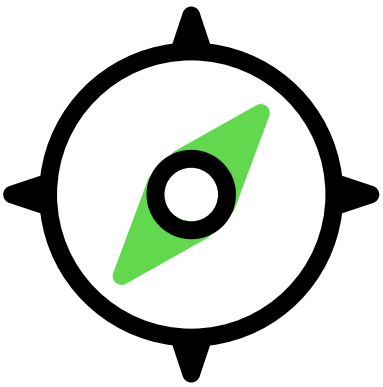
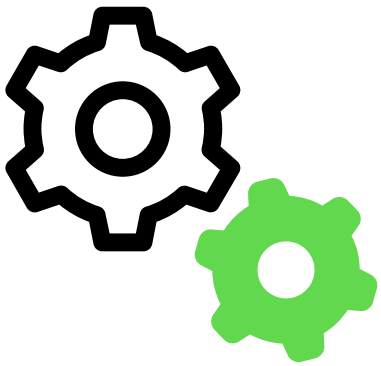
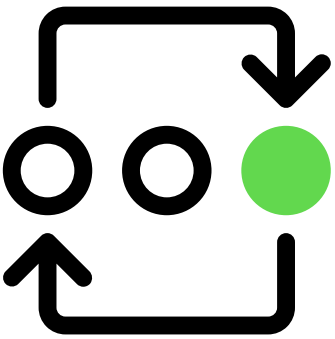
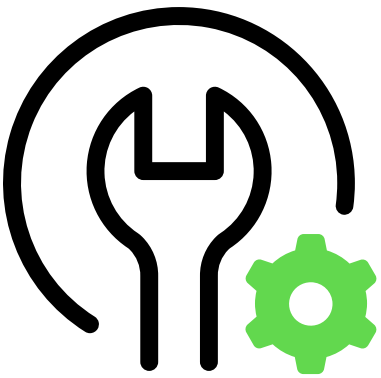
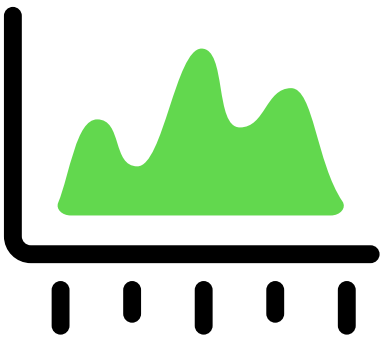
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

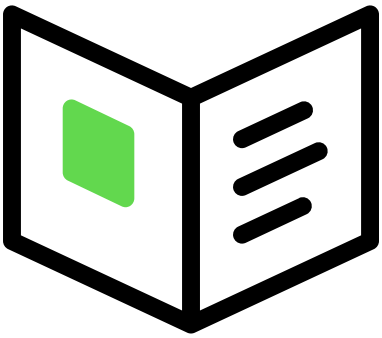
コンテナ脆弱性対応

探索	構成	統合
		
Container Vulnerability Response の概念と機能について説明します。	Container Vulnerability Response を構成します。	他のアプリケーションと統合することで、Container Vulnerability Response を拡張します。
脆弱性対応ワークスペースの使用	**修復**	**アナリティクスとレポート**
		
脆弱性マネージャー、IT 修復、および脆弱性アセスメントのワークスペースで CVIT を監視、管理、および修正する方法について説明します。	コンテナーの脆弱性を修復する方法について説明します。	Container Vulnerability Response アナリティクスの表示

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンテナ脆弱性対応 (続く)

	Reference (参照)	
	 フィールド、テーブル、プロパティなどのコンテナ脆弱性対応コンポーネントの詳細を取得します。	

メリット

コンテナ脆弱性対応 アプリケーションには次のメリットがあります。

- サードパーティのコンテナセキュリティ製品 (Palo Alto Networks の Prisma Cloud Compute など) と統合します。
- ランタイムに展開されているイメージの脆弱性データをインポートし、ランタイムコンテキスト情報 (ホスト、Kubernetes クラスター、サービス、名前空間など) によって脆弱性データを拡張します。
- ServiceNow Kubernetes 検出を使用して、脆弱性から関連する Kubernetes エンティティに対して作成された参照のリストを 構成管理データベース (CMDB) に表示します。
- 脆弱性と修復の傾向に関するインサイトを示す包括的なレポートダッシュボードを提供します。

主な機能

コンテナ脆弱性対応 アプリケーションは、コンテナで検出された脆弱性を管理します。次の機能を提供します。

- 実行中のコンテナではなく、CVIT のソース Docker イメージをポイントします。
- イメージ、Kubernetes クラスター、名前空間、またはサービスレベルで追跡する CVIT の粒度を設定します。
- 新しいイメージバージョンを追跡して、修正された脆弱性を特定します。古いバージョンで報告された脆弱性は、新しいイメージバージョンが実行時に展開されると ServiceNow で自動的に解決されます。
- アプリケーションイメージとは別にベースイメージ内の CVIT を追跡して、独立した修復を有効にします。
- 例外要求または誤検出要求を作成します。これらは、複数レベルの承認者プロセスで確認できます。
- CVIT を自動的に保留するための例外ルールを定義します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユースケース

コンテナは、複数の環境でアプリケーションを展開およびスケーリングするための優れた方法であり、オーバーヘッドが少なく、移植性が向上します。ただし、コンテナイメージの脆弱性は、基盤となるホストにリスクをもたらし、最終的にはコンテナがこれらのイメージから起動されているインフラストラクチャにリスクをもたらす可能性があります。コンテナイメージで脆弱性をスキャンするコンテナセキュリティ製品は多数ありますが、脆弱性の修復に関連する考慮事項と問題がいくつかあります。コンテナ脆弱性対応 は、コンテナイメージの脆弱性の修復に関連するさまざまな問題やユースケースの解決に役立ちます。コンテナ脆弱性対応 モジュールを活用する方法を説明します。

ランタイムコンテキスト

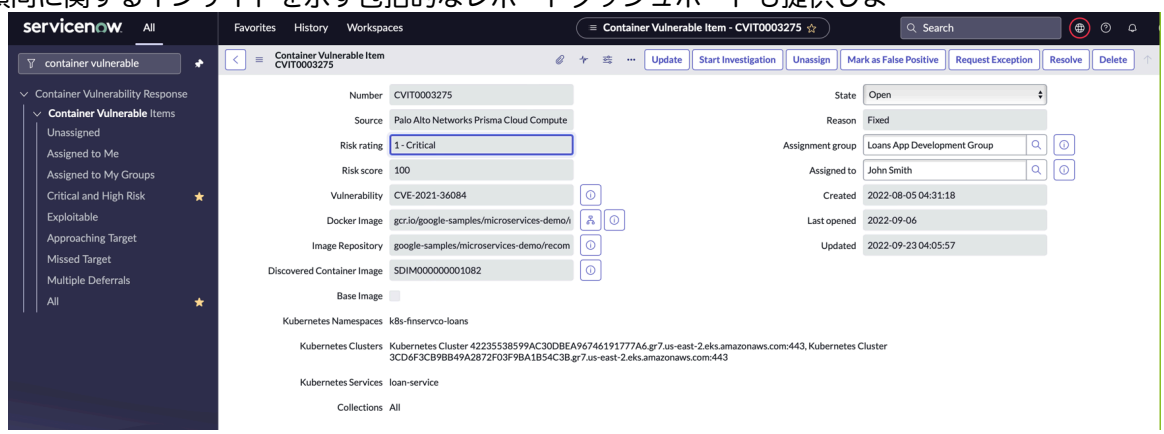
コンテナイメージの脆弱性は、アプリケーションライフサイクルの次のステージでイメージをスキャンすることで検出できます。

- ステージ 1：CI/CD パイプラインでイメージがビルドされるステージ。
- ステージ 2：イメージがレジストリに公開されるステージ。
- ステージ 3：イメージがランタイムに展開されるステージ。

ステージ 1 とステージ 2 のできるだけ早期の段階で脆弱性を特定することが重要ですが、ランタイム環境に展開されているイメージに対してスキャンを実行することも同様に重要です。これには次のメリットがあります。

- 公開された新しい共通脆弱性識別子 (CVE) を特定します。
- 展開されているアプリケーションのリスク体制を正確に可視化します。
- 解決する必要がある脆弱性に優先順位を付けます。脆弱性が原因で影響を受けるアプリケーションサービスまたはビジネスサービスに関するランタイムコンテキストは、優先順位付けの際に役立つ可能性があります。

コンテナ脆弱性対応 は、Palo Alto Networks の Prisma Cloud Compute などのコンテナセキュリティ製品と統合して、ランタイムに展開されているイメージの脆弱性データをプルし、ランタイムコンテキスト情報 (ホスト、Kubernetes クラスター、サービス、名前空間など) で脆弱性データを拡張します。ServiceNow Kubernetes 検出を使用しているお客様に対し、脆弱性から関連する Kubernetes エンティティに対して作成された参照のリストが 構成管理データベース (CMDB) に表示されます。ServiceNow は、メタデータの拡張の他に、脆弱性と修復の傾向に関するインサイトを示す包括的なレポートダッシュボードも提供します。



所有責任の特定

前提条件

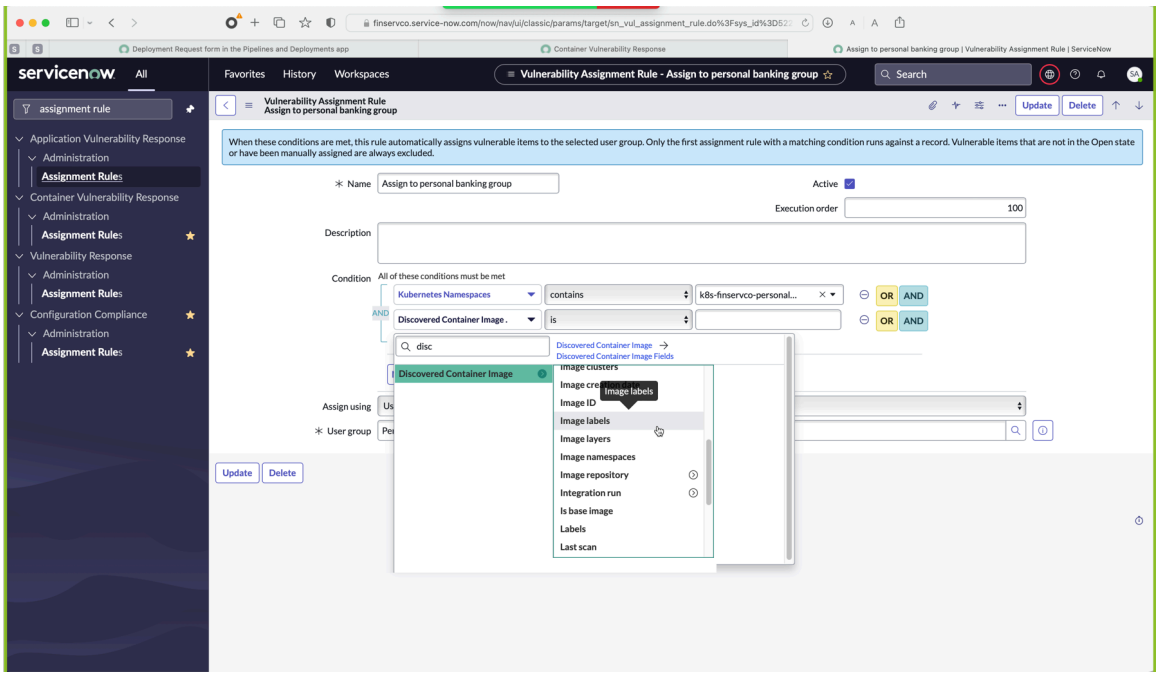
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- **Kubernetes** メタデータと参照：コンテナ脆弱性対応 が Kubernetes メタデータ (名前空間、クラスターなど) と 構成管理データベース (CMDB) エントリへの参照を入力できるようにするには、Information Technology Operations Management (ITOM) から Kubernetes 検出を実装する必要があります。Kubernetes 検出により、Docker イメージ、実行中の Docker コンテナ、ポッド、Kubernetes クラスターなどが CMDB に入力されます。コンテナ脆弱性対応 は、イメージ ID に基づいて CMDB 内の Docker イメージを識別してから、関連する Kubernetes エンティティを識別して、脆弱性一致アイテムからそれらのエンティティへの参照を入力します。

- クラウドメタデータと **Docker** イメージラベル：コンテナ脆弱性対応 は、Docker イメージラベル、クラウドアカウント ID、およびイメージが展開されているリージョンも入力します。このデータは、脆弱性一致アイテムに関連付けられている「検出されたコンテナイメージ」レコードに保持されます。このデータを入力するための前提条件はありません。コンテナ脆弱性対応 は、コンテナセキュリティ製品 (Palo Alto Prisma Cloud Compute など) から返されたデータを使用して、これらのエントリを入力します。

コンテナイメージの脆弱性にパッチを適用する所有責任は、組織によって異なります。この情報は、さまざまな場所で取得できます。特定のコンテナイメージを所有するアプリケーションチームを確認する方法として Docker イメージラベルを使用する組織がありますが、他の組織では、正しい所有者を特定する方法として、コンテナイメージが展開されている Kubernetes 名前空間またはクラウドアカウントが使用されます。

コンテナ脆弱性対応 は、「アサインルール」モジュールで Docker イメージラベル、Kubernetes クラスター/サービス/名前空間メタデータ、またはクラウドアカウントメタデータ (クラウドアカウント ID、リージョン、プロバイダーなど) をキャプチャして使用できるようにするために必要なデータモデル要素を提供します。また、イメージのメタデータまたはランタイム環境に基づいて、脆弱性を適切なアプリケーションチームに自動的にアサインします。



ベースイメージの脆弱性の追跡

前提条件

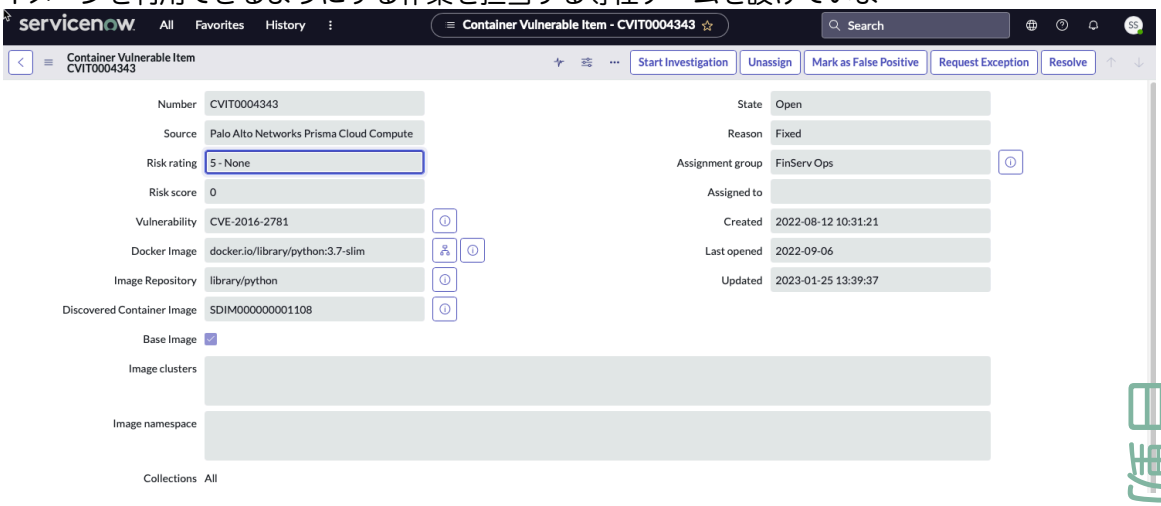
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

コンテナ脆弱性対応 で [基準イメージ] プロパティが入力されるようにするには、Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute コンソールでベースイメージを明示的に設定する必要があります。Prisma Cloud でベースイメージを構成する方法の詳細については、https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/base_images を参照してください。

コンテナ脆弱性対応 を使用すると、ベースレイヤーの個別の脆弱性レコードを作成でき、このレコードを別のチームにアサインできます。

コンテナイメージの他のレイヤーで検出された脆弱性から、Alpine などのベース OS イメージで特定された脆弱性を追跡します。多くの組織では、ベース OS イメージにパッチを適用し、すべてのアプリケーションチームがベース OS イメージを利用できるようにする作業を担当する専任チームを設けています。

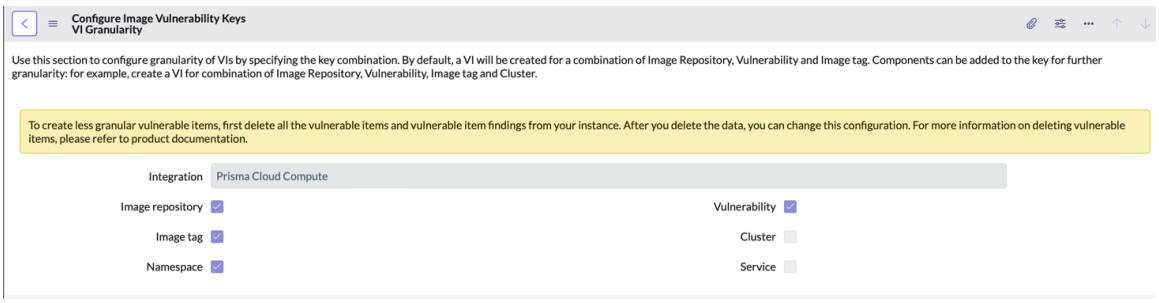


す。

脆弱性一致アイテムの粒度の定義

前提条件

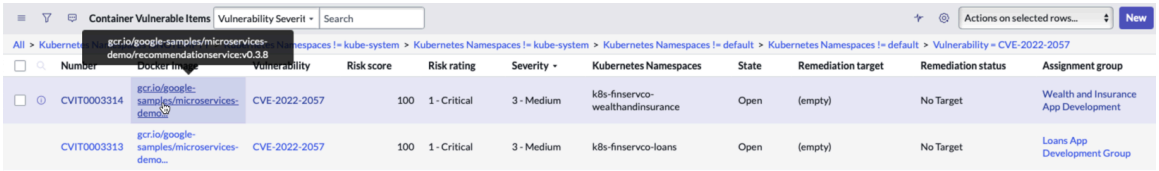
に移動すると、CVIT の粒度が設定されます。 **All** (すべて) > **Container Vulnerability Response** > アドミニストレーション > **VI** の粒度の構成.



デフォルトでは、CVE と Docker イメージバージョン (参照 + タグ) の一意の組み合わせごとに脆弱性一致アイテムが作成されます。ただし、いくつかの Docker イメージが複数の Kubernetes 名前空間に展開されており、各名前空間が異なる事業部門またはチームによって所有されていることがあります。各チームが、脆弱性を修正するための新しいバージョンのコンテナイメージのロールアウトを、それぞれ独自の頻度で行う可能性があります。このような状況に対応するために、コンテナ脆弱性対応 では脆弱性一致アイテムの粒度を定義できます。つまり、Docker イメージバージョンと脆弱性の一意の組み合わせの Kubernetes 名前空間/クラスター/サービスごとに、1 つの脆弱性一致アイテムを作成するかどうかを定義できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



この例では、同じ Docker イメージと CVE の組み合わせに対して 2 つの脆弱性一致アイテムが作成されていることがわかります。1 つは Kubernetes 名前空間「k8s-finservco-loans」の脆弱性一致アイテム、もう 1 つは「k8s-finservco-wealthandinsurance」の脆弱性一致アイテムです。

タグベースのサービス識別を使用して影響を受けるサービスを識別する

前提条件

- アプリケーション内のさまざまなサービスを識別し、それらのサービスを表すタグ/キーと値のペアを定義します。
- これらのタグまたはラベルを使用して、Docker イメージと Kubernetes ポッドを展開します。
- 適切なタグまたはラベルを使用して「タグベースのサービス」を定義します。
- ITOM Kubernetes ディスカバリーを展開します。
- 適切なタグまたはキーと値のペアを使用して「タグベースのサービス」を定義します。
- コンテナ脆弱性対応 を使用して脆弱性データを ServiceNow にインポートする

脆弱性一致アイテムのリスク計算は、CMDB で CI (Docker イメージ) と関連サービスの重要度を確認することで実行できます。ただし、影響を受けるサービスを簡単に特定できるように、コンテナ脆弱性対応 にはタグベースのサービス識別機能があります。

Kubernetes ポッドまたはエンティティが、ServiceNow で任意の「タグベースのサービス」で定義されているキー値に一致するキー値またはラベルを使用して公開されると、コンテナ脆弱性対応 は、Docker イメージと影響を受けるアプリケーションサービスの間の関係を自動的に確立し、リスク計算でそのアプリケーションサービスの重要度を使用します。

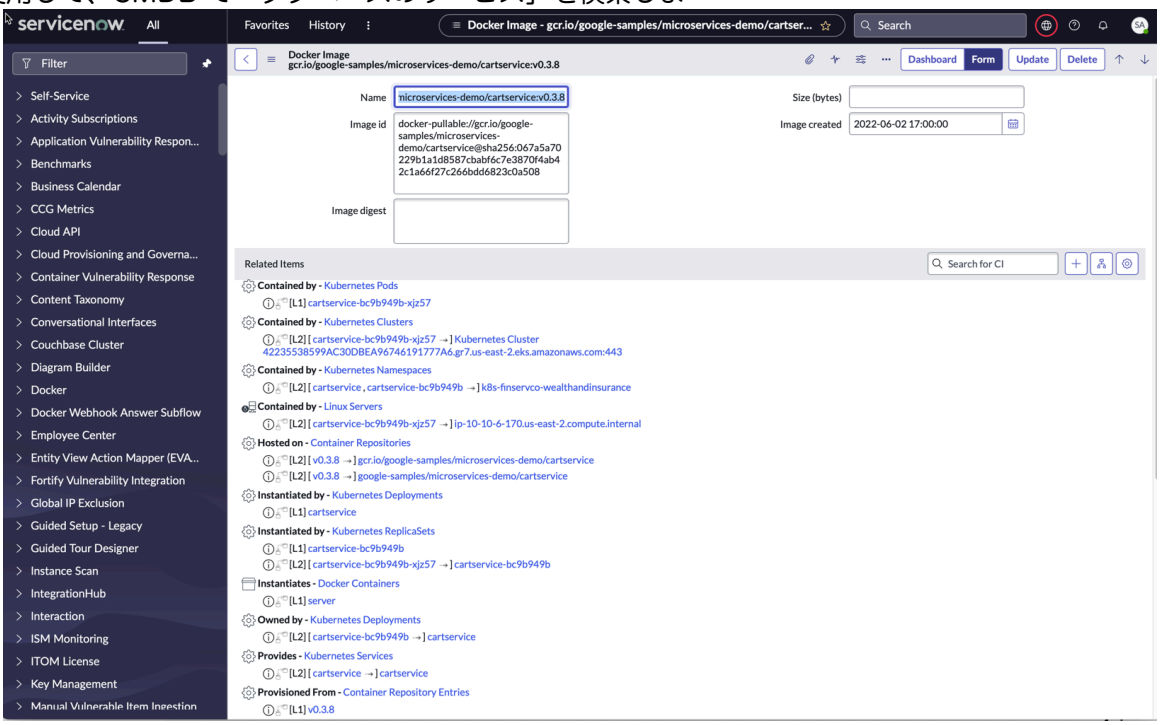
フローは次のようになります。

1. コンテナ脆弱性対応 がコンテナセキュリティ製品から脆弱性データをインポートします。
2. コンテナ脆弱性対応 はコンテナ脆弱性一致アイテムごとに、脆弱性がある Docker イメージを CMDB から取り込みます。
3. 次に コンテナ脆弱性対応 は Docker イメージラベル、またはこのイメージが展開されている Kubernetes ポッドで公開されているラベル/キー値を調べます。Kubernetes 検出を実行している場合、このイメージは CMDB で利用可能です。

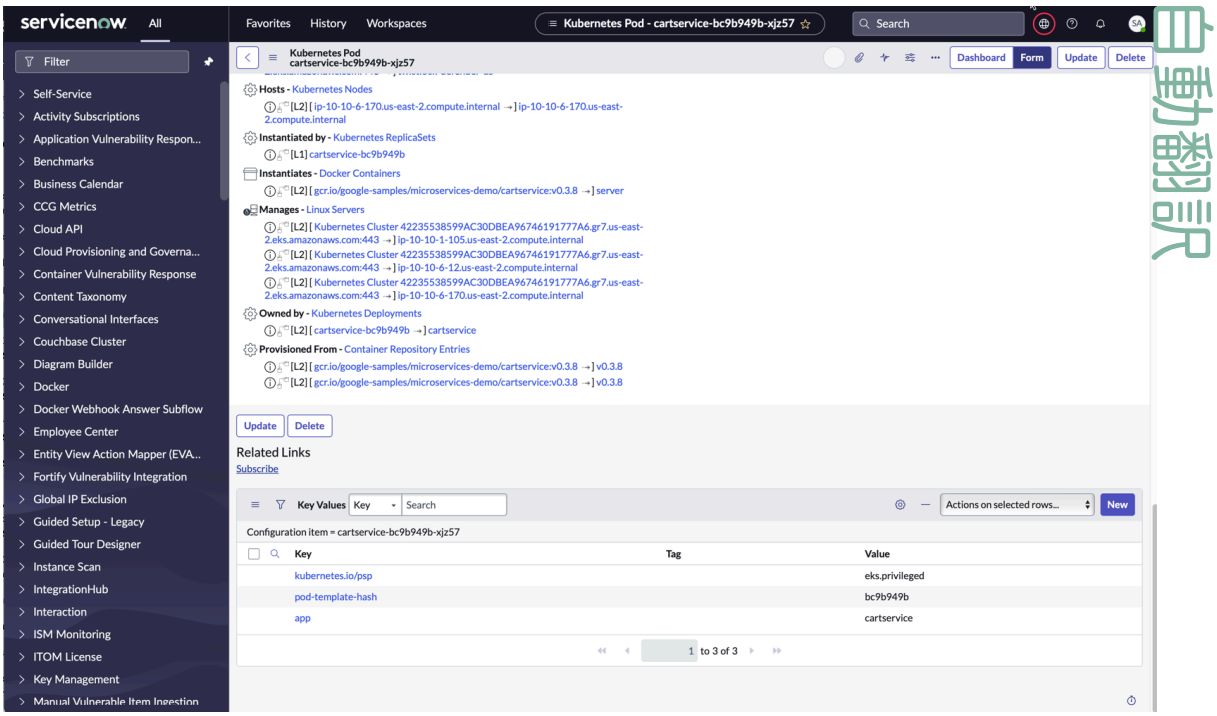
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. コンテナ脆弱性対応 は、一致する同じ定義済みのキー値のペアを使用して、CMDB で「タグベースのサービス」を検索します。

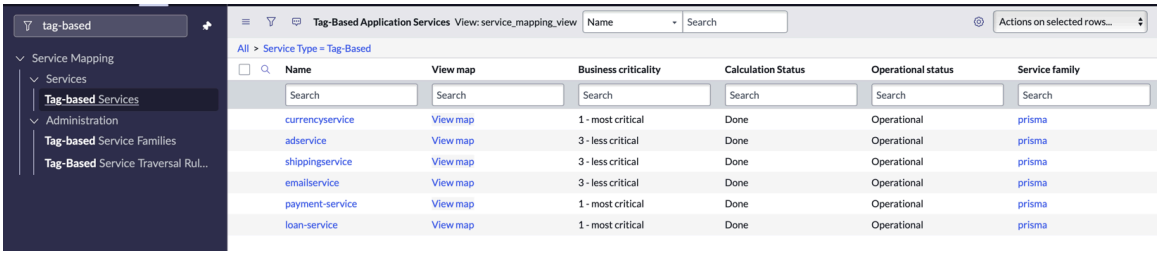


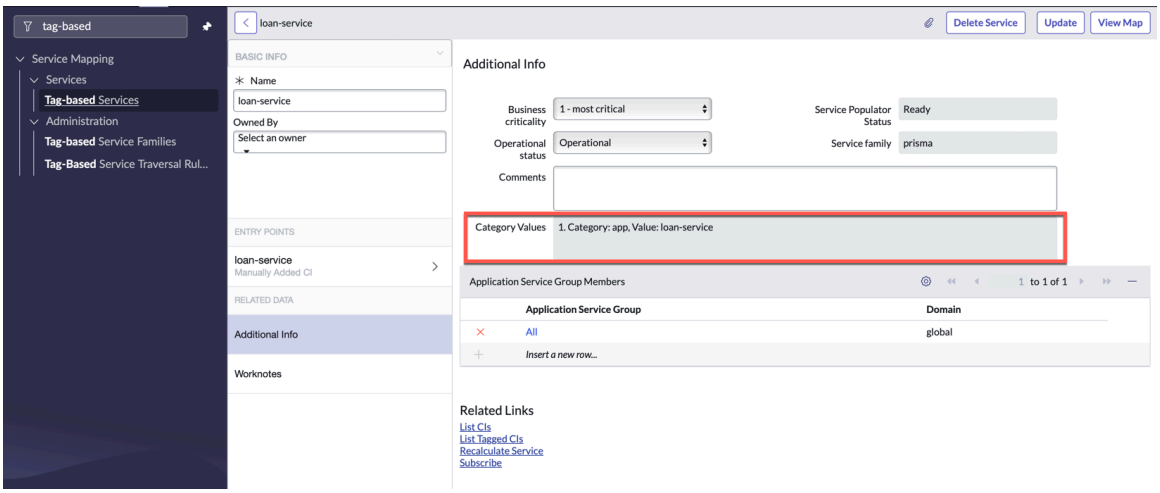
す。



5. コンテナ脆弱性対応 は、一致する「タグベースのサービス」(検出された場合) の「事業上の重要度」を使用して、コンテナ脆弱性一致アイテムのリスクを計算します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

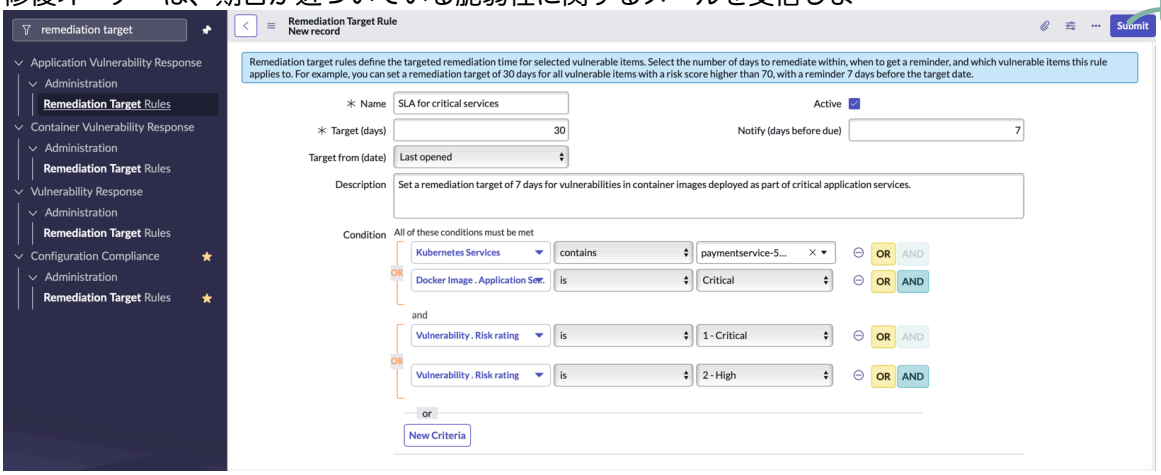




脆弱性の追跡

修復ターゲットの設定

ServiceNow では、脆弱性マネージャーが「修復ターゲットルール」を定義できます。これにより、コンテナイメージで見つかった脆弱性の修復に関する Service Level Agreement (SLA) を定義できます。修復ターゲット日は、イメージメタデータまたは脆弱性情報の条件/基準に基づいて定義できます。修復オーナーは、期日が近づいている脆弱性に関するメールを受信します。



修正された脆弱性の特定

ホストにパッチを適用することで修正できるホスト脆弱性とは異なり、コンテナ脆弱性にはパッチを適用できません。古いバージョンのコンテナイメージを置き換えるため、新しいバージョンのコンテナイメージを作成して展開する必要があります。この新しいバージョンの ID (イメージ ID) は以前のバージョンとは異なるため、どの脆弱性が既に修正されているかを追跡することが困難になります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

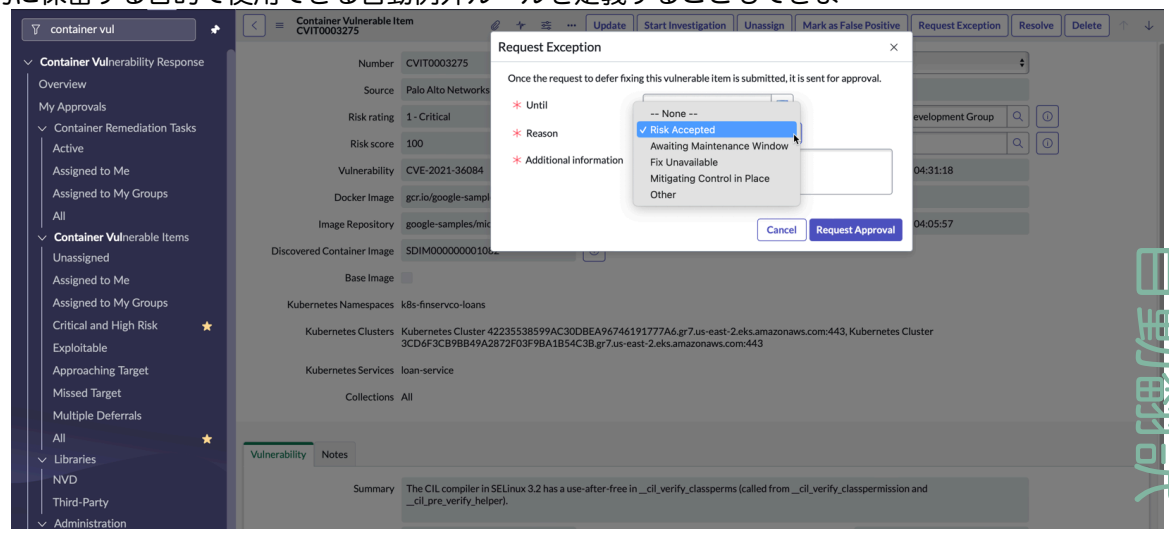
ServiceNow は、以前のバージョンのコンテナイメージで報告されているが、最新バージョンのイメージでは解決されている脆弱性を特定し、これらの脆弱性を自動的に「クローズ済み/修正済み」ステータスに移行します。これにより、セキュリティチームは常に最新のリスク体制を正確に把握できます。

例外の管理

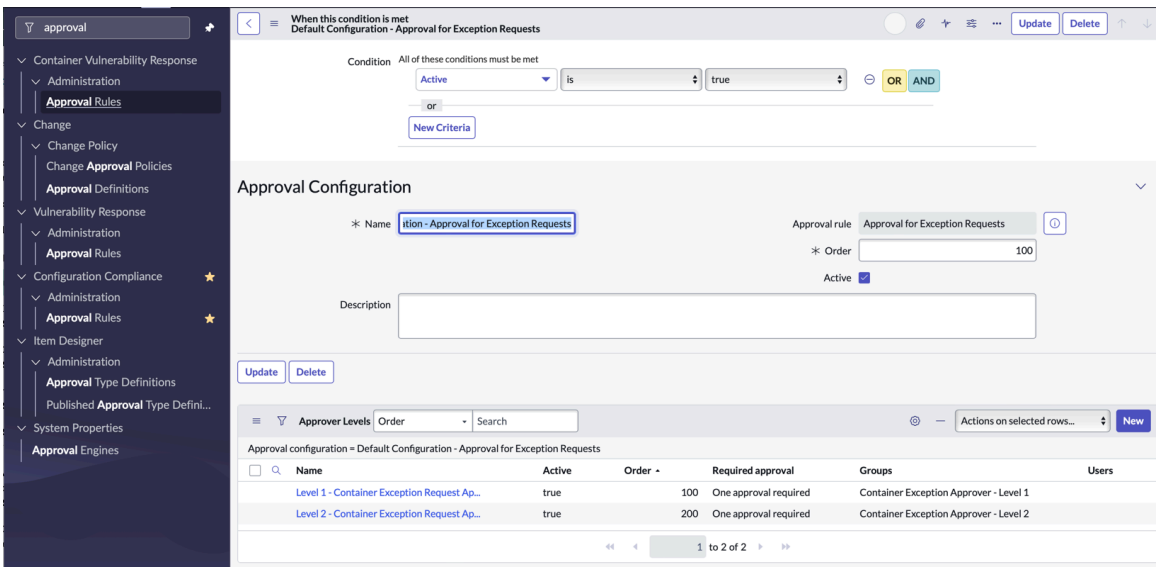
次の理由から、脆弱性のアプリケーションチームまたは修復オーナーが例外を要求する必要があることがあります。

- 緩和コントロールが既に導入されている。
- リスクの受容
- 修正をプッシュするためメンテナンス期間待ちである。

ServiceNow ではセキュリティアドミニストレーターが例外要求に対して複数レベルで承認者を定義できます。特定の条件に一致する脆弱性を自動的に保留する目的で使用できる自動例外ルールを定義することもできます。



す。



最新情報

Yokohama の新機能と変更点の詳細については、Yokohama のリリースノートを参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

開始するには

- Now Platform インスタンスの セキュリティオペレーション の概要については、「Understanding Security Operations (Security Operations の理解)」を参照してください。
- ServiceNow Store からダウンロードできる セキュリティオペレーション アプリケーションの詳細については、「Security Operations and the ServiceNow Store (Security Operations と ServiceNow Store)」を参照してください。

コンテナ脆弱性対応 の詳細

コンテナ脆弱性対応 アプリケーションは、コンテナ脆弱性一致アイテム (CVIT) をインポートします。ルールに従って、この機能を使用してコンテナの脆弱性を修正できます。コンテナ脆弱性対応 は個別のサブスクリプションで利用できます。

従来のアプリケーションとは異なり、コンテナはすべてのアプリケーションソースコードをその依存関係とともに、コンテナイメージというバイナリファイルにパッケージ化します。イメージはレジストリに公開されるため、任意のプラットフォームでアプリケーションまたはコンテナインスタンスとしてこのイメージを実行することができます。コンテナ導入前のライフサイクルには、次のステージがあります。

1. コンテナイメージを作成する：コンテナイメージが作成され、ソースコードまたは依存ライブラリに指定されます。
2. コンテナイメージをビルドする
3. コンテナイメージを公開する：コンテナイメージファイルがレジストリに公開されます。イメージごとに、イメージのコンテンツに基づいた固有の ID が付いています。これらのイメージは、展開後モードでレジストリからランタイム環境に取得されます。その後、本番環境のホスト上でコンテナインスタンスとして実行されます。

コンテナイメージのスキャン

コンテナイメージを展開する前後にスキャンして、脆弱性がないかどうかを調べることができます。展開前のフェーズでコンテナイメージがスキャンされると、すぐに対応する必要のない脆弱性アラートが多数表示される可能性があります。一方、展開後のフェーズで脆弱性をスキャンすると、次のような大きなメリットがあります。

- 展開したアプリケーションに関連するリスクが可視化される。
- 本番環境の画像のみにフォーカスしたビューが提供される。
- すぐに対処する必要がある脆弱性が特定され、優先順位が付く。
- イメージのメタデータに基づいて脆弱性がグループされ、アサインされる。たとえば、イメージリポジトリ、イメージラベル、およびコンテナイメージに関連するその他の属性を、グループ化やアサインルールに使用できる。

コンテナイメージにはそれぞれ、次の主要なコンポーネントがあります。

- コンテナまたはイメージリポジトリ：リポジトリがある、または名前がついている Docker イメージを表します。イメージのすべてのバージョンをホストします。
- Docker イメージ：特定のバージョンのビルドの Docker イメージを表します。
- Docker コンテナ：Docker イメージの実行中のインスタンスを表します。バージョンごとに固有の ID があり、本番環境で動いているコンテナの複数のインスタンスがあります。

コンテナ脆弱性対応 モジュール

コンテナ脆弱性対応 モジュールは、次の詳細を提供します。

コンテナ脆弱性一致アイテム

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

コンテナ脆弱性一致アイテム (CVIT) は、アサイン、重要度、エクスプロイト可能性、および修復ステータスに基づいてグループ化され、リストされます。

ライブラリ

脆弱性情報データベース (NVD) およびサードパーティのライブラリにアクセスします。NVD ライブラリは脆弱性一致アイテム ID に限定された情報を提供しますが、サードパーティのライブラリは脆弱性一致アイテムの詳細のほとんどを提供します。[NVD] 画面の情報は、NVD 統合がトリガーされた場合にのみ入力されます。

管理

[管理] モジュールは、脆弱性一致アイテムのアサインルール、修復ターゲットルール、およびコンテナ脆弱性統合に関する情報を提供します。さらに、脆弱性一致アイテムを自動クローズするまでの期間を設定することもできます。[VI の粒度の構成 (Configure VI Granularity)] セクションを使用して、キーの組み合わせを指定して CVIT の粒度を構成できます。デフォルトでは、CVIT はイメージリポジトリ、イメージタグ、および脆弱性の組み合わせに対して作成されます。キーにコンポーネントを追加して、さらに詳細に設定することができます。たとえば、イメージリポジトリ、イメージタグ、脆弱性、クラスターを組み合わせて CVIT を作成できます。

利用可能バージョン

リリースバージョン	リリースノート
コンテナ脆弱性対応 v2.1 コンテナ脆弱性対応 v2.06 コンテナ脆弱性対応 v2.0.4	Container Vulnerability Response リリースノート 互換性情報については、「KB0856498 Vulnerability Response 互換性マトリクスおよびリリーススキーマの変更」を参照してください。

自動翻訳

コンテナ脆弱性対応の修復タスクとコンテナ脆弱性一致アイテムのステータス

コンテナ脆弱性対応 アプリケーションでは、状況モデルを使用して、いつでも修復タスクのステータスを確認できます。各ステータスが互いにどのように関連し、影響を与えているかを知ることで、コンテナ脆弱性一致アイテム (CVIT) をいつどのように修正すればよいかを判断できます。

修復タスクステータス

複雑なユースケースでは、コンテナ脆弱性一致アイテムがその修復タスクとは異なるステータスになることがあります。状況の仕組みを理解すると、この動作を説明でき、修復タスクの作成や修復タスクルールの作成または編集に役立ちます。

次の図に示すように、修復タスクの想定される状況は数多くあります。

コンテナ脆弱性対応状況フロー

注:

- コンテナ脆弱性一致アイテムを手動で閉じることはできません。
- 各タスクフォームには、ServiceNow タスクの標準である [フォロー] および [更新] ボタンが含まれています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンテナ脆弱性対応 の構成

Now Platform インスタンスで コンテナ脆弱性対応 を実行する場合は、事前に構成する必要があります。

コンテナの脆弱性対応とコンフィグレーションコンプライアンス のインストール

Now Platform インスタンスで コンテナの脆弱性対応とコンフィグレーションコンプライアンス アプリケーションを実行する前に、エンタイトルメントを取得して、ServiceNow Storeからアプリケーションをダウンロードする必要があります。Now Platform インスタンスにアプリケーションをインストールし、セットアップアシスタントでいくつかのインストール手順を実行します。

始める前に

インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

セットアップタスク	説明
アプリケーションがインストールされ、有効化されていることを確認します。	アクティブ化されていることを確認するには、サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 アプリケーションがインストールも有効化もされていない場合は、「脆弱性対応 のインストール」を参照して下さい。
インスタンスに必要な ServiceNow ロールがアサインされていることを確認します。	インストールには admin ロールが必要です。 まだアサインされていない場合は、システム アドミニストレーター [admin] が脆弱性アドミン、sn_vul.vulnerability_admin または sn_vul.admin (非推奨) ロールもアサインします。

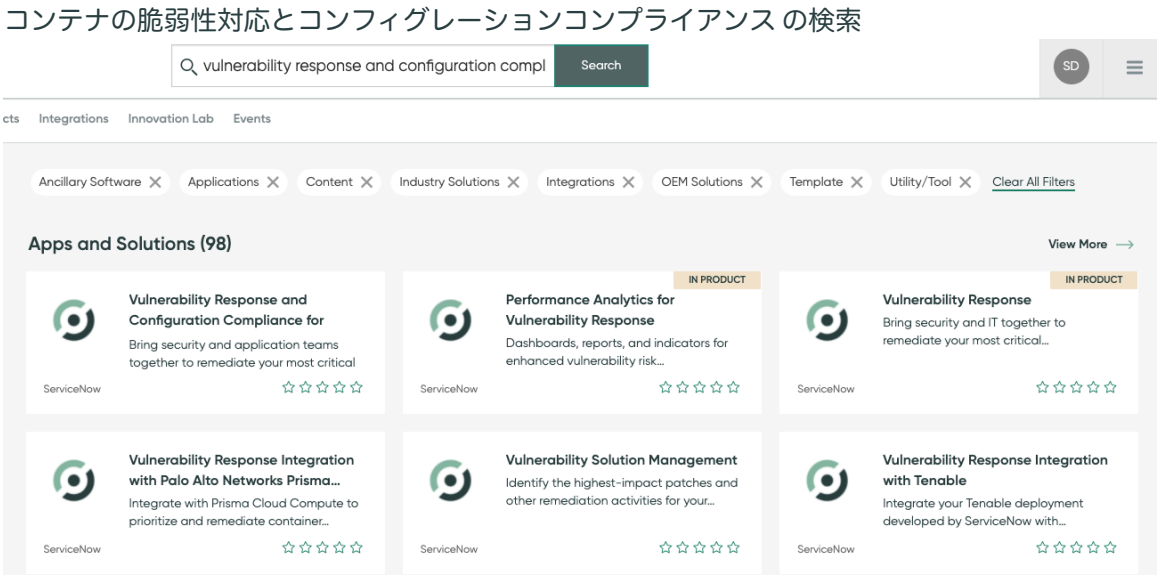
必要なロール：admin

手順

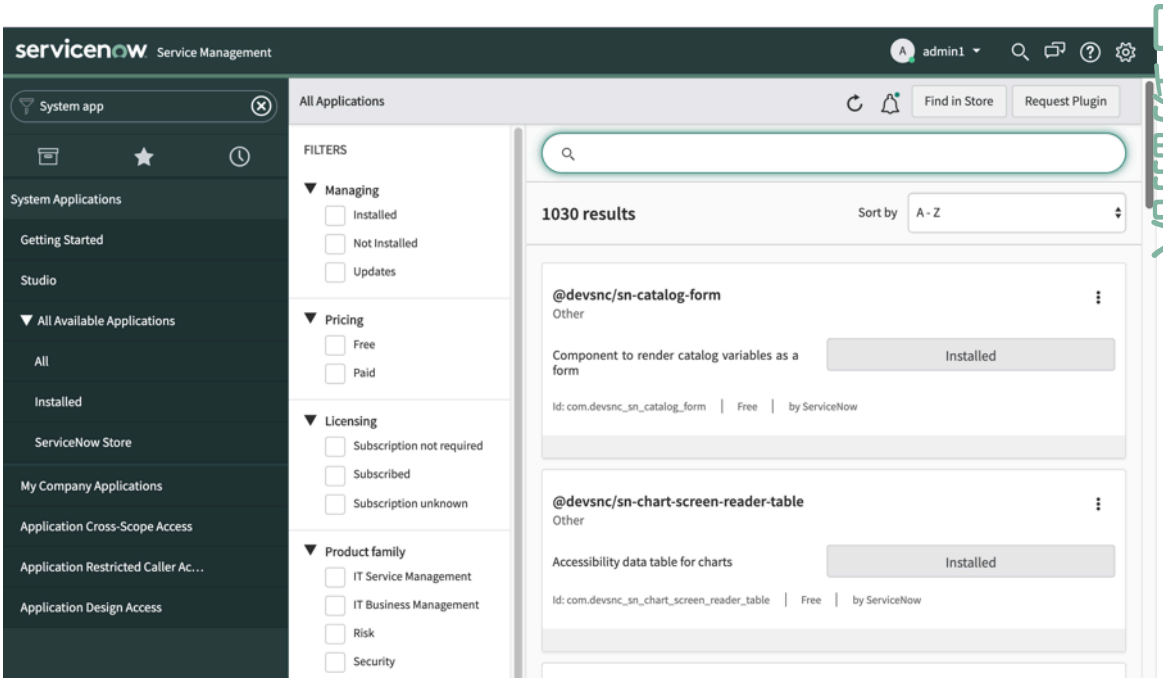
1. エンタイトルメントを取得して コンテナの脆弱性対応とコンフィグレーションコンプライアンス アプリケーションをダウンロードするには、ServiceNow Storeに移動します。
2. ページ右上にある [ログイン] をクリックします。
3. 検索バーに「コンテナの脆弱性対応とコンフィグレーションコンプライアンス」と入力します。
4. [アプリとソリューション] で、[コンテナの脆弱性対応とコンフィグレーションコンプライアンス] タイルをクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. [インストールを要求] をクリックします。
6. コンテナの脆弱性対応とコンフィグレーションコンプライアンス アプリケーションをインストールする Now Platform インスタンスにログインします。
7. 次のように移動する。 システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて).



8. リストされたアプリケーションから コンテナの脆弱性対応とコンフィグレーションコンプライアンス アプリケーションを見つけ、リストからバージョンを選択して、[インストール] をクリックします。
   [アプリケーションのインストール] ダイアログが表示されます。インストールされている依存関係がすべて表示されます。
9. [クローズ] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンテナ脆弱性対応 メール通知を定義する

メール通知を設定して、誤検出要求の承認や却下など、重要な更新やアクティビティに関する有用な情報を共有します。メール通知を作成するときに、送信時期、受信者、内容を指定できます。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > メールテンプレート.
2. **[New** (新規)] を選択します。

   メール通知を作成するための詳細な手順については、「Create an email notification」を参照してください。

タスクの結果
脆弱性対応 の v21.0 以降の場合、受信者がメール通知のリンクをクリックすると、そのロールに応じてレコードは Vulnerability Manager ワークスペース または IT 修復ワークスペース で開きます。

- ユーザーのロールが sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin の場合、Vulnerability Manager ワークスペースでリンクが開きます。
- ユーザーのロールが sn_vul_container.remediation_owner の場合、IT 修復ワークスペースでリンクが開きます。

受信者に前述のいずれのロールもない場合は、メール通知のリンクがクラシック UI で開きます。

修復ターゲット通知の作成または編集

脆弱性アドミニストレーターは、修復ターゲット通知を編集するか、新しい通知を追加して、通知の送信タイミング、通知の受信者、通知の内容を指定できます。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 通知.
2. 修復ターゲットの通知レコードを選択するか、[新規] を選択します。
3. 必要に応じて、フォームのフィールドに入力します。
   フォームフィールドの詳細については、「Create an email notification」を参照してください。
4. [通知をプレビュー] を選択してメッセージを表示します。

タスクの結果
脆弱性対応 の v21.0 以降の場合、受信者がメール通知のリンクをクリックすると、そのロールに応じてレコードは Vulnerability Manager ワークスペース または IT 修復ワークスペース で開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ユーザーのロールが sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin の場合、Vulnerability Manager ワークスペースでリンクが開きます。
- ユーザーのロールが sn_vul_container.remediation_owner の場合、IT 修復ワークスペースでリンクが開きます。

受信者に前述のいずれのロールもない場合は、メール通知のリンクがクラシック UI で開きます。

コンテナ脆弱性対応 の例外管理の設定

コンテナ脆弱性対応 モジュールを使用して、要求された例外の期間を制限し、例外要求または誤検出要求にアンケートを追加します。デフォルトでは、 ServiceNow コンテナ脆弱性対応 モジュールを使用して例外が要求されます。GRC: ポリシーとコンプライアンス管理 の統合を使用して例外を要求することもできます。

始める前に
必要なロール：sn_vul_container.manage_exception_configuration

このタスクについて
コンテナ脆弱性対応 が有効であれば、例外を要求できる期間を制限できます。同様に、GRC: ポリシーとコンプライアンス管理 モジュールがインストールされていれば、構成画面で GRC: ポリシーとコンプライアンス管理 を選択できます。このオプションを有効にすると、GRC からポリシーおよびコントロール目標を指定する例外を要求できます。

アンケートを追加すると、例外要求または誤検出要求を出しているユーザーにアンケートが送信されます。デフォルトのアンケートを使用することも、要件に基づいて作成することも可能です。。

アンケートは、例外が要求されている理由を例外承認者が理解する際に役立ちます。

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > アドミニストレーション > 例外管理.
2. [例外管理構成] フォームで、[例外の管理に使用] リストからオプションを選択して、例外を管理する方法を選択します。
   脆弱性対応 または GRC: ポリシーとコンプライアンス管理 のいずれかを選択できます。
3. 脆弱性対応 オプションを選択した場合は、次の情報を入力します。

脆弱性対応 フィールド

フィールド	説明
期間	例外を要求できる期間。
単位	指定された期間の時間単位。
誤検出をマークするアンケートを有効化	上がっている誤検出要求にアンケートを追加するオプション。
例外を要求するアンケートを有効化	上がっている例外要求にアンケートを追加するオプション。
例外を要求するアンケート	例外を要求するために自分が選択したアンケートを表示します。デフォルトでは、[例外のアンケート] が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
GRC: ポリシーとコンプライアンス管理 を選択すると、ガバナンス、リスク、コンプライアンス がそのフローを処理するため、 [期間] および [単位] フィールドが表示されなくなります。

4. [保存] を選択します。

例外管理の承認ルールの構成

脆弱性対応 v15.0 以降では、フローデザイナーを使用して、例外管理、例外ルール、および誤検出管理の例外要求を承認します。脆弱性対応 (VR) を初めて展開した場合、フローデザイナーはデフォルトで有効になっています。

始める前に
必要なロール：sn_vul.vulnerability_admin

このタスクについて
フローデザイナーを使用するには、 承認ルールモジュールを使用してルールを作成します。このモジュールを使用すると、以下の各例外管理ワークフローの承認ルールを構成できます。

- 修復タスクの要求例外
- コンテナの脆弱性一致アイテムの例外要求
- 例外ルール
- 修復タスクの誤検出
- コンテナの脆弱性一致アイテムの誤検出

ルール内に複数の承認レベルを含む条件を定義することもできます。フローデザイナーは、このモジュールで作成されたルールを自動的に継承し、一致する承認ワークフローを処理します。

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > アドミニストレーション > 承認ルール.
2. [承認ルール] ページで、承認ルールを設定するグループを選択します。
3. フォームのフィールドに入力します。

承認ルールフォーム

フィールド	説明
名前	承認構成名。
テーブル	ルールが適用されるテーブル。
アプリケーション	デフォルト値は脆弱性対応です。
ルールタイプ	ルールタイプを指定します。たとえば、例外管理、誤検出、例外ルールなどです。
有効	デフォルトで有効になっており、承認ルールが使用中であることを示します。
説明	承認ルールの簡単な説明。
承認の有効期限 (日数)	承認者が要求を承認できる期限。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
コンテナ脆弱性対応の v2.5 以降	
承認者に通知 (日数) コンテナ脆弱性対応の v2.5 以降	承認者にアクションを実行するよう通知される日付。

4. [更新] を選択します。
[承認構成] タブには、デフォルトで 2 つのレベルの承認者が設定されています。ルールを選択して、ルール内のさまざまなユースケースに基づいて条件を定義できます。詳細については、「承認ルールの構成の作成」を参照してください。

> **注:**
> 各構成ページで、複数の承認レベルを作成できます。詳細については、「例外管理の承認レベルの作成」を参照してください。

Example:
さまざまなユースケースに基づいて、異なる構成アイテムで見つかった同じ脆弱性に対して、異なる承認プロセスを定義できます。

コンテナ脆弱性対応のクイックスタートテスト

アプリケーションの開発やアップグレードの適用などの構成変更を行った後も、コンテナ脆弱性対応が変わらず正常に動作するかを検証します。自分のインスタンスに固有のデータを使用するときは、それが成功するように、これらのクイックスタートテストをコピーしてカスタマイズします。

本番システムでテストを実行できないようにするために、テスト実行プロパティはデフォルトでは無効になっています。開発、テスト、およびその他の非本番インスタンスでのみテストを実行してください。デモデータやデモアカウントが作成されている場合は、非本番環境または本番環境でインスタンスを使用する前に、すべてのデモデータを削除する必要があります。コンテナ脆弱性対応 のテストスイートの設定と実行の詳細については、「脆弱性対応 の自動テストフレームワーク (ATF) テストスイートの実行」を参照してください。

コンテナ脆弱性対応 クイックスタートテストでは、コンテナ脆弱性対応 アプリケーション (sn_vul_container) をアクティブ化する必要があります。

コンテナ脆弱性対応 テスト

テスト	説明	リリースバージョン
CVR：アサインルール	アサインルールのサンプルセットがコンテナ脆弱性一致アイテムをアサイン先グループに自動アサインして修復できるかどうかを確認します。	Vancouver
CVR：例外ルール	例外ルールをテストします。	Vancouver
CVR：誤検出フローとしてマーク	誤検出としてマークするフローがコンテナ脆弱性一致アイテムで機能しているかどうかをテストします。	Vancouver
CVR：修復ターゲットルール	修正ターゲットルールを作成します。	Vancouver

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンテナ脆弱性対応 テスト (続く)

テスト	説明	リリースバージョン
CVR：例外要求フロー	例外要求フローが期待どおりに機能しているかどうかをテストします。	Vancouver
CVR：脆弱性算出	コンテナ脆弱性算出をテストします。	Vancouver

関連情報

クイックスタートテスト

コンテナ脆弱性対応 の自動テストフレームワーク **(ATF)** テストスイートの実行

コンテナ脆弱性対応 アプリケーションをインストールまたはアップグレードした後に、自動テストフレームワーク (ATF) テストスイートを実行します。

始める前に
正常にインストールされ、インスタンスが設計どおりに機能することを確認します。

本番システムでテストを実行できないようにするために、テスト実行プロパティはデフォルトでは無効になっています。開発、テスト、およびその他の非本番インスタンスでのみテストを実行してください。デモデータやデモアカウントが作成されている場合は、非本番環境または本番環境でインスタンスを使用する前に、すべてのデモデータを削除する必要があります。

- テストを有効にするには、次の手順を実行します。
  1. 次のように移動する。 **All** (すべて) > 自動テストフレームワーク **(ATF)** > アドミニストレーション > プロパティ.
  2. [テスト/テストスイートの実行を有効にする] チェックボックスがオンになっていない場合は、オンにします。
  3. [保存] をクリックします。
  4. ヘッダーでスコープが [コンテナ **Vulnerability Response]** に設定されていないか、ヘッダーにスコープが表示されていない場合は、設定アイコンをクリックします。
  5. [システムの設定] ウィンドウで、[開発者] をクリックします。
  6. 選択されていない場合は、[ヘッダーにアプリケーションピッカーを表示 **(Show application picker in header)]** をクリックしてウィンドウを閉じます。
  7. [システムアドミニストレーター] の横に表示されるリストで、フィールドの [コンテナ **Vulnerability Response]** をクリックします。

必要なロール：admin または atf_test_admin

手順

1. 次のように移動する。 **All** (すべて) > 自動テストフレームワーク **(ATF)** > テスト.
2. [パッケージ] リストでコンテナ用 **Vulnerability Response** および **Configuration Compliance** を見つけます。
3. テストを選択してレコードを開きます。
4. 開いたレコードで、[アクティブ] チェックボックスをオンにします。
5. [テストステップ] 関連リストの [アクティブ] 列で [true] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [更新] をクリックします。
7. テストをもう一度開き、「ここからテストおよびテストスイートの実行を有効にしてください **(Enable tests and test suite execution here)**」をクリックします。
8. [テストおよびテストスイートプロパティ (Test/ Test Suite Properties)] と [テストデバッグプロパティ] を有効にします。
9. [保存] をクリックします。
10. [テストを実行] ボタンが表示されない場合は、画面をリフレッシュしてレコードを再度開き、[テストを実行] をクリックしてテストを開始します。
しばらくすると、[テストを実行] ダイアログにテストの成功が表示されます。詳細については、[結果に移動] をクリックしてください。

次のタスク
おめでとうございます!コンテナ脆弱性対応 の構成を続行できます。

コンテナ脆弱性対応 の自動テスト、自動テスト、テストスイート、および自動テストの作成の詳細については、「自動テストフレームワーク (ATF)」を参照してください。

他のアプリケーションとの コンテナ脆弱性対応 の統合

他のアプリケーションと統合することで コンテナ脆弱性対応 の機能を拡張します。

コンテナ脆弱性対応 はコンテナセキュリティ製品と統合して、ランタイムに展開されるイメージの脆弱性データをプルします。次に、ランタイムコンテキスト情報 (これらのコンテナイメージが展開されているホスト、Kubernetes クラスター、サービス、名前空間など)によって脆弱性データを拡張します。ServiceNow の Kubernetes 検出を使用すると、脆弱性から関連する Kubernetes エンティティに対して作成された参照を 構成管理データベース (CMDB)で確認できます。ServiceNow は、メタデータの拡張の他に、脆弱性と修復の傾向に関するインサイトを示す包括的なレポートダッシュボードも提供します。

コンテナ脆弱性対応 は、次のアプリケーションとの統合を提供します。

- Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute の統合
- Atlassian Jira と 脆弱性対応 の統合の概要

> **重要:**
> 脆弱性マネージャーワークスペースでは、リストアクションとフォームアクションを使用してアジャイルの問題を手動で作成し、CVIT と RT の修復を追跡できます。

統合に関するその他の注意事項

統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信エラーを回避するために、コンテナ脆弱性対応 バージョン 2.1.2 以降では、キューがアクティブでデータを処理中であるかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute の統合

Prisma Cloud Compute 統合を使用すると、コンテナイメージをスキャンして脆弱性を検出できます。

脆弱性対応 のバージョン 23.0 以降では、コンテナ脆弱性対応 アプリケーションのVulnerability Response Integration with Palo Alto Networks Prisma Cloud Computeを使用して、実行中のホストに脆弱性をインポートできます。Prisma ホスト API を使用すると、特定のホストの包括的な脆弱性情報を取得でき、特定の時点でのホスト脆弱性のスナップショットも提供します。この API を使用すると、Prisma と ServiceNow インスタンス間の定期的な同期が可能になります。Prisma は Software as a Service (SaaS) とオンプレミスソリューションの両方として提供されるため、ServiceNow インスタンスから Prisma API を呼び出すには MID サーバーを使用する必要があります。

脆弱性対応 のバージョン 16.1 以降では、コンテナ脆弱性対応 アプリケーションの Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute を使用して、展開されたコンテナのコンテナイメージ脆弱性データをインポートできます。そうすると、脆弱性対応 ダッシュボードで脆弱性と脆弱性一致アイテムに関するレポートを表示できます。また、これらの脆弱性に優先順位を付けて修正することができます。

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 製品と Now Platform インスタンスが同じ環境にない場合は、MID サーバーを使用する必要があります。詳細については、「MID Server system requirements (MID サーバーのシステム要件)」を参照してください。

統合の表示

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute の一部である統合を表示できます。統合を表示するには、次に移動します: **All** (すべて) > **Prisma Cloud Compute** 統合 > 統合.

次の統合を使用できます。

実行シーケンス	スケジュール	統合	説明
1	日次	Prisma Cloud Compute 基本イメージ統合	Prisma API から基本イメージの脆弱性を取得し、基本イメージの脆弱性を個別にレポートします。また、基本イメージをポイントするイメージの検出結果と脆弱性一致アイテムも作成されます。
2	日次	Prisma Cloud Compute 脆弱性統合	コンテナ脆弱性を取得します。検索結果とコンテナ脆弱性一致アイテム (CVIT) および検出されたコンテナイメージを作成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

実行シーケンス	スケジュール	統合	説明
3	オンデマンド	Prisma Cloud Compute コンテナ数統合	各非基本イメージのコンテナ数を取得します。
4	日次	Prisma Cloud Compute レジストリ統合	Prisma レジストリスキャンから取得された静的イメージの検出結果を取得し、 コンテナ脆弱性対応に取り込みます。

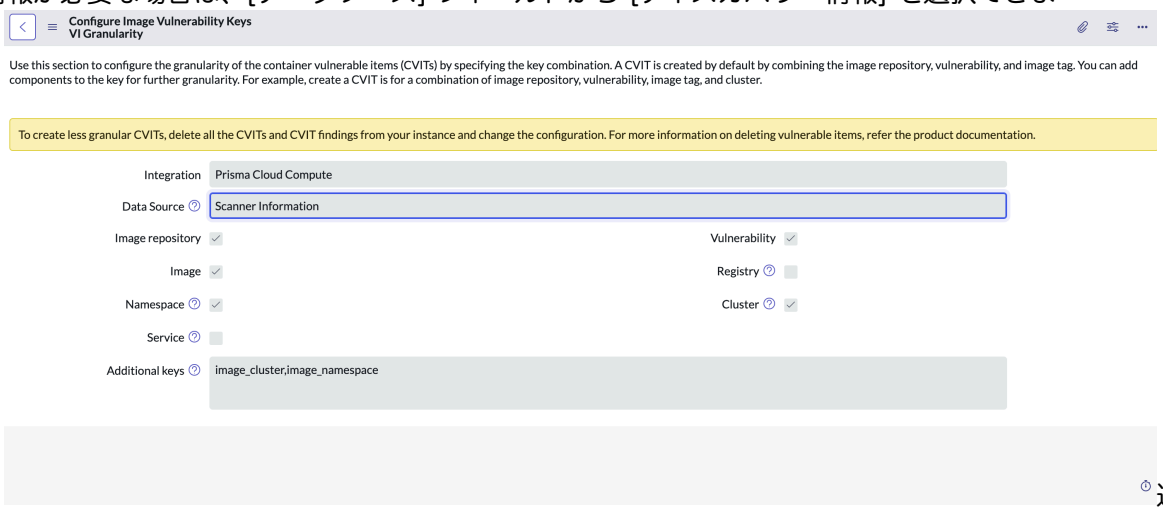
Prisma の基本イメージ構成

Prisma コンソールでは、レジストリを構成し、それらのレジストリから基本イメージを構成できます。基本イメージに脆弱性が存在する場合、Prisma Cloud Compute 基本イメージ統合を実行すると、[基本イメージ] チェックボックスがオンになり、基本イメージに脆弱性が存在することが示されます。

CVR ベースの VI 粒度の構成

CVIT の粒度を設定するには、次に移動します: **All** (すべて) > **Prisma Cloud Compute** 統合 > **CVR** ベース **VI** の粒度の構成 をクリックし、キーの組み合わせを指定します。デフォルトでは、CVIT はイメージリポジトリ、イメージ、および脆弱性の組み合わせに対して作成されます。キーにコンポーネントを追加して、さらに詳細に設定することができます。たとえば、イメージリポジトリ、イメージ、脆弱性、クラスターを組み合わせて CVIT を作成できます。

コンテナ脆弱性対応 の v2.12.1 以降では、レジストリ情報とデータソースを使用して、コンテナ脆弱性一致アイテム (CVIT) の粒度を設定することもできます。名前空間とクラスターの情報は、スキャナーと ディスカバリーの両方から受信されます。ディスカバリーからのみこの情報が必要な場合は、[データソース] フィールドから [ディスカバリー情報] を選択できます。

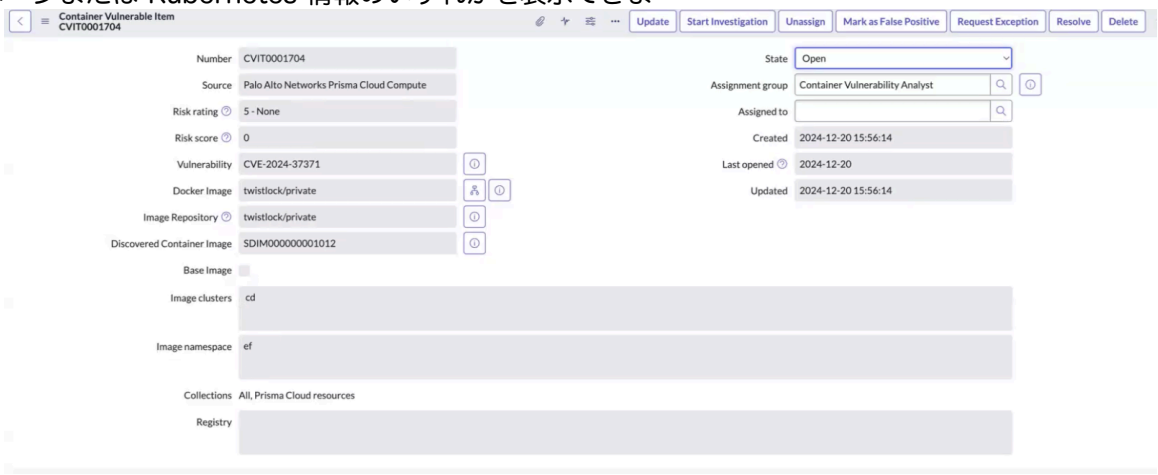


選択したデータソースに応じて、CVIT レコードに関連する

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

イメージまたは Kubernetes 情報のいずれかを表示できま



す。

[スキャナー情報] を選択すると、CVIT レコードに [イメージクラスター] フィールドと [イメージ名前空間] フィールドが表示されます。

ディスカバリー情報が選択されている場合、CVIT レコードには **Kubernetes** クラスターと **Kubernetes** 名前空間フィールドが表示されます。

Prisma 統合プロセス

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute が実行されると、脆弱性情報データベース (NVD) テーブルに共通脆弱性識別子 (CVE) が存在するかどうかが確認されます。既に存在する場合は、既存の情報が使用されます。ただし、CVE が見つからない場合は、プレースホルダーレコードが NVD テーブルに生成されます。これらのプレースホルダー NVD レコードを作成すると、最初は CVE とその名前のみが入力されます。その他の詳細は、入力されません。NVD 統合によって後で入力されることを前提としているためです。統合インスタンスパラメーター *update_nvd* が true に設定されている場合、プレースホルダーの NVD レコードが更新されます。デフォルトでは、インスタンスパラメーターは false に設定されています。ただし、少なくとも NVD 統合が実行されてこれらの詳細が入力されるまでは、重大度や問題に関するその他の詳細など、CVE についてある程度理解する必要があります。この要件を満たすために、[エクスプロイト有無] フィールドと [修復メモ] フィールドには、Prisma から取得した詳細が入力されます。さらに、この構成はカスタマイズ可能であり、Prisma によって提供される情報に基づいて NVD エントリを他のフィールドに入力するよう指定できます。

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute の準備

次のセットアップタスクを実行して、Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute を準備できます。

事前準備

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute アプリケーションをインストールして設定するには、次のチェックリストを印刷してください。アプリケーションをインストールして脆弱性データを Now Platform インスタンスにインポートする前に、リストされている項目が完了していることを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統合準備チェックリスト

タスク	説明
☐	次の情報セットがあることを確認します。 • API ベース URL • ユーザー名とパスワード これらの認証情報は、Prisma Cloud Compute 統合から脆弱性をプルするために使用されます。詳細については、「https://pan.dev/compute/api/」を参照してください。 注: MID サーバーはオプションです。 Prisma Cloud Compute 統合に使用されるユーザー認証情報には、画像を監視するための権限が必要です。次のコードを参照してください。 `{"permission":"monitorImages","saas":true,"self-hosted":true}`
☐	まだインストールしてアクティブ化していない場合は、サードパーティアプリケーションをインストールする前に 脆弱性対応 アプリケーションをインストールします。 脆弱性対応 アプリケーションのインストールとアクティブ化の詳細については、「脆弱性対応 のインストール」を参照してください。この統合には、脆弱性対応 のバージョン 16.1 以降が必要です。
☐	エンタイトルメントを取得して、Vulnerability Response Integration with Palo Alto®Networks Prisma Cloud Compute アプリケーションを Now Platform インスタンスにダウンロードします。
☐	インポートする予定の脆弱性一致アイテムの数を見積もります。 インポートする予定の脆弱性一致アイテムの数をインスタンスが受け入れることができることを確認します。インスタンスが小さすぎると、ロードに時間がかかることがあります。インスタンスのサイズがわからない場合、またはサポートが必要な場合は、ServiceNow テクニカルサポートにお問い合わせください。
☐	統合を管理し、脆弱性一致アイテムを修正する次のグループまたはユーザーがいることを確認します。 admin Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute アプリケーションをインストールします。アサインされていない場合、アドミニストレーターはコンテナ脆弱性アドミン (sn_vul_container.vulnerability_admin) およびその他のロールをアサインします。 sn_vul_container.vulnerability_admin Prisma Cloud Compute 統合の構成を完了します。このロールは、コンテナ脆弱性対応 (CVR) アプリケーションとそのレコードに完全にアクセスできます。このアドミニスト

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統合準備チェックリスト (続く)

タスク	説明
	レーターは、コンテナ脆弱性対応 で統合とルールを設定します。 脆弱性対応グループ デフォルトで脆弱性対応グループは利用可能になっています。脆弱性対応グループにアサインされたユーザーは sn_vul.read_all、sn_vul_container.read_all を継承します。 コンテナ修復オーナーグループ デフォルトでは、コンテナ修復オーナーグループが利用可能です。このグループにアサインされたユーザーは、sn_vul_container.remediation_owner を継承します。コンテナ修復オーナーは、自分または所属するグループにアサインされたコンテナの脆弱性を修復します。 脆弱性アナリスト コンテナ脆弱性アナリストグループにアサインされたユーザーは、sn_vul.vulnerability_analyst を継承します。脆弱性アナリストは、すべての脆弱性一致アイテムの修復を監視します。 まだ作成されていない場合は、追加のグループを作成して、ユーザー管理モジュールでインスタンスにユーザーを追加することをお勧めします。詳細については、「ユーザーグループの作成」を参照してください。
☐	脆弱性対応 Integration with NVD をインストールし、NIST National Vulnerability Database Integration - API (CVE のみ) を実行します。

これで、「Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute アプリケーションの構成」に進む準備が整いました。

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute をインストールする

インスタンスで統合を実行する前に、インストールと構成の手順を完了して、Prisma Cloud Compute 製品が 脆弱性対応 および コンテナ脆弱性対応 と適切に統合されるようにします。このアプリケーションは別のサブスクリプションとして利用できます。

始める前に
インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

必要なロール：admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute をインストールするインスタンスにログインします。
2. ServiceNow Store に移動します。
3. ServiceNow Store で、Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute アプリケーションを検索します。
4. アプリケーションタイルをクリックします。
   インストールしているアプリケーションに関する詳細情報が表示されます。

   注:
   必要に応じて、「その他の要件」および「依存関係」のセクションをお読みください。

5. [アプリを要求] をクリックし、Now Support ログイン認証情報を入力します。
6. [取得] をクリックします。
7. [インスタンス名] フィールドと [インスタンスの理由] フィールドを更新し、[インスタンスを検証] をクリックします。
8. [要求] をクリックします。
   詳細なインストール手順が記載されたメールが届きます。
9. 次のように移動する。 システムアプリケーション > アプリケーション.
10. アプリケーションを見つけて選択し、[インストール] をクリックします。

タスクの結果
アプリケーションはインスタンスに自動でインストールされます。

次のタスク
環境に Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute を構成します。「Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute アプリケーションの構成」を参照してください。

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute アプリケーションの構成

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute アプリケーションをインストールして構成します。Prisma Cloud Compute からデータをインポートします。インポートされたデータを使用して、Docker イメージとホストの脆弱性に優先順位を付けて修正できます。

始める前に
必要なロール：admin

手順

1. 統合に関する ServiceNow からのメールを開きます。
2. アドミニストレーターとしてインスタンスにログインします。
3. メールの指示に従って Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute を取得します。
4. 次のように移動する。 **All** (すべて) > **Prisma Cloud Compute** 統合 > アドミニストレーション > 構成.
   Prisma Cloud Compute 構成フォームの各フィールドに記入します。詳細については、「Prisma Cloud Compute の構成フォーム」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. [プロジェクト] リストから、[すべてのプロジェクト] または [特定のプロジェクト **(Specific Projects)]** のいずれかを選択して、すべてのプロジェクトまたは選択したプロジェクトをそれぞれ構成します。
   [特定のプロジェクト **(Specific Projects)]** を選択すると、[利用可能] リストからプロジェクトを選択できます。
6. [完了] または [認証情報を保存してテスト] を選択して、構成を完了します。
   - プロジェクトを構成した場合は、[完了] を選択します。
   - プロジェクトを構成していない場合は、[認証情報を保存してテスト] を選択します
7. 次に移動して新しく作成されたインスタンスを表示します。 **Prisma Cloud Compute** 統合 > アドミニストレーション > 統合インスタンス.
8. [統合インスタンスパラメーター] を選択して、以前に構成したプロジェクトを表示します。
9. 新しく作成された統合インスタンスを実行して、次のデータをインポートします。
   - Docker イメージ：識別および調整エンジン (IRE) を使用して作成された Docker イメージを一覧表示します。各 Docker イメージは、リポジトリとインストールされているバージョンの関係に関する情報も提供します。
   - 検出されたコンテナイメージ：検出されたコンテナイメージのモジュールは、イメージ ID、Docker イメージ、およびイメージリポジトリに関する情報を提供します。また、レイヤー情報も保存し、検出されたイメージに関連付けます。ここでは、プロジェクトとコンテナ数を表示することもできます。検出されたコンテナイメージについては、クラウドプロバイダー、クラウドリージョン、クラウドアカウント ID、クラウドリソース ID などのクラウドメタデータを表示できます。
   - コンテナイメージパッケージ：脆弱性が存在するパッケージに関する情報を提供します。バイナリパッケージの詳細もカンマ区切り値として提供されます。
   - コンテナイメージレイヤー：この画面には、各イメージレイヤーのレコードが表示されます。
   - コンテナイメージの検索：この画面には、関連する脆弱性、イメージレイヤー、Docker イメージ、イメージリポジトリ、および検出されたイメージに関する情報とともに検出結果のリストが表示されます。現在、脆弱性情報は ID のみに制限されています。脆弱性情報データベース (NVD) 統合がトリガーされると、追加情報が入力されます。
   - コンテナ脆弱性一致アイテム：各検出結果には対応する脆弱性があります。粒度に基づいて CVIT がさらに作成されます。
10. 脆弱性一致アイテムの粒度を構成します。

    a. 次のように移動する。 **All** (すべて) > **Prisma Cloud Compute** 統合 > イメージ脆弱性キーを構成

    b. 必要なチェックボックスをオンにして、CVIT の粒度を構成します。
    脆弱性一致アイテムは、次回のインポート時に選択したキーに基づいて作成されます。

    > **注:**
    > デフォルトでは、CVIT はイメージリポジトリ、脆弱性、およびイメージタグの組み合わせに対して作成されます。キーにコンポーネントを追加して、さらに詳細に設定することができます。たとえば、イメージリポジトリ、脆弱性、イメージタグ、クラスターの組み合わせに対して CVIT を作成できます。脆弱性一致アイテムまたは脆弱性一致アイテムの検出結果が作成されると、チェックボックスは編集できなくなります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンテナの脆弱性の修正

修復の監視は、ステータスの確認で始まり、コンテナ脆弱性一致アイテム (CVIT) のクロージングで終わるプロセスです。コンテナ脆弱性対応 は、そのプロセスをより生産的かつ効率的に行うたのツールと手順を提供します。

コンテナ脆弱性対応 の算出ルール

脆弱性算出は、コンテナ脆弱性一致アイテムのフィールドの初期値の計算を自動化します。各算出の条件が順番に評価され、最初に一致した算出が使用されます。

脆弱性算出を表示および作成するには、次に移動します: **All** (すべて) > **Container Vulnerability Response** > アドミニストレーション > 脆弱性の算出.

コンテナ脆弱性対応 ベースシステムには、コンテナ脆弱性一致アイテムのベースリスクスコアを設定する 2 つの脆弱性算出が含まれています。ベースシステムで使用できる算出グループは次のとおりです。

- 脆弱性重大度：正規化された脆弱性重大度を使用して、脆弱性一致アイテムのリスクスコアを計算します。
- デフォルトのリスク計算機：リスクルールに基づいて算出されます。

注:
コンテナ脆弱性対応 のバージョン 2.10 以降の場合：

- [デフォルトのリスク計算機] ルール：コンテナ脆弱性一致アイテム (CVIT) のリスクスコアが変更されるたびに、CVIT の [メモ] セクションに次の詳細が文書化されます。
  - 算出グループ名
  - 算出名：
  - 1 より大きい重み付けを持つフィールド値とそのリスクスコアの寄与度。
  - 最終的なリスクスコア
- [脆弱性重大度] リスクルール：CVIT のリスクスコアが更新されるたびに、[メモ] セクションが次の詳細で更新されます。
  - 算出グループ名
  - 算出名：算出ルールがテンプレートとスクリプトのどちらに基づいているかに応じて、名前に括弧で囲まれた詳細が追加されます。算出ルールの基準を変更または表示するには、任意のルールを選択し、[詳細表示] チェックボックスをオンにします。[値のタイプ **(Value type)]** ドロップダウンボックスから、必要なオプションを選択します。[テンプレート] を選択した場合、リスクスコアはルールで指定された条件に従って更新されます。[スクリプト] を選択した場合、既存のスクリプトを追加または更新できます。システムプロパティ *`sn_sec_cmn.risk_score_changes_add_worknotes`* は、作業メモセクションへの入力に役立ちます。コンテナ脆弱性対応 v2.12.2 以降、システムプロパティ*`sn_sec_cmn.risk_score_changes_add_worknotes`*はデフォルトで無効になっています。これを有効にした場合にのみ、コンテナ脆弱性一致アイテムのリスクスコアに関連するすべての変更が [作業メモ] セクションに表示されます。また、作業メモは、リスクスコアに変更がある場合にのみ更新されます。

脆弱性のリスクスコアの重み付け

すべての脆弱性には、重大度、重要度、エクスプロイト情報などの要素に基づいてリスクスコアと評価がアサインされます。このリスク評価の算出を担当するのが、コンテナ脆弱性一致アイテムのテーブルのビジネスルール *`Update Risk Rating from Risk Score`* です。リスクスコアが変更されるたびに、コンテナ脆弱性一致アイテムのリスク評価が算出されて入力されます。脆弱性対応

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

(VR) アプリケーションのバージョン 17.1 より前では、次のリスク評価がスクリプトインクルード VulnerabilityUtils の一部として提供され、ハードコードされていました。

値 (リスク評価)	重み付け (リスクスコア)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

脆弱性対応 のバージョン 18.0 以降では、

- リスク評価タイプは、ベーステーブルであるリスクスコアの重み付け [sn_sec_cmn_risk_scorew_weights] に cvr_risk_rating として含まれています。リスク評価タイプは、リスク評価が計算される各テーブルのビジネスルールまたはスクリプトインクルードの一部として渡されます。
- リスク評価の算出の対象となる [リスクスコアの重み付け] テーブルの値をクエリできるように、スクリプトが変更されます。
- 既存のタイプにエントリを追加するか、新しいタイプを作成します。新しいタイプを作成するときは、新しいリスク評価のラベルを追加し、関連するスクリプトとビジネスルールも変更してください。新しいリスクスコアのスタイルも新たに追加する必要があります。
- ベーステーブルのレコードをクエリするようにスクリプトを変更します。

[リスクスコアの重み付け] テーブルにアクセスするには、フィルターナビゲーターに「sn_sec_cmn_risk_score_weight」と入力します。

さらに、次のシナリオではリスクスコアが自動的に再計算されます。

- 構成アイテム (CI) が非インターネットフェーシングからインターネットフェーシングに変更されたとき。
- 脆弱性一致アイテム (VI) の関連する一般的な脆弱性とエクスポージャー (CVE) またはサードパーティエントリ (TPE) が、CVE の既知の悪用された脆弱性 (KEV) にリンクされている場合。

詳細については、「脆弱性対応 の算出と脆弱性算出ルール」を参照してください。

コンテナ脆弱性対応 のアサインルール

コンテナ脆弱性一致アイテム (CVIT) が修復のためにアサイン先グループに自動的にアサインされる基準を定義します。

コンテナ脆弱性一致アイテムのアサインルールを作成および表示するには、次の手順に従います。次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > アドミニストレーション > アサインルール. アサインルールの作成時に、条件を設定できます。設定した条件が満たされると、選択したユーザーグループに、ルールによってコンテナ脆弱性一致アイテムが自動的にアサインされます。一致条件を備えた最初のアサインルールのみがレコードに対して実行されます。

注:
ステータスが [オープン] ではないコンテナ脆弱性アイテム、または手動でアサインされたコンテナ脆弱性一致アイテムは、常に除外されます。

詳細については、「脆弱性対応 アサインルールの概要」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **重要:**
> 脆弱性アドミンおよびアナリストは、Vulnerability Manager ワークスペースで選択した CVIT の最新のアサインを取得できます。この方法は、クラシック UI ですべての CVIT にアサインルールを再適用する時間のかかるプロセスよりも効率的です。詳細については、「Vulnerability Manager ワークスペース でレコードの修復プロパティを再評価」を参照してください。

コンテナ脆弱性対応 の修復ターゲットルール

修復ターゲットルールは、コンテナ脆弱性一致アイテム (CVIT) を修復するための予定期間を定義するものです。このルールは、SLA が脆弱性自体を修正するための期間を指定する方法に類似しています。

コンテナ脆弱性の修復ターゲットルールを作成して表示するには、次に移動します: **All** (すべて) > **Container Vulnerability Response** > アドミニストレーション > 修復ターゲットルール.

修復ターゲットルールで、選択したコンテナ脆弱性一致アイテム (CVIT) の予定修復期間を定義します。修復にかける日数を選択して、脆弱性の修復期限を設定します。修復のリマインダーを設定し、ルールを適用するコンテナ脆弱性一致アイテムを設定します。脆弱性の修復を完了すべき日数の修復ターゲットを設定して、ターゲットの日が近づく前にリマインダーが届くように設定することもできます。詳細については、「脆弱性対応 の修復ターゲットルール」を参照してください。

> **重要:**
> 脆弱性アドミンおよびアナリストは、Vulnerability Manager ワークスペースで選択した CVIT の最新の修復ターゲット日を取得できます。この方法は、クラシック UI ですべての CVIT に修復ターゲットルールを実行する時間のかかるプロセスよりも効率的です。詳細については、「Vulnerability Manager ワークスペース でレコードの修復プロパティを再評価」を参照してください。

コンテナ脆弱性対応 の例外管理

公開されている脆弱性管理やセキュリティポリシー、標準、指針に組織が準拠できない場合は、例外を要求できます。例外管理では、ポリシーに従って修復できないコンテナ脆弱性一致アイテム (CVIT) に対する例外を要求、レビュー、承認、または却下します。

コンテナ脆弱性 (CVIT) によっては、既存のパッチ、修正、またはソリューションがないこともあります。例外が承認されるということは、脆弱性を修復しなかった場合の結果を認識し、同意していることになるため、リスクを受け入れているということでもあるのです。

例外のライフサイクル

例外の定義

例外は、CVIT または RT の修復を指定した期間保留することを要求するものです。たとえば、修復オーナーは、マシンにパッチが適用できない場合に例外を要求できます。

例外の要求

修復オーナーは、例外管理プロセスを使用して、CVIT または RT の免除を要求できます。例外承認者がこの要求を承認すると、CVIT または RT は [保留] ステータスに移行します。

例外要求を承認する

すぐに修復できない CVIT または RT は、脆弱性アナリストによってレビューされ、リスクが評価され、修復できるまでの保留が承認されます。例外要求の承認は 2 レベルワークフローにすることができます。第 1 レベルの承認者のみが存在する場合、例外を要求して承認できます。ただし、第 1 レベルの承認者がいない場合は、例外を要求できません。詳細については、「例外承認者の追加」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

脆弱性対応 v15.0 以降では、VR アプリケーションを初めて展開する場合は、例外管理のフローデザイナーがデフォルトで有効になります。既にワークフローを使用している場合は、フローデザイナーに更新できます。どちらの場合も、ワークフローに戻すことはできません。例外管理と誤検出の承認ルールを設定するには、「例外管理の承認ルールの構成」を参照してください。

CVIT または RT の例外要求が承認されると、以下のアクションを実行できます。

- 再オープン
- 削除
- [アサイン先] または [アサイン先グループ] フィールドの更新

例外要求の追跡

例外を申請した後、CVIT または RT の [ステータス変更承認 **(State Change Approvals)]** タブを使用してそのステータスを追跡できます。RT に対してアクションが実行された場合、その RT の個々の CVIT のステータスを追跡することはできません。

例外要求の有効期限

特定の CVIT または RT に対する例外要求が期限切れになると、影響を受ける CVIT または RT は [オープン] ステータスに戻ります。

単一の CVIT または RT 内のすべての CVIT が次のスキャンで合格すると、CVIT と、該当する場合は RT の [ステータス] フィールドが [クローズ済み] に変更され、サブステートは [修正済み] になります。

承認ルールの構成

承認ルールを表示および設定するには、次の場所に移動します。 **All** (すべて) > **Container Vulnerability Response** > アドミニストレーション > 承認ルール. 影響を受ける脆弱性、構成アイテム (CI)、または CVIT を特定して、すぐに修復も保留もできない CVIT の例外を要求します。CVIT の保留プロセスを自動化します。CVIT が識別されると、一致する CVIT が設定したルールに基づいて保留されます。

デフォルトでは、次の承認ルールが設定されています。

- 例外要求の承認：2 つの承認レベルがあるデフォルト構成がベースシステムに用意されています。脆弱性一致アイテムに例外要求がある場合、承認要求はレベル 1 に存在するユーザーまたはグループに送信されます。レベル 1 の承認者によって要求が承認されると、レベル 2 の承認者に送信されます。

  注:
  デフォルトのレベルは必要に応じて変更および編集することができます。コンテナ脆弱性対応 v2.0.6 以降、システムプロパティ [sys_properties] テーブルのワークフローによる例外処理に、ベースシステムのシステムプロパティを使用できます。このため、ワークフローで例外または誤検出要求が作成されると、この要求はシステムプロパティで定義されているグループ ID に承認のために送信されます。次のように移動する。 **All** (すべて) > システムプロパティ をクリックし、[*sn_vul_container.container_exception_approver_L1*]、[*sn_vul_container.container_exception_approver_L2*]、または [*sn_vul_container.container_false_positive_approver_group*] を選択して、プロパティ値を変更します。

- 例外ルールの承認：設定はありませんが、承認レベルが 2 つあります。
- 誤検出の承認：承認レベルが 1 つの構成が 1 つあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
コンテナ脆弱性対応 の v2.5 以降では、誤検出と例外を承認する期間を設定できます。また、設定した日数経過後の承認者と要求者の両方に対するメール通知も可能です。要求が発生すると、コンテナ脆弱性一致アイテムが [レビュー中] ステータスに変わり、ステータス変更レコードが作成されます。設定された期間内に承認者が応答しない場合、コンテナ脆弱性一致アイテムまたは修復タスクは [オープン] ステータスに戻ります。以前のステータスは **backup_state** フィールドに保存されます。詳細については、「例外管理の承認ルールの構成」を参照してください。

コンテナ脆弱性対応 での例外の要求と承認

コンテナ脆弱性一致アイテム (CVIT) の修復を指定した期間保留するように要求できます。たとえば、マシンにパッチが適用されない場合に、開発者が例外を要求できます。アクセス権を持つ承認者は、他のユーザーからの要求を承認できます。

例外を要求または承認するには、次のページを参照して下さい。

- コンテナ脆弱性一致アイテムの例外の要求
- GRC: ポリシーとコンプライアンス管理 を使用したコンテナ脆弱性の例外の要求

注:

例外管理の全ステージでメール通知が送信され、要求のステータスやその他の詳細情報が通知されます。たとえば、例外が要求されると、要求が発生したことを確認するメールが要求者に届きます。承認者にも、例外が要求されたことを示すメールが届きます。 コンテナ脆弱性対応 の v2.5 以降では、誤検出と例外を承認する期間を設定できます。また、設定した日数経過後の承認者と要求者の両方に対するメール通知も可能です。要求が発生すると、コンテナ脆弱性一致アイテムが [レビュー中] ステータスに変わり、ステータス変更レコードが作成されます。設定された期間内に承認者が応答しない場合、コンテナ脆弱性一致アイテムまたは修復タスクは [オープン] ステータスに戻ります。以前のステータスは **backup_state** フィールドに保存されます。詳細については、「例外管理の承認ルールの構成」を参照してください。

コンテナ脆弱性一致アイテムの例外の要求

すぐには修復できないコンテナ脆弱性一致アイテム (CVIT) の例外を要求します。たとえば、マシンにパッチが適用できない場合に、修復オーナーとして例外を要求できます。

始める前に
必要なロール：開発者グループ

このタスクについて
Vulnerability Manager ワークスペースの一括編集機能を使用して、複数の CVIT の例外を同時に要求できます。詳細については、「脆弱性マネージャーワークスペースでの一括例外の要求」を参照してください。

手順

1. 次のように移動する。 **Container Vulnerability Response** > コンテナ脆弱性一致アイテム > **All** (すべて).
2. 例外を要求するアイテムを選択します。
   選択したアイテムは、[オープン] または [調査中] ステータスである必要があります。
3. [コンテナ脆弱性一致アイテム] フォームで、[例外の要求] をクリックします。
   [store-future: BEGIN review]

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
で 脆弱性対応 または GRC: ポリシーとコンプライアンス管理 が選択されているかどうかに応じて **Container Vulnerability Response** > 例外管理 画面で、[例外の要求] フォームが変更されます。

[End]

4. [store-future: BEGIN review][例外管理] 画面で 脆弱性対応 が選択されている場合は、次の操作を行います。[End]

   a. フォームのフィールドに入力します。

   [例外の要求] フォーム

フィールド	説明
期限	例外要求の有効期限が切れる日付この日付は、次で選択した期間内である必要があります: **All** (すべて) > **Container Vulnerability Response** > アドミニストレーション > 例外管理 スクリーン。 例外要求の有効期限が切れると、グループは [オープン] ステータスに戻ります。 注: コンテナ脆弱性対応 のバージョン 1.2 以降では、脆弱性一致アイテムが例外管理機能を使用した修正のために保留された場合、スキャナーによって再オープンされた場合でも、脆弱性に設定された保留日は保持されます。この機能を有効にするには、*sn_vul.container.auto_defer_cvit_in_activ* システムプロパティの値を [true] に設定します。また、保留期限の日付は、CVIT がクローズした後や例外の有効期限が切れた後も保持されます。読み取りと書き込みの両方に必要なロールは sn_vul_container.manage_exception_configuration です。
理由	例外の理由。選択肢は次のとおりです。 ▪ リスクの受容 ▪ メンテナンス期間待ち ▪ 修正が利用不可 ▪ コントロールの緩和を実施 ▪ その他 理由の新しい選択肢を追加する方法については、「ポリシー理由のマッピングの定義」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
追加情報	この要求が行われている理由に関連する詳細情報。このフィールドは修復オーナーが更新します。

b. [承認要求] をクリックして例外要求を送信します。
コンテナ脆弱性一致アイテムの状況が [レビュー] に変わります。[ステータス変更承認] タブを使用して、例外要求のステータスを追跡します。

コンテナ修復タスクに対する例外の要求

修復タスクをすぐに解決できない場合に、コンテナ修復タスクを指定された期間保留する例外を要求します。

始める前に

例外は 脆弱性対応 のワークスペースから要求できます。「IT 修復ワークスペースで例外を要求する」を参照してください。

必要なロール：

sn_vul.remediation_owner、sn_vul.app_security_champion、または sn_vul_container.remediation_owner。

クラシック環境のコンテナ修復タスクに対して例外を要求することもできます。

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > 修復タスク > **All** (すべて).
2. 例外を要求するグループを選択します。
選択するタスクは、[オープン]、[調査中]、または [実装待ち] ステータスである必要があります。
3. コンテナ修復タスクレコードで、[例外の要求] を選択します。
4. フォームのフィールドに入力します。

[例外の要求] フォーム

フィールド	説明
期限	例外要求の有効期限が切れる日付。この日付は、構成で定義された例外期間内である必要があります。
理由	例外を要求する理由。
追加情報	この要求が行われている理由に関連する詳細情報。このフィールドは修復オーナーが更新します。

5. [承認要求] をクリックします。

GRC: ポリシーとコンプライアンス管理 を使用したコンテナ脆弱性の例外の要求

コンテナ脆弱性対応 内の ポリシーとコンプライアンス管理 アプリケーションの GRC ポリシー例外管理機能を使用して、ポリシー例外を要求します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
ポリシー例外統合を使用してポリシー例外を要求する前に、ServiceNow Store から GRC: ポリシーとコンプライアンス管理 アプリケーションをダウンロードする必要があります。

必要なロール： sn_vul.remediation_owner

クラシック UI で例外を要求することもできます。手順は次のとおりです。

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > コンテナ脆弱性一致アイテム (または [修復タスク]>[すべて] をクリックし、例外を要求するアイテムまたはグループを開きます。
   選択するアイテムまたはグループは、[オープン]、[調査中]、または [実装待ち] ステータスである必要があります。
2. 選択したフォームで、[例外の要求] をクリックします。

   注:
   [例外管理] 画面で GRC: ポリシーとコンプライアンス管理 が選択されている場合は、[例外管理] フォームのフィールドに入力します。フォームフィールドの詳細については、「[例外の要求] フォーム」を参照してください。

   a. [承認要求] をクリックして例外要求を送信します。
   脆弱性一致アイテムのステータスが [レビュー中] に変わり、ポリシー例外が作成されます。[ステータス変更承認] タブを使用して、例外要求のステータスを追跡します。

   b. [ポリシー例外] 関連リストをクリックして、作成したポリシー例外を確認します。

   c. ポリシー例外番号をクリックします。

   d. [承認者] フィールドで、承認者の名前を選択します。

   e. [ソース] タブをクリックし、[コントロール目標] フィールドからコントロール目標を選択します。

   f. [リスクアセスメント] タブをクリックし、[リスク評価] フィールドからリスク評価を選択します。

   g. フォームを保存します。

   h. [影響を受けるコントロール] タブをクリックします。

   i. [追加] をクリックしてコントロールを追加します。

   j. フォームを保存します。

      注:
      [コンプライアンスレビューを要求] をクリックすると、コンプライアンスレビューを作成できます。

   承認フォームが承認者に送信されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

承認者は [承認] をクリックして要求を承認するか、[追加の承認を要求] をクリックして追加の承認を要求します。

レコードのステータスが [保留] に変わります。表示されている理由は、例外要求を出したときに選択したものです。[保留] タブにはレコードに関する追加のメモが表示されます。

> **注:**
> 要求が却下された場合、レコードは前のステータスに移行します。

3. **[Submit]** をクリックします。
   ポリシー例外統合および修復オーナーとコンプライアンスマネージャー間の引き渡しの詳細については、「ポリシーとコンプライアンス管理オプションのセットアップ」を参照してください。

ポリシー理由のマッピングの定義

例外を要求するすべてのユーザーが使用可能な理由の選択肢を定義します。

始める前に
必要なロール：sn_vul.compliance.manager および
sn_vul_container.manage_exception_configuration

手順

1. 次のように移動する。 **All** (すべて) > ポリシーとコンプライアンス > ポリシー例外 > 統合レジストリ.

   > **注:**
   > [理由の選択肢] テーブルで利用可能な理由の選択肢から選択する方法と、新しい理由を追加する方法があります。

2. [Container Vulnerability Response - CVIT (Container Vulnerability Response - CVIT)] 統合レジストリをクリックします。
3. [理由の選択肢] リストで、[新規] をクリックします。
4. 虫眼鏡アイコンをクリックします。
5. 既存の理由の選択肢を追加して、新しい選択肢を作成します。
   - 既存の理由の選択肢を追加する場合は、理由を選択します。
   - [理由の選択肢] テーブルに新しい理由の選択肢を追加する場合は、[新規] をクリックし、フォームのフィールドに入力します。

[理由の選択リスト] フォーム

フィールド	説明
ラベル	この選択肢の一意のラベル。
値	この選択肢の一意の値。この値は、それぞれのアプリケーションの [ポリシーの理由のマッピング (Policy Reason Mapping)] テーブルでマッピングされます。このテーブルに移動するには、フィルターナビゲーターに「sn_vul_policy_reason_mapping.LIST」と入力します。
順序	この選択肢の順序。理由はこの番号に基づいて順序付けされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
デフォルト	オンデマンドポリシー例外が要求されたときには常にこの理由の選択肢が利用可能であることを示すオプション。統合レジストリにアプリケーション固有の選択肢が入っていない場合は、[デフォルト] フィールドが選択されているすべての選択肢が使用可能になります。
有効	理由の選択肢のリストに選択肢を表示するオプション。

6. [送信] をクリックします。

タスクの結果
理由の選択肢が追加されます。追加した理由の選択肢は、選択したアプリケーションのポリシー例外要求フォームの [理由] フィールドで使用可能になります。

コンテナ脆弱性対応 の例外要求を承認する

すぐに修復できないコンテナ脆弱性一致アイテムまたは修復タスクの例外要求を承認します。これらの要求のリスクを評価した上で、修復できるまで保留にすることを承認する必要があります。

始める前に
必要なロール：sn_vul.exception_approver

このタスクについて
Vulnerability Manager ワークスペースで例外要求と誤検出要求を承認できます。「Vulnerability Manager ワークスペース で要求を承認または却下」を参照してください。

クラシック環境で例外要求を承認することもできます。

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > 自分の承認.
2. キューから要求を選択します。
3. 適切なコメントを添えて、要求を承認または却下します。

コンテナ脆弱性対応 でのコンテナ脆弱性一致アイテムの保留

コンテナ脆弱性一致アイテム (CVIT) に関連する問題が低リスクで、それ以上分析することなくすぐに保留できると判断した場合は、[保留] 機能を使用できます。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)
脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

このタスクについて
スケジュール済みジョブで、再オープン日に達した保留中の脆弱性一致アイテムが毎日チェックされます。CVIT の保留が期限切れになる日に、レコードが再オープンされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > コンテナ脆弱性一致アイテム.
2. 脆弱性一致アイテムを開きます。
3. [例外の要求] をクリックします。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
期限	保留ステータスが期限切れになり、修復タスクが再アクティブ化される日付を選択します。 **注:** コンテナ脆弱性対応 のバージョン 18.0 以降は、保留されたコンテナ脆弱性一致アイテム (CVIT) がクローズされ、例外期間が終了する前にスキャナーによって再オープンされると、CVIT のステータスがアクティブな例外ウィンドウに従って [保留] ステータスに戻ります。この機能を有効にするには、*sn_vul.container.auto_defer_cvit_in_active* システムプロパティの値を [true] に設定します。また、保留期限の日付は、脆弱性一致アイテムがクローズした後や例外の有効期限が切れた後も保持されます。読み取りと書き込みの両方に必要なロールは sn_vul_container.manage_exception_configuration です。 レコードが送信された後、メール通知が定義されている場合、有効期限が 1 週間以内になると コンテナ脆弱性対応 グループのメンバーにメールが送信されます。保留日が期限切れになると、脆弱性一致アイテムは [オープン] に戻され、2 回目のメール通知が送信されます。
理由	問題を保留する理由を入力します。 次の選択肢があります。 ○ メンテナンス期間待ち ○ 誤検出 ○ 修正が利用不可 ○ リスクの受容 ○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. **[Submit]** をクリックします。
   グループは [レビュー中] とマークされます。[再オープン **(Reopen)]** 関連リンクが表示されます。再オープンの日付と理由は、[ステータス変更承認] タブの作業メモに表示されます。

   コンテナ脆弱性対応 v2.3 以降では、保留されたコンテナ脆弱性一致アイテムの [メモ] セクションの [作業メモ] フィールドに関連情報を追加できます。

保留されたコンテナ脆弱性一致アイテムの延長の要求

保留されたコンテナ脆弱性一致アイテムがその保留された期限に達する前に、この脆弱性一致アイテムの延長を要求します。修復オーナーは、この要求を行うために保留期日まで待つ必要がなくなりました。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

このタスクについて
脆弱性対応 ワークスペースから延長を要求することもできます。詳細については、「脆弱性マネージャーのワークスペースでの保留された脆弱性一致アイテムの延長の要求」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > コンテナ脆弱性一致アイテム.
2. 保留されているコンテナ脆弱性一致アイテムを開きます。
3. [拡張を要求] を選択します。

   注:
   [拡張を要求 (Request Extension)] ボタンは、コンテナ脆弱性一致アイテムのステータスが [保留] の場合にのみ表示されます。

4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
拡張期限	保留されたコンテナ脆弱性一致アイテムを修復のために延長する必要がある期限を選択します。
理由	問題を保留する理由を入力します。 次の選択肢があります。 ○ メンテナンス期間待ち ○ 修正が利用不可 ○ リスクの受容 ○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

5. [要求承認] を選択します。
   要求が送信され、承認者によって後続のアクションが実行されると、メールがトリガーされます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:

- 要求は 2 段階の承認を経過します。
- 保留されたコンテナ脆弱性一致アイテムが再度延長されると、バックエンドで延長保留カウントが増加します。

6. 要求が承認されると、[期限]、[理由]、および [保留メモ] が更新されます。

コンテナ脆弱性対応 での例外ルールの操作

すぐには修復または保留できないコンテナ脆弱性一致アイテム (CVIT) の例外を要求できます。VI 保留プロセスを自動化することで、一致する CVIT が識別されたときにルールに基づいてそうした CVIT を保留できます。

例外ルールに対し、以下のタスクを実行できます。

- コンテナ脆弱性対応 での例外ルールの作成
- コンテナ脆弱性対応 での例外ルール要求の承認
- コンテナ脆弱性対応 での例外ルールのアクティブ化
- コンテナ脆弱性対応 での例外ルールの再オープン
- コンテナ脆弱性対応 での承認された例外ルールの更新
- コンテナ脆弱性対応 での例外ルールの削除
- コンテナ脆弱性対応 でのコンテナ脆弱性一致アイテムの保留

注:
コンテナ脆弱性対応 の v2.5 以降では、誤検出と例外を承認する期間を設定できます。また、設定した日数経過後の承認者と要求者の両方に対するメール通知も可能です。要求が発生すると、コンテナ脆弱性一致アイテムが [レビュー中] ステータスに変わり、ステータス変更レコードが作成されます。設定された期間内に承認者が応答しない場合、コンテナ脆弱性一致アイテムまたは修復タスクは [オープン] ステータスに戻ります。以前のステータスは **backup_state** フィールドに保存されます。詳細については、「例外管理の承認ルールの構成」を参照してください。

コンテナ脆弱性対応 での例外ルールの作成

コンテナ脆弱性一致アイテム (CVIT) のグループについて特定の条件の例外を自動的に要求するルール (これらの CVIT の脆弱性重大度に基づく条件を含むルールなど) を作成します。このルールでは、新規および既存の CVIT が承認済みルールの条件に一致する場合に、そうした CVIT を自動的に保留にすることができます。

始める前に
必要なロール：sn_vul.vulnerability_admin

このタスクについて
ルールは「有効期間開始日」から「有効期限終了」の日付まで適用されます。ルールが承認されると、修復タスク (VUL) が作成されます。この VUL のグループ化方法は、例外ルールと呼ばれます。VUL は [保留] ステータスで作成されます。この VUL をクローズ、再オープン、削除することはできません。新規および再オープンされた CVIT は、この VUL に追加され、「有効期間開始日」から「有効期限終了」の日付でグループが期限切れになるまで保留されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

メール通知は、例外ルールワークフローのすべてのステージで送信されます。こうしたメールには、要求のステータスとその他の詳細が記載されています。たとえば、例外ルールが要求されると、要求が送信されたことを確認するメールが要求者に届きます。

注:
ルールが却下された場合は、[ドラフト] ステータスで再オープンして更新し、承認のために再送信できます。

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > アドミニストレーション > 例外ルール.
2. 例外ルールの新規レコードページで、[新規] をクリックしてルールを作成します。
3. [例外ルール] フォームのフィールドに入力します。

   注:
   フォームフィールドの詳細については、「例外ルールフォーム」を参照してください。

4. ルールの作成時にアサイン先グループを追加します。
5. フォームを承認のために送信します。
   要求のステータスが [レビュー中] に変わります。例外ルールを送信するまで、[ドラフト] ステータスのままになります。
6. 例外ルールを管理するグループを表示および作成するには、次の手順を実行します。

   a. 次のように移動する。 **All** (すべて) > ユーザー管理 **(User Administration)** > グループ.

   b. 例外ルールで、[要求された承認] タブをクリックして要求のステータスを表示します。
   スケジュール済みジョブは毎日実行され、既存のデータに対して例外ルールを実行します。条件に一致するすべての脆弱性一致アイテムが [保留] ステータスに移行します。承認された例外ルールが削除されると、保留されたすべての脆弱性一致アイテムが前の状態に戻ります。詳細については、「例外ルールの操作」を参照してください。

コンテナ脆弱性対応 での例外ルール要求の承認

ユーザーからの例外ルール要求を評価して、こうした要求を承認または却下できるようにします。

始める前に
必要なロール：sn_vul.exception_approver

このタスクについて
例外承認者レベル 1 ユーザーグループのメンバーは、レベル 1 の例外ルール要求を承認できます。同様に、例外承認者レベル 2 ユーザーグループのメンバーは、レベル 2 の例外ルール要求を承認できます。デフォルトでは、両方のユーザーグループが例外承認者ロールを継承します。

注:

VR アプリケーションを初めて展開する場合は、例外管理のフローデザイナーがデフォルトで有効になります。既にワークフローを使用している場合は、フローデザイナーに更新できます。どちらの場合も、ワークフローに戻すことはできません。例外管理と誤検出の承認ルールを設定するには、「例外管理の承認ルールの構成」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > 自分の承認.
2. キューから要求を選択します。
3. 要求を承認または却下し、要求を承認または却下した理由を説明します。
   例外ルールが承認されると、デフォルトでは修復タスク (RT) が [保留] ステータスで作成されます。「有効期間開始日」以降は、作成されたすべての CVIT と、ステータスが「クローズ済み」から「オープン」に移行した CVIT に対して、このルールが実行されます。定義された条件に一致する CVIT が RT に追加され、指定された期間保留されます。

   注:
   ルールが却下された場合は、[ドラフト] ステータスで再オープンして更新し、承認のために再送信できます。

コンテナ脆弱性対応 での例外ルールのアクティブ化

ルールは「有効開始日」にアクティブ化されます。アクティブ化すると、コンテナ脆弱性一致アイテム (CVIT) の例外プロセスが自動化されます。

例外ルールのライフサイクルは次のとおりです。

1. 作成または再オープンされた、指定された条件を満たす新しい CVIT は保留されます。例外ルールを初めて実行するときに [既存のデータで実行 (Execute on existing data)] オプションを有効にすると、例外ルールの条件に一致するすべてのアクティブな CVIT と保留されていない CVIT は新しく作成された修復タスク (RT) に移動され、そのステータスは [保留] に変更されます。
2. 新しく作成された CVIT が例外ルールの条件に一致する場合、その CVIT はルールに関連付けられている保留された RT に移動され、グループルールは実行されません。
3. 「有効期限開始」の日付で [既存のデータで実行 (Execute on existing data)] オプションを有効にすると、既存の CVIT が追加されます。
4. 「有効期限」の日付でルールが期限切れになると、RT は新しい CVIT の受け入れを停止します。RT は「保留期限」の日付まで存在し続けます。
5. 例外ルールは「有効期限」の日付で期限切れになります。

コンテナ脆弱性対応 での例外ルールの再オープン

却下されたけれども再送信したい例外ルールを再オープンします。ルールを再オープンすると、[ドラフト] ステータスに移行します。

始める前に
必要なロール：sn_vul.vulnerability_admin

このタスクについて
次に、承認のためにルールを更新して再送信できます。

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > アドミニストレーション > 例外ルール.
2. 再オープンするルールを検索し、[再オープン] をクリックします。
3. フォームを更新し、承認のために再送信します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンテナ脆弱性対応 での承認された例外ルールの更新

承認されたルールをキャンセルすると更新できるようになります。たとえば、日付を変更したり、承認済みルールに条件を追加したりする場合は、そのルールをキャンセルして修復タスク (VUL) を削除し、コンテナ脆弱性一致アイテム (CVIT) を [オープン] ステータスに移行する必要があります。

始める前に
必要なロール：sn_vul.vulnerability_admin

このタスクについて
グループルールがこうした CVIT に再適用されます。変更を行った後にルールを送信し、承認プロセスをもう一度繰り返します。

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > アドミニストレーション > 例外ルール.
2. キャンセルする例外ルールを開き、[キャンセル] をクリックします。
3. [ルールをキャンセル] ダイアログボックスで、[ルールをキャンセル] をクリックします。
   ルールが [ドラフト] ステータスに戻り、関連する VUL が削除されます。関連する CVIT が再オープンされ、グループルールが個々の CVIT に適用されます。

コンテナ脆弱性対応 での例外ルールの削除

不要になった例外ルールを削除します。たとえば、取り込み中にコンテナ脆弱性一致アイテム (CVIT) を保留しない場合は、ルールを削除できます。

始める前に
必要なロール：sn_vul.vulnerability_admin

このタスクについて
ルールを削除すると、関連する修復タスク (VUL) がキャンセルされます。関連する CVIT が再オープンされ、グループルールが個々の CVIT に適用されます。

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > アドミニストレーション > 例外ルール.
2. 削除する例外ルールを開き、[削除] をクリックします。
3. [削除ルール] ダイアログボックスで、[削除ルール] をクリックして、選択したルールを削除します。
   関連する修復タスクも削除されます。関連する CVIT が再オープンされ、グループルールが個々の CVIT に適用されます。

コンテナ脆弱性対応 での保留された修復タスクの延長の要求

保留された例外ルールがその保留された期限に達する前に、保留された修復タスク (VUL) の延長を要求します。修復オーナーは、この要求を行うために保留期日まで待つ必要がなくなりました。

始める前に
必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

このタスクについて
脆弱性対応 ワークスペースから延長を要求することもできます。詳細については、「脆弱性マネージャーのワークスペースでの保留された脆弱性一致アイテムの延長の要求」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > 修復タスク.
2. 保留された修復タスクを開きます。
3. [拡張を要求] を選択します。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
拡張期限	保留ステータスが期限切れになり、コンテナ脆弱性一致アイテムが再アクティブ化される日付を選択します。
理由	問題を保留する理由を入力します。 次の選択肢があります。 ○ メンテナンス期間待ち ○ 修正が利用不可 ○ リスクの受容 ○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

5. [要求承認] を選択します。
   要求が承認されると、修復タスクに対する変更が、修復タスクの一部であるコンテナ脆弱性一致アイテムにもロールダウンされます。ただし、コンテナ脆弱性一致アイテムが保留ステータスであり、現在の期限日が更新期限日より前である必要があります。また、要求が送信され、承認者によって後続のアクションが実行されると、メールがトリガーされます。

   注:
   - 要求は 2 段階の承認を経過します。
   - [拡張を要求] ボタンは、例外ルールの一部として作成された修復タスクでは使用できません。
   - 保留された修復タスクが再度延長されると、バックエンドで延長保留カウントが増加します。

コンテナ脆弱性対応 での例外ルールの延長の要求

保留された例外ルールがその保留された期限に達する前に、この例外ルールの延長を要求します。修復オーナーは、この要求を行うために保留期日まで待つ必要がなくなりました。

始める前に
必要なロール：sn_vul.exception_approver

このタスクについて
脆弱性対応 ワークスペースから延長を要求することもできます。詳細については、「脆弱性マネージャーのワークスペースでの保留された脆弱性一致アイテムの延長の要求」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > 例外ルール.
2. 保留された例外ルールを選択します。
3. [拡張を要求] を選択します。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
拡張期限	例外ルールを延長する必要がある期限の日付を選択します。
理由	例外ルールを保留する理由を入力します。 次の選択肢があります。 ○ リスクの受容 ○ メンテナンス期間待ち ○ 修正が利用不可 ○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

5. [要求承認] を選択します。
   要求が承認されると、例外ルールおよびコンテナ脆弱性一致アイテムの [保留期限]、[理由]、および [補足情報] フィールドが更新されます。また、要求が送信され、承認者によって後続のアクションが実行されると、メールがトリガーされます。

   注:
   - 要求は 2 段階の承認を経過します。
   - [拡張を要求] ボタンは、例外ルールの一部として作成された修復タスクでは使用できません。
   - 保留された例外ルールが再度延長されると、バックエンドで延長保留カウントが増加します。

誤検出コンテナ脆弱性一致アイテムのマークと承認

コンテナ脆弱性一致アイテム (CVIT) と修復タスク (VUL) は誤検出としてマークできます。書き込みアクセス権を持つ承認者は、他のユーザーからのそのような要求を承認できます。

- コンテナ脆弱性対応 での誤検出としてマーク
- 誤検出の承認

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

誤検出ワークフローの全ステージでメール通知が送信され、要求のステータスやその他の詳細情報が通知されます。たとえば、CVIT または修復タスクが誤検出としてマークされると、要求者は確認メールを受信します。同時に、承認者は、CVIT または修復タスクが誤検出としてマークされたことを示すメールを受信します。 コンテナ脆弱性対応 の v2.5 以降では、誤検出と例外を承認する期間を設定できます。また、設定した日数経過後の承認者と要求者の両方に対するメール通知も可能です。要求が発生すると、コンテナ脆弱性一致アイテムが [レビュー中] ステータスに変わり、ステータス変更レコードが作成されます。設定された期間内に承認者が応答しない場合、コンテナ脆弱性一致アイテムまたは修復タスクは [オープン] ステータスに戻ります。以前のステータスは **backup_state** フィールドに保存されます。詳細については、「例外管理の承認ルールの構成」を参照してください。

重要:
脆弱性アナリストと修復オーナーは、脆弱性マネージャーワークスペースと IT 修復ワークスペースのそれぞれから誤検出を要求および承認できます。

コンテナ脆弱性対応 での誤検出としてマーク

スキャナーによって発出された警告が実際には問題ではない場合、コンテナ脆弱性一致アイテム (CVIT) または修復タスクを誤検出としてマークします。たとえば、CVIT が廃止されてもスキャナーでそのアイテムに関連する問題がまだ発生している場合は、誤検出としてマークします。

重要:
脆弱性アナリストと修復オーナーは、脆弱性マネージャーワークスペースと IT 修復ワークスペースのそれぞれから誤検出を要求できます。

始める前に
必要なロール：修復オーナー

手順

1. 次のように移動する。 **All** (すべて) > コンテナ脆弱性対応 (または修復タスク) > **All** (すべて).
2. 誤検出としてマークする CVIT を開き、[誤検出としてマーク] をクリックします。
   CVIT のステータスが [オープン] である必要があります。
3. [誤検出] フォームで、[追加情報] に詳細を入力し、[承認要求] をクリックします。
   要求が承認のために送信され、CVIT のステータスが [レビュー中 **(In Review)]** に変わります。要求は要求者と承認者の両方にメールで通知されます。

誤検出の承認

誤検出承認者は、他のユーザーからの誤検出要求を承認できます。

重要:
Vulnerability Manager ワークスペースで誤検出要求を承認または却下できます。詳細については、「Vulnerability Manager ワークスペース で要求を承認または却下」を参照してください。

始める前に
必要なロール：false_ positive_approver
クラシック環境で例外と誤検出の要求を承認することもできます。

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > 自分の承認.
2. キューから要求を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. 適切なコメントを添えて、要求を承認または却下します。

> **注:**
> 誤検出は期限を定めることができます。承認者のみが終了日を設定できます。

コンテナ脆弱性対応の修復タスクとタスクルールの概要

修復タスク (CVUL) を設定すると、アナリストと修復スペシャリストがコンテナ脆弱性一致アイテム (CVIT) を整理して一括で分析できるようになります。修復タスクを形成する基準は、CVIT が修復タスクに自動的にアサインされるように構成されます。修復タスクを使用すると、進捗状況を監視し、修復プロセスをより効率的に進めることができます。

コンテナ脆弱性一致アイテムと修復タスクの保留数の追跡

脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、または修復タスクが保留された回数を追跡します。スケジュール済みジョブ [保留数の設定] は毎日実行され、[保留数] 列で複数回保留されたレコード数が提示されます。レコードは、VR、AVR、および CVR の複数の保留モジュールに表示されます。

修復タスクルールについて

修復タスクルールを使用すると、コンテナ脆弱性一致アイテムを自動的にグループ化してアサインする方法を定義できます。デフォルトのルール「脆弱性」は、脆弱性に基づいて CVIT を収集するベースシステムに含まれています。ただし、CVIT からアクセス可能な列では、その他の値セットでグループ化できます。こうした値には、構成アイテム (CI) や脆弱性エントリなどが含まれる場合があります。

コンテナ脆弱性対応には、脆弱性対応アプリケーションをアクティブ化したときに使用可能な、そのアプリケーションに含まれているタスクルールがあります。

条件ビルダーを使用して複数の条件を作成できます。[グループ分け基準] セクションで、フィールドのペアを設定すると、別の行が表示されます。最大 6 つの [グループ分け基準] の選択を設定できます。グループのアサインを自動化することもできます。

たとえば、コンテナ脆弱性一致アイテムを、構成アイテム別または製品モデル別にグループ化できます。低重大度の脆弱性または低リスクの CI に対して、1 つのタスクルールを設定できます。重要なサーバーに対して、会社をより大きなリスクにさらす脆弱性に対しては、別のタスクルールを設定できます。利用可能なオプションの詳細については、「コンテナ脆弱性対応の修復タスクルールの作成、編集、または削除」を参照してください。

会社がより多くのリスクにさらされるコンテナ脆弱性一致アイテムには、別のルールセットを使用できます。修復タスク名が修復タスクルールの [グループ分け基準] の値に追加され、新しいレコードの簡単な説明が作成されます。

新しいコンテナ脆弱性一致アイテムが作成、インポート、またはクローズ後に再オープンされると、それに対してルールが評価されます。CVIT は 1 回のみ自動的に評価されます。ただし、クローズ後に再オープンする場合や、ルールを手動で再適用する場合は除きます。

新規の CVIT または再オープンされた CVIT ごとに、以下の処理が行われます。

- 修復タスクルールごとに、CVIT が修復タスクルールフィルターと比較されます。
- 修復タスクルール条件が一致するルールごとに、CVIT の [グループ化] の選択に基づいてデータがルールによってプルされます。グループ名とフィールドがビルドされます。この場合は、高リスク：QID-32342：**QID-3242** のサマリー (名前：脆弱性 ID：脆弱性サマリー) となります。

> **注:**
> 簡単な説明フィールドは 160 文字に制限されています。これより長い脆弱性サマリーは切り捨てられます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このルールでは、CVIT と同じアサイン先グループにアサインされている、一致するオープン修復タスクがあるかどうかを確認します。

- タスクが見つかった場合、CVIT は [オープン] ステータスの既存のタスクに追加されます。
- [オープン] ステータスのタスクが見つからない場合は、高リスク：**QID-32342** タスクが作成され、CVIT と同じアサイン先グループにアサインされて、CVIT が修復タスクに配置されます。

複数の修復タスクルールを定義すると、さまざまな種類の脆弱性をグループ化できます。各脆弱性は、修復タスクに配置される前に修復タスクルールの条件と比較されるため、ルールが多すぎるとパフォーマンスに影響を与える恐れがあります。重複する修復タスクを作成しない条件となるように、タスクルールを設定します。

デフォルトでは、修復タスクルールで、アイテムのグループ化の際に CVIT のアサインルールによって設定されたアサイン先グループが使用され、CVIT に一致するように修復タスクがアサインされます。

デフォルトのタスクルールの一部として、こうした修復タスクのアサインは [アサインルール] モジュールのルールによって制御されます。アサインルールの詳細については、「脆弱性対応アサインルールの概要」を参照してください。

タスクルールが削除されると、フォームまたはリストビューから、そのルールによって作成されたすべてのオープンタスクを削除できます。[オープン] ステータスでないタスクは除外されます。

修復タスクルールの再適用

修復タスクルールを変更する場合は、修復タスクルールページの [再適用] ボタンを使用して、そのルールによって作成されたすべてのアクティブなオープン修復タスクに対し、変更されたルールを再実行します。変更されたルールに基づいて、修復タスクが自動的に削除され、再作成されます。

[再適用] は、既存の修復タスクのみをチェックします。

[再適用] を選択すると、[この修復タスクルールを最適用すると、このルール用の修復タスクが削除されてから再作成されます。オープン状態にない修復タスクは削除対象になりません。] というメッセージが表示されます。

重要:
脆弱性アドミンおよびアナリストは、Vulnerability Manager ワークスペースで選択した脆弱性一致アイテムの修復タスクルールを評価することができます。この方法は、時間のかかるクラシック UI で修復タスクルールを再適用するよりも効率的です。詳細については、「Vulnerability Manager ワークスペース でレコードの修復プロパティを再評価」を参照してください。

修復タスクルールと **CVIT** の作成と更新

スキャンの CI が既知の脆弱性に関連付けられている場合、CVIT が作成されます。作成後、CVIT は一致の修復タスクルールの条件に照らして評価されます。既存の修復タスクに一致するものがある場合は、CVIT が追加されます。一致する修復タスクが見つからない場合は、新しい修復タスクが CVIT に対して作成されます。

修復タスクのフィルタリング条件でキャプチャされたプロパティが CVIT で更新または変更された場合、更新された CVIT も一致の修復タスクルールに照らして評価されます。既存の修復タスクに一致するものがある場合は、CVIT が追加されます。一致する修復タスクが見つからない場合は、新しい修復タスクが CVIT に対して作成されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ステータスのロールアップとロールダウン

修復タスクを [オープン] に更新するか、[オープン] から [調査中] に更新すると、関連付けられているすべての CVIT に対して新しいステータスがロールダウンされます。ステータスのロールダウンは、ステータスを変更した直後に発生します。

CVIT から修復タスクへの状況のロールアップは、タスクのすべての CVIT が [保留] または [クローズ済み - 修正済み **(Closed - Fixed)]** 状況である場合にのみ発生します。ロールアップは、脆弱性に対するコンテナ脆弱性一致アイテムの値をロールアップし、15 分ごとに実行されるグループのスケジュール済みジョブを使用して実行されます。ジョブが実行されるまでステータスはロールアップされません。CVIT から修復タスクにステータスをロールアップするには、すべての CVIT が同じステータスである必要があります。

コンテナ脆弱性対応の修復タスクルールの作成、編集、または削除

フィルター条件に基づいて、コンテナ脆弱性一致アイテム (CVIT) を修復タスク (CVUL) に自動的にグループ化するルールを作成できます。こうしたルールは、インポート時または手動作成時に CVIT を自動的にグループ化します。

始める前に

新しいルールを作成しても、既存のデータには適用されません。送信すると、新しいインポートに対して実行されます。

必要なロール：アプリケーションセキュリティマネージャー

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > アドミニストレーション > 修復タスクルール。.
2. ルールを開くか、[新規] を選択します。
3. フォームのフィールドに入力するか、またはフィールドを編集します。

修復タスクルール

フィールド	説明
名前	タスクルールの名前。
有効	タスクがアクティブかどうかを示します。
説明	ルールの説明。
大文字と小文字を区別	条件が大文字と小文字を区別するかどうかを決定します。 **注:** デフォルト値は、大文字と小文字の区別なしです。
条件	ルールのオプションのフィルター条件。 デフォルト ([大文字と小文字を区別] チェックボックスが選択されていない) では、タスクルールのレコードとフォームで条件ビルダーに入力する検索テキストは、大文字と小文字が区別されません。選択によって、タスクのレコードとフォームで大文字と小文字を区別する検索を有効にできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	条件の例: 脆弱性 > 次の値に等しい > **VULNENT123451** (インポートされた既知の脆弱性)。この脆弱性があるすべての CVIT がこの条件に一致します。
グループ (最大 **6** つの条件セットが利用可能)	
コンテナ脆弱性一致アイテムのグループ化元	ルールが CVIT をグループ化するために使用するテーブル。 ツリーから要素を選択します。 ○ コンテナ脆弱性一致アイテム [sn_vuln_vulnerable_item] ○ コンテナ脆弱性一致アイテム - Docker イメージ ○ コンテナ脆弱性一致アイテム - コンテナ脆弱性 **注:** 拡張テーブルを選択した場合、[使用フィールド] はその拡張テーブルを使用するアプリケーション脆弱性一致アイテムにのみ適用されます。
使用フィールド	ルールが CVIT をグループ化するために使用するテーブルのフィールド。ツリーから条件を選択します。
アサイン	
修復タスクをアサインする基準	修復タスクを自動的にアサインする場合、[グループ] の選択肢に加えて [アサイン] の選択肢が、脆弱性一致アイテムをグループ化するために使用されます。必要に応じて新しいタスクが作成され、一致するアサイン先グループが設定されたタスクに各 CVIT が配置されます。 このルールに基づいて作成されたタスクのアサインを自動化するには、利用可能なオプションのいずれかを選択します。 ○ [グループ化フィールド] ：[グループ化] セクションの [使用フィールド **(Using field)]** からユーザーグループフィールドを選択すると、そのフィールドがドロップダウンメニューに表示されます。 ○ ユーザーグループ：ルックアップリストを使用して、静的ユーザーグループを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
フォームまたはリストビューからルールを削除すると、そのルールによって作成されたすべてのオープン修復タスクを削除できるようになります。[オープン] ステータスでないグループは除外されます。

4. 新しいルールの [送信] を選択します。
[送信] を選択すると、ルールが [修復タスクルール] リスト [sn_vul_grouping_rule] に表示されます。次の状況でルールが開始されます。
   - 新しい CVIT が作成されたとき。
   - [再適用] を選択したとき。既存の修復タスクのみのタスクルールを評価するには、[再適用] を選択します。
   - CVIT がユーザーまたはシステムによって更新されたとき。

     CVIT が更新されると、タスクルールが既存の修復タスクと一致するかどうかが評価されます。ルールチェックを開始する一般的な更新には次のようなものがあります。
     - ステータスが [クローズ済み] から [オープン] に、または [クローズ済み] から [調査中] に変わったとき。
     - 構成アイテム (CI) が変更されたとき。
     - 脆弱性が変更されたとき。

   すべてのタスクルールで、更新された CVIT との一致がチェックされます。ルールの条件が修復タスクの条件と一致する場合、一致する CVIT がそのルールにアサインされます。

   一致するものが見つからない場合は、新しい修復タスクが作成されます。

   CVIT から修復タスクへのステータスのロールアップ、および修復タスクから CVIT へのステータスのロールダウンの詳細については、「コンテナ脆弱性対応の修復タスクとタスクルールの概要」を参照してください。

   修復タスクルールの例については、「アプリケーション脆弱性対応の修復タスクルールの例」を参照してください。

5. タスクルールを削除するには、[修復タスクルール] リストからルールを選択し、[削除] を選択します。
次のメッセージが表示されます。選択した修復タスクルールによって n 個の修復タスクが作成されました (The selected remediation task rule created n remediation tasks)。そのうち、n 個のステータスがオープンです。

オプション	説明
チェックボックスは無効です (デフォルト)。	ルールのみを削除します。[オープン] ステータスでないタスクは除外されます。
チェックボックスをオンにします。	この修復タスクルールを削除する際に、[オープン] ステータスの修復タスクの削除を含めます。[オープン] ステータスのルールと修復タスクを削除します。

6. いずれかのオプションを選択し、[削除] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

の自動クローズルールの作成 コンテナ脆弱性対応

自動クローズルールを使用して、設定したフィルター条件に基づいて古いコンテナ脆弱性一致アイテム (CVIT) を自動的にクローズします。

始める前に
必要なロール:sn_vul.container_manage_auto_close_stale_vi

手順

1. 次のように移動する。 **All** (すべて) > **Container Vulnerability Response** > コンテナ脆弱性一致アイテム > 自動クローズルール.

   ベースシステムには、次の自動クローズルールがあります。前回スキャンされたコンテナ脆弱性：過去 90 日以内に報告されていない脆弱性は、[古い] ステータスに移行します。

2. [新規] を選択して、自動クローズルールを作成します。
3. フォームのフィールドに入力します。

フィールド	値
名前	自動クローズルールの名前
アクティブ	ルールをアクティブ化するためのオプション有効にすると、フィルター基準に一致するすべての検出が自動的にクローズされます。
実行順序	自動クローズルールの実行に対する一意の値。この値によって実行順序が決まります。デフォルト値は 100 です。
統合タイプ	コンテナ脆弱性統合 **注:** Prisma Cloud Compute 統合を使用してホスト脆弱性をスキャンするには、[脆弱性スキャナー統合] を選択します。
説明	自動クローズルールの説明。
条件	クローズする必要がある検出を識別するために使用されるフィルター条件。

4. [**Submit** (送信)] を選択します。
   自動クローズルールのスケジュール済みジョブは、毎日実行されます。指定された条件に基づいて CVIT を識別し、一致した CVIT を [古い] ステータスに移行します。ステータスが [クローズ済み] と [古い] の両方の CVIT がある場合、CVIT はサブステータスが [修正済み] に設定されてクローズされます。

修復タスクをクローズ

アプリケーション修復タスクに関連する問題をそれ以上分析することなくすぐにクローズできると判断した場合は、[クローズ] 機能を使用できます。コンテナ脆弱性対応 の v2.10 以降では、コンテナ修復タスクの [クローズ] ボタンが削除されました。

始める前に
必要なロール：admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタスクについて
脆弱性対応 ワークスペースでは、修復タスクは、以前のバージョンの 脆弱性対応 での修復タスクと同じ状況に移行します。ある修復タスクのすべての脆弱性一致アイテム (VIT) がクローズされると、その修復タスクは [非アクティブ] ステータスに移行します。

> **重要:**
> 状況同期を有効にした状態で、それぞれのレコードのライフサイクルの状況を介して変更要求と修復タスクを手動で移行することはできますが、CHG の状況が変化したことをシステムが登録したり、各自が CHG を追加したり、修復タスクから CHG を削除したりすると、状況同期によって手動による介入が無効になる可能性があります。ただし、変更要求の状況により、修復タスクのステータスが [クローズ済み] または [保留] 状況から自動的に移行されることはありません。

手順

1. レビューを要求するレコードを開きます。
2. [クローズ] ボタンをクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
ステータス	ステータスとして [クローズ済み] を選択します。
理由	問題をクローズする理由を入力します。
追加情報	その他の関連情報を入力します。

4. [送信] を選択します。
   修復タスクは [クローズ済み] とマークされます。

IT Operations Management (ITOM) とパターン検出

検出を有効にすると、Information Technology Operations Management (ITOM) チームから情報が届きます。ITOM ディスカバリーが有効な場合、コンテナ脆弱性一致アイテム (CVIT) を開くと、[Kubernetes 名前空間]、[Kubernetes クラスター]、および [Kubernetes サービス] が表示されます。有効でない場合は、Prisma ペイロード情報が表示されます。

Prisma ペイロードに表示されたイメージラベルは、Docker イメージの下にキーと値のペアとして格納されます。Prisma ペイロードのラベルは cmdb_key_value テーブルに格納されます。この機能を有効にするため、cmdb_ci_docker_image 用の識別ルールが ITOM チームによって初期実装されています。Docker イメージを開くと、関連アイテムのリストが表示されます。ほとんどのアイテムは ITOM チームによって設定されています。値をキーと値のペアとして表示するため、Docker イメージの識別エントリが初期実装されています。

ビジネス上の重要度は、ITOM チームから届いたサービスの重要度に関する情報に基づいて決定されます。スケジュール済みジョブを実行して、イメージに関連付けられたすべてのサービスからデータを取得します。実行したジョブによって、サービスマッピングに基づいてビジネス上の重要度が計算されます。リスクスコアはビジネス上の重要度に依存するため、リスクスコアもそれに基づいて計算されます。

コンテナ脆弱性対応 のアナリティクスおよびレポート作成ソリューション

このプラットフォームアナリティクスソリューションには、他の Now Platform 製品とともに使用するために、パッケージ化されたプラットフォームアナリティクスのコンテンツが含まれています。このプラットフォームアナリティクスソリューションでは、各種のグラフを通じて、脆弱性がどのように管理されているかが示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

必要なロール

このソリューションには、次のロールとタスクが関連付けられています。

- Now Platform 管理者 (admin)：この分析およびレポートのソリューションをインストールしてアクティブ化し、システムプロパティに必要な変更を加えます。
- プラットフォームアナリティクス アドミン (pa_admin)：インジケーター、ブレークダウン、ウィジェット、およびダッシュボードを確認します。データ収集を設定して開始します。適切なステークホルダーとダッシュボードを共有します。

関連情報

アナリティクスおよびレポートのソリューション

コンテナ脆弱性対応 ダッシュボード

アナリティクスおよびレポートのソリューションには、他の Now Platform 製品とともに使用するためのパッケージ化された パフォーマンスアナリティクス と レポート のコンテンツが含まれています。このプラットフォームアナリティクスソリューションでは、脆弱性の初期分析と検出から封じ込めや修復までのボリューム、パフォーマンス、および進捗状況を追跡できます。アサイン先グループやエクスプロイト、リスク評価、ステータスでレポートをフィルタリングできます。

必要な **Now Platform** ロール

- Now Platform アドミン (admin)：このアナリティクスおよびレポートのソリューションをインストールして有効にし、システムのプロパティに必要な変更を加えます。
- パフォーマンスアナリティクス アドミン (pa_admin)：インジケーター、ブレークダウン、ウィジェット、およびダッシュボードを確認します。データ収集を設定して開始します。適切なステークホルダーとダッシュボードを共有します。

コンテナ脆弱性対応 ダッシュボードへのアクセス

ダッシュボードを開くには、次の場所に移動します。 **All** (すべて) > **Container Vulnerability Response** > 概要.

重要:

コンテナ脆弱性対応 バージョン 2.2 以降、このダッシュボードは ネクストエクスペリエンス UI で表示することもできます。新しい UI でダッシュボードを表示するには、次に移動します: ワークスペース > 脆弱性マネージャーワークスペース をクリックし、[ダッシュボード] アイコンを選択します。ロールに応じてデフォルトのダッシュボードが表示されます。他のダッシュボードを表示するには、ダッシュボード名の横にあるドロップダウンを選択します。詳細については、「の [ダッシュボード] ページ Vulnerability Manager ワークスペース」と「の [ダッシュボード] ページ IT 修復ワークスペース」を参照してください。

注:

- 新規ユーザーは、ワークスペースからのみダッシュボードを表示できます。
- Tokyo を使用している場合は、Next Experience UI でダッシュボードを表示できますが、一部の機能が失われます。

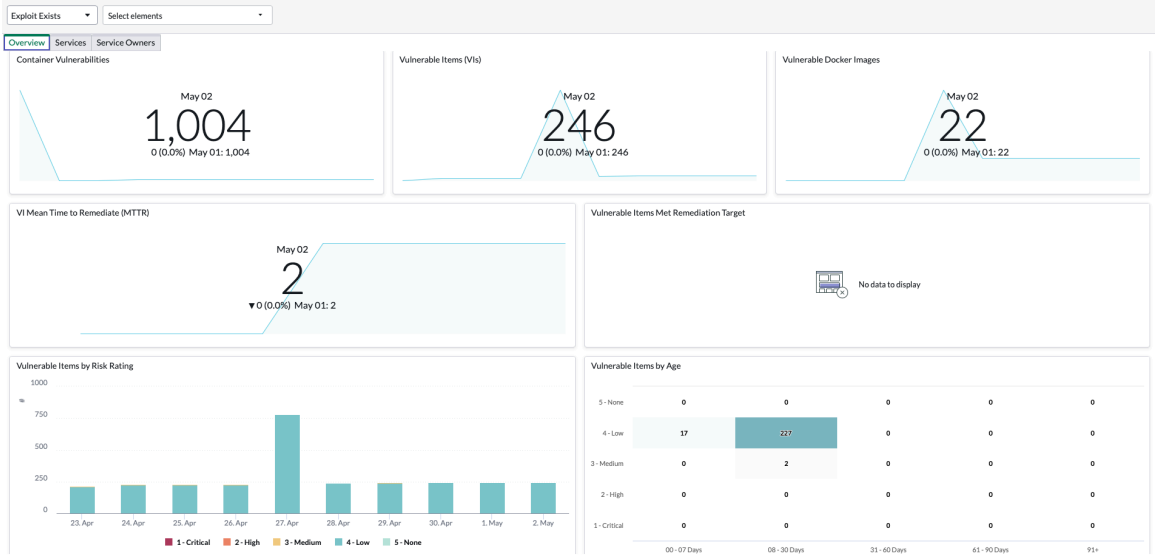
[コンテナ脆弱性管理] のタブ

このダッシュボードでは、コンテナに存在する脆弱性を確認できます。脆弱性とそれに関連するデータを、地域、経過時間、サービス、その他のブレークダウンごとに見ることができます。

自動翻訳

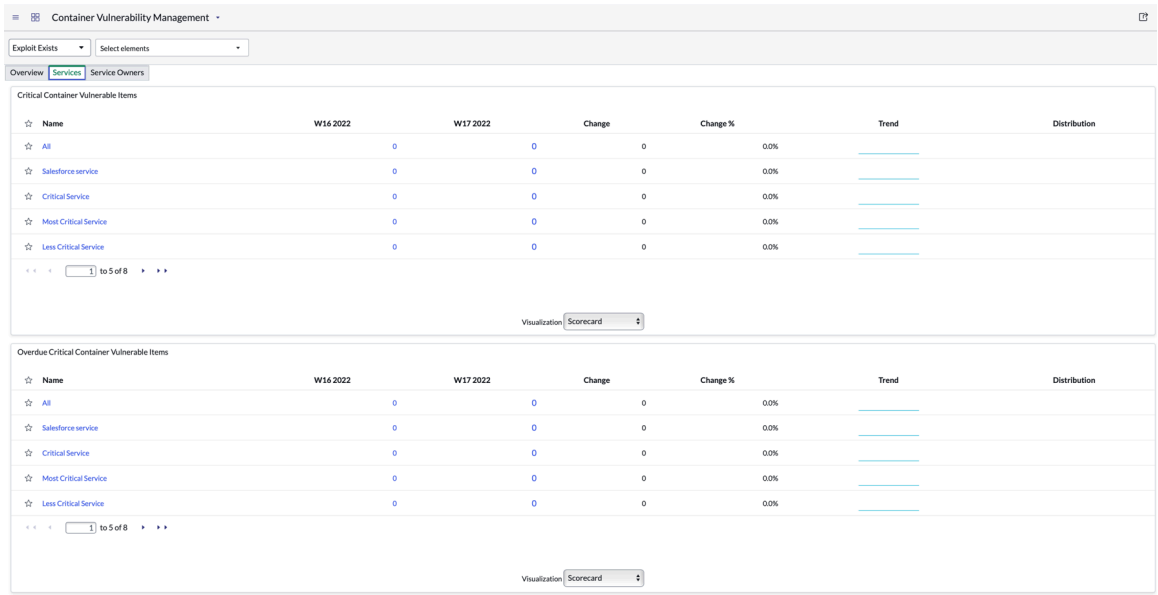
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[概要] タブには、システム内のコンテナ脆弱性管理の全体的なステータスが表示されま

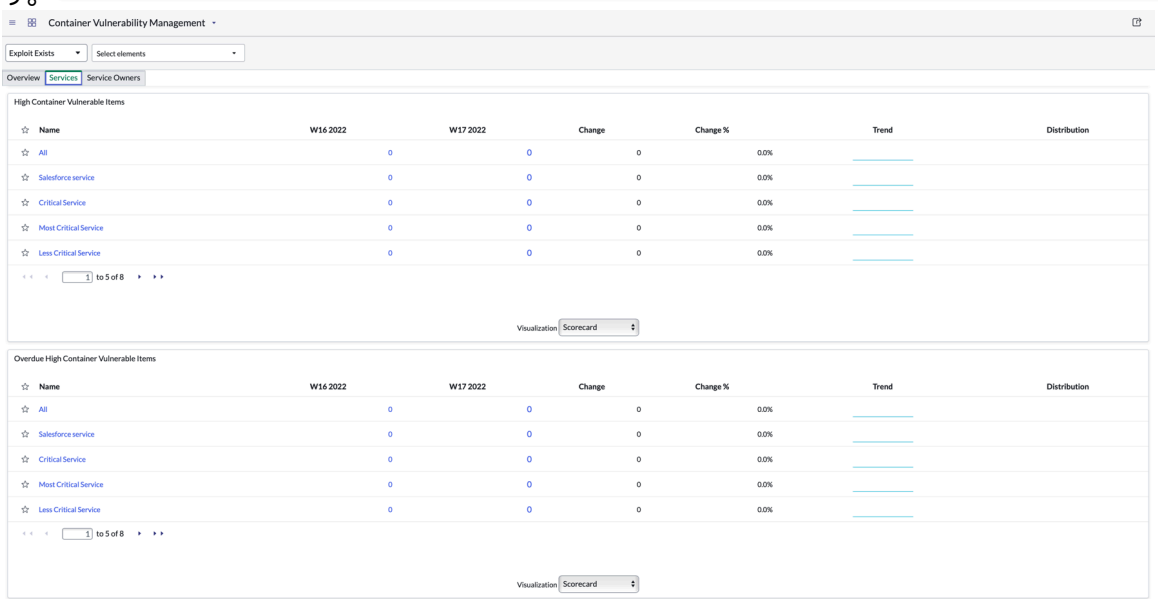


す。

[サービス] タブには、アプリケーションサービスに影響を与えるコンテナ脆弱性一致アイテムが表示されま

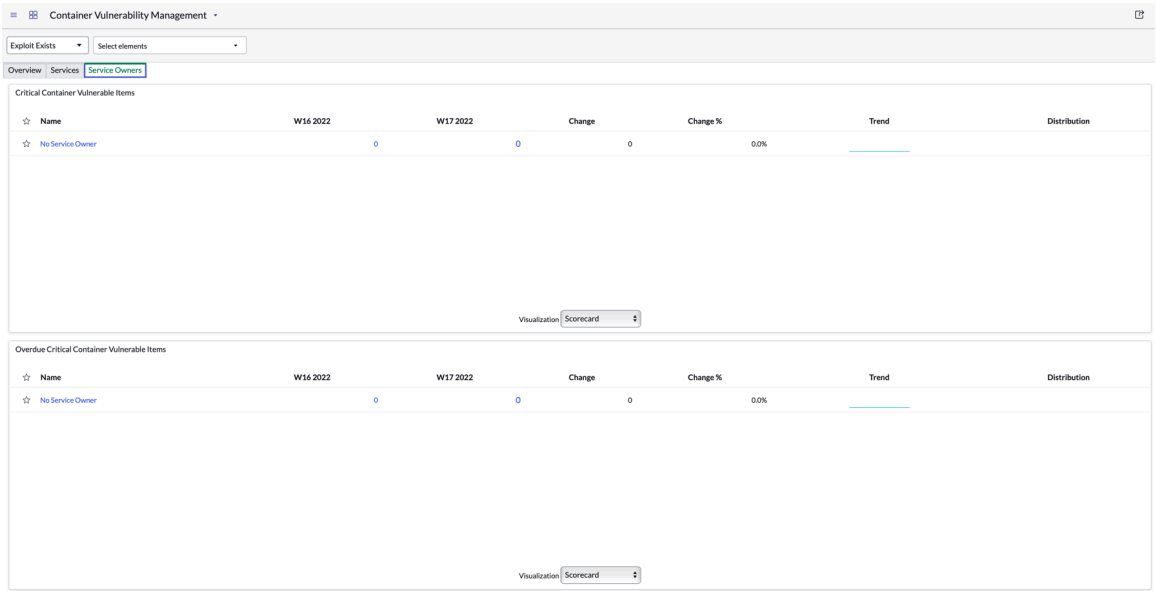


す。

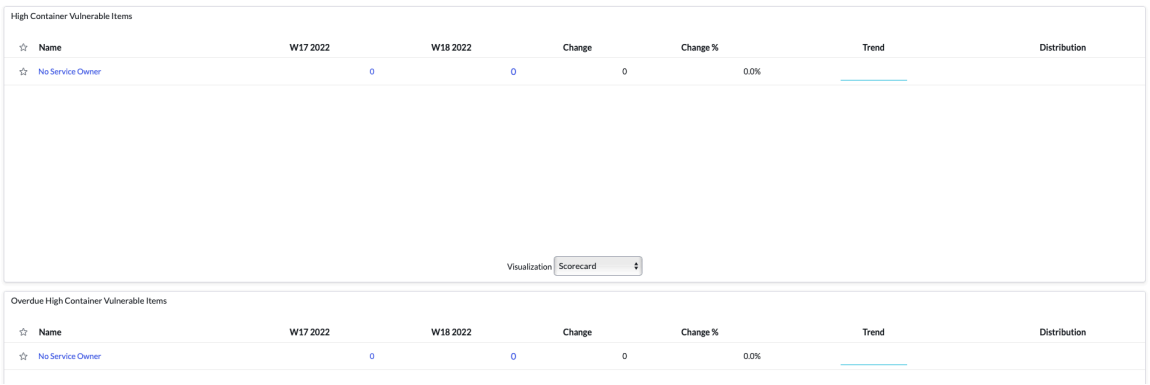


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[サービスオーナー] タブには、サービスオーナーに影響を与えるコンテナ脆弱性一致アイテムが表示されま



す。



ブレークダウン

- エクスプロイト有無
- エクスプロイト攻撃ベクトル
- エクスプロイトスキルレベル
- 修復ターゲットステータス
- リスク評価
- 状況
- アサイン先グループ

自動翻訳

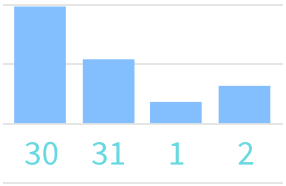
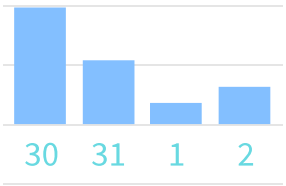
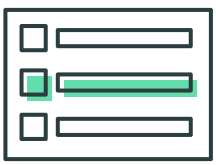
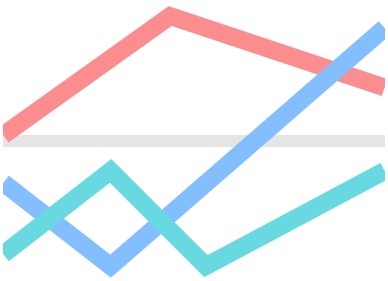
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データの可視化

名前	タイプ	説明
コンテナ脆弱性	単一スコア	1 つ以上のアクティブなコンテナ脆弱性一致アイテムに関連付けられたコンテナ脆弱性の数。
脆弱なアイテム (VI)	単一スコア	アクティブな (クローズされていない) コンテナ脆弱性一致アイテムの数。
脆弱な Docker イメージ	単一スコア	アクティブコンテナの脆弱性一致アイテムに関連付けられている Docker イメージの数。
VI 平均修正時間 (MTTR)	単一スコア	脆弱性一致アイテムを修正 (クローズ) する平均時間 (30 日間の実行平均として表示)。
修復ターゲットを満たした脆弱性一致アイテム	単一スコア	現在の四半期と前の四半期の修復ターゲット日を達成した、クローズされたコンテナ脆弱性一致アイテムの割合。修復ターゲットは、最後のオープン日に日数を加算して計算されます。

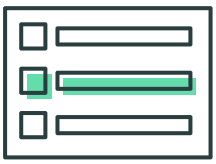
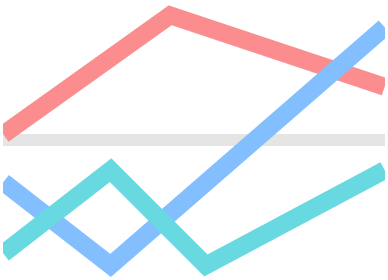
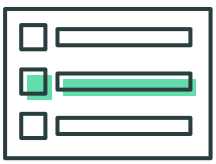
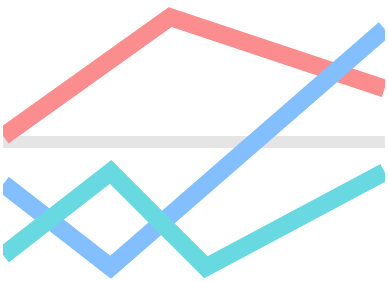
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	タイプ	説明
リスク評価別の脆弱性一致アイテム	棒グラ  フ	選択した時間スパンにおけるリスク評価によってグループ化された、アクティブなコンテナ脆弱性一致アイテムの数。
経過時間ごとの脆弱性一致アイテム	棒グラ  フ	リスク評価および経過時間 (日) でグループ化された、アクティブなコンテナ脆弱性一致アイテムの数。 **注:** コンテナ脆弱性一致アイテム (CVI) の経過時間とクローズ所要時間の計算をカスタマイズすると、これらのメトリクスを含むパフォーマンスアナリティクス (PA) レポートが急激に増減する可能性があります。CVI の経過時間とクローズ所要時間の計算をカスタマイズする方法の詳細については、KB1703270 KB 記事を参照してください。
重大なコンテナ脆弱性一致アイテム	リストと折れ線  	サービスごとにグループ化された、リスク評価が重大であるアクティブなコンテナ脆弱性一致アイテムの数。

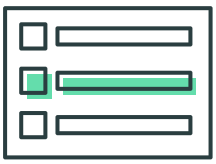
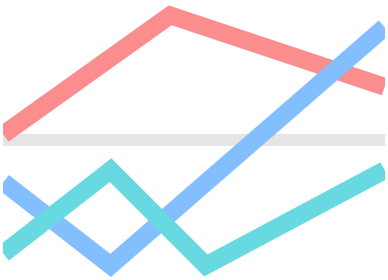
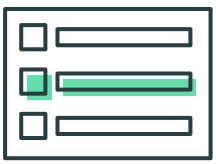
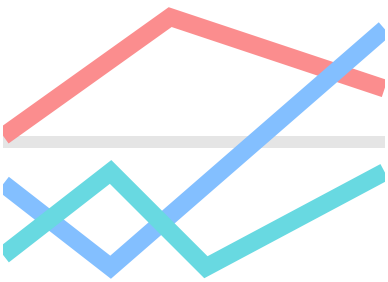
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	タイプ	説明
期限切れの重大なコンテナ脆弱性一致アイテム	リストと折れ線グラ  フ 	サービスごとにグループ化された、リスク評価が重大で修復ターゲット日が過去の日付になっている、アクティブなコンテナ脆弱性一致アイテムの数。
高リスクのコンテナ脆弱性一致アイテム	リストと折れ線グラ  フ 	サービスごとにグループ化された、リスク評価が高いアクティブなコンテナ脆弱性一致アイテムの数。

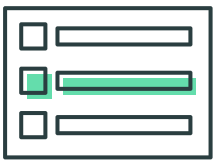
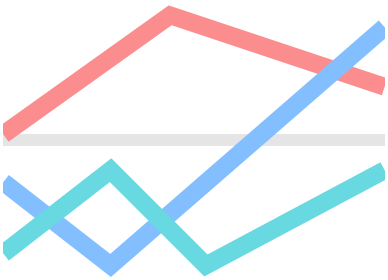
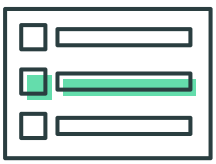
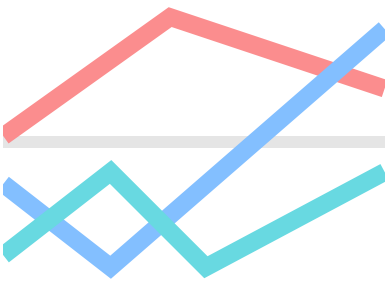
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	タイプ	説明
期限切れの高リスクのコンテナ脆弱性一致アイテム	リストと折れ線グラ  フ 	サービスごとにグループ化された、リスク評価が高く修復ターゲット日が過去の日付になっている、アクティブな脆弱性一致アイテムの数。
重大なコンテナ脆弱性一致アイテム	リストと折れ線グラ  フ 	サービスオーナーごとにグループ化された、リスク評価が重大であるアクティブなコンテナ脆弱性一致アイテムの数。

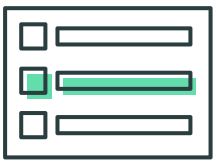
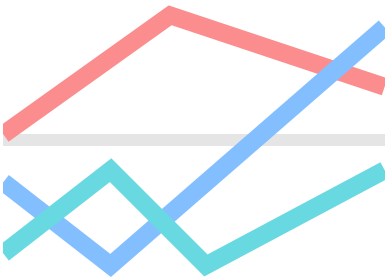
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	タイプ	説明
期限切れの重大なコンテナ脆弱性一致アイテム	リストと折れ線グラ  フ 	サービスオーナーごとにグループ化された、リスク評価が重大で修復ターゲット日が過去の日付になっている、アクティブなコンテナ脆弱性一致アイテムの数。
高リスクのコンテナ脆弱性一致アイテム	リストと折れ線グラ  フ 	サービスオーナーごとにグループ化された、リスク評価が高いアクティブなコンテナ脆弱性一致アイテムの数。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	タイプ	説明
期限切れの高リスクのコンテナ脆弱性一致アイテム	リストと折れ線グラ  フ 	サービスオーナーごとにグループ化された、リスク評価が高く修復ターゲット日が過去の日付になっている、アクティブな脆弱性一致アイテムの数。

の集計レポートフレームワーク コンテナ脆弱性対応

集計レポートフレームワークを使用すると、複雑で長時間実行されるオンザフライクエリを含むデータのレポートを作成して、パフォーマンスを向上させることができます。

集計されたレポートフレームワークは、次の方法でパフォーマンスを向上させます。

- より少ないリソース使用量で、迅速にレポートをレンダリングする
- データを集計し、集計とブレークダウン ([グループ分け基準]) を再利用する
- データベースへの照会を減らす

100 万を超えるコンテナ脆弱性一致アイテム (CVIT) がある場合は、標準レポートと一緒に集計レポートフレームワークを使用します。

必要なロール

このソリューションには、次のロールとタスクが関連付けられています。

- Now Platform アドミン (admin)：この プラットフォームアナリティクスソリューション をインストールしてアクティブ化し、システムのプロパティに必要な変更を加えます。
- パフォーマンスアナリティクス アドミン (pa_admin)：集計、ウィジェット、およびダッシュボードを確認します。データ収集を設定して開始します。適切なステークホルダーとダッシュボードを共有します。
- アドミン (sn_vul_cmn.admin)：集計を作成します。
- VR 書き込み (sn_vul_cmn.write)：集計および集計結果のデータを編集します。
- VR 読み取り (sn_vul_cmn.read)：集計および集計結果のデータを確認します。
- 脆弱性アナリスト [sn_vul.vulnerability_analyst]：集計結果を確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連情報

- ソースデータの集計を構成する
- 複数の集計を同時に実行する
- 同時に実行できる集計の数を構成する
- 集計を使用してレポートを作成する

コンテナ脆弱性対応 の参照

コンテナ脆弱性対応 とともにインストールされるテーブル、ロール、およびプロパティに関する情報を含む参照トピック。

コンテナ脆弱性対応 とともにインストールされるコンポーネント

コンテナ脆弱性対応 アプリケーションが有効になると、いくつかのタイプのコンポーネント (テーブル、ユーザーロール、スケジュール済みジョブなど) がインストールされます。

注:
アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「アプリケーションとともにインストールされているコンポーネントの検索」を参照してください。

この機能ではデモデータを利用できます。

コンテナ脆弱性対応 v2.11 以降、最も頻繁に使用されるシステムプロパティに コンテナ脆弱性対応 アプリケーション内でアクセスできるようになりました。これらのシステムプロパティを表示するには、次に移動します: **All** (すべて)コンテナ脆弱性対応プロパティ.

コンテナ脆弱性対応 と一緒にインストールされるロール

ロールは、コンテナ脆弱性対応 のアクティブ化とともに追加されます。

脆弱性対応 アプリケーションでユーザーとグループが表示および実行できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

注:

アップグレードのお客様の場合、v10.3 より前に sn_vul.vulnerability_read および sn_vul.vulnerability_write 権限によりアサインされたユーザーとグループのアクセス権は変更されていません。ユーザーとグループには、変更するまでこれらのロールが割り当てられたままになります。ただし、v10.3 以降では、 脆弱性対応 アプリケーションでユーザーやグループが実行および表示できる内容をより詳細に制御するために、詳細なロールを割り当てることをお勧めします。これらのロールの管理に関する概要と詳細については、「脆弱性対応 のペルソナと詳細なロール」および「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

ロールタイトル [名前]	説明
V2.10：sn_vul_container.delete	ソースレコードを削除sn_vul_ ロールと sn_vul_container.d ルが含まれています。
sn_vul_container.ci_manager	一致しない構成アイテム (CI) 理します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロールタイトル [名前]	説明
sn_vul_container.configure_integrations	コンテナ統合を構成します。
sn_vul_container.configure_vi_granularity	コンテナ脆弱性一致アイテムの します。
sn_vul_container.create_vi	コンテナ脆弱性一致アイテムを できます。
sn_vul_container.delete_vi	コンテナ脆弱性一致アイテムを できます。
sn_vul_container.exception_approver	コンテナ脆弱性一致アイテムの 留、およびクローズを承認しま sn_vul.view_manager_works が含まれます。 v2.3 以降では、このロールの sn_vul_container.read_all が べてのコンテナ脆弱性一致ア タスクではなく、自分と自分の アサインされたコンテナ脆弱性 ムと修復タスクにアクセスでき りました。
sn_vul_container.false_positive_approver	コンテナ脆弱性一致アイテムを て承認または却下します。 sn_vul.view_manager_works が含まれています。
sn_vul_container.manage_assignment_rules	コンテナ脆弱性一致アイテムの ルールを定義および更新しま
sn_vul_container.manage_auto_close_stale_vi	古いコンテナ脆弱性一致アイテ ローズを設定します。
sn_vul_container.manage_auto_exception_rule	例外ルールを管理 (作成/読み 除) します。
sn_vul_container.manage_normalized_severity	マッピングを更新して重大度を ます。
sn_vul_container.manage_permissions	コンテナ脆弱性対応ロールを インできます。
sn_vul_container.manage_remediation_targ…	コンテナの修復ターゲットル て更新します。
sn_vul_container.manage_risk_score_confi…	コンテナ脆弱性一致アイテムの ア算出、リスクルール、およ ルアップ算出を定義して更新
sn_vul_container.read_all	すべてのコンテナ脆弱性一致 連情報を確認できます。 sn_vul.view_manager_works が含まれています
sn_vul_container.read_assigned	自分または自分のグループに たコンテナ脆弱性一致アイテ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロールタイトル [名前]	説明
	シック UI または IT 修復ワー 表示できます。 sn_vul.view_rem_workspace まれています。 **重要:** 脆弱性対応 v24.0 以 降、sn_vul_container.re ロールにはIT 修復ワーク クセスする権限がありま
sn_vul_container.read_assignment_rules	コンテナ脆弱性一致アイテム ルールを確認できます。
sn_vul_container.read_auto_exception_rule	例外ルールを読み取ります。
sn_vul_container.read_discovered_image	検出されたアイテムを確認で
sn_vul_container.read_integrations	統合実行の結果を確認できま
sn_vul_container.read_normalized_severity	正規化された重大度マッピン ます。
sn_vul_container.read_remediation_target...	修復ターゲットルールを確認
sn_vul_container.read_risk_score_configu...	コンテナ脆弱性一致アイテム ア算出、リスクルール、およ ルアップ算出を確認できます。
sn_vul_container.remediation_owner	自身にアサインされているコ 一致アイテムの読み取りと書 ます。このロールを持つユー レコードも読み取ることがで
sn_vul_container.update_assigned_to	コンテナ脆弱性一致アイテム 更新できます。 sn_vul_container.write_all ま sn_vul_container.write_assi す。
sn_vul_container.update_assignment_group	コンテナ脆弱性一致アイテム グループを更新できます。 sn_vul_container.write_all ま sn_vul_container.write_assi す。
sn_vul_container.update_state	脆弱性一致アイテムのステー きます。 sn_vul_container.write_all ま sn_vul_container.write_assi す。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロールタイトル [名前]	説明
sn_vul_container.vulnerability_admin	コンテナ脆弱性対応 製品のル どをすべて設定します。
sn_vul_container.vulnerability_analyst	すべてのコンテナ脆弱性一致 復を監視します。
sn_vul_container.write_all	すべてのコンテナ脆弱性一致 復タスクを更新できます。
sn_vul_container.write_assigned	自分または自分のグループに たコンテナ脆弱性一致アイテ タスクを更新できます。
sn_vul_container.read_watch_topic	コンテナ脆弱性の監視トピッ ことができます。
sn_vul_container.create_watch_topic	コンテナ脆弱性の監視トピッ ます。
sn_vul_container.edit_watch_topic	コンテナ脆弱性の監視トピッ ます。
sn_vul_container.manage_exception_configuration	例外管理構成を管理できます。

コンテナ脆弱性対応 とともにインストールされるテーブル

テーブルは、コンテナ脆弱性対応 (CVR) のアクティブ化とともに追加されます。

自動翻訳

テーブル	説明
コンテナイメージの検索 sn_vul_container_image_findings	関連する脆弱性、イメージレイヤー、Docker イメージ、イメージリポジトリ、および検出されたイメージに関する情報が格納されます。 コンテナ脆弱性対応 の v2.11.3 以降では、検出結果が表示されるパスを表示することもできます。
コンテナイメージレイヤー sn_vul_container_image_layer	各イメージレイヤーの情報が入っています。イメージは、コンピューティングシステム上にコンテナを作成できる実行可能コードを含む静的ファイルです。
コンテナイメージパッケージ sn_vul_container_image_package	脆弱性が存在するパッケージに関する情報を提供します。バイナリパッケージの詳細もカンマ区切り値として提供されます。 コンテナ脆弱性対応 の v2.11.3 以降では、パッケージ URL (PURL) を表示することもできます。
コンテナ脆弱性一致アイテム sn_vul_container_image_vulnerable_item	それぞれの検出結果とそれに対応する脆弱性の詳細情報が含まれます。 コンテナ脆弱性対応 v2.11.3 以降では、コンテナとして実行されているイメージの最終スキャン日に関する情報を表示することもできます。
脆弱性エントリー (v2.11.3) sn_vul_entry	CVE の重大度に関する情報と、Prisma によって送信された追加情報を提供します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
検出されたコンテナイメージ sn_vul_container_image	イメージ ID、Docker イメージ、およびイメージリポジトリに関する情報を提供します。また、レイヤー情報も保存し、検出されたイメージに関連付けます。 コンテナ脆弱性対応 の v2.11.3 以降では、Docker イメージのイメージダイジェストと、コンテナーおよびレジストリーとして実行されているイメージの前回のスキャン日に関する情報も提供します。
マッピングの検索 sn_vul_container_finding_m2m_vul_item	コンテナイメージの検出結果とコンテナ脆弱性一致アイテム (CVIT) の M2M 関係。
脆弱性一致アイテムの自動クローズ sn_vul_container_image_auto_close_config	古いコンテナイメージの検出結果をクローズし、CVIT にステータスをロールアップする方法に関する情報が入っています。
コンテナイメージ脆弱性キー sn_vul_container_image_vulnerability_keys	コンテナイメージの検出結果から CVIT を作成するための粒度の構成が入っています。
Docker 関連サービス sn_vul_container_m2m_ci_services	コンテナイメージに関連するすべてのビジネスサービスが含まれます。
VR コンテナ数 sn_vul_container_vr_container_counts	過去 90 日間のコンテナイメージからスピンオフされたコンテナインスタンスのローリング平均が含まれます。
コンテナ修復タスクアイテム sn_vul_container_m2m_vul_group_item	CVIT とコンテナ修復タスク間の M2M テーブル。
コンテナ修復タスク sn_vul_container_vulnerability	コンテナ修復タスクが含まれます。
コンテナ修復タスクマニフェスト sn_vul_container_rt_manifest	修復タスクの更新は、スケジュール済みジョブがこのマニフェストテーブルを使用することで行われます。

インストールされているスケジュール済みジョブ コンテナ脆弱性対応

コンテナ脆弱性対応 のアクティブ化によってスケジュール済みジョブが追加されます。

注:
アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「アプリケーションとともにインストールされているコンポーネントの検索」を参照してください。

この機能ではデモデータを利用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みジョブ	説明
既存のコンテナ VI を自動例外ルールに関連付ける (Associate existing Container VIs with Auto Exception Rule)	自動例外ルールを既存のコンテナ脆弱性一致アイテム (CVIT) と自動的に関連付けます。
コンテナ脆弱性一致アイテムの保留の有効期限を確認する (Check Container Vulnerable Item Deferment Expiration)	コンテナ脆弱性一致アイテムまたはコンテナ脆弱性が期限切れになった場合 (および 1 週間以内に期限切れになる場合) に通知を送信します。
Vulnerability Response コンテナ数 (アプリケーション - Vulnerability Response およびコンテナ用 Configuration Compliance) (Vulnerability Response Container Count (Application - Vulnerability Response and Configuration Compliance for Containers))	毎日実行して、コンテナの 90 日間の移動平均を計算する sn_vul_container_vr_container_counts テーブルに入力します。
CVIT を自動クローズする (Auto-Close CVITs)	自動クローズ構成で定義された条件に一致するコンテナ脆弱性一致アイテムを自動的にクローズします。ステータスは「修復済み」に変更されます。
CVIT の事業上の重要度を計算する (Calculate Business Criticality for CVIT)	すべてのアクティブな CVIT を処理し、CVIT の Docker イメージの影響を受けるサービスに基づいて [事業上の重要度] フィールドを更新します。
Docker イメージが関連付けられていないキャンセル CVIT をクローズする (Close cancel CVITs that do not have a Docker Image associated)	CI が関連付けられていない CVIT を自動的に期限切れにします。ステータスは [クローズ済み] に設定され、サブステートは [キャンセル] に設定されます。
コンテナ修復タスクの関連 VI 数を計算する (Calculate Related VI Counts for Container Remediation Task)	コンテナ修復タスクレコードの数を計算します。
コンテナ脆弱性一致アイテムの値を脆弱性とグループにロールアップする (Rollup container vulnerable item values to vulnerability and group)	コンテナ脆弱性一致アイテムの脆弱性とグループのロールアップを計算します。 **注:** コンテナ脆弱性対応 の v2.10 以降では、スケジュール済みジョブが拡張され、マルチスレッド機能を備えたバックグラウンドジョブが作成できるようになりました。このアップグレードでは、ジョブをいくつかの小さな子ジョブに分割し、並列または同時に実行します。この変更により、複数のレコードを同時に処理できるようになり、タスク全体の速度が大幅に向上します。

コンテナ脆弱性対応 の用語集

コンテナ脆弱性対応 固有の用語や概念について説明します。

主要な用語

コンテナ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

コンピューティング環境間でアプリケーションがシームレスかつ確実に実行されるように、コードとそのすべての依存関係をパッケージ化するソフトウェアのユニット。

コンテナイメージ

コンピューティングシステム上にコンテナを作成できる実行可能コードを含む静的ファイル。コンテナイメージは変更できないため、どの環境でも一貫して展開できます。

クラスタ

コンテナ化されたアプリケーションを実行する、ノードと呼ばれる一連のワーカーマシン。

Docker

サーバーおよびクラウド上でアプリケーションコンテナを作成、展開、および管理するためのソフトウェア。

Docker イメージ

コード、必要なライブラリ、構成などを含むテンプレートファイル。このファイルは、コンテナインスタンスを起動するために使用されます。階層化されたファイルシステムが結合されて構成されています。

Dockerfile

複数のレイヤーを追加してコンテナイメージを作成するための指示を含むテキストファイル。たとえば、Base Ubuntu、Nginx、およびアプリコードの階層化。

Docker Compose

Docker を使用して複雑なアプリケーションを定義して実行するためのツール。Compose を使用すると、複数コンテナのアプリケーションを 1 つのファイルで定義できます。

Docker コンテナ

Docker コンテナは、Docker イメージから起動したランタイムインスタンスです。

イメージレイヤー

レイヤーは、画像への変更です。これは Dockerfile の指示によって表されます。レイヤーがベースイメージに順番に適用されて、最終的なイメージが作成されます。

画像リポジトリ

さまざまなタグまたはバージョンを持つ Docker イメージのコレクション。

イメージラベル

メタデータとして画像とともに保存されるキーと値のペアのセット。

名前空間

単一クラスター内のリソースグループの分離をサポートするために Kubernetes によって使用される抽象化。

ポッド

実行中のコンテナのセット (コンテナ上の別の抽象化)。

レジストリ

画像のリポジトリを含むホストサービス。

サービス

一連のポッドで実行されているアプリケーションをネットワークサービスとして公開する抽象化方法。

タグ

タグは指定の画像リポジトリ内の Docker イメージに適用されるラベルです。タグは、リポジトリ内のさまざまな画像を互いに区別する方法です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[コンテナ脆弱性一致アイテム] フォームのフィールド

コンテナ脆弱性一致アイテム (CVIT) は、サードパーティの脆弱性統合のインポート中に自動的に作成されます。

コンテナ脆弱性一致アイテムのフォームフィールド

[アサイン先グループ]、[アサイン先] フィールド、 および [メモ] を除き、CVIT の他のすべてのフィールドは読み取り専用です。

フィールド	説明
番号	このレコードに対して自動的に生成された CVIT 識別子。
ソース	脆弱性を特定したスキャナー。
リスク評価	脆弱性一致アイテムを [重大]、[高]、[中]、[低]、および [なし] に分類する数値化された [リスクスコア] 。
リスクスコア	CVIT が環境にもたらすリスク量を算出したもの。
修復ターゲットルール	修復ターゲット日の計算の基準となる修復ターゲットルール。
修復ターゲット	CVIT が最初に識別されてから、修復されるべき日付。該当する場合にのみ表示されます。
修復ステータス	CVIT の修復のステータス。
脆弱性	このアプリケーション脆弱性一致アイテムに関連付けられた脆弱性の ID。
Docker イメージ	コード、必要なライブラリ、構成などを含むテンプレートファイル。ファイルを使用してコンテナーインスタンスを開始します。階層化されたファイルシステムを統合したもので構成されています。
検出されたコンテナイメージ	各イメージ ID の一意のレコード。
基本イメージ	必須のオペレーティングシステムとライブラリを含む、コンテナ化されたアプリケーションの作成に使用される基本イメージ。これは、Docker などの環境でアプリケーションをビルドおよびカスタマイズするための出発点として機能します。
イメージクラスター	機械学習内の類似画像やリポジトリ内のコンテナ画像のクラスタリングなど、さまざまなコンテキストで使用される関連画像のグループ。
イメージの名前空間	レジストリ内のコンテナイメージを整理および分離し、異なるチームやプロジェクトが別々のコレクションを維持できるようにするために使用します。
状況	このフィールドは、作成時のデフォルトで [オープン] になっています。状況のマッピング方法の詳細については、「アプリケーション脆弱性一致アイテム (AVI) の状況」を参照してください。
アサイン先グループ	この CVIT で作業するように選択されたグループ。
Assigned to (アサイン先)	この CVIT で作業する、選択されたアサイン先グループの個人。アプリセキュリティマネージャーが手動で追加または編集できます。
作成日時	CVIT が作成された日時。
最終オープン日時	CVIT が再開された最新の日時。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
更新日時	CVIT が最後に変更された日時。
初回検出 (v2.12.1)	脆弱性が最初に検出された日付。 v2.12.1 以降では、最初に検出された正確な日時を確認できるため、明確になり、さまざまなタイムゾーンを考慮できます。 最初に検出された日時の詳細を入力するには、統合を再実行する必要があります。
前回検出 (v2.12.1)	この脆弱性が最後に検出された日付。 v2.12.1 以降では、最後に見つかった正確な日時を確認できるため、明確さが確保され、さまざまなタイムゾーンが考慮されます。 最後に検出された日時の詳細を入力するには、統合を再実行する必要があります。
解決日 (v2.12.1)	脆弱性が解決された日付。 v2.12.1 以降では、解決された正確な日時を確認できるため、明確になり、さまざまなタイムゾーンが考慮されます。 解決日は、CVIT がワークフローの一部として解決されると入力されます。
最終オープン日時 (v2.12.1)	この脆弱性が最後にオープンされた日付。 v2.12.1 以降では、最後に開いた正確な日時を確認できるため、明確になり、さまざまなタイムゾーンが考慮されます。 このフィールドにデータが入力されるスケジュール済みジョブ *Add default values for last_opened_dt_tm from last _opened* 。オンデマンドで 1 回だけ実行する必要があります。
脆弱性	
まとめ	脆弱性の説明。
重大度	この脆弱性の重大度を正規化したもの。重大度マップは、脆弱性情報データベース (NVD) および ServiceNow サードパーティ統合に提供されます。
脆弱性スコア (v3)	共通脆弱性スコアリングシステム (CVSS) v3 スコア。
脆弱性スコア (v2)	CVSS v2 スコア。
エクスプロイト有無	この脆弱性一致アイテムに関連付けられた脆弱性に少なくとも 1 つのエクスプロイトが関連付けられている場合は、有り。
エクスプロイト攻撃ベクトル	この脆弱性一致アイテムに関連付けられた脆弱性のエクスプロイトの最も脆弱な攻撃ベクトル。
エクスプロイトスキルレベル	この脆弱性一致アイテムに関連付けられた脆弱性のエクスプロイトに必要な最低スキルレベル。
公開日	この脆弱性が公開された日付。
最終変更日	この脆弱性が前回変更された日付。
脅威	脅威に関する関連情報。脆弱性エントリーレコードから取得されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: ここで変更を加えると、脆弱性エントリーレコードが更新されます。
修復メモ	脆弱性エントリーレコードから取得された、脅威に対する関連ソリューション。
メモ	
作業メモ	関連情報。作業メモのテキストボックスを選択して情報を追加します。
イメージの検出結果	コンテナイメージの脆弱性をスキャンした結果。
要求された承認	CVIT に対して発生した承認要求。
ステータス変更承認	CVIT に対して発生したステータス変更承認要求。

CVIT の経過時間計算:

- CVIT のリストの [経過時間] 列には、CVIT がアクティブである期間 (形式:日数 HH:MM:SS) が表示されます。クローズ済み CVIT の場合、経過時間の値はゼロです。
- CVIT のリストの [クローズ所要時間] 列には、CVIT がクローズされる前にアクティブである期間 (形式:日数 HH:MM:SS) が表示されます。CVIT の場合、[クローズ済み] ステータス以外の場合、[クローズ所要時間] の値はゼロです。

経過時間およびクローズ所要時間の計算をカスタマイズする方法の詳細については、KB1703270 記事を参照してください。

Prisma Cloud Compute の構成フォーム

Prisma Cloud Compute の構成フォームには、Prisma Cloud Compute 統合モジュール内からアクセスします。

Prisma Cloud Compute の構成フォームを表示するには、 **All** (すべて) > **Prisma Cloud Compute** 統合 > アドミニストレーション > 構成.

Prisma Cloud Compute 構成

フィールド	説明
統合インスタンス	新しい統合インスタンスの名前。 インスタンスを作成するか、ルックアップアイコンをクリックして既存のインスタンスを選択できます。
API ベース URL	Prisma Cloud Compute と統合するための URL
ユーザー名	Prisma Cloud Compute にアクセスするためのユーザー名
パスワード	Prisma Cloud Compute にアクセスするためのパスワード
MID サーバー	ローカルネットワーク内のサーバーで Windows サービスまたは UNIX デーモンとして動作する Java アプリケーション。MID サーバーは、ServiceNow インスタンスと外部のアプ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Prisma Cloud Compute 構成 (続く)

フィールド	説明
	リケーション、データソース、サービスの間のデータの通信や移動を支援します。
プロジェクトを使用	プロジェクトを構成するオプション。チェックボックスをオンにすると、構成ページでプロジェクトを選択し、プロジェクト固有の詳細を入力するように構成されたプロジェクトに基づいて統合を実行できます。 **注:** このチェックボックスをオンにすると、[プロジェクトを構成する] タブが有効になります。[次へ] をクリックして、プロジェクトの構成を続行します。

[例外の要求] フォーム

コンテナ脆弱性対応 内の ポリシーとコンプライアンス管理 アプリケーションの GRC ポリシー例外管理機能を使用して、ポリシー例外を要求します。

Prisma Cloud Compute の構成フォームを表示するには、 **All** (すべて) > **Container Vulnerability Response** > コンテナ脆弱性一致アイテム (または [修復タスク]>[すべて] をクリックし、例外を要求するアイテムまたはグループを開きます。

[例外の要求] フォーム

フィールド	説明
ポリシー	例外を要求している脆弱性管理ポリシー。
コントロール目標	選択したポリシーに関連付けられているコントロール目標。ポリシーが選択されていない場合は、すべてのコントロール目標が一覧表示されます。
有効開始日	例外が開始される日付。デフォルト値は現在の日付です。過去の日付にすることはできません。
有効期限	ポリシー例外が期限切れになり、脆弱性一致アイテムまたはグループのステータスが [保留] から [オープン] に変更される日付。 **注:** ポリシー例外が有効である日数を、Policy and Compliance でポリシーに設定した [最大例外期間 (日数)] を超える日数に設定することはできません。詳細については、「ポリシーの作成」を参照してください。
理由	例外を要求する理由。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[例外の要求] フォーム (続く)

フィールド	説明
理由	この要求が行われている理由に関連する詳細情報。このフィールドは修復オーナーが入力する必要があります。

例外ルールフォーム

コンテナ脆弱性一致アイテム (CVIT) のグループについて特定の条件の例外を自動的に要求するルール (これらの CVIT の脆弱性重大度に基づく条件を含むルールなど) を作成します。このルールでは、新規および既存の CVIT が承認済みルールの条件に一致する場合に、そうした CVIT を自動的に保留にすることができます。

[例外ルール] フォームを表示するには、次に移動します: **All** (すべて) > **Container Vulnerability Response** > アドミニストレーション > 例外ルール.

例外ルールフォーム

フィールド	説明
名前	例外ルールの名前。
有効期限開始	このルールがアクティブになり、CVIT が保留される開始日付。
有効期限	修復タスクが新しい CVIT の受け入れを停止する日付。
理由	この例外ルールを作成する理由。
アサイン先グループ	保留された CVIT の追跡用に作成された修復タスクがアサインされているグループ。
追加情報	要求者が承認者に提供する追加情報。この情報は、修復タスクの説明フィールドに入力されます。
条件	CVIT の処理中に定義できる CVIT のフィルター条件。
既存のデータで実行	このルールが初めて実行されるときに既存のデータでこのルールを実行できるようにするオプション。
ワークフローステージ	例外ルールの現在の承認ステータス。
状態	例外ルールのステータス。
実行順序	各例外ルールの一意の順序。
保留期限	VUL および CVIT の保留期限となる日付。この日付になると、作成された VUL がクローズされ、すべての CVIT がグループから離脱し、グループルールが再適用されます。

コンフィグレーションコンプライアンス

ServiceNow® コンフィグレーションコンプライアンス アプリケーションは、サードパーティの構成スキャンアプリケーションとの統合からスキャン結果を集計する Secure Configuration Assessment (SCA) アプリケーションです。構成管理データベース (CMDB) を使用して、コンフィ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

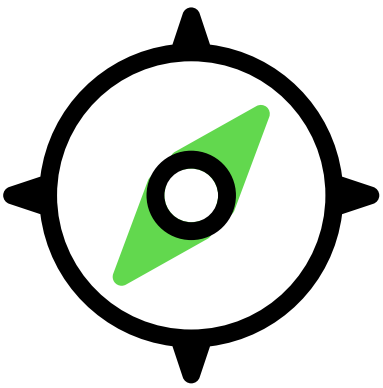
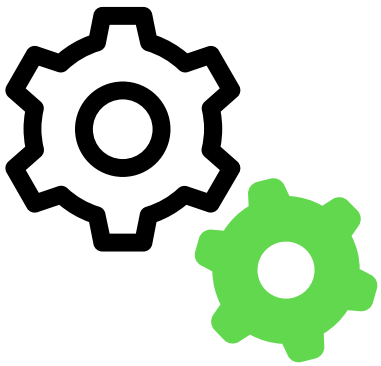
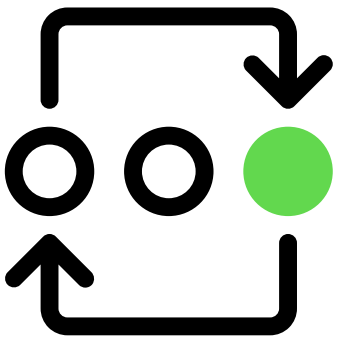
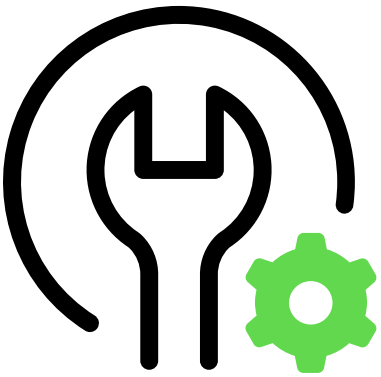
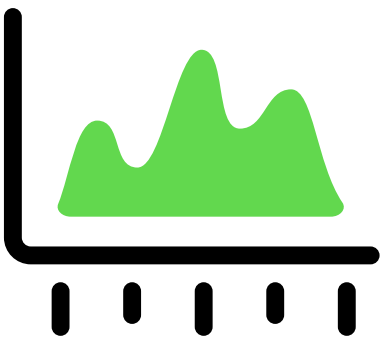
自動翻訳

ギュレーションコンプライアンスに関する問題に優先順位を付けることができます。コンフィグレーションコンプライアンス は IT 変更管理プロセスと緊密に統合し、非準拠の構成を修復します。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

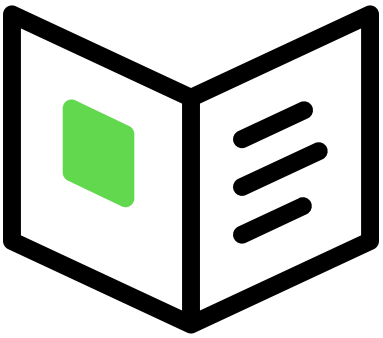
コンフィグレーションコンプライアンス

探索  コンフィグレーションコンプライアンスの概念と機能について説明します	セットアップ、インストール、構成  コンフィグレーションコンプライアンスの構成	統合  他のアプリケーションとの統合による Configuration Compliance の拡張
脆弱性対応ワークスペースの使用 脆弱性マネージャー、IT 修復、および脆弱性アセスメントのワークスペースで構成の問題を監視、管理、修正する方法について説明します。	修復  コンフィグレーションコンプライアンスで非準拠の資産を修復する方法を学ぶ	アナリティクスおよびレポート  Configuration Compliance でのレポートとダッシュボードの表示

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Reference (参照)



フィールド、テーブル、プロパティなどのコンフィグレーションコンプライアンスコンポーネントの詳細を取得します

トラブルシューティングとサポート

- セキュリティオペレーションリソースライブラリ
- セキュリティオペレーションコミュニティ
- 既知のエラーポータルで既知のエラー記事を検索する
- 連絡先 カスタマーサービス & サポート

コンフィグレーションコンプライアンス の詳細

サードパーティの Third-party Secure Configuration Assessment (SCA) 統合から取得したテスト結果を使用して、セキュリティや企業ポリシーへの準拠を検証します。非準拠構成アイテムの識別、優先順位付け、修復を行います。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

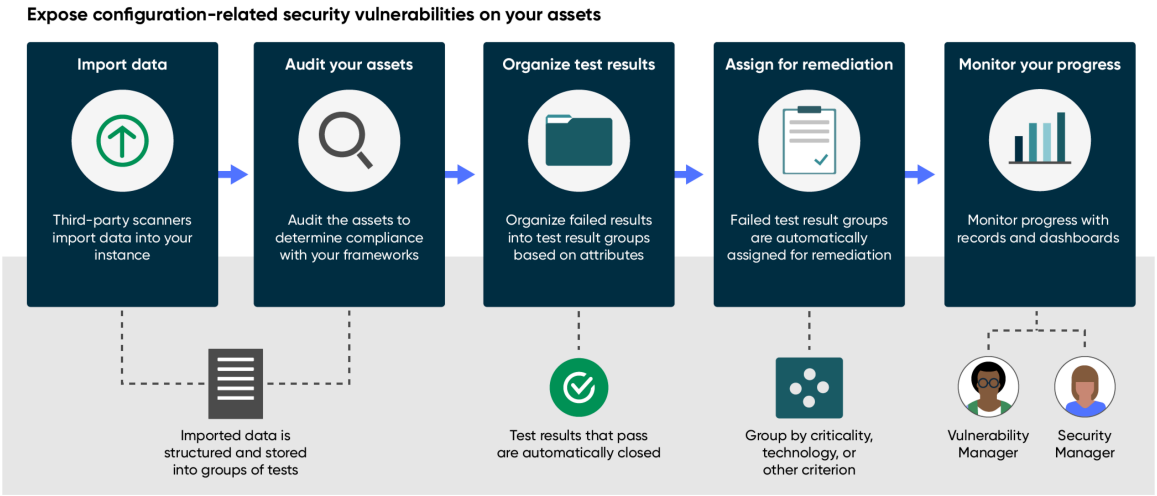
v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンフィグレーションコンプライアンス の概要

ServiceNow® コンフィグレーションコンプライアンス アプリケーションを使用すると、迅速かつ効率的に環境内の最も重要な構成関連の脆弱性に優先順位を付け、修復できます。コンフィグレーションコンプライアンス は ServiceNow® Store のサブスクリプションで使用できます。



コンフィグレーションコンプライアンス の主な機能

Now Platform® の 構成管理データベース (CMDB) を使用すると、最も重要な構成関連のセキュリティ脆弱性を明らかにして、修復できます。リスクを最も軽減するアクティビティに修復リソースを集中させることができます。セキュリティ、IT、ビジネスプロセスのステークホルダー全体で修復プロセスを簡素化します。コンフィグレーションコンプライアンス アプリケーションには次の主な機能が含まれています。

- サポートされているサードパーティ統合により、ポリシー、テスト、信頼できるソース、およびテクノロジーが自動的にインポートされます。サポートされている統合の詳細については、「コンフィグレーションコンプライアンス の統合」を参照してください。
- ポリシーとテストを構成アイテム (資産) に関連付けて、構成関連の脆弱性を識別し、資産がポリシーとコントロールに準拠していることを確認できるようにします。
- すべての資産において、構成アセスメント、アサイン、および修復を一元化します。
- 構成スキャンコンテンツは、主要な Secure Configuration Assessment (SCA) エコシステム統合アプリケーションからインポートできます。
- 修復スペシャリストのスキルセットと責任範囲に基づいて、構成結果やテストの失敗を自動的にグループ化してルーティングできます。インテリジェントワークフローおよび変更管理との緊密な統合により、グループ間でのスムーズなタスクの引き継ぎが実現します。
- ServiceNow ガバナンス、リスク、コンプライアンス (GRC) アプリケーションと併用すると、コンフィグレーションコンプライアンス の構成テストを対応する GRC コントロールにロールアップできます。
- 拡張された変更管理により、コンフィグレーションコンプライアンス から直接 IT に事前入力された変更要求を作成し、追加リソースを必要とする修復タスクを支援します。
- ダッシュボードでは、修復タスク、コンプライアンステスト、ポリシーレコードの修復ステータスメトリクスを表示します。

コンフィグレーションコンプライアンス のユーザー

コンフィグレーションコンプライアンス アクティビティには、さまざまな管理レベルが含まれることがあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- システムアドミニストレーター
- 脆弱性アドミン
- 脆弱性マネージャー
- 脆弱性アナリスト
- コンプライアンスアドミニストレーター

コンフィグレーションコンプライアンス タスクには次のロールが含まれます。

- sn_vulc.admin：読み取り、書き込み、削除が可能
- sn_vulc.write：読み取りと書き込みが可能
- sn_vulc.remediation_owner：アサインされたレコードの読み取りと更新が可能

> **注:**
> sn_vulc.remediation_owner ロールは、ユーザーに itil ロールをアサインすると自動的にアサインされます。

- sn_vulc.read：読み取りが可能

コンフィグレーションコンプライアンス および セキュリティオペレーション

Qualys 脆弱性統合 と Tenable 脆弱性統合 がインストールされると、脆弱性対応 にアクセスできるようになります。これらの統合に複数の展開を含めることができます。各展開から供給されたデータは、GRC の単一インスタンスで識別されて利用可能です。

Yokohama の利用可能バージョン

リリースバージョン	リリースノート
コンフィグレーションコンプライアンス v15.2	コンフィグレーションコンプライアンスリリースノート。 互換性情報については、「KB0856498 脆弱性対応互換性マトリクスおよびリリーススキーマの変更」を参照してください。 アプリケーションのアクティブ化の詳細については、 コンフィグレーションコンプライアンス アプリケーションのセットアップ、インストール、および構成 を参照してください。

コンフィグレーションコンプライアンス インポートデータ

コンフィグレーションコンプライアンス アプリケーションは、サードパーティの統合からポリシー、テスト、信頼できるソース、およびテスト結果をインポートし、表示するためにモジュールに保存します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

サポートされる統合

サードパーティ統合により、構成アセスメントの結果、テストグループ、テスト、テクノロジー、信頼できるソース、テスト結果がコンフィグレーションコンプライアンスアプリケーションにインポートされます。脆弱性マネージャーまたは脆弱性アナリストは、このデータを使用して、資産の構成関連の脆弱性を特定して対応します。

サポートされている統合の詳細については、「コンフィグレーションコンプライアンス の統合」を参照してください。

テストグループ

テストグループは、各種法令・基準等とテストレコードに関連しています。テストグループは、構成テストのグループで定義されます。テストグループは、通常、Windows、Oracle データベース、Cisco IOS などのテクノロジークラスに応じており、多くの場合、主要な業界標準に由来しています。テストグループは、組織のニーズに合わせて変更できます。1 つの構成テストは複数のテストグループに属することができます。

データ連携	説明
Qualys 脆弱性統合	スケジュール済みジョブ (**[Qualys PC** ポリシー]) によって午前 1:00 にテストグループが取得され、コントロール ID が入力されます。 スケジュール済みジョブを表示するには、次に移動します: **Qualys Vulnerability Integration** > プライマリ統合 > **Qualys PC** ポリシー. 注: 統合の手動実行を選択した場合は、最初に **[Qualys PC** ポリシー] を実行します。
Tenable 脆弱性統合	スケジュール済みジョブ [Tenable.io コンプライアンス結果統合] は、ポリシーをインポートします。 統合を手動で実行することを選択した場合、無視された資産をアセスメントデータと調整するまで、次の順序で統合を実行します。 • Tenable.io 資産統合 • Tenable.io コンプライアンス結果統合 • Tenable.io コンプライアンス結果バックフィル統合

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データ連携	説明
	• Tenable.io 資産統合 • Tenable.io コンプライアンス結果バックフィル統合 ポリシーレコードを表示するには、次に移動します: **All** (すべて) > コンフィグレーションコンプライアンス > テストグループ. テストグループレコードを正しく識別して作成するために、テストグループの監査情報がインポートされ、[簡単な説明] フィールドに表示されます。

テスト

テストは、コンピューティング資産のスキャンを整理するデータレコードのライブラリです。構成テストでは、テクノロジー資産のクラスを管理する方法を定義します。

コンフィグレーションコンプライアンス テストは、サードパーティ統合アプリケーションが資産を脆弱性のタイプごとにグループ化するために使用するメカニズムです。Qualys のような一部のサードパーティ VA スキャンソリューションには、信頼できるソースのポリシーと「フレームワーク」にマッピングされた非常に大規模なテストライブラリ (8,000 にも及ぶ) があります。

テストには、1 対多、予想値対実際値など、多くの値を含めることができます。テストとは、準拠していないソフトウェアまたはハードウェア資産のクラスを識別するために使用できるものです。たとえば、リリース番号やハードウェア番号などです。

統合	説明
Qualys 脆弱性統合	スケジュール済みジョブ **[Qualys PC** コントロール] がテストを取得します。スケジュール済みジョブを表示するには、次に移動します: **Qualys Vulnerability Integration** > プライマリ統合 > **Qualys PC** コントロール. **注:** 統合の手動実行を選択した場合は、**[Qualys PC** ポリシー] の後で **[Qualys PC** コントロール] を実行します。
Tenable 脆弱性統合	スケジュール済みジョブ [Tenable.io コンプライアンス結果統合] は、構成テスト (テスト) をインポートします。 統合を手動で実行することを選択した場合、無視された資産をアセスメントデータと調整するまで、次の順序で統合を実行します。 • Tenable.io 資産統合 • Tenable.io コンプライアンス結果統合 • Tenable.io コンプライアンス結果バックフィル統合

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統合	説明
	• Tenable.io 資産統合 • Tenable.io コンプライアンス結果バックフィル統合 構成テストレコードを表示するには、次に移動します: コンフィグレーションコンプライアンス > テスト. レコードでは、インポートされたデータが [簡単な説明] フィールドと [修復ステータス]、 [説明]、および [修復] タブに表示されます。データは、[引用]、[ポリシー]、および [テスト結果] の関連リンクにも表示されます。

テクノロジー

サードパーティの脆弱性スキャナーが、ソフトウェアとハードウェアの構成アイテムを分析するためのテストグループを作成する際に用いる手法の 1 つに、テクノロジーごとに整理する方法があります。テクノロジーとは、ポリシーに関連付けられている OS、ネットワークデバイス、データベース、およびアプリをインポートしたライブラリのことです。テストには、さまざまなテクノロジーに対応した複数の実装があります。修復もテクノロジーによって異なります。

テストに適用されるテクノロジーを表示することで、コントロールがどのようなソフトウェアまたはハードウェア資産に適用できるかをよく知ることができます。コントロールに適用できるテクノロジーの例には、CentOS 7.x、Windows 8.1、Windows 2016 Server などがあります。テクノロジーのリストは読み取り専用で、Qualys クラウドプラットフォーム アプリケーションで定義されているテクノロジーと一致します。

テクノロジーは、データベース関連の構成アセスメントのためにのみインポートされます。インポートの *db_type* (空でない場合) は、テクノロジーを作成するために使用されます。構成テストレコード、テスト結果レコード、ポリシーレコードなど、[テクノロジー] セクションに入力されたテクノロジーを表示します。 コンフィグレーションコンプライアンス > サポートデータ > テクノロジー.

各種法令・基準等

コンフィグレーションコンプライアンス は、テストの脆弱性アラートを生成するときに信頼できるソースと引用を使用します。通常、信頼できるソースは、「NIST 800-53 version 3 (2009) 3: 2009, SA-4」などの公開された業界標準のセクションにマッピングされます。

注:
Qualys 脆弱性統合 では、この組み合わせをフレームワークと呼びます。

信頼できるソースと引用 (指令とも呼ぶ) は、サードパーティの脆弱性スキャナーからインポートされます。

これらの信頼できるソースレコードには、コンピューターセキュリティの分野のエキスパートからの既知のソフトウェアおよびハードウェア構成の問題に関する情報が含まれています。これらは、セキュリティ方針と手順の要件を定義します。構成テストでは、引用を通じて複数の信頼できるソースを参照できます。信頼できるソースは、監査に備え、指定された基準に対するコンプライアンスについて報告できます。

統合	説明
Qualys 脆弱性統合	スケジュール済みジョブ **[Qualys PC** ポリシーの詳細 **(Qualys PC Policies Detail)]** は、信頼

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

統合	説明
	できるソースと引用を取得します。このスケジュール済みジョブを表示するには、次に移動します: **Qualys Vulnerability Integration** > プライマリ統合 > **Qualys PC** ポリシーの詳細. 注: 統合の手動実行を選択した場合は、**[Qualys PC** ポリシー] の後で **[Qualys PC** ポリシーの詳細 **(Qualys PC Policies Detail)]** を実行します。
Tenable 脆弱性統合	スケジュール済みジョブ [Tenable.io コンプライアンス結果統合] は、信頼できるソースを引用データの一部としてインポートします。 統合を手動で実行することを選択した場合、無視された資産をアセスメントデータと調整するまで、次の順序で統合を実行します。 • Tenable.io 資産統合 • Tenable.io コンプライアンス結果統合 • Tenable.io コンプライアンス結果バックフィル統合 • Tenable.io 資産統合 • Tenable.io コンプライアンス結果バックフィル統合 データは、構成テストレコードの [引用] 関連リンクに表示されます。

テスト結果

コンフィグレーションコンプライアンス はテスト結果を計算しませんが、サードパーティ統合の一部としてインポートします。コンフィグレーションコンプライアンスで表示できるようになると、[修復タスク] を使用して修正されます。詳細については、「コンフィグレーションコンプライアンス の相関」を参照してください。

統合	説明
Qualys 脆弱性統合	テスト結果は、次のいずれかの方法で取得できます。 スケジュール済みジョブ **[Qualys PC** 結果] がテスト結果を取得します。このスケジュール済みジョブを表示するには、次に移動します: **Qualys Vulnerability Integration** > プライマリ統合 > **Qualys PC** 結果.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統合	説明
	注: 統合の手動実行を選択した場合は、**[Qualys PC** ポリシー] および **[Qualys PC** ポリシーの詳細 **(Qualys PC Policies Detail)]** の後で **[Qualys PC** 結果] を実行します。 **[Qualys PC** 結果] インポートでは、[統合の詳細] タブの *Start Time* パラメーターを使用します。他のすべての コンフィグレーションコンプライアンス インポートでは、*Start Time* に関係なく、利用可能なすべてのデータが取り込まれます。 **[Qualys PC** 結果] インポートが完了すると、インポート終了の計算をトリガーするイベントが発生します。詳細については、「コンフィグレーションコンプライアンス のステータス」を参照してください。 または、V14.5 以降では、次の統合を実行してテスト結果を取得することもできます。 • Qualys PCRS ポリシーホスト統合:各ポリシーのホスト ID を取得します。このスケジュール済みジョブを表示するには、[Qualys Vulnerability Integration] > [プライマリ統合] > [Qualys PCRS ポリシーホスト統合 (Qualys PCRS Policy Host Integration)] に移動します。 注: 統合の手動実行を選択した場合は、[Qualys PC ポリシー] および [Qualys PC ポリシーの詳細 (Qualys PC Policies Detail)] の後で [Qualys PCRS ポリシーホスト統合 (Qualys PCRS Policy Host Integration)] を実行します。 このスケジュール済みジョブが完了すると、Qualys PCRS テスト結果統合が自動的にトリガーされます。 • Qualys PCRS テスト結果統合:各ホスト ID のテスト結果を取得します。このスケジュール済みジョブを表示するには、 [Qualys Vulnerability Integration] > [プライマリ統合] > [Qualys PCRS テスト結果統合 (Qualys PCRS Test Results Integration)] に移動します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統合	説明
	注: 統合の手動実行を選択した場合は、[Qualys PC ポリシー]、[Qualys PC ポリシーの詳細 (Qualys PC Policies Detail)]、および [Qualys PCRS ポリシーホスト統合 (Qualys PCRS Policy Host Integration)] の後に [Qualys PCRS テスト結果統合 (Qualys PCRS Test Results Integration)] を実行します。 この統合では、[統合の詳細] タブの [開始時間] パラメーターを使用します。
Tenable 脆弱性統合	スケジュール済みジョブ [Tenable.io コンプライアンス結果統合] は、テスト結果をインポートします。 統合を手動で実行することを選択した場合、無視された資産をアセスメントデータと調整するまで、次の順序で統合を実行します。 • Tenable.io 資産統合 • Tenable.io コンプライアンス結果統合 • Tenable.io コンプライアンス結果バックフィル統合 • Tenable.io 資産統合 • Tenable.io コンプライアンス結果バックフィル統合 構成テストレコードを表示するには、次に移動します: コンフィグレーションコンプライアンス > テスト結果. レコードでは、インポートされたデータが [テスト] および [構成アイテム] フィールドに表示されます。データは、[必要な値 **(Expected Values)**]、[実際の値 **(Actual Values)**]、および [修復] タブにも表示されます。[修復タスク] および [テスト結果の履歴] の関連リンクが設定されます。

コンフィグレーションコンプライアンス 検出

コンフィグレーションコンプライアンス データは、サードパーティの SCA スキャナーアプリケーションからインポートされます。ソフトウェアとハードウェアのテストグループをデータレコードに構造化し、アセスメントの実施を迅速化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

インポートが完了すると、インポート終了のアクションを示すイベントを送信します。アクティブな修復タスクでは、次のアクションが実行されます。

- 結果が失敗の解決済み修復タスクは、[実装待ち] ステータスに戻ります。
- すべての結果が「合格」となった修正タスクは [クローズ済み] になります。
- アクティブな修復タスクに属しているテスト結果のステータスが更新されます。
- 結果がアクティブな修復タスクに属しているかどうかを示すフラグが更新されます。

コンフィグレーションコンプライアンス の相関

コンフィグレーションコンプライアンス は、非準拠の問題を修復するための優先順位付けとテスト結果のグループ化 (修復タスク) を行います。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

資産中心の優先順位付け

構成スキャンは、多数の検出結果をもたらす可能性があります。最もリスクを低減するために、結果に優先順位を付けます。優先順位には、構成テストの重要度と資産の重要度の両方が含まれます。構成テスト結果の優先順位は、0 ～ 100 スケールのリスクスコアで表されます。リスクスコアを計算する算出グループで、カスタマイズできます。

サードパーティのインポートが完了すると、コンフィグレーションコンプライアンス はインポート終了のアクションを示すイベントを送信します。アクティブな結果グループごとに、次のアクションが実行されます。

- 結果が失敗の解決済み修復タスクは、[実装待ち] ステータスに戻ります。
- すべての結果が「合格」となった修復タスクは、[クローズ済み] になります。
- アクティブな修復タスクに属しているテスト結果のステータスが更新されます。
- 結果がアクティブな修復タスクに属しているかどうかを示すフラグが更新されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクの優先順位

テスト結果が複数のグループに属する場合、優先順位に従ってテスト結果の [ステータス] が導出されます。

[構成テスト **(Configuration Test)**] フォームの [ステータス] および [解決] フィールド、および [テスト結果] フォームの [結果] フィールドは、この優先順位に従って計算されます。

注:

グループメンバーシップの優先順位は、アイテムが構成テストに合格しなかったアイテムにのみ適用されます。[合格] アイテムは、常に [クローズ済み - 修復済み **(Closed - Fixed)**] ステータスになります。

[結果] の値によってステータスが決まります。[クローズ済み - 修復済み **(Closed - Fixed)**] および [クローズ済み - キャンセル済み **(Closed-Canceled)**] ステータスの修復タスクは無視されます。アイテムの状況は、それが属する他のすべての修復タスクの状況から算出されるか、アイテムに他のグループが存在しない場合は [オープン]に設定されます。

Order of Precedence for Test Results belonging to multiple Test Result Groups						
Group A	**Group B**					
	Open	**Under Investigation**	**Awaiting Implementation**	**Resolved**	**Deferred**	**Closed-Invalid**
Open	Open	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Under Investigation	Under Investigation	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Resolved	Resolved	Resolved	Resolved	Resolved	Deferred	Closed-Invalid
Deferred	Deferred	Deferred	Deferred	Deferred	Deferred	Closed-Invalid
Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid

修復タスクの作成

コンフィグレーションコンプライアンス修復タスクは手動で作成されます。

修復タスクを作成し、入力する方法は 2 つあります。

- [修復タスク] モジュールから、[テスト結果] タブに自動入力されるフィルターを使用します。

  この方法は、使用するフィルタリングがわかっている場合に適しています。たとえば、重要度が中以上で、Windows ベースのインフラストラクチャに影響を与え、SAP サプライチェーンアプリケーションにのみ適用される、失敗したすべてのテスト結果をキャプチャします。

- [テスト結果] リストでテスト結果を選択し、[選択した行のアクション...] メニューから修復タスクを作成します。

  この方法は、簡単にフィルタリングできない結果や、修復のためにテスト結果を指定する場合に適しています。たとえば、共通点がない外れ値などです。

注:
[テスト結果] リストから修復タスクを作成し、後でその修復タスクにフィルターを使用することにした場合、元のエントリーは削除され、フィルター結果に置き換えられます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

グループ解除済みのテスト結果

[グループ解除済みのテスト結果 **(Ungrouped Test Results)]** には、アクティブな ([クローズ済み] でない) 修復タスクのメンバーではない、合格していないすべてのテスト結果が含まれます。このモジュールは、インポートが実行され、テスト結果が追加されるか、修復タスクから削除されるたびに更新されます。

コンフィグレーションコンプライアンス に対して検出されたアイテム

資産は、ホストとテスト結果の統合を使用してインポートされると、[CI ルックアップルール] を使用して自動的に構成アイテム (CI) と照合されます。検出されたアイテムにより、資産の識別が CMDB の CI にどのようにマッピングされているかを把握できます。

検出されたアイテムは、[一致 **(Matched)]**、[不一致]、または [再分類] と見なされます。識別された CI は [一致 **(Matched)]** ステータス です。

潜在的な一致の問題を見つけやすくするために、CI に一致した CI ルックアップルールが **[CI** 一致ルール] フィールドに表示されます。

> **注:**
> **[CI** 一致ルール] フィールドサポートは、Qualys 統合でのみ使用できます。

一致が見つからなかった場合は、CMDB の [一致しない *CI]* クラス [sn_sec_cmn_unmatched_ci]、[cmdb_ci_unclassed_hardware]、または [cmdb_ci_incomplete_ip] に CI が作成されます。元の一致しない CI が再分類された場合、そのステータスを反映するために検出されたアイテムレコードが更新されます。詳細については、「一致しない CI」および「一致しない構成アイテムの表示と再分類」を参照してください。

デフォルトでは、[セキュリティオペレーション > **CMDB** > 検出済みアイテム モジュールは一致しない構成アイテムをリストします。フィルターを削除すると、インポートから検出されたすべてのアイテムを表示できます。

[検出されたアイテム] の各フィールドの説明については、「検出されたアイテムフォームフィールド」を参照してください。

コンフィグレーションコンプライアンス の検出されたアイテムの **CI** 変更

プロパティ sn_sec_cmn.update_on_ci_change のデフォルト値は true です。したがって、検出されたアイテムの構成アイテム (CI) が更新されると、テスト結果も更新されます。

> **注:**
> コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

テスト結果の外部 ID が更新され、リスクスコア、アサインルール、修復タスクルール、修復ターゲットルールが再評価されます。同じテストと CI のテスト結果が存在する場合、テスト結果は既存のテスト結果で更新され、現在のテスト結果はサブステート invalidCI でクローズされます。それに応じて作業メモが追加されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

既存のテスト結果の CI を更新しない場合は、プロパティを false に設定します。この場合、CI が変更されると、新しいテスト結果が作成され、既存のテスト結果は invalidCI としてクローズされます。

コンフィグレーションコンプライアンス の一致しない検出されたアイテムを調整する

スケジュール済みジョブを作成して、一致しない検出されたアイテムを調整します。テスト結果を作成する際、作成時に追加された構成アイテム (CI) が古くなることがあります。

始める前に
必要なロール：admin

このタスクについて
CMDB 内の情報が変更された場合は、一致しない CI 情報は調整されません。調整するには、CMDB が最新の CI で更新されたときに、一致しないステータスのテスト結果に CI ルックアップルールを適用します。
スケジュール済みジョブがオンデマンドで実行され、一致しないステータスの検出されたアイテムに CI 一致ルールが再適用されます。ルックアップルールを再適用した後に CI が変更された場合、検出されたアイテムは新しい CI で更新されます。影響を受けるテスト結果も更新されます。詳細については、「コンフィグレーションコンプライアンス の検出されたアイテムの CI 変更」を参照してください。

注:

コンフィグレーションコンプライアンス v24 以降では、システムプロパティ*sn_sec_cmn.skipItemsWithCIDecommissioned*を有効にすることで、サブステートが「CI 廃止」の検出済みアイテムへの CI ルックアップルールの再適用をスキップできます。

手順

1. 次のように移動する。 **All** (すべて) > **Security Operations** >一致しない検出済みアイテムを調整.
2. [バックグラウンドジョブ] ページで、[調整ジョブを作成] をクリックします。
3. フォームのフィールドに入力します。

注:
[パラメーター] フィールドのみを編集できます。

バックグラウンドジョブ

フィールド	説明
数値	一意のジョブ番号。
作成者	ジョブを作成したユーザー。
パラメーター	一致しない検出されたアイテムを調整するパラメーター： ○ limit：調整される検出されたアイテムの最大数。値を入力しない場合、検出された 10,000 アイテムが調整されます。 ○ firstDiscovereditem：調整が必要な最初のディスカバリーアイテム。値を入力しない場合、調整プロセスは最初に検出されたアイテムから開始されます。
状態	バックグラウンドジョブの現在のステータス。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ステータスの説明	バックグラウンドジョブの現在のステータスの説明。
ジョブタイプ	ジョブのタイプ。値は、[一致しない検出されたアイテムを調整] です。
開始時刻	ジョブの開始時刻。
終了時刻	ジョブの完了時刻。
ジョブ期間	ジョブムの完了に要した合計時間。
サブステート	選択したステータスのサブステート。
メモ	処理されたレコードの数。

4. **[Submit]** をクリックします。

注:

- ジョブの実行を停止するには、[キャンセル] をクリックします。
- ホストまたはテスト結果のインポート時に、一致しない CI を調整したり、CI ルックアップルールを再適用したりすることはできません。

コンフィグレーションコンプライアンス の選択した検出されたアイテムに **CI** ルックアップルールを再適用する

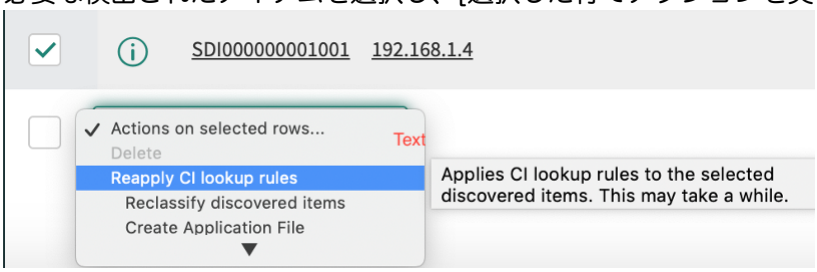
検出されたアイテムのリストビュー選択アクションから、選択した検出されたアイテムに構成アイテム (CI) ルックアップルールを再適用します。アドミニストレーターは、複数の理由についてルックアップルールを編集または更新する必要があります。ルックアップルールが変更された場合は、検出されたアイテムに再適用できます。

始める前に
必要なロール：

このタスクについて
CI ルックアップルールを再適用した後に CI が変更された場合、検出されたアイテムは新しい CI とテスト結果で更新されます。詳細については、「コンフィグレーションコンプライアンス の検出されたアイテムの CI 変更」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > **CMDB** > 検出済みアイテム.
2. 必要な検出されたアイテムを選択し、[選択した行でアクションを実行] をクリックします。



3. リストから **[CI** ルックアップルールを再適用] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

これらの検出されたアイテムにルールが再適用されます。

注:

コンフィグレーションコンプライアンス v15.1.5 以降では、システムプロパティ*sn_sec_cmn.skipItemsWithCIDecommissioned*を有効にすることで、サブステートが「CI 廃止」の検出済みアイテムへの CI ルックアップルールの再適用をスキップできます。

コンフィグレーションコンプライアンス 付きの **Tenable** 脆弱性統合

Tenable 脆弱性統合 の Tenable.io 製品は、コンフィグレーションコンプライアンス アプリケーションで処理するためのポリシー、コントロール (テスト結果)、構成テストをインポートします。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

Tenable.io

Tenable 脆弱性統合 がサポートされています。

インポートされたデータは次の目的で使用できます。

- 構成管理データベース (CMDB) にリストアップされている資産における構成関連の脆弱性を識別します。
- 資産がポリシーとコントロールに準拠していることを確認します。

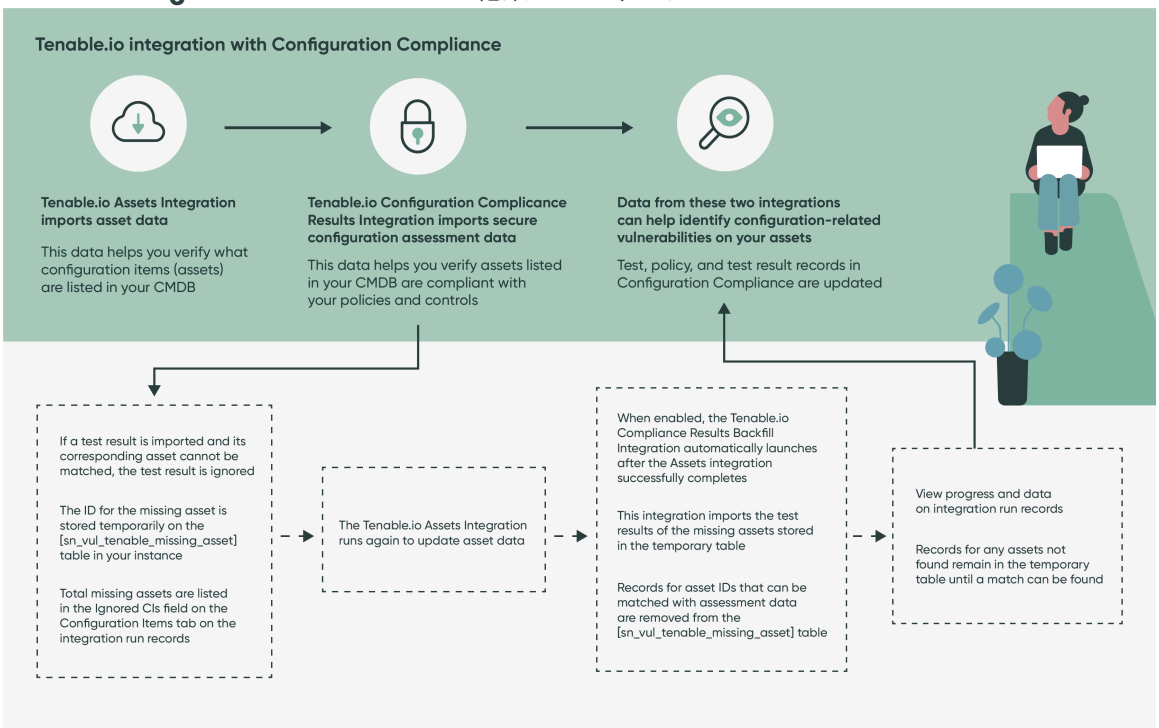
資産データ、ポリシー、コントロール (テスト結果)、および構成テストは、次の統合によってインポートされます。

- Tenable.io 資産統合
- Tenable.io コンプライアンス結果統合
- Tenable.io コンプライアンス結果バックフィル統合

次の図は、資産と構成アセスメントデータをインポートして、インポート時に無視され見落とされた CI を調整するために、どのように統合を行うかを示しています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Secure Configuration Assessment の結果のインポートフロー



データは、コンフィグレーションコンプライアンス アプリケーションのテスト結果、ポリシー、および構成テストのレコードにインポートされ、更新され、表示されます。

Tenable.io 資産統合と Tenable.io コンプライアンス結果統合では、インポートされる構成アイテム (CI) の数が異なる場合があります。このような場合、無視された資産 ID に対して一時的なレコードが作成されて保存されます。これらのレコードは、コンプライアンス結果バックフィル統合からインポートすることによって、インポートされたアセスメントデータと後で照合できます。

たとえば、資産統合では統合実行時に 80 件の資産をインポートし、コンプライアンス結果統合では 100 件の資産をインポートするとします。

注:
統合実行で無視された CI の数を確認するには、次に移動します: **Tenable** 脆弱性統合 > アドミニストレーション > 統合. 統合の名前をクリックしてレコードを開きます。[脆弱性統合実行] 関連リンクで、統合実行レコードを開き、[アイテム] タブを選択して、[無視された **CI]** フィールドの値を確認します。このフィールドは、インポートから無視された (欠落した) 資産の合計を追跡します。

各統合実行レコードの [無視された **CI]** フィールドの値を比較すると、無視された CI に 20 件の差があることがわかります。その結果、前の図に示すように、バックフィル統合が自動的に実行されます。この統合では、コンプライアンス結果統合では見つかったものの、資産統合では見落とされた 20 件の資産について、構成アセスメント情報がインポートされます。欠落した資産のアセスメントデータはインポートされないため、Tenable.io コンプライアンス結果バックフィル統合では、統合実行ごとに最大 200 個の資産 ID をインポートして、欠落した資産と対応するアセスメントデータを調整します。欠落または無視された資産に対して作成され、一時テーブルにリストアップされたすべてのレコードは、これらの資産とそのデータの照合後、削除されます。

注:
無視されたすべての資産をインポートするには、これらの統合を複数回実行する必要があります。

Tenable.io 資産統合を有効にして構成する方法の詳細については、「セットアップアシスタントを使用した Tenable 脆弱性統合の構成」を参照してください。統合の詳細については、「Tenable 脆弱性統合の概要」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.io コンプライアンス結果統合と Tenable.io コンプライアンス結果バックフィル統合は、デフォルトでは非アクティブです。

それらをアクティブ化するには、次の手順を実行します。

1. 次のように移動する。 **Tenable** 脆弱性統合 > アドミニストレーション > 統合.
2. [Tenable 脆弱性統合] リストで、統合名をクリックしてレコードを開き、[アクティブ] チェックボックスをオンにして有効にします。これらの統合を開始するには、スケジュール設定をデフォルト値のままにすることをお勧めします。

コンフィグレーションコンプライアンス サードパーティ脆弱性統合の構成アイテムを識別するための **CI** ルックアップルール

サードパーティ統合からデータをインポートすると、コンフィグレーションコンプライアンス は自動的にホストデータを使用して、構成管理データベース (CMDB) 内で一致するものを検索します。その際に **CI** ルックアップルールを使用します。これらのルールは、構成アイテム (CI) を識別し、それらをテスト結果レコードに追加して修復に役立てるために使用されます。

資産がインポートされると、最初にサードパーティ ID を使用して [検出されたアイテム] リストでルックアップが実行され、構成アイテム (CI) に一致するものが以前のインポートから検索されます。一致するホスト ID が見つかると、テスト結果レコードの [構成アイテム] フィールドとして使用されます。

[検出されたアイテム] リストを使用して、インポートした資産が CI にどのようにマッピングされているかを確認できます。一致するものが見つからない場合、または cmdb_ci フィールドが空の場合、ルールは他のホスト情報を使用して CI を正しく識別しようとします。それでも一致が見つからない場合は、プレースホルダー CI が作成され、[一致しない **CI**] としてマークされます。これらの CI の処理方法に関する詳細については、「Unmatched CIs」を参照してください。

新しく検出されたアイテムが作成され、この CI にマッピングされます。

> **注:**
> CI ルックアップルールは、Qualys Integration for Security Operations でのみ使用できます。

CI ルックアップルールはドメインセパレーションすることができ、ソース固有です。各ソースには複数の展開を含めることができます。Qualys には、Qualys 統合の複数の展開を含めることができます。各展開には、独自の CI ルックアップルールのセットがあります。

> **注:**
> CI ルックアップルールは、脆弱性統合のすべての展開で共有されます。ルールが削除または変更された場合、その削除または変更は脆弱性統合のすべての展開に影響します。

一致を試みる場合、最初のステップは、source、source_instance、およびベンダー ID 間で完全に一致するベンダー ID のルックアップです。次に、ルックアップルールが順番に実行され、ルールが一致する CI を 1 つ返すと停止します。複数の CI を返すようにルールが作成されている場合は、最初に一致したもののみが使用されます。

> **注:**
> 低レベルのネットワーク要素での一致を避けるため、一致した CI が dscy_switchport、cmdb_ci_network_adapter、cmdb_ci_nic、または cmdb_ci_ip_address のいずれかである場合は、親 CI が返されます。

CI クラスを除外するためのシステムプロパティが利用可能です。このプロパティはアップグレードでは使用できません。アップグレード情報とプロパティの設定手順については、「CI クラスの無視」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

一致する問題を見つけやすくするために、一致が見つかったときに、その問題を見つけるために使用された CI ルックアップルールが **[CI** 一致ルール] フィールドの検出されたアイテムレコードに追加されます。ルックアップルールでは、[順番 **(Order)]** 値が最も小さいものから評価されます。

次の Qualys の CI ルックアップルールの一部はベースシステムに付属しています。

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

次の Microsoft Defender の CI ルックアップルールの一部はベースシステムに付属しています。

- S3 バケット
- 名前
- リソース ID

次の Palo Alto Prisma Cloud の CI ルックアップルールの一部はベースシステムに付属しています。

- S3 バケット
- 名前
- リソース ID

テスト結果データのインポートはインスタンスに負荷をかける可能性があり、慎重にルールをビルドしないと、リソースのパフォーマンス問題が発生する可能性があります。CMDB 内で反復して照合を実行するために使用されるロジックでは、処理時間が長くなる可能性があります。リソースの潜在的なデグレードやパフォーマンスの複雑化を回避するために、カスタム作成された CI ルックアップルールまたは事前定義された **CI** ルックアップルールの変更をテストします。孤立レコードの重複防止、データの削除、およびデータのクリーンアップの詳細については、「脆弱性対応 CI ルックアップルールの実行後にレコードが重複または孤立しないようにするための手順」を参照してください。

更新された **CI** ルックアップルールの再適用

CI ルックアップルールを変更する場合は、[CI ルックアップルール] リストページの [変更を適用] をクリックして、検出されたアイテムに対して次のすべてのルールを再実行します。

- 更新されたルールに一致した
- どのルールにも一致しない

ルックアップルールを再適用した後に構成アイテム (CI) が変更された場合、検出されたアイテムは新しい CI で更新されます。テスト結果も更新されます。詳細については、「コンフィグレーションコンプライアンス の検出されたアイテムの CI 変更」を参照してください。

コンフィグレーションコンプライアンス の既存構成アイテムの重複を排除する

重複排除タスクの重複 CI レメディエーターは、sn_sec_cmn_src_ci.cmdb_ci プロパティで更新されます。

重複排除タスクを使用して構成アイテム (CI) を更新するときは常に、その CI に関連する検出されたアイテムも更新されます。したがって、テスト結果は CI で更新されます。詳細については、「コンフィグレーションコンプライアンス の検出されたアイテムの CI 変更」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

識別および調整エンジンを使用して コンフィグレーションコンプライアンス の **CI** を作成する

コンフィグレーションコンプライアンス 11.1 以降では、識別および調整エンジン (IRE) API を使用して、構成管理データベース (CMDB) に構成アイテム (CI) を作成できます。IRE API を使用して CI を作成すると、CI が重複して作成されることを防ぎ、信頼できるデータソースにのみ CMDB への書き込みを許可することで、CI 属性を調整できます。

CI クラス (テーブル) は、インスタンスデータベース内の元のテーブル名です。CMDB には、CI に関するデータを格納する基本システムのクラスが含まれています。

CI の作成に IRE を使用する

バージョン 11.1 より前では、一致する CI が [検出されたアイテム] リストまたは CMDB で見つからなかった場合、CI は [一致しない CI] クラス ([sn_sec_cmn_unmatched_ci]) で作成されていました。

詳細については、「一致しない CI」を参照してください。

バージョン 11.1 以降では、IRE API を使用して CMDB に CI を作成できます。[一致しない CI] クラスを使用する代わりに、 [未分類のハードウェア] または [不完全な IP 識別済みデバイス] クラスで CI が作成されます。

CMDB CI クラス

> **注:**
> 新しいクラスを使用するには、CMDB CI Class Models プラグインをアクティブ化します。それ以外の場合は、CI が [一致しない CI] クラスに作成されます。

バージョン 11.1 以降では、サードパーティのスキャナーからインポートしたホストが [検出されたアイテム] リストまたは CMDB で見つからない場合、次の新しい CMDB CI クラスのいずれかに格納されます。

CMDB CI クラス

CMDB CI クラス	説明
不完全な IP 識別デバイス (cmdb_ci_incomplete_ip)	スキャナーから受信したホスト情報で IP アドレスのみが使用可能な場合は、このテーブルに CI が作成されます。
未分類のハードウェア (cmdb_unclassed_hardware_ci)	スキャナーから受信したホスト情報で以下の情報が使用可能な場合は、このテーブルに CI が作成されます。 • ホスト名 • IP アドレス • DNS • NETBIOS • MAC アドレス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CMDB CI クラス (続く)

CMDB **CI** クラス	説明
	注: MAC アドレスが利用可能な場合、ネットワークアダプタエントリーが作成され、未分類のハードウェア CI に関連付けられます。IP アドレスと MAC アドレスの両方が利用可能な場合、IP アドレス CI が作成され、未分類のハードウェア CI に関連付けられます。

次のいずれかが発生した場合、システムは自動的に [一致しない CI] クラスを使用します。

- CMDB CI Class プラグインがアクティブ化されていません。
- 新しい CI の作成時に IRE が例外を発生させます。

関連情報

CMDB CI クラスモデルストアアプリ

識別および調整エンジン (IRE)

コンフィグレーションコンプライアンス アサインルールの概要

テスト結果が修復のためにアサイン先グループに自動的にアサインされる基準を定義します。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

デフォルトのアサインルール **[CI** サポートグループにアサイン] は、テスト結果を **[CI** サポートグループ] にアサインするベースシステムに含まれています。デフォルトでは非アクティブです。

アサインルールによって設定されたアサイン先グループは、修復タスク (RT) にオーナーをアサインするために [修復タスクルール] によって使用されます。

テスト結果を自動的にアサインする

[次を使用してアサイン] を使用してテスト結果をアサインするには、3 つの異なる方法があります。

- アサイン先グループ：このオプションを使用すると、既存の Now Platform® ユーザーグループを選択できます。
- アサイン先グループフィールド：このオプションを使用すると、cmdb_ci テーブルを使用して利用可能なアサイン先グループフィールドを選択できます。デフォルトでは、次の 3 つのグループフィールドが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- なし：この必須フィールドにデフォルト値がないことを示します
- 構成アイテム：承認グループ
- 構成アイテム：アサイン先グループ
- 構成アイテム：サポートグループ

- スクリプト：このオプションを使用すると、スクリプトを使用して条件を定義できます。このオプションには、コーディングまたは高度な ServiceNow　の専門知識が必要です。

アサインルールの作成の詳細については、「コンフィグレーションコンプライアンス アサインルールの作成または編集」を参照してください。

sn_vulc.remediation_owner ロールを使用すると、自分または自分のアサイン先グループにアサインされたテスト結果や修復タスクを表示および更新できます。モジュールを表示するには、 **All** (すべて) > コンフィグレーションコンプライアンス > テスト結果 > 自分のオープンなテスト結果又は コンフィグレーションコンプライアンス > 修復タスク > 自分のオープンタスク.

sn_vulc.remediation_owner ロールは、ユーザーに直接アサインすることも可能で、ユーザーに itil ロールをアサインすると自動的にアサインされます。

アサインルールの評価プロセス

新しいテスト結果がインポート、またはクローズされてから再度オープンされると、そのテスト結果に対してアサインルールが評価されます。アサインルールは、CI との照合とリスクスコアの算出後に評価されます。テスト結果は、初回インポート時およびルールが変更されたときにのみ自動的に評価されます (クローズされてから再度オープンされた場合を除く)。変更後にルールを手動で再適用することができます。

新規または再オープンされたテスト結果ごとに、次の処理が使用されます。

- テスト結果アサインルールごとに、テスト結果がアサインフィルター (順序が最下位のアサインルールが優先) と比較されます。
- 条件に一致すると、テスト結果にアサイン先グループがアサインされます。ルックアップは停止します。
- すべてのルールで条件が一致しない場合、テスト結果は未アサインの状態のままになります。

アサインルールを再適用する

アサインルールを変更する場合は、[アサインルール] リストページの [変更を適用] ボタンを使用して、すべてのアクティブなオープンテスト結果で変更されたルールを再実行します (手動でアサインされたルールを除く)。

注:
アサインルールは、手動作成されたアサインは再評価しません。

スケジュール済みジョブ [*Reapply all assignment rules*] は、デフォルトでは非アクティブです。アクティブ化すると、手動でアサインされたものを除くすべてのアクティブなルールに対して、すべてのオープンなテスト結果を評価します。[Daily (日次)]、[Weekly (週次)]、[Monthly (月次)]、[Periodically (定期的)]、[Once (1 回)]、または [On Demand (オンデマンド)] で実行できます。

重要:
アドミンおよびアナリストは、Vulnerability Manager ワークスペース で選択したテスト結果の最新のアサインを取得できます。この方法は、クラシック UI でアサインルールを再適用するという時間のかかるプロセスよりも効率的です。詳細については、「Vulnerability Manager ワークスペース でレコードの修復プロパティを再評価」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

アサインルールと修復タスクのアサイン

通常、修復タスク (RT) は、テスト結果と同じアサイン先グループにアサインします。デフォルトでは、これが修復タスクルールで実行されます。

たとえば、RT が構成アイテムクラスでグループ化されている場合、作成された修復タスクは異なるアサイン先グループによって分割できます。グループ 1 には 1 つの Oracle データベースの TRG を、グループ 2 には 1 つの Oracle データベースの TRG をアサインできます。

アサイン先グループが修復タスクレベルで変更されると、同じアサイン先グループを持つ修復タスク内のすべてのテスト結果が新しいアサイン先グループに更新されます。テスト結果は手動アサインとしてマークされ、以降のルール評価の対象にはなりません。

コンフィグレーションコンプライアンス修復タスクからのアサインの削除

自分または自分のグループに誤ってアサインされている可能性があると判断した TRG レコードから、修復タスク (RT) とその関連テスト結果の [アサイン先] フィールドと [アサイン先グループ] フィールドを直接クリアできます。

概要

コンフィグレーションコンプライアンス アプリケーションの v14.3 以降では、修復オーナーは再アサインのためのレコードを [アサイン解除 **(Unassign)]** ボタンで更新できます。

sn_vulc.remediation_owner のユースケース

RT とその関連テスト結果が修復範囲外であると判断した場合、またはレコードが自分または自分のグループに誤ってアサインされていると思われる場合、その修復タスクレコードの [アサイン先] フィールドと [アサイン先グループ] フィールドから自分または自分のグループを削除できます。

モジュールのアサイン解除

[クローズ済み] または [解決済み] 以外の状況の RT レコードには、[アサイン解除] ボタンが表示されます。

[アサイン解除] を選択すると、修復タスクに関連付けられているすべてのテスト結果を再アサインして [未アサイン] アサインタイプに移行するように求められます。

UI ボタンまたは手動で更新したレコードは、コンフィグレーションコンプライアンス の下の [未アサイン (Unassigned)] モジュールに表示されます。

Unassigned UI アクションを使用してレコードを再アサインする方法については、「自分または自分のグループの修復タスクからアサインを削除する」を参照してください。

システムプロパティと通知

sn_vulc.vulnerability_admin ロールを持つアドミンの場合は、レコードで [アサイン解除 **(Unassign)]** を選択すると、デフォルトではシステムプロパティ *sn_vulc.unassign_test_result_group.approval_required* によって、ステータス変更承認レコードと承認要求レコードがトリガーされます。また、要求は承認者の [自分の承認] リストに表示されます。

> **注:**
> 脆弱性アドミニストレーター は、*sn_vulc.unassign_test_result_group.approval_required* システムプロパティを **[false]** に設定して、承認プロセスを無効にできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 承認者が要求を承認すると、デフォルトでは、 システムプロパティ *sn_vulc.default_assignment_group* によって [アサイン先] フィールドと [アサイン先グループ] フィールドがクリアされ、 [アサインのタイプ] フィールドに [未アサイン **(Unassigned)**] と入力されます。脆弱性アドミニストレーターは、アサインフィールドがクリアされ特定のグループがアサインされるように、*sn_vulc.default_assignment_group* システムプロパティの値を変更できます。たとえば、ユーザーがレコードで [アサイン解除] を選択し、それをレビューのために特定のグループにリダイレクトする場合は、選択したグループのシステム ID をシステムプロパティの値フィールドに追加できます。
- 承認者が要求を却下した場合、却下理由が [メモ] タブに表示されます。

または、*sn_vulc.default_assignment_group* が特定のグループに対して設定されていない場合、デフォルトでは、[通知のアサイン解除 (Unassign notification)] ユーザーグループに追加されたユーザーに対し、レコードがアサイン解除されたときにアラートが送信されます。システムプロパティ *sn_vulc.default_notification_group* によって、このグループへの通知が決まります。

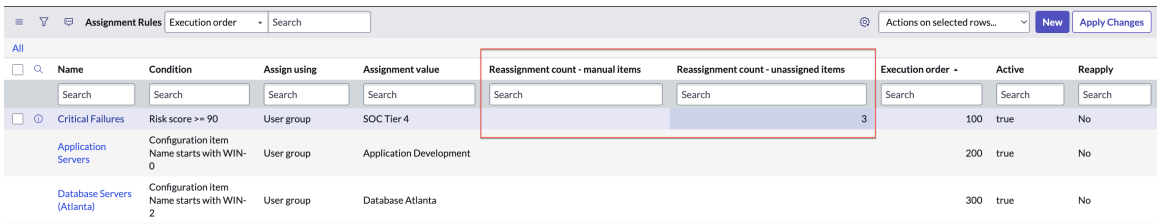
アサインタイプ [手動]、[ルール]、または [未アサイン] は、RT レコードとリストビューから使用できます。アサインタイプ [未アサイン **(Unassigned)**] は、機能のシステムプロパティによって [アサイン先] および [アサイン先グループ] フィールドがクリアされた後に表示されます。

この機能のスケジュール済みジョブによるアサインルールの監視

日次スケジュール済みジョブでは、レコードのアサインタイプが [未アサイン **(Unassigned)**] に移行されるときにレコード数がカウントされます。この数を使用して、脆弱性アナリストは未アサインの RT 数が多いアサインルールに基づいて、パフォーマンスが悪いアサインルールを監視および調整できます。

Reassignment count for assignment rules スケジュール済みジョブは毎日実行され、この機能によって特定のアサインルールに対してアサインされていない RT の合計数を提示します。

このジョブは、手動でアサイン解除されたレコードもカウントします。手動によるカウントとこの機能によって収集されたカウントはともに、脆弱性アサインルールリストの [*Reassignment count - manual items*] と [*Reassignment count - unassigned items*] の 2 つの列に提示されます。



1. 脆弱性アドミニストレーターは、次の場所に移動してこれらの数を表示できます コンフィグレーションコンプライアンス > アドミニストレーション > アサインルール.
2. リストの右上にある歯車アイコンを選択し、表示する [再アサイン回数 - 手動アイテム数] および [再アサイン回数 - 未アサインのアイテム] を選択します。
3. 最初にルールによってアサインされたが、以降に自動または手動で再アサインされた RT には、リストビューに元のルールへの参照が含まれています。

コンフィグレーションコンプライアンス修復タスクとタスクルールの概要

修復タスク (RT) を自動的に作成し、修復タスクルールを使用して結果を一括で分析します。テスト結果を修復タスクに手動でアサインする必要がないように、タスクを形成する基準が構成されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

修復タスクについて

修復タスクは、修復する一連のテスト結果を表します。テスト結果のグループ化には多くの利点があります。修復ステータスを使用してテスト結果を移動したり、調査中としてマークしたり、保留したり、グループを使用してまとめて解決済みとしてマークしたりすることができます。指定した結果、テクノロジー、リスクスコア、およびテスト結果に関連するその他のデータを使用して、すべての結果を自動的にグループ化する条件を作成できます。テスト結果は複数の修復タスクに属することができるため、1 つの修復タスクに対して積極的に作業を行いながら他のグループを監視するといった柔軟性があります。すべて、柔軟な形で同時に実行することが可能です。たとえば、アサイン別にグループ化して、テクノロジーを含むグループを作成することもできます。

修復タスクは次のように作成されます。

- 2 つのオプションのいずれかを使用して、手動でテスト結果をグループに追加します。
  - 手動：エントリーなしで修復タスクを作成します。テスト結果は手動で追加する必要があります。
  - フィルター：修復タスクを作成し、条件を使用してテスト結果をその修復タスクに自動的に追加します。

  注:
  手動で追加されたテスト結果は、修復タスクルールまたは修復タスク条件によって自動的に修復タスクから削除されることはありません。

- 修復タスクルールを使用して自動的にこのオプションは最も簡単なオプションです。一度構成すると、修復タスクルールによって必要なすべての修復タスクが作成されます。

修復タスクから、テスト結果のグループをユーザーにアサインしたり、後日まで保留にしたり、[変更要求] の作成に使用したり、使い方は様々です。

注:

sn_vulc.remediation_owner ロールを使用すると、自分または自分のアサイン先グループにアサインされたテスト結果や修復タスクを表示および更新できます。モジュールを表示するには、 **All** (すべて) > コンフィグレーションコンプライアンス > テスト結果 > 自分のオープンなテスト結果又は コンフィグレーションコンプライアンス > 修復タスク > 自分のオープンタスク.

新しいテスト結果を修復タスクに追加できると判断されると、テスト結果は修復タスクの [テスト結果] 関連リストに含められます。

修復タスクのステータスを更新すると、関連するテスト結果ではステータスをこの修復タスクに合わせて更新できます。ステータス変更の詳細については、「コンフィグレーションコンプライアンスのステータス」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクルールについて

修復タスクルールを使用すると、テスト結果を自動的にグループ化してアサインする方法を定義できます。テスト結果の [アサイン先グループ] および [テスト] フィールドを基づきテスト結果をグループ化するベースシステムには、デフォルトルールである [アサイン先グループ、テスト **(Assignment group, Test)]** が含まれています。このルールはデフォルトで無効になっています。テスト結果からアクセス可能な列では、値の他のセットでグループ化できます。キーは最大 6 つまで、条件はいくつでも使用できます。詳細については、「コンフィグレーションコンプライアンス 修復タスクルールの作成または編集」を参照してください。

重要:
管理者およびアナリストは、脆弱性マネージャーワークスペースで選択したテスト結果の修復タスクルールを評価できます。この方法は、時間のかかるクラシック UI で修復タスクルールを再適用するよりも効率的です。詳細については、「Vulnerability Manager ワークスペース でレコードの修復プロパティを再評価」を参照してください。

たとえば、アサイン先グループまたはテクノロジー、構成アイテム (CI) 別にテスト結果をグループ化できます。会社がより大きなリスクにさらされるテスト結果には、別のルールセットを使用できます。低重大度または低リスクの CI に対して、1 つの修復タスクルールを設定できます。使用可能なフィールドの詳細については、「コンフィグレーションコンプライアンス テスト結果の表示」を参照してください。

新しいテスト結果がインポート、またはクローズされてから再度オープンされると、そのテスト結果に対して修復タスクルールが評価されます。テスト結果は、クローズ後に再オープンされない限り、1 回しか評価されません。

修復タスクルールは、CI との照合、リスクスコアの算出、アサインルールの後で評価されます。

新規または再オープンされたテスト結果ごとに、次の処理が使用されます。

- 修復タスクルールごとに、テスト結果が条件フィルターと比較されます。
- ルール条件が一致する各ルールについて、テスト結果のグループキー列からデータがプルされます。このルールでは、テスト結果と同じアサイン先グループにアサインされている、一致するオープン修復タスクがあるかどうかを確認します。

  修復タスクが見つかった場合、テスト結果は [オープン **]** ステータスの既存の修復タスクに追加されます。

- [オープン] ステータスの修復タスクが見つからない場合は、ルールによって修復タスクが作成され、ルールの [ユーザーグループ] または [キー] の値に基づいてアサインされ、そこにテスト結果が配置されます。

複数のテスト結果ルールを定義して、さまざまな種類の結果をグループ化できます。各結果は修復タスクに配置される前にルール条件と比較されるため、ルールが多すぎるとパフォーマンスに影響を与える可能性があります。

修復タスクルールが削除されると、そのルールによって作成されたすべてのオープンタスクを削除することができます。これは、ルールのフォームビューとリストビューの両方に適用されます。

修復タスクがアサインされたり変更されたりすると、テスト結果が RT と異なるアサイン先グループである場合を除き、[アサイン先グループ] フィールドと [アサイン先] フィールドがロールダウンしてすべてのテスト結果が表示されます。アサインルールについては、「コンフィグレーションコンプライアンス アサインルールの概要」を参照してください。これらのアサインは、次のインポート時にこのグループに対して自動的に使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テスト結果と修復タスクの保留数を追跡する

v14.3 以降では、テスト結果または修復タスクが複数の保留モジュールで保留された回数を追跡します。スケジュール済みジョブである [保留数の設定 **(set deferral counts)**] は毎日実行され、複数の保留モジュールにリストされているレコードの [保留数] 列で複数回保留されたレコード数が提示されます。

コンフィグレーションコンプライアンス の算出グループと算出を設定する

コンフィグレーションコンプライアンス算出は、事前定義された条件が満たされたときにレコード値を更新するために使用されます。算出は、レコードの更新方法を決定するために使用される基準に基づいてグループ化されます。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

コンフィギュレーションコンプライアンスの算出

コンフィギュレーションコンプライアンスアプリケーションには、リスク算出とリスクスコアロールアップ算出の 2 つのタイプがあります。これらの算出グループはデフォルトで有効になっています。

リスクスコア算出グループは、リスク算出に名称変更されました。

リスクスコアロールアップ算出には、構成テストと修復タスクのロールアップ算出が含まれています。

テスト結果および修復タスクの修復のためのリスク算出およびロールアップ算出の設定には、次のタスクが含まれます。

- リスク算出の作成
- リスクスコアロールアップ算出の作成

リスク算出を作成すると、次のデータの取り込みで計算が可能になります。作成後に、オンデマンドで適用することもできます。

算出および算出グループの詳細については、「コンフィグレーションコンプライアンス 算出グループ」を参照してください。

コンフィグレーションコンプライアンス の例外管理の概要

公開されている脆弱性管理やセキュリティポリシー、標準、指針に組織が準拠できない場合は、例外を要求できます。例外管理では、ポリシーに従って修復できない修復タスクに対する例外の要求、レビュー、承認、または却下を行います。

重要:
例外管理は、 脆弱性マネージャーワークスペース と IT 修復ワークスペースでサポートされています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

脆弱性によっては、既存のパッチ、修正、またはソリューションがないこともあります。例外が承認されるということは、構成関連の脆弱性を修復しなかった場合の結果を認識し、同意していることになるため、リスクを受け入れているということでもあるのです。

例外のライフサイクル

例外は、修復タスクの修復を指定した期間保留することを要求するものです。

例外のライフサイクルは次のとおりです。

- 例外の要求
- 例外要求を承認する
- 例外要求の追跡
- 例外要求の有効期限

例外の要求

修復オーナーは、例外管理プロセスを使用して、修復タスクの免除を要求できます。承認プロセス中、修復タスクは [レビュー中] ステータスを維持します。例外承認者がこの要求を承認すると、修復タスクは [保留] ステータスに移行します。

重要:
IT 修復ワークスペースから例外を要求できます。詳細については、「IT 修復ワークスペースで例外を要求する」を参照してください。

例外要求を承認する

すぐに修復できない修復タスクは、レビューしてリスク評価され、修復できるまでの保留が承認されます。例外要求の承認は 2 レベルワークフローにすることができます。第 1 レベルの承認者のみが存在する場合、例外を要求して承認できます。ただし、第 1 レベルの承認者がいない場合は、例外を要求できません。詳細については、「コンフィグレーションコンプライアンス の例外承認者を追加する」を参照してください。

重要:
脆弱性マネージャーワークスペースから例外要求を承認または却下できます。詳細については、「で修復タスクとレコードの例外を要求する Vulnerability Manager ワークスペース」を参照してください。

注:

コンフィグレーションコンプライアンス v13.0 以降では、CC アプリケーションを初めて展開する場合は、例外管理のフローデザイナーがデフォルトで有効になります。既にワークフローを使用している場合は、フローデザイナーに更新できます。どちらの場合も、ワークフローに戻すことはできません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

修復タスクの例外要求が承認されると、次のアクションを実行できます。

- 再オープン
- 削除

注:
却下コメントは、修復タスクの作業メモに表示されます。例外要求が却下された場合、この修復タスクは前のステータスに戻ります。

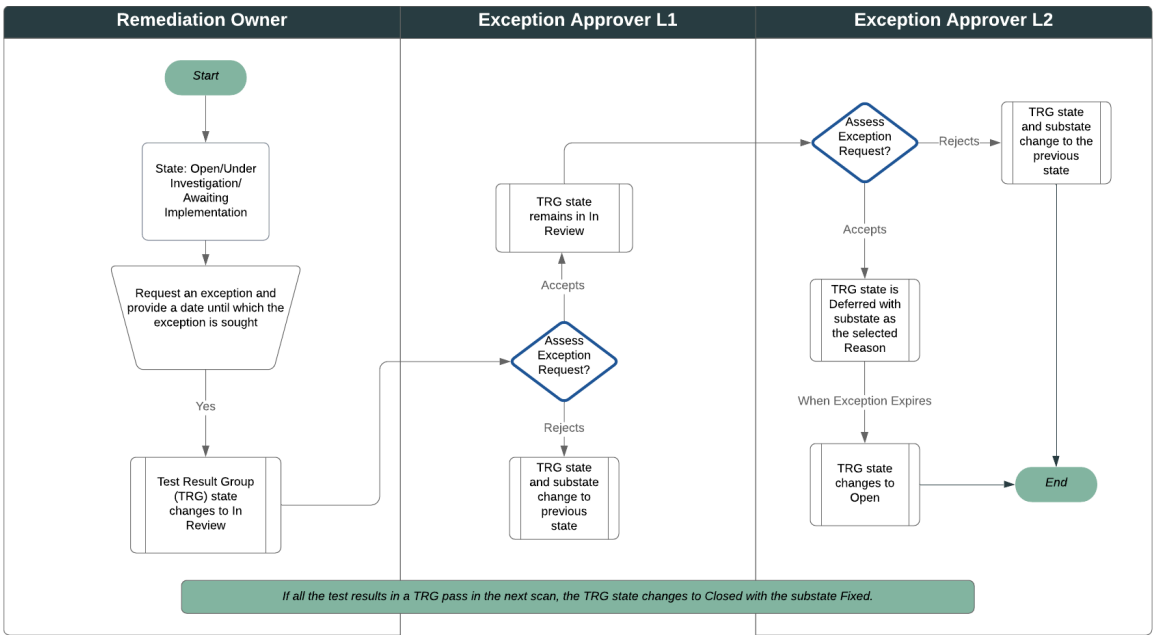
例外要求の追跡

例外が発生した後、修復タスクの [ステータス変更承認] タブを使用してそのステータスを追跡できます。修復タスクに対してアクションが実行された場合、その修復タスクで個々のテスト結果のステータスを追跡することはできません。

例外要求の有効期限

修復タスクの例外要求の有効期限が切れると、修復タスクは [オープン] ステータスに戻ります。

CC v13.0 より前の例外管理承認プロセス



コンフィグレーションコンプライアンス の変更管理

IT 修復オーナーは、コンフィグレーションコンプライアンスアプリケーションの修復タスク (RT) から直接変更要求 (CHG) を作成および管理できます。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

変更要求および コンフィグレーションコンプライアンス のワークフロー

変更要求と変更管理は、コンフィグレーションコンプライアンス のワークフローの修復プロセスに含まれます。この修復フェーズでは、テスト結果の優先順位付け、追跡、および修復を支援するために、変更要求を使用することがあります。

コンフィグレーションコンプライアンス アプリケーションは、Now Platform® の IT 変更管理プロセスと連携して、環境内における非準拠のソフトウェアやテクノロジーの修復を支援します。

コンフィグレーションコンプライアンスアプリケーションの変更管理を使用すると、テスト結果を既存の変更要求に関連付けたり、修復タスクを分割して、選択したテスト結果に対してのみ新しい修復タスクを作成したりできます。

詳細については、「コンフィグレーションコンプライアンスで変更要求を作成する」を参照してください。

主要な用語

テスト

テストは、コンピューティング資産のスキャンを整理するデータレコードのライブラリです。構成テストでは、テクノロジー資産のクラスを管理する方法を定義します。テストとは、準拠していないソフトウェアまたはハードウェア資産のクラスを識別するために使用できるものです。

テスト結果

テスト結果は、サードパーティ統合によってインポートされます。コンフィグレーションコンプライアンスで表示できるようになると、[修復タスク] を使用して修正されます。グループは、アサインルールに従って修復のためにアサインされます。

> **注:**
> コンフィグレーションコンプライアンス のバージョン 14.9 以降では、テスト結果には「結果」というラベルが付いています。

修復タスク

テスト結果はアサインルールに応じて修復タスクにグループ化され、修復のために修復オーナーに自動的にアサインされます。

> **注:**
> コンフィグレーションコンプライアンス のバージョン 14.9 以降では、テスト結果には「修復タスク」というラベルが付いています。

テストグループ

テストグループは、各種法令・基準等とテストレコードに関連しています。テストグループは、構成テストのグループで定義されます。

変更要求

変更要求によって、修復のための制御プロセスを実装することができます。コンフィグレーションコンプライアンスの修復タスクで変更要求を使用すると、追加のリソースを必要とする、または保留の対象となる非準拠の資産 (構成アイテム) を識別、追跡、および解決することができます。

テスト結果と修復タスクの詳細については、「コンフィグレーションコンプライアンス修復タスクとタスクルールの概要」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンフィグレーションコンプライアンス で変更要求を使用する場合

変更要求によって、テスト結果の修復アクティビティを開始および追跡することができます。修復オーナーが未修復のテスト結果または構成アイテムを多数持っている場合は、変更要求を使用して保留するテスト結果を識別できます。または、元の修復タスクで最初に識別されたよりも多くのリソースを必要とするテスト結果と構成アイテムを識別して、再グループ化することもできます。

修復タスクから変更要求を作成する

修復タスク内ですべてのテスト結果に対する修復タスクから変更要求を直接作成するか、フィルタリングを使用して特定の基準に一致するテスト結果のみを特定します。事前設定された情報を使用して変更要求を作成し、手動での介入が必要なテスト結果の調査を迅速化します。

修復タスクの分割

既存の修復タスクから、新しい修復タスクに移動するテスト結果のサブセットを特定します。新しい TRG を作成することで、元の修復タスクに影響を与えることなく、特定のテスト結果グループを処理できます。

テスト結果を既存の変更要求に関連付ける

テスト結果を既存のタスクに関連付けて、修復タスクを解決するときに重複する変更要求が作成されないようにします。インスタンスで既に利用可能な変更要求に修復タスクを関連付けることで、タスクの既存リストを使用できます。

修復タスクの変更要求のタイプ

アサインされた修復タスクから、変更要求を直接作成、承認、実装、レビュー、およびクローズすることができます。修復タスクから事前入力された情報を使用して、次の 3 つのタイプの変更要求を作成できます。

- 標準。事前に承認された、リスクの低い、比較的一般的な変更を指し、指定された手順または作業指示書に従って行います。
- 通常。通常の変更要求は、実装、レビュー、およびクローズする前に 2 レベルの承認が必要な規範的なプロセスに従います。
- 緊急。重大なインシデントを解決するための変更。

コンフィグレーションコンプライアンス アプリケーションのセットアップ、インストール、および構成

Now Platform® インスタンスでアプリケーションを実行する前に、ServiceNow® Store から コンフィグレーションコンプライアンス アプリケーションを最初にダウンロードしてインストールする必要があります。このアプリケーションは別のサブスクリプションとして利用できます。

インストールの前に、次の表に示されたセットアップチェックリストのステップを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

コンフィグレーションコンプライアンス アプリケーションのリリースバージョン、それと互換性のあるサードパーティアプリケーションや ServiceNow アプリケーションについて詳しくは、HI ナレッジベースの「Vulnerability Response Compatibility Matrix and Release Schema Changes (脆弱性対応互換性マトリクスおよびリリーススキーマの変更) [KB0856498]」の記事を参照してください。

ストアアプリのエンタイトルメント取得の詳細については、「セキュリティオペレーション および ServiceNow Store」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリストタスクのセットアップ

セットアップタスク	説明
インスタンスに必要な ServiceNow ロールがあることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。 • まだアサインされていない場合、システムアドミニストレーター [admin] は、アプリケーションをインストールし、コンフィギュレーションコンプライアンスアドミニストレーター [sn_vulc.admin] ロールをアサインします。 • コンフィギュレーションコンプライアンスアドミニストレーター [sn_vulc.admin] は、設定の監視、予想される結果の検証を行います。 • 修復オーナー [sn_vulc.remediation_owner] は、アサインされたレコードの読み取りと更新を行います。sn_vulc.remediation_owner ロールは、ユーザーに itil ロールをアサインすると自動的にアサインされます。
サポートされる統合	コンフィグレーションコンプライアンス を使用して構成アイテムを修復する前に、サードパーティのスキャナー統合をインストールし、少なくとも 1 回のネットワークスキャンを実行する必要があります。 サポートされているサードパーティ統合を設定する前に、脆弱性対応 アプリケーションがインストールされてアクティブ化されていることを確認してください。「脆弱性対応 のインストール」を参照してください。 統合アプリケーションがインストールされ、アクティブ化されていることを確認するには、次の場所に移動します サブスクリプション管理 > サブスクリプション インスタンス内にありますリストには、組織で購入したサブスクリプションが表示されます。 サードパーティ統合とサポートされている製品のリストの詳細については、「コンフィグレーションコンプライアンス の統合」を参照してください。

Qualys 脆弱性統合

- Qualys 脆弱性統合 が既にシステムにインストールされており、API 認証情報が コンフィグレーションコンプライアンス で使用するものと異なる場合は、(脆弱性対応 内の) セットアップアシスタントに移動し、各 **Qualys PC** 統合にアサインします。
- 次のように移動する。 **Qualys Vulnerability Integration** > プライマリ統合 をクリックし、[**Qualys REST** 詳細] タブの [**Qualys API** 認証情報] フィールドを編集します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Qualys 脆弱性統合 の詳細については、「Qualys 脆弱性統合の概要」を参照してください。

これで、コンフィグレーションコンプライアンス アプリケーションをインストールする準備ができました。「コンフィグレーションコンプライアンス のインストール」を参照してください。

コンフィグレーションコンプライアンス のインストール

Now Platform® インスタンスで コンフィグレーションコンプライアンス を実行する前に、ServiceNow Store から コンフィグレーションコンプライアンス アプリケーションを最初にダウンロードしてインストールする必要があります。このアプリケーションは別のサブスクリプションとして利用できます。

始める前に

インストールの前に、「 コンフィグレーションコンプライアンス アプリケーションのセットアップ、インストール、および構成 」で説明されているセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。必要なロール:admin

手順

1. ServiceNow製品にオプトインするには、Opt in to the ServiceNow Store products の手順に従います。
2. ServiceNow Store から購入したアプリケーションをインストールするには、「Install a ServiceNow Store application 」の手順に従います。
3. オプション: または、他の Now Platform インスタンスで コンフィグレーションコンプライアンス アプリケーションのエンタイトルメントを管理する場合は、「Manage entitlements from your ServiceNow instance 」の手順に従います。
4. コンフィグレーションコンプライアンスアプリケーションを既にインストールしていて、更新する場合は、「Install an update to a ServiceNow Store application 」を参照してください。
5. サポートされているアプリケーションをインストールします。

   個別のサードパーティアプリケーションが コンフィグレーションコンプライアンスでデータを取得および変換します。コンフィグレーションコンプライアンス を使用して構成アイテムを修復する前に、サードパーティのスキャナー統合をインストールし、少なくとも 1 回のネットワークスキャンを実行する必要があります。

   コンフィグレーションコンプライアンス のサードパーティ統合のインストールについては、「コンフィグレーションコンプライアンス の統合」を参照してください。

コンフィグレーションコンプライアンス アサインルールの作成または編集

フィルター条件に基づいてテスト結果を自動的にアサインするルールを作成します。これらのルールは、インポート時にテスト結果をアサインするものです。

始める前に

必要なロール：sn_vulc.admin

このタスクについて

ベースシステムには、**[CI** サポートグループにアサイン] という 1 つの コンフィグレーションコンプライアンス アサインルールが付属しています。このルールは、CI サポートグループと同じアサイン先グループにテスト結果をアサインします。デフォルトでは、このルールは非アクティブです。フィルター条件を使用して変更できます。アサインルールでは、1 つ以上のアサインの条件と実行順序を定義します。テスト結果がルール条件に一致すると、アサインルックアップは停止します。

注:
新規または更新されたルールは、次回のインポート時に自動的に評価されるか、[アサインルール] リストの [変更を適用] ボタンを使用して手動で評価されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > アサインルール.
2. **[CI** サポートグループに割り当て] ルールを開くか、[新規] をクリックします。
3. **[CI** サポートグループにアサイン] ルールを編集するか、[新規] の場合は、必要に応じてフォームのフィールドに入力します。

コンフィグレーションコンプライアンスアサインルール

フィールド	説明
名前	アサインルールの名前。
実行順序	このルールが評価される順番。最も小さい番号が最初に評価されます。 最優先のルール (リスクが重要で、特別な処理が必要なテスト結果、または規制コンプライアンスで処理されるべきテスト結果など) が最初に実行されます。次に、一般的なルールを実行します。この場合、特別な処理は必要なく、誰が責任を負うべきかがわかっています。最後に、テスト結果が属するべきアサイン先グループを決定するグループに、テスト結果をアサインするためのデフォルトルールを作成します。このグループは、決定を対象に別のルールを追加できます。このデフォルトルールは最後に実行されます。
有効	アサインルールがアクティブかどうかを示します。
条件	
条件フィールド	満たす必要がある条件。 条件ビルダーに入力した検索テキストの大文字と小文字の区別は、このレコードまたはフォームではサポートされていません。
新しい基準	選択する条件フィルターフィールドを追加します。
説明	アサインルールを説明するテキスト。
次を使用してアサイン	このルールに基づいて作成されたグループのアサインを自動化するには、利用可能なオプションの 1 つを選択します。 ○ ユーザーグループ：ルックアップテーブルからユーザーグループを選択します。 ○ ユーザーグループフィールド：ドロップダウンメニューからユーザーグループフィールドを選択します。 ○ スクリプト：スクリプトを作成または編集します。 **注:** スクリプトの作成または編集には ServiceNow の専門知識が必要です。
ユーザーグループ	アサインルールの条件に一致するテストの修復を担当するユーザーグループを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
フィールド	

4. **[Submit]** をクリックします。

コンフィグレーションコンプライアンス の修復ターゲットルール

修復ターゲットルールを使用すると、テスト結果を修復する予定期間を設定できます。目標期日が近づいたとき、および期限が過ぎているときに、ユーザーとグループに通知を送信できます。

重要:
コンフィグレーションコンプライアンスのアドミニストレーターまたはアナリストは、脆弱性マネージャーワークスペースで特定のテスト結果セットの最新の修復ターゲット日を取得できます。この方法は、時間のかかるクラシック UI で修復ターゲットルールをすべてのテスト結果に対して実行するよりも効率的です。詳細については、「Vulnerability Manager ワークスペース でレコードの修復プロパティを再評価」を参照してください。

必要なロール：コンフィグレーションコンプライアンスアドミニストレーター (sn_vulc_admin)、または sn_vulc.manage_remediation_target_rules ロールを持つマネージャー。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

修復ターゲットルール

スケジュール済みジョブである *Evaluate and notify remediation targets* は毎日実行され、アクティブな修復ターゲットルールを使用してアクティブなテスト結果レコードを評価します。修復タスクに関連付けられたテスト結果レコードが更新または変更されるたびに、変更された値がターゲットルールによって評価され、関連する修復タスクに変更がロールアップされて表示されます。

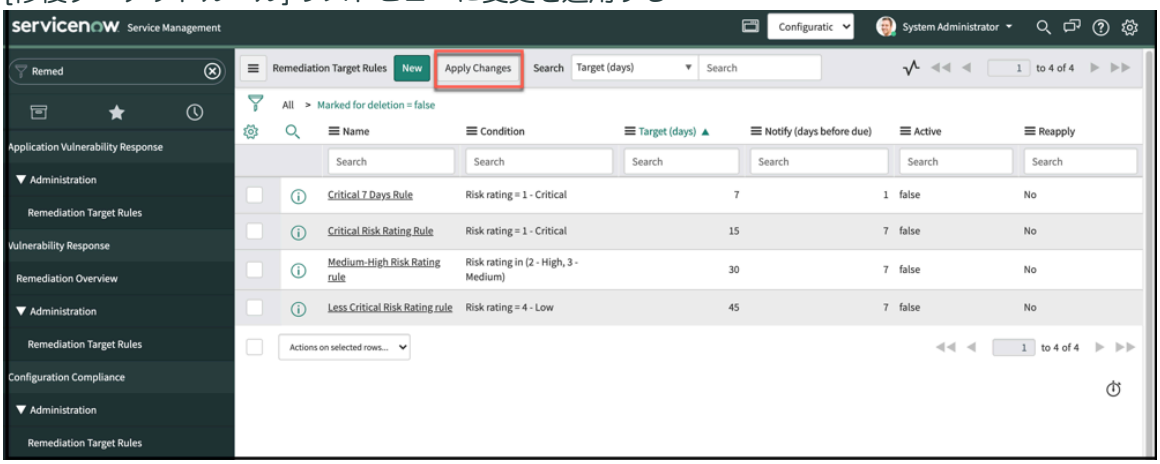
既存の修復ターゲットルールの編集、無効化、または削除を行ったり、新しいルールを作成したりできます。ルールを変更、無効化、または新しいルールを作成する場合は、[修復ターゲットルール] リストビューから [変更を適用] をクリックし、次のスケジュール済みジョブの前に導入した変更を手動で適用することができます。このオプションを使用すると、待機することなく、テスト結果レコードを再評価できます。変更を手動で適用しない場合は、次の日次スケジュール済みジョブが変更を取得して適用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > 修復ターゲットルール 修復ターゲットルールを表示します。

[修復ターゲットルール] リストビューに変更を適用する



2. [名前] 列でルールをクリックしてレコードを開きます。
3. 修復ターゲットルールレコードの [アクティブ] チェックボックスをオンにして、無効なルール (false) を有効 (true) にします。

ターゲットルールを変更または追加する場合は、変更を手動で適用するか、次のスケジュール済みジョブまで待機するかに関係なく、その変更は、変更によって影響を受ける他のターゲットルールとともにすべてのアクティブなテスト結果を評価するために使用されます。変更を手動で適用する場合、変更によって影響を受けるすべてのルールが評価に使用されるため、アクティブなテスト結果が大量にある場合、この評価には時間がかかることがあります。

たとえば、ターゲット修復日数のデフォルト値は 30 です。ターゲット修復日数が 30 日の新しいルールを作成した場合、このルールと、ターゲット日が 30 日以上のターゲットルールがそれぞれテスト結果に適用されます。

非アクティブ化および削除されたターゲットルール

ルールがアクティブな場合、[修復ターゲットルール] リストビューの [アクティブ] 列に true が表示されます。ルールを非アクティブ化 (false) すると、新しいテスト結果には適用されなくなります。ただし、スケジュール済みジョブは、ルールが適用された既存のテスト結果のトラッキングを続行します。非アクティブ化されたルールが後で再アクティブ化されると、[修復ターゲット日] フィールドが空のテスト結果が再アクティブ化されたルールに対して評価されます。これには、ルールが非アクティブ化されたときに作成されたテスト結果が含まれます。

ルールが削除されると、クローズされたテスト結果の [修復ターゲット日] と関連フィールドは保持されます。クローズされていないテスト結果の [修復ターゲット日] と関連フィールドはクリアされ、依存ルールが再適用されます。

ルールを非アクティブ化にするには、修復ターゲットルールレコードで [アクティブ] チェックボックスをオフにし、[更新] をクリックします。[修復ターゲットルール] リストビューの [アクティブ] 列に false が表示されます。

ルールを削除するには、フォームで [削除] をクリックするか、またはリストビューからルールを選択し、[行アクション] リストから [削除] をクリックします。ルールはリストに表示されなくなり、操作順序の次のルールが削除されたルールに置き換わります。

ルールを非アクティブ化または削除し、次のスケジュール済みジョブの前に変更を適用することを選択した場合、ルール参照はフィールドからクリアされますが、修復日とステータスデータは保持され

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ます。変更を手動で適用しない場合、ルール参照は次のスケジュール済みジョブでフィールドからクリアされます。

ターゲットルールおよびスケジュール済みジョブ [修復ターゲットの評価と通知 **(Evaluate and notify remediation targets)]** について

スケジュール済みジョブ [*Evaluate and notify remediation targets*] は、毎日 4:30:00 に 1 回実行されます。アクティブな修復ターゲットルールが選択され、最も早い修復ターゲット日のテスト結果からアクティブなすべてのテスト結果が評価されます。次の基準を満たすすべてのテスト結果が評価されます。

- [クローズ済み] ステータスではない。
- 修復ターゲット日がない。
- 修復ターゲットルールの日付より後の修復ターゲット日がある。
- スキャナーインポートが完了した後に作成されている。スケジュール済みジョブは、インポートの結果として作成された新しいテスト結果を選択して、評価する。

ターゲットルールが定義されると、修復ターゲット日がスケジュール済みジョブ [*Evaluate and notify remediation targets*] によって算出されます。スケジュール済みジョブは、修復ターゲット日が存在しない場合は追加し、このルールにレコード内の日付よりも前の日付が含まれている場合は、既存のターゲット日を更新します。

期限切れのレコードとリマインダー日がターゲットルールに一致するものは、ジョブによって選択され、通知が送信されます。無効なルールの場合、ジョブはテスト結果レコードの修復フィールドをクリアし、通知の送信を停止します。

sn_sec_cmn.evaluate_targetmissed_records プロパティを有効にすると、 *Evaluate and notify remediation targets* スケジュール済みジョブがターゲットの未達成テスト結果を評価できなくなります。このプロパティはデフォルトで有効になっています。

リストとフォームビューにターゲット日とステータスを表示する

コンフィグレーションコンプライアンス マネージャーは、テスト結果フォームとリストビューの両方から修復ターゲット日を確認できます。また、修復ターゲットルールはスキャナーインポートの後に実行され、テスト結果が再オープンされた場合に再実行されます。

スケジュール済みジョブにより、テスト結果リストビューの [修復ターゲット] および [修復ステータス] が更新され、テスト結果フォームの [修復ターゲットルール]、[修復ターゲットルール]、および [修復ステータス] フィールドが更新されます。

注:
デフォルトでは、[修復ターゲット] と [修復ステータス] 列は [テスト結果] リストビューに表示されません。これらの列を表示するには、リストビューにも追加する必要があります。同様に、[修復ターゲットルール]、[修復ターゲット]、および [修復ステータス] フィールドをテスト結果フォームに追加します。

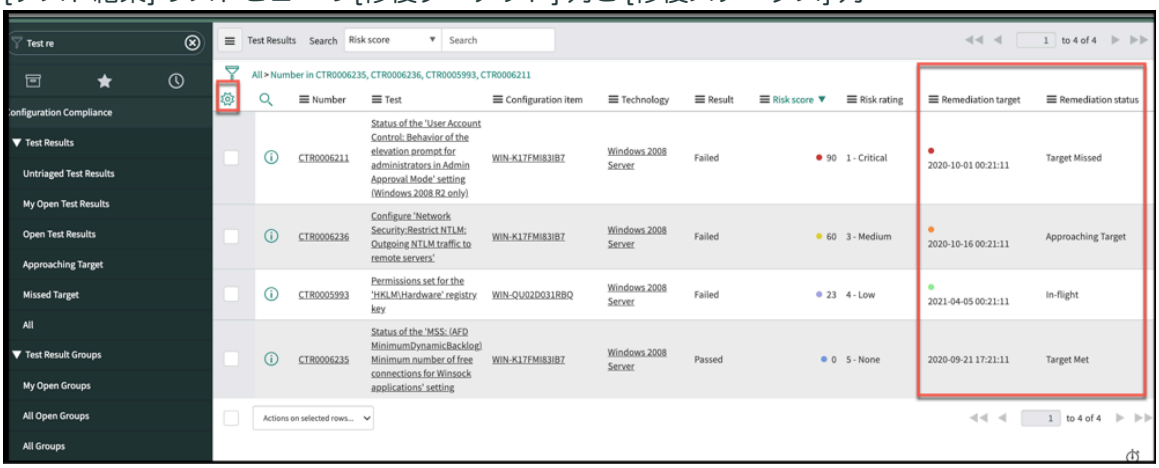
これらの列とフィールドを表示するには、次の図に示すように、それぞれ [設定] および [他のアクション] メニューのスラッシュバケットを使用します。テスト結果レコードの [他のアクション] メニューで、メニューアイコン、[構成]、および [フォームレイアウト] の順にクリックしてスラッシュバケットを表示し、フィールドを [利用可能 **(Available)]** から [選択済み **(Selected)]** に移動します。

[修復ターゲット日] は、テスト結果リストビューでは色分けされた点で表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

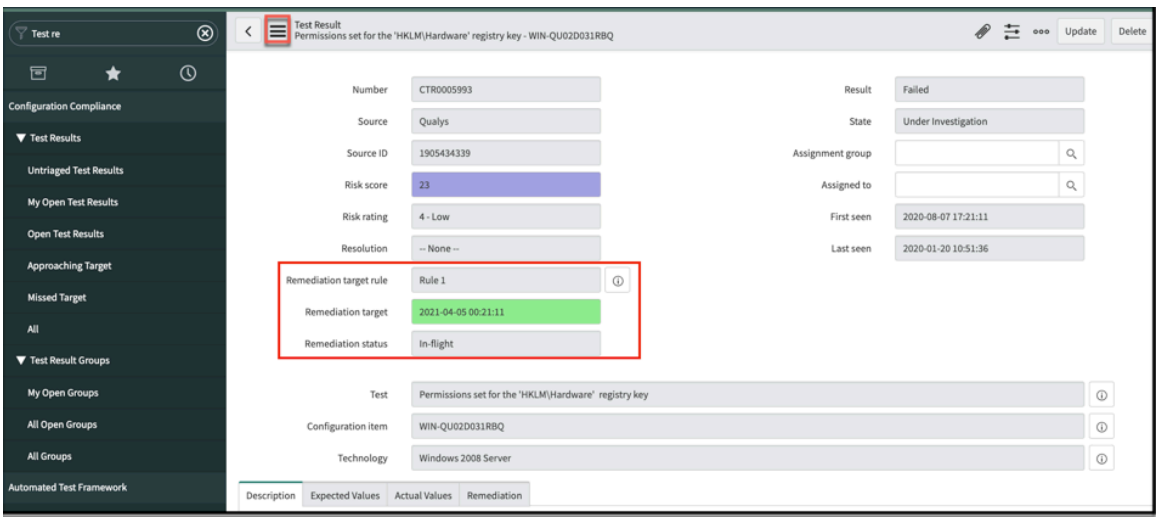
- 通知日に達していないテスト結果は緑色で示されます。
- 修復ターゲット日が近づいているテスト結果はオレンジ色で示されます。
- 修復ターゲット日が過ぎたテスト結果は赤色で示されます。

[テスト結果] リストビューの [修復ターゲット] 列と [修復ステータス] 列



- ターゲット経過：ターゲット日を過ぎています
- ターゲット内：テスト結果は処理中です

テスト結果レコードのターゲットルール、ターゲット、およびステータスの各フィールド



テスト結果レコードは、コンフィグレーションコンプライアンス ダッシュボードにも視覚的に表示されます。次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > 概要 ダッシュボードでステータスを確認します。概要には、既存のウィジェットと修復ステータスが含まれます。グラフの色は、[テスト結果] リストビューと [テスト結果] レコードに表示される色と一致します。

修復ターゲットルールのシナリオ

複数の修復ターゲットルールが同じテスト結果に適用される場合は、最も制限の厳しいルールが適用されます。

たとえば、2018 年 3 月 1 日に最初に識別されたテスト結果が 2 つの修復ターゲットルールの条件を満たす場合：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 修復ターゲットルール 1：2018 年 3 月 7 日に定義、修復ターゲットは初めて閲覧されてから 15 日、算出された修復ターゲット日は 2018 年 3 月 16 日 10:00:00。
- 修復ターゲットルール 2：2018 年 3 月 10 日に定義、修復ターゲットは初めて閲覧されてから 10 日、算出された修復ターゲット日は 2018 年 3 月 11 日 10:00:00。

注:

修復ターゲットは、[最終確認日] の日付に日数 (24 時間単位として測定) を加えて算出されます。

V14.5 以降では、修復ターゲットは [ターゲット開始 (日付)] から算出されます。デフォルト値は [最終確認日] のままです。 v14.12 以降、デフォルト値は [最終合格 **(Last pass)]** です。

このシナリオでは、 より厳しい日付制限の修復ターゲットルール 2 がテスト結果に適用されます。(テスト結果の最初の識別日時から 10 日、15 日。)

ターゲットルールの作成または変更、変更の再適用

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > 修復ターゲットルール して、新しい修復ターゲットルールを表示、編集、および作成します。
2. [名前] 列でルールをクリックしてターゲットルールを開き、レコードを編集します。または、[新規] をクリックして新しいターゲットルールを作成します。
3. フォームに入力して、修復予定期間を定義し、このルールを適用するテスト結果を条件と一緒に指定し、ユーザーまたはグループ、またはその両方にリマインダーを送信するタイミングを決定します。

修復ターゲットルールフォーム

フィールド	説明
名前	ルールの名前。
有効	ルールを有効または無効にします。デフォルトでルールは自動的に有効 (true) になり、手動変更の適用を選択した場合または次のスケジュール済みジョブの後に、テスト結果に適用されます。
ターゲット (日数)	修復の目標期限日を日数で設定します。ターゲット修復日数のデフォルト値は 30 です。 たとえば、ターゲット値が 30 の新しいルールを作成した場合、新しいルールと、同様に 30 日以上の目標期日を持つ他の既存のルールがテスト結果に適用されます。
ターゲット開始 (日付)	ターゲット日付が算出される日付。日付タイプまたは日付と時刻タイプのフィールドのみを指定できます。v14.12 以降、デフォルト値は [最終合格 *(Last pass)]* です。 次のいずれかを選択します。 ○ 最終確認日 ○ 初回確認日

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ 作成日時 ○ 最終合格 最後のパスが空の場合、作成日は修復ターゲットの計算で考慮されます。 ○ 最終オープン日時 このフィールドの値をカスタマイズするには、「KB1642413」を参照してください。
通知 (期限前の日数)	ユーザーとグループにリマインダーを送信する期限日までの日数を設定します。
説明	ルールの簡単な説明。
条件	条件ビルダーを使用して、このルールが適用されるテスト結果を指定します。たとえば、リスクスコアが 70 を超えるすべてのテスト結果に対して、30 日の修復ターゲット日を設定します。修復日の 7 日前にユーザーまたはグループ、またはその両方にリマインダーを送信します。 条件ビルダーに入力した検索テキストの大文字と小文字の区別は、このレコードまたはフォームではサポートされていません。v 12.0 より前では、条件ビルダーに入力した検索テキストの大文字と小文字の区別は、サポートされています。
ユーザー、ユーザーグループ、またはその両方	ユーザーまたはグループ、またはその両方を選択して、設定した期限日が近づいていることや過ぎていることについて通知を送信します。

4. **[Submit]** をクリックします。または、編集済みのルールを保存するために、[更新] をクリックします。

   更新されたルールまたは新しいルールがリストビューに表示されます。リスト内のルールは順に並べられ、修復ターゲット日が最も近いルールから順に実行されます。ルールを無効化または削除すると、順番に、次のルールが非アクティブまたは削除されたルールに置き換わります。

5. 新しい変更を今すぐ適用するには、[変更を適用] をクリックします。

コンフィグレーションコンプライアンス 算出グループ

コンフィグレーションコンプライアンス 算出は、事前定義された条件が満たされたときにレコード値を更新するために使用されます。算出は、レコードの更新方法を決定するために使用される基準に基づいてグループ化されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

コンフィグレーションコンプライアンス 算出グループ

デフォルトリスク算出のレコードから、影響を受けるすべてのテスト結果とコレクションに算出ルールをオンデマンドで適用できます。脆弱性マネージャーは、この機能を使用してリスク算出の構成を調整できます。また、展開の初期段階でいくつかの優先順位付けスキームを試し、その変更をオンデマンドで適用して、インポート結果にどのような影響を与えるかを確認することもできます。

リスクスコア算出グループは、リスク算出に名称変更されました。

リスクスコアロールアップ算出は、コンフィグレーションコンプライアンス に含まれてします。個々のロールアップ算出には次の 2 つのタイプがあります。

構成テストリスクロールアップ

すべてのテスト結果のリスクスコアを同じ構成テストでロールアップし、構成テストの全体的なリスクスコアを提供します。ロールアップされた値は [リスクスコア] フィールドに表示されます。

修復タスクのリスクスコアをロールアップ

これらの計算機能は、修復タスクの全テスト結果のリスクスコアをロールアップし、その修復タスクの全体的なリスクスコアを提供します。ロールアップされた値は [リスクスコア] フィールドに表示されます。

リスクスコア算出グループとリスクスコアロールアップ算出グループの両方がデフォルトで有効になっています。

詳細については、コンフィグレーションコンプライアンス 算出の次の主要な用語を確認してください。

テスト結果

テスト結果は、構成アイテム (CI) と関連するテクノロジーに対する構成テストの結果です。[失敗]、[エラー]、および [不明] 状況のテスト結果は、ポリシーに準拠していないハードウェア、ソフトウェア、および資産を明らかにします。

修復タスク

テスト結果は、事前定義された修復タスクルールに基づいて、データインポート時にグループ化されます。これらの修復タスクは、脆弱性対応の脆弱性グループと類似しています。修復タスクは、テスト結果を一括分析用グループに整理し、修復するアイテムセットを表します。

テスト結果のリスクスコア

資産のビジネスコンテキストと関連するテストの重大度に基づいて、リスクスコア算出によって計算された値。CMDB で定義された影響を受ける資産のビジネス上の重要度、およびスキャナーから通知されるテストの重大度の平均です。

各資産には、複数のサービスを関連付けることができます。資産のビジネス上の重要度は、最も重要度の高いサービスによって決まります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

計算された値は、テスト結果の [リスクスコア] フィールドに表示されます。スコアには 0 ～ 100 の範囲の値が表示されます。また、フィールドは色分けされており、一目で重大度がわかるようになっています。

修復タスクのリスクスコア

このスコアは修復タスクのレコードに表示され、修復タスク内のすべてのアクティブなテスト結果のリスクスコアをロールアップした値です。このスコアは、修復タスク内でテスト結果が修復されると変更されます。

構成テストのリスクスコア

このスコアは構成テストに表示され、その構成テストに関連するすべてのアクティブなテスト結果のリスクスコアをロールアップした値です。このスコアは、この構成テストに関連付けられたテスト結果が修復されると変更されます。

リスク評価

失敗したテスト結果がシステムにもたらすリスクの量を表します。これは、リスクを重大 (1) ～ なし (5) として評価する 1 ～ 5 の数値スケールによるリスクスコアの範囲に基づいています。スコアはリスクスコアの範囲に基づいており、[リスク評価] フィールドに表示されます。

リスク評価範囲

リスク評価	リスクスコア
1- 重大	90 ～ 100
2 - 高	70 ～ 89
3 - 中	40 ～ 69
4 - 低	1 ～ 39
5 - なし	0

リスクスコアロールアップ算出

ロールアップ算出には次の 2 つのタイプがあります。

- 構成テストのリスクロールアップ：すべてのテスト結果のリスクスコアを同じ構成テストでロールアップし、構成テストの全体的なリスクスコアを提供します。ロールアップされた値は [リスクスコア] フィールドに表示されます。これらの算出の重み付けとスコアのスクリプト値は編集できます。
- 修復タスクのリスクスコアロールアップ：修復タスク内のすべてのテスト結果のリスクスコアをロールアップし、その修復タスクの全体的なリスクスコアを提供します。ロールアップされた値は [リスクスコア] フィールドに表示されます。これらの算出の重み付けとスコアのスクリプト値は編集できます。リスクスコアロールアップ算出の例とスコアの計算方法については、「コンフィグレーションコンプライアンスのリスクロールアップ算出の例 (v15.0 より前)」を参照してください。

履歴リスクスコア

修復タスク内のすべての合格したテスト結果全体にわたる固有のリスクスコア。このフィールドは、テストグループによって修復されたリスク量を表示し、テストグループが「クローズ済み」ステータスにあり、リスクスコアがゼロの場合にのみ表示されます。

スコアは、リスクスコアが変更されたとき、またはテスト結果が追加されたとき、または修復タスクから削除されたときに計算されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
このスクリプトを正しく動作させるには、サービスマッピング プラグインが必要です。サービスマッピング は別のサブスクリプションとして利用可能であり、ServiceNow 担当者によるアクティブ化が必要です。

コンフィグレーションコンプライアンス 算出グループの作成

コンフィグレーションコンプライアンス 算出グループは、使用方法に基づいた算出のグループ化に使用されます。

始める前に
必要なロール：sn_vulc.admin

このタスクについて
コンフィグレーションコンプライアンス ベースシステムには、[リスクスコア] という 1 つの算出グループが含まれています。他の算出を作成すると、このグループに追加したり、他のグループや算出を作成したりすることができます。各グループ内で、テスト結果に一致する最初の算出が実行されます。

コンフィグレーションコンプライアンスアプリケーションには、次の 2 つの算出グループが含まれています。

- リスク算出
- リスクスコアロールアップ算出

リスク算出は、テスト結果のリスクスコアとリスク評価を計算します。

リスクスコアロールアップ算出は、すべてのテスト結果と修復タスクのリスクスコアを同じ構成テストでロールアップし、全体的なリスクスコアを提供します。

これらのグループから直接新しい算出を作成することもできます。

手順

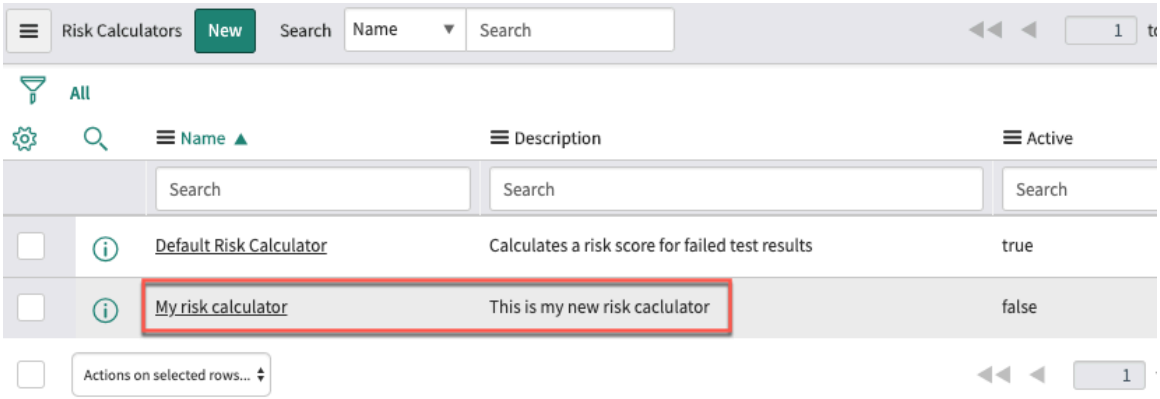
1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > 算出グループ.
2. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション をクリックし、[リスク算出] または [リスクスコアロールアップ算出] を選択します。
3. [**New**] をクリックします。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
名前	算出の名前。
説明	この算出グループの説明。
有効	算出グループを有効または無効にします。

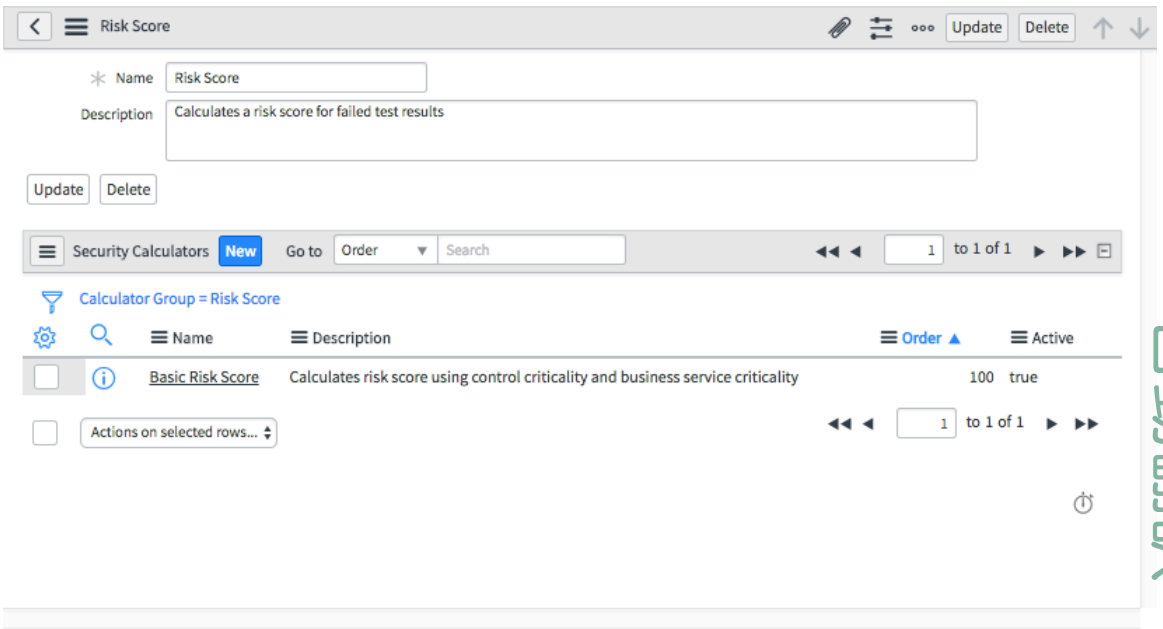
5. フォームヘッダーの [保存] を右クリックし、[送信] をクリックします。
新しい算出グループは、他の算出とともにグループリストに表示されます。新しい算出グループの名前をクリックして、レコードを開きます。条件と表示値の設定、および算出の再適用の詳細については、「コンフィグレーションコンプライアンス のリスク算出を作成、編集、および再適用する」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[セキュリティ算出] 関連リストが表示されます。



6. [新規] をクリックして、算出をその条件とともにグループに追加します。

条件ビルダーに入力した検索テキストの大文字と小文字の区別は、このレコードまたはフォームではサポートされていません。

コンフィグレーションコンプライアンス の算出と算出ルール

コンフィグレーションコンプライアンス は、テスト結果におけるフィールドの初期値算出を自動化します。各算出の条件が順番に評価され、最初に一致した算出が使用されます。

コンフィグレーションコンプライアンス の算出

コンフィグレーションコンプライアンスのベースシステムには、テスト結果にベースのリスクスコアを設定するコンフィグレーションコンプライアンスの算出 (デフォルトリスク算出) が一つ含まれています。コンフィグレーションコンプライアンス算出は、条件フィルターを使用することにより、任意の条件に基づいてテスト結果の影響度を優先順位付けして評価するようにビルドすることができます。脆弱性のビジネスインパクト、構成アイテム (CI) のクラスなど、追加のコンフィグレーションコンプライアンス算出を作成してテスト結果の他のフィールドを設定するか、既存のコンフィグレーションコンプライアンス算出をカスタマイズすることができます。算出は、どのような優先順位でも反映できるように記述できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

各算出には、算出ルールのリストと、それを適用するタイミングを決定する条件が含まれています。算出が実行されると、各算出ルールの条件が順番に評価され、最初に一致した算出ルールが使用されます。

すべての有効なコンフィグレーションコンプライアンス算出は、テスト結果が作成されるたび、関連する CI または構成テストが変更されたとき、またはテスト結果の [リスクスコアを計算] 関連リンクが使用されたときに、選択されたフィールドを設定します。たとえば、インポートされたテスト結果で control.criticality の値が更新されると、テスト結果レコードのリスクスコアが自動的に更新されます。テスト結果のインポートによってテスト結果スコアが更新された後、[算出を再適用] ボタンを選択して、テスト結果のリスクスコアを再計算できます。

既存のテスト結果から [リスクスコアを計算 **(Calculate Risk Score)]** 関連リンクを選択し、いずれかの算出が有効になっている場合、テスト結果の [リスクスコア] フィールドが更新されます。

注:

- [リスクスコアを計算] 関連リンクは、少なくとも 1 つのコンフィギュレーションコンプライアンス算出が有効になっている場合にのみ表示されます。
- 脆弱性対応の v22.0 以降では、レコードビューの [リスクスコアを計算 **(Calculate Risk Score)]** ボタンを選択することで、脆弱性マネージャーワークスペースと IT 修復ワークスペースでテスト結果のリスクスコアを更新できます。
- コンフィグレーションコンプライアンスのバージョン 14.13 以降では、テスト結果のリスクスコアが変更されるたびに、テスト結果の [メモ] セクションに次の詳細が文書化されます。
  - 算出グループ名
  - 算出名：算出ルールがテンプレートとスクリプトのどちらに基づいているかに応じて、名前に括弧で囲まれた詳細が追加されます。算出ルールの基準を変更または表示するには、任意のルールを選択し、[詳細表示] チェックボックスをオンにします。[値のタイプ **(Value type)]** ドロップダウンボックスから、必要なオプションを選択します。[テンプレート] を選択した場合、リスクスコアはルールで指定された条件に従って更新されます。[スクリプト] を選択した場合、既存のスクリプトを追加または更新できます。
  - 重み付けとリスクスコアの寄与度を含むフィールド値
  - 最終的なリスクスコア
  - システムプロパティ *sn_sec_cmn.risk_score_changes_add_worknotes* は、作業メモセクションへの入力に役立ちます。コンフィグレーションコンプライアンス の v15.2.1 以降、システムプロパティ*sn_sec_cmn.risk_score_changes_add_worknotes*はデフォルトで無効になっています。これを有効にした場合にのみ、テスト結果のリスクスコアに関連するすべての変更を [作業メモ] セクションで確認できます。また、作業メモは、リスクスコアに変更がある場合にのみ更新されます。

コンフィグレーションコンプライアンス の算出ルール

デフォルトでは、ベースシステムの [デフォルトリスク算出 **(Default Risk Calculator)]** が提供されます。この算出のリスクルールを作成する場合は、[デフォルトリスク算出 **(Default Risk Calculator)]** のターゲットフィールドを [リスクスコア] に設定する必要があります。[新しいリスクルール] ボタンを選択し、新しいリスクルール を作成します。これによって、リスクルールと呼ばれる特殊なテスト結果算出ルールが作成され、複数の値に基づいてリスクスコアが計算されます。デフォルトでは 、リスクスコアを計算するための次の値が考慮されます。

- ビジネス上の重要度
- 重要度

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[デフォルトのリスクルール] で使用する値と、これらの各値の重み付けを調整できます。重み付けは、ベースのリスクスコアを設定するときに各要素をどの程度考慮するかを調整するために使用されます。

コンフィグレーションコンプライアンスバージョン 13.0 以降では、デフォルトのリスクルールの基準をカスタマイズできます。詳細については、「Define fields and weights for the risk rule (リスクルールのフィールドと重み付けを定義する)」を参照してください。

重み付けパーセンテージをアサインする

フィールド値レベルで重み付けのパーセンテージ (0 ～ 100) をアサインすることもできます。たとえば、各レベルの重大度 (なし～重大) に重み付けのパーセンテージをアサインできます。リスクルールの重要度の重み付けが 50 で、重要度レベルに次の重み付け値がアサインされている場合：

重み付けパーセンテージをアサインする

重要度	リスクスコア
重大	100
高	50
中	20
なし	0

重要度が「重大」の場合、対応する重み付けは 50 です。重要度が「高」の場合、重み付けは 25 で、重要度が「中」の場合、重み付けは 10 です。重要度が「なし」の場合、対応する重み付けは 0 です。詳細については、「Risk score calculation example for Configuration Compliance (コンフィグレーションコンプライアンスのリスクスコアの計算例)」を参照してください。

各ルールには [順序] 設定がありますが、条件に一致する最初のルールによってテスト結果の [リスクスコア] フィールドが更新されます。通常、スクリプト化されていない算出ルールは、スクリプト化された算出ルールよりもパフォーマンスへの影響が少なくなります。

ベースシステムの コンフィグレーションコンプライアンス の算出には、重要度レベル (なし～重大) ごとに、重大度に基づいて [リスクスコア] の値 (0 ～ 100) をアサインする算出ルールが含まれています。[不明な重大度] には、リスクスコア 100 が自動的にアサインされます。これらの値は調整可能で、[デフォルトリスク算出 (Default Risk Calculator)] のように、新しい算出ルールやリスクルールを作成できます。

脆弱性のリスクスコアの重み付け

すべての脆弱性には、重大度、重要度、エクスプロイト情報などの要素に基づいてリスクスコアと評価がアサインされます。このリスク評価の算出を担当するのが、脆弱性一致アイテムのテーブルのビジネスルール `Update Risk Rating from Risk Score` です。リスクスコアが変更されるたびに、脆弱性一致アイテムのリスク評価が算出されて入力されます。脆弱性対応 (VR) アプリケーションのバージョン 17.1 より前では、次のリスク評価がスクリプトインクルード VulnerabilityUtils の一部として提供され、ハードコードされていました。

値 (リスク評価)	重み付け (リスクスコア)
1	90–100
2	70–89
3	40–69
4	1–39

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

値 (リスク評価)	重み付け (リスクスコア)
5	0

脆弱性対応 のバージョン 18.0 以降では、

- 出荷時のリスク評価タイプはベーステーブルで base table as cc_risk_rating となっています。リスク評価タイプは、リスク評価が計算される各テーブルのビジネスルールの一部として渡されます。
- リスク評価の算出の対象となる [リスクスコアの重み付け] テーブルの値をクエリできるように、スクリプトが変更されます。
- 既存のタイプにエントリを追加するか、新しいタイプを作成します。新しいタイプを作成するときは、新しいリスク評価のラベルを追加し、関連するスクリプトとビジネスルールも変更してください。新しいリスクスコアのスタイルも新たに追加する必要があります。
- ベーステーブルのレコードをクエリするようにスクリプトを変更します。

[リスクスコアの重み付け] テーブルにアクセスするには、フィルターナビゲーターに「sn_sec_cmn_risk_score_weight」と入力します。

さらに、次のシナリオではリスクスコアが自動的に再計算されます。

- 構成アイテム (CI) が非インターネットフェーシングからインターネットフェーシングに変更されたとき。
- 脆弱性一致アイテム (VI) の関連する一般的な脆弱性とエクスポージャー (CVE) またはサードパーティエントリー (TPE) が、CVE の既知の悪用された脆弱性 (KEV) にリンクされている場合。

自動翻訳

リスクルールのフィールドと重み付けを定義する

組織に固有のテストと資産データを利用したリスクスコアを生成できるように、リスクルールのパラメーターと重み付けをカスタマイズします。リスクルールに含まれるフィールドを選択することで、効果的なリスクスコアリングフレームワークを定義できます。

始める前に

必要なロール：sn_vulc.admin

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > リスク算出.
2. [デフォルトのリスク算出] をクリックします。
3. ターゲットフィールドを [リスクスコア] に選択します。
   [新しいリスクルール] ボタンが算出ルールテーブルに表示されます。
4. [新しいリスクルール] ボタンをクリックして、[コンフィギュレーションコンプライアンスルール] フォームに移動します。
5. [リスク算出基準] セクションで、全体的なリスクスコアの計算における重要性に従って、各基準の重み付けを設定します。
6. ルールを非アクティブ化するには、[アクティブ] チェックボックスをオフにします。
7. [基準を追加] をクリックして、リスク算出基準にリスクルールフィールドを追加します。
8. フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リスクルールのフィールドフォーム

フィールド	説明
参照テーブルを選択	リスクスコアの重み付けの定義に使用するテーブル。 次のオプションのいずれかを選択します。 ○ [テスト結果]：テスト結果 (TR) から直接ドット連結できるフィールドを追加します。 ○ [テスト結果 - 構成アイテム]：ハードウェアテーブルなど、ベーステーブルの拡張の一部であるドット連結可能なフィールドを追加します。 これらのフィールドはベーステーブル (cmdb_ci) に含まれていません。 ○ [テスト結果 - テスト]：サードパーティエントリーなど、ベーステーブルを拡張するテーブルに含まれるドット連結可能なフィールドを追加します。これらのフィールドは構成テストのベーステーブルに含まれていません。 ○ [テスト結果参照テーブル]：関連テーブル (m2m) に含まれるフィールド、またはテスト結果への参照を持つテーブルを追加します。これらのフィールドは、テスト結果から直接ドット連結することはできません。 ○ [構成アイテム参照テーブル]：関連テーブル (m2m) に含まれるフィールド、または cmdb_ci への参照を持つテーブルを追加します。これらのフィールドは、TR から直接ドット連結することはできません。 ○ [テスト参照テーブル]：sn_vulc_test の関連テーブル (m2m) に含まれるフィールド、または sn_vulc_test への参照を持つテーブルを追加します。これらのフィールドは、TR から直接ドット連結することはできません。 ○ [カスタム条件]：条件を評価することでルールに重み付けをアサインするには、このオプションを使用します。たとえば、インターネット向けフィルターは、構成アイテム (CI) が外部か内部かを判断します。
フィールド	このルールのリスクスコア算出に使用するフィールド。
重み付け	リスクルール内でのこのフィールドの重み付け。値は 0 ～ 100 の整数である必要があります。
テーブル	○ テスト結果 > 構成アイテム ○ テスト結果 > テスト ○ テスト結果参照テーブル

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ 構成アイテム参照テーブル ○ テスト参照テーブル このフィールドは、[参照テーブルを選択] フィールドでリストされたオプションのいずれかが選択されている場合にのみ表示されます。
集計	関連テーブル (m2m) から [フィールド] が選択されている場合に、算出で考慮する最小値または最大値を選択します。 このフィールドは、[参照テーブルを選択] フィールドから参照テーブルが選択されている場合にのみ表示されます。
値の重み付けを定義	各フィールド値に重み付けをアサインするコンポーネント。数値フィールドの場合、フィールド値を範囲 (1 ～ 5 など) として定義します。値は 0 ～ 100 の整数でなければなりません。 [カスタム条件] オプションが [参照テーブルを選択] フィールドで選択されている場合、このフィールドは表示されません。
条件テーブル	条件をリストから選択します。 このフィールドは、[カスタム条件] オプションが [参照テーブルを選択] フィールドで選択されている場合のみ表示されます。
フィールド名	リスク基準の名前を入力します。 このフィールドは、[カスタム条件] が [参照テーブルを選択] フィールドで選択されている場合のみ表示されます。
条件	定義された条件に一致するこのテーブルのアイテムをプレビューします。 このフィールドは、[カスタム条件] が [参照テーブルを選択] フィールドで選択されている場合のみ表示されます。

9. [Submit] をクリックします。

次のタスク
[ルール] ページで、ルールをアクティブ化して再適用し、アクティブなテスト結果のリスクスコアを再評価します。

コンフィグレーションコンプライアンス のリスクロールアップ算出を編集

既存のリスクロールアップ算出を編集します。

始める前に
必要なロール：sn_vulc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション をクリックし、[リスクスコアロールアップ算出 **(Risk Score Rollup Calculators)**] を選択します。
2. リスクスコアロールアップ算出のリストが表示された状態で、算出をクリックしてレコードを開き、フォームを編集します。

フィールド	説明
名前	構成テストまたは修復タスクロールアップ算出の名前。
説明	リスクロールアップ算出の説明。
テーブル	ロールアップ算出が適用されるテーブル。
保留を含める	リスクスコアのロールアップ時に保留されたテスト結果を含めます。

3. 次のいずれかの方法で重み付けを定義します。
   - [ロールアップの重み付け] セクションで、次の重み付けをアサインします。

     ロールアップの重み付け

フィールド	説明	デフォルトの重み付け
最大リスクスコア	考慮されるテスト結果における最大リスクスコア。	85
平均リスクスコア	考慮されるテスト結果におけるリスクスコアを集計します。	0
テスト結果の数	テスト結果の数。	15

   - [詳細ビュー] チェックボックスをオンにし、必要に応じてスクリプト値エディターでスクリプトの値を編集します。

     注:
     スクリプトを編集するには、Now Platform および コンフィグレーションコンプライアンス アプリケーションに関する高度な知識が必要です。

4. [更新] をクリックして編集を保存します。

ロールアップ算出は、1 時間ごとに実行されるスケジュール済みジョブで、変更を取得します。これらのスケジュール済みジョブでは、構成テストや修復タスクに対して、総合的なリスクスコアの提供も行っています。ロールアップされた値は [リスクスコア] フィールドに表示されます。

リスクロールアップ算出によるスコアの決定方法については、「コンフィグレーションコンプライアンスのリスクロールアップ算出の例 (v15.0 より前)」を参照してください。

コンフィグレーションコンプライアンス のリスク算出を作成、編集、および再適用する

算出ルールは、影響を受けるすべてのテスト結果とコレクションにオンデマンドで適用できます。脆弱性マネージャーは、この機能を使用してリスク算出の構成を調整し、オンデマンドで変更を適用して変更をインポートできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_vulc.admin

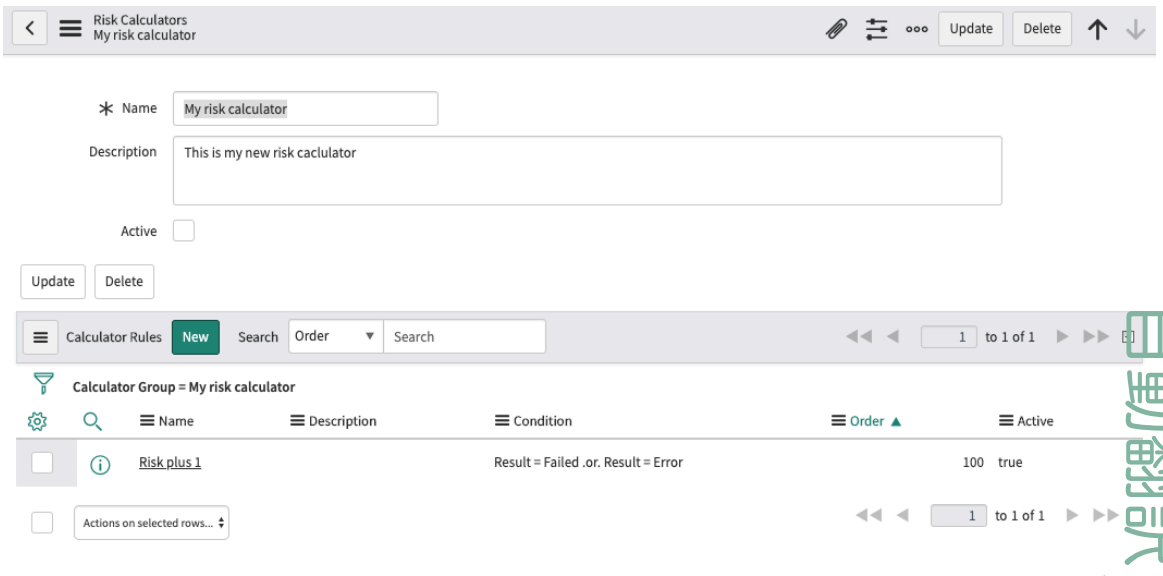
手順

1. 新しいリスク算出を作成するには、次の手順に従います。

   a. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション をクリックし、[リスク算出] を選択します。

   b. リスク算出リストで、[新規] をクリックします。

   c. 新しい算出の名前と説明を入力し、[送信] をクリックします。
   新しい算出がリスク算出リストに表示されます。



   d. リストで、新しい算出をクリックして、その算出が実行される条件を作成し、テスト結果レコードと修復タスクに表示するフィールドと値を指定します。

   e. 表示されるレコードで、[新規] をクリックします。

   f. 必要に応じて、タブのフィールドに入力します。

タブ	説明
この条件を満たしている場合	条件ビルダーを使用して、算出を実行する条件を作成します。例：結果が失敗または結果がエラー。
これらの値を設定	テンプレートを使用して、表示するフィールドと値を選択します。

   g. **[Submit]** をクリックします。
   レコードには、新しい算出ルールとそれが属するグループが表示されます。

2. 既存の算出をテスト結果に再適用したり、既存のリスク算出のルールや表示値を編集したりするには、次の手順を実行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. [リスク算出] または [リスクロールアップ算出] リストから、編集する算出を選択します。

b. レコードから既存のテスト結果データにリスク算出を再適用するには、[算出を再適用] をクリックします。
算出の条件を満たすすべてのテスト結果が更新されます。

> **注:**
> テスト結果の数によっては、この更新に時間がかかる場合があります。

c. 条件や値を編集するには、[名前] 列の左下で、算出の名前をクリックします。
リスク算出の場合、レコード、[この条件を満たしている場合] および [これらの値を設定 **(Set these values)]** タブが表示されます。

d. 必要に応じて、フォームに入力します。

タブ	フィールドの説明
この条件を満たしている場合	フィルター条件ビルダーを使用して、算出を実行する条件を作成します。
これらの値を設定	1 つ選択して続行します。 ▪ 値タイプ：テンプレート。リストからフィールドおよび対応する値を選択します。 ▪ スクリプト：エディターを使用して変更を入力します。 **注:** スクリプトを編集するには、Now Platform および コンフィグレーションコンプライアンス アプリケーションに関する高度な知識が必要です。

3. オプション: 既存のテスト結果データに新しいルールをオンデマンドで適用するには、次の手順を実行します。

a. [リスク算出] リストが表示された状態で、適用する算出をクリックします。
レコードが表示されます。

b. [算出を再適用] をクリックしてテストし、インポート結果にオンデマンドで変更を適用します。

4. テスト結果の変更を表示し、必要に応じて算出の編集を続けます。

コンフィグレーションコンプライアンス のリスクスコア算出の例

コンフィグレーションコンプライアンス v13.0 以降では、デフォルトのリスクルールの基準をカスタマイズできます。リスクスコア算出には、Qualys や Tenable などのサードパーティベンダーが提供するリスクスコアを使用します。

Qualys や Tenable などのサードパーティベンダーが独自のスコアを提供します。これらのスコアは、sn_vul_entry テーブルの [重要度] フィールドに入力されます。このフィールドはリスクスコアの算出に使用します。このスコアを使用してリスクスコアを算出するには、次の手順に従います。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

リスクルールの基準としてソースの重要度を追加する

サードパーティベンダーから提供された重要度に基づくスコアを使用して、リスクスコアを計算します。

始める前に

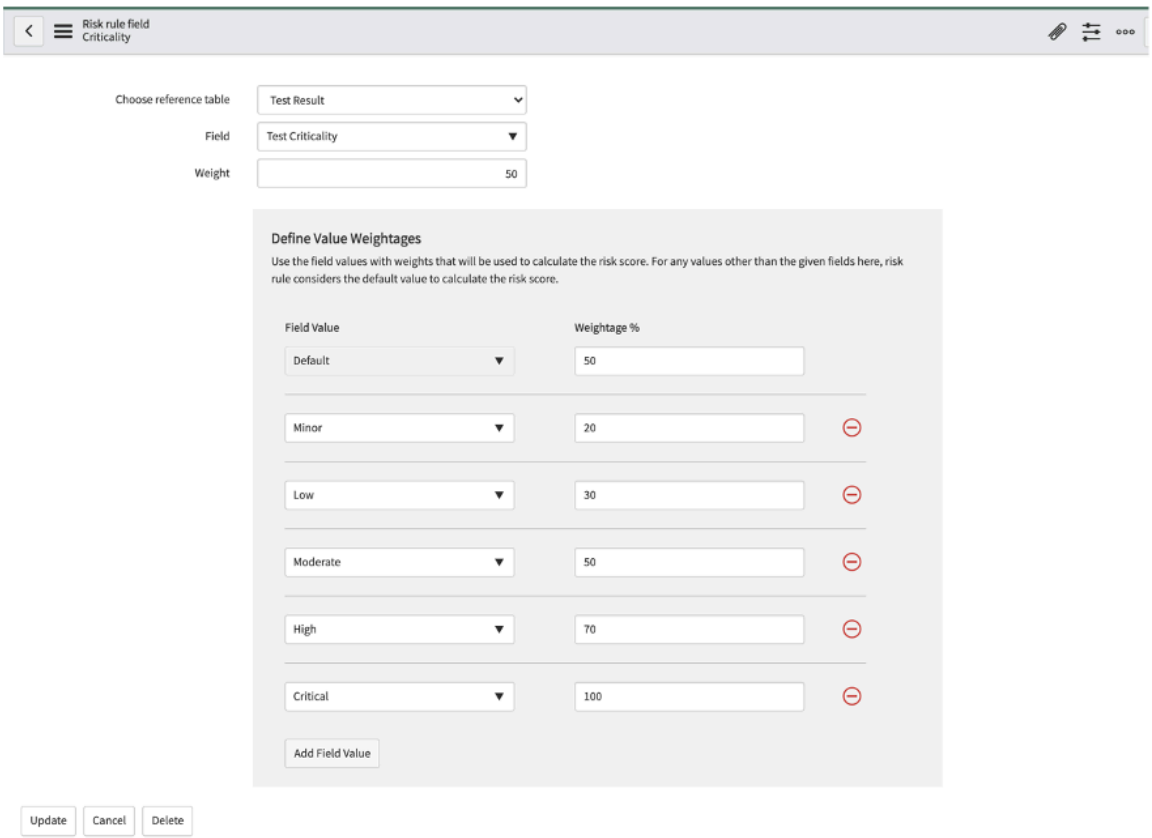
必要なロール：sn_vulc.admin

このタスクについて

Qualys や Tenable などのサードパーティベンダーが独自のリスクスコアを提供します。これらのスコアは、sn_vul_entry テーブルの [重要度] フィールドに入力されます。このフィールドは、リスクスコアの計算やコンピューティングに使用します。

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > リスク算出.
2. [リスクルール] フォームに移動します。
3. ルールを非アクティブ化するには、[アクティブ] チェックボックスをオフにします。
4. [基準を追加] をクリックします。
5. [参照テーブルを選択] リストから、[テスト結果]を選択します。
6. [フィールド] リストから、 [テストの重要度] を選択します。
7. [重み付け] フィールドで、このフィールドの相対的な重要度を入力します。
   値は 0 ～ 100 の整数である必要があります。
8. [値の重み付けを定義] セクションで、フィールド値を追加し、そのフィールドに重み付けパーセンテージをアサインします。



9. **[Submit]** をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

リスクルールの基準としてビジネス上の重要度を追加する

ビジネスサービスに対する重要度の値を指定し、ビジネス上の重要度を使用してリスクスコアを計算します。

始める前に

必要なロール：sn_vulc.admin

このタスクについて

組織にはさまざまなビジネスサービスがあり、ある構成アイテム (CI) が次のサービスで使用されていると仮定します。

ビジネスサービスの重要度

ビジネスサービス	重要度
Cloud Management	1：最重要
e-コマース	2：ある程度重要
クライアントサービス	3：やや重要
出張費と経費	4：重要ではない

CI とサービス間のマッピングは、サービス [cmdb_ci_services] テーブルに格納されます。CI が構成テストに合格しない場合、テスト結果 (TR) が作成されます。影響を受けるサービスのビジネス上の重要度の値を使用して、この TR のリスクスコアを計算できます。手順に従って、これらのサービスの重要度の値を使用してリスクスコアを計算します。

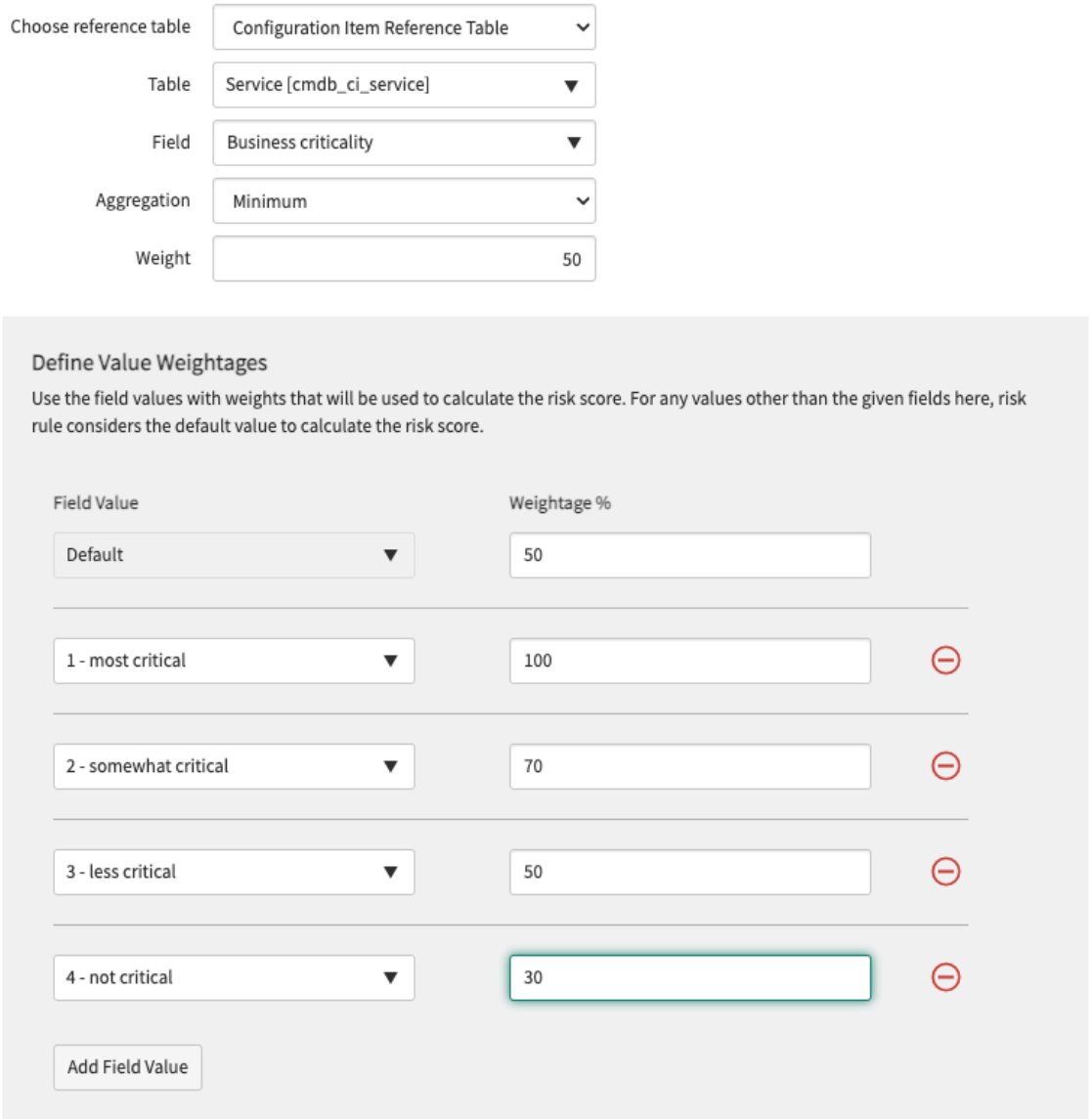
手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > リスク算出.
2. [算出ルール] セクションから [リスクルール] フォームに移動します。
3. ルールを非アクティブ化するには、[アクティブ] チェックボックスをオフにします。
4. [基準を追加] をクリックします。
5. [参照テーブルを選択] リストから、[構成アイテム参照テーブル] を選択します。
6. [テーブル] リストから、[サービス **[cmdb_ci_service]]**を選択します。
7. [フィールド] リストから、[ビジネス上の重要度] を選択します。
8. [集計] フィールドで、[最小] を選択してこのユースケースの最も重要なサービスを検索するか (1 - 最重要の値)、[最大] を選択してこのユースケースの最も重要ではないサービスを検索します (4 - 重要ではない値)。
9. [重み付け] フィールドで、このフィールドの相対的な重要度を入力します。
   値は 0 ～ 100 の整数である必要があります。
10. [値の重み付けを定義] セクションで、フィールド値を追加し、重み付けをアサインします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

カスタムのビジネス上の重要度リスクルールの重み付け



11. [Submit] をクリックします。

リスク算出に条件付き基準を追加する

リスクスコア算出のリスクルールにカスタム条件を使用します。

始める前に

必要なロール：sn_vulc.admin

このタスクについて

組織に複数の構成アイテム (CI) があり、外部ユーザーはそのうちのいくつかにのみアクセスできると仮定します。ユーザーは、これらの外部向き CI に対してリスクスコアの重み付けを追加できます。

注:
これらの CI は名前で識別できます。名前は「外部 (external)」で始まります。

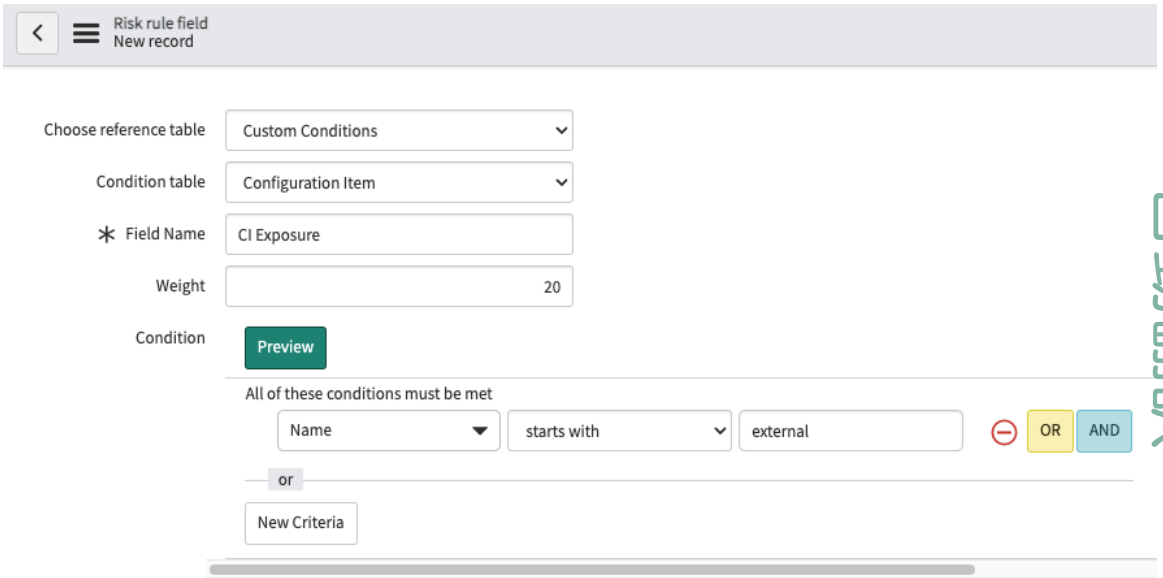
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > リスク算出.
2. [リスクルール] フォームに移動します。
3. ルールを非アクティブ化するには、[アクティブ] チェックボックスをオフにします。
4. [基準を追加] をクリックします。
5. [参照テーブルを選択] リストから、[カスタム条件] を選択します。
6. [条件テーブル] リストから、[構成アイテム] を選択します。
7. [名前] フィールドに「CI エクスポージャー」と入力します。
8. [重み付け] フィールドで、このフィールドの相対的な重要度を入力します。
   値は 0 ～ 100 の整数である必要があります。
9. [条件] フィールドで、[名前] > [次で始まる] を選択し、値を「外部」に指定します。

新しいリスクルールのカスタム条件



10. **[Submit]** をクリックします。

関連情報

Configuration Compliance 算出グループ

コンフィグレーションコンプライアンス のリスクスコア算出の例

リスクスコア算出を決定し、組織に固有のテストおよび資産データを使用するリスクスコアを生成します。

リスクルール算出スコアを決定する例

次の例は、リスクルール算出のスコアを決定する方法を示しています。リスクルール算出がこの表のフィールドで構成されていると仮定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リスクルール算出スコアの決定

フィールド	重み付け	重み付けブレークダウン
Control.Criticality	50	デフォルト：0 マイナー：20 低：30 中：50 高：70 重大：100
Business_Criticality	50	デフォルト：0 マイナー：20 低：30 中：50 高：70 重大：100

この表に示されているテスト結果がシステムに存在すると仮定します。

テスト結果のマッピング

ID	ビジネス上の重要度	コントロールの重要度
CTR0000001	1：最重要	マイナー
CTR0000002	1：最重要	低
CTR0000003	2：ある程度重要	マイナー
CTR0000004	2：ある程度重要	中
CTR0000005	3：やや重要	低

テスト結果のリスクスコア算出は、次の式に基づいて計算されます。

リスクスコア = (W(control.criticality) * FV (control.criticality). + W(business_criticality) * FV(business_criticality)) / 100、 W はフィールド値の重み付けで、FV は重み付けのパーセンテージ値です。

これらのテスト結果に対する計算後のリスクスコアは、次の表のとおりです。

テスト結果に基づくリスクスコア

ID	ビジネス上の重要度 (50%)	コントロールの重要度 (50%)	結果のリスクスコア
CTR0000001	1：最重要 (50% x 100)	マイナー (50% x 20)	60
CTR0000002	1：最重要 (50% x 100)	低 (50% x 30)	65

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テスト結果に基づくリスクスコア (続く)

ID	ビジネス上の重要度 (50%)	コントロールの重要度 (50%)	結果のリスクスコア
CTR0000003	2：ある程度重要 (50% x 70)	マイナー (50% x 30)	45
CTR0000004	2：ある程度重要 (50% x 70)	中 (50% x 50)	60
CTR0000005	3：やや重要 (50% x 50)	低 (50% x 30)	40

いずれかのフィールド値の重み付けのパーセンテージが変更された場合は、結果についてのこの表を参照してください。

変更された重み付けパーセンテージの結果

フィールド	重み付け	重み付けブレークダウン
Control.Criticality	50	デフォルト：0 マイナー：20 低：30 中：60 高：70 重大：100
Business_Criticality	50	デフォルト：50 1：最重要：100 2：ある程度重要：70 3：やや重要：20 4：重要ではない：30

この表には、算出を再適用した後のテスト結果のリスクスコアを示しています。

算出を再適用する際の **TR** のリスクスコア

ID	ビジネス上の重要度 (50%)	コントロールの重要度 (50%)	結果のリスクスコア
CTR0000001	1：最重要 (50% x 100)	マイナー (50% x 20)	60
CTR0000002	1：最重要 (50% x 100)	低 (50% x 30)	65
CTR0000003	2：ある程度重要 (50% x 70)	マイナー (50% x 30)	45
CTR0000004	2：ある程度重要 (50% x 70)	中 (50% x 60) * 改訂値	65 * 改訂値

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

算出を再適用する際の **TR** のリスクスコア (続く)

ID	ビジネス上の重要度 **(50%)**	コントロールの重要度 **(50%)**	結果のリスクスコア
CTR0000005	3：やや重要 (50% x 20) * 改訂値	低 (50% x 30)	25 * 改訂値

コンフィグレーションコンプライアンスのリスクロールアップ算出の例 **(v15.0** より前)

次の例は、リスクロールアップ算出のスコアを決定する方法を示しています。

次の修復タスクロールアップ算出では、修復タスクリスクスコアの計算式は次のとおりです。

(最大リスクスコア/100) * 85 + (係数 * 15)。

前式の係数は、次の表に示すテスト結果の数によって決まります。

テスト結果数	係数
<10	0.2
10 ～ 99	0.4
100 ～ 1000	0.6
1001 ～ 9999	0.8
>10000	1

テスト結果のリスクスコアが 3 つある次の修復タスク TRG0003066 では、最大スコアは 90 です。

番号	リスクスコア	修復タスク	結果	ステータス
CTR000123	90	TRG0003066	失敗	オープン
CTR000124	70	TRG0003066	失敗	オープン
CTR000125	40	TRG0003066	失敗	オープン

修復タスク TRG0003066 の場合：

リスクスコアは 79 です。(90/100) * 85 + 0.2 * 15 = Math.floor (76.5 + 3) = 79

修復タスクがまだ「オープン」であるため、履歴リスクスコアは Null です。

データ取り込み後、次の表に示すように、テスト結果は「合格」になり、修復タスクは「クローズ済み」に移行します。

番号	リスクスコア **(v15.0** より前)	修復タスク	結果	ステータス
CTR000123	0	TRG0003066	合格	クローズ済み
CTR000124	0	TRG0003066	合格	クローズ済み
CTR000125	0	TRG0003066	合格	クローズ済み

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テスト結果の履歴は、次の表のように表示されます。

番号	リスクスコア	最新の結果	結果
CTRH000111	90	CTR000123	失敗
CTRH000112	70	CTR000124	失敗
CTRH000113	40	CTR000125	失敗

修復タスクにアクティブなテスト結果がないため、リスクスコアはゼロです。

修復タスク TRG0003066 の場合：

履歴リスクスコアは 79 です。(90/100) * 85 + 0.2 * 15 = Math.floor (76.5 + 3) = 79

コンフィグレーションコンプライアンスのリスクロールアップ算出の例 **(v15.0** 以降)

次の例は、リスクロールアップ算出のスコアを決定する方法を示しています。

次の修復タスクロールアップ算出では、修復タスクリスクスコアの計算式は次のとおりです。

(最大リスクスコア * 80/100) + (平均リスクスコア * 5/100) + (係数 * 15)

ここで、重み付けは次のとおりです。

- 最大リスクスコア：80
- 平均リスクスコア：5
- 係数：15

平均リスクスコアのデフォルトの重み付けは 0 です。重み付けの設定方法の詳細については、「コンフィグレーションコンプライアンス のリスクロールアップ算出を編集」を参照してください。

前式の係数は、次の表に示すテスト結果の数によって決まります。

テスト結果数	係数
<10	0.2
10 ～ 99	0.4
100 ～ 1000	0.6
1001 ～ 9999	0.8
>10000	1

次の修復タスク TRG0003066 では、テスト結果のリスクスコアが 3 つあり、最大リスクスコアは 90、平均リスクスコア 66.67 です。

番号	リスクスコア	修復タスク	結果	ステータス
CTR000123	90	TRG0003066	失敗	オープン
CTR000124	70	TRG0003066	失敗	オープン
CTR000125	40	TRG0003066	失敗	オープン

修復タスク TRG0003066 の場合：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リスクスコアは 81 です。(90 * 80/100) + (66.67 * 5/100) + (0.2 * 15) = Math.floor (78.3 + 3) = 81

修復タスクがまだ「オープン」であるため、履歴リスクスコアは Null です。

データ取り込み後、次の表に示すように、テスト結果は「合格」になり、修復タスクは「クローズ済み」に移行します。コンフィグレーションコンプライアンス の v15.0 以降では、合格したテスト結果のリスクスコアが入力され、軽減されたリスクが判断されます。

番号	リスクスコア	修復タスク	結果	ステータス
CTR000123	90	TRG0003066	合格	クローズ済み
CTR000124	70	TRG0003066	合格	クローズ済み
CTR000125	40	TRG0003066	合格	クローズ済み

テスト結果の履歴は、次の表のように表示されます。

番号	リスクスコア	最新の結果	結果
CTRH000111	90	CTR000123	失敗
CTRH000112	70	CTR000124	失敗
CTRH000113	40	CTR000125	失敗

修復タスクにアクティブなテスト結果がないため、修復タスクのリスクスコアはゼロです。

修復タスク TRG0003066 の場合：

履歴リスクスコアは 81 です。(90* 80/100) + (66.67* 5/100) + (0.2 * 15) = Math.floor (78.3 + 3) = 81

コンフィグレーションコンプライアンス 修復タスクルールの作成または編集

フィルター条件に基づいてテスト結果を自動的にアサインするルールを作成できます。これらのルールは、インポート時にテスト結果を自動的にグループ化するものです。フィルターを使用して、エクスプロイトを含むすべてのテスト結果を選択するなど、このルールによってグループ化されたテスト結果を制限します。

始める前に
必要なロール：sn_vulc.admin

このタスクについて
ベースシステムには、修復タスクルールとして、[アサイン先グループ、テスト **(Assignment group, Test)]** が 1 つ付属しており、アサイン先グループ ([アサインルール] から事前設定される) とテスト結果 [テスト] フィールドによってテスト結果をグループ化します。このルールは、フィルター条件とグループキーを使用して変更できます。グループキーは、テスト結果テーブルの列です。最大 6 つのキーを選択して、テスト結果のグループ化に使用する値を示します。

コンフィグレーションコンプライアンスのバージョン 14.7 以降、新しい実装では [アサイン先グループ、テスト **(Assignment group, Test)]** の修復タスクルールが非アクティブ化されます。

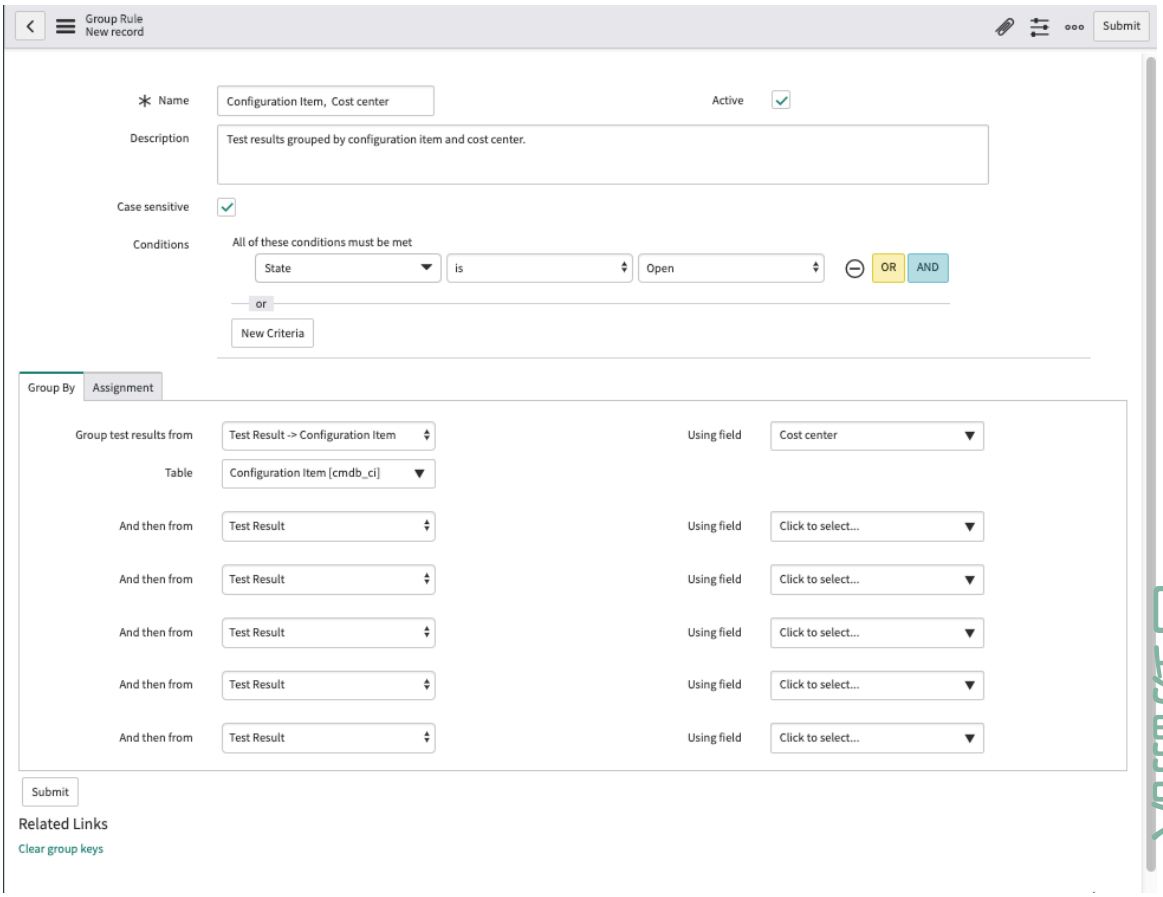
注:
新規または更新されたルールは、次回のインポート時に自動的に評価されるか、[修復タスクルール] フォームの [再適用] ボタンを使用して手動で評価されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > 修復タスクルール.
2. [アサイン先グループ、テスト **(Assignment group, Test)]** ルールを開くか、[新規] をクリックします。



3. [新規] の場合、必要に応じて、フォームのフィールドに入力します。

コンフィグレーションコンプライアンス修復タスクルール

フィールド	説明
名前	修復タスクルールの名前。
アクティブ	修復タスクルールがアクティブかどうかを示します。
説明	この修復タスクルールのテキスト説明。
大文字と小文字を区別	ルールの照合で大文字と小文字を区別するかどうかを決定します。 **注:** デフォルト値は、大文字と小文字の区別なしです。
条件	満たす必要がある条件。 デフォルト ([大文字と小文字を区別] チェックボックスが無効) では、修復タスクルールのレコードとフォームで条件ビルダーに入力する検索テキストでは、大文字

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	と小文字は区別されません。選択によって、グループのレコードとフォームで大文字と小文字を区別する検索を有効にできます。
グループ	
テスト結果のグループ化元	このルールに基づいてグループの作成を自動化します。利用可能ないずれかのオプションを選択します。 ○ テスト結果 | 使用フィールド ○ テスト結果->構成アイテム | テーブル | 使用フィールド 拡張された [テーブル] フィールドが選択されている場合、対応する拡張テーブルを使用しないテスト結果は別の修復タスクにグループ化されます。
アサイン	
次によってテスト結果グループをアサイン	このルールに基づいて、作成されたグループのアサインを自動化します。利用可能ないずれかのオプションを選択します。 ○ グループキー 選択すると、[キー値] フィールドが表示され、使用可能なフィールドがドロップダウンメニューに一覧表示されます。 ○ ユーザーグループ 選択すると、ユーザーグループルックアップフィールドが表示されます。

4. **[Submit]** をクリックします。

> **注:**
> [グループキーをクリア] 関連リンクは、フォームの [グループ化 (Group By)] タブにあるグループキーを削除します。

修復タスクに対して要求される例外の期間を指定する

システムのプロパティを使用して、修復タスクに対して例外が要求される期間を制限します。修復タスクの修復が指定された期間保留されます。

始める前に
必要なロール：sn_vulc.admin

このタスクについて
sn_vulc.exception_max_request_days プロパティは、修復タスクの例外を要求できる最大日数を指定するために使用されます。デフォルト値は 365 日です。

> **注:**
> sn_vulc.exception_approval_required プロパティを使用することで、必要ない場合に、修復タスクの例外承認ワークフローを無効にできます。デフォルトでは、このプロパティは有効になっており、値は true です。

手順

1. 次のように移動する。 **All** (すべて) > システムプロパティ > すべてのプロパティ.
2. [システムのプロパティ] ページで、sn_vulc.exception_max_request_days を検索します。
3. プロパティ名をクリックし、システムプロパティレコードを開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

4. このレコードを編集できるようにするには、現在のアプリケーションに コンフィグレーションコンプライアンス が選択されていることを確認してください。
5. 正の [値] を入力し、[更新] をクリックします。
   レコードが更新されて保存されます。

コンフィグレーションコンプライアンス の例外管理の設定

コンフィグレーションコンプライアンス モジュールを使用して、要求された例外の期間を制限し、例外にアンケートを追加します。デフォルトでは、ServiceNow　脆弱性対応 モジュールを使用して例外が要求されます。GRC: ポリシーとコンプライアンス管理 の統合を使用して例外を要求することもできます。

始める前に
必要なロール：sn_vulc.admin

このタスクについて
脆弱性対応 が有効であれば、例外を要求できる期間を制限できます。同様に、GRC: ポリシーとコンプライアンス管理 モジュールがインストールされていれば、構成画面で GRC: ポリシーとコンプライアンス管理 を選択できます。このオプションを有効にすると、GRC からポリシーおよびコントロール目標を指定する例外を要求できます。

アンケートを追加すると、例外要求または誤検出要求を出しているユーザーにアンケートが送信されます。デフォルトのアンケートを使用することも、要件に基づいて作成することも可能です。

アンケートは、例外が要求されている理由を例外承認者が理解する際に役立ちます。

手順
1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > 例外管理.
2. [例外管理構成] フォームで、[例外の管理に使用] リストからオプションを選択して、例外を管理する方法を選択します。
   - 脆弱性対応

     注:
     脆弱性対応の 22.0 以降では、脆弱性対応 オプションの誤検出要求に対するアンケートを設定することもできます。

   - GRC: ポリシーとコンプライアンス管理

     注:
     GRC: ポリシーとコンプライアンス管理 を使用して例外を要求するには、GRC プラグインをアクティブ化する必要があります。

   注:
   構成を変更しても、既存のデータには影響しません。
3. フォームのフィールドに入力します。

CC 例外管理フォームの設定

フィールド	説明
期間	例外を要求できる期間。
単位	指定された期間の時間単位。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
例外を要求するアンケートを有効化	上がっている例外要求にアンケートを追加するオプション。
例外を要求するアンケート	例外を要求するために自分が選択したアンケートを表示するオプション。デフォルトでは、[例外のアンケート] が表示されます。
誤検出をマークするアンケートを有効化	上がっている誤検出要求にアンケートを追加するオプション。
誤検出をマークするアンケート	誤検出としてマークするために自分が選択したアンケートを表示するオプション。デフォルトでは、誤検出要求のアンケートが表示されます。

4. [保存] を選択します。

コンフィグレーションコンプライアンス の例外承認者を追加する

コンフィグレーションコンプライアンスの修復タスクの例外を要求できるように、ユーザーを承認者グループに追加します。

始める前に

必要なロール：sn_vulc.admin

このタスクについて

修復タスクの例外要求は、デフォルトの 2 レベルの承認ワークフローを使用して承認されます。第 1 レベルのグループへのユーザーの追加は必須です。第 2 レベルにユーザーがいない場合、要求は第 1 レベルの承認後に自動的に承認されます。

注:
第 1 レベルの承認者がいない場合は、例外を要求できません。

注:
コンフィグレーションコンプライアンス v13.0 までは、第 1 レベルの承認者がいない場合は、例外を要求できません。ただし、コンフィグレーションコンプライアンス v13.0 以降では、CC アプリケーションを初めて展開する場合は、例外管理のフローデザイナーがデフォルトで有効になります。既にワークフローを使用している場合は、フローデザイナーに更新できます。どちらの場合も、ワークフローに戻すことはできません。

手順

1. 次のように移動する。 **All** (すべて) > システムセキュリティ > ユーザーとグループ > グループ.

2. [名前] 列で [例外] を検索し、[例外承認者：レベル **1 CC]** をクリックします。

注:
コンフィグレーションコンプライアンス の v14.7.5 以降では、システムプロパティ [sys_properties] テーブルのワークフローで、ベースシステムのシステムプロパティを使用して例外承認を行うことができます。このため、ワークフローで例外要求が作成されると、この要求はシステムプロパティで定義されているグループ ID に承認のために送信されます。次のように移動する。 **All** (すべて) > システムプロパティ をクリックし、[*sn_vulc.exception_approver_L1_CC*] または [*sn_vulc.exception_approver_L2_CC*] を選択してプロパティ値を変更します。

3. [グループ例外承認者 - レベル 1 CC] フォームで、次の場所に移動します グループメンバー > 新規 (または 編集)をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

4. フォームのフィールドに入力します。

ユーザーフォーム

フィールド	説明
ユーザー ID	ユーザーの一意の識別子。
名	ユーザーの名。
姓	ユーザーの姓。
タイトル	ユーザーの役職。タイトルまたはジョブの説明を入力するか、リストから選択します。
部門	ユーザーの部門。
パスワード	ユーザーにアサインされたパスワード。このパスワードは、永続的または一時的なものにすることができます。
パスワードのリセットを強制	セキュリティを確保するためにユーザーがパスワードをリセットできるようにするオプション。
ロックアウト	ユーザーをインスタンスからロックアウトし、ユーザーのすべてのアクティブなセッションを終了するオプション。admin ロールを持つユーザーはロックアウトできません。
有効	このユーザーをアクティブにするオプション。次の領域では、自分だけが非アクティブなユーザーを見ることができます。 ○ ユーザーのリスト ○ 参照フィールドの選択リスト (虫眼鏡アイコン) ○ 参照フィールドに入力すると表示されるオートコンプリートリスト
Web サービスへのアクセスのみ	このユーザーを非インタラクティブユーザーとして指定するオプション。
内部統合ユーザー	このユーザーを内部統合ユーザーとして指定するオプション。
メール	ユーザーのメールアドレス。
言語	ユーザーの優先言語。
カレンダー同期	ワークスケジュールの管理に使用されるカレンダー。たとえば、 Outlook です。
タイムゾーン	このユーザーがいる場所のタイムゾーン。
日付形式	ユーザーの優先日付形式。
電話 (勤務先)	ユーザーの勤務先電話。
携帯電話	ユーザーの携帯電話。
写真	[クリックして追加...] をクリックしてアップロードできる写真。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. **[Submit]** をクリックします。
6. オプション: ステップ 1 ～ 5 を繰り返して、例外承認者：レベル 2 CC を作成します。

   注:
   第 2 レベルの承認者の作成時に、[例外承認者：レベル **2 CC]** を選択します。

7. オプション: [編集] を選択した場合は、ユーザーを [コレクション] から [グループメンバー] パネルに移動し、[保存] をクリックします。
   承認者は次の場所に移動する必要があります **All** (すべて) > コンフィグレーションコンプライアンス > 自分の承認 要求を承認します。

コンフィグレーションコンプライアンス 重要度マップの作成

コンフィグレーションコンプライアンス 重要度マッピングは、サードパーティソースの重要度フィールドを コンフィグレーションコンプライアンス 重大度の認識可能なフィールドに変換するための変換マップを提供します。

始める前に
必要なロール：sn_vulc.admin

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > 重要度マッピング.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

フィールドマッピング

フィールド	説明
ソース	重大度マッピングのソースの名前。
ソース値	ソース重要度の値
ターゲット値	ターゲット値。選択肢は次のとおりです。 重大 コントロールに関連する構成の問題は、1 つ以上の事業上重要な CI の中断を引き起こしています。 高 コントロールに関連する構成の問題は脅威ではありますが、重要なネットワークリソースのシャットダウンを引き起こしているわけではありません。 中 コントロールに関連する構成の問題はリスクではありますが、差し迫った脅威ではありません。 低 コントロールに関連する構成の問題は低レベルの脅威であり、よりリスクの高い CI を優先して無視できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	マイナー コントロールに関連する構成の問題は軽微なリスクであり、必要に応じて無視できます。

4. **[Submit]** をクリックします。

メール通知を作成する

脆弱性アドミニストレーターは、通知を編集するか、新しい通知を追加して、通知の送信タイミング、通知の受信者、通知の内容を指定できます。

始める前に
必要なロール：sn_vulc.admin

このタスクについて
さまざまなタイプのメール通知用にメールテンプレートを作成できます。メールテンプレートの作成方法の詳細については、「脆弱性対応 のメールテンプレートを削除」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > 通知.
2. 修復ターゲットの通知レコードを選択するか、[新規] を選択します。
3. 必要に応じて、フォームのフィールドに入力します。
   フォームフィールドの詳細については、「Create an email notification」を参照してください。
4. [通知をプレビュー] を選択してメッセージを表示します。

タスクの結果
コンフィグレーションコンプライアンスの v14.11 以降の脆弱性対応では、受信者がメール通知のリンクをクリックすると、ロールに基づいてレコードが Vulnerability Manager ワークスペースまたは IT 修復ワークスペースで開きます。

- リンクが Vulnerability Manager ワークスペース で sn_vulc.admin ロールを持つユーザー用に開きます。
- リンクが IT 修復ワークスペース で sn_vulc.remediation_owner ロールを持つユーザー用に開きます。

受信者に前述のいずれのロールもない場合は、メール通知のリンクがクラシック UI で開きます。

コンフィグレーションコンプライアンスでの例外管理の承認ルールの構成

コンフィグレーションコンプライアンス v13.0 以降では、フローデザイナーを使用して、例外管理および例外ルールの例外要求を承認します。CC を初めて展開した場合、フローデザイナーはデフォルトで有効になっています。

始める前に
必要なロール：sn_vulc.admin

このタスクについて
既存のコンフィグレーションコンプライアンスユーザーの場合、デフォルトのオプションはワークフローです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンフィグレーションコンプライアンス v13.0 以降を展開した場合、システムプロパティ *sn_vulc.flow_designer_activation* の値は true に設定されます。つまり、フローデザイナーはデフォルトで有効になっています。

v13.0 より前のコンフィグレーションコンプライアンスを既に使用している場合、このシステムプロパティの値は false に設定されます。値を true に変更すると、フローデザイナーをアクティブ化できます。

注:
フローデザイナーをアクティブ化した後、 ワークフローの使用に戻すことはできません。ワークフローとフローデザイナーの詳細な比較については、「コンフィグレーションコンプライアンスでの例外管理ワークフローとフローデザイナー」を参照してください。

フローデザイナーを使用するには、 承認ルールモジュールを使用してルールを作成します。このモジュールを使用すると、以下の各例外管理ワークフローの承認ルールを構成できます。

- 修復タスクの例外承認ルール
- 自動例外ルールの承認ルール

注:
ルール内に複数の承認レベルを含む条件を定義することもできます。フローデザイナーは、このモジュールで作成されたルールを自動的に継承し、一致する承認ワークフローを処理します。承認レベルの構成の詳細については、「コンフィグレーションコンプライアンスでの例外管理の承認レベルの作成」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > 承認ルール > 修復タスクの例外承認ルール.
2. [承認ルール] ページで、承認ルールを設定するグループを選択します。
3. フォームのフィールドに入力します。

承認ルールフォーム

フィールド	説明
名前	承認構成名。
テーブル	ルールが適用されるテーブル。
アプリケーション	デフォルト値はコンフィグレーションコンプライアンスです。
ルールタイプ	ルールタイプを指定します。たとえば、例外管理や例外ルールなどです。
有効	デフォルトで有効になっており、承認ルールが使用中であることを示します。
説明	承認ルールの簡単な説明。
承認の有効期限 (日数) コンフィグレーションコンプライアンスの v14.11 以降	承認者が要求を承認できる期限。
承認者に通知 (日数)	承認者にアクションを実行するよう通知される日付。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
コンフィグレーションコンプライアンスの v14.11 以降	

4. [更新] を選択します。
   [承認構成] タブには、デフォルトで 2 つのレベルの承認者が設定されています。ルールを選択して、ルール内のさまざまなユースケースに基づいて条件を定義できます。詳細については、「コンフィグレーションコンプライアンスでの承認ルールの構成の作成」を参照してください。

   注:
   各構成ページで、複数の承認レベルを作成できます。詳細については、「コンフィグレーションコンプライアンスでの例外管理の承認レベルの作成」を参照してください。

Example:
さまざまなユースケースに基づいて、異なる修復タスクで見つかった同じテスト結果に対して、異なる承認プロセスを定義できます。

コンフィグレーションコンプライアンスでの承認ルールの構成の作成

承認レベルの一致する修復タスクを除外するための条件を定義します。

始める前に
必要なロール：sn_vulc.admin

このタスクについて
承認構成モジュールでは、さまざまな構成に対して複数のレベルの承認を構成できます。条件ベースのルールを定義します。各ルールには複数の承認レベルが含まれています。

注:
承認ルールモジュールを使用して、例外管理ワークフローの承認ルールを構成します。承認ルールの構成の詳細については、「コンフィグレーションコンプライアンスでの例外管理の承認レベルの作成」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > 承認ルール.
2. 承認ルールを選択し、[承認構成] タブに移動します。
3. 構成を選択します。
4. フォームのフィールドに入力します。

[承認構成] フォーム

フィールド	説明
名前	承認構成名。
承認ルール	承認ルールのテーブルとタイプの詳細が含まれています。
順序	ルール内のさまざまな構成の実行順序。たとえば、順序エントリーが 100 の構成は、順序エントリーが 200 の構成よりも前に実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
有効	デフォルトで有効になっており、承認構成が使用中であることを示します。
説明	承認構成レベルの簡単な説明。

5. 次のいずれかの方法で、テスト結果または修復タスクの条件を設定します。

フィールド	説明
条件	一致するテスト結果または修復タスクを識別します。
詳細条件	テスト結果または修復タスクの条件を定義するスクリプト。 **注:** このフィールドは、[詳細] チェックボックスをオンにした場合に表示されます。

6. [更新] を選択します。
ルール内に複数の承認レベルを含む条件を定義できます。フローデザイナーは、このモジュールで作成されたルールを自動的に継承し、一致する承認ワークフローを処理します。承認レベルの構成の詳細については、「コンフィグレーションコンプライアンスでの例外管理の承認レベルの作成」を参照してください。

Example:
さまざまなタイプの修復タスクごとに異なる承認パスを定義できます。

コンフィグレーションコンプライアンスでの例外管理の承認レベルの作成

例外要求を承認するユーザーとユーザーグループのレベルを定義します。

始める前に
必要なロール：sn_vulc.admin

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > 承認ルール.
2. 承認ルールを選択し、[承認構成] タブに移動します。
3. 構成を選択します。
4. [承認者レベル] セクションで、承認者レベルを選択します。
5. フォームのフィールドに入力します。

[承認者レベル] フォーム

フィールド	説明
名前	承認レベル名。
承認が必要	選択したレベルに必要な承認数を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	○ 1 人の承認者が必要 ○ すべてのユーザーの承認が必要
有効	デフォルトで有効になっており、承認レベルが使用中であることを示します。
順序	ルール内のさまざまな構成の実行順序。たとえば、順序エントリーが 100 の構成は、順序エントリーが 200 の構成よりも前に実行されます。
承認ルール	承認ルールのテーブルとタイプの詳細が含まれています。このフィールドは読み取り専用です。
承認構成	承認構成が含まれています。このフィールドは読み取り専用です。
次を使用してアサイン	以下のいずれかのオプションを選択します。 ○ ユーザーおよびユーザーグループ ○ 承認テーブルフィールド ○ スクリプト
グループ	複数のユーザーで構成される承認者レベルグループ。ユーザーは、例外管理および例外ルールのための次のいずれかのロールを持っている必要があります。 ○ sn_vulc.exception_approver ○ sn_vulc.read ○ sn_vulc.read_auto_exception_rule
ユーザー	グループにリストされているユーザーを編集します。

6. 変更を保存するには、[更新] を選択します。

> **注:**
> v13.0 より前では、例外レベル 1 にのみユーザーがいる場合、ワークフロープロセスは機能します。ただし、v13.0 以降は、各レベルに少なくとも 1 人のユーザーが必要です。
>
> v13.0 より前では、ワークフローで第 2 レベルにユーザーが存在しない場合、修復タスクは保留されていました。しかし、v13.0 以降では、第 2 レベルにユーザーが存在しない場合、承認要求は自動的に却下されます。

Example:
Linux サーバーと Windows サーバーの修復タスクには、さまざまな承認レベルが存在する場合があります。

コンフィグレーションコンプライアンスでの例外管理ワークフローとフローデザイナー

コンフィグレーションコンプライアンス (CC) v13.0 以降では、CC を初めて展開する場合は、例外管理で例外要求を承認するためのフローデザイナーがデフォルトで有効になります。既存の CC ユーザーの場合、デフォルトのオプションはワークフローです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ワークフローとフローデザイナー

考慮事項	Workflow	フローデザイナー
バージョン	CC の v13.0 より前。	CC の v13.0 以降。
デフォルトオプション	既存の CC ユーザーのデフォルトのオプション。	v13.0 以降の新しい CC ユーザーのデフォルトのオプションです。
承認プロセスの設定	例外管理には、例外ルールとともに例外の要求が含まれます。	さまざまなユースケースに対する各種のレベルの定義、各種の承認者の追加などがあります。ワークフローより簡単に実装できます。例外管理には、例外ルールとともに例外の要求が含まれます。
フローデザイナーへのアップグレード	ワークフローからフローデザイナーにアップグレードできます。ただし、既存の要求は、ワークフローを使用してのみ承認できます。	フローデザイナーはデフォルトで有効になっています。
システムプロパティ *sn_vulc.flow_designer_activation*	v13.0 より前の例外管理にワークフローを使用している場合、システムプロパティは false に設定されます。フローデザイナーをアクティブ化するには、このプロパティを true に設定します。 **注:** フローデザイナーをアクティブ化した後、 ワークフローの使用に戻すことはできません。	v13.0 以降で CC を初めて使用する場合、システムプロパティ値はデフォルトで true に設定されています。
承認ルールモジュール	システムプロパティを true に設定すると、「承認ルールモジュールを有効化」スケジュール済みジョブが 24 時間以内に実行されます。このスケジュール済みジョブにより、承認ルールモジュールが有効になります。このモジュールをすぐにアクティブ化するには、このジョブを手動で実行します。	CC v13.0 から、初めて CC を展開した場合、このモジュールはデフォルトで使用可能です。
承認レベル	2 つのレベルの承認者のみを設定するオプションを提供します。	任意の数の構成、承認者レベルの設定、各ルールの承認者の動的な追加など、複数のオプションを提供します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンフィグレーションコンプライアンス の統合

サードパーティ統合により、構成アセスメントの結果、ポリシー、テスト、テクノロジー、信頼できるソース、テスト結果が、その他の脆弱性データとともに コンフィグレーションコンプライアンス アプリケーションにインポートされます。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

コンフィグレーションコンプライアンス アプリケーションは、次のサードパーティ統合をサポートしています。

- v14.11 以降では、コンフィグレーションコンプライアンスアプリケーションで結果をテスト結果として公開することで、セキュリティポスチャコントロールアプリケーションによって特定されたエンタープライズ資産のセキュリティギャップの修復が促進されます。セキュリティポスチャコントロールアプリケーションとそのサポートされているアプリケーションは、ServiceNow Store から個別のサブスクリプションで利用できます。詳細については、「セキュリティポスチャコントロール」を参照してください。
- Microsoft Defender for Cloud Integration for セキュリティオペレーション
- Palo Alto Prisma Cloud 脆弱性統合
- Qualys と コンフィグレーションコンプライアンス との統合
- Tenable 脆弱性統合の Tenable.io 製品

統合に関するその他の注意事項

統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、コンフィグレーションコンプライアンスのバージョン 14.8.5 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

Microsoft Defender for Cloud Integration for セキュリティオペレーション

Microsoft Defender for Cloud Integration 製品は、クラウド環境のセキュリティ体制を強化するインフラストラクチャセキュリティ管理システムです。

Microsoft Defender for Cloud Integration for セキュリティオペレーション が コンフィグレーションコンプライアンス アプリケーションと統合して、テストを構成アイテム (CI) にマッピングしてテスト結果を作成します。ワークロード全体に展開された新しいクラウドリソースを継続的に検出し、Center for Internet Security (CIS) などのセキュリティ標準に従って構成されているかどうかを判断します。

バージョン 2.2 以降、Microsoft Azure Security Center は Microsoft Defender for Cloud Integration for セキュリティオペレーション に名前が変更されました。

利用可能バージョン

アプリケーション	バージョン
Microsoft Defender for Cloud Integration for セキュリティオペレーション	2.3
コンフィグレーションコンプライアンス	14.3
Security Support Common	13.2
脆弱性対応	16.2

Microsoft Defender for Cloud プラットフォームの複数展開

Microsoft Defender for Cloud Platform アプリケーションを複数展開している場合は、展開ごとに統合を追加できます。複数のサードパーティの展開によって識別されるリソースは、構成管理データベース (CMDB) と統合され、調整されます。この統合は、複数の展開間でスキャンプロセスが重複している場合でも行われます。

ServiceNow Microsoft Defender for Cloud 統合

Microsoft Defender for Cloud Integration for セキュリティオペレーション は、Microsoft Defender for Cloud からデータを取得することによってインスタンスのコンプライアンスデータを強化します。一連のスケジュール済みジョブによって、統合が自動的に呼び出されます。これらのスケジュール済みジョブは手動で実行することもできます。スケジュール済みジョブは、Microsoft Defender for Cloud とのインスタンスの同期を維持することで、テスト結果の修復ライフサイクルを簡素化します。

統合レコードごとに run-as ユーザーが構成され、デフォルト値は **VR.System** です。この値は同じでなければなりません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
有効な run-as ユーザーを設定しないと、データソースレコードに重複したファイルまたは複数のデータ取得添付ファイルが作成されます。統合が実行されるたびに添付ファイルの数が増えます。これにより処理時間が増え、変換結果に一貫性がなくなります。

Microsoft Defender for Cloud Platform 統合タスクには、次のロールが含まれます。

- sn_vul_asc.configure_integration：レコードを読み取り、書き込み、削除することができます。
- sn_vul_asc.read_integration：レコードを読み込むことができます。

Microsoft Defender for Cloud 統合の表示

に移動して統合を表示するには **All** (すべて) > **Microsoft Defender for Cloud** の統合 > 統合.

ベースシステムには、次の統合が含まれています。

統合	説明
ポリシー定義統合	ポリシーを取得し、インスタンスにポリシーエントリーを作成します。
アセスメントメタデータ統合	アセスメントメタデータを取得し、インスタンスにテストを作成します。
コンプライアンス標準とコントロール統合	標準とコントロールを取得し、認証ソースと引用を作成します。次に、それらを作成したテストにリンクさせます。
アセスメント統合	アセスメントを取得し、インスタンスで処理します。この統合の出力はテスト結果です。

識別および調整エンジンを使用した CI の作成

既存の CI がサードパーティのスキャナーからインポートされたホストと一致しない場合、識別および調整エンジン (IRE) を使用して CI を作成します。

CI が CMDB で一致しない場合、CI は *cmdb_ci_cmp_resource* クラスに作成されます。後で、検出で同じ CI が見つかると、CI が拡張されるか、別の CI が作成されます。

注:
クラウドリソースでは自動調整は行われません。

Microsoft Defender for Cloud Integration for セキュリティオペレーション のインストールと構成

Microsoft Defender for Cloud からインポートされたデータを使用して、優先順位を付け、資産の構成ミスを修正できるように、Microsoft Defender for Cloud Integration for セキュリティオペレーション をインストールして構成します。

始める前に
Azure Active Directory で新しいアプリ登録を作成します。Azure Active Directory で新しいアプリケーションを登録する方法の詳細については、Microsoft ドキュメント サイトで「Register a client application in Azure Active Directory (Azure Active Directory でクライアントアプリケーションを登録する)」を検索してください。ServiceNow への接続に使用する関連スコープで、新しく作成されたアプリ登録のセキュリティリーダーロールをアサインします。これは、管理グループまたはサブスクリプションレベルで行うことができます。

必要なロール：sn_vulc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > システム定義 > プラグイン.
2. 検索バーで、Microsoft Defender for Cloud Integration for Security Operations を検索します。
3. [インストール] を選択します。

   インストールされる依存関係が表示されます。
4. [] に移動します。**All** (すべて) > **Microsoft Defender for Cloud** の統合 > アドミニストレーション > 構成 > **Microsoft Defender for Cloud** の構成.
5. フォームのフィールドに入力します。

Microsoft Defender for Cloud 構成フォーム

フィールド	説明
API URL	インスタンスのリソース URL 。 例：https://management.azure.com (Azure パブリッククラウド)
テナント ID	組織のテナント ID。
統合インスタンス	デフォルトインスタンス。インスタンスを作成して、複数の Microsoft Defender テナントまたはサブスクリプションからデータを取得することもできます。
クライアント ID	Microsoft Defender for Cloud Integration アプリケーションが登録された後に生成されるクライアント ID。
クライアントシークレット	Microsoft Defender for Cloud Integration アプリケーションが登録された後に生成されるクライアントシークレット。
結果のインポート元	選択された管理グループ ID と取得されるサブスクリプション IDに対応するリソースとアセスメント。
管理グループ ID	取得される管理グループ ID に対応するリソースとアセスメント。 **注:** このフィールドは、[結果のインポート元] フィールドで [特定の管理グループ] を選択した場合にのみ表示されます。
サブスクリプション ID	リソースとアセスメントを取得するサブスクリプションの識別番号。 **注:** このフィールドは、[結果のインポート元] フィールドで [特定のサブスクリプション] を選択した場合にのみ表示されます。
検証ステータス	指定された認証情報とサブスクリプション ID が有効かどうか。

6. [保存してテスト] を選択して、統合を設定または実行します。

コンフィグレーションコンプライアンスインポートされたデータ：**Microsoft Defender for Cloud Integration**

コンフィグレーションコンプライアンス は、サードパーティの統合からポリシー、テスト、信頼できるソース、およびテスト結果をインポートし、表示するためにモジュールに保存します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

テストグループ

テストグループは設定テストのグループで構成されます。テストグループは信頼できるドキュメントとテストレコードに関連しており、組織のニーズに合わせて変更できます。1 つの設定テストは複数のテストグループに属することができます。

Microsoft Defender for Cloud Integration がインストールされている場合、テストグループはスケジュール済みジョブであるポリシー定義統合によって取得され、入力されます。スケジュール済みジョブを表示するには、次に移動します: **All** (すべて) > **Microsoft Defender for Cloud** の統合 > アドミニストレーション > 統合 > ポリシー定義の統合.

注:
統合の手動実行を選択した場合は、最初にポリシー定義統合 を実行します。

テスト

テストは、コンピューティング資産のスキャンを整理するデータレコードのライブラリです。設定テストでは、資産を管理する方法を定義します。

コンフィグレーションコンプライアンス テストは、サードパーティの統合アプリケーションがテスト結果タイプ別に資産をグループ化するために使用するメカニズムです。

Microsoft Defender for Cloud Integration がインストールされている場合、スケジュール済みジョブであるアセスメントメタデータ統合がテストを取得します。スケジュール済みジョブを表示するには、次に移動します: **Integration** (統合) > プライマリ統合 > アセスメントメタデータ統合.

注:
統合の手動実行を選択した場合は、ポリシー定義統合の後に、アセスメントメタデータ統合を実行します。

コンフィグレーションコンプライアンスの v15.0 以降では、テストが属するテストグループが [テスト] リストの [テストグループ] 列に入力されます。

信頼できるソース

コンフィグレーションコンプライアンス は、テストの脆弱性アラートを生成するときに信頼できるソースと引用を使用します。通常、信頼できるソースは、**ISO 27001** や **PCI DSS 3.2.1** などの公開された業界標準のセクションにマッピングされます。

これらのソースレコードには、コンピューターセキュリティの分野のエキスパートからの既知のソフトウェアおよびハードウェア構成の問題に関する情報が含まれています。これらは、セキュリティ方針と手順の要件を定義します。

Microsoft Defender for Cloud Integration がインストールされている場合、スケジュール済みジョブであるコンプライアンス標準とコントロールは、信頼できるソースと引用を取得します。この

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みジョブを表示するには、次に移動します: **All** (すべて) > **Microsoft Defender for Cloud** の統合 > 統合 > コンプライアンス標準とコントロール統合.

> **注:**
> 統合の手動実行を選択した場合は、アセスメントメタデータ統合の後に、コンプライアンス標準とコントロール統合を実行します。

資産

アセスメント統合は、リソースタグやクラウド属性などの重要な情報を提供します。この情報は、[検出されたアイテム] フォームに表示されます。これは主に、コンフィグレーションコンプライアンスのアサインルールと修復タスクルールでのフィルタリングに使用されます。

- リソースタグ：すべてのクラウドリソースタグは、アセスメント統合の一部としてホストタグとしてインポートされます。クラウドリソースタイプのクラウドタグは、リソースがホストであるかどうかにかかわらずここに格納されます。
  - タグストレージでは大文字と小文字は区別されません。「Tokyo」タグが作成された場合、「**TOKYO**」タグを [ホストタグ] テーブルに格納することはできません。「**Tokyo**」と「**TOKYO**」は同じホストタグと見なされます。最初にインポートされたタグが優先されます。
  - グループルールでホストタグをグループキーとして使用すると、予期しない結果になる可能性があります。ホストタグは、条件ビルダー専用です。
- 資産のクラウド属性：統合が Microsoft Defender for Cloud から取得するクラウド属性は次のとおりです。
  - クラウドアカウント
  - クラウドリージョン
  - クラウドリソースタイプ
  - クラウドサービスプロバイダー

テスト結果

コンフィグレーションコンプライアンス はテスト結果を計算しませんが、サードパーティ統合の一部としてインポートします。コンフィグレーションコンプライアンスで表示できるようになると、[修復タスク] を使用して修正されます。

Microsoft Defender for Cloud 統合がインストールされている場合、スケジュール済みジョブであるアセスメント統合はテスト結果を取得します。このスケジュール済みジョブを表示するには、次に移動します: **All** (すべて) > **Microsoft Defender for Cloud** の統合 > 統合 > アセスメント統合.

アセスメント統合のインポートは、[統合の詳細] タブで *`Start Time`* パラメーターを使用する唯一の統合です。他のすべての コンフィグレーションコンプライアンス インポートでは、*`Start Time`* に関係なく、利用可能なすべてのデータが取り込まれます。

アセスメント統合のインポートが完了すると、インポート終了の計算をトリガーするイベントが開始されます。

デフォルトでは、アセスメント統合は、過去 1 日間の最後の正常な統合実行からステータスが変更された場合にのみ、データアセスメントをプルします。そのため、アセスメントが過去数日間にわたり継続的に失敗している場合、アセスメントのステータスは変更されていないため、統合はアセスメントをフェッチしません。Defender アセスメントでテスト結果を最新の状態に保つために、過去 7 日間のデータをプルする新しい包括的なアセスメント統合が追加されています。この統合は毎週実行され、合格しなかったすべてのテスト結果をプルします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Microsoft Defender for Cloud 統合から CI を識別するための CI ルックアップルール

サードパーティの統合からデータがインポートされると、コンフィグレーションコンプライアンスは自動的にリソースデータを使用して、CI ルックアップルールに基づいて 構成管理データベース (CMDB) 内で一致するものを検索します。これらのルールは、構成アイテム (CI) を識別し、それらをテスト結果レコードに追加して修復する際に使用されます。ベースシステムの CI ルックアップルールは、リソース ID、名前、および S3 バケットで使用できます。CI ルックアップルールの詳細については、「CI lockup rules for Microsoft Defender for Cloud Integration for Security Operations (Microsoft Defender for Cloud Integration for Security Operations の CI ルックアップルール)」を参照してください。

Vulnerability Response Integration with Palo Alto Prisma Cloud の概要

Prisma Cloud は、API ベースのクラウドインフラストラクチャセキュリティソリューションです。クラウド環境に接続し、Amazon Web サービス (AWS)、 Microsoft Azure などのパブリッククラウド環境に展開されたリソースを監視します。パブリッククラウドインフラストラクチャ内のリスクを完全に可視化して制御できます。

Vulnerability Response Integration with Palo Alto Prisma Cloud アプリケーションは、コンフィグレーションコンプライアンス アプリケーションで Prisma Cloud からのポリシーとアラートをテストおよびテスト結果として取り込めるようにします。適切な構成を使用すると、適切なリスクスコアをアサインし、それらをグループ化して関連するユーザーとグループにアサインすることで、テスト結果をシームレスに管理できます。

利用可能バージョン

このテーブルには、Vulnerability Response Integration with Palo Alto Prisma Cloud が依存するアプリケーションとそのバージョンが表示されます。

アプリケーション	バージョン
Prisma Cloud integration for Security Operations	2.3
コンフィグレーションコンプライアンス	14.7
Security Support Common	13.5
脆弱性対応	18.0

ServiceNow Prisma Cloud 統合

Vulnerability Response Integration with Palo Alto Prisma Cloud アプリケーションは、Prisma データを ServiceNow インスタンスにインポートして、より適切に管理できるようにインスタンスを強化するのに役立ちます。一連のスケジュール済みジョブによって、統合が自動的に呼び出されます。これらのスケジュール済みジョブは手動で実行することもできます。スケジュール済みジョブは、Prisma Cloud から定期的にデータを取得してインスタンスを最新の状態に保つことで、テスト結果の修復ライフサイクルを簡素化します。

Prisma Cloud 統合タスクには、次のロールが関与します。

- sn_vul_prismacloud.configure_integration：レコードの読み取り、書き込み、削除が可能です。
- sn_vul_prismacloud.read_integration：レコードの読み取りが可能です。

統合の表示

Vulnerability Response Integration with Palo Alto Prisma Cloudの一部である統合を表示するには、次に移動します: **Prisma Cloud** 統合 > 統合.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

次の統合がベースシステムで使用できます。

実行シーケンス	スケジュール	統合	説明
1	週次	Prisma ポリシー統合	• Prisma Cloud からポリシーを取得し、インスタンスのテストエントリーを作成します。 • 増分サポートは提供していません。過去 10 日間の統合を実行すると、以前の統合実行の結果も表示されます。
2	日次	Prisma アラート統合	• Prisma Cloud からアラートを取得し、インスタンスのテスト結果のエントリーを作成します。 • 増分サポートを提供しています。統合は、前回の統合実行時間の後に毎日実行されます。

Vulnerability Response Integration with Palo Alto Prisma Cloud のインストールの準備

セットアップタスクを実行して、Vulnerability Response Integration with Palo Alto Prisma Cloud のインストールを準備します。

事前準備

脆弱性対応を Palo Alto Prisma Cloud と統合するには、ポリシーおよびアラートデータへの読み取り専用アクセスを提供する Prisma の権限グループがアサインされている必要があります。権限グループの詳細については、「Prisma Cloud Administrator Roles (Prisma Cloud 管理者ロール)」を参照してください。

さまざまな権限グループに割り当てられたロールの詳細については、「Prisma Cloud Administrator Permissions (Prisma Cloud 管理者権限)」ページを参照してください。

さらに、アラートを読み取れるようにアクセスキーを作成する必要があります。アクセスキーの作成の詳細については、「Create and Manage Access Keys (アクセスキーの作成と管理)」を参照してください。

Vulnerability Response Integration with Palo Alto Prisma Cloud をインストールして設定するには、次のチェックリストを使用します。アプリケーションをインストールする前に、リストされたアイテムが完了していることを確認してください。

統合準備チェックリスト

タスク	説明
☐	次の情報セットがあることを確認します。 • API ベース URL • アクセスキー ID • 秘密キー • Prisma Cloud にアクセスするためのユーザー名とパスワード。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統合準備チェックリスト (続く)

タスク	説明
	これらの認証情報は、Now Platform® インスタンスから Prisma Cloud インスタンスに接続するために使用されます。アクセスキー ID と秘密鍵は、登録後に Prisma Cloud ポータルから生成する必要があります。
☐	まだインストールしてアクティブ化していない場合は、Vulnerability Response Integration with Palo Alto Prisma Cloud アプリケーションをインストールする前に 脆弱性対応 アプリケーションをインストールします。 脆弱性対応 アプリケーションのインストールとアクティブ化の詳細については、「脆弱性対応 のインストール」を参照してください。この統合には、脆弱性対応 のバージョン 15.2.0 以降が必要です。
☐	まだアプリケーションがインスタンスにない場合は、エンタイトルメントを取得して、Vulnerability Response Integration with Palo Alto Prisma Cloud アプリケーションを Now Platform® インスタンスにダウンロードします。 「」を参照してください。
☐	スムーズな統合を実行するために、次のプラグインがインストールされていることを確認してください。 • 脆弱性対応 • コンフィグレーションコンプライアンス • Vulnerability Response Integration with Palo Alto Prisma Cloud 次のプラグインはオプションですが、役に立つ場合があります。 • Cloud Provisioning and Governance • ディスカバリーとサービスマッピングパターン
☐	インポートする予定のテスト結果の数を見積もります。 インポートする予定のテスト結果の数をインスタンスが受け入れることができることを確認します。インスタンスが小さすぎると、ロードに時間がかかることがあります。インスタンスのサイズがわからない場合、またはサポートが必要な場合は、ServiceNow テクニカルサポートにお問い合わせください。
☐	統合を管理し、テスト結果を修正するアドミニストレーターがいることを確認します。 アドミニストレーターは、Vulnerability Response Integration with Palo Alto Prisma Cloud アプリケーションをインストールします。アサインされていない場合、アドミニストレーターは脆弱性アドミン (sn_vul.vulnerability_admin) およびその他のロールをアサインします。

これで、「Vulnerability Response Integration with Palo Alto Prisma Cloud アプリケーションのインストールと構成」に進む準備が整いました。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Vulnerability Response Integration with Palo Alto Prisma Cloud アプリケーションのインストールと構成

Prisma Cloud からインポートされたデータを使用するには、Vulnerability Response Integration with Palo Alto Prisma Cloud アプリケーションをインストールします。このデータを使用して、資産の構成ミスに優先順位を付けて修正します。

始める前に

必要なロール：admin

手順

1. 次のように移動する。 システム定義 > プラグイン.
2. 検索バーで、「Vulnerability Response Integration with Palo Alto Prisma Cloud」を検索します。
3. [インストール]をクリックします。

   インストールされる依存関係が表示されます。
4. 次のように移動する。 **All** (すべて) > **Prisma Cloud** 統合 > アドミニストレーション > 構成 > **Prisma** クラウド構成.
5. フォームのフィールドに入力します。

フィールド	説明
統合インスタンス	新しい統合インスタンスの名前。 インスタンスを作成するか、ルックアップアイコンをクリックして既存のインスタンスを選択できます。
API URL	Prisma Cloud と統合するための URL。
アクセスキー ID	Prisma Cloud へのアクセス要求を認証するための一意のキー。 **注:** Prisma Cloud ポータルにログインした後にキーを生成する必要があります。
秘密キー	Prisma Cloud へのアクセス要求を認証するための秘密鍵。 **注:** Prisma Cloud ポータルにログインした後に秘密鍵を生成する必要があります。

6. [保存してテスト] をクリックします。

次のタスク

インストールが完了したら、次に移動します: **Prisma Cloud** 統合 > 構成 構成を続行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Vulnerability Response Integration with Palo Alto Prisma Cloud アプリケーションの構成

Vulnerability Response Integration with Palo Alto Prisma Cloud アプリケーションを構成します。Prisma Cloud からインポートされたデータを使用して、資産の構成ミスに優先順位を付けて修正します。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 **Prisma Cloud** 統合 > 構成.
2. フォームのフィールドに入力します。

Prisma クラウド構成

フィールド	説明
統合インスタンス	新しい統合インスタンスの名前。 インスタンスを作成するか、ルックアップアイコンをクリックして既存のインスタンスを選択できます。
API URL	Prisma Cloud と統合するための URL。
アクセスキー ID	Prisma Cloud へのアクセス要求を認証するための一意のキー。 Prisma Cloud ポータルにログインした後にキーを生成する必要があります。
秘密キー	Prisma Cloud へのアクセス要求を認証するための秘密鍵。 Prisma Cloud ポータルにログインした後に秘密鍵を生成する必要があります。

3. [保存してテスト] をクリックします。

次のタスク
構成が完了したら、次に移動します: **Prisma Cloud** 統合 > 統合 統合の実行が成功したことを確認します。

Vulnerability Response Integration with Palo Alto Prisma Cloud インポートの実行状況の確認

Vulnerability Response Integration with Palo Alto Prisma Cloud インポートの実行状況を使用して、統合が正常に実行されたことを確認し、問題を特定します。

始める前に
必要なロール：admin

このタスクについて
統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タの処理を続行します。この通信ミスを回避するために、コンフィグレーションコンプライアンスのバージョン 14.8.5 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

手順

1. 次のように移動する。 **Prisma Cloud** 統合 > 統合.
2. **[Prisma** ポリシー統合 **(Prisma Policies Integration)]** をクリックします。
3. [今すぐ実行] をクリックします。
   この統合を実行すると、次のテーブルがこの順序で入力されます。
   a. sn_vulc_test.list (構成テスト)
   b. sn_vulc_auth_src (信頼できるソース)
   c. sn_vulc_citation (引用)
4. [アイテム] タブで、[脆弱性統合実行] をクリックして、作成、更新、および無視された新しいテストの数を表示します。

   注:
   選択したクラウドインスタンスに対して Prisma Cloud でポリシーが定義されます。インスタンスは、定義されたポリシーに基づいてスキャンされます。

5. **[Prisma** アラート統合 **(Prisma Alerts Integration)]** をクリックします。
6. [今すぐ実行] をクリックします。
   統合に基づいて、次のテーブルに入力されます。
   - テスト結果
   - 検出されたアイテム：構成アイテムがシステムで利用できない場合に作成されます。クラスは常にクラウドリソースです。[検出されたアイテム] ページに、[クラウドリソースタイプ]、[クラウドサービスプロバイダー]、[資産カテゴリ] の 3 つの新しいフィールドが作成されます。

     [アイテム] タブで、[脆弱性統合実行] をクリックして、インポート、更新、および無視された新しいテストの数を表示します。[構成アイテム] タブにも、作成されたテスト結果の数に基づいて入力されます。

データマッピング

Prisma Cloud のデータは ServiceNow インスタンスの コンフィグレーションコンプライアンス モジュールにインポートされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

Prisma Cloud からのデータは、テーブルに記載されている コンフィグレーションコンプライアンス 内に別の名前でインポートされます。

コンフィグレーションコンプライアンスでの **Prisma Cloud** データのマッピング

Prisma Cloud	コンフィグレーションコンプライアンス
ポリシー	テスト
アラート	テスト結果
コンプライアンス標準	信頼できるソース
セクション	引用
資産	ディスカバリーアイテム/構成アイテム (CI)

テスト

Prisma Cloud のポリシーは、コンフィグレーションコンプライアンス にテストとしてインポートされます。ポリシーは信頼できるドキュメントとテストレコードに関連しており、組織のニーズに合わせて変更できます。に移動すると、テストを表示できます。 コンフィグレーションコンプライアンス > テスト.

Vulnerability Response Integration with Palo Alto Prisma Cloud がインストールされている場合、*`Prisma Policy Integration`* がテストを取得します。この統合ジョブを表示するには、次に移動します: **All** (すべて) > **Prisma Cloud** 統合 > **Prisma** ポリシー統合.

テスト結果

Prisma Cloud のアラートは、コンフィグレーションコンプライアンス にテスト結果としてインポートされます。アラートは、修復タスクを使用して修復されます。テスト結果を表示するには、次に移動します: コンフィグレーションコンプライアンス > テスト結果.

コンフィグレーションコンプライアンスは、サードパーティ統合の一部としてテスト結果をインポートします。コンフィグレーションコンプライアンスアプリケーションで表示できるようになると、[修復タスク] を使用して修正されます。

Palo Alto Prisma Cloud との脆弱性対応統合がインストールされている場合、統合ジョブ **Prisma** アラート統合がテストを取得します。この統合ジョブを表示するには、次に移動します: **All** (すべて) > **Prisma Cloud** 統合 > 統合 > **Prisma** アラート統合.

Prisma アラート統合は、毎日実行される統合ジョブであり、[統合] タブの [開始時間] フィールドで定義された時間が経過すると、ステータス変更を含むテスト結果をプルします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
統合ジョブ **Prisma** アラート統合を手動で実行する場合は、統合ジョブ **Prisma** ポリシー統合を実行した後に実行します。

Prisma アラート統合がデータのインポートを完了すると、インポート終了の計算をトリガーするイベントが開始されます。アラートが過去数日間にわたり継続的に失敗している場合、アラートのステータスは変更されていないため、統合はアラートをフェッチしません。そのため、Prisma アラートでテスト結果データを最新の状態に保つために、過去 7 日間に更新されたアラートをプルする新しい統合ジョブ、**Prisma** 包括的アラート統合が追加されます。この統合は毎週実行され、合格しなかったすべてのテスト結果をプルします。

信頼できるソース

コンフィグレーションコンプライアンス は、テストの脆弱性アラートを生成するときに信頼できるソースと引用を使用します。通常、信頼できるソースは、ISO 27001 や PCI DSS 3.2.1 などの公開された業界標準のセクションにマッピングされます。

これらのソースレコードには、コンピューターセキュリティの分野のエキスパートからの既知のソフトウェアおよびハードウェア構成の問題に関する情報が含まれています。これらのリファレンスはセキュリティポリシーと手順の要件を定義します。次のように移動する。 コンフィグレーションコンプライアンス > 信頼できるソース して、信頼できるソースを表示します。

資産

Vulnerability Response Integration with Palo Alto Prisma Cloud がインストールされている場合、スケジュール済みジョブ *`Prisma Alerts Integration`* は、検出されたアイテムモジュールまたはテーブルのアラート関連情報をキャプチャします。このスケジュール済みジョブを表示するには、次に移動します: **Prisma Cloud** 統合 > 統合.

Prisma アラート統合は、テーブルに格納されている追加のタイプの情報 (リソースタグやクラウド属性など) をインポートします。この情報は、[検出されたアイテム] フォームに表示されます。

- ホストタグ：リソースには複数のタグを使用できます。ホストタグはキーと値のペア形式で使用できます。たとえば、オペレーティングシステムが Windows 10 で、Java バージョンが 1.8。
- 資産のクラウド属性：次のクラウド属性を使用できます。
  - クラウドアカウント：統合からのアカウント ID を提供します。情報は、クラウドアカウント [sn_sec_cmn_cloud_account.LIST] テーブルから入力されます。
  - クラウドリージョン：リソースがホストされている場所を提供します。情報は、クラウドリージョン [sn_sec_cmn_cloud_account.LIST] テーブルから入力されます。
  - クラウドリソースタイプ：仮想マシンまたはデータベースインスタンスなど、リソースのタイプに関する情報を提供します。情報は、クラウドリソースタイプ [sn_sec_cmn_cloud_resource_type.LIST] テーブルから入力されます。
  - クラウドサービスプロバイダー：Amazon Web Services (AWS)、Oracle Cloud などのクラウドサービスプロバイダーに関する情報を提供します。情報は、クラウドサービスプロバイダー [sn_sec_cmn_cloud_service_provider.LIST] テーブルから入力されます。
  - クラウドアカウントグループ：アカウントグループに関する情報を提供します。情報は、クラウドアカウントグループ [sn_vul_prismacloud_account_group.list] テーブルから入力されます。

    注:
    クラウドアカウントグループ属性は、Prisma でのみ使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CI ルックアップルール

ベースシステムの CI ルックアップルールは、リソース ID、名前、および S3 バケットで使用できます。CI ルックアップルールの詳細については、「Microsoft Defender for Cloud Integration for セキュリティオペレーション と Palo Alto Prisma Cloud の CI ルックアップルール」を参照してください。

Prisma クラウド REST メッセージ

Prisma REST メッセージは、Prisma アプリケーションプログラミングインターフェイス (API) を呼び出してコンプライアンスデータをフェッチするために使用されます。

次の REST メッセージはベースシステムに付属しています。

Prisma クラウド統合

すべての Prisma クラウド統合は、認証と承認に JSON Web トークン (JWT) を使用します。

Prisma ログイン REST メッセージ

エンドポイント	説明	メソッド	本文	ドキュメントリンク
/login	後続のすべての統合で使用する JWT トークンを取得します。	*POST*	{ "username": <<access key id >>, "password": <<secret access key>>}	https://pan.dev/prisma-cloud/api/cspm/app-login/

Prisma リフレッシュトークン REST メッセージ

エンドポイント	説明	メソッド	本文	ドキュメントリンク
/auth_token/extend	有効期限が切れたときに JWT トークンを自動的に更新します。トークンの有効期限のデフォルト期間は 60 分です。	*GET*	NA	https://pan.dev/prisma-cloud/api/cspm/extend-session/

Prisma ポリシー REST メッセージ

エンドポイント	説明	メソッド	本文	ドキュメントリンク
/v2/policy	Prisma からすべてのポリシーデータを取得します。	*GET*	NA	https://pan.dev/prisma-cloud/api/cspm/get-policies/

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Prisma アラート REST メッセージ

エンドポイント	説明	メソッド	本文	ドキュメントリンク
/v2/alert	Prisma からすべてのアラートを取得します。	*POST*	{ "detailed": "false", "filters": [{ "name": "timeRange.type", "operator": "=", "value": "ALERT_STATUS_UPDATED" }], "sortBy": ["resource.id"], "pageToken": "", "offset": 0, "limit": 2000, "timeRange": { "type": "absolute", "value": { "startTime": <<Import since at integration level>>, "endTime": << Current integration run time>> } } }	https://pan.dev/prisma-cloud/api/cspm/post-alerts/

Prisma Comprehension アラート統合では、上記の POST 本文のフィルターを次のように置き換える必要があります。

```
"filters": [
{
            "name": "alert.status",
            "operator": "=",
            "value": "open"
        },
        {
            "name": "alert.status",
            "operator": "=",
            "value": "dismissed"
        },
        {
            "name": "alert.status",
            "operator": "=",
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
            "value": "snoozed"
         },
         {
            "name": "alert.status",
            "operator": "=",
            "value": "pending_resolution"
         },
         {
            "name": "timeRange.type",
            "operator": "=",
            "value": "ALERT_UPDATED"
         }

   ],
```

Qualys と コンフィグレーションコンプライアンス との統合

QualysPolicy Compliance がデータを収集して Qualys アプリケーションに自動的に送信すると、情報が継続的に分析され、関連付けられます。Security Operations の Qualys 統合として簡単に統合し、構成の検索結果を CI とビジネスサービスにマッピングして、潜在的な構成ミスの影響度と優先度を判断します。

Qualys クラウドプラットフォーム アプリケーションを複数展開している場合は、展開ごとに統合を追加できます。 複数のサードパーティの展開と脆弱性によって識別される資産は、CMDB と統合され、調整されます。この統合は、複数の展開間でスキャンプロセスが重複している場合でも行われます。各展開から供給されたデータは、脆弱性対応 の単一インスタンスで識別されて利用可能です。

注:
元の脆弱性統合は削除できませんが、無効にすることはできます。非アクティブなテンプレートから作成された統合は、デフォルトで無効になっています。

ホストタグ

すべてのホストタグは Qualys ホストリスト統合の一部としてインポートされます。ホストタグは、主に 脆弱性対応 アサインおよび修復タスクルールでのフィルタリングに使用されます。これらは [検出されたアイテム] フォームに表示されます。

注:
Qualys ホストリスト統合は、脆弱性一致アイテムがインポートされてグループ化される前にすべてのタグがルール内に存在できるように、脆弱性対応 でのアサインルールまたは修復タスクルールを作成する前に実行する必要があります。

- タグストレージでは大文字と小文字は区別されません。**[San Diego]** タグが作成されると、**[SAN DIEGO]** タグを [ホストタグ] テーブルに格納できなくなります。「San Diego」と「SAN DIEGO」は同じホストタグと見なされます。最初にインポートされたタグが優先されます。
- 修復タスクルールのグループキーとしてホストタグを使用すると、予期しない結果になることがあります。ホストタグは、条件ビルダー専用です。
- ホストタグは、グローバルシステムプロパティ **sn_vul.import_host_tags** で制御されます。このプロパティはデフォルトで [true] に設定されています。タグをオフにすると、すべてのインスタンスでオフになります。

ホストタグ (資産タグとも呼ばれます) は、組織の資産の整理と追跡に使用されます。ホスト資産にはタグを割り当てることができます。これにより、スキャンを開始するときに、スキャンするホストに関連付けられたタグを選択できます。ホストタグモジュールを使用すると、スケジュールに基づいて Qualys からインスタンスにホストタグデータをダウンロードできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テストとそのテストグループの関連付け

テストフォームの [テストグループ] フィールドに入力するには、 *sn_vulc.add_policy_as_key* システムプロパティを有効にします。テストをテストグループに関連付ける方法、このシステムプロパティを有効にした場合の影響、および事後要件の詳細については、 KB1644268 記事を参照してください。

> **警告:**
> *sn_vulc.add_policy_as_key* システムプロパティは、一度有効にすると無効にできません。そのため、このシステムプロパティを有効にする前に、 KB1644268 記事の [影響度] セクションを確認してください。

このシステムプロパティを有効にすると、次の取り込み後に [テストグループ] フィールドがテストテーブルに追加され、テストが属するテストグループが設定されます。したがって、次のことを簡単に行うことができます。

- テストからテストグループへとドット連結して、テスト結果が属するテストグループを特定します。
- 異なるテストグループに関連付けられている同じテスト ID を持つテストレコードを区別します。

Qualys と ServiceNow® コンフィグレーションコンプライアンス アプリケーションの統合

Qualys 脆弱性統合 が既にシステムにインストールされており、API 認証情報が コンフィグレーションコンプライアンス で使用するものと異なる場合は、(脆弱性対応 内の) セットアップアシスタントに移動し、各 **Qualys PC** 統合にアサインします。

次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > プライマリ統合 をクリックし、[**Qualys REST** 詳細] タブの [**Qualys API** 認証情報] フィールドを編集します。

PCRS パラメーターの構成

セキュリティオペレーションの Qualys 統合 の v12.6.3 以降では、Qualys PCRS ポリシーホスト統合および Qualys PCRS テスト結果統合を使用して、新しい Qualys API のセットでテスト結果をインポートできます。この統合には、Qualys から情報を取得するためのゲートウェイ URL が必要です。

始める前に
必要なロール：admin

このタスクについて
セキュリティオペレーションの Qualys 統合 for 脆弱性対応 をインストールするときに、コンフィグレーションコンプライアンスで新しい PCRS 統合の **gateway_url** パラメーターを構成できます。API URL のゲートウェイ URL を確認する方法の詳細については、「Identify your Qualys platform (Qualys プラットフォームの識別)」を参照してください。

ゲートウェイ URL を ServiceNow インスタンスに追加する必要があります。

手順

1. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > アドミニストレーション > 統合インスタンス.

   > **注:**
   > 現在のスコープが Qualys for Security Operations であることを確認します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

2. PCRS 統合で使用されているインスタンスを開きます。
3. [統合インスタンスパラメーター] タブで、**gateway_url** 構成のゲートウェイ URL を追加します。

> **注:**
> Qualys PCRS テスト結果統合 (Qualys PCRS Test Results Integration) は、Qualys PCRS ポリシーホスト統合 (Qualys PCRS Policy Host Integration) に依存しています。そのため、Qualys PCRS テスト結果統合 (Qualys PCRS Test Results Integration) を過去にさかのぼって実行する場合は、同じ順序で再度実行する必要があります。

Qualys Integration for Security Operations とともにインストールされるコンポーネント

次のロール、スケジュール済みジョブ、テーブルが Qualys Integration for Security Operations とともにインストールされます。

> **注:**
> アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「アプリケーションとともにインストールされているコンポーネントの検索」を参照してください。

アプリケーションとともにインストールされるコンポーネントのフィルター済みリストの表示

アプリケーションファイルテーブルをフィルタリングして、アプリケーションとともにインストールされたロール、スケジュール済みジョブ、およびテーブルのみを表示します。これらのコンポーネントを表示するアプリケーションは、そのファイルがインスタンスとメタデータテーブルにロードされるようにインストールする必要があります。アプリケーションファイルテーブルからフィルター済みリストを表示するには、次の手順に従います。

1. フィルターナビゲーターで、「**sys_metadata.list**」と入力してメタデータテーブルに移動します。
2. 条件ビルダー (フィルターアイコン) を選択し、次を選択します。 アプリケーション > 次の値に等しい その後にアプリケーションの名前が続きます。たとえば アプリケーション > 次の値に等しい > 脆弱性対応.
3. 条件ビルダーで 2 番目のフィルターを追加するには、[**AND**] を選択してから次を選択します。 クラス > は をクリックし、リストから [ロール]、[スケジュール済みジョブ]、または [テーブル] のいずれかのクラスを選択します。
4. **[Run** (実行)] を選択します。

選択したクラスの結果がフィルター済みリストに表示されます。

インストールされるロール

ロール タイトル [名前]	説明	含んでいるロール
sn_vul_qualys.read	Qualys 脆弱性統合レコードの読み取りアクセス権があります。	
sn_vul_qualys.user	Qualys 脆弱性統合のユーザー。レコードの読み取りと書き込みが可能です。	sn_vul_qualys.read

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロール タイトル [名前]	説明	含んでいるロール
sn_vul_qualys.admin	Qualys 脆弱性統合のアドミン。たとえば、統合の開始日を変更し、いくつかの詳細構成を設定できます。	• sn_vul_qualys.user • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	Qualys 脆弱性統合を構成できます。	sn_vul_qualys.admin

インストールされるスケジュール済みジョブ

スケジュール済みジョブ	説明
Qualys PC ポリシー	Qualys からポリシーを取得します。出力は sn_vulc_policy テーブルに格納されます。この統合で使用される API はページネーションをサポートしていないため、すべてのポリシーが 1 つのページにダウンロードされます。
Qualys PC ポリシーの詳細	テクノロジーやセクションなど、ポリシーの全詳細を取得します。
Qualys PC コントロール	Qualys からさまざまなコントロール ID のコンプライアンスコントロール情報を取得します。
Qualys PC 結果	Qualys からコンプライアンス体制レコードを取得します。この統合の出力はテスト結果です。デフォルトでは、ホスト情報、前回のスキャン日時、コントロール ID、および証拠情報をインポートするためにパラメーターの詳細が渡されます。
Qualys PC 包括的な結果 (Qualys Comprehensive Results)	合格しなかったテスト結果の最終評価日に基づいて、Qualys からコンプライアンス体制レコードを取得します。このジョブは週に 1 回実行されます。 この統合の出力はテスト結果です。デフォルトでは、ホスト情報、前回のスキャン日時、コントロール ID、および証拠情報をインポートするためにパラメーターの詳細が渡されます。
Qualys PCRS ポリシーホスト統合	Qualys からホストデータを取得し、インスタンスで処理します。 この統合の出力はポリシーホスト ID です。 Qualys ホストデータがこの統合にインポートされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みジョブ	説明
	注: • このスケジュール済みジョブは、コンフィグレーションコンプライアンス がインストールされている場合にのみ表示されます。 • この統合を実行する前に、統合インスタンスパラメーター gateway_url および pcrs_page_size を設定します。 この 2 つの統合は非アクティブな OOB になります。これらの統合のいずれかをアクティブにすると、PC 結果 (PC Results) 統合は非アクティブになります。この 2 つの統合は、Qualys の新しいストリーミング API に基づいて追加されます。
Qualys PCRS テスト結果統合	各ホスト ID のテスト結果を取得します。この統合では、[統合の詳細] タブの [開始時間] パラメーターを使用します。 注: • このスケジュール済みジョブは、コンフィグレーションコンプライアンス がインストールされている場合にのみ表示されます。 • この統合を実行する前に、統合インスタンスパラメーター gateway_url および pcrs_page_size を設定します。 • 統合を手動で実行する場合は、Qualys PC ポリシー、Qualys PC ポリシーの詳細、および Qualys PCRS ポリシーホスト統合の後に Qualys PCRS テスト結果統合を実行します。

注:
Qualys PCRS ポリシーホスト統合 (Qualys PCRS Policy Host Integration) と Qualys PCRS テスト結果統合 (Qualys PCRS Test Results Integration) は、デフォルトでは非アクティブです。この 2 つの統合は、Qualys の新しいストリーミング API に基づいて追加されます。これらの統合のいずれかをアクティブにすると、PC 結果 (PC Results) 統合は非アクティブになり、PC 結果 (PC Results) 統合をアクティブにすると、これらの統合が非アクティブになります。

インストールされるテーブル

テーブル	説明
Qualys PC 結果インポート sn_vul_qualys_pc_result_import	インポートセット行を拡張するテーブル。フィールドマップ変換はスキップされ、応答添付ファイルは onComplete スクリプトで直接処理されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

テーブル	説明
ポリシーホスト ID sn_vul_qualys_policy_host_id	ポリシーとこのポリシーがスキャンされたホスト間のマッピングを格納するテーブル。このテーブルは、新しい Qualys PCRS 統合で使用されます。 **注:** このテーブルは、コンフィグレーションコンプライアンス がインストールされている場合にのみ表示されます。
Qualys PCRS ポリシーホストインポート sn_vul_qualys_pcrs_policy_host_import	インポートセット行を拡張するテーブル。フィールドマップ変換はスキップされ、応答添付ファイルは onComplete スクリプトで直接処理されます。 **注:** このテーブルは、コンフィグレーションコンプライアンス がインストールされている場合にのみ表示されます。
Qualys PC ポリシーインポート sn_vul_qualys_pc_policy_import	インポートセット行を拡張するテーブル。フィールドマップ変換はスキップされ、応答添付ファイルは onComplete スクリプトで直接処理されます。

Qualys 統合のネットワークパーティション識別子を使用して構成アイテムを更新する

IP アドレスを共有する環境内の資産に対して、一意の構成アイテム (CI) を作成します。環境全体で個別の資産を特定し、検出された既存のアイテム、脆弱性一致アイテム、および検出レコードで CI を自動的に更新して、脆弱性に関する詳細を提供します。

始める前に
必要なロール：admin

このタスクについて
デフォルトでは、脆弱性対応 アプリケーションで資産を識別する方法の 1 つは IP アドレスです。場合によっては、資産は IP アドレスを共有できますが、それらは 1 つの CI として CMDB に保存されます。

たとえば、次の表に示すように、環境内の複数の資産 (CI) が IP アドレスを共有できますが、ネットワークとリポジトリの ID は一意です。ただし、デフォルトでは、これらの資産は通常、IP アドレスのルックアップ中に単一の CI（CI 1）として識別され、保存されます。

デフォルトの **IP** ルックアップと **CI** の作成

ソース	IP アドレス	NETWORK_ID	構成アイテム
Qualys 脆弱性統合：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ソース	IP アドレス	REPOSITORY_ID	構成アイテム
Qualys 脆弱性統合：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

同じ IP アドレスを持つ資産に対して個別の CI を作成して、それらを個別の資産として識別できるようにすることができます。新規のデータのインポートから開始し、スケジュール済みジョブ *Update existing discovered items with network partition identifier* を実行することで、ネットワークパーティション識別子 [network_partition_identifier] を含む既存の CI をより細かく更新できます。

このスケジュール済みジョブは、デフォルトでは非アクティブです。セットアップアシスタントで Qualys 脆弱性統合 の資産と修正済みおよびオープンな脆弱性の統合に対してこの機能をアクティブ化して、この識別子をレコードに表示します。

このスケジュール済みジョブを有効にすると、インポートされたデータから既存の CI レコードにネットワークパーティション識別子 [network_partition_identifier] が追加されます。IRE によって作成された既存の CI も更新されます。スケジュール済みジョブは、次のインポートから始まるネットワークパーティション識別子を含む CI も作成します。または、オンデマンドでジョブを開始して既存のデータを更新することもできます。

脆弱性対応 の v14.0 および Qualys 脆弱性統合 脆弱性統合の v12.1 以降、CMDB CI クラスモデル (1.0.21.) がサポートされています。クラスモデルでは、識別および調整 (IRE) 識別ルールにネットワークパーティション識別子 [network_partition_identifier] があります。

オプション	説明
スケジュール済みジョブをオンデマンドで実行します。	検出された既存のアイテムを更新します。既存の Qualys 脆弱性統合データの CI は、ネットワークパーティション識別子の粒度を含むように作成または更新されます。検出されたアイテム、脆弱性一致アイテム、および検出レコードはすべて新しい CI で更新されます。
次のスケジュール済みジョブとの統合からの新しいデータのインポートを待機します。	次のスケジュール済みジョブから始まるネットワークパーティション識別子を使用して、新しい資産ごとに CI を作成します。CI、脆弱性一致アイテム、および検出レコードはすべて、新しい粒度を含むように更新されます。完全一致が見つからない場合は、新しい CI が作成されます。

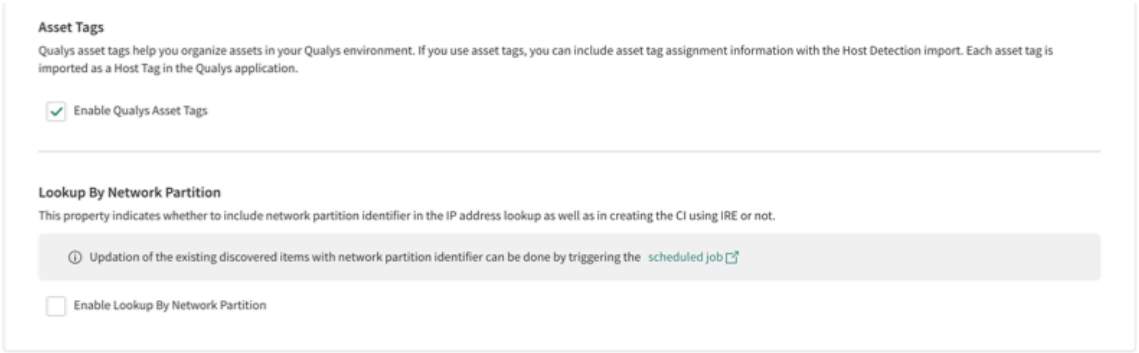
手順

1. 次のように移動する。 脆弱性対応 > セットアップアシスタント > 統合設定 > スキャナー統合.
2. Qualys 脆弱性統合 を選択します。
3. 必要な統合を編集します。
4. 選択 ホスト検出設定.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

5. 選択 ネットワークパーティションによるルックアップを有効化 の
チェックボックス ネットワークパーティションによるルックアップ



節。

6. [完了] をクリックします。

IP ルックアップと **CI** の作成に含まれるネットワークパーティション識別子 **NETWORK_ID** と **REPOSITORY _ID**

ソース	**IP** アドレス	**NETWORK_ID**	ネットワークパーティション識別子のない資産の **CI**	ネットワークパーティション識別子のある **CI** 資産
Qualys 脆弱性統合：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

ソース	**IP** アドレス	**REPOSITORY_ID**	ネットワークパーティション識別子のない資産の **CI**	ネットワークパーティション識別子のある **CI** 資産
Qualys：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

Qualys 脆弱性統合 の資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合からデータをインポートできるように、IP アドレスおよび不完全な IP アドレス CI の識別ルックアップルールにネットワークパーティション識別子属性が自動的に含まれます。

スケジュール済みジョブをアクティブ化してレコードを保存した後、スケジュール済みジョブをオンデマンドで起動して、ネットワークパーティション識別子を含む CI で検出された既存のアイテムを更新することもできます。既存の検出されたアイテム、脆弱性一致アイテム、および検出レコードの CI は自動的に更新されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Qualys インポートの追加のフィルターパラメーターの設定

Qualys 脆弱性統合を使用してスケジュール設定済みクエリのフィルタリングパラメーターをカスタマイズすると、サポートされている Qualys 統合でインポートする脆弱性データをさらに絞り込むことができます。

始める前に

ユースケース：脆弱性マネージャーまたはアナリストは、特定の脆弱性の詳細のみを確認できるように、クエリからデータを除外できます。たとえば、特定の IP または IP 範囲でフィルタリングされたインポート済み脆弱性を表示するとします。または、スコープ内にあるマシンのみ (外部デバイスではない企業ネットワーク内のマシンのみなど) をインポートします。

このデータを収集するには、Qualys パラメーターを追加して、必要な特定の脆弱性の詳細をインポートします。

この機能を使用すると、API コールを追加したり追加のコーディングをしたりすることなく、Now Platform の Qualys パラメーターを使用して HTTP 要求情報をカスタマイズできます。サポートされている Qualys 脆弱性統合の Qualys 統合の REST メソッドにある HTTP メソッドレコードで、これらの値を変更または追加します。

必要なロール：sn_vul.vulnerability_admin

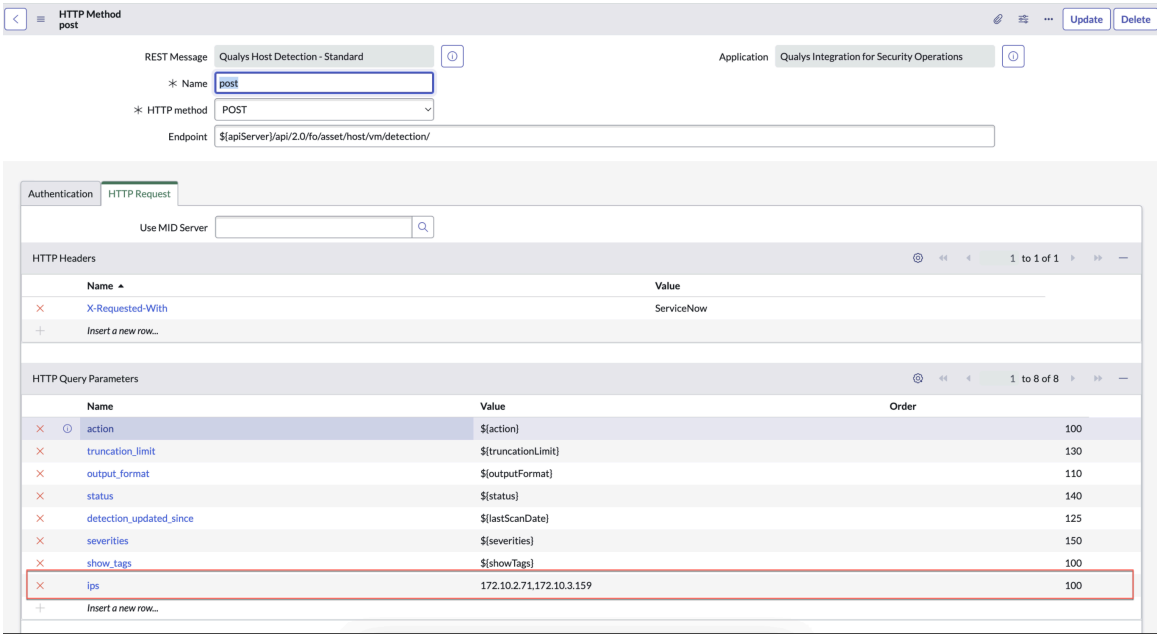
手順

1. フィルタリングに使用する開発者サイトで、Qualys 製品でサポートされているパラメーターを見つけます。
   Qualys 製品から入力するパラメーターと値は、Now Platform の統合インスタンスレベルでのみサポートされます。すべての Qualys 統合は、クエリパラメーターを使用したフィルタリングをサポートしています。
2. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > アドミニストレーション > プライマリ統合.
3. [Qualys 統合] リストページで、レコードを開く統合のレコードをクリックします。
4. [Qualys REST 詳細] タブを選択した状態で、REST メソッドの情報アイコン (I) を見つけてクリックし、続いて [レコードを開く] をクリックして HTTP メソッドレコードを開きます。
5. **[HTTP** 要求] タブを選択します。
6. 要求本文の [HTTP クエリパラメーター (HTTP Query Parameters)] で、Qualys 開発者サイトから取得した値を追加します。

   次の画像では、例として、特定の IP アドレス/範囲のみを取り込むパラメーター *ips={value}* が追加されています。この場合、[値] は指定した 1 つ以上の IP/範囲です。複数のエントリーは「172.10.2.71, 172.10.3.159」のようにカンマ区切りにし、範囲は「10.10.10.1-10.10.10.100」のようにハイフンで指定します。詳細については、Qualys 開発者サイトを参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



複数のパラメーターを入力する場合は、各値を区切る方法の詳細について、Qualys ドキュメントを参照してください。

> **注:**
> API 要件を把握しておく必要があります。これらの API プロパティをクエリパラメーターまたは本文のコンテンツに追加する必要が生じる場合があります。

Qualys 開発者サイトに記載されている役に立つと思われるその他のパラメーター：

- `ag_ids`：取得する資産グループリスト ID。このパラメーターは、スコープ内のマシンのみが取り込まれるようにします。
- `qids`：このパラメーターは、結果を特定の脆弱性 (サードパーティのエントリーテーブルの QID) のみに制限します。この設定により、システムが情報レコードであふれるのを防ぎます。

7. [更新] をクリックします。

[store-future: BEGIN review]

で **Qualys** テスト結果をテストグループに関連付けます。 コンフィグレーションコンプライアンス

Qualysテストグループへのマッピングを使用して、コンフィグレーションコンプライアンスでテストとテスト結果を作成します。

始める前に
必要なロール：admin

このタスクについて
Qualys ポリシーとコントロールのデフォルトライブラリを維持しながら、カスタムポリシーとコントロールの作成を可能にします。これらのコントロールはポリシーにマッピングでき、IT 資産のセキュリティ体制を評価するための包括的なフレームワークを提供します。資産が評価されると、ポリシーは Qualys 体制を生成し、 コンフィグレーションコンプライアンスでテスト結果に変換されます。Qualys ポリシーにマッピングされたコントロールが、Qualysライブラリに存在するデフォルトのコントロールとは異なります。これにより、ポリシーレベルでコントロールの重要度、ステータス (アクティブまたは非アクティブ)、テクノロジーなどの属性を柔軟に定義できます。

以前は、コンフィグレーションコンプライアンス では、テストは通常、Qualys ポリシーにマッピングされたコントロールではなく、Qualysライブラリコントロールに対して作成されていました。テ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

スト結果は、テストグループマッピングのないテストを参照します。したがって、Qualysの姿勢と比較して、コンフィグレーションコンプライアンスのテスト結果が少ない可能性があります。

テストグループへのマッピング コンフィグレーションコンプライアンス テストとテスト結果を作成するために、テストレベルに新しい列 [テストグループ] が追加されました。この列の入力は、システムプロパティ *sn_vulc.add_policy_as_key* によって制御されます。このシステムプロパティを有効にすると、 コンフィグレーションコンプライアンス ライブラリコントロール (テストグループは空になります) とポリシーにマッピングされたコントロール (テストグループはポリシー ID になります) の両方のテストが作成されます。テスト結果は、ポリシーマッピングを使用したテストを参照します。

すべてのテスト結果がテストグループマッピングを使用して新しいテストに移行されるようにするには:

手順

1. sn_vulc.add_policy_as_key システムプロパティを有効にします。
   a. フィルターナビゲーターで sys_properties.list と入力して、インスタンスのシステムプロパティのリストを表示します。
   b. sn_vulc.add_policy_as_key システムプロパティを検索して開きます。
   c. 警告メッセージ内のリンクを選択して、システムプロパティを編集します。
   d. [値] フィールドを True に設定して、sn_vulc.add_policy_as_key システムプロパティを有効にします。
2. オプション: Configuration Compliance に既存のデータ (テストとテスト結果) があるカスタマーの場合:
   a. sn_vulc.add_policy_as_key システムプロパティの開始時間フィールドをクリアします。
   b. 次の順序で統合を実行します。
      - Qualys PC ポリシー
      - Qualys PC コントロール
      - Qualys PC ポリシーの詳細
      - Qualys PC 結果/Qualys PCRS テスト結果の統合
3. 次のことを確認します。
   - Qualys PC ポリシーを実行した後、テストグループ参照を使用して新しいテストが作成されているかどうかを確認します。
   - Qualys PC 結果/Qualys PCRS テスト結果統合を実行した後、すべてのテスト結果が、テストグループ参照が入力された新しいテストを指していることを確認します。

タスクの結果

- 新しいテストは、テストグループへの参照を使用して作成されます。新しいテストの [テストグループ] 関連リストが入力されていません。新しいテストは、 Qualysのポリシーにマッピングされたコントロールに基づいており、ポリシーレベルでのコントロールの重要度、ステータス (アクティブまたは非アクティブ)、およびテクノロジーを反映します。
- テストグループ参照を使用しないテストでは、 Qualys ライブラリにコントロールが反映されます。
- すべてのテスト結果は、テストグループマッピングを使用した新しいテストを指します。テスト結果のテストグループは、関連するテストにドット連結することで識別できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[End]

Qualys Vulnerability Integration の問題の解決

よく発生する問題とワークアラウンドについて説明します。

インポート後に添付ファイルが表示されない

サードパーティの統合インポート後に添付ファイルが想定どおりに表示されない場合や、セキュリティインシデントで表示されない場合は、IP 制限を確認してください。

安全な IP からログインしていないと、IP アクセス制限により、添付ファイルが表示されないことがあります。インポートするたびに新しい添付ファイルが追加されるため、削除する必要がある重複が発生する可能性があります。

たとえば、サードパーティのホストインポート統合を実行するときにデータソースに添付ファイルが表示されない場合は、インポートする前に IP 制限を確認し、ユーザーをセーフリストに追加します。

変換マップの変更

変換マップは基本構成で提供され、通常はこれで十分です。組織のニーズに応じて変換マッピングを変更できます。

始める前に
必要なロール：sn_vul_qualys.admin + import_admin

手順

1. 次のように移動する。 **All** (すべて) > システムインポートセット > アドミニストレーション > 変換マップ をクリックして REST メッセージを表示します。
2. 結果のリストをアプリケーションでフィルタリングし、リストを **[Qualys Vulnerability Integration]** アプリケーションに制限します。
3. 顧客の要件に従って変換マップを変更します。

   Qualys API によって提供されるデータの詳細については、Qualys API のドキュメント を参照してください。

XML 添付ファイルのプロパティサイズのチェック

大きなファイルに対して XML 添付ファイルプロパティが十分であることを確認します。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > システムプロパティ > インポートエクスポート.
2. 下にスクロールして プロパティをインポート > **XML** 形式 関連する検出

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 必要に応じて値を 250 に変更し、[保存] をクリックします。

関連情報

利用可能なシステムプロパティ

データ検索の制限

デフォルトでは、Qualys からのデータの取得方法に制限はありません。多くのレコードは、顧客が脆弱性対応プロセスを使用して修正しようとしない、重大度の低い脆弱性に関連している可能性があります。対応する REST メッセージ/メソッドのパラメーターを更新すると、この動作が変更される場合があります。

この更新を処理する REST メッセージ/メソッドは、**[Qualys** ホスト検出 **-** 標準/投稿 **(Qualys Host Detection – Standard/post)]** です。値を更新するには、次の値を使用して新しい HTTP クエリパラメーターを post メソッドに追加します。

- 名前：重大度
- 値：3 ～ 5 (または必要な適切な重大度)

Qualys ナレッジベース統合が失敗する

Qualys から受信したペイロード添付ファイルのサイズを指定された制限まで縮小して、Qualys ナレッジベース統合を解決します。

始める前に
必要なロール：sn_vul.vulnerability_admin

手順

1. ペイロード添付ファイルのサイズが指定された制限内であることを確認します。
   a. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > 統合インスタンス.
   b. [統合インスタンスパラメーター] タブを選択します。
   c. **[max_delta_days]** を選択し、デフォルト値を 3 に変更します。
2. それでも統合に失敗する場合は、次の手順を実行します。
   a. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > プライマリ統合.
   b. **[Qualys** ナレッジベース] を選択します。
   c. [**Integration Details**] を選択します。
   d. [開始日時 **(Start time)]** フィールドで、現在の日付を選択して、その日の実行をスキップします。
   e. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > 統合インスタンス.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

f. [統合インスタンスパラメーター] タブを選択します。

g. **[kb_backfill_full_import]** を選択し、デフォルト値を true に変更します。

タスクの結果
Qualys ナレッジベースバックフィル統合を実行すると、システム内のすべてのサードパーティエントリ (TPE) が更新されます。Qualys ホスト検出統合ではプレースホルダーエントリが作成されますが、Qualys ナレッジベースバックフィル統合ではプレースホルダーエントリが更新されます。

Qualys 統合実行状況チャート

[Qualys 連携実行状況] モジュールは、Qualys 統合実行のステータスをグラフィカルに表示します。

統合実行のステータスを表示するには、次に移動します: **Qualys Vulnerability Integration** > 統合実行ステータス.

脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で使用可能です。

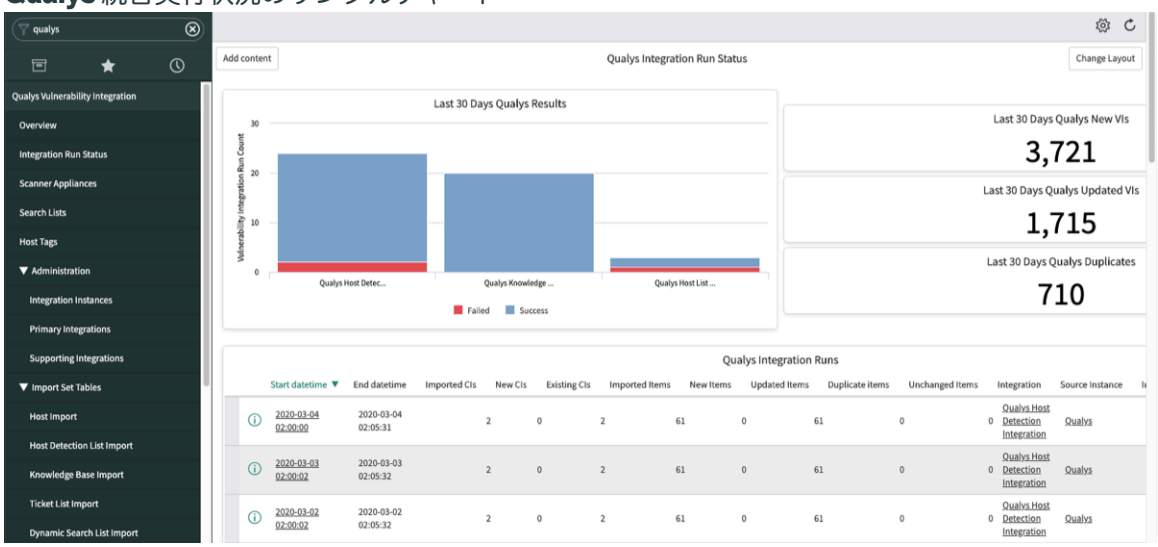
注:
Tokyo を使用している場合は、Next Experience UI でダッシュボードを表示できますが、一部の機能が失われます。

チャートで、任意の部分 (棒、円、データポイントなど) をポイントして、その部分に固有の一般的なデータを表示できます。レポートの任意の部分をクリックすると、詳細な情報を提供するリストが開きます。

Qualys 統合実行状況には、過去 30 日間の脆弱性統合実行状況が表示されます。Qualys[qualys] 更新済み VI 数は、同じ資産内の一意の検出数を示します。その後、VI は新しい検出で更新されます。

注:
脆弱性統合の実行数は、アクティブ状況に設定されている統合にのみ表示されます。次のように移動する。 **Qualys Vulnerability Integration** > アドミニストレーション > プライマリ統合をクリックし、ステータスをアクティブに設定します。

Qualys 統合実行状況のサンプルチャート



- [インポートされたアイテム (Imported Items)] 列の値は、統合実行から作成されるレコードの合計数を表します。
- [新規アイテム (New Items)] 列には、統合実行から作成されるレコードの数が表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- [重複アイテム] 列には入力されなくなりました。この列を表示から削除することもできます。
- [更新されたアイテム] 列には、統合実行中のレコードの更新回数が表示されます。この値は、更新される一意のレコードの数ではありません。たとえば、統合実行中にレコードが 2 回更新された場合、2 回とカウントされ、更新済みアイテムが 2 つと表示されます。
- [未変更のアイテム (Unchanged items)] 列には、既にデータベースに存在し、統合実行中に検出されたものの、関連するフィールド値が変更されていないために更新されなかったレコードが表示されます。

注:
[新規 **CI]**、[既存の **CI]**、[新規アイテム]、[更新されたアイテム] の 4 つの値がすべてゼロの場合、統合を実行すると、これらの値は **[Qualys** 連携実行] リストから除外されます。

Qualys 統合実行状況チャートレポート

名前	説明
過去 30 日間の Qualys 結果	各統合で完了した統合実行の数。成功した実行と失敗した実行の両方が表示されます。視覚的な棒グラフで実行されます。
過去 30 日間の Qualys 新規 VI	過去 30 日間にインポートされた新規レコードの数。整数として表示されます。
過去 30 日間の Qualys 更新済み VI	過去 30 日間にインポートされた更新済みレコードの数。整数として表示されます。
過去 30 日間の Qualys 重複	過去 30 日間にインポートされた重複レコードの数。整数として表示されます。
Qualys 統合実行	リストの統合実行レコード **注:** V16.1：この統合の検出を検証するには、検出または検出結果を *sn_vul_detection* テーブルの ServiceNow 検出データと比較します。 統合の進行中は、検出数または検出結果数が変更される可能性があります。このレポートでは、統合実行の完了後に、インスタンスの [現在までの数] 列に検出数が表示されます。
過去 30 日の Qualys 脆弱性一致アイテムの取り込みパフォーマンスメトリクス	過去 30 日間の脆弱性一致アイテムの日次パフォーマンスメトリクス
過去 30 日の Qualys 脆弱性一致アイテムの取り込みパフォーマンススループット	過去 30 日に測定された Qualys ホスト検出統合の脆弱性一致アイテムの日次取り込みスループット

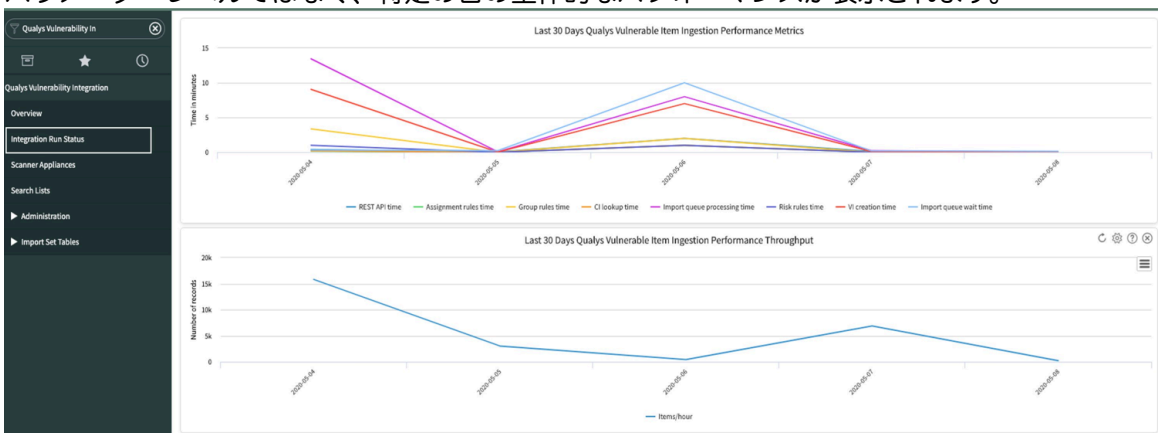
データ量やこのデータの処理にかかる時間など、複数の要因によって統合実行のパフォーマンスが影響を受ける可能性があります。次の 2 つのグラフでパフォーマンスメトリクスを比較します。

- Qualys 脆弱性一致アイテムの取り込みパフォーマンスメトリクス：アサインルール、グループルール、リスクルール、キュー待機時間、キューの処理時間、および過去 30 日間の脆弱性一致アイテムのその他の統計に関する日次パフォーマンスメトリクスを比較して、パフォーマンスの逸脱の原因を特定します。パフォーマンスは、各アクティビティにかかった時間に基づいて計算されます。これらのパラメーターは、統合実行レベルで計算され、関連付けられます。各パラメーターは、簡単に識別できるように色分けされています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- Qualys 脆弱性一致アイテムの取り込みパフォーマンススループット：Qualys ホスト検出統合について、脆弱性一致アイテム取り込みスループットを毎日比較します。スループットは 1 時間あたりのアイテム数で測定されます。このレポートには、個々のパラメーターレベルではなく、特定の日の全体的なパフォーマンスが表示されます。



Qualys REST メッセージ

Qualys REST メッセージは、コンプライアンスデータを取得するために Qualys API の呼び出しに使用されます。

次の REST メッセージはベースシステムに付属しています。

Qualys PC ポリシー (Qualys PC Policies) の REST メッセージ

Qualys PC ポリシー (Qualys PC Policies) の REST メッセージは、Qualys からポリシーデータを取得します。REST メッセージメソッドレコードを変更すると、ポリシー情報を取得するための Qualys への要求が影響を受けます。

Qualys PC ポリシー (Qualys PC Policies) の REST メッセージのパラメーター

パラメーター名	値	説明
action	リスト	要求された操作のタイプを示します。 必要なパラメーター。
details	すべて	取得されたポリシーの詳細レベルを示します。 要件に応じて変更しても安全です。

Qualys PC コントロール (Qualys PC Controls) の REST メッセージ

Qualys PC コントロール (Qualys PC Controls) の REST メッセージは、Qualys からさまざまなコントロール ID のコンプライアンスコントロール情報を取得します。

Qualys PC コントロール (Qualys PC Controls) の REST メッセージのパラメーター

パラメーター名	値	説明
action	リスト	要求された操作のタイプを示します。 必要なパラメーター。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Qualys PC コントロール (Qualys PC Controls) の REST メッセージのパラメーター (続く)

パラメーター名	値	説明
details	すべて	取得されたコントロールの詳細レベルを示します。 要件に応じて変更しても安全です。

Qualys PC ポリシーの詳細 (Qualys PC Policies Detail) の REST メッセージ

Qualys PC ポリシーの詳細 (Qualys PC Policies Detail) の REST メッセージは、テクノロジーやセクションなどの完全なポリシーの詳細を取得します。

Qualys PC ポリシーの詳細 (Qualys PC Policies Detail) の REST メッセージのパラメーター

パラメーター	値	説明
action	リスト	要求されている操作のタイプを示します。 必要なパラメーター。
show_user_controls	ブーリアン	• XML 出力にユーザー定義コントロール (UDC) を含めるには、1 に設定します。 • 指定しない場合、UDC は含まれません。 このパラメーターはオプションです。要件に応じて変更しても安全です。
show_appendix	ブーリアン	(オプション) XML 出力に付録セクションを表示するには、1 に設定します。指定しない場合は です。

Qualys PC 結果 (Qualys PC Results) の REST メッセージ

Qualys PC 結果 (Qualys PC Results) の REST メッセージは、Qualys からコンプライアンス体制レコードを取得します。

Qualys PC 結果 (Qualys PC Results) の REST メッセージのパラメーター

ソースフィールド	値	説明
action	リスト	要求された操作のタイプを示します。 必要なパラメーター。変更は推奨されません。
show_extended_evidence	ブーリアン	• 出力に詳細証拠情報を表示するには、1 に設定します。 • 0 に設定するかまたは未指定の場合、出力に詳細証拠情報が表示されません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Qualys PC 結果 **(Qualys PC Results)** の **REST** メッセージのパラメーター (続く)

ソースフィールド	値	説明
		注: • hide_evidence=1 が指定されている要求では、show_extended_evidence=1 を指定することはできません。このようにするとエラーが発生します。詳細証拠は証拠データの一部であり、証拠データが表示されている場合にのみ表示されます。 • このパラメーターは、ベースシステムには付属していません。
cause_of_failure	ブーリアン	「1」を渡すと、Qualys は失敗の原因を返します。 「0」を渡すと、Qualys はこれらの属性を返しません。 注: このパラメーターは、ベースシステムには付属していません。
policy_id		指定されたポリシーのコンプライアンス体制情報レコードを表示します。有効なポリシー ID が必要です。
details	すべて	取得された体制の詳細レベルを示します。 要件に応じて変更しても安全です。
show_remediation_info		(オプション) 1 に設定すると、XML または CSV 出力に修復情報が表示されます。デフォルトでは、修復情報は出力に含まれません。指定しない場合、修復情報は出力に含まれません。

Qualys PCRS ポリシーホスト統合 **(Qualys PCRS Policy Host Integration)** の **REST** メッセージ

Qualys PCRS ポリシーホスト統合 (Qualys PCRS Policy Host Integration) は、Qualys からホストデータを取得し、インスタンスでそのデータを処理します。

Qualys PCRS ポリシーホスト統合 **(Qualys PCRS Policy Host Integration)** の **REST** メッセージのパラメーター

パラメーター名	値	説明
policyId	${lastRunDatetime}	コンプライアンス評価のポリシー ID。

Qualys PCRS テスト結果統合 **(Qualys PCRS Test Results Integration)**

次の表に、送信される要求パラメーターを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Qualys PCRS テスト結果統合 **(Qualys PCRS Test Results Integration)** の **REST** メッセージのパラメーター

パラメーター名	値	説明
evidenceRequired	${lastRunDatetime}	• デフォルト値は 0 です。これは、ホスト体制の証拠データが取得されないことを示します。 • 証拠データを取得するには、値を 1 に設定します。 **注:** 値を 1 に変更すると、体制データの取得に必要な時間が長くなります。
compressionRequired		• デフォルト値は 1 で、出力が圧縮されることを示します。 • データを圧縮しない場合は、値を 0 に設定します。 **注:** データを圧縮しないと、体制データの取得に必要な時間が長くなります。

Tenable 脆弱性統合の概要

Tenable 脆弱性統合の ServiceNow エンジニアリングによって開発された Vulnerability Response Integration with Tenable アプリケーションでは、Tenable.io および Tenable.sc 製品からインポートしたデータを使用して、資産の脆弱性に優先順位を付けて修正できます。アプリケーションは ServiceNow Store の個別のサブスクリプションで利用できます。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

Tenable 脆弱性統合では、資産と脆弱性に関するサードパーティのスキャナーデータをインポートできるように Tenable.io と Tenable.sc の 2 つの Tenable 統合を採用しています。Vulnerability Response Integration with Tenable アプリケーションは、バージョン 5.13 以降の Tenable.sc 製品をサポートしています。

- Tenable.io はクラウドベースのエンタープライズ統合です。
- Tenable.sc は、Tenable.sc 製品と Now Platform インスタンスが同じ環境にある場合に MID サーバーを使用するオプションを提供するオンプレミスの統合です。
- Tenable.sc 製品と Now Platform インスタンスが同じ環境にない場合は、MID サーバーを使用する必要があります。

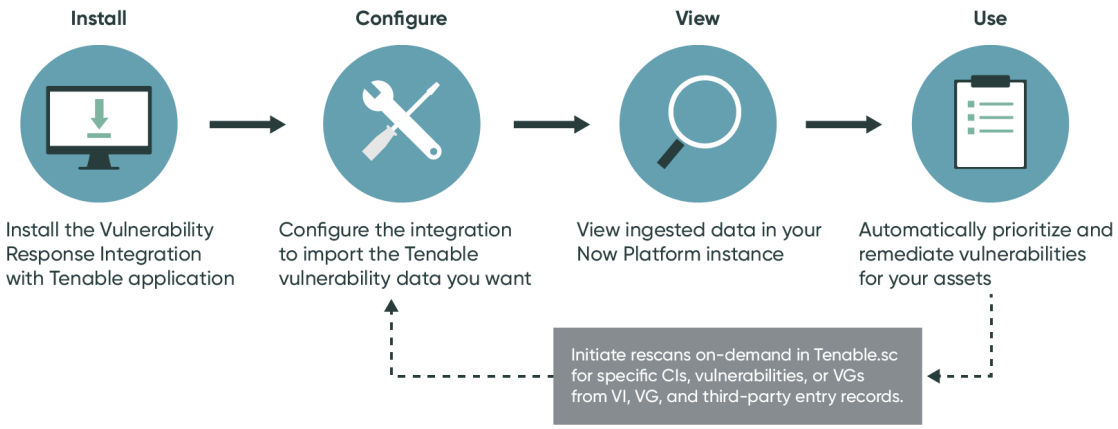
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Vulnerability Response Integration with Tenable アプリケーションは ServiceNow Store の別のサブスクリプションで利用できます。

Tenable 脆弱性統合の統合のリストと説明については、「脆弱性対応 および コンフィグレーション コンプライアンス アプリケーションとの Tenable.io 統合」および「脆弱性対応 アプリケーションとの Tenable.sc 統合」を参照してください。

Tenable 脆弱性統合



Yokohama の利用可能バージョン

リリースバージョン	リリースノート
Vulnerability Response Integration with Tenable v3.5、v3.6	互換性情報については、「KB0856498 脆弱性対応互換性マトリクスおよびリリーススキーマの変更」を参照してください。

自動翻訳

統合に関する用語と主な機能

脆弱性一致アイテムと脆弱性

次の場合に Now Platform インスタンスに脆弱性一致アイテムが作成されます。

- サードパーティのスキャナーからインポートした脆弱性が既存の資産 (CMDB の構成アイテム) と一致する。Tenable 製品では、これらの一致を [脆弱性] と呼びます。
- サードパーティのスキャナーからインポートした脆弱性が CMDB の既存の資産と一致しない。この場合、脆弱性一致アイテムとともに一致しない CI も作成されます。

  CI が一致せず、既存の CI がホストと一致しない場合、識別および調整エンジン (IRE) を使用して CI を 2 つのクラスに作成することもできます。それ以外の場合は、一致しない CI が [不一致] CI クラスに作成されます。詳細については、「識別および調整エンジンを使用して 脆弱性対応 の CI を作成する」を参照してください。

サードパーティ脆弱性エントリーとプラグイン

サードパーティ脆弱性エントリーはサードパーティスキャナーからインポートされ、Now Platform インスタンスの [サードパーティ脆弱性エントリー] テーブルにリストされます。脆弱性対応 v24.0 以降、[サードパーティ脆弱性エントリー] テーブルの [ソフトウェア] 列には、サードパーティ エントリーに関連付けられた共通プラットフォーム一覧 (CPE) が入力されます。Tenable からのサードパーティ脆弱性エント

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リーが 脆弱性対応 に取り込まれ、CMDB にリストされている既存の資産と照合されます。Tenable では、サードパーティ脆弱性エントリーを [プラグイン] と呼びます。

構成アイテム (CI)

構成アイテムは、CMDB にリストされている既存の資産です。

検出されたアイテム

Tenable 資産インポートから取り込まれた資産は、CMDB の既存の構成アイテムと照合されます。インポートされた資産は更新されます。

一致するものが見つからない場合は、CMDB の [一致しない CI] クラスに CI が作成されます。CMDB CI クラスモデルプラグインが有効の場合、識別および調整エンジン (IRE) が新しいクラスを使用して新しい CI を作成します。詳細については、「識別および調整エンジンを使用して 脆弱性対応 の CI を作成する」を参照してください。元の一致しない CI が再分類され、検出されたアイテムレコードを更新してステータスが反映されます。検出されたアイテムにより、資産がどのように識別され、CMDB の CI にマッピングされるかを把握できます。

CI ルックアップルール

サードパーティ統合からデータがインポートされると、脆弱性対応はホスト (資産) データを自動的に使用して、Configuration Management Database (CMDB) で一致するものを検索します。CI ルックアップルールは CI の識別に使用され、修復に使用できるように、VI が作成されると VI レコードに追加されます。

再スキャンと修復スキャン

Now Platform インスタンス内の脆弱性一致アイテム、修復タスク、およびサードパーティの脆弱性エントリーレコードから、特定の構成アイテム、修復タスク、またはサードパーティのエントリーでターゲットの再スキャンコマンドを開始できます。Tenable では、この再スキャンを [修復スキャン **(remediation scan)]** と呼びます。

古い VI を自動的にクローズします。

Now Platform の [古い脆弱性一致アイテムの自動クローズ (Auto-Close Stale Vulnerable Items)] モジュールを使用すると、サードパーティ統合によって最近検出されていない古い脆弱性一致アイテム (VI) をクリーンアップできます。これらの VI を [クローズ済み] に移動すると、アクティブな脆弱性一致アイテムと修復タスクの数を減らし、CMDB の資産を調整できます。Vulnerability Response Integration with Tenable との統合をすべて使用して、古い VI を自動的にクローズできます。

インスタンス

この用語は、Now Platform® アプリケーションの個別の発生を指します。

統合

統合は、Tenable.io 資産統合や Tenable.sc プラグイン統合などの統合への製品固有の参照です。これらは、インスタンスの Tenable 脆弱性統合の特定の Tenable 製品に属する個別の統合です。

統合インスタンス

この用語は、Tenable.io および Tenable.sc 製品によってリストされている個別の Tenable 統合を指します。

展開

統合でマルチソースがサポートされている場合、単一の個別の統合の存在は、統合の展開と呼ばれます。この用語は、環境全体での統合と製品を指すのに使用されます。たとえば、Tenable.io および Tenable.sc 製品のさまざまな統合を環境に複数展開する場合があります。

Tenable.io および Tenable.sc の統合には、次の主な機能もあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 構成アセスメントの結果 (テスト結果と、ポリシー、構成テスト (コントロール)、および信頼できるソースの引用) を Tenable.io 製品で コンフィグレーションコンプライアンス アプリケーションにインポートできます。この統合が コンフィグレーションコンプライアンス アプリケーションでどのように機能するかの詳細については、「脆弱性対応 および コンフィグレーションコンプライアンス アプリケーションとの Tenable.io 統合」および「コンフィグレーションコンプライアンスの詳細」を参照してください。
- v2.1 の Tenable 脆弱性統合 から、同じ IP アドレスを共有する環境内の資産に対して、異なるネットワークパーティション識別子を含む一意の構成アイテム (CI) を作成します。環境全体で個別の資産を特定し、検出された既存のアイテム、脆弱性一致アイテム、および検出レコードで CI を更新して、脆弱性に関する詳細を提供します。
- すべての Tenable.io および Tenable.sc 統合でジョブを実行するタイミングをスケジュールできます。スケジュール済みジョブをオンデマンドで手動実行することもできます。
- Tenable.io を使用した資産インポートでは、資産タグを有効にして Tenable.io 環境の CMDB にリストされている資産を整理して追跡できます。
- Tenable.io および Tenable.sc 統合では、Now Platform CMDB の構成アイテム (CI) を特定するためにサードパーティソースの資産データを使用する方法を CI ルックアップルールで定義できます。
- Tenable.io および Tenable.sc 統合では、必要な脆弱性のみを Tenable からインポートできるように、脆弱性インポート時にインポートフィルターを設定できます。Tenable.io には、脆弱性インポートを使用して Tenable から [修正済み] の脆弱性をインポートするオプションがあります。
- Tenable.sc には、Now Platform インスタンスの脆弱性一致アイテム、修復タスク、およびサードパーティエントリーレコードから直接オンデマンドで再スキャンを開始するオプションがあります。VI が [クローズ済み]/[修正済み] に移行しても、インスタンスでまだ更新されていない場合は、特定の構成アイテムの脆弱性が修正されていることを確認できます。「Tenable.sc 統合の再スキャンの開始」を参照してください。

次のセクションでは、Tenable 統合の詳細について説明します。

必要な **Now Platform** ロール

統合タスクには、Now Platform インスタンスで次のロールが必要です。

admin

システムアドミニストレーターは、セットアップアシスタントを使用して Vulnerability Response Integration with Tenable アプリケーションをインストールします。アサインされていない場合、アドミニストレーターはセットアップアシスタントで脆弱性アドミン (sn_vul.vulnerability_admin) およびその他のロールをアサインします。

sn_vul.vulnerability_admin

アサインされると、脆弱性アドミニストレーターはセットアップアシスタントで Tenable 統合の構成を比較します。このロールは、脆弱性対応 (VR) アプリケーションとそのレコードに完全にアクセスできます。脆弱性アドミニストレーターは、インストールされたサードパーティ統合のすべての VR アプリケーションとルールを構成します。

sn_vul_tenable.configure_integration

このロールには詳細なロール sn_vul_tenable.read_integration が含まれており、このロールを持つユーザーは Vulnerability Response Integration with Tenable アプリケーションを設定できます。

sn_vul_tenable.read_integration

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このロールを持つユーザーは、Vulnerability Response Integration with Tenable アプリケーションのレコードを表示 (読み取り) できますが、編集することはできません。

脆弱性対応グループ

デフォルトで脆弱性対応グループはセットアップアシスタントで利用可能になっています。脆弱性対応グループにアサインされたユーザーは sn_vul.read_all および sn_vul.remediation_owner ロールを自動的に継承します。

脆弱性一致アイテム

脆弱性一致アイテムは、修復タスクルールに従って修復タスクにグループ化され、アサインルールに基づいて修復にアサインされます。詳細については、「脆弱性対応修復タスクとタスクルールの概要」と「脆弱性対応 アサインルールの概要」を参照してください。

構成アイテム (CI) ルックアップルール

CI ルックアップルールでは、CI を識別して、それらを脆弱性一致アイテムに追加するタイミングを決定します。CI ルックアップルールの詳しい仕組みについては、「脆弱性対応 サードパーティ脆弱性統合の構成アイテムを識別するための CI ルックアップルール」を参照してください。

注:
ルールは、一度削除すると元に戻せません。新しいルールを作成する場合は、既存のルールを削除せずに無効にします。

次の Tenable.io ルックアップルールはベースシステムに付属しています。

- MAC_ADDRESS
- FQDN
- NetBIOS
- HostName
- DNS
- IP

注:
Tenable.io CI ルックアップルールは、検出されたアイテムの通常の FDQN、IPV4、および MacAddress 値よりも、空でないネットワークインターフェイス値 (FDQN、IPV4、および MacAddress) を優先して入力します。これらのネットワークインターフェイスの値が空の場合、通常の FDQN、IPV4、および MacAddress の値が検出されたアイテムに設定されます。

次の Tenable.sc ルックアップルールはベースシステムに付属しています。

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

注:
ip_address、mac_address、fqdns、および network_interfaces の複数の値が資産に使用されます。すべての値が照合用の CI ルックアップルールで考慮されます。IRE を使用して複数のネットワークアダプターを作成するためにすべての値が使用されます。

一致しないクラウドリソースの分類を優先 CI クラスに構成する方法の詳細については、「一致しないクラウド資産の CI クラスの更新」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

IP アドレスを無視する新しいプロパティ

Tenable.io では、CI ルックアップルールの一部として、複数の IP アドレスまたは複数の Mac アドレスを無視する場合に使用できるプロパティが 2 つあります。

ignoreIPAddress
: CI のルックアップと CI の作成で無視する IP アドレスのリスト

ignoreMacAddress
: CI のルックアップと CI の作成で無視する MAC アドレスのリスト

検出されたアイテム

このモジュールは、Tenable 脆弱性一致アイテム統合および Tenable 資産統合からのインポート中に検出された構成アイテムをリストします。

注:
このリストのデフォルトのフィルターは [不一致] に設定されています。フィルターを削除すると、インポートから検出されたすべてのアイテムを表示できます。

[検出されたアイテム] モジュールの詳細については、「検出されたアイテム」を参照してください。

資産タグ

資産タグ (ホストタグとも呼ばれます) は、組織の資産の整理と追跡に使用されます。資産にタグを割り当てることができます。これにより、スキャンを開始するときに、スキャンする資産に関連付けられたタグを選択できます。資産タグモジュールを使用すると、スケジュールに基づいて Tenable.io からインスタンスに資産タグデータをダウンロードできます。資産タグを含む資産データは Tenable.io からプルされ、Tenable.io 資産変換統合変換マップを使用して変換されます。

すべての資産タグは Tenable.io 資産統合の一部としてインポートされます。資産タグは、主に 脆弱性対応 アサインルールおよび修復タスクルールでのフィルタリングに使用されます。タグは [検出されたアイテム] フォームに表示されます。

注:
脆弱性対応 アプリケーションで 脆弱性対応 アサインルールまたは修復タスクルールを作成する前に Tenable.io 資産統合を実行し、脆弱性一致アイテムをインポートしてグループ化する前に、これらのルールですべてのタグを使用できるようにします。タグに関する次の点にも注意してください。

- タグストレージでは大文字と小文字は区別されません。たとえば、San Diego の場所で資産を説明するタグを作成し [San Diego] タグを作成する場合、[SAN DIEGO] タグを作成して資産タグテーブルに保存することはできません。San Diego と SAN DIEGO は同じホストタグと見なされます。最初にインポートされたタグが格納され、以後認識されるようになります。
- 修復タスクルールのグループキーとして資産タグを使用すると、予期しない結果になることがあります。資産タグは条件ビルダー専用です。
- 資産タグは、グローバルシステムプロパティ sn_vul.import_asset_tags で制御されます。このプロパティはデフォルトで [true] に設定されています。タグを無効にすると、すべての Now Platform インスタンスで無効になります。

データ検索フィルター

データ検索設定は、Tenable アプリケーションから Now Platform® インスタンスにインポートするデータのタイプとスコープを具体的に決定するのに役立ちます。最も一般的に使用される設定のリストについては、「Tenable 脆弱性統合のデータ検索設定」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性優先評価 (VPR)

脆弱性優先評価 (VPR) は、脆弱性対応 の新しいデフォルトのリスク算出でインポートして使用される Tenable 製品の属性です。Tenable リスクルールは、脆弱性対応 の脆弱性算出のデフォルトのリスク算出の一部として Vulnerability Response Integration with Tenable アプリケーションとともにインストールされます。

このリスクルールデフォルトでは無効になっています。

Tenable リスク算出ルールを有効にすると、インポートされた VPR 値が脆弱性一致アイテムのリスクスコアの計算に使用されます。このリスク算出のデフォルトの重み付け分布：VPR = 70%、資産 = 15%、ビジネス上の重要度 = 15%。この Tenable リスク算出ルールを有効にすると、データ取り込みのパフォーマンスが影響を受ける可能性があります。脆弱性対応 算出と Tenable リスク算出ルールの詳細については、「脆弱性対応 の算出と脆弱性算出ルール」を参照してください。

インストールと構成

ServiceNow® Store から Vulnerability Response Integration with Tenable をダウンロードすると、インストールと構成は 脆弱性対応 のセットアップアシスタントでサポートされます。詳細については、「セットアップアシスタントを使用した 脆弱性対応 の構成」を参照してください。

脆弱性対応 および コンフィグレーションコンプライアンス アプリケーションとの Tenable.io 統合

Vulnerability Response Integration with Tenable アプリケーションの Tenable.io 統合は、脆弱性対応 および コンフィグレーションコンプライアンス アプリケーションで使用できます。

Tenable.io 統合のリスト

マルチソースは Tenable.io および Tenable.sc のすべての統合でサポートされます。脆弱性対応 のセットアップアシスタントから、次の統合の複数のインスタンスを環境全体に追加して展開できます。セットアップアシスタントから Vulnerability Response Integration with Tenable アプリケーションをインストールして構成することもできます。

Tenable.io はクラウドベースのエンタープライズ統合です。Tenable.io 製品でサポートされている統合の名前と説明については、次の表を参照してください。

Tenable.io コンプライアンス結果統合と Tenable.io コンプライアンス結果バックフィル統合は、デフォルトでは非アクティブです。

それらをアクティブ化するには、次の手順を実行します。

1. 次のように移動する。 **Tenable** 脆弱性統合 > アドミニストレーション > 統合.
2. [Tenable 脆弱性統合] リストで、統合名をクリックしてレコードを開き、[アクティブ] チェックボックスをオンにして有効にします。これらの統合を開始するには、スケジュール設定をデフォルト値のままにすることをお勧めします。

Tenable.io の統合

統合	説明
Tenable.io 資産統合	• 資産タグを含むすべての資産データを Tenable.io 製品から取得して、インスタンスで処理します。 • v3.0 以降では、Tenable.io コンプライアンス結果統合がアクティブになっている場合は、インポートされた資産データとともに安全な構成アセスメントデータをインポートできます。このデータは、資産の構成関連の脆弱性を特定して対応するのに役立ちます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Tenable.io の統合 (続く)

統合	説明
	• 一致しない資産に対して一意の CI を作成するか、同じ IP アドレスを共有する環境全体の資産に対してネットワークパーティション識別子属性を使用して既存の CI を更新します。 • 資産 API への REST メッセージ呼び出しを調整します。 • この統合の出力は検出されたアイテムです。 • データはチャンクでインポートされ、[sn_vul_tenable_chunk_status] テーブルに格納されます。テーブルクリーナーは、保存されたデータを 30 日後にこのテーブルから自動的に削除します。 • v2.2 以降では、脆弱性がある資産に対してのみ *Last Scan Time* がインポートされて更新されます。
Tenable.io コンプライアンス結果統合	• v3.0 以降、資産統合からインポートされたデータとともに、コンプライアンス結果統合からインポートされた安全な構成アセスメントデータは、資産の構成関連の脆弱性を特定して対応するのに役立ちます。 • 有効にすると、高レベルの安全な構成アセスメントデータを取得し、Now Platform インスタンスで処理します。インポートされたデータには、ポリシー、構成テスト (コントロール)、信頼できるソースの引用とともにテスト結果が含まれます。 • 不足している資産または資産 ID のない資産のアセスメントデータはインポートされません。 • テスト結果がインポートされ、対応する資産がインスタンスで一致しない場合、テスト結果は無視され、不足している資産の ID が [sn_vul_tenable_missing_asset] テーブルの一時レコードに保存されます。 • 無視された (不足している) 資産の合計値は、この統合の統合実行レコードの [構成] タブの [無視された **CI]** フィールドに一覧表示されます。
Tenable.ioコンプライアンス結果バックフィル統合	• アクティブにすると、資産統合がチェーン統合実行の一部として正常に完了した後に、この統合が自動的に実行されます。この統合は、[sn_vul_tenable_missing_asset] テーブルにリストされている不足している資産と構成アセスメントデータを照合します。 • 資産統合のインポートが正常に完了した後に、インスタンスで検出またはインスタンスに存在する不足している資産について、最大 200 の資産 ID をインポートします。 • 対応する構成アセスメントデータと資産を照合できる場合、[sn_vul_tenable_missing_asset] テーブルから一時レコードを削除します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.io の統合 (続く)

統合	説明
Tenable.ioスキャン認証情報統合	• この統合は、Tenable.io で構成されたスキャン認証情報を取得します。 • 認証情報 API への REST メッセージ呼び出しを調整します。 • この統合の出力は、[sn_vul_tenable_scan_credential] テーブルに入力されるスキャン認証情報です。 • インポートされた認証情報は、スキャン要求が Now Platform から開始されたときにスキャナーにアクセスするために使用されます。 • この統合は毎週実行されるようにスケジュールされています。
Tenable.ioテンプレート統合	再スキャン中にテンプレートレコードが Tenable.io に送信されます。この統合は、再スキャンに使用する利用可能な Tenable.io 認証情報を取得します。認証情報はインスタンス固有であり、単一のテンプレートレコードがインポートされ、[sn_vul_tenable_io_template] テーブルに一時的に安全に格納されます。
Tenable.io プラグイン統合	• Tenable.io 製品からプラグインデータを取得します。取得されるデータは、Tenable.io 統合実行によってプラグインが最後に更新された日付に基づいています。 • このインポートにより、Tenable.io 識別子 (10 個の ID) が最新の状態になります。 • プラグイン API への REST メッセージ呼び出しを調整します。 • この統合の出力はサードパーティ脆弱性です。
Tenable.io の修正された脆弱性統合	• 重大度フィルターに基づいて、Tenable.io 製品から脆弱性データを取得し、インスタンスで処理します。脆弱性一致アイテムは「オープン」および「再オープン」ステータスの検出レコードに対して作成されます。これらのレコードには修復が必要なためです。検出が「修正済み」の場合、既存の脆弱性一致アイテムは脆弱性対応によって更新されますが、Tenable は「修正済み」の脆弱性を「脅威緩和」とみなすため、デフォルトでは「 修正済み」の検出に対して脆弱性一致アイテムは作成されません。 • セットアップアシスタントで「修正済みの脆弱性検出に対して脆弱性一致アイテムを作成」フラグがアクティブ化されている場合、新しい VI は「修正済み」ステータスで作成されるため、それらを作成した検出を表示できます。VI はインスタンスにまだ存在しない「修正済み 」の検出に対して作成されるため、インポートのパフォーマンスに悪影響を与える可能性があります。この機能を非アクティブのままにして、 修正済みの検出によって既存の脆弱性一致アイテムの状況だけが更新されるようにすることもできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.io の統合 (続く)

統合	説明
	• 一致しない資産に対して一意の CI を作成するか、同じ IP アドレスを共有する環境全体の資産に対してネットワークパーティション識別子属性を使用して既存の CI を更新します。 • 脆弱性 API への REST メッセージ呼び出しを調整します。 • この統合の出力は [クローズ済み]/[修正済み] の脆弱性一致アイテム (VI) です。これは、資産とサードパーティのエントリーが存在しない場合にも作成されます。 • データはチャンクでインポートされ、[sn_vul_tenable_chunk_status] テーブルに格納されます。テーブルクリーナーは、保存されたデータを 30 日後にこのテーブルから自動的に削除します。 この統合実行はスケジュールされています。これはチェーン統合であり、実行が正常に完了すると、後述のオープンな脆弱性統合がトリガーされます。 Tenable v3.3 以降では、脆弱性統合の実行に関する次の情報を表示できます。 • 合計チャンク：Tenable によって生成されているチャンクの合計数 • 利用可能なチャンク：ServiceNow のダウンロード可能なチャンクの数
Tenable.io のオープンな脆弱性統合	• この統合は、Tenable.io の修正された脆弱性統合が正常に完了するとトリガーされます。 • 重大度フィルターに基づいて、Tenable.io 製品から脆弱性データを取得し、インスタンスで処理します。 • 一致しない資産に対して一意の CI を作成するか、同じ IP アドレスを共有する環境全体の資産に対してネットワークパーティション識別子属性を使用して既存の CI を更新します。 • 脆弱性 API への REST メッセージ呼び出しを調整します。 • この統合の出力は [新規]/[再オープン] の脆弱性一致アイテム (VI) です。これは、構成アイテムとサードパーティのエントリーが存在しない場合にも作成されます。Tenable はアクティブな脆弱性を [累積] (現在) と見なします。 • データはチャンクでインポートされ、[sn_vul_tenable_chunk_status] テーブルに格納されます。テーブルクリーナーは、保存されたデータを 30 日後にこのテーブルから自動的に削除します。 Tenable v3.3 以降では、脆弱性統合の実行に関する次の情報を表示できます。 • 合計チャンク：Tenable によって生成されているチャンクの合計数 • 利用可能なチャンク：ServiceNow のダウンロード可能なチャンクの数

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 アプリケーションとの **Tenable.sc** 統合

Vulnerability Response Integration with Tenable アプリケーションとの Tenable.sc 統合。

脆弱性対応 v20.0 以降では、資産がエージェントによってスキャンされた場合、[エージェントが存在します] 列に、それが本物のスキャンであることを示す値、true が [検出されたアイテム] リストに表示されます。

Tenable.sc 統合のリスト

マルチソースは Tenable.io および Tenable.sc のすべての統合でサポートされます。脆弱性対応 のセットアップアシスタントから、次の統合の複数のインスタンスを環境全体に追加して展開できます。セットアップアシスタントから Vulnerability Response Integration with Tenable アプリケーションをインストールして構成することもできます。

- Tenable.sc は、Tenable.sc 製品と Now Platform インスタンスが同じ環境にある場合に MID サーバーを使用するオプションを提供するオンプレミスの統合です。
- Tenable.sc 製品と Now Platform インスタンスが同じ環境にない場合は、MID サーバーを使用する必要があります。

Tenable.sc の統合

統合	説明
Tenable.sc 資産統合	インポートされた資産データで検出されたアイテムが重複して作成されるのを避けるために、Tenable.sc 製品の資産統合は 2 つの統合で構成されています。 Tenable.sc オープン資産統合 この統合により、Tenable が累積 (現在) またはオープンと見なす資産に関する脆弱性データがインポートされます。このインポートされた資産データを使用してインスタンスで作成された脆弱性一致アイテム (VI) は、オープンしている、つまり [オープン] ステータスにあると見なされます。これらの脆弱性一致アイテムは調査が必要で、修正が必要な場合があります。 Tenable.sc 固定資産統合 この統合により、Tenable が脅威緩和 (脆弱性なし) または修正済みと見なす資産に関する脆弱性データがインポートされます。スキャンの結果、脆弱性がなくなったことが示されるため、これらの資産の脆弱性一致アイテムは、インスタンスで [オープン] ステータスから [クローズ済み]/[修正済み] ステータスに移行します。 • すべての資産データを Tenable.sc 製品から取得して、インスタンスで処理します。 • 一致しない資産に対して一意の CI を作成するか、同じ IP アドレスを共有する環境全体の資産に対してネットワークパーティション識別子属性を使用して既存の CI を更新します。 • 資産 API への REST メッセージ呼び出しを調整します。 • この統合の出力は検出されたアイテムです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.sc の統合 (続く)

統合	説明
	• セットアップアシスタントで選択した Tenable クエリフィルターは、Tenable.sc 資産統合にも適用されます。クエリフィルターの条件に一致する脆弱性がある資産のみがインポートされます。
Tenable.sc プラグイン統合	• Tenable.sc 製品からプラグインデータを取得します。取得されるデータは、Tenable.sc 統合実行によってプラグインが最後に更新された日付に基づいています。 • このインポートにより、Tenable.sc 識別子 (10 個の ID) が最新の状態になり、アクティブな脆弱性のみがインポートされます。 • プラグイン API への REST メッセージ呼び出しを調整します。 • この統合の出力はサードパーティ脆弱性です。
Tenable.sc の修正された脆弱性統合	• 重大度フィルターに基づいて、Tenable.sc 製品から脆弱性データを取得し、インスタンスで処理します。脆弱性一致アイテムは「オープン」および「再オープン」ステータスの検出レコードに対して作成されます。これらのレコードには修復が必要なためです。検出が「修正済み」の場合、既存の脆弱性一致アイテムは脆弱性対応によって更新されますが、Tenable は「修正済み」の脆弱性を「脅威緩和」とみなすため、デフォルトでは「 修正済み」の検出に対して脆弱性一致アイテムは作成されません。 • セットアップアシスタントで「修正済みの脆弱性検出に対して脆弱性一致アイテムを作成」フラグがアクティブ化されている場合、新しい VI は「修正 済み」ステータスで作成されるため、それらを作成した検出を表示できます。VI はインスタンスにまだ存在しない「修正済み 」の検出に対して作成されるため、インポートのパフォーマンスに悪影響を与える可能性があります。この機能を非アクティブのままにして、 修正済みの検出によって既存の脆弱性一致アイテムの状況だけが更新されるようにすることもできます。 • 一致しない資産に対して一意の CI を作成するか、同じ IP アドレスを共有する環境全体の資産に対してネットワークパーティション識別子属性を使用して既存の CI を更新します。 • 脆弱性 API への REST メッセージ呼び出しを調整します。 • この統合の出力は [クローズ済み]/[修正済み] の脆弱性一致アイテム (VI) です。これは、資産とサードパーティのエントリーが存在しない場合にも作成されます。 この統合実行はスケジュールされた実行です。これはチェーン統合であり、実行が正常に完了すると、後述の Tenable.sc オープンな脆弱性統合がトリガーされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.sc の統合 (続く)

統合	説明
	注: デフォルトでは、ファミリー ID 0 と 39 はこの統合から除外されます。
Tenable.sc のオープンな脆弱性統合	• この統合は、Tenable.sc の修正された脆弱性統合が正常に完了するとトリガーされます。 • 選択したクエリフィルターに基づいて、Tenable.sc 製品から脆弱性データを取得し、インスタンスで処理します。 • アクティブな脆弱性に対応する脆弱性一致アイテムを作成します。 • 一致しない資産に対して一意の CI を作成するか、同じ IP アドレスを共有する環境全体の資産に対してネットワークパーティション識別子属性を使用して既存の CI を更新します。 • 脆弱性 API への REST メッセージ呼び出しを調整します。 • この統合の出力は、[更新]/[新規作成] の脆弱性一致アイテム (VI) となります (まだ存在しない場合)。これは、構成アイテムとサードパーティのエントリーが存在しない場合にも作成されます。 **注:** デフォルトでは、ファミリー ID 0 と 39 はこの統合から除外されます。
Tenable.sc スキャン認証情報統合	• この統合は、Tenable.sc で構成されたスキャン認証情報を取得します。 • 認証情報 API への REST メッセージ呼び出しを調整します。 • この統合の出力は、テーブル [sn_vul_tenable_scan_credential] に入力されるスキャン認証情報です。 • インポートされた認証情報は、スキャン要求が Now Platform から開始されたときにスキャナーにアクセスするために使用されます。 • この統合は毎週実行されるようにスケジュールされています。
Tenable.sc バックフィル脆弱性統合	• このバックフィル統合は、インポート中に見落とされた可能性があるオープンおよび修正された脆弱性をインポートします。 • この統合では、過去 7 日間のオープンな脆弱性と修正された脆弱性の両方をインポートして、検出と脆弱性一致アイテムを更新します。 • この統合により、パフォーマンスが影響を受ける可能性があります。 • この統合はデフォルトで無効になっています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.sc の統合 (続く)

統合	説明
	• 脆弱性データを更新し、潜在的なパフォーマンスの問題を回避するために、他のスキャンが実行されていないときに Tenable.sc の修正された脆弱性とオープンな脆弱性統合をスケジュールすることをお勧めします。 • この統合の出力は次のようになります。 ○ [クローズ済み]/[修正済み] 脆弱性一致アイテム (VI)。これは、資産とサードパーティのエントリーが存在しない場合にも作成されます。 ○ [更新]/[新規作成] の脆弱性一致アイテム (VI) (まだ存在しない場合)。これは、構成アイテムとサードパーティのエントリーが存在しない場合にも作成されます。

ユーザー認証と **Tenable.sc**

ユーザー認証は、Now Platform® インスタンスとバージョン 5.13 の Tenable.sc 製品でサポートされています。バージョン 5.12 以前の Tenable.sc 製品を使用している場合は、ユーザー認証が必要です。

Tenable.sc 統合のユーザー認証を選択すると、統合の実行中にトークンが期限切れになり、置き換えられる可能性があります。トークンの有効期限が切れると、脆弱性統合実行レコード (VIN) の [メモ] 列に、[エラー：トークンの検証に失敗しました (Error: Token validation is failed)] のメッセージが表示されます。このメッセージが表示された場合は、アクションは必要ありません。期限切れのトークンはバックグラウンドで自動的に更新され、メッセージには統合プロセスの一時停止やエラーは表示されません。

Tenable 脆弱性統合の準備

次のセットアップタスクを実行して ServiceNow® Tenable 脆弱性統合を準備します。

事前準備

統合を成功させるには、統合前のタスクを計画して慎重に実行する必要があります。Vulnerability Response Integration with Tenable アプリケーションのインストールと構成をスムーズに行えるように、アプリケーションをインストールして、脆弱性データを Now Platform® インスタンスにインポートする前に、次のチェックリストを印刷し、リストされているアイテムが完了していることを確認することをお勧めします。

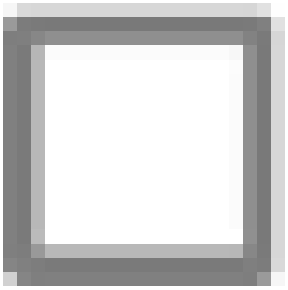
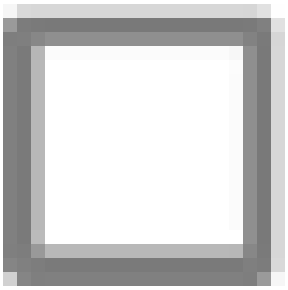
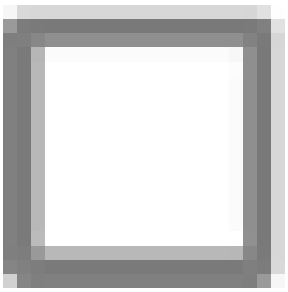
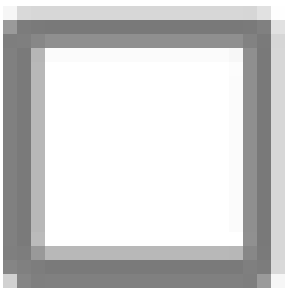
注:
Tenable でビルドされた統合を使用してデータをインポートし、ServiceNow® Vulnerability Response Integration with Tenable の使用を開始する場合は、次を参照してください。

Tenable でビルドされた統合から ServiceNow によってビルドされた統合への現在のデータのクリーンアップおよび移行情報については、「Guidelines to migrate from the Tenable Vulnerability Response Integration to the ServiceNow Vulnerability Response Integration with Tenable [KB0960667] (Tenable Vulnerability Response Integration から ServiceNow Vulnerability Response Integration with Tenable への移行に関するガイドライン [KB0960667])」の記事を参照してください。

必要なロール：アプリケーションをダウンロードしてインストールするアドミン

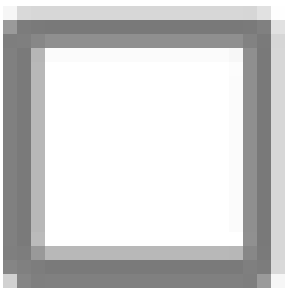
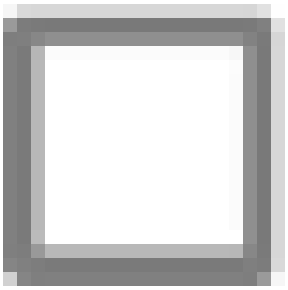
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスク	説明
	(オプション) まだインストールしてアクティブ化していない場合は、サードパーティアプリケーションをインストールする前に 脆弱性対応 アプリケーションをインストールすることもできます。 脆弱性対応 アプリケーションのインストールとアクティブ化の詳細については、「脆弱性対応 のインストール」を参照してください。この統合には、脆弱性対応 のバージョン 12.1 以降が必要です。
	まだインスタンスにない場合は、エンタイトルメントを取得して、Vulnerability Response Integration with Tenable アプリケーションを Now Platform インスタンスにダウンロードします。Vulnerability Response Integration with Tenable アプリケーションは、バージョン 5.13 以降の Tenable.sc 製品をサポートしています。 「」を参照してください。
	インポートする予定の脆弱性一致アイテムの数を見積もります。 インポートする予定の脆弱性一致アイテムの数をインスタンスが受け入れることができることを確認します。インスタンスが小さすぎると、ロードに時間がかかることがあります。インスタンスのサイズがわからない場合、またはサポートが必要な場合は、ServiceNow テクニカルサポートにお問い合わせください。
	統合を管理し、脆弱性一致アイテムを修正するグループまたはユーザーがいることを確認します。 admin システムアドミニストレーターは、セットアップアシスタントを使用して Vulnerability Response Integration with Tenable アプリケーションをインストールします。アサインされていない場合、アドミニストレーターはセットアップアシスタントで脆弱性アドミン (sn_vul.vulnerability_admin) およびその他のロールをアサインします。 sn_vul.vulnerability_admin アサインされると、脆弱性アドミニストレーターは Tenable 統合の構成を完了します。このロールは、脆弱性対応 (VR) アプリケーションとそのレコードに完全にアクセスできます。すべての VR アプリケーションとルールを構成し、サードパーティ統合を構成します。 sn_vul_tenable.configure_integration Tenable 脆弱性統合を構成できます。このロールには、sn_vul_tenable.read_integration の詳細なロールが含まれます。

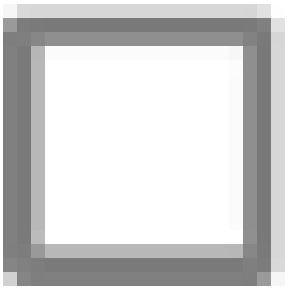
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスク	説明
	sn_vul_tenable.read_integration Tenable 脆弱性統合のレコードを表示 (読み取り) できます。 脆弱性対応グループ デフォルトで脆弱性対応グループはセットアップアシスタントで利用可能になっています。Vulnerability Response (脆弱性対応) グループにアサインされたユーザーは sn_vul.read_all および sn_vul.remediation_owner ロールを自動的に継承します。 システムアドミンは、ユーザーとグループへのロールの最初のアサインをセットアップアシスタントで実行して統合します。デフォルトで、Vulnerability Response (脆弱性対応) グループは利用可能になっています。まだ作成されていない場合は、セットアップアシスタントを使用する前に、追加のグループを作成し、ユーザー管理モジュールでインスタンスにユーザーを追加することをお勧めします。「ユーザーグループを作成」を参照してください。 脆弱性対応アプリケーションでユーザーが実行および表示できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。
	最初のインポートのパフォーマンスを改善するには、インスタンスの特定の機能、ルール、またはジョブを無効にすることをお勧めします。 • 脆弱性算出を使用しない場合は無効にします。これらの算出では、定義した算出に加え、脆弱性一致アイテムレコードが作成および更新されるたびに実行されます。「脆弱性算出を無効化」を参照してください。 • レコードの最初のインポート中に、特定の通知関連のビジネスルールによって大量の通知が生成され、パフォーマンスが影響を受ける可能性があることを確認します。最初のインポートの前に、「Tenable 脆弱性統合のインポートの変更」で説明されているように通知関連のビジネスルールを無効にすることをお勧めします。
	統合に必要なインスタンス内の機能、ルール、依存関係プラグイン、またはジョブが有効になっていることを確認します。 • Tenable.sc は、Vulnerability Response Integration with Tenable 製品と Now Platform インスタンスが同じ環境にある場合に MID サーバーを使用するオプションを提供するオンプレミスの統合です。Tenable.sc 製品と Now Platform インスタンスが同じ環境にない場合は、MID サーバーを使用する必要があります。インスタンスの MID サーバーの詳細については、「MID サーバー」を参照してください。 • IntegrationHub プラグインがンストールされ、アクティブ化されていることを確認します。このプラグインにより、ベースシステムコンポーネントが統合 API を使用して外部システムを呼び出せるようになり、REST などのプロトコルステップをアクティブ化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスク	説明
	次のように移動する。 システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて) をクリックし、プラグインを見つけます。インスタンスにインストールされていない場合は、インストールしてアクティブ化します。
	Tenable 資格証明を取得します。 Tenable 製品にアクセスするために必要なアカウント名、パスワード、その他のサービス情報があることを確認します。 Tenable.io には 64 以上の権限属性を持つアドミニストレーターアクセスが必要です。Tenable.sc にはセキュリティアナリストまたはマネージャーアクセスが必要です。 **注:** Vulnerability Response Integration with Tenable の v3.8 以降、Tenable.io へのアクセスにアドミン権限は不要になりました。権限属性が 16 に等しい基本ユーザーも製品にアクセスできます。

これで、「セットアップアシスタントを使用して、Vulnerability Response Integration with Tenable アプリケーションをインストールします。」に進む準備が整いました。

セットアップアシスタントを使用して、**Vulnerability Response Integration with Tenable** アプリケーションをインストールします。

ServiceNow® Tenable 脆弱性統合を実行する前に、ServiceNow Store から Vulnerability Response Integration with Tenable アプリケーションをダウンロードし、脆弱性対応 アプリケーションのセットアップアシスタントを使用してインストールおよび構成する必要があります。

始める前に
Tenable アプリケーションをインストールする前に、「Tenable 脆弱性統合の準備」のチェックリストのすべてのアイテムを完了していることを確認します。

注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

必要なロール：sn_vul.vulnerability_admin ロールを最初にアサインし、セットアップアシスタントで Tenable アプリケーションをインストールするアドミン。インストール後に、セットアップアシスタントでアプリケーションを構成する脆弱性アドミンロール (sn_vul.vulnerability_admin または sn_vul.admin (使用廃止))。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント > 統合アプリケーションのインストール.

   しばらくすると、インスタンスにインストールできるアプリケーションが表示されます。

2. **Tenable (Tenable** プラットフォーム) タイルを見つけて、[インストール] をクリックします。

   このアクションにより、ServiceNow Store からダウンロードした Vulnerability Response Integration with Tenable アプリケーションがインストールされます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. セットアップアシスタントで表示されるプロンプトに従い、インストールを続行します。
4. セットアップアシスタントを使用したアプリケーションのインストールの詳細については、「セットアップアシスタントを使用した 脆弱性対応 サードパーティアプリケーションのインストール」を参照してください。

次のタスク

セットアップアシスタントでインストールを完了したら、セットアップアシスタントで [統合設定] > [スキャナー統合] に移動して、構成を続行します。セットアップアシスタントで表示されるプロンプトを補足する詳細情報を確認する場合は、「セットアップアシスタントを使用した Tenable 脆弱性統合の構成」を参照してください。

Tenable 脆弱性統合のデータ検索設定

次のデータ検索設定は、ServiceNow® Tenable 脆弱性統合から Now Platform® インスタンスにインポートするデータのタイプとスコープを具体的に決定するのに役立ちます。

次のセクションで説明する設定は、インポートするデータを制御するのに役立ちます。さらに、これらのフィルターの値は統合インスタンスで設定できます。統合インスタンスを表示するには、次に移動します: **Tenable** 脆弱性統合 > 統合インスタンス をクリックし、統合、 Tenable.io 、または Tenable.scをクリックします。

表示される [統合インスタンス] ページで、[統合インスタンスパラメータ] をクリックして、パラメーターのリストを表示するか、[脆弱性統合] タブでスケジュール、REST 詳細、統合の詳細、データソース、および統合実行情報を表示します。

Now Platform インスタンスの **Tenable.io** および **Tenable.sc** の一般的な重大度と取得の設定およびフィルター

次の設定は、Now Platform インスタンスの Tenable.io および Tenable.sc 統合で使用できます。これらの構成設定およびその他の構成設定は、Now Platform インスタンスの [統合インスタンス] ページに表示されます。最初の数回の実行では、これらの設定をデフォルトのままにすることをお勧めします。

Tenable.io

insert_fixed
: 脆弱性インポート統合のセットアップアシスタントで **insert_fixed** フラグを有効にすると、インスタンスにまだ存在しない [修正済み] ステータスの検出に対して新しい VI が作成されます。

severity_critical
: このフィルターは、Tenable.io のオープンな脆弱性統合と Tenable.io の修正された脆弱性統合から最重要の重大度の脆弱性を受信できるようにデフォルトで有効になっています (true)。

severity_high
: このフィルターは、Tenable.io のオープンな脆弱性統合と Tenable.io の修正された脆弱性統合から高レベルの重大度の脆弱性を受信できるようにデフォルトで有効になっています (true)。

severity_medium
: このフィルターは、デフォルトでは非アクティブです (false)。Tenable.io のオープンな脆弱性統合と Tenable.io の修正された脆弱性統合から中レベルの重大度の脆弱性を受信するには、このフィルターを有効にします。

severity_info

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このフィルターは、デフォルトでは非アクティブです (false)。Tenable.io のオープンな脆弱性統合と Tenable.io の修正された脆弱性統合から情報レベルの重大度の脆弱性を受信するには、このフィルターを有効にします。

severity_low

このフィルターは、デフォルトでは非アクティブです (false)。Tenable.io のオープンな脆弱性統合と Tenable.io の修正された脆弱性統合から低レベルの重大度の脆弱性を受信するには、このフィルターを有効にします。

size

この設定では、Tenable.io プラグイン統合からの結果セットに含めるプラグインレコードの数を定義します。int32 形式である必要があります。デフォルト値は 1,000 です。最大サイズは 10,000 です。

num_assets

Tenable.io の修正された脆弱性統合と Tenable.io のオープンな脆弱性統合からエクスポートされたチャンクあたりの脆弱性の最大数。デフォルト値は 50 です。

chunk_size

Tenable.io 資産統合によってエクスポートされたチャンクあたりの資産数を指定します。デフォルトは 1,000 です。

Tenable.sc

async_request

このパラメーターは、デフォルトでは非アクティブです (false)。Tenable.sc を使用して非同期または同期 API コールを実行するには、このパラメーターを有効または無効にします。同期呼び出しで 30 秒でタイムアウトする場合は、Tenable 製品のサポートに連絡してボックスを調整してください。このパラメーターを有効にすると、Tenable.sc のすべての統合に適用されます。既存の顧客が非同期呼び出しを使用している場合は、既存の Tenable.sc 統合インスタンスに新しい async_request パラメーターを追加する修正スクリプトを利用できます。修正スクリプトを表示するには、次に移動します: システム定義 > 修正スクリプト.

insert_fixed

脆弱性インポート統合のセットアップアシスタントで **insert_fixed** フラグを有効にすると、インスタンスにまだ存在しない [修正済み] ステータスの検出に対して新しい VI が作成されます。

offset

1 回の統合実行でインポートされる資産、プラグイン、および脆弱性の数を指定します。

クエリフィルター

クエリフィルターは、Tenable コンソール内から構成されます。これらのクエリフィルターには、セットアップアシスタントまたは Now Platform インスタンスの [統合インスタンス] ページから選択できる ID があります。これらのフィルターは、Tenable.sc 統合からデータを取得するときに適用されます。

Tenable 脆弱性統合の **REST** メッセージ

ServiceNow® Tenable 脆弱性統合 REST メッセージは、Tenable API の呼び出しに使用されます。

Tenable.io 資産 **REST** メッセージ

Tenable.io 資産 REST メッセージは、Tenable.io 資産統合の資産情報を取得します。REST メッセージメソッドレコードを変更すると、資産情報を取得するための Tenable.io への要求が影響を受けます。資産のエクスポートジョブは、次のフィルターを使用して送信されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- "is_deleted"：false
- "is_licensed"：true

Tenable.io プラグイン REST メッセージ

Tenable.io プラグイン REST メッセージは、Tenable.io プラグイン統合のプラグイン情報を取得します。REST メッセージメソッドレコードを変更すると、プラグイン情報を取得するための Tenable.io への要求が影響を受けます。

Tenable.io 脆弱性 REST メッセージ

Tenable.io 脆弱性 REST メッセージは、Tenable.io 脆弱性統合からオープンとクローズ済みの両方の脆弱性の脆弱性情報を取得します。REST メッセージメソッドレコードを変更すると、脆弱性情報を取得するための Tenable.io への要求が影響を受けます。

Tenable.sc クエリ REST メッセージ

Tenable.sc クエリ REST メッセージは、クエリフィルターが構成されている Tenable.sc 資産統合および Tenable.sc 脆弱性統合のクエリフィルター情報を取得します。

Tenable.sc プラグイン REST メッセージ

Tenable.sc プラグイン REST メッセージは、Tenable.sc プラグイン統合のプラグイン情報を取得します。REST メッセージ Get プラグインメソッドレコードを変更すると、プラグイン情報を取得するための Tenable.sc への要求が影響を受けます。

パラメーター名	値	説明
type	active	Tenable がデータをプルするソースを示します。コードで使用されます。変更は推奨されません。
fields	id、description、cvssVector、cvssVectorV3、cvssV3TemporalVector、synopsis、vprScore、vprContext	取得するプラグインのフィールドのリストを示します。

Tenable.sc 脆弱性 REST メッセージ

Tenable.sc 脆弱性 REST メッセージは、Tenable.sc 統合から脆弱性情報を取得します。REST メッセージの [脆弱性をフェッチ (Fetch Vulnerabilities)] または [パッチが適用された脆弱性をフェッチ (Fetch Patched Vulnerabilities)] メソッド (v14.0 の 脆弱性対応 および Tenable 脆弱性統合の v2.2 以降の場合は、[バックフィル脆弱性のフェッチ (Fetch Backfill Vulnerabilities)] レコード) を変更すると、脆弱性情報を取得するための Tenable.sc への要求が影響を受けます。

Tenable.sc スキャン認証情報 REST メッセージ

Tenable.sc ポリシー REST メッセージ

Tenable.sc ポリシーの POST REST メッセージは、要求されたプラグインのポリシーを追加します。生成されたポリシーは Tenable.sc スキャン要求で使用されます。

Tenable.sc スキャン REST メッセージ

Tenable.sc スキャン POST REST メッセージは、REST メッセージの要求本文で定義されたアクセスと権限に依存するスキャンを追加します。スキャン要求の要求本文でポリシー、プラグイン ID、および IP を使用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.sc スキャン結果 REST メッセージ

Tenable.sc スキャン結果 GET REST メッセージは、スキャン REST メッセージを使用して生成されたスキャンの詳細を提供します。スキャン REST メッセージの応答で scanResultId を使用し、トリガーされたスキャンの詳細を取得します。

Tenable.sc スキャン認証情報

Tenable.sc スキャン認証情報 REST メッセージは、Tenable.sc から認証情報を取得します。REST メッセージ「Import」メソッドレコードを変更すると、認証情報を取得するための Tenable.sc への要求が影響を受けます。

パラメーター名	値	説明
fields	id、name、description、type	Tenable.sc からインポートされたフィールドのリストを示します。
filter	usable	統合が Tenable.sc から使用可能な認証情報のみをプルすることを示します。 どちらのパラメーターも変更しないことをお勧めします。

Tenable 脆弱性統合のデータ変換

インポートするデータを特定すると、Tenable 製品からデータが取得され、インスタンス内の一連のデータソースと変換によって処理されます。

インストール時に、正規化された重大度マップが [正規化された重大度マッピング (Normalized Severity Mapping)] モジュールにインストールされます。これらのマップ変換では、Tenable 重大度レベルを標準の重大度レベルにインポートし、インスタンス処理します。重大度マップの作成については、脆弱性対応 ドキュメントの Vulnerability Response 重大度マップの作成についてを参照してください。

Tenable.io 資産インポート

インポートされた資産データは、最初に Tenable.io 資産インポート [sn_vul_tenable_io_asset_import] テーブルにロードされます。

Tenable.io 資産統合変換マップは、インポートされた資産情報の変換に使用されます。この変換を変更すると、Tenable 資産インポートからのデータの処理方法が変更されます。この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ. 「Tenable.io Asset Transform」を検索します。

次の表に、統合別の変換マップフィールドを示します。

Tenable.io 資産変換マップのフィールド

ソースフィールド	ターゲットフィールド	説明
u_id	source_id	Tenable は資産の一意の ID を提供して、検出されたアイテムレコードにマッピングし、CI ルックアップに使用されます。
u_ipv4s	ip_address	最初の ip 値を検出されたアイテムレコードの ip_address

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.io 資産変換マップのフィールド (続く)

ソースフィールド	ターゲットフィールド	説明
		フィールドにマッピングします。
u_mac_addresses	mac_address	最初の mac_address 値を検出されたアイテムレコードの mac_address フィールドにマッピングします。
u_fqdns	fqdn	最初の fqdn 値を検出されたアイテムレコードの fqdn フィールドにマッピングします。
u_netbios_names	netbios	最初の netbios 値を検出されたアイテムレコードの netbios フィールドにマッピングします。
u_operating_systems	os	最初の OS 値を検出されたアイテムレコードの os フィールドにマッピングします。
(v 14.0 の 脆弱性対応 および v2.2 の Tenable 脆弱性統合より前)u_last_scan_time	last_scan_date	検出されたアイテムレコードの last_scan_date フィールドにマッピングします。
u_last_authenticated_scan_date	last_auth_scan_date	検出されたアイテムレコードの last_auth_scan_date フィールドにマッピングします。
[script]	name	スクリプトのロジックを使用してホスト名をマッピングします。
u_tags		タグは sn_sec_cmn_host_tag に保存されます。タグから資産へのマッピングは sn_sec_cmn_m2m_src_ci_tag に保存されます。

変換プロセスでは、3 つの変換スクリプトが実行されます。次の表に、各スクリプトが実行されるタイミングとその目的を示します。

Tenable.io 資産変換マップスクリプトのタイミングと目的

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	この変換は、統合プロセスの import_set の値を初期化するために使用されます。内部使用。変更または削除することはお勧めしません。
onBefore (インポートセットの変換が完了する前)。	ホストの値を更新し、ホストが既に存在するかどうかを確認するために使用される機能。結果に基づいて、import_set の値を変更します。内部使用。変更または削除することはお勧めしません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

スクリプトが実行されるタイミング	目的
onComplete (インポートセットが変換を完了したとき)	この変換は、作成された新しい CI と更新されて無視された CI の値を設定するために使用されます。内部使用。変更または削除することはお勧めしません。

Tenable.io プラグイン統合

Tenable.io プラグイン変換マップは、Tenable.io からインポートされたプラグインを変換するために使用されます。

注:
この変換マップを変更すると、Tenable プラグインから取得するデータの処理方法が変更されます。

この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ. Tenable.io プラグイン変換を検索します。

Tenable.io プラグインのペイロードには、sn_vul_tenable_io_plugin_import テーブルの u_attributes 列のすべてのフィールドが含まれます。次の表に示すように、属性フィールドが解析され、サードパーティのエントリーテーブルレコードにマッピングされます。

ソースフィールド	ターゲットフィールド	説明
id	id	ソースから ID をマッピングし、TEN プリフィックスを追加します。たとえば、受信した ID が 12345 の場合、ターゲットテーブルの ID は TEN-12345 です。
説明	summary	プラグインの説明を summary 列にマッピングします。
[script]	source	インポートされた TPE のソースは Tenable.io です。
[script]	source_instance	このレコードをインポートする Tenable 展開への参照
family	category	プラグインのファミリを category 列にマッピングします。
plugin_modification_date	last_modified	plugin_modification_date を最後に変更されたフィールドにマッピングします。
plugin_publication_date	date_published	plugin_publication_date を公開日にマッピングします。
has_patch	remediation_type	has_patch 値から修復タイプをマッピングします。
synopsis	threat	この脆弱性に関する脅威情報をマッピングします。
cvss_base__score	score	cvss ベーススコアをサードパーティのエントリーテーブル

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
		の score 列にマッピングします。
solution	solution	スキャナーによって提供されたソリューションをサードパーティのエントリーテーブルの solution 列にマッピングします。
exploit_available	exploit	スキャナーによって提供された exploit_available をサードパーティのエントリーテーブルの exploit 列にマッピングします。
vpr.score	source_risk_score	スキャナーによって提供された vpr スコアをサードパーティのエントリーテーブルの source_risk_score にマッピングします。
[script]	source_risk_rating	スコア範囲に基づいて、vpr スコアを標準リスク評価にマッピングします。 • 9 ～ 10 - 重大 • 7 ～ 9 – 高 • 4 ～ 7 - 中 • 0 ～ 4 - 低
vpr.drivers.age_of_vuln	age_of_vuln	スキャナーからの脆弱性の経過時間をサードパーティのエントリーテーブルの age_of_vuln 列にマッピングします。
vpr.drivers.exploit_code_maturity	exploit_code_maturity	スキャナーからのエクスプロイトコードの成熟度をサードパーティのエントリーテーブルの exploit_code_maturity にマッピングします。
vpr.drivers.product_coverage	product_coverage	スキャナーからの製品範囲をサードパーティのエントリーテーブルの product_coverage にマッピングします。
vpr.drivers.threat_sources_last28	threat_sources	スキャナーからの過去 28 日間の脅威ソースをサードパーティテーブルの threat_sources にマッピングします。
vpr.drivers.threat_intensity_last28	threat_intensity	スキャナーからの過去 28 日間の脅威の強さをサードパーティのエントリーテーブルの threat_intensity にマッピングします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
vpr.drivers.threat_recency	threat_recency	スキャナーからの脅威の最新性情報をサードパーティのエントリーテーブルの threat_recency にマッピングします。
vpr.drivers.cvss3_impact_score	v3_impact_subscore	cvss3 影響スコアをサードパーティのエントリーテーブルの v3_impact_subscore 列にマッピングします。
cvss_temporal_score	cvss_temporal_score	CVSS v2 の一時スコアをマッピングします。
cvss_v3_temporal_score	v3_temporal_score	CVSS v3 の一時スコアをマッピングします。
risk_factor	source_severity	サードパーティのエントリーテーブルのソース重大度にマッピングします。
name	name	プラグインの名前をサードパーティのエントリーテーブルの名前にマッピングします。
stig_severity	stig_severity	スキャナーによって提供された vpr スコアをサードパーティのエントリーテーブルの source_risk_score にマッピングします。
plugin_type	check_type	プラグインタイプをサードパーティのエントリーテーブルの check_type にマッピングします。
unsupported_by_vendor	unsupported_by_vendor	unsupported_by_vendor フィールドを unsupported_by_vendor 列にマッピングします。
[script]	exploit_attack_vector	サードパーティのエントリーテーブルの exploit_attack_vector 列は、列の exploit_available と v3_attack_vector に基づいて入力されます。

direct フィールドに加えて、その他の情報が関連リストとしてサードパーティのエントリーに追加されます。

ソースフィールド	説明
cve	CVE 関連データを参照テーブル (sn_vul_nvd_entry) に挿入します。NVD エントリーテーブル (sn_vul_nvd_entry) で同じ CVE が見つかった場合、現在の脆弱性が NVD

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	説明
	エントリーに関連付けられます。マッピングは sn_vul_m2m_entry_cve にあります。
bid	バグトラックのリストが参照として追加されます。
see_also	URL のリストが参照として追加されます。
xref	X-REF のリストが参照として追加されます。
[script]	そのプラグインのエクスプロイトのリスト。該当するエクスプロイトフレームワークとプラグインの sn_vul_m2m_framework_vul へのマッピングを挿入します。

変換プロセスでは、3 つの変換スクリプトが実行されます。次の表に、各スクリプトが実行されるタイミングとその目的を示します。

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	この変換は、統合プロセスの import_set の値を初期化するために使用されます。内部使用。変更または削除することはお勧めしません。
onBefore (インポートセットの変換が完了する前)。	サードパーティエントリーの値を更新し、サードパーティエントリーが既に存在するかどうかを確認するために使用される機能。結果に基づいて、サードパーティエントリーの値を変更します。内部使用。変更または削除することはお勧めしません。
onComplete (インポートセットが変換を完了したとき)	この変換は、作成された新しい CI と更新されて無視された CI の値を設定するために使用されます。内部使用。変更または削除することはお勧めしません。

TenableIOPluginsImportProcessor スクリプトインクルードは onBefore 変換スクリプトから呼び出されます。Tenable.io プラグイン統合からの出力を取得し、Now Platform サードパーティの脆弱性エントリーに変換します。このスクリプトインクルードを変更すると、サードパーティのエントリーテーブルの Tenable.io プラグインデータの変換が変更される可能性があります。

Tenable.io 脆弱性のインポート

Tenable.io 脆弱性一致アイテム変換マップは、Tenable.io からインポートされたオープンおよび修正された脆弱性情報を変換するために使用されます。

注:
この変換マップを変更すると、Tenable 脆弱性インポートからのデータの処理方法が変更されます。

Tenable.io の修正された脆弱性統合と Tenable.io のオープンな脆弱性統合の両方に同じ変換マップが使用されます。この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ. 「Tenable.io Vulnerable Item transform map」を検索します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
u_asset.uuid	id	uuid は cmdb_ci レコードの id フィールドにマッピングされます。
u_asset.ipv4	ip_address	ipv4 フィールドは cmdb_ci レコードの ip_address フィールドにマッピングされます。
u_asset .last_authenticated_results	last_auth_scan_date	前回の認証済みスキャン日は、cmdb_ci レコードの前回の認証済みスキャン日にマッピングされます。
u_asset.mac_addess	mac_address	MAC アドレスは cmdb_ci レコードの host mac address フィールドにマッピングされます。
u_asset.netbios_name	netbios	netbios は、cmdb_ci レコードの netbios フィールドにマッピングされます。
u._plugin.cvss3_base_score	v3_base_score	CVSS v3 ベーススコアは、サードパーティのエントリーレコードの v3 ベーススコアにマッピングされます。
u._plugin.cvss3_temporal_score	v3_temporal_score	CVSS v3 一時スコアは、サードパーティのエントリーレコードの v3 一時スコアにマッピングされます。
u._plugin.cvss_base_score	score	CVSS ベーススコアは、サードパーティのエントリーレコードの score フィールドにマッピングされます。
u._plugin.cvss_temporal_score	temporal_score	一時スコアは、サードパーティのエントリーレコードの一時スコアにマッピングされます。
u_plugin.description	summary	説明は、サードパーティのエントリーレコードの summary フィールドにマッピングされます。
u_plugin.family	category	プラグインのファミリをサードパーティのエントリーレコードの category 列にマッピングします。
u_plugin.modification_date	last_modified	最終変更日は、サードパーティのエントリーレコード

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
		のプラグインの最終変更日にマッピングされます。
u_plugin.publication_date	date_published	公開日は、サードパーティのエントリーレコードの date_published フィールドにマッピングされます。
u_plugin.risk_factor	source_severity	リスク要因は、サードパーティのエントリーレコードの source_severity フィールドにマッピングされます。
u_plugin.solution	solution	ソリューションは、サードパーティのエントリーレコードの solution フィールドにマッピングされます。
u_plugin.synopsis	threat	概要は、サードパーティのエントリーレコードの threat フィールドにマッピングされます。
u_severity_id	priority	優先度は、ペイロードの重大度 ID にマッピングされます。デフォルト値は 5 です。
u_plugin.exploit_available	exploit	スキャナーによって提供された exploit_available をサードパーティのエントリーテーブルの exploit 列にマッピングします。
vpr.score	source_risk_score	スキャナーによって提供された vpr スコアをサードパーティのエントリーテーブルの source_risk_score にマッピングします。
[script]	source_risk_rating	スコア範囲に基づいて、vpr スコアを標準リスク評価にマッピングします。 • 9 ～ 10 - 重大 • 7 ～ 9 – 高 • 4 ～ 7 - 中 • 0 ～ 4 - 低
u_plugin.vpr.drivers.age_of_vuln	age_of_vuln	スキャナーからの脆弱性の経過時間をサードパーティのエントリーテーブルの age_of_vuln にマッピングします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
u_plugin.vpr.drivers.exploit_code_maturity	exploit_code_maturity	スキャナーからのエクスプロイトコードの成熟度をサードパーティのエントリーテーブルの exploit_code_maturity にマッピングします。
u_plugin.vpr.drivers.product_coverage	product_coverage	スキャナーからの製品範囲をサードパーティのエントリーテーブルの product_coverage にマッピングします。
u_plugin.vpr.drivers.threat_sources_last28	threat_sources	スキャナーからの過去 28 日間の脅威ソースをサードパーティのエントリーテーブルの threat_sources にマッピングします。
u_plugin.vpr.drivers.threat_intensity_last28	threat_intensity	スキャナーからの過去 28 日間の脅威の強さをサードパーティのエントリーテーブルの threat_intensity にマッピングします。
u_plugin.vpr.drivers.threat_recency	threat_recency	スキャナーからの脅威の最新性情報をサードパーティのエントリーテーブルの threat_recency にマッピングします。
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	CVSS3 v3 影響スコアをサードパーティのエントリーテーブルの v3_impact_subscore 列にマッピングします。
u_plugin.type	check_type	プラグインタイプをサードパーティのエントリーテーブルの check_type にマッピングします。
u_plugin.unsupported_by_vendor	unsupported_by_vendor	プラグインの unsupported_by_vendor フィールドを unsupported_by_vendor 列にマッピングします。
[script]	exploit_attack_vector	サードパーティのエントリーテーブルの exploit_attack_vector 列は、列の exploit_available と v3_attack_vector に基づいて入力されます。
u_plugin.family_id	family_id	プラグインのファミリ ID をサードパーティのエントリーテーブルの family_id 列にマッピングします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
port	port	ポートは、脆弱性一致アイテムレコードの port フィールドにマッピングされます。
protocol	protocol	プロトコルは、脆弱性一致アイテムレコードの protocol フィールドにマッピングされます。
u_first_found	first_found	初回検出は、脆弱性一致アイテムレコードの first_found フィールドにマッピングされます。
u_last_found	last_found	前回検出は、脆弱性一致アイテムレコードの last_found フィールドにマッピングされます。
u_state	state	ステータスは、脆弱性一致アイテムレコードの [ステータス (State)] フィールドにマッピングされます。
[script]	source	統合のソースが入力されます。この統合から作成された脆弱性一致アイテムには、Tenable.io がソースとして含まれています。
[script]	integration_instance	integration_instance は、脆弱性一致アイテムのインポート元のインスタンスの名前です。
u_plugin.name	name	プラグインの名前をサードパーティのエントリーテーブルの名前にマッピングします。
u_plugin.stig_severity	stig_severity	プラグインの stig 重大度をサードパーティのエントリーテーブルの stig_severity 列にマッピングします。

direct フィールドに加えて、その他の情報が関連リストとしてサードパーティのエントリーに追加されます。

ソースフィールド	説明
cve	CVE 関連データを参照テーブル (sn_vul_nvd_entry) に挿入します。NVD エントリーテーブル (sn_vul_nvd_entry) で同じ CVE が見つかった場合、現在の脆弱性が NVD

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	説明
	エントリーに関連付けられます。マッピングは sn_vul_m2m_entry_cve にあります。
bid	バグトラックのリストが参照として追加されます。
see_also	URL のリストが参照として追加されます。
xref	X-REF のリストが参照として追加されます。
[script]	そのプラグインのエクスプロイトのリスト。該当するエクスプロイトフレームワークとプラグインの sn_vul_m2m_framework_vul へのマッピングを挿入します。

変換プロセスでは、3 つの変換スクリプトが実行されます。次の表に、各スクリプトが実行されるタイミングとその目的を示します。

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	この変換は、インポートセットを使用して Tenable.io からデータをインポートする TenableIOVulnerabilitiesProcessor をトリガーし、各レコードを CMDB CI テーブル、脆弱性一致アイテムテーブル、およびサードパーティ脆弱性テーブルに内部使用のためにロードします。変更または削除することはお勧めしません。
onBefore (インポートセットの変換が完了する前)。	サードパーティのエントリーと検出が既に存在するかどうかを確認する機能。そうでない場合、これらのレコードはそれぞれのテーブルに作成されます。内部使用。変更または削除することはお勧めしません。
onComplete (インポートセットが変換を完了したとき)	この変換は、Tenable.io からインポートされた CI、VI および検出の数を更新するのに使用されます。内部使用。変更または削除することはお勧めしません。

Tenable.sc 資産インポート

Tenable.sc からインポートされた資産データは、最初に Tenable.sc 資産インポートテーブル (sn_vul_tenable_sc_asset_import) にロードされます。Tenable.sc 資産統合変換マップは、インポートされた資産情報の変換に使用されます。この変換を変更すると、Tenable 資産インポートからのデータの処理方法が変更されます。この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ. 「Tenable.sc Asset Transform」を検索します。

ソースフィールド	ターゲットフィールド	説明
u_uuid	id	uuid は Tenable API から入力されないため、「u_uniqueness」属性を使用して資産の一意の uuid フィールドを作成し、それを cmdb_ci レコードにマッピングします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ソースフィールド	ターゲットフィールド	説明
u_ip	ip_address	API からの ip フィールドを cmdb_ci レコードの ip_address フィールドにマッピングします。
u_macaddress	mac_address	API からの macaddress フィールドを cmdb_ci レコードの address フィールドにマッピングします。
u_dnsname	fqdn	API からの dnsname フィールドを cmdb_ci レコードの fqdn フィールドにマッピングします。
u_netbiosname	netbios	API からの netbios フィールドを cmdb_ci レコードの netbios フィールドにマッピングします。
u_oscpe	os	OS 情報はペイロードの oscpe 属性から抽出され、cmdb_ci レコードの os フィールドにマッピングされます。
u_lastauthrun	last_auth_scan_date	API からの lastauthrun フィールドを、検出されたアイテムレコードの last_auth_scan_date フィールドにマッピングします。
u_lastauthrun および u_lastunauthrun	last_scan_date	lastauthrun は、Tenable API または lastunauthrun から抽出されます。検出されたアイテムレコードの last_scan_date フィールドは、ペイロードに表示される値に基づいて入力されます。

変換プロセスでは、3 つの変換スクリプトが実行されます。次の表に、各スクリプトが実行されるタイミングとその目的を示します。

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	この変換は、統合プロセスの import_set の値を初期化するために使用されます。内部使用。変更または削除することはお勧めしません。
onBefore (インポートセットの変換が完了する前)。	ホストの値を更新し、ホストが既に存在するかどうかを確認するために使用される機能。結果に基づいて、import_set の値を変更します。内部使用。変更または削除することはお勧めしません。
onComplete (インポートセットが変換を完了したとき)	この変換は、作成された新しい CI と更新されて無視された CI の値を設定するために使用されます。内部使用。変更または削除することはお勧めしません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Tenable.sc プラグインのインポート

Tenable.sc からインポートされたプラグインデータは、最初に Tenable.sc プラグインインポートテーブル (sn_vul_tenable_sc_plugin_import) にロードされます。Tenable.sc プラグイン変換マップは、インポートされたプラグイン情報の変換に使用されます。この変換を変更すると、Tenable プラグインインポートからのデータの処理方法が変更されます。この変換マップにアクセスするには、次に移動します: システムインポートセット > 変換マップ. 「Tenable.sc Plugin Transform Map」を検索します。

ソースフィールド	ターゲットフィールド	説明
u_id	id	ソースから ID をマッピングし、TEN プリフィックスを追加します。たとえば、受信した ID が 12345 の場合、ターゲットテーブルの ID は TEN-12345 です。
u_description	summary	プラグインの説明を summary 列にマッピングします。
[script]	source	この統合からインポートされた TPE には、Tenable.sc がソースとして含まれています。
[script]	source_instance	このレコードをインポートする Tenable 展開への参照
u_family	category	プラグインのファミリオブジェクトの name フィールドを category 列にマッピングします。
u_plugin_modification_date	last_modified	plugin_modification_date を最後に変更されたフィールドにマッピングします。
u_plugin_publication_date	date_published	plugin_publication_date を公開日にマッピングします。
u_has_patch	remediation_type	has_patch 値から修復タイプをマッピングします。
u_synopsis	threat	この脆弱性に関する脅威情報をマッピングします。
u_cvss_base_score	score	CVSS ベーススコアをサードパーティのエントリーテーブルの score 列にマッピングします。
u_solution	solution	スキャナーによって提供されたソリューションをサードパーティのエントリーテーブルの solution 列にマッピングします。
u_cvss_temporal_score	cvss_temporal_score	CVSS v2 の一時スコアをマッピングします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
u_cvss_v3_temporal_score	v3_temporal_score	CVSS v3 の一時スコアをマッピングします。
u_risk_factor	source severity	サードパーティのエントリーテーブルのソース重大度にマッピングします。
u_cvss_v3_base_score	v3_base_score	サードパーティのエントリーテーブルの CVSS ベーススコアをマッピングします。
u_exploit_available	exploit	スキャナーによって提供された exploitAvailable をサードパーティのエントリーテーブルの exploit 列にマッピングします。
u_vpr_score	source_risk_score	スキャナーからの VPR スコアをサードパーティのエントリーテーブルのソースリスクスコアにマッピングします。
[script]	source_risk_rating	スコア範囲に基づいて、vpr スコアを標準リスク評価にマッピングします。 • 9 ～ 10 - 重大 • 7 ～ 9 – 高 • 4 ～ 7 - 中 • 0 ～ 4 - 低
u_vpr_context[id=age_of_vuln]	age_of_vuln	スキャナーからの脆弱性の経過時間をサードパーティのエントリーテーブルの age_of_vuln にマッピングします。
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	スキャナーからのエクスプロイトコードの成熟度をサードパーティのエントリーテーブルの exploit_code_maturity にマッピングします。
u_vpr_context[id=product_coverage]	product_coverage	スキャナーからの製品範囲をサードパーティのエントリーテーブルの product_coverage にマッピングします。
u_vpr_context[id="threat_sources_last_28"]	threat_sources	スキャナーからの過去 28 日間の脅威ソースをサードパーティテーブルの threat_sources にマッピングします。
u_vpr_context[id="threat_intensity_last_28"]	threat_intensity	スキャナーからの過去 28 日間の脅威の強さをサードパーティのエントリーテーブルの threat_intensity にマッピングします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
u_vpr_context[id="threat_recency"]	threat_recency	スキャナーからの脅威の最新性情報をサードパーティのエントリーテーブルの threat_recency にマッピングします。
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	スキャナーからの CVSS v3 影響スコアをサードパーティのエントリーテーブルの v3_impact_subscore にマッピングします。
u_name	name	プラグインの名前をサードパーティのエントリーテーブルの name 列にマッピングします。
u_stig_severity	stig_severity	プラグインの stig_severity フィールドをサードパーティのエントリーテーブルの stig_severity にマッピングします。
u_check_type	check_type	チェックタイプをサードパーティのエントリーテーブルの check_type にマッピングします。
u_family.id	family_id	プラグインの family_id をサードパーティのエントリーテーブルの family_id にマッピングします。
[script]	exploit_attack_vector	サードパーティのエントリーテーブルの exploit_attack_vector 列は、列の exploit_available と v3_attack_vector に基づいて入力されます。

direct フィールドに加えて、その他の情報が関連リストとしてサードパーティのエントリーに追加されます。

ソースフィールド	説明
u_cpe	CPE のリストが参照として追加されます。
u_see_also	URL のリストが参照として追加されます。
u_exploit_frameworks	そのプラグインのエクスプロイトのリスト。該当するエクスプロイトフレームワークとプラグインの sn_vul_m2m_framework_vul へのマッピングを挿入します。

変換プロセスでは、3 つの変換スクリプトが実行されます。次の表に、各スクリプトが実行されるタイミングとその目的を示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	この変換は、統合プロセスの import_set の値を初期化するために使用されます。内部使用。変更または削除することはお勧めしません。
onBefore (インポートセットの変換が完了する前)。	サードパーティエントリーの値を更新し、サードパーティエントリーが既に存在するかどうかを確認するために使用される機能。結果に基づいて、サードパーティエントリーの値を変更します。内部使用。変更または削除することはお勧めしません。
onComplete (インポートセットが変換を完了したとき)	この変換は、作成されて無視されたプラグインの値を設定するために使用されます。内部使用。変更または削除することはお勧めしません。

TenableSCPluginsImportProcessor スクリプトインクルードは onBefore 変換スクリプトから呼び出されます。Tenable.sc プラグイン統合からの出力を取得し、Servicenow サードパーティの脆弱性エントリーに変換します。このスクリプトインクルードを変更すると、サードパーティのエントリーテーブルの Tenable.sc プラグインデータの変換が変更される可能性があります。

Tenable.sc 脆弱性インポート

Tenable.sc のオープンな脆弱性変換マップは、Tenable.sc のオープンな脆弱性統合からインポートされたデータを変換するために使用され、Tenable.sc および修正された脆弱性変換マップは、Tenable.sc の修正された脆弱性統合からインポートされたデータを変換するために使用されます。

注:
これらの変換マップを変更すると、[修正済み]/[オープン] の Tenable 脆弱性インポートからのデータの処理方法が変更されます。

Tenable.sc オープンおよび修正された脆弱性変換マップにアクセスするには、次に移動します: **Tenable** 脆弱性統合 > アドミニストレーション > 統合インスタンス > **Tenable.sc** 修正済み/オープンな脆弱性統合 > データソース > オープン/修正された脆弱性 **Tenable.sc** > 変換.

ソースフィールド	ターゲットフィールド	説明
u_pluginID	Id	プラグインの識別子として使用されます。このフィールドは、サードパーティのエントリーレコードの plugin Id にマッピングされます。
u_riskfactor	source_severity	このフィールドは、サードパーティのエントリーレコードの source_severity にマッピングされます。
u_severity	priority	priority フィールドは重大度にマッピングされます。デフォルト値は 5 です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ソースフィールド	ターゲットフィールド	説明
u_hasbeenmitigated	state	hasbeenmitigated は、脆弱性レコードの [ステータス (State)] フィールドにマッピングされます。修正された脆弱性統合では、すべての VI が [クローズ済み] ステータスになっています。
u_ip	ip_address	IP アドレスは、cmdb_ci テーブルの host ip フィールドにマッピングされます。
u_port	port	ポートは、脆弱性一致アイテムレコードの port フィールドにマッピングされます。
u_protocol	protocol	プロトコルは、脆弱性一致アイテムレコードの port フィールドにマッピングされます。
u_firstSeen	first_found	初回検出値は、VI レコードの first_found フィールドにマッピングされます。
u_lastSeen	last_found	前回検出値は、VI レコードの last_found フィールドにマッピングされます。
u_exploitAvailable	exploit	exploitAvailable は、サードパーティのエントリーレコードの exploit フィールドにマッピングされます。
u_synopsis	threat	概要は、サードパーティのエントリーレコードの threat フィールドにマッピングされます。
u_description	summary	説明は、サードパーティのエントリーレコードの summary フィールドにマッピングされます。
u_solution	solution	ソリューションは、サードパーティのエントリーレコードの solution フィールドにマッピングされます。
u_basescore	score	baseScore は、サードパーティのエントリーレコードの score フィー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
		ルドにマッピングされます。
u_temporalScore	temporal_score	一時スコアは、サードパーティのエントリーレコードの一時スコアにマッピングされます。
u_cvssv3basescore	v3_base_score	cvssv3basescore は、サードパーティのエントリーレコードの v3_base_score にマッピングされます。
u_cvsstemporalscore	v3_temporal_score	cvssv3temporal スコアは、サードパーティのエントリーレコードの v3_temporal_score にマッピングされます。
u_pluginpubdate	date_published	プラグイン公開日は、サードパーティのエントリーレコードのプラグイン公開日にマッピングされます。
u_pluginmoddate	last_modified	最終変更日は、サードパーティのエントリーレコードのプラグインの最終変更日にマッピングされます。
u_dnsname	fqdn	dnsName は cmdb_ci レコードの FQDN フィールドにマッピングされます。
u_macaddress	mac_address	macAddress は cmdb_ci レコードの mac_address フィールドにマッピングされます。
u_netbiosName	netbios	netbiosName は、cmdb_ci レコードの NETBIOS フィールドにマッピングされます。
u_ip	ip	IP は cmdb_ci レコードの IP フィールドにマッピングされます。
hostUniqueness	uuid	ホストの一意性はどのフィールドにもマッピングされませんが、ホストの uuid を決定するために使用されます。
u_family	category	プラグインのファミリオブジェクトの name

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
		フィールドをサードパーティのエントリーレコードの category 列にマッピングします。
u_plugintext	proof	プラグインテキストは tpe レコードの proof にマッピングされます。
[script]	source	統合のソースが入力されます。この統合から作成された脆弱性一致アイテムには、Tenable.sc がソースとして含まれています。
[script}	integration_instance	integration_instance は、脆弱性一致アイテムのインポート元のインスタンスの名前です。
u_vpr_score	source_risk_score	スキャナーからの VPR スコアをサードパーティのエントリーテーブルのソースリスクスコアにマッピングします。
[script]	source_risk_rating	スコア範囲に基づいて、vpr スコアを標準リスク評価にマッピングします。 • 9 ～ 10 - 重大 • 7 ～ 9 – 高 • 4 ～ 7 - 中 • 0 ～ 4 - 低
u_vpr_context[id=age_of_vuln]	age_of_vuln	スキャナーからの脆弱性の経過時間をサードパーティのエントリーテーブルの age_of_vuln にマッピングします。
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	スキャナーからのエクスプロイトコードの成熟度をサードパーティのエントリーテーブルの exploit_code_maturity にマッピングします。
u_vpr_context[id=product_coverage]	product_coverage	スキャナーからの製品範囲をサードパーティのエントリーテーブルの product_coverage にマッピングします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	ターゲットフィールド	説明
u_vpr_context[id="threat_sources_last_28]	threat_sources	スキャナーからの過去 28 日間の脅威ソースをサードパーティテーブルの threat_sources にマッピングします。
u_vpr_context[id="threat_intensity_last_28]	threat_intensity	スキャナーからの過去 28 日間の脅威の強さをサードパーティのエントリーテーブルの threat_intensity にマッピングします。
u_vpr_context[id="threat_recency"]	threat_recency	スキャナーからの脅威の最新性情報をサードパーティのエントリーテーブルの threat_recency にマッピングします。
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	スキャナーからの CVSS v3 影響スコアをサードパーティのエントリーテーブルの v3_impact_subscore にマッピングします。
u_pluginname	name	プラグインの名前をサードパーティのエントリーテーブルの name 列にマッピングします。
u_stigseverity	stig_severity	プラグインの stig_severity フィールドをサードパーティのエントリーテーブルの stig_severity にマッピングします。
u_checktype	check_type	チェックタイプをサードパーティのエントリーテーブルの check_type にマッピングします。
u_family.id	family_id	プラグインの family.id をサードパーティのエントリーテーブルの family_id にマッピングします。
[script]	exploit_attack_vector	third_party_entry テーブルの exploit_attack_vector 列は、列の exploit_available と v3_attack_vector に基づいて入力されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースフィールド	説明
u_cve	CVE 関連データを参照テーブル (sn_vul_nvd_entry) に挿入します。NVD エントリーテーブル (sn_vul_nvd_entry) で同じ CVE が見つかった場合、現在の脆弱性が NVD エントリーに関連付けられます。マッピングは sn_vul_m2m_entry_cve にあります。
u_bid	バグトラックのリストが参照として追加されます。
u_cpe	CPE のリストが参照として追加されます。
u_seealso	URL のリストが参照として追加されます。
u_xrefs	X-REF のリストが参照として追加されます。
u_exploitframeworks	そのプラグインのエクスプロイトのリスト。該当するエクスプロイトフレームワークとプラグインの sn_vul_m2m_framework_vul へのマッピングを挿入します。

変換プロセスでは、3 つの変換スクリプトが実行されます。次の表に、各スクリプトが実行されるタイミングとその目的を示します。

スクリプトが実行されるタイミング	目的
onStart (インポートセットが変換を開始したとき)	この変換は、統合プロセスの import_set の値を初期化するために使用されます。内部使用。変更または削除することはお勧めしません。
onBefore (インポートセットの変換が完了する前)。	脆弱性の値を更新し、脆弱性が既に存在するかどうかを確認するために使用される機能。結果に基づいて、脆弱性一致アイテムテーブルの値を変更します。内部使用。変更または削除することはお勧めしません。
onComplete (インポートセットが変換を完了したとき)	この変換は、作成された新しい VI と更新されて無視された VI の値を設定するために使用されます。内部使用。変更または削除することはお勧めしません。

Tenable.io インポートの追加のフィルターパラメーターの設定

Tenable 脆弱性統合 を使用してスケジュール設定済みクエリのフィルタリングパラメーターをカスタマイズすると、Tenable.io 製品でインポートする脆弱性データをさらに絞り込むことができます。

始める前に

ユースケース：脆弱性マネージャーまたはアナリストは、特定の脆弱性の詳細のみを確認できるように、クエリからデータを除外できます。たとえば、`cidr_range`、`num_assets`、`indexed_at`、および `plugin_family` でフィルタリングされたインポート済み脆弱性を表示するとします。または、1 つは重大な脆弱性のみを 4 時間ごとにインポートし、もう 1 つは重大でない他のすべての脆弱性を 24 時間ごとにフェッチするなど、Tenable.io 統合を実行するとします。

このデータを収集するには、Tenable サポートのパラメーターを追加して、必要な特定の脆弱性の詳細をインポートします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

この機能を使用すると、API コールを追加したり追加のコーディングをしたりすることなく、Now Platform の Tenable パラメーターを使用して HTTP 要求情報をカスタマイズできます。次の Tenable.io 統合は、要求本文に JSON コンテンツを指定することによってフィルタリングをサポートしています。

- 資産統合
- 修正された脆弱性統合
- オープンな脆弱性統合

この機能の JSON 文字列の使用方法を理解している必要があります。

必要なロール：sn_vul.vulnerability_admin

手順

1. フィルタリングに使用する開発者サイトで、Tenable.io 製品でサポートされているパラメーターを見つけます。

   Tenable.io 製品から入力するパラメーターと値は、統合インスタンスレベルでのみサポートされます。

2. 次のように移動する。 **All** (すべて) > **Tenable** 脆弱性統合 > アドミニストレーション > 統合.
3. [Tenable 統合] リストページで、開く Tenable.io 統合のレコードをクリックします。
4. [Tenable REST メソッド (Tenable REST methods)] タブを選択した状態で、REST メソッドの情報アイコン (ⓘ) を見つけてクリックし、続いて [レコードを開く] をクリックします。
5. **[HTTP** 要求] タブを選択します。
6. レコードを編集するには、ページの上部にあるリンクをクリックします。レコードを編集するには、[ここ] をクリックします。
7. [コンテンツ] フィールドの REST メソッドレコードで、要求本文の一部として必要な JSON コンテンツを入力します。

   たとえば、インポートされた脆弱性の重大度パラメーターを Tenable.io 資産統合の重大度パラメーターを `{"filters": {"severity": ["critical"]}}` に設定すると、重大な脆弱性 (CVSS スコア 10.0) のみがインポートされます。

   複数のパラメーターを入力する場合は、各値を区切る方法の詳細について、Tenable.io ドキュメントを参照してください。

8. [更新] をクリックします。

Tenable 脆弱性統合レポート

脆弱性対応 ダッシュボードで脆弱性と脆弱性一致アイテムに関するレポートを表示します。

脆弱性対応 のワークスペースのデータの可視化

脆弱性対応 ワークスペースには、修復の進捗状況を監視するのに役立つデータの可視化が含まれています。脆弱性データの変更に応じて更新される動的なデータ表示で組織にとって重要なアクティブな脆弱性の数と重大度を表示することで、組織に対する脅威のレベルを判断できます。利用可能な動的なデータ表示方法の詳細については、「脆弱性対応 ワークスペース」、「Vulnerability Manager ワークスペース の探索」および「IT 修復ワークスペース の探索」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性対応 の前のバージョン

脆弱性対応概要ダッシュボード (脆弱性管理) では、脆弱性と脆弱性一致アイテムに関するエグゼクティブビューが用意されており、脆弱性アドミニストレーターが懸念事項をすばやく特定するのに役立ちます。脆弱性対応修復ダッシュボード (脆弱性修復) を使用すると、修復スペシャリストが担当するする修復タスクと脆弱性一致アイテムに集中できます。

詳細については、「デフォルトの 脆弱性対応 ダッシュボードを使用する」を参照してください。

必要なロール：修復オーナー

脆弱性対応アプリケーションでユーザーが実行および表示できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。

詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

ダッシュボードを表示するには、次に移動します: 脆弱性対応 > 修復の概要.

Tenable 脆弱性統合の統合実行状況チャート

[Tenable 統合実行状況] モジュールは、Tenable 統合実行のステータスをグラフィカルに表示します。

チャートで、グラフの任意の部分をポイントすると、その部分に固有のデータの概要が表示されます。棒グラフの任意の部分をクリックすると、より詳細な情報を提供するリストが開きます。

必要なロール：脆弱性管理者

脆弱性対応アプリケーションでユーザーが実行および表示できることを管理できるように、ペルソナと詳細ルールが用意されています。セットアップアシスタントでのペルソナロールの初期アサインについては、「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。

詳細なロール管理の詳細については、「脆弱性対応 のペルソナと詳細ロールの管理」を参照してください。

データを表示するには、次に移動します: **All** (すべて) > **Tenable** 脆弱性統合 > 統合実行ステータス.

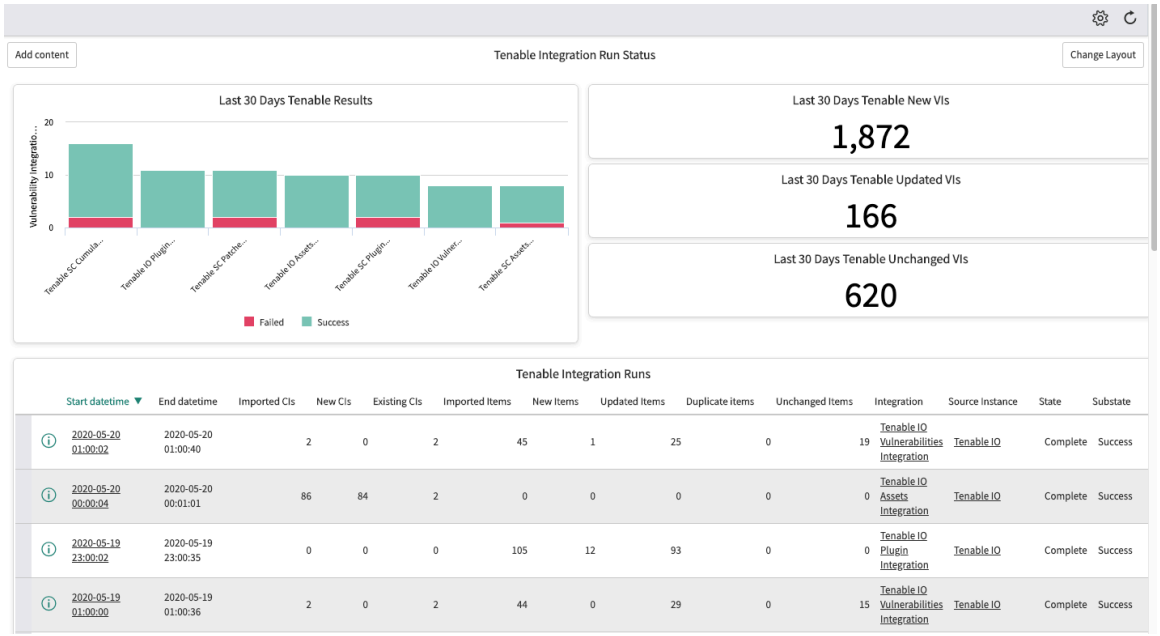
脆弱性対応 のバージョン 19.0 以降では、このダッシュボードは New Experience UI で使用可能です。

> **注:**
> Tokyo を使用している場合は、Next Experience UI でダッシュボードを表示できますが、一部の機能が失われます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

実行ステータス



Tenable 統合実行状況チャートレポート

名前	説明
過去 30 日間の Tenable 結果	各統合で完了した統合実行の数。成功した実行と失敗した実行の両方が表示されます。各実行は棒グラフで表示されます。
過去 30 日間の Tenable 新規 VI	過去 30 日間にインポートされた新規脆弱性一致アイテムの数。整数として表示されます。
過去 30 日間の Tenable 更新済み VI	過去 30 日間にインポートされた更新済み脆弱性一致アイテムの数。整数として表示されます。
過去 30 日間の Tenable 未変更 VI	過去 30 日間にインポートされた重複脆弱性一致アイテムの数。整数として表示されます。
Tenable 統合実行	リストの統合実行レコード **注:** V16.1：この統合の検出を検証するには、検出または検出結果を *sn_vul_detection* テーブルの ServiceNow 検出データと比較します。 統合の進行中は、検出数または検出結果数が変更される可能性があります。このレポートでは、統合実行の完了後に、インスタンスの [現在までの数] 列に検出数が表示されます。

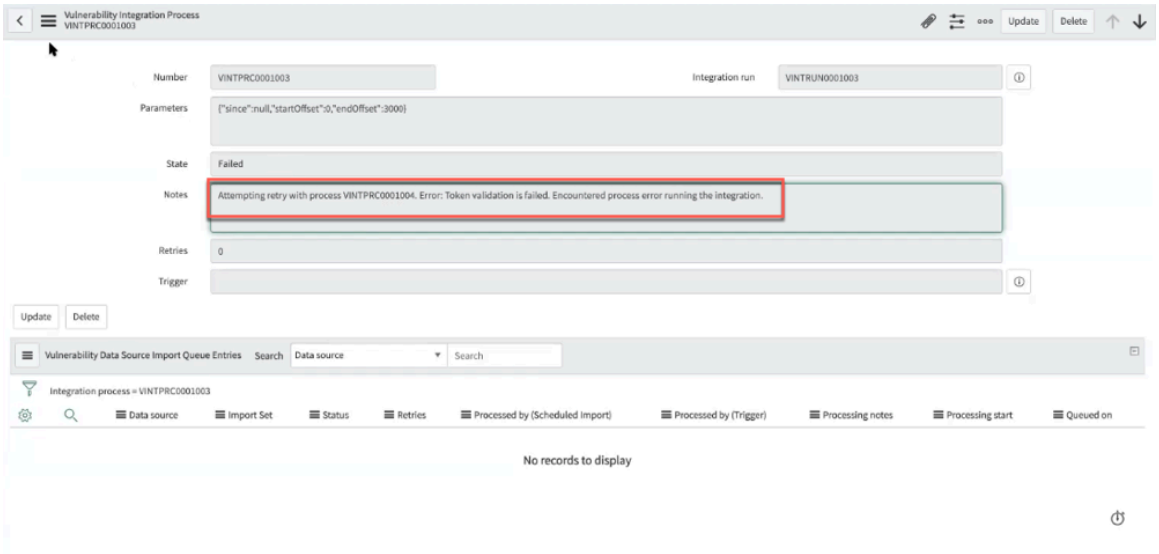
トークン検証の有効期限

何らかの理由で Tenable.sc 統合の実行に失敗した場合、Tenable.sc の認証トークンは自動的に期限切れになり、脆弱性統合プロセスレコードにメッセージが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

期限切れのトークンメッセージ



次の統合プロセス用に新しいトークンが自動的に生成されます。すべての統合プロセス (失敗および成功) は、脆弱性統合プロセスレコードの [脆弱性統合プロセス] タブに表示されます。

Tenable.sc 統合の再スキャンの開始

Tenable プラットフォームで再スキャンを開始し、スケジュールされたスキャンサイクル間で脆弱性一致アイテムが修正されたことを確認します。Now Platform® インスタンスから Tenable.sc 製品の脆弱性一致アイテムの再スキャンをオンデマンドで開始できます。

始める前に

必要なロール：sn_vul.write_all または sn_vul.write_assigned

注:
Tenable.sc は、エージェントベースのマシンでの再スキャンの開始をサポートしていません。

開始する前に、スキャナーがアクティブ化されていることを確認します。次のように移動する。 脆弱性対応 > 脆弱性スキャン > スキャナー.

このタスクについて

ワークスペースから再スキャンを開始するには、「脆弱性対応 ワークスペースからの Tenable.io および Tenable.sc 脆弱性一致アイテムの再スキャン」を参照してください。

クラシック環境で再スキャンを開始するには、以下の手順に従います。

修復オーナー、IT スペシャリスト、脆弱性アナリスト、または脆弱性マネージャーは、スケジュール設定済みのフルスキャンに関連するオーバーヘッドとボリュームを削減するために、環境内の資産 (構成アイテム) の特定の脆弱性についてターゲットの再スキャンをオンデマンドで開始できます。脆弱性一致アイテム (VI)、修復タスク (RT)、サードパーティエントリー (TPE)、または Now Platform インスタンスから検出されたアイテムレコードから再スキャンを開始できます。

再スキャンにより、修復アクティビティ、パッチ、およびその他のアクションによって構成アイテム (CI) の特定の脆弱性が正常に修正されたことを修復オーナーおよび脆弱性アナリストが確認できます。

たとえば、3 週間に 1 回環境全体をスキャンするとします。最新のフルスキャンは 1 週間前に完了しましたが、重大な脆弱性を修正するために昨日パッチを適用しました。この脆弱性の特性を考えると、この脆弱性が修正されたことを確認するのに次のスケジュール済みスキャンまで 2 週間待つことはできません。以前のスキャン中に検出された重大な脆弱性がパッチによって正常に修正されたことを確認するために、Now Platform for Tenable.sc 脆弱性一致アイテムからターゲット再スキャンを開始できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
Now Platform® インスタンスから再スキャンを要求する場合、Vulnerability Response Integration with Tenable 認証情報の選択はオプションです。ServiceNow® Tenable.sc スキャン認証情報統合は、インスタンスの Tenable.sc 製品からスキャナー認証情報をインポートして更新します。この統合は毎週実行され、Tenable 認証情報データをインポートして安全に保存します。

このインポートされたデータには、Tenable パスワードやその他の機密性の高い Tenable アカウント情報は含まれません。Tenable.sc 脆弱性統合 (Tenable.sc のオープンな脆弱性統合および修正された脆弱性統合) を構成すると、インスタンスのセットアップアシスタント内から ServiceNow® Tenable.sc スキャン認証情報統合が自動的に有効 ([アクティブ]) になります。

ユーザーが必要に応じて Now Platform インスタンスから表示できるように、インポートする認証情報に関する次の情報に注意してください。

- Tenable.sc アドミンユーザーロールで作成された認証情報は、すべての組織のユーザーが使用できます。
- Tenable.sc 組織ユーザーロールで作成された認証情報は、その組織内のユーザーのみが使用できます。これらの認証情報は、インスタンスへの接続に使用されているユーザーのアカウントと共有されない限り、作成者の組織外のユーザーの Now Platform にはインポートされません。

詳細については、Tenable.sc のドキュメントを参照してください。

Tenable.sc アプリケーションの構成の詳細については、「セットアップアシスタントを使用した Tenable 脆弱性統合の構成」を参照してください。スキャン認証情報統合の詳細を表示するには、次に移動します: **All** (すべて) > **Tenable** 脆弱性統合 > 統合 > **Tenable.sc** スキャン認証情報統合.

統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロードサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、 脆弱性対応のバージョン 18.2.4 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム.
2. 再スキャンをトリガーする脆弱性一致アイテムレコードを見つけて開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

> **注:**
> ソースが Tenable.sc の VI の再スキャンのみを開始できます。VI リストビューの [ソース] 列、または個々のレコードの [ソース] フィールドに Tenable.sc が表示されていることを確認します。条件ビルダーを使用して、VI をソース別にグループ化できます。または、[ソース] 列が VI リストビューに表示されていない場合は、リストの左上にある [リストをカスタマイズ] アイコン (歯車アイコン) をクリックし、スラッシュバケットを使用して [ソース] を [利用可能] から [選択済み] に移動します。

3. または、 **All** (すべて) > 脆弱性対応 > 修復タスク または 脆弱性対応 > ライブラリー > サードパーティ は、それぞれ再スキャンに使用する修復タスクまたはサードパーティのエントリーレコード用です。

   選択内容に応じて、次のレコードで [再スキャン] ボタンを使用できます。

   - 単一の VI レコードでは、VI のソースが Tenable.sc 製品で、[クローズ済み] 以外のステータスである必要があります。複数の VI レコードの場合、すべての VI のソースが Tenable.sc 製品で、[クローズ済み] 以外のステータスである必要があります。
   - RT レコードでは、修復タスクは [クローズ済み] を除くあらゆるステータスをとることが可能ですが、関連する VI はすべてソースが Tenable.sc 製品である必要があります。
   - サードパーティエントリー (TPE) レコードには、[クローズ済み] 以外のステータスでソースが Tenable.sc 製品の関連する VI レコードが少なくとも 1 つ必要です。

4. レコードの右上にある [再スキャン] をクリックします。
   スキャナーにアクセスするためのスキャナー認証情報を選択するように求められます。これらは、Tenable.sc スキャン認証情報統合によってインポートされた認証情報です。
5. ダイアログで、必要なフィルターと認証情報タイプを選択します。
6. [スキャンの要求 **(Request Scan)]** をクリックします。

   スキャンが処理されていることを示すメッセージが表示されます。すべての再スキャンのステータスは、再スキャンの開始に使用した VI、RT、および TPE レコードの [スキャン] 関連リストでいつでも確認できます。メッセージで [詳細を表示] をクリックして再スキャンのステータスを表示し、指定されたレコードから開始された他の再スキャンを表示します。

   すべての子スキャンが正常に完了すると、親スキャンレコードの [ステータス (State)] フィールドが完了としてマークされます。子はインポートデータをスキャンします。親スキャンレコードは、子スキャンのコンテナです。

   Now Platform® インスタンスは、正常に完了するか設定された追跡期間がタイムアウトするまで、再スキャンステータスを追跡します。 タイムアウトしてもスキャンは停止しません。タイムアウトは、実際の再スキャンが停止したときではなく、Now Platform® が再スキャンステータスの追跡を停止したときです。[クローズ済み]/[修正済み] に移行した、または移行する予定のすべての VI は、Tenable.sc の修正された脆弱性統合の次のスケジュール済みインポートとともにインポートされます。

Tenable.io 統合の再スキャンの開始

Tenable プラットフォームで再スキャンを開始し、スケジュールされたスキャンサイクル間で脆弱性一致アイテムが修正されたことを確認します。Now Platform® インスタンスから Tenable.io 製品の脆弱性一致アイテムの再スキャンをオンデマンドで開始できます。

始める前に

必要なロール：sn_vul.write_all または sn_vul.write_assigned

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

開始する前に、スキャナーがアクティブ化されていることを確認します。次のように移動する。 脆弱性対応 > 脆弱性スキャン > スキャナー.

このタスクについて

- 脆弱性対応ワークスペースから再スキャンを開始するには、「でのレコードと修復タスクの再スキャン Vulnerability Manager ワークスペース」および「IT 修復ワークスペースでの脆弱性一致アイテムと修復タスクの再スキャン」を参照してください。
- クラシック環境で再スキャンを開始するには、以下の手順に従います。

注:
Tenable.io は、エージェントベースのマシンでの再スキャンの開始をサポートしていません。

修復オーナー、IT スペシャリスト、脆弱性アナリスト、または脆弱性マネージャーは、スケジュール設定済みのフルスキャンに関連するオーバーヘッドとボリュームを削減するために、環境内の資産 (構成アイテム) の特定の脆弱性についてターゲットの再スキャンをオンデマンドで開始できます。脆弱性一致アイテム (VI)、修復タスク (RT)、サードパーティエントリー (TPE)、または Now Platform インスタンスから検出されたアイテム (SDI) レコードから再スキャンを開始できます。再スキャンにより、修復アクティビティ、パッチ、およびその他のアクションによって構成アイテム (CI) の特定の脆弱性が正常に修正されたことを確認できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注: Now Platform® インスタンスから再スキャンを要求する場合、Vulnerability Response Integration with Tenable 認証情報の選択はオプションです。ServiceNow® Tenable.io スキャン認証情報統合は、インスタンスの Tenable.io 製品からスキャナー認証情報をインポートして更新します。この統合は毎週実行され、Tenable 認証情報データをインポートして安全に保存します。

このインポートされたデータには、Tenable パスワードやその他の機密性の高い Tenable アカウント情報は含まれません。

次の情報では、ユーザーが必要に応じて Now Platform インスタンスから表示できるように、インポートする認証情報について説明しています。

- Tenable.io アドミンユーザーロールで作成された認証情報は、すべての組織のユーザーが使用できます。
- Tenable.io 組織ユーザーロールで作成された認証情報は、その組織内のユーザーのみが使用できます。これらの認証情報は、インスタンスへの接続に使用されているユーザーのアカウントと共有されない限り、作成者の組織外のユーザーの Now Platform にはインポートされません。

  詳細については、Tenable.io のドキュメントを参照してください。

- 再スキャンを開始する前に、Tenable.io テンプレート統合と Tenable.io スキャン認証情報統合をアクティブにする必要があります。スキャン認証情報統合の詳細を表示するには、次に移動します: **Tenable** 脆弱性統合 > 統合 > **Tenable.io** スキャン認証情報の統合.

  テンプレートとスキャンの認証情報統合はデフォルトで非アクティブになっています。Tenable.io の認証情報を入力すると、すべての Tenable.io 統合が自動的にアクティブになります。これらの統合を手動でアクティブまたは非アクティブにするには、次の手順を実行します。

  1. 次のように移動する。 **All** (すべて) > **Tenable** 脆弱性統合 > アドミニストレーション > 統合.
  2. 表示されるリストで、必要な Tenable.io 統合レコードを見つけます。
  3. 各レコードを開き、[アクティブ] チェックボックスをオンにして統合をアクティブ化します。
  4. [更新] をクリックして変更を保存します。
  5. セットアップアシスタントに戻り、脆弱性対応 で Tenable 脆弱性統合の構成を続行します。

Tenable.io および Tenable.sc 製品の構成の詳細については、「セットアップアシスタントを使用した Tenable 脆弱性統合の構成」を参照してください。

たとえば、3 週間に 1 回環境全体をスキャンするとします。最新のフルスキャンは 1 週間前に完了しましたが、重大な脆弱性を修正するために昨日パッチを適用しました。この脆弱性の特性を考えると、この脆弱性が修正されたことを確認するのに次のスケジュール済みスキャンまで 2 週間待つことはできません。以前のスキャン中に検出された重大な脆弱性がパッチによって正常に修正されたことを確認するために、Now Platform for Tenable.io 脆弱性一致アイテムからターゲット再スキャンを開始できます。

スキャンを開始したレコードの更新された結果は、修正された脆弱性統合の次のスケジュール設定済みのインポート後に表示できます。

統合の実行中に複数のプロセスが生成され、データがページの形式で受信されます。各プロセスには、ページ形式のデータが添付された 1 つ以上のインポートキューエントリを含めることができます。これらのエントリは、1 時間の制限時間内にデータを処理する必要があります。ただしペイロー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドサイズが大きい場合は、処理時間が 1 時間を超えることやスタックすることがあり、その結果統合タイムアウトエラーが発生する可能性があります。タイムアウトエラーが発生しても、統合はデータの処理を続行します。この通信ミスを回避するために、 脆弱性対応のバージョン 18.2.4 以降では、キューがアクティブでデータを処理しているかどうかを示すタイムスタンプ (ハートビート) が定期的に送信されます。[キューエントリをインポート] ページの [最後の処理済みレコード] フィールドは、インポートキューにより作成または更新されるレコードの数に基づいて更新されます。インポートキューエントリが 1 時間の時間制限を超えた場合、システムは **[Last Record Processed** (最後の処理済みレコード)] フィールドをチェックして、経過時間が 1 時間を超えているかどうかを確認します。1 時間を超えている場合は、インポートキューエントリがスタックしており、処理のさらなる遅延を防ぐためにタイムアウトしています。

注:
[最後の処理済みレコード] フィールドは、次のシステムプロパティの定義に基づいて更新されます。

- *sn_sec_cmn.record_threshold_heartbeat*：処理されたレコードの数を定義します。これ以降、ハートビート (タイムスタンプ) がインポートキューエントリに送信されます。
- *sn_sec_cmn.maximum_heartbeat_delay*：インポートキューエントリがタイムアウトするまでの経過時間を定義します。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテム.
2. 再スキャンをトリガーする脆弱性一致アイテムレコードを見つけて開きます。

   注:
   Tenable.io スキャナーを使用している場合は、ソースが Tenable.io の VI の再スキャンのみを開始できます。VI リストビューの [ソース] 列、または個々のレコードの [ソース] フィールドに Tenable.io が表示されていることを確認します。条件ビルダーを使用して、VI をソース別にグループ化できます。または、[ソース] 列が VI リストビューに表示されていない場合は、リストの左上にある [リストをカスタマイズ] アイコン (歯車アイコン) をクリックし、スラッシュバケットを使用して [ソース] を [利用可能] から [選択済み] に移動します。

3. または、 **All** (すべて) > 脆弱性対応 > 修復タスク または 脆弱性対応 > ライブラリー > サードパーティ 再スキャンに使用するレコード用。

   選択内容に応じて、次のレコードで [再スキャン] ボタンを使用できます。

   - 単一の VI レコードでは、VI が [クローズ済み] 以外のステータスである必要があります。複数の VI レコードの場合、すべての VI のソースが Tenable.io 製品で、[クローズ済み] 以外のステータスである必要があります。
   - 修復タスクレコードの場合、[クローズ済み] 以外のステータスの修復タスクのみがサポートされます。関連するすべての VI は [クローズ済み] 以外のステータスで、ソースとして Tenable.io を使用する必要があります。
   - サードパーティエントリー (TPE) レコードには、[クローズ済み] 以外のステータスでソースが Tenable.io 製品の関連する VI レコードが少なくとも 1 つ必要です。
   - [検出されたアイテム] レコードには、[クローズ済み] 以外のステータスの Tenable.io 製品の関連する VI レコードが少なくとも 1 つ必要です。
   - [脆弱性一致アイテム] リストから、再スキャンする個々の脆弱性一致アイテムを選択できます。画面の左下にある [選択した行のアクション] メニューを使用して、再スキャンを開始します。認証情報を入力するように求められます。

4. レコードの右上にある [再スキャン] をクリックします。

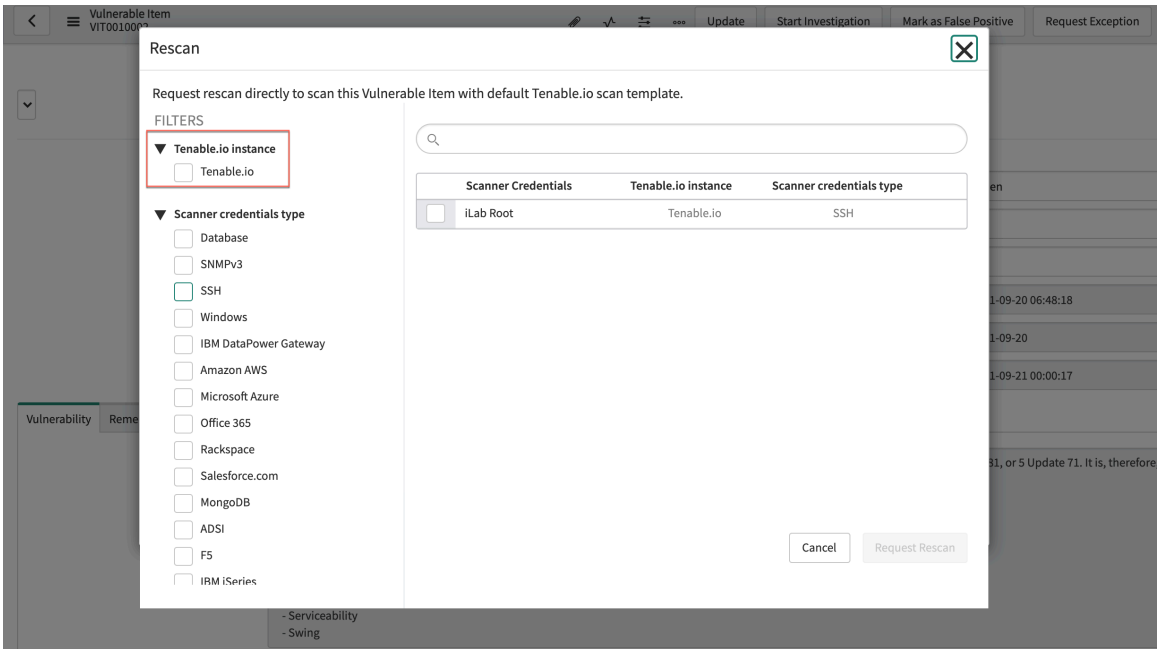
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

再スキャンのインスタンスとスキャナーへのアクセスに使用するスキャナー認証情報を選択するように求められます。表示される認証情報は、Tenable.io スキャン認証情報統合によってインポートされた認証情報です。

5. ダイアログで、使用するインスタンス (1 つまたは複数) と認証情報タイプを選択します。

次の画像では、1 つの統合インスタンス Tenable.io が表示されています。複数の Tenable.io インスタンスがある場合、それらはすべてフォームの [Tenable.io] セクションに表示されます。



6. [再スキャンを要求] をクリックします。

スキャンが処理されていることを示すメッセージが表示され、親スキャンレコードが作成されます。すべての子スキャンのステータスは、再スキャンの開始に使用した VI、修復タスク、TPE、および SDI レコードの [スキャン] 関連リストでいつでも確認できます。メッセージで [詳細を表示] をクリックして再スキャンのステータスを表示し、指定されたレコードから開始された他の再スキャンを表示します。

すべての子スキャンが正常に完了すると、親スキャンレコードの [ステータス (State)] フィールドが完了としてマークされます。子はインポートデータをスキャンします。各スキャンは、統合インスタンス、TPE、IP、およびネットワーク ID の一意の組み合わせをサポートしています。親スキャンレコードに複数の子スキャンが表示される場合があります。たとえば、子スキャンでサポートできる IP アドレスの最大数は 1000 です。脆弱性一致アイテムに 1002 個の IP がある場合、要求をサポートするために 2 つの子スキャンが作成され、[スキャン] 関連リストに一覧表示されます。親スキャンレコードは子スキャンのコンテナであり、そのステータスは子スキャンのステータスを反映します。

Now Platform® インスタンスは、正常に完了するか設定された追跡期間がタイムアウトするまで、再スキャンステータスを追跡します。 タイムアウトしてもスキャンは停止しません。タイムアウトは、実際の再スキャンが停止したときではなく、Now Platform® が再スキャンステータスの追跡を停止したときです。[クローズ済み]/[修正済み] に移行した、または移行する予定のすべての VI は、Tenable.io の修正された脆弱性統合の次のスケジュール済みインポートとともにインポートされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エラーが発生したスキャンについては、親スキャンレコードで子スキャンを確認できます。子スキャンの応答ペイロードのエラーを表示します。

スキャンを開始したレコードの更新された結果は、修正された脆弱性統合の次のスケジュール設定済みのインポート後に表示できます。

Tenable 脆弱性統合 のネットワークパーティション識別子で構成アイテムを更新する

IP アドレスを共有する環境内の資産に対して、一意の構成アイテム (CI) を作成します。環境全体で個別の資産を特定し、検出された既存のアイテム、脆弱性一致アイテム、および検出レコードで CI を自動的に更新して、脆弱性に関する詳細を提供します。

始める前に
必要なロール：admin

このタスクについて
デフォルトでは、脆弱性対応 アプリケーションで資産を識別する方法の 1 つは IP アドレスです。場合によっては、資産は IP アドレスを共有できますが、それらは 1 つの CI として CMDB に保存されます。

たとえば、次の表に示すように、環境内の複数の資産 (CI) が IP アドレスを共有できますが、ネットワークとリポジトリの ID は一意です。ただし、デフォルトでは、これらの資産は通常、IP アドレスのルックアップ中に単一の CI（CI 1）として識別され、保存されます。

デフォルトの **IP** ルックアップと **CI** の作成

ソース	IP アドレス	Network_id	構成アイテム
Tenable.io：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

ソース	IP アドレス	Repository_id	構成アイテム
Tenable.sc：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

同じ IP アドレスを持つ資産に対して個別の CI を作成して、それらを個別の資産として識別できるようにすることができます。新規のデータのインポートから開始し、スケジュール済みジョブ *`Update existing discovered items with network partition identifier`* を実行することで、ネットワークパーティション識別子 [network_partition_identifier] を含む既存の CI をより細かく更新できます。

このスケジュール済みジョブは、デフォルトでは非アクティブです。セットアップアシスタントで Tenable.io と Tenable.sc 製品の資産と修正済みおよびオープンな脆弱性の統合に対してこの機能をアクティブ化して、この識別子をレコードに表示します。

このスケジュール済みジョブを有効にすると、インポートされたデータから既存の CI レコードにネットワークパーティション識別子 [network_partition_identifier] が追加されます。IRE によって作成された既存の CI も更新されます。スケジュール済みジョブは、次のインポートから始まるネッ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

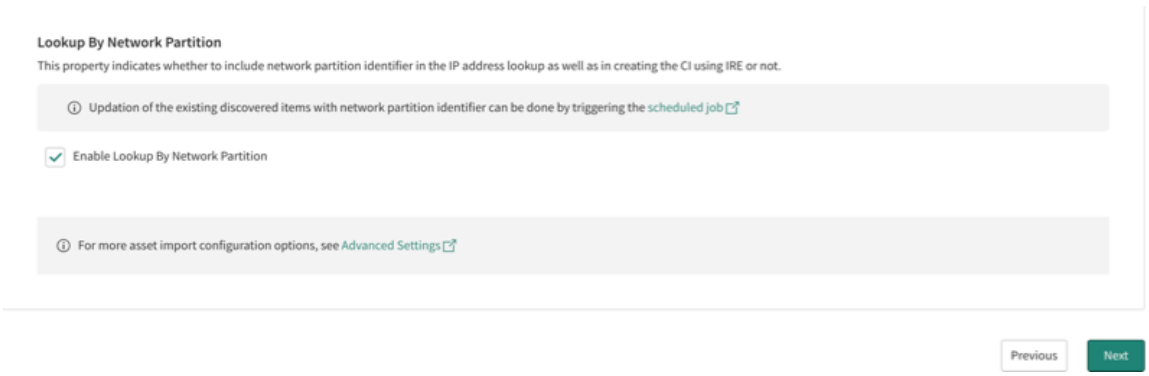
トワークパーティション識別子を含む CI も作成します。または、オンデマンドでジョブを開始して既存のデータを更新することもできます。

脆弱性対応 の v14.0 および Tenable 脆弱性統合の v12.1 以降、アップグレード時に CMDB CI クラスモデル (1.0.21.) がサポートされています。クラスモデルでは、識別および調整 (IRE) 識別ルールにネットワークパーティション識別子 [network_partition_identifier] があります。

オプション	説明
スケジュール済みジョブをオンデマンドで実行します。	検出された既存のアイテムを更新します。既存の Tenable データの CI は、ネットワークパーティション識別子の粒度を含むように作成または更新されます。検出されたアイテム、脆弱性一致アイテム、および検出レコードはすべて新しい CI で更新されます。
次のスケジュール済みジョブとの統合からの新しいデータのインポートを待機します。	次のスケジュール済みジョブから始まるネットワークパーティション識別子を使用して、新しい資産ごとに CI を作成します。CI、脆弱性一致アイテム、および検出レコードはすべて、新しい粒度を含むように更新されます。完全一致が見つからない場合は、新しい CI が作成されます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > セットアップアシスタント > 統合設定 > スキャナー統合.
2. Tenable.io 統合または Tenable.sc 統合を選択します。
3. 必要な統合を編集します。
4. 選択 資産インポート構成.
5. 選択 ネットワークパーティションによるルックアップを有効化 のチェックボックス ネットワークパーティションによるルックアップを有効化 節。



6. [次へ] をクリックします。

   ネットワークパーティション識別子 NETWORK_ID および REPOSITORY _ID が含まれており、既存の CI を更新するか、次のスケジュール済みジョブで CI を作成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

IP ルックアップと **CI** の作成に含まれるネットワークパーティション識別子属性

ソース	**IP** アドレス	**NETWORK_ID**	ネットワークパーティション識別子のない資産の **CI**	ネットワークパーティション識別子のある **CI** 資産
Tenable.io：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

ソース	**IP** アドレス	**REPOSITORY_ID**	ネットワークパーティション識別子のない資産の **CI**	ネットワークパーティション識別子のある **CI** 資産
Tenable.sc：資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

次のスケジュール済みジョブでは、Tenable.io および Tenable.sc 製品の資産脆弱性統合、修正された脆弱性統合およびオープンな脆弱性統合からデータをインポートできるように、IP アドレスおよび不完全な IP アドレス CI の識別ルックアップルールにネットワークパーティション識別子属性が自動的に含まれます。

システムのプロパティを有効にしてレコードを保存した後、スケジュール済みジョブをオンデマンドで起動して、ネットワークパーティション識別子を含む CI で検出された既存のアイテムを更新することもできます。

自動翻訳

Tenable 脆弱性統合のインポートの変更

ServiceNow® Tenable 脆弱性統合の Tenable 脆弱性インポート統合に特化したオプションの変更を構成し、一部のデータを簡素化します。

始める前に

必要なロール：sn_vul.vulnerability_admin

このタスクについて

この一連のタスクには、Now Platform に関するコーディングと高度な知識が必要です。

Tenable 脆弱性統合のドメインセパレーションインポートを作成するには、次の手順に従います。次の例は、Tenable.io のオープンな脆弱性統合用ですが、この内容は他の Tenable 統合にも適用できます。

手順

1. ドメインを作成します。
2. 作成するドメインごとに、ユーザーを作成してそのドメインにアサインします。

   このユーザーは、Tenable.io のドメインの run_as プレースホルダーと考えてください。

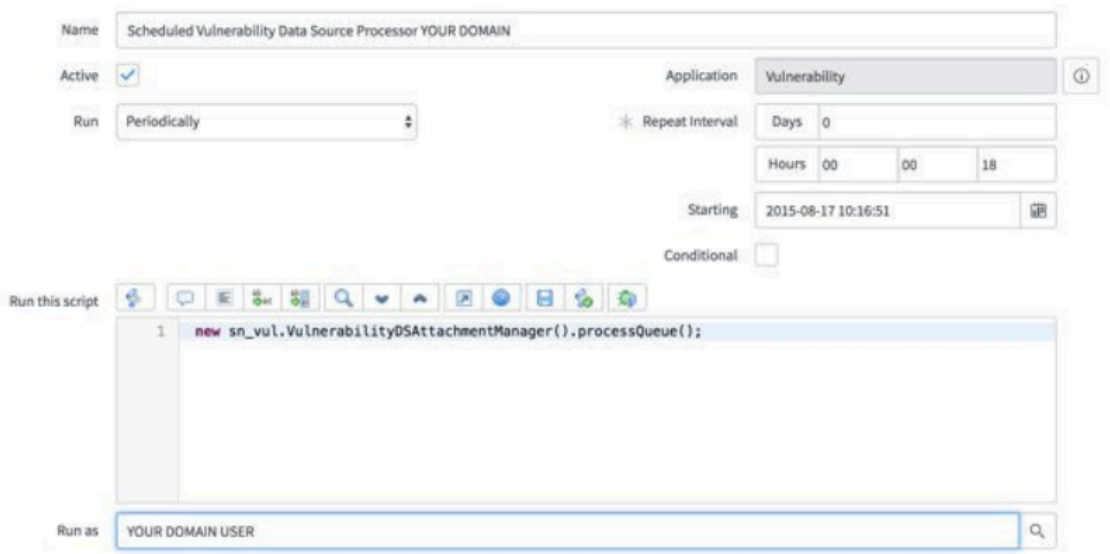
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 脆弱性統合を開きます。
   ユーザーは、グローバルドメイン内の VR.System ユーザーに相当し、ロール sn_vul.tenable_configure_integration、import_admin、および sn_vul.vulnerability_write が必要です。このユーザーには、データソース、変換マップおよび脆弱性データへのアクセスが必要です。

   注:
   このユーザーをこのロールに固有のものと見なします。ユーザーに他の目的はありません

4. 各ドメインで、[スケジュール設定済み脆弱性データソースプロセッサー] をコピーしてスケジュール済みジョブを作成します。 システム定義 > スケジュール済みジョブ.
5. スケジュール済みジョブを識別する名前にドメインを追加します。
6. run_as ユーザーを前のステップで作成したユーザーに変更します。

   注:
   次の UI アクションを編集して、統合が run_as ユーザードメインで実行されるようにします。



7. Tenable.io のオープンな脆弱性統合の [今すぐ実行] UI アクションを編集して、このコードブロックをファイルの先頭に追加します。
   `//sys id below is of Tenable.io integration if(current.sys_id == "4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID (); }`

   注:
   次のスクリプトインクルードを編集して、統合が run_as ユーザードメインで実行されるようにします。

8. VulnerabilityIntegrationUtils スクリプトインクルードメソッド addIntegrationRun を編集して、ハイライト表示されたコードを追加します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. VulnerabilityIntegrationUtils スクリプトインクルードのメソッド addProcessRun を編集して、ハイライト表示されたコードを追加します。

```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. DataSourceVulnReportRefreshProcessor スクリプトインクルード メソッド _processFromDataSourceGroups を編集して、元のコード _processFromDataSourcesGroups コードを Edited _processFromDataSourcesGroups コードに変更します。
11. VulnerabilityDSAttachmentManager スクリプトインクルードメソッドの queueItem を編集して、ハイライト表示されたコードブロックの queueItem、_getNext、_processQueueEntry 関数を追加します。

ドメインセパレーションされたホスト検出インポートの準備ができました。

インポート前に算出を無効にする

使用しない場合は、次の手順に従ってデフォルトの算出を無効にします。脆弱性算出を使用しない場合は、定義した他の脆弱性算出に加えて、デフォルトの算出を無効にすることをお勧めします。脆弱性算出は、脆弱性一致アイテムレコードにアクセスするたびに実行され、インスタンスのパフォーマンスに影響を与える可能性があります。

必要なロール：sn_vul.vulnerability_admin。

12. 次のように移動する。 **All** (すべて) > 脆弱性 > アドミニストレーション > 脆弱性の算出.
13. [脆弱性影響 (Vulnerability Impact)] グループを開きます。
14. スコアとサービスに基づく影響の算出を開きます。
15. [アクティブ] フィールドの選択を解除して、産出を非アクティブ化します。
16. [更新] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

デフォルトの算出を無効にしました。

最初のインポート前に通知ベースのビジネスルールを無効にします。

次の手順に従い、レコードの最初のインポート前に通知関連のビジネスルールを無効にします。レコードの最初のインポート中に、特定の通知関連のビジネスルールによって大量の通知が生成され、パフォーマンスが影響を受ける可能性があることを確認します。これらのビジネスルールは、インポート中に無効になるように変更する必要があります。

必要なロール：sn_vul.vulnerability_admin

17. 次のように移動する。 **All** (すべて) > システム定義 > ビジネスルール.
18. [影響を受ける CI 通知 (Affected ci notifications)] を検索します。
19. ビジネスルールを開き、条件「 `current.sys_class_name != "sn_vul_vulnerable_item"`」を挿入します。
20. [更新] をクリックします。
21. 次のビジネスルールについてこの手順を繰り返します。
    - 影響を受けるコストセンター通知
    - 影響を受けるグループ通知
    - 影響を受ける場所の通知

    注:
    最初のレコードのインポートが完了した後、これらのビジネスルールを再度有効にすることができます。ただし、無効にしておくことを検討してください。大量の通知が生成され、インスタンスのパフォーマンスに影響を与える可能性があります。

    最初の開始日の変更

    最初の開始日を変更するには、次の手順に従います。セットアップアシスタントを使用してインストール中に、Tenable 統合の最初の開始日を設定します。その開始日は、次のステップに示すように、セットアップアシスタントまたはプライマリ統合からリセットできます。
22. 次のように移動する。 **All** (すべて) > **Tenable** 脆弱性統合 > アドミニストレーション > 統合.
23. 統合をクリックします。
24. [統合の詳細] をクリックします。
25. [開始時間] フィールドを過去の値に設定すると、その時間以降にスキャンおよび検出されたすべての脆弱性が検出されます。

    セットアップアシスタントを使用して Tenable を構成した場合、[開始時間] フィールドには、最初に今日の日付の 3 か月前、その後は今日の日付が事前に入力されます。注意：過去最大 1 か月前の値を設定することを検討してください。これにより、大量のデータで Tenable API レート制限を超えることがなくなり、実行タイムアウトがトリガーされなくなります。
26. [送信] または [更新] をクリックします。
27. オプション: [今すぐ実行] をクリックして、今すぐ実行します。

脆弱性インスタンスに基づいて **Tenable** 検出を分割し、脆弱性一致アイテムを分割します

ServiceNow® 脆弱性対応では、Tenable スキャナーからの検出を分割して、検出された脆弱性インスタンスごとに一意の脆弱性一致アイテム (VIT) を作成できます。この分割により、VIT をさまざまな修復チームにアサインできるため、脆弱性の管理と追跡が強化されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：admin

このタスクについて
Tenable スキャナーのペイロードには検出データが含まれており、実証内の各パスが検出の分割に使用されます。ペイロードの出力タグは脆弱性の場所を識別し、特定のパスに従って脆弱性を正確に特定および管理を容易にします。

手順

1. サードパーティ統合テーブル [sn_sec_int_integration] で、Tenable.io と Tenable.sc の **[VI** キー列に証明を含める] の値を true に設定します。
2. 次のように移動する。 **All** (すべて) > 脆弱性対応 > アドミニストレーション > **VI** の粒度の構成.
3. [ポートを含める] フォームで、[ポートを含める] チェックボックスをオンにして、[ここをクリック] リンクを選択します。
4. [VI キーに証明を追加] リストで、[新規] を選択します。
5. [VI キー新規レコードに実証を追加 (Add proof to the VI key- New record)] フォームの [脆弱性] フィールドに、実証を含める Tenable ID を追加します。

   注:
   パス情報のみに基づいて、またはパスとバージョンの詳細を組み合わせて、検出を分割できます。詳細については、このページの「Tenable スキャナーからの検出の分割」セクションを参照してください。

6. **[Tenable VIT** を分割する正規表現] フィールドで、次の操作を行います。
   - パスのみに基づいて検出を分割するには、「パス\s+:\s+([A\n]+)」と入力します。
   - 「パス\s+:\s+([A\n]+)\n\s+Installed\s+version\s+:\s+([A\n]+)\n\s+Fixed\s+version\s+:\s+([A\n]+)」と入力して、パス、インストール済みバージョン、および修正済みバージョンに基づいて検出を分割します。
7. [**Submit** (送信)] を選択します。

Example: Tenable スキャナーからの検出の分割

Tenable スキャナーからの次の検出は、パスとバージョンの両方の情報を含む出力タグの証明を示しています。

```
"results":


        "asset":
            "agent_uuid": *92124caabdb9459baa9d053186df48b9",
           "bios_uuid": "ec2cbbfd-dc9e-efbf-acdd-485daZe8c7df"
           "device_ type": "aws-ec2-instance",
            "fqdn": "ip-ac0a0004. secops.com",
            "hostname": "ip-ac0a0004",
      "uuid": "486acb3b-674f-477a-bc37-660a7bba37b3",
            "ipv4": "18.220.145.158",
            "last_authenticated_results": "2024-05-17T03:34:04.424Z",

            "mac_address": "0a:3e:8b:ed:63:e6",
           "netbios name": "IP-AC0A0094".
           "operating_system": [
```

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

```
                    "Microsoft Windows Server 2019 Datacenter Build 17763"

                  "network_id": "00000000-0000-0000-0000-000000000008",

                "tracked": true

            "output": "In                    C: 11 Program Files (x86) \ \Common
Files\\0racle\\Java\\javapath_target_119044062511\n Installed version : 1.8.0_361.9\n Fixed
version
                                                                    Path
            "plugin":
                "bid":
                    123456

                "checks_for_default_account": false,
              "checks_for malware": false,

                "coe":
              "cpe:/a:notepad-plus-plus:notepad%5c%2b15ck2b"

                "cvSs3_base_score": 7.8,
              "cvss3 temporal score": 7.0,

              "cvss3_temporal_vector": {
                    "exploitability": "Proof-of-Concept",
                    "remediation level": "Official Fix",
                    "report_confidence": "Confirmed",
                    "raw": "E: P/RL:0/RC: C"
```


自動翻訳

コンフィグレーションコンプライアンス 修復

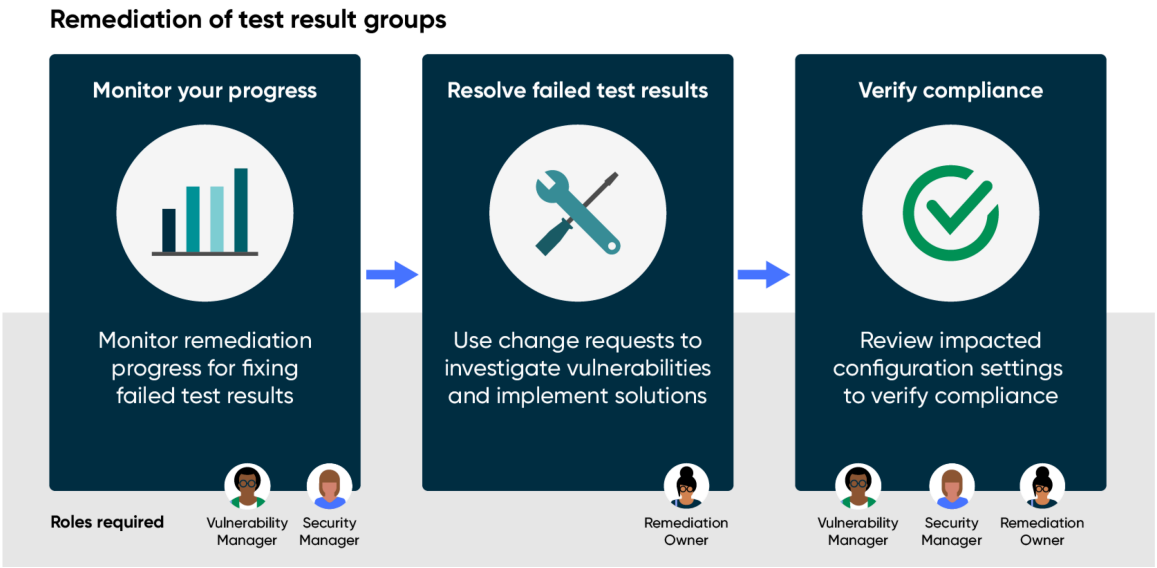
コンフィグレーションコンプライアンス 修復は主に、スケジュール済みジョブ (統合)、修復タスク、ワークフロー、変更要求によって拡大された手動的なプロセスとなります。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



個別のサードパーティ SCA プラグインが、コンフィグレーションコンプライアンスでデータを取得し、変換します。コンフィグレーションコンプライアンス を使用して構成アイテムを修復する前に、サードパーティのスキャナー統合をインストールし、少なくとも 1 回のネットワークスキャンを実行する必要があります。

修復タスクから個々のテストの失敗を修復するために、変更要求を使用します。

変更要求と修復タスク間のステータスの同期 により、関連する変更要求がライフサイクル全体を通じて変化すると、修復タスクのステータスは自動的に移行します。itil ロールを持つユーザーは、修復タスクから直接変更要求を作成、管理できます。

コンフィグレーションコンプライアンス修復タスクの手動作成

[修復タスク] モジュールから修復タスクを手動で作成し、修復を実行できます。

重要:
修復タスクは、次の方法で作成できます。

- Vulnerability Manager ワークスペース sn_vulc.admin ロールを持つユーザーとして。
- IT 修復ワークスペース sn_vulc.remediation_owner ロールを持つユーザーとして。

始める前に
必要なロール：sn_vulc.admin

このタスクについて
修復タスクルールを使用すると、[テスト結果] タブに自動入力されます。手動作成は、ルールや繰り返しが必要ない修復タスクに役立ちます。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

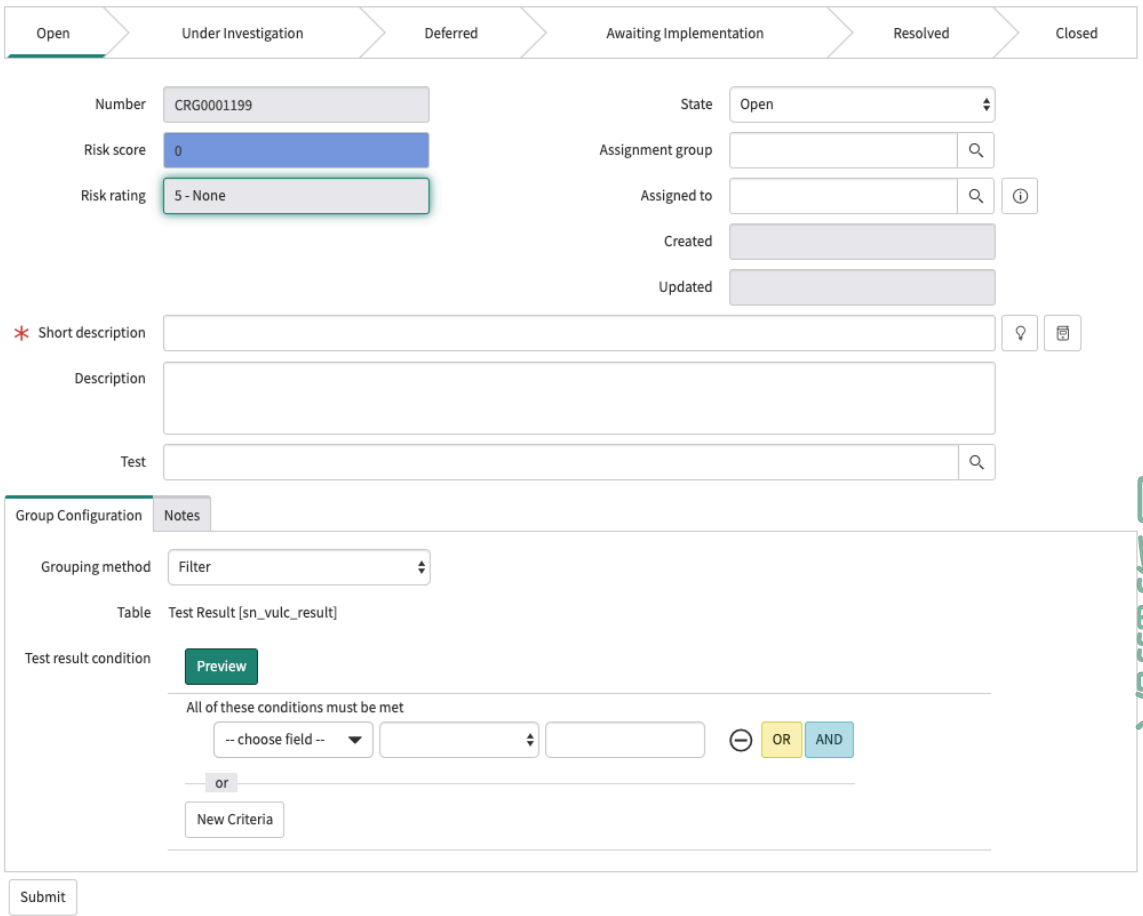
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > 修復タスク.
2. ナビゲーションパネルで、[自分のオープンタスク **(My Open Tasks)]** または [すべてのオープンタスク] をクリックしてリストを表示します。
3. [新規] をクリックします。

修復タスクフォーム



4. 修復タスクフォームで、必要に応じてフィールドに入力します。

修復タスクフォーム

フィールド	説明
数値	システムで自動アサインされた ID。
リスクスコア	リスクスコア算出で自動入力されます。 ロールアップリスクスコアです。このリスクスコアは、「クローズ済み」ではない ([オープン]、[調査中]、[実装待ち]、[保留中]、[解決済み]) すべてのテスト結果における最大リスクスコアから 85%、「クローズ済み」ではないテスト結果数の 15% のスコアで、重み付けされています。
リスク評価	リスクスコア算出で自動入力されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

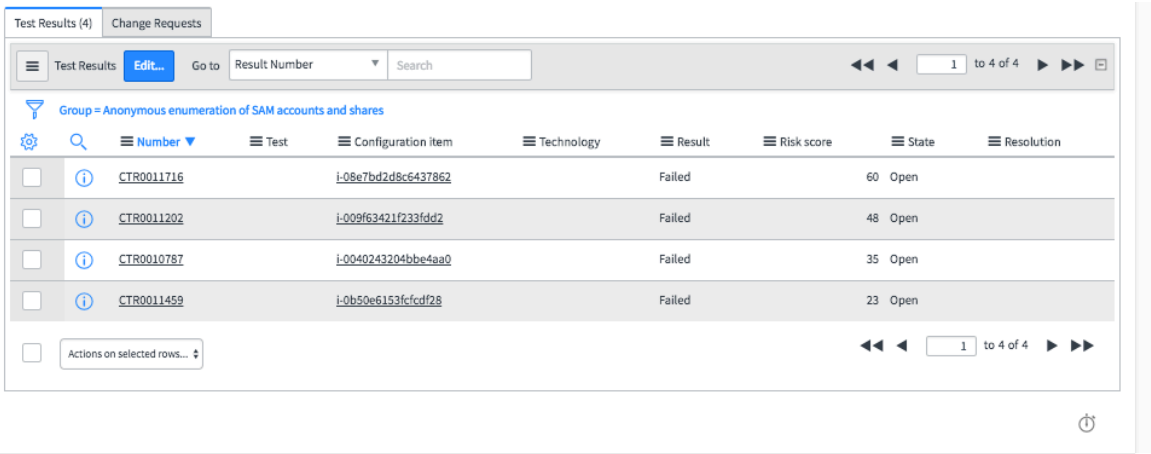
フィールド	説明
	リスクスコア範囲に基づき、全体的なリスクを [1 - 重大] ～ [5 - なし] の 1 ～ 5 の数値スケールで評価します。このフィールドは、以前のバージョンの [優先度] フィールドに代わるものです。
状況	初期状態は [オープン] で、修復タスクの修復ステータスです。詳細については、「コンフィグレーションコンプライアンス のステータス」を参照してください。
アサイン先グループ	修復タスクを修復グループにアサインします。
アサイン先	修復タスクを修復する担当者をアサインします。
作成日時	この修復タスクを作成した日付。
更新日時	この修復タスクを更新した日付。
Short Description (簡単な説明)	修復タスクの名前。
説明	この修復タスクの説明。
テスト	この修復タスクの構成テストを選択します。
[関連タブ]	
グループ構成	使用するグループ化の方法は次のとおりです。 ○ 手動 (デフォルト) : ○ フィルターまたはグループルール : テーブル：テスト結果 [sn_vulc_result] として事前に選択済み テスト結果の条件：使用するフィルターを選択します。 **注:** フィルター条件の上にある [レコードが条件に一致] リンクをクリックすると、選択したテスト結果レコードが新しいウィンドウに表示されます。 [プレビュー] をクリックして、新しいグループを保存する前に、フィルター基準によって返される結果の数を確認します。 [テスト結果] 関連リストは、[テスト結果] 関連タブの [編集] ボタンをクリックして手動で作成する必要があります。
メモ	この修復タスクに関連する作業メモ。

5. ヘッダーを右クリックして [保存] するか、[送信] をクリックして保存し、修復タスクのリストに戻ります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[テスト結果] および [変更要求] 関連リストを表示します。



[テスト結果] リストからコンフィグレーションコンプライアンス修復タスクを手動で作成する

[テスト結果] リストから修復タスクを手動で作成し、結果として得られた修復タスクから修復を実行できます。

始める前に

必要なロール：sn_vulc.admin

このタスクについて

この方法では、含めるテスト結果を選択し、[選択した行のアクション...] メニューからグループを作成する必要があります。この方法は、簡単にフィルタリングできない結果や、修復のためにテスト結果を指定する場合に適しています。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

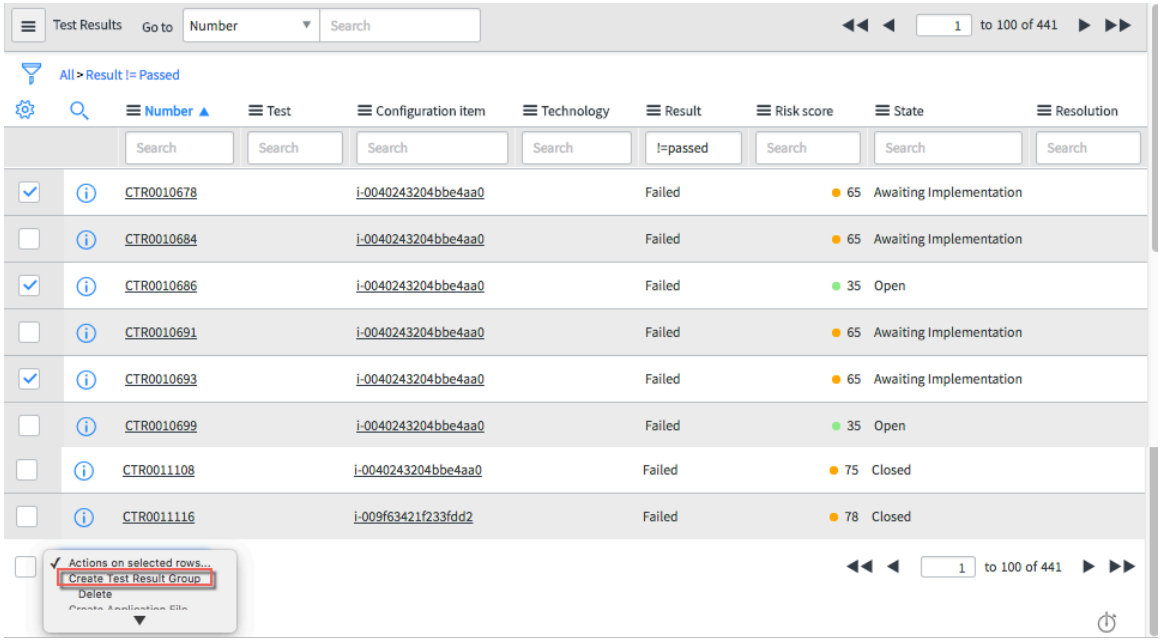
v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > テスト結果.
2. ナビゲーションパネルで、 [テスト結果] モジュールを選択してリストを開きます。
3. 各テスト結果の横にあるチェックボックスをオンにして、修復タスクに含めるテスト結果を選択します。
4. リストの下部にある [選択した行のアクション...] メニューを開きます。

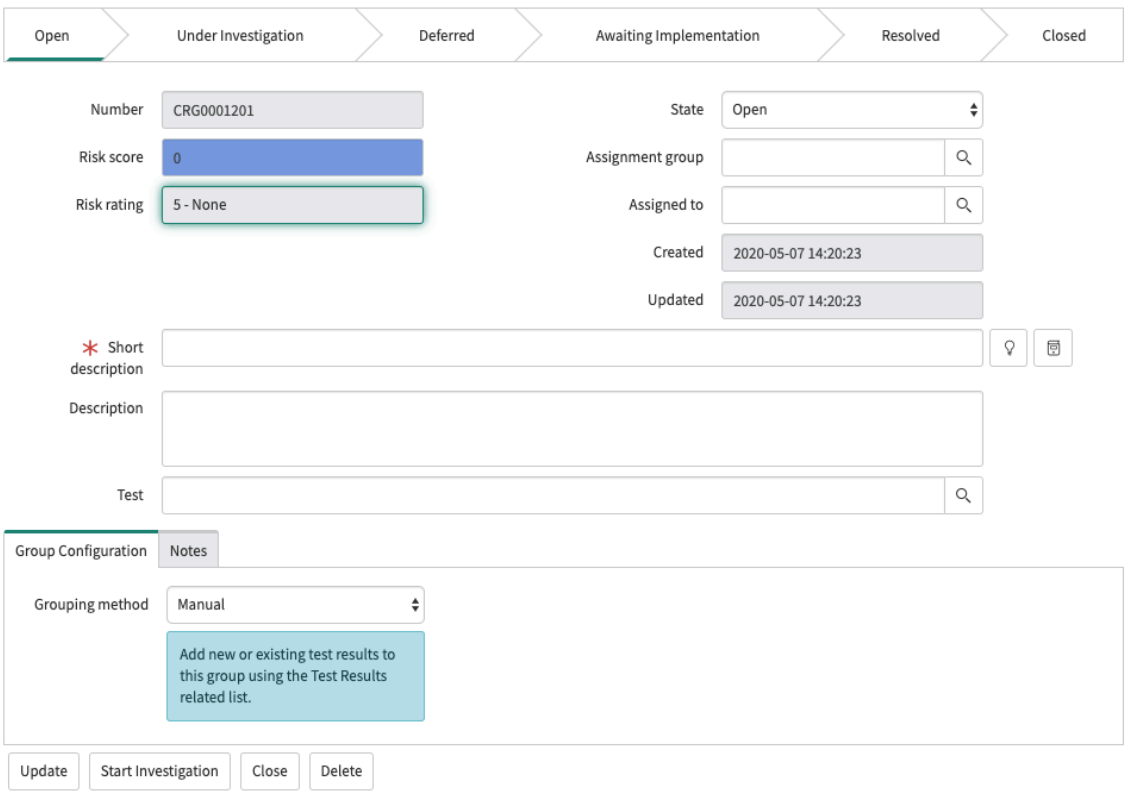
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



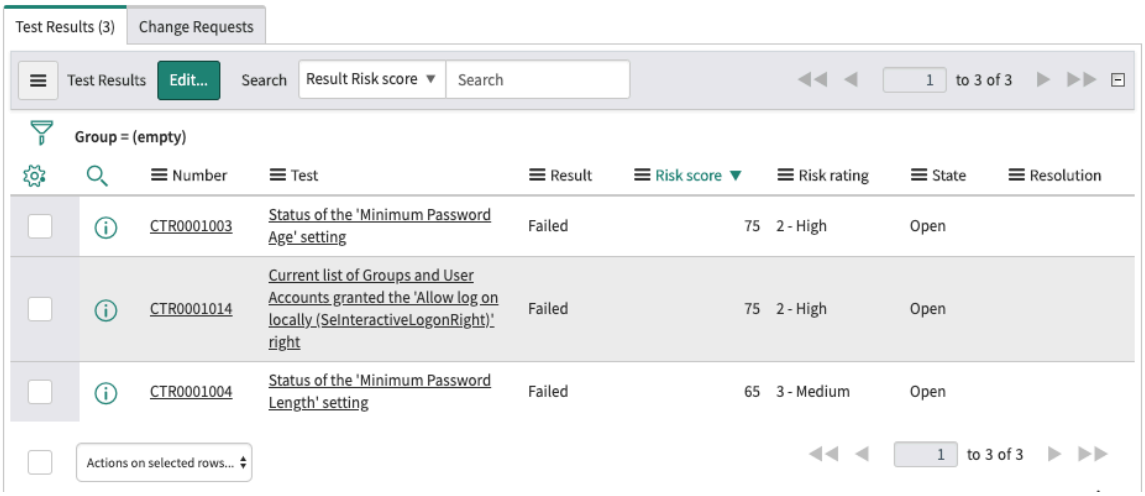
5. [修復タスクの作成] を選択します。
修復タスクが作成され、開きます。

修復タスクフォーム



修復タスクに対して選択したテスト結果は、関連する変更要求とともに [テスト結果] 関連リストに表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



6. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
数値	システムで自動アサインされた ID。
スコア	リスクスコアロールアップ算出で自動入力されます。 ロールアップリスクスコアです。このリスクスコアは、「クローズ済み」ではない ([オープン]、[調査中]、[実装待ち]、[保留中]、[解決済み]) すべてのテスト結果における最大リスクスコアから 85%、「クローズ済み」ではないテスト結果数の 15% のスコアで、重み付けされています。
評価	リスクスコアロールアップ算出で自動入力されます。 リスクスコア範囲に基づき、全体的なリスクを [1 - 重大] ～ [5 - なし] の 1 ～ 5 の数値スケールで評価します。このフィールドは、以前のバージョンの [優先度] フィールドに代わるものです。
履歴リスクスコア	リスクスコアロールアップ算出で自動入力されます。 修復タスク内のすべての合格したテスト結果全体にわたる固有のリスクスコア。このフィールドは、テストグループによって修復されたリスク量を表示し、テストグループが「クローズ済み」ステータスにあり、リスクスコアがゼロの場合にのみ表示されます。
状況	初期状態は [オープン] で、修復タスクの修復ステータスです。詳細については、「コンフィグレーションコンプライアンス のステータス」を参照してください。
アサイン先グループ	修復タスクを修復グループにアサインします。
アサイン先	修復タスクを修復する担当者をアサインします。
作成日時	この修復タスクを作成した日付。
更新日時	この修復タスクを更新した日付。
Short Description (簡単な説明)	修復タスクの名前。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
説明	この修復タスクのテキスト説明。
	この修復タスクの構成テストを選択します。
[関連タブ]	
グループ構成	使用するグループ化の方法は次のとおりです。 ○ 手動 (デフォルト) ○ フィルター テーブル：テスト結果として事前に選択済み テスト結果の条件：使用するフィルターを選択します。 注: フィルター条件の上にある [レコードが条件に一致] リンクをクリックすると、選択したテスト結果レコードが新しいウィンドウに表示されます。 [プレビュー] をクリックして、新しい修復タスクを保存する前に、フィルター基準が返す結果の数を確認します。
メモ	この修復タスクに関連する作業メモ。
関連リスト	
テスト結果	この修復タスクに含まれるテスト結果。
変更要求	この修復タスクに関連付けられた変更要求。

7. ヘッダーを右クリックして [保存] するか、[送信] をクリックして保存し、修復タスクのリストに戻ります。

コンフィグレーションコンプライアンスで変更要求を作成する

コンフィグレーションコンプライアンスアプリケーションの修復タスクから変更要求を作成できます。

始める前に
必要なロール：itil ロールを持つユーザー

このタスクについて
IT または修復スペシャリストは、修復タスクからすべてのテスト結果に対する変更要求 (CHG) を直接作成します。事前設定された情報を使用して変更要求を作成し、手動での介入が必要な脆弱性の調査を迅速化します。

アサインされた修復タスクから、変更要求を直接作成、承認、実装、レビュー、およびクローズすることができます。修復タスクから事前入力された情報を使用して、次の 3 つのタイプの変更要求を作成できます。

標準

事前に承認されたリスクの低い変更で、比較的一般的で、指定された手順または作業指示書に従います。

通常

通常の変更要求は、実装、レビュー、およびクローズする前に 2 レベルの承認が必要な規範的なプロセスに従います。

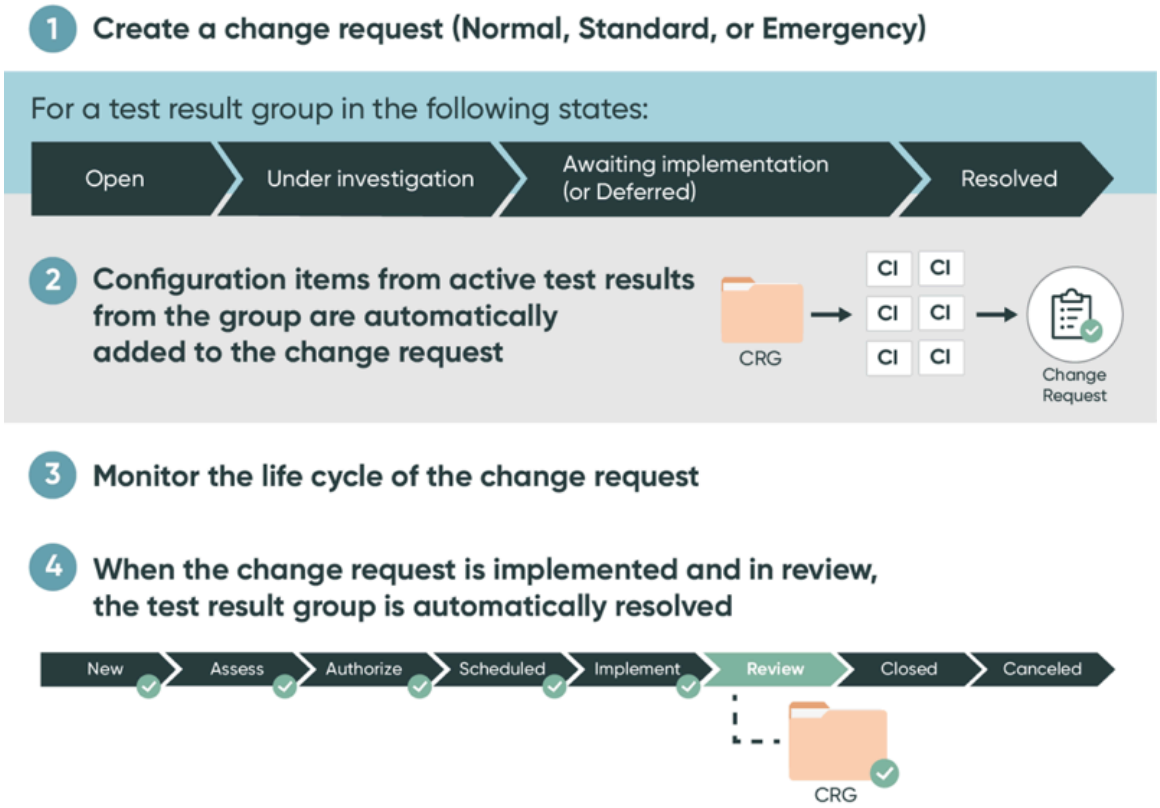
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

緊急

重大なインシデントを解決するための変更。

次の図は、修復タスクから変更要求を作成する基本的なフローを示しています。このフローの詳細な手順は、図に沿って説明します。



脆弱性対応のバージョン 19.0 以降では、IT 修復ワークスペースから修復タスクの変更要求を作成できます。詳細については、「IT 修復ワークスペースで変更要求を作成する」を参照してください。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > 修復タスク > 自分のオープンタスク.
   自分のグループにアサインされている修復タスクのリストが表示されます。
2. [番号] 列で、変更要求を作成する修復タスクをクリックします。
   [クローズ済み] または [レビュー中] 以外のステータスの修復タスクから変更要求を作成できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

修復タスクのレコードが表示されます。

3. レコードの右上にある [変更を作成] をクリックします。
   変更要求フォームが表示されます。
4. フィールドに入力します。
   a. [適用先] フィールドのリストから、1 つを選択して続行します。
5. **[CR** に **CI** を追加] チェックボックスで、1 つを選択して続行します。
6. [変更タイプ] フィールドのリストから、1 つを選択して続行します。

   この機能は、ITSM 変更管理のカタログで設定した変更要求のタイプを自動的に読み取ります。たとえば、ITSM の標準的な変更要求の名前を「標準」から「事前承認済み」に変更すると、[変更要求の作成] フォームの [変更タイプ] リストに新しい名前が自動的に表示されます。
7. フォームの [変更要求プレビュー] セクションのフィールドには、修復タスクの情報が事前に入力されています。
   必要に応じて、これらのフィールドを編集します。
8. [変更を作成] をクリックします。
   変更要求が表示されます。[Affected CIs (影響を受ける CI)] 関連リストには、基準に一致するテスト結果の CI が表示されます。変更要求に承認が必要な場合は、[承認要求] ボタンが表示されます。

   変更要求が作成されると、テスト結果グループは [実装待ち] ステータスに移行します。この修復タスクの変更要求が解決された後、この修復タスクに関連付けられた他のオープンな変更要求がない場合、この修復タスクも [解決済み] ステータスに移行します。

   詳細については、「変更要求と修復タスク間のステータスの同期」を参照してください。

   注:
   ステータス同期を有効にした状態で、それぞれのレコードのライフサイクルのステータスを介して変更要求と修復タスクを引き続き手動で移行することはできますが、変更要求状況が変化したことをシステムが登録したり、各自が変更要求を追加したり、修復タスクから変更要求を削除したりすると、ステータス同期によって手動による介入が無効になる可能性があります。ただし、変更要求の状況により、修復タスクのステータスが [クローズ済み] または [保留] 状況から自動的に移行されることはありません。

既存の変更要求への修復タスクの関連付け

コンフィグレーションコンプライアンスアプリケーションの修復タスクを既存の変更要求に関連付けます。

始める前に
必要なロール：itil ロールを持つユーザー

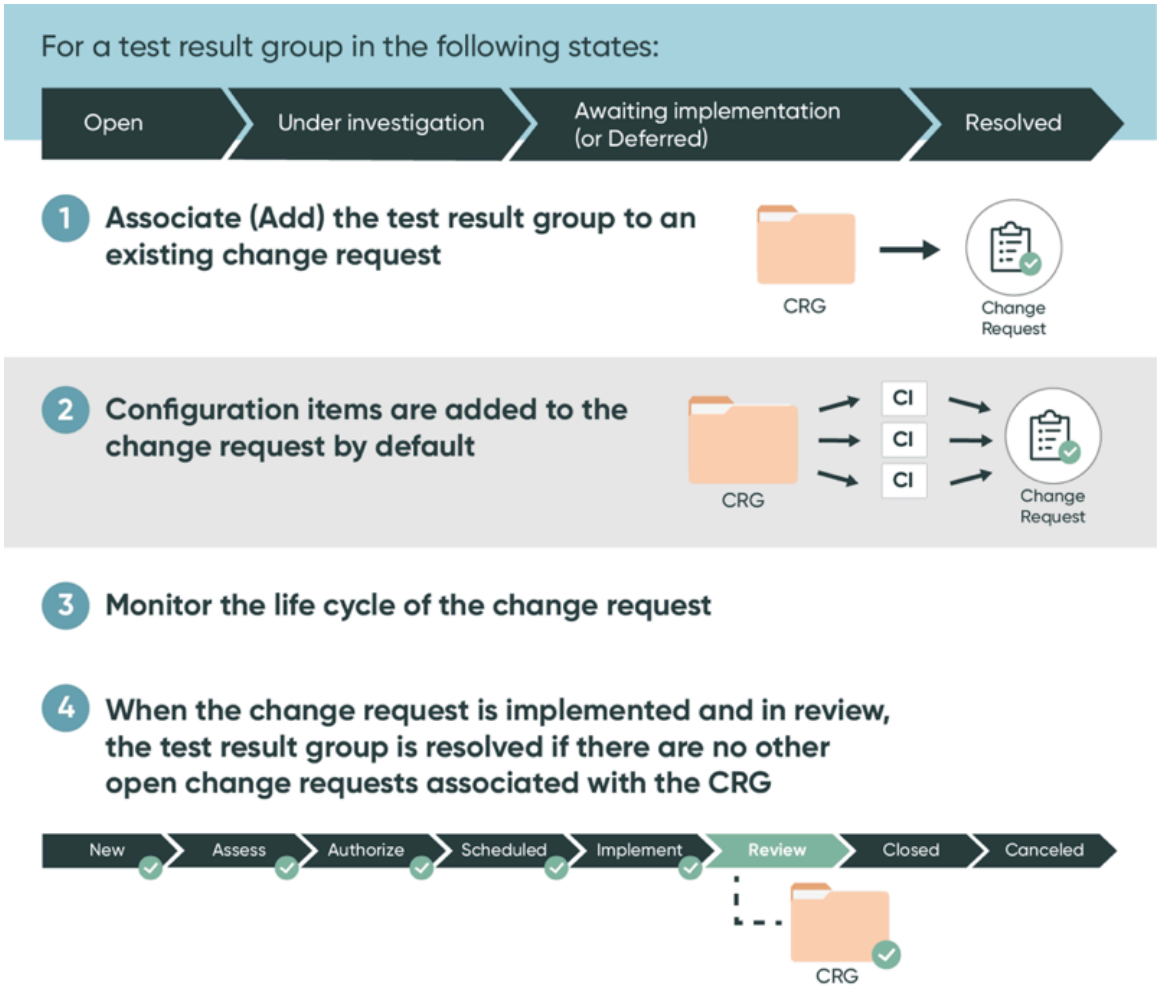
このタスクについて
IT または修復スペシャリストは、修復タスク (RT) をインスタンスで既に利用可能な変更要求 (CHG) に関連付けることで、修復タスクの解決に取り組むときに重複した変更要求を作成しないようにします。

自分または自分のアサイン先グループにアサインされた修復タスクを、修復タスクレコードから直接、既存の変更要求に関連付けることができます。次の図は、既存の変更要求を修復タスクに関連付ける基本的なフローを示しています。このフローの詳細な手順は、図に沿って説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[キャンセル] 以外のステータス ([オープン]、[調査中]、[実装待ち]、[クローズ済み]、および [保留]) で、既存の変更要求を修復タスクに関連付けることができます。過去 90 日以内にクローズされたものを含む変更要求は、フォームから関連付けることができます。変更要求を既存の修復タスクに関連付けると、アクティブなテスト結果とその構成アイテムのみが変更要求に追加されます。



注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > 修復タスク > 自分のオープンタスク.
   自分のグループにアサインされている修復タスクのリストが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

2. [番号] 列で、変更要求を作成する修復タスクをクリックします。

   修復タスクのレコードが表示されます。

3. レコードの右上にある [変更を作成] をクリックします。
   変更要求フォームが表示されます。
4. [変更要求] 関連リストまでスクロールして、選択します。
   修復タスクに関連付けられている変更要求が [追加] ボタンとともに表示されます。
5. [追加] をクリックします。
   [既存の変更要求を修復タスクに追加] ダイアログが表示されます。
6. 検索アイコンをクリックし、リストからアイテムを選択します。
   表示されるリストをフィルタリングして検索を絞り込むことができます。
7. [送信] をクリックします。
   TRG は、変更要求が修復タスクに正常に関連付けられたことを示すメッセージとともに表示されます。[変更の要求] 関連リストの下に、新しい変更要求が表示されます。修復タスクの CI は、デフォルトで変更要求に追加され、[影響を受ける CI] 関連リストに表示されます。この関連リストから、変更要求に CI を追加することもできます。新しい修復タスクに移動されたテスト結果の数を示すメッセージが表示され、新しい RT が表示されます。

   注:
   200 件未満のテスト結果の場合、分割操作は同期的に実行され、テスト結果は新しい修復タスクに表示されます。

   200 件を超えるテスト結果の場合、分割操作はバックグラウンドで非同期に実行され、テスト結果が新しい修復タスクに表示されるまでに数秒かかる場合があります。次のメッセージも表示されます: n 件のテスト結果が、まもなく TRGxxxxxxx から新しい修復タスク GRCxxxxx に移動されます。

   次の例外を除いて、任意の変更要求を修復タスクに関連付けることができます。

   - [キャンセル] ステータスの変更要求。
   - 90 日以上経過した [クローズ済み] ステータスの変更要求。
   - 既に RT に関連付けられている変更要求。すでに RT に関連付けられている変更要求を関連付けることは、システム上できません。

   この修復タスクの変更要求が解決された後、この修復タスクに関連付けられた他のオープンな変更要求がない場合、この修復タスクも [解決済み] ステータスに移行します。

   注:
   ステータス同期を有効にした状態で、それぞれのレコードのライフサイクルのステータスを介して変更要求と修復タスクを引き続き手動で移行することはできますが、変更要求状況が変化したことをシステムが登録したり、各自が変更要求を追加したり、修復タスクから変更要求を削除したりすると、ステータス同期によって手動による介入が無効になる可能性があります。ただし、変更要求の状況により、修復タスクのステータスが [クローズ済み] または [保留] 状況から自動的に移行されることはありません。

   詳細については、「変更要求と修復タスク間のステータスの同期」を参照してください。

修復タスクの分割

コンフィグレーションコンプライアンスアプリケーションの既存の修復タスクから、新しい修復タスクに移動するテスト結果のサブセットを特定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

重要:
アドミンと修復オーナーは、 脆弱性マネージャーワークスペース と IT 修復ワークスペース から修復タスクをそれぞれ分割できます。

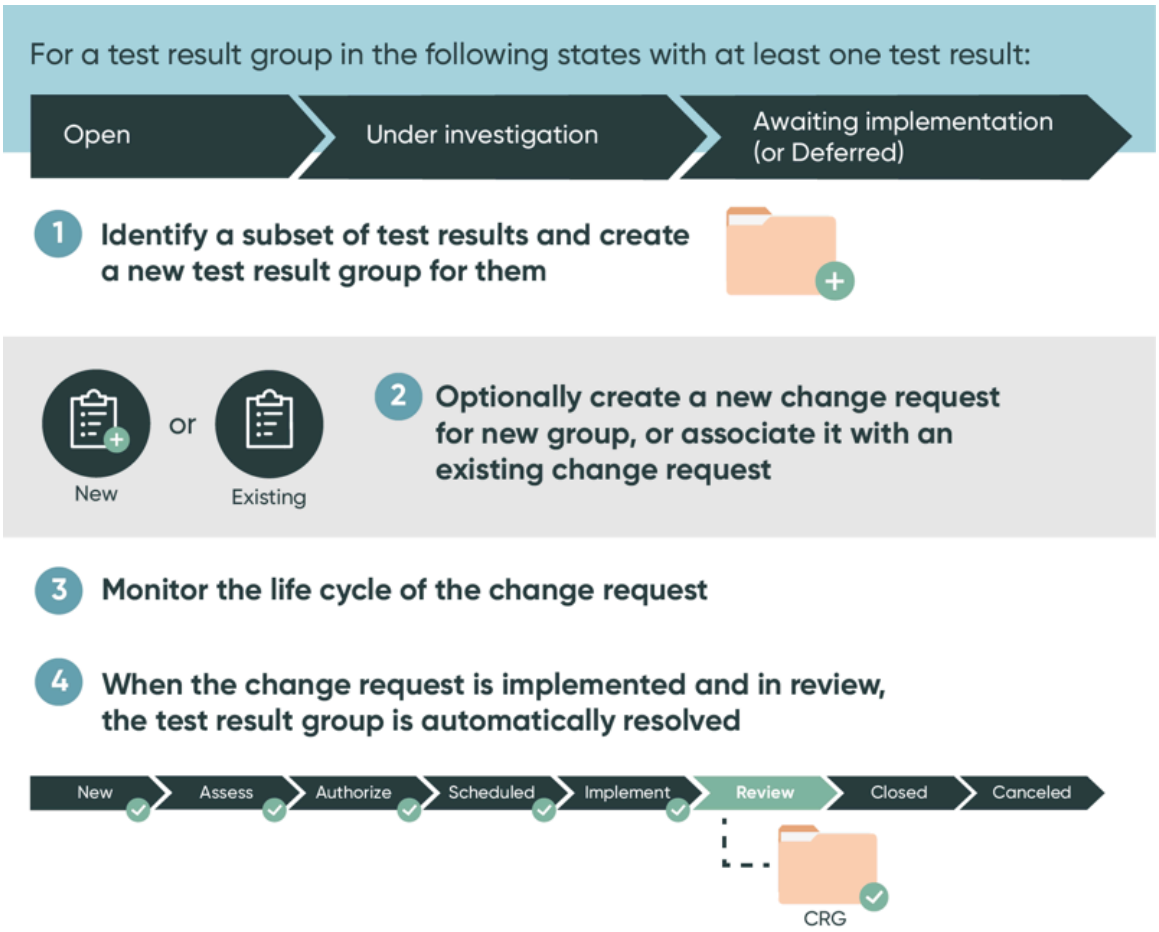
始める前に
必要なロール：itil ロールを持つユーザー

このタスクについて
IT または修復スペシャリストは、複数のテスト結果を使用して、[オープン]、[調査中]、または [実装待ち] 状況で既存の修復タスクを分割できます。特定の条件に一致するテスト結果を含む新しい修復タスクを作成することで、元の修復タスクに影響を与えることなく、特定のテスト結果グループを処理できます。

条件ビルダーで新しい修復タスクに移動するテスト結果の条件を指定すると、条件に一致するアクティブなテスト結果のみが新しいタスクに移動されます。修復タスクを分割する場合は、変更要求 (CHG) を作成する必要はありません。選択によって、変更要求を作成すると同時に修復タスクを分割するか、または変更要求を作成せずに修復タスクを分割することができます。

次の図は、修復タスクを分割する基本的なフローを示しています。このフローの詳細な手順は、図に沿って説明します。

修復タスクを分割するためのフロー



既存の修復タスクのテスト結果を新しいタスクに分割するユースケースには、以下のような例が考えられます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 分割されたタスクに対して変更要求を作成する場合。
- 分割されたタスクをアサイン先グループの別のユーザーに再アサインする場合。
- 特定の構成アイテム (CI) に関する一部のテスト結果が指定された期間内に修復できないことがわかっているために、分割されたタスクの保留または例外を要求する場合。

[store-future: BEGIN review]脆弱性対応のバージョン 19.0 以降では、IT 修復ワークスペースで修復タスクを分割できます。[End]

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > テスト > 修復タスク > 自分のオープンタスク.
   自分のグループにアサインされている修復タスクのリストが表示されます。
2. [番号] 列で、分割する修復タスクをクリックします。

   修復タスクのレコードが表示されます。
3. 特定の条件に一致する新しいタスクについてテスト結果のサブセットを作成するには、次の手順に従います。

   レコードの右上にある [タスクを分割] をクリックします。

   複数のテスト結果を含む大規模なグループで作業している場合は、この方法で新しい修復タスクを作成することをお勧めします。

   [修復タスクを分割] フォームが表示されます。
4. 条件ビルダーを表示した状態で、新しい修復タスクに移動するテスト結果に対する条件を指定します。

   たとえば、次の条件に一致するテスト結果のみを除外することができます。

   - [オープン] ステータス。
   - リスクスコアが 75 より大きい。
   - 結果が [失敗]。

   条件を入力した後にテスト結果がフィルターに一致する場合は、一致するテスト結果の数を示すメッセージが表示されます。

   フィルターに一致するテスト結果がない、またはすべてのテスト結果が条件に一致するというメッセージが表示された場合は、少なくとも 1 つのテスト結果がフィルター基準に一致するように条件を調整します。
5. [アイテムのプレビュー] をクリックし、一致するテスト結果を表示します。
   新しいウィンドウ [修復タスク] にアイテムが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. フィルター基準に一致するテスト結果の詳細をプレビューするには、[タスクを分割] をクリックして新しいグループを作成する前に、次の手順を実行します。
これらの詳細には、アサイン先グループとテスト結果のアサイン先が含まれます。プレビューでこの情報を表示すると、新しいタスクが適切にアサインされていることを確認できます。

   a. プレビューに [修復] リストを表示した状態で、 [結果] 列のアイテムをクリックします。
   テスト結果レコードが表示されます。

   b. [アサイン先グループ] フィールドと [アサイン先] フィールドが正しいことを確認します。

   c. **[Update** (更新)] をクリックします。

7. 新しい修復タスクを作成する準備ができたら、[タスクを分割] をクリックします。
新しい修復タスクに移動されたテスト結果の数を示すメッセージが表示され、新しい修復タスクが表示されます。新しいタスクを識別できるようにするには、[簡単な説明] フィールドのテキストを編集し、必要に応じて、[アサイン先グループ] または [アサイン先] フィールドを再度編集することもできます。

   注:
   200 件未満のテスト結果の場合、分割操作は同期的に実行され、テスト結果が新しいタスクに表示されます。

   200 件を超えるテスト結果の場合、分割操作はバックグラウンドで非同期に実行され、テスト結果が新しいタスクに表示されるまでに数秒かかる場合があります。次のメッセージも表示されます: n 件のテスト結果が、まもなく TRGxxxxxxx から新しい修復タスク GRCxxxxx に移動されます。

8. または、修復タスクの [テスト結果] 関連リストからテスト結果を直接選択することで、新しい修復タスクを作成することもできます。

   修復タスクのテスト結果が数件しかない場合、または新しい修復タスクに移行するテストが明確にわかっている場合は、この方法をお勧めします。

   a. 修復タスクレコードが表示された状態で、[テスト結果] 関連リストまでスクロールします。

   b. 左端の列で、新しい修復タスクを作成するテスト結果のチェックボックスをオンにします。

   c. レコードの左下にある [選択した行のアクション] リストから、[タスクを分割] をクリックします。

   d. 表示される [修復タスクを分割] フォームで、新しいグループを識別できるようにするために、[簡単な説明] フィールドのテキストを編集することもできます。

   e. [タスクを分割] をクリックします。
   新しいタスクに移動されたテスト結果の数を示すメッセージが表示され、新しい修復タスクが表示されます。

   この修復タスクの変更要求が解決された後、この修復タスクに関連付けられた他のオープンな変更要求がない場合、この修復タスクも [解決済み] ステータスに移行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> ステータス同期を有効にした状態で、それぞれのレコードのライフサイクルのステータスを介して変更要求と修復タスクを引き続き手動で移行することはできますが、変更要求状況が変化したことをシステムが登録したり、各自が変更要求を追加したり、修復タスクから変更要求を削除したりすると、ステータス同期によって手動による介入が無効になる可能性があります。ただし、変更要求の状況により、修復タスクのステータスが [クローズ済み] または [保留] 状況から自動的に移行されることはありません。

詳細については、「変更要求と修復タスク間のステータスの同期」を参照してください。

次のタスク
新しい修復タスクの変更要求を作成または関連付けることができます。詳細については、「既存の変更要求への修復タスクの関連付け」と「コンフィグレーションコンプライアンスで変更要求を作成する」を参照してください。

自分または自分のグループの修復タスクからアサインを削除する

テスト結果レコードが自分またはグループに誤ってアサインされている場合は、コンフィグレーションコンプライアンス アプリケーションで再アサインします。

始める前に
必要なロール：sn_vulc.remediation_owner

このタスクについて
コンフィグレーションコンプライアンス アプリケーション v14.3 以降 修復タスク (RT) とそれに関連するテスト結果が修復の範囲外であると判断した場合、またはレコードが自分または自分のグループに誤ってアサインされていると思われる場合、RT レコードの [アサイン先] フィールドと [アサイン先グループ] フィールドから自分または自分のグループを削除できます。

[クローズ済み] または [解決済み] 以外のステータスの修復タスクレコードには、[アサイン解除] ボタンが表示されます。

> **注:**
> コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

手順
1. [クローズ済み] または [解決済み] 以外のステータスの自分にアサインされている修復タスクレコードに移動します。
2. [アサイン先] および [アサイン先グループ] フィールドをクリアするには、レコードの上部にある [アサイン解除] を選択します。
3. [アサイン解除] ダイアログで、作業メモを入力し、[送信] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 入力した作業メモが [メモ] セクションに表示されます。
- [ステータス変更承認] タブでは、ステータス変更承認レコード (CA#) に [レビュー中] ステータスが表示されるため、承認ワークフローを追跡できます。
- [要求済みの承認 **(Requested Approvals)]** タブでは、自分または自分のアサイン先グループの削除要求が [要求済み (Requested)] ステータスで表示されます。

タスクの結果

要求は、デフォルトの 1 レベルの承認ワークフローを使用して承認されます。詳細については、「Approve an unassign request in Configuration Compliance (コンフィグレーションコンプライアンスでアサイン解除要求を承認する)」を参照してください。

- 要求が承認されると、ステータス変更承認レコードと要求された承認レコードが [承認済み] に移行します。自分と自分のグループが [アサイン先] フィールドと [アサイン先グループ] フィールドから削除されます。[未アサイン] が [アサインタイプ] フィールドに表示され、修復タスクが コンフィグレーションコンプライアンス アプリケーションの [未アサイン] モジュールのリストに表示されます。

  レコードが未アサインであるという通知は、[通知のアサイン解除 (Unassign notification)] グループの脆弱性マネージャーまたはアナリストに自動的に送信されます。この機能の通知とプロパティの詳細については、「Removing assignments from Configuration Compliance test result groups (コンフィグレーションコンプライアンスのテスト結果グループからアサインを削除する)」を参照してください。

- 要求が却下されると、ステータス変更承認レコードと要求された承認レコードが [却下 (Rejected)] に移行します。

注:
脆弱性アドミニストレーター は、*sn_vulc.unassign_test_result_group.approval_required* システムプロパティを **[False]** に設定して、承認プロセスを無効にできます。

次のタスク

コンフィグレーションコンプライアンスアプリケーションの [未アサイン] モジュールに移動し、未アサインレコードを監視し、スコープ内に該当する可能性があるアイテムを確認して、自分に再アサインします。

コンフィグレーションコンプライアンス のアサイン解除要求を承認する

コンフィグレーションコンプライアンスアプリケーションのアサイン先グループまたは個々のユーザーからの修復タスクの削除要求を承認します。

始める前に

必要なロール：sn_vulc.unassign_approver

このタスクについて

デフォルトでは、承認構成が提供されます。承認をアサイン解除するには、承認者 - レベル 1 承認グループに 1 人の承認者が必要です。デフォルトでは、アサイン解除承認グループ ([承認者のアサイン解除 CC - レベル 1]) が作成され、このグループに属するユーザーが要求を承認できます。デフォルトでは、このグループにはアサイン解除承認者ロール sn_vulc.unassign_approver が含まれています。に移動すると、グループを変更または作成し、承認構成を更新できます **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > 承認ルール > 修復タスクフィールドの変更要求 > 修復タスクのアサインを解除.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > 自分の承認.
2. キューから要求を選択します。
3. 適切なコメントを添えて、要求を承認または却下します。

テスト結果の自動クローズ

廃止された構成アイテム (CI) に関連付けられたテスト結果 (TR) を自動的に閉じることができます。

自動クローズオプションを設定するには、**[sn_vulc.auto_close_test_results_linked_to_retired_CIs]** システムプロパティに移動して、true に設定します。廃止された CI に関連する TR を自動的にクローズするには、「廃止された CI に関連するテスト結果を自動的にクローズする」を参照してください。

廃止された構成アイテムの操作については、「コンフィギュレーションコンプライアンスで廃止された構成アイテムを操作する」を参照してください。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

コンフィギュレーションコンプライアンスで廃止された構成アイテムを操作する

廃止された構成アイテム (CI) は、構成管理データベース (CMDB) で [廃止]、[アーカイブ化済み]、または [削除済み] ステータスに移行します。コンフィグレーションコンプライアンス には、CI で構成されるテスト結果 (TR) が含まれています。CI のステータスが [廃止] に更新されると、関連する TR は「CI 廃止」サブステートでクローズされます。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

CMDB が CI のライフサイクルステージのステータスを [廃止] に変更した場合、関連する TR を自動的にクローズすることが選択できます。関連する TR を自動的に閉じる際の詳細については、「廃止された CI に関連するテスト結果を自動的にクローズする」を参照してください。

廃止された CI はアーカイブされるか、最終的に CMDB から完全に削除されます。

CI の廃止による影響：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [検出されたアイテムへの影響 **(Impact on discovered items)**]：CI が廃止されると、関連する DI は「CI 廃止」とマークされます。
- [テスト結果への影響 **(Impact on test results)**]： DI のステータスが「CI 廃止」に更新されると、関連する TR がクローズされ、[メモ] セクションが自動的に更新されます。

> **注:**
> CI のライフサイクル状況が更新されるたびに、DI のステータスが自動的に「CI 廃止」に更新されます。一方、TR のステータスは、**[sn_vulc.auto_close_test_results_linked_to_retired_CIs]** プロパティが true に設定されている場合のみ [クローズ済み] に更新されます。関連する TR を自動的に閉じる際の詳細については、「廃止された CI に関連するテスト結果を自動的にクローズする」を参照してください。

スケジュール済みジョブ [*Close Test Results for decommissioned CIs*] は、更新された DI に対して毎日実行されます。廃止された CI に対して自動クローズ構成オプションが有効になっている場合は、廃止された CI を含む DI が識別され、サブステートが「CI 廃止」である関連 TR がクローズされます。修復タスク内のすべての TR がクローズされ、そのサブステートが「CI 廃止」の場合、修復タスクもクローズされ、サブステートは「キャンセル済み」になります。

> **注:**
> CI が「廃止」ステータスから元のステータスに戻ると、「検出されたアイテム」エントリーも更新されます。スキャナーから再度データが取り込まれると、TR が自動的に開きます。

廃止された **CI** に関連するテスト結果を自動的にクローズする

構成管理データベース (CMDB) が構成アイテム (CI) のライフサイクルステージのステータスを変更した場合、関連するテスト結果を自動的にクローズすることが選択できます。

始める前に
必要なロール：sn_vulc.admin

このタスクについて
関連する TR を自動的にクローズするには、システムプロパティ **[sn_vulc.auto_close_test_results_linked_to_retired_CIs]** を有効にして、廃止された CI に関連付けられている TR を自動クローズする必要があります。このオプションを有効にすると、同じ CI で報告された新規および既存の TR は、自動的に「クローズ済み」ステータスで作成または更新されます。これらは、スキャナーペイロードの資産 ID と検出されたアイテムのエントリーステータスに基づいています。廃止された CI の影響の詳細については、「コンフィギュレーションコンプライアンスで廃止された構成アイテムを操作する」を参照してください。

> **注:**
> CI のライフサイクル状況が更新されるたびに、DI のステータスが「CI 廃止」に更新されます。一方、TR のステータスは、**[sn_vulc.auto_close_test_results_linked_to_retired_CIs]** システムプロパティが有効の場合のみ [クローズ済み] に更新されます。

手順

1. 次のように移動する。 システムプロパティ > すべてのプロパティ をクリックし、[名前] 列で *sn_vulc.auto_close_test_results_linked_to_retired_CIs* でフィルタリングします。
2. プロパティを選択します。
3. 廃止された CI に関連付けられたテスト結果を自動的にクローズするには、 プロパティの値を true に設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンフィグレーションコンプライアンス の古いテスト結果を自動的にクローズする

古いテスト結果の自動クローズ機能をアクティブ化して、サードパーティ統合によって最近検出されなかった古いテスト結果を自動的にクローズできます。これらのテスト結果を [クローズ済み - 古い **(Closed-Stale)]** に移動すると、インスタンス内のアクティブなテスト結果と修復タスクの数を減少させて、構成管理データベース (CMDB) の資産を調整することができます。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

概要

[古いテスト結果の自動クローズ] モジュールを使用すると、サードパーティ統合によって最近検出されなかった古いテスト結果を自動的にクローズできます。テスト結果は、条件ビルダーで設定した条件に基づいて、[クローズ済み - 古い **(Closed-Stale)]** に移動されます。

主要な用語

テスト結果

テスト結果は、テクノロジー資産のクラスの管理方法を定義するフレームワーク、ポリシー、および信頼できるソースにマッピングされた構成テストのライブラリからインポートされた結果です。コンフィグレーションコンプライアンス アプリケーションは、テスト結果を算出せず、サードパーティ統合からテスト結果をインポートします。

資産の前回スキャンの日付

テスト結果に関連する [検出されたアイテム] テーブルの [前回の Configuration Compliance スキャン日] 列の値を参照します。この日付は、サードパーティのスキャナーによって資産が最後にスキャンされた日時を示します。

前回の失敗日

[結果] フィールド値が [失敗] の場合、テスト結果テーブルの [最終確認日] 列の日付を参照します。

古いテスト結果

インスタンス内のテスト結果のうち、古く、長期間にわたってサードパーティ統合のスキャンによって発見、更新、または検出されていないものを参照します。

最後に検出されたテスト結果

この検索オプションは、サードパーティのスキャナーによって提供された日付と時刻を使用します。この用語は、スキャナーによってテスト結果が再度検出された最新の日付 (日前) を指します。このパラメーターは設定可能です。

ユースケース

資産 (構成アイテム) は、自分の環境で廃止されたり、サードパーティのスキャナーによって消去されたりすることがあります。これが発生すると、資産が関連する構成テスト結果はインポートされた検出によって コンフィグレーションコンプライアンス アプリケーションで更新されることなく、非アクティブ (古い状態) になります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インスタンス内のアクティブなテスト結果 (TR) と修復タスク (RT) の数を減少させるには、[古いテスト結果の自動クローズ] 機能をアクティブ化します。この機能は、ステータスが変更されていない、または統合によって最近インポートされていない古いテスト結果を自動的にクローズします。

たとえば、特定の構成アイテム (CI) に複数の資産 ID があり、そのうちの 1 つの ID が過去 90 日間にサードパーティのスキャナーからの検出でインポートされていなかったとします。[古いテスト結果の自動クローズ] モジュールで条件ビルダーを設定して、過去 90 日以上検出または更新されていないテスト結果をクローズすると、この機能によってこのフィルタリングに一致するテスト結果が自動的にクローズされます。

注:
この機能は、条件ビルダーで設定し、サードパーティのスキャナー統合によって検出されたフィルター条件に基づいて、テスト結果の検出のみをクローズします。

[解決] フィールド

Qualys や Tenable.io 製品などのサードパーティのスキャナーによってクローズされた検出と、インスタンスの古いテスト結果の自動クローズ機能を区別するために、[解決] フィールドの新しい値 [クローズ済み - 古い (Closed-Stale)] が追加されました。[クローズ済み - 古い **(Closed-Stale)]** は、TR が自動クローズ機能によってクローズされたことを示します。[クローズ済み] または [修復済み - クローズ済み **(Fixed-Closed)]** は、TR がスキャナーによってクローズされたことを示します。

自動クローズ機能を使用して **TRG** に **TR** 状況をロールアップする

テスト結果のステータスの進捗状況と優先順位は次のとおりです。 オープン > クローズ済み > 修正済み - クローズ済み > クローズ済み - 古い.

1. TRG 内のいずれかの TR が [オープン] である場合、TRG ステータスは変更されません。
2. 少なくとも 1 つの TR が [クローズ済み - 修復済み **(Closed - Fixed)]** で、残りが [クローズ済み - 古い **(Closed - Stale)]**の場合、TRG 状況は [クローズ済み - 修復済み **(Closed - Fixed)]** に移行します。
3. TRG 内のすべての TR が [クローズ済み - 修正済み **(Closed - Fixed)]** の場合、TRG 状況は [クローズ済み - キャンセル済み **(Closed - Canceled)]** に移行します。

サポートされる統合

この機能をサポートするサードパーティ統合の詳細については、「Qualys 脆弱性統合の概要」および「脆弱性対応 および コンフィグレーションコンプライアンス アプリケーションとの Tenable.io 統合」を参照してください。

コンフィグレーションコンプライアンス の [古いテスト結果の自動クローズ] を使用する

[古いテスト結果 (TR) の自動クローズ] をアクティブ化して、設定したフィルター条件に基づいて古いテスト結果を自動的にクローズします。

始める前に
この機能、重要な用語、およびテスト結果データをインポートするサードパーティ統合に必要なセットアップの詳細については、「コンフィグレーションコンプライアンス の古いテスト結果を自動的にクローズする」を参照してください。

必要なロール：sn_vulc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > 古いテスト結果の自動クローズ.
2. フィールドに入力します

フィールド	値
名前	この設定レコードの名前。
有効	選択すると、このレコードがアクティブになり、そのフィルター基準に一致するテスト結果が自動的にクローズします。
保留された TR の古い TR を無視	選択すると、[レビュー中 **(In-review)]** または [保留] 状況にマッピングされた TR は無視され、クローズされません。このオプションをオフにすると、基準に一致するすべての TR がクローズされます。
実行順序	デフォルト値は 100 です。この値は、古いテスト結果の検索とマーキングのために使用される各設定レコードの実行順序を昇順で決定します。
説明	このレコードの説明。このテキストは、多数のレコードを作成した場合に、再度見つけるのに役立つ場合があります。
条件	クローズする TR を検索するために使用するフィルター条件。デフォルトのフィルターは 検出済みアイテム > 前回スキャン > .

3. [**Submit** (送信)] を選択します。

スケジュール済みジョブ [*Auto-Close Stale Test Results*] を毎日実行します。このジョブは、指定した条件に基づいて TR を識別し、一致する TR を [ステータス: クローズ済み] に移行します。

TR が [ステータス:クローズ済み - 古い (State: **Closed-Stale)]** としてマークされた後、スキャナーがこれらの TR を再度検出すると、テスト結果が再オープンされ、状況が[オープン] に戻ります。

TR が [ステータス:クローズ済み - 古い (State: **Closed-Stale**)] としてマークされ、スキャナーが修復済み ([解決: 修復済み **(Resolution: Fixed)**)] を検出した場合、TR は [ステータス: クローズ 済み (Closed Resolution: **Fixed**)] に移行します。[結果:合格] の TR は、[ステータス:クローズ済み 解決:修正済み (State: **Closed**)] のままです。ステータスは、次のリストで説明されているように修復タスクにもロールアップされます。

a. 修復タスクの TR のいずれかが [オープン] の場合、修復タスクのステータスは変更されません。
b. 少なくとも 1 つの TR が [ステータス:クローズ済み 解決:修正済み] で、残りが [クローズ済み - 古い **(Closed-Stale)]** の場合、修復タスクのステータスは [クローズ済み 解決:修正済み (**Closed** Resolution: Fixed)] に移行します。
c. 修復タスクのすべての TR が [クローズ 済み 解決: 修正済み (Closed Resolution: Fixed)] の場合、TRG 状況は [ステータス: クローズ 済み 解決: キャンセル済み (Closed Resolution: Canceled)] に移行します。

状況移行の詳細については、「 コンフィグレーションコンプライアンスアプリケーションのテスト結果と修復タスクのステータス移行」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

修復タスクをクローズ

修復タスクに関連する問題をそれ以上分析することなくすぐにクローズできると判断した場合は、[クローズ] 機能を使用できます。

始める前に
必要なロール：

- sn_vulc.admin
- sn_vulc.remediation_owner

> **注:**
> sn_vulc.remediation_owner ロールを使用すると、自分や自分のアサイン先グループにアサインされた修復タスクを再アサインまたはクローズできます。

このタスクについて
コンフィグレーションコンプライアンスの v15.0 以降では、修復タスクの [クローズ] ボタンが削除されました。

修復タスクを解決すると、その解決メモはすべてのテスト結果の作業メモに反映されます。

手順

1. 修復タスクレコードを開きます。
2. [クローズ] ボタンをクリックします。
3. 問題がクローズされる理由をポップアップウィンドウに記述します。
4. [クローズ] をクリックします。

関連情報

コンフィグレーションコンプライアンス のステータス

修復タスクに対する例外の要求と承認

修復タスクの修復を指定した期間保留するように要求できます。承認者グループに属しているユーザーは、例外要求を承認できます。

> **注:**
> コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

例外要求を要求または承認するには、次を参照してください。

- コンフィグレーションコンプライアンスの修復タスクに対する例外を要求する
- コンフィグレーションコンプライアンス の例外要求を承認する

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

例外管理の全ステージでメール通知が送信され、要求のステータスやその他の詳細情報が通知されます。たとえば、例外が要求されると、要求が発生したことを確認するメールが要求者に届きます。承認者にも、例外が要求されたことを示すメールが届きます。

コンフィグレーションコンプライアンスの v14.11 以降では、例外を承認する期間を設定できます。また、設定した日数経過後の承認者と要求者の両方に対するメール通知も可能です。要求が発生すると、テスト結果が [レビュー中] ステータスに変わり、ステータス変更レコードが作成されます。設定された期間内に承認者が応答しない場合、テスト結果は [オープン] ステータスに戻ります。以前のステータスは **[backup_state]** フィールドに保存されます。詳細については、「例外管理の承認ルールの構成」を参照してください。

コンフィグレーションコンプライアンスの修復タスクに対する例外を要求する

修復タスクをすぐに修復できない場合に、修復タスクの修復を指定した期間保留する例外を要求します。

始める前に
必要なロール：sn_vulc.remediation_owner

このタスクについて

重要:
以下の例外を要求できます。

- Vulnerability Manager ワークスペースとIT 修復ワークスペースの修復タスク詳細については、「IT 修復ワークスペースで例外を要求する」を参照してください。
- Vulnerability Manager ワークスペースからの複数のテスト結果を同時に取得詳細については、「脆弱性マネージャーワークスペースでの一括例外の要求」を参照してください。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > 修復タスク > すべてのタスク.
2. 例外を要求する修復タスクを選択します。
   選択するタスクは、[オープン]、[調査中]、または [実装待ち] ステータスである必要があります。
3. 修復タスクフォームで、[例外の要求] をクリックします。

注:
で 脆弱性対応 または GRC: ポリシーとコンプライアンス管理 が選択されているかどうかに応じて コンフィグレーションコンプライアンス > 例外管理 画面で、[例外の要求] フォームが変更されます。「コンフィグレーションコンプライアンス の例外管理の設定」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [例外管理] 画面で 脆弱性対応 が選択されている場合は、次の操作を行います。

   a. フォームのフィールドに入力します。

   [例外の要求] フォーム

フィールド	説明
期限	例外要求の有効期限が切れる日付この日付は、次で選択した期間内である必要があります: **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > 例外管理 スクリーン。 例外要求の有効期限が切れると、修復タスクは [オープン] ステータスに戻ります。 **注:** コンフィグレーションコンプライアンス (CC) のバージョン 14.7 以降、保留された修復タスクは例外期間が終了する前にスキャナーによって再オープンされると、修復タスクのステータスが [オープン] から [保留] に変わります。この機能はデフォルトでは無効になっています。この機能を有効にするには、*sn_vulc.auto_defer_test_result_in_active_* システムプロパティの値を [true] に設定します。また、保留期限の日付は、有効期限後に修復タスクが再オープンされた後も保持されます。
理由	例外の理由。選択肢は次のとおりです。 ▪ リスクの受容 ▪ メンテナンス期間待ち ▪ 修正が利用不可 ▪ コントロールの緩和を実施 ▪ その他 理由の新しい選択肢を追加する方法については、「ポリシーの理由のマッピングの定義」を参照してください。
追加情報	この要求が行われている理由に関連する詳細情報。このフィールドは修復オーナーが更新します。

   b. [承認要求] をクリックして例外要求を送信します。

タスクの結果
修復タスクのステータスが [レビュー中] に変わります。[ステータス変更承認] タブを使用して、例外要求のステータスを追跡します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクの延長の要求

保留された修復タスクがその保留された期限に達する前に、保留された修復タスクの延長を要求します。修復オーナーは、この要求を行うために保留期日まで待つ必要がなくなりました。

始める前に

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

このタスクについて

脆弱性対応 ワークスペースから延長を要求することもできます。詳細については、「脆弱性マネージャーのワークスペースでの保留された脆弱性一致アイテムの延長の要求」を参照してください。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > 修復タスク.
2. 保留された修復タスクを開きます。
3. [拡張を要求] を選択します。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
拡張期限	保留ステータスが期限切れになり、修復タスクが再アクティブ化される日付を選択します。
理由	問題を保留する理由を入力します。 次の選択肢があります。 ○ メンテナンス期間待ち ○ 修正が利用不可 ○ リスクの受容 ○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. [要求承認] を選択します。

注:

- 要求は 2 段階の承認を経過します。
- [拡張を要求] ボタンは、例外ルールの一部として作成された修復タスクでは使用できません。
- 保留された修復タスクが再度延長されると、バックエンドで延長保留カウントが増加します。

コンフィグレーションコンプライアンス での例外ルールの延長の要求

保留された例外ルールがその保留された期限に達する前に、この例外ルールの延長を要求します。修復オーナーは、この要求を行うために保留期日まで待つ必要がなくなりました。

始める前に

必要なロール：sn_vul.exception_approver

このタスクについて

脆弱性対応 ワークスペースから延長を要求することもできます。詳細については、「脆弱性マネージャーのワークスペースでの保留された脆弱性一致アイテムの延長の要求」を参照してください。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > 例外ルール.

2. 承認済みの例外ルールを選択します。

3. [拡張を要求] を選択します。

4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
拡張期限	例外ルールを延長する必要がある期限の日付を選択します。
理由	例外ルールを保留する理由を入力します。 次の選択肢があります。 ○ リスクの受容 ○ メンテナンス期間待ち ○ 修正が利用不可

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

5. [要求承認] を選択します。
   要求が承認されると、例外ルール、関連する修復タスクの [保留期限]、[理由]、および [補足情報] フィールドが更新されます。要求が送信され、承認者によって後続のアクションが実行されると、メールがトリガーされます。

   注:
   - 要求は 2 段階の承認を経過します。
   - 保留された例外ルールが再度延長されると、バックエンドで延長保留カウントが増加します。

GRC: ポリシーとコンプライアンス管理 を使用して修復タスクに対する例外を要求する

コンフィグレーションコンプライアンス 内の ポリシーとコンプライアンス管理 アプリケーションの GRC ポリシー例外管理機能を使用して、ポリシー例外を要求します。

始める前に
ポリシー例外統合を使用してポリシー例外を要求する前に、ServiceNow Store から GRC: ポリシーとコンプライアンス管理 アプリケーションをダウンロードする必要があります。

必要なロール：sn_vulc.remediation_owner

クラシック UI で例外を要求することもできます。

このタスクについて

重要:
アドミンと修復オーナーは、 脆弱性マネージャーワークスペース と IT 修復ワークスペース でそれぞれ修復タスク (RT) のポリシー例外を要求できます。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

手順

1. 次のように移動する。 **All** (すべて) > アプリケーション脆弱性対応 > アプリケーション脆弱性一致アイテム (または [修復タスク]>[すべて] をクリックし、例外を要求するアイテムまたはグループを開きます。
   選択するアイテムまたはグループは、[オープン]、[調査中]、または [実装待ち] ステータスである必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. 選択したフォームで、[例外の要求] をクリックします。
3. [例外管理] 画面で GRC: ポリシーとコンプライアンス管理 が選択されている場合は、次の操作を行います。

   a. フォームのフィールドに入力します。

   [例外の要求] フォーム

フィールド	説明
ポリシー	例外を要求している脆弱性管理ポリシー。
コントロール目標	選択したポリシーに関連付けられているコントロール目標。ポリシーが選択されていない場合は、すべてのコントロール目標が一覧表示されます。
有効開始日	例外が開始される日付。デフォルト値は現在の日付です。過去の日付にすることはできません。
有効期限	ポリシー例外が期限切れになり、脆弱性一致アイテムまたはグループのステータスが [保留] から [オープン] に変更される日付。 **注:** ポリシー例外が有効である日数を、Policy and Compliance でポリシーに設定した [最大例外期間 (日数)] を超える日数に設定することはできません。詳細については、「ポリシーの作成」を参照してください。
理由	例外を要求する理由。
理由	この要求が行われている理由に関連する詳細情報。このフィールドは修復オーナーが入力する必要があります。

   b. [承認要求] をクリックして例外要求を送信します。
   修復タスクのステータスが [レビュー中] に変わり、ポリシー例外が作成されます。[ステータス変更承認] タブを使用して、例外要求のステータスを追跡します。

   c. [ポリシー例外] 関連リストをクリックして、作成したポリシー例外を確認します。

   d. ポリシー例外番号をクリックします。

   e. [承認者] フィールドで、承認者の名前を選択します。

   f. [ソース] タブをクリックし、[コントロール目標] フィールドからコントロール目標を選択します。

   g. [リスクアセスメント] タブをクリックし、[リスク評価] フィールドからリスク評価を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

h. フォームを保存します。

i. [影響を受けるコントロール] タブをクリックします。

j. [追加] をクリックしてコントロールを追加します。

k. フォームを保存します。

> **注:**
> [コンプライアンスレビューを要求] をクリックすると、コンプライアンスレビューを作成できます。

承認フォームが承認者に送信されます。

承認者は [承認] をクリックして要求を承認するか、[追加の承認を要求] をクリックして追加の承認を要求します。

レコードのステータスが [保留] に変わります。表示されている理由は、例外要求を出したときに選択したものです。[保留] タブにはレコードに関する追加のメモが表示されます。

> **注:**
> 要求が却下された場合、レコードは前のステータスに移行します。

4. **[Submit]** をクリックします。
ポリシー例外統合および修復オーナーとコンプライアンスマネージャー間の引き渡しの詳細については、「ポリシーとコンプライアンス管理オプションのセットアップ」を参照してください。

コンフィグレーションコンプライアンス の例外要求を承認する

すぐに修正できない修復タスクの例外要求を承認します。これらの要求のリスクを評価した上で、修復できるまで保留にすることを承認する必要があります。

> **重要:**
> アドミンまたはアナリストは、脆弱性マネージャーワークスペースからの例外要求を承認または却下できます。詳しくは、「Vulnerability Manager ワークスペース で要求を承認または却下」を参照してください。

始める前に

必要なロール：sn_vulc.exception_approver

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > 自分の承認.
2. キューから要求を選択します。
3. 適切なコメントを添えて、要求を承認または却下します。

> **注:**
> 2 レベルの承認ワークフローの場合、第 1 レベルの承認後、第 2 レベルの承認のために要求が送信されます。第 2 レベルにユーザーがいない場合、要求は第 1 レベルの承認後に自動的に承認されます。
>
> 要求が承認されると、修復タスクは [保留] ステータスに移行します。却下されると、修復タスクは以前のステータスに戻ります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ポリシーの理由のマッピングの定義

例外を要求するすべてのユーザーが使用可能な理由の選択肢を定義できます。

始める前に
必要なロール：sn_vul.compliance.manager および sn_vulc.admin

手順

1. 次のように移動する。 **All** (すべて) > ポリシーとコンプライアンス > ポリシー例外 > 統合レジストリ.

   注:
   [理由の選択肢] テーブルで利用可能な理由の選択肢から選択する方法と、新しい理由を追加する方法があります。

2. [Container Vulnerability Response - CVIT (Container Vulnerability Response - CVIT)] 統合レジストリをクリックします。
3. 既存の理由の選択肢を追加するには、次の手順を実行します。
   a. [理由の選択肢] リストで、[新規] をクリックします。
   b. 虫眼鏡アイコンをクリックし、理由を選択します。
4. [理由の選択肢] テーブルに新しい理由の選択肢を追加するには、次の手順を実行します。
   a. [理由の選択肢] リストで、[新規] をクリックします。
   b. 虫眼鏡アイコンをクリックします。
   c. [新規] をクリックします。
   d. フォームのフィールドに入力します。

[理由の選択リスト] フォーム

フィールド	説明
ラベル	この選択肢の一意のラベル。
値	この選択肢の一意の値。 この値は、それぞれのアプリケーションの [ポリシー例外理由マッピング] テーブルでマッピングされます。このテーブルに移動するには、フィルターナビゲーターに「sn_sec_cmn_policy_reason_mapping.LIST」と入力します。
順序	この選択肢の順序。理由はこの番号に基づいて順序付けされます。
デフォルト	オンデマンドポリシー例外が要求されたときには常にこの理由の選択肢が利用可能であることを示すオプション。統合レジストリにアプリケーション固有の選択肢が入ってい

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	ない場合は、[デフォルト] フィールドが選択されているすべての選択肢が使用可能になります。
有効	理由の選択肢のリストに選択肢を表示するオプション。

5. **[Submit]** をクリックします。

コンフィグレーションコンプライアンス のアナリティクスおよびレポート作成

監視用として次のレポートが提供されています。

コンフィグレーションコンプライアンス 概要レポートにポリシー、CI、テスト、テスト結果を表示します。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

コンフィグレーションコンプライアンス のレポート

コンフィグレーションコンプライアンス のホームページでは、ポリシー、CI、テスト、およびテスト結果を一覧で見ることができ、セキュリティ担当者が懸念事項をすばやく特定するのに役立ちます。コンフィグレーションコンプライアンス の重要度チャートを必要に応じて追加できます。また、グローバル検索機能を使用して、コンフィグレーションコンプライアンス に関連する情報を返すこともできます。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

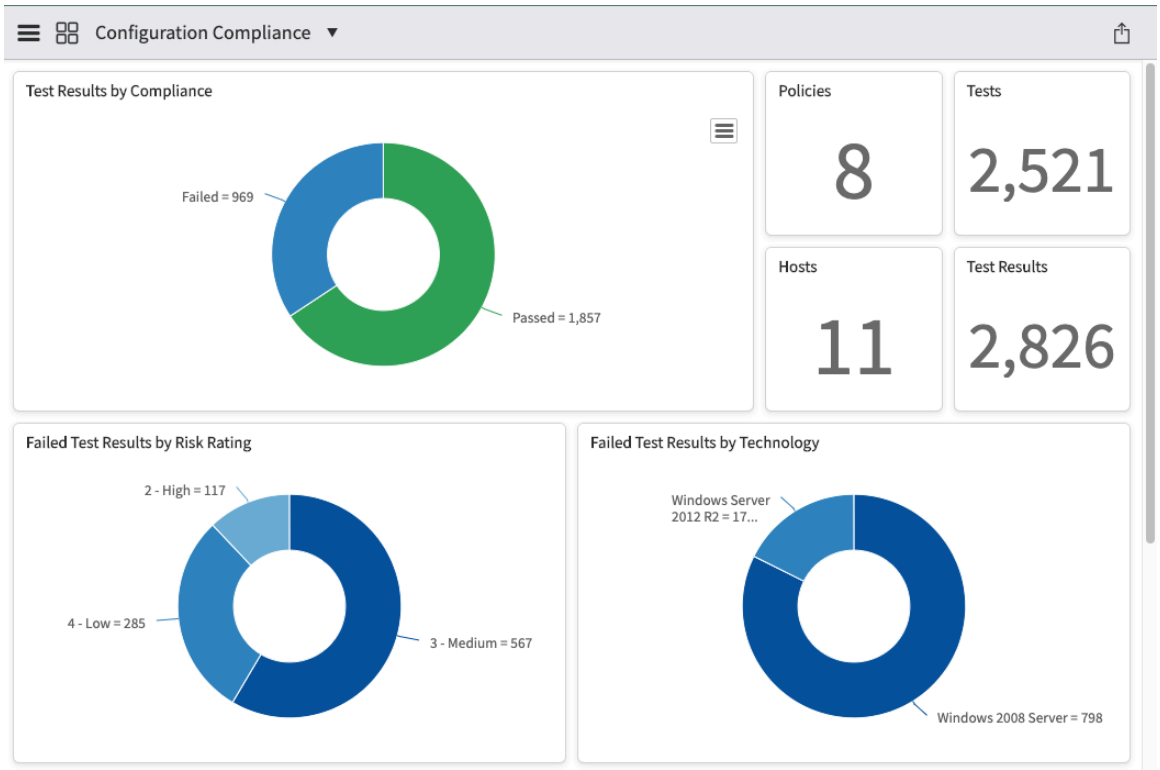
各チャートでは、チャートの任意の部分 (棒、円、データポイント) を指すと、その部分に固有の一般的なデータを表示できます。レポートの任意の部分をクリックすると、詳細な情報を提供するリストが開きます。

注:
sn_vulc.read ロールを持つユーザーは誰でもダッシュボードを表示できます。sn_vulc.write または sn_vulc.admin ロールを持つユーザーは、ダッシュボードを作成および編集できます。ダッシュボードを削除できるのは、sn_vulc.admin だけです。

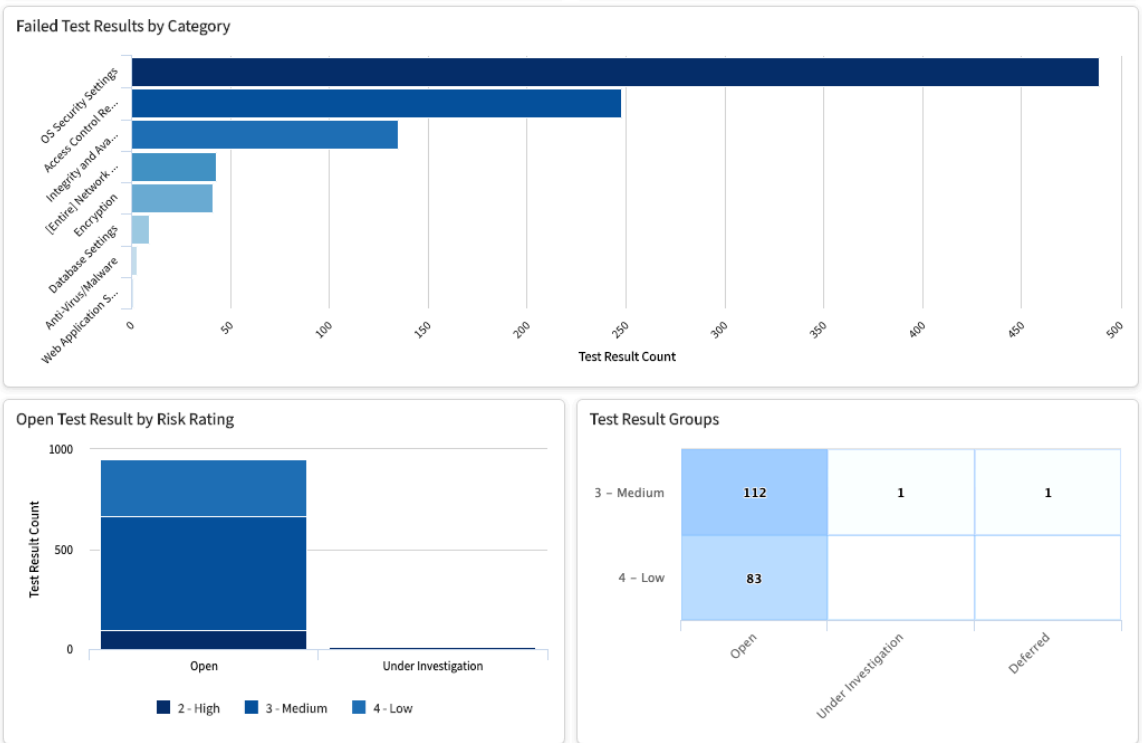
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性概要レポート



Configuration Compliance レポート



脆弱性概要レポート

名前	ビジュアル	説明
コンプライアンス別のテスト結果	ドーナツグラフ	合格または失敗のオープンテストの数を表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性概要レポート (続く)

名前	ビジュアル	説明
ポリシー	数値	失敗したテスト結果のポリシーの数。
テスト	数	失敗したテスト結果のテストの数。
ホスト	数	失敗したテスト結果のホストの数
テスト結果	数	テスト結果の数を表示します。
リスク評価別の失敗したテスト結果	ドーナツグラフ	失敗したテストの数をリスク評価別に表示します。
テクノロジー別の失敗したテスト結果	ドーナツグラフ	失敗したテストのモデルを表示します。
カテゴリ別の失敗したテスト結果	棒グラフ	失敗したテスト結果が最も多いカテゴリを表示します。
リスク評価別のオープンなテスト結果	棒グラフ	オープンなテスト結果の数をリスク評価別に表示します。
修復タスク	チャート	ステータス別およびリスク評価別で修復タスクを表示します。

コンフィグレーションコンプライアンス ダッシュボード

このプラットフォームアナリティクスソリューションには、他の Now Platform 製品とともに使用するために、パッケージ化されたパフォーマンスアナリティクスとレポートのコンテンツが含まれています。 この プラットフォームアナリティクスソリューション によって、非準拠のホストレベルとクラウドコントロールプレーンの構成が可視化されます。

このプラットフォームアナリティクスソリューションには、他の Now Platform 製品とともに使用するためのパッケージ化されたパフォーマンスアナリティクスとレポートのコンテンツが含まれています。このプラットフォームアナリティクスソリューションによって、非準拠のホストレベルとクラウドコントロールプレーンの構成が可視化されます。

コンフィグレーションコンプライアンスのパフォーマンスアナリティクスのダッシュボードには複数のウィジェットが含まれており、さまざまなディメンションのデータが表示されます。コンプライアンスの傾向や構成の問題、修復の傾向、例外管理を、このダッシュボードで総合的に見ることができます。

注:
ネクストエクスペリエンス フレームワークで コンフィグレーションコンプライアンス [PA] ダッシュボードを表示するには、パフォーマンスアナリティクス for コンフィグレーションコンプライアンス プラグインがインストールされている必要があります。インストールされていない場合は、レポートフレームワークを使用してビルドされた既存のダッシュボードが表示されます。

コンフィグレーションコンプライアンス 向け パフォーマンスアナリティクス の有効化

プラットフォームアナリティクスソリューション のコンテンツパック ServiceNow Store アプリケーションをアクティブ化します。

始める前に

この プラットフォームアナリティクスソリューション を有効にしているインスタンス上で パフォーマンスアナリティクス の完全なサブスクリプションバージョンを有効にします。非本番インスタンスでは、サブスクリプションを購入せずに パフォーマンスアナリティクス をアクティブ化できます。詳細については、「パフォーマンスアナリティクスサブスクリプションのアクティブ化」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

検討中のインスタンスのアプリケーションを要求するには、Now Support アカウントと権限が必要です。Now Support アカウントとインスタンスは同じ会社のものである必要があります。詳細については、ServiceNow Store の「ServiceNow 製品のインストール」参照してください。

必要なロール：admin

このタスクについて

コンフィグレーションコンプライアンスダッシュボードの パフォーマンスアナリティクス を使用して、修復タスク、コンプライアンスのステータス、修復アクション、および例外要求に関するレポートを生成します。

手順

1. 次のように移動する。 **All** (すべて) > システムアプリケーション > すべてのアプリケーション > **ServiceNow Store**.
2. パフォーマンスアナリティクス for コンフィグレーションコンプライアンス を参照し、有効なエンタイトルメントが付与されていることを確認します。
3. 「コンフィグレーションコンプライアンスのパフォーマンスアナリティクス」を検索します。
4. アプリケーションをインストールします。

   このアプリケーションをインストールすると、コンフィグレーションコンプライアンス アプリケーションも有効になります。

パフォーマンスアナリティクス **for** コンフィグレーションコンプライアンス ダッシュボードの表示

コンフィグレーションコンプライアンス パフォーマンスアナリティクス (PA) ダッシュボードのレポートを確認することで、最も重要な構成の問題を管理し、迅速に修正できます。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

必要な **Now Platform** ロール

コンフィグレーションコンプライアンス パフォーマンスアナリティクス ダッシュボードには、次のロールが必要です。

- admin：アドミニストレーターは、パフォーマンスアナリティクス for コンフィグレーションコンプライアンス をインストールして有効にし、システムのプロパティを変更することができます。
- pa_admin：パフォーマンスアナリティクスアドミニストレーターは、バックグラウンドジョブ、インジケーター、ブレークダウン、ウィジェット、およびダッシュボードを作成およびレビューできます。このアドミニストレーターは、データ収集を設定して開始することもできます。
- sn_vulc.read：読み取りロールを持つユーザーは、ダッシュボードのデータをレビューできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンフィグレーションコンプライアンス ダッシュボードにアクセスします。

ダッシュボードを開くには、次の場所に移動します。 **All** (すべて) > コンフィグレーションコンプライアンス > 概要.

重要:

コンフィグレーションコンプライアンス のバージョン 14.9 以降、このダッシュボードはネクストエクスペリエンス UI でも表示できます。新しい UI でダッシュボードを表示するには、次に移動します: ワークスペース > 脆弱性マネージャーワークスペース をクリックし、[ダッシュボード] アイコンをクリックします。ロールに応じてデフォルトのダッシュボードが表示されます。他のダッシュボードを表示するには、ダッシュボード名の横にあるドロップダウンをクリックします。詳細については、「脆弱性マネージャーワークスペースのダッシュボード」および「Dashboards in the IT Remediation Workspace (IT 修復ワークスペースのダッシュボード)」を参照してください。

注:
Tokyo を使用している場合は、ネクストエクスペリエンス UI でダッシュボードを表示できますが、一部の機能が失われます。

コンフィグレーションコンプライアンス **[PA]** ダッシュボードのタブ

[概要] タブ

[概要] タブには 5 つのフィルターがあります。これらのフィルターは、[資産カテゴリ]、[クラウドリソースタイプ]、[クラウドサービスプロバイダー]、[クラウドアカウント]、および [クラウドリージョン] で、適用されたフィルターのレポートを可視化するために適用できます。カテゴリを選択して変更を適用すると、そのカテゴリをサポートするすべてのウィジェットが更新されます。各ウィジェットの下部には適用されたフィルターが表示され、ウィジェットのフィルターアイコンには適用されたフィルターの数が付きます。ウィジェット内のレポートをクリックすると、**[KPI** 詳細] タブに追加情報が表示されます。**[KPI** 詳細] タブでは、次のことができます。

- レコードを表示する。
- レコードを比較する。
- グラフのタイプを変更する。
- 日付範囲を選択する。
- 期間に基づいた傾向を確認する。
- [概要] タブで使用できないフィルターを含む追加のフィルターを適用する。たとえば、[ホスト] タグなどです。

次の例は、[概要] タブでフィルターを適用し、**[KPI** 詳細] タブでアクションを実行する方法を示しています。

Configuration Compliance ダッシュボードの [概要] タブ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[コンプライアンス] タブ

[コンプライアンス] タブには、医療保険の相互運用性と説明責任に関する法律(HIPAA)や Data Interchange Standards Association (DISA) など、さまざまな信頼できるソースのコンプライアンス率が表示されます。列ヘッダーフィルターを使用してカテゴリを選択すると、このリストを絞り込むことができます。

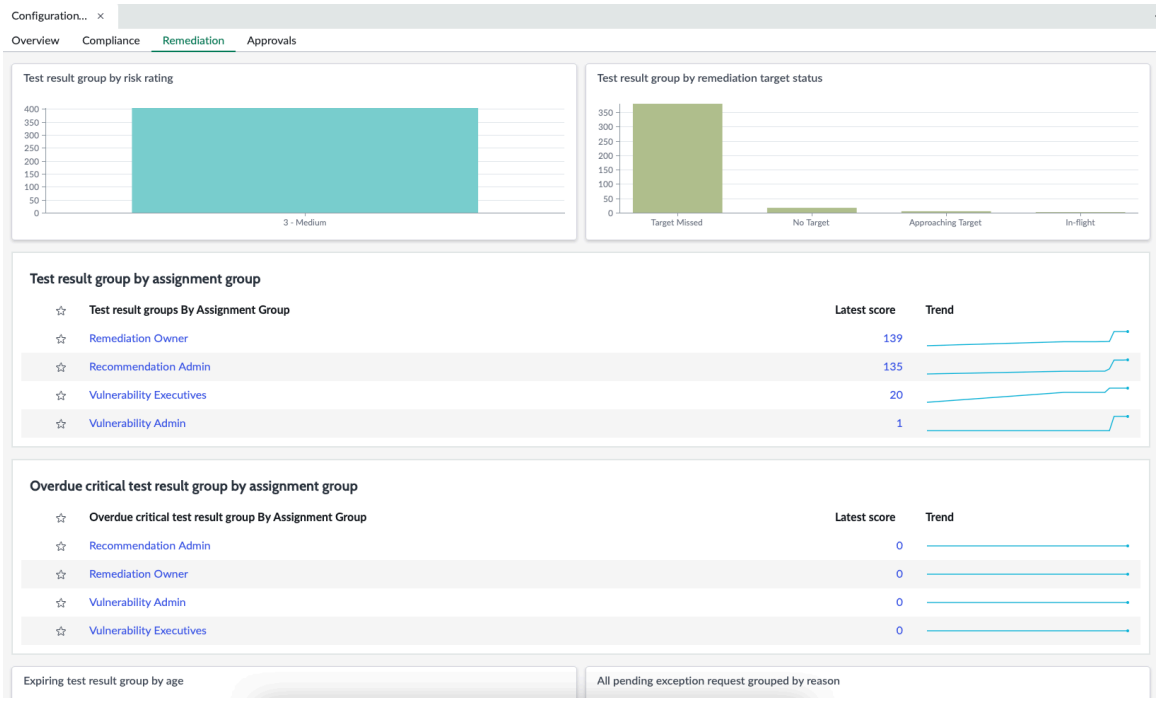
次の例は、[コンプライアンス] タブでデータをフィルタリングする方法を示しています。

Configuration Compliance ダッシュボードの [コンプライアンス] タブ

[修復] タブ

[修復] タブには、修復の進捗状況に関する情報が表示されます。このタブを使用して、構成ミスの修復手段を確認できます。

次の例は、[修復] タブを示しています



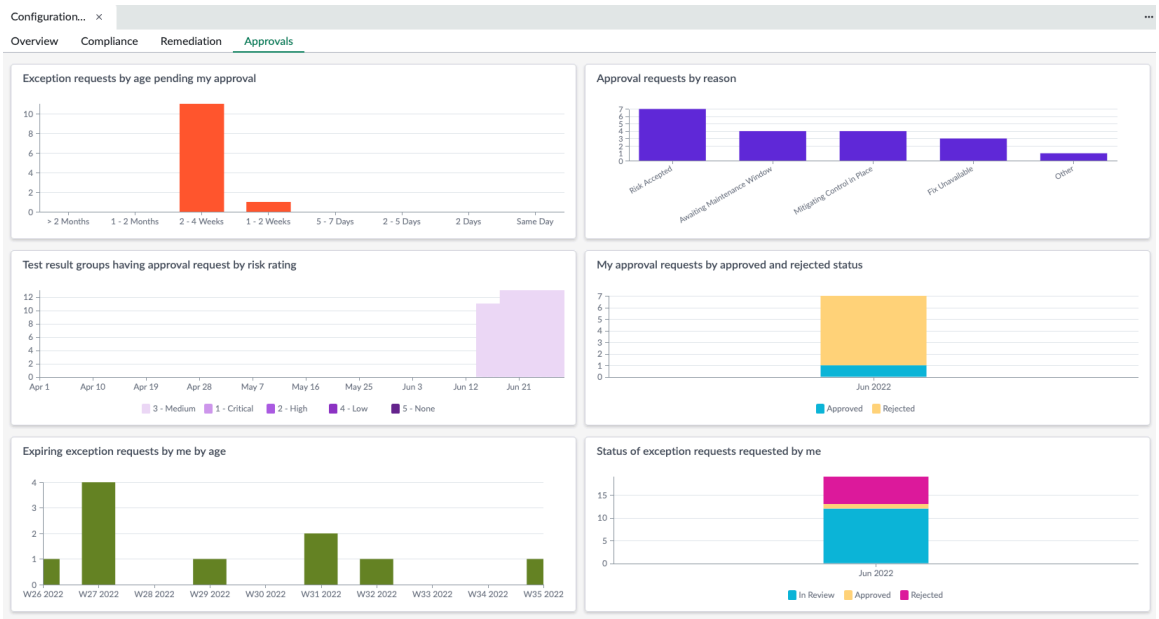
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[承認] タブ

[承認] タブのレポートには、例外要求とその承認ステータスに関する情報が表示されます。

次の例は、[承認] タブを示しています



ブレークダウン

インジケーターで使用されるブレークダウンは次のとおりです。

- 保留理由
- 経過時間
- アサイン先グループ
- 修復ステータス
- 結果
- リスク評価
- 資産カテゴリ
- ホストタグ
- 設定テスト
- クラウドサービスプロバイダー
- クラウドリージョン
- クラウドアカウント
- クラウドリソースタイプ

注:
テスト結果の経過時間とクローズ所要時間の計算をカスタマイズすると、これらのメトリクスを含むパフォーマンスアナリティクス (PA) レポートが急激に増減する可能性があります。テスト結果の経過時間とクローズ所要時間の計算をカスタマイズする方法の詳細については、KB1703270 KB 記事を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィルター

[概要] タブでは、次のフィルターをウィジェットに適用して、フィルタリングされたデータを可視化できます。

名前	タイプ	説明
資産カテゴリ	選択肢	資産の種類。 4 つのオプションは次のとおりです。 • クラウド • コンテナ • インフラ • OT
クラウドリソースタイプ	選択肢	リソースのタイプ。仮想マシンなどです。 統合を実行すると、フィルター内のデータが入力されます。
クラウドサービスプロバイダー	選択肢	クラウドのサービスプロバイダー。 3 つのオプションは次のとおりです。 • Amazon Web サービス (AWS) • Microsoft Azure • Google Cloud Platform (GCP)
クラウドアカウント	選択肢	クラウドサービスでアカウントが作成されたときに作成されるアカウント ID。AWS など。統合を実行すると、アカウント ID のデータがフィルターに入力されます。
クラウドリージョン	選択肢	リソースがホストされている場所。

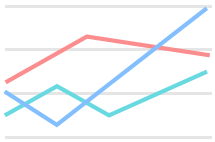
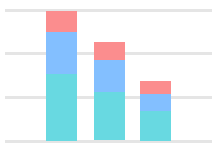
注:
フィルターから複数のオプションを選択して [適用] を選択できます。各ウィジェットに、適用されているフィルターと適用されていないフィルターが表示されます。利用可能なデータに応じてレポートが生成されます。サポートされているフィルターの数もウィジェットに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データの可視化

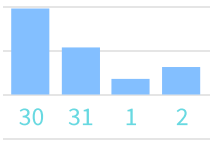
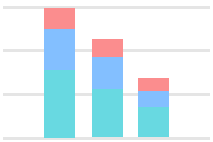
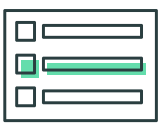
[概要] タブの可視化

レポート名	タイプ	ソーステーブル	説明
コンプライアンスの傾向	線グラフ 	テスト結果	コンプライアンスの傾向 に関する情報。 • リソース：システムで利用可能なリソースの合計数。 • 失敗：1 つ以上のテスト結果が失敗であったリソースの数。 • 合格：すべてのテスト結果が合格ステータスのリソースの数。
修復タスク	単一スコア	テスト結果	システムに存在し、アクティブなステータスになっている修復タスクの数。
期限間近の重大な修復タスク	単一スコア	テスト結果	リスク評価が「重大」であり、修復ステータスが「ターゲット間近」である修復タスクの数。
リスク評価別のテスト結果	棒グラフ 	テスト結果	失敗ステータスのテスト結果。リスク評価に従ってグループ化されます。
経過時間別のテスト結果	棒グラフ	テスト結果	失敗ステータスのテスト結果。テスト結果が作成された時間に従ってグループ化されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

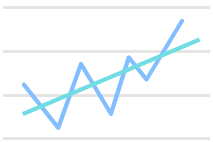
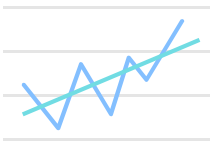
[概要] タブの可視化 (続く)

レポート名	タイプ	ソーステーブル	説明
			注: テスト結果の経過時間とクローズ所要時間の計算をカスタマイズすると、これらのメトリクスを含むパフォーマンスアナリティクス (PA) レポートが急激に増減する可能性があります。テスト結果の経過時間とクローズ所要時間の計算をカスタマイズする方法の詳細については、KB1703270 KB 記事を参照してください。
修正ターゲット遵守別のクローズ済みテスト結果	棒グラフ 	テスト結果	このテストがクローズされたことを示す合格ステータスのテスト結果。
アサイン先グループ別の期限切れの重大なテスト結果	リストとスコア 	テスト結果	リスク評価が「重大」であり、修復ステータスが「ターゲット経過」であるテスト結果の数。レポートは、テスト結果が [オープン] ステータスであることを示しています。テスト結果が修復ターゲットの日付を過ぎると、期限切れとみなされます。
期限切れのテスト結果 - サービス	リスト、スコア、および傾向	サービスの PA ダッシュボードデータベースビュー	修復ステータスが「ターゲット経過」であるサービスのテスト結果の数。このレポートには、テスト結果が最も良いサービスまたは部門の名前も表示されます。

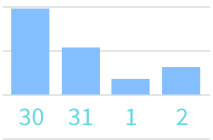
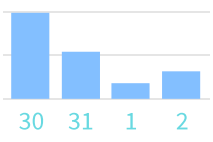
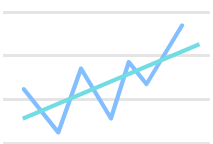
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[概要] タブの可視化 (続く)

レポート名	タイプ	ソーステーブル	説明
			
期限切れのテスト結果 - サービスオーナー	リスト、スコア、および傾向	サービスの PA ダッシュボードデータベースビュー 	修復ステータスが「ターゲット経過」であるサービスオーナーのテスト結果の数。このレポートには、テスト結果が最も良いサービスまたは部門の名前も表示されます。

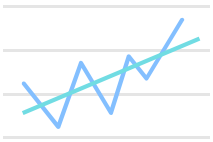
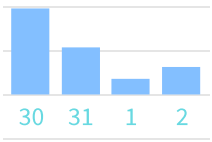
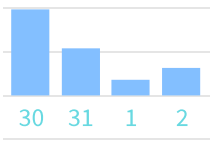
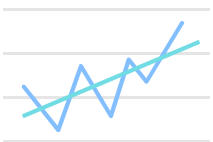
[修復] タブの可視化

タイトル	タイプ	ソーステーブル	説明
リスク評価別の修復タスク	棒グラフ 	修復タスク	アクティブ状況であるすべてのテスト結果グループのリスク評価のブレークダウン。
修復ターゲットステータス別の修復タスク	棒グラフ 	修復タスク	テスト結果グループのうち、ターゲットを達成できなかったものと、ターゲットがないものと、ターゲット間近のものすべての、修復ターゲットのブレークダウン。
アサイン先グループ別の修復タスク	リスト、スコア、および傾向	修復タスク 	修復タスクのアサイン先グループに基づくブレークダウン。

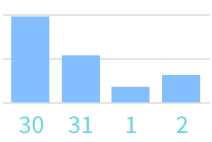
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[修復] タブの可視化 (続く)

タイトル	タイプ	ソーステーブル	説明
アサイン先グループ別の期限切れの重大な修復タスク	リスト、スコア、および傾向	修復タスク 	修復タスクのアサイン先グループに基づくブレークダウン。これらの修復タスクのリスク評価は「重大」であり、修復ターゲットは達成されていません。
経過時間別の期限切れが迫る修復タスク	棒グラフ 	修復タスク	特定の期間内に期限切れになる修正タスク。最大 10 個の期間バケットを作成できます。
理由別にグループ化されたすべての処理待ちの例外要求	棒グラフ 	ステータス変更承認	例外の理由ごとにグループ化されたステータス変更承認要求。
アサイン先グループ別のテスト結果の重大な例外	リスト、スコア、および傾向	テスト結果 	アサイン先グループに基づいてグループ化した、保留中および重大なステータスのテスト結果。

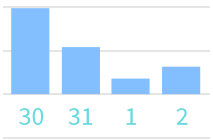
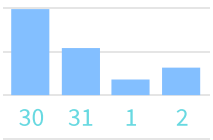
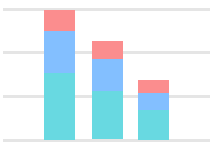
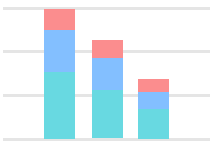
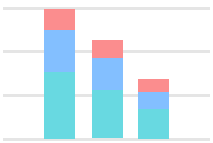
[承認] タブの可視化

レポート	タイプ	ソーステーブル	説明
自分の承認処理待ちのの時間別の例外要求	棒グラフ 	承認	自分が作成した、承認処理待ち状態の例外要求。要求は、要求の期間に応じてグループ化されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[承認] タブの可視化 (続く)

レポート	タイプ	ソーステーブル	説明
理由別の承認要求	棒グラフ 	ステータス変更承認	例外の作成に対する、例外の理由を含めたステータス変更承認要求。
リスク評価別の承認要求がある修復タスク	棒グラフ 	修復タスク	重大度に基づいた承認要求がある修復タスク。
[承認] および [却下] ステータス別の自分の承認要求	棒グラフ 	ステータス変更承認	承認および却下のステータスごとにグループ化された例外要求。
経過時間別の自分が行った期限切れ例外要求	棒グラフ 	ステータス変更承認	今後数週間で期限切れになる例外要求。例外要求は週ごとにグループ化されます。 例外要求が作成されるたびに、例外要求の有効期限日が選択されます。要求の経過時間はこの日付に基づいて計算されます。
自分が要求した例外要求のステータス	棒グラフ 	ステータス変更承認	自分が作成し、次のステータスに従ってグループ化された例外要求。 • レビュー中 • 承認済み • 却下

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

の集計レポートフレームワーク コンフィグレーションコンプライアンス

集計レポートフレームワークを使用すると、複雑で長時間実行されるオンザフライクエリを含むデータのレポートを作成して、パフォーマンスを向上させることができます。

集計されたレポートフレームワークは、次の方法でパフォーマンスを向上させます。

- より少ないリソース使用量で、迅速にレポートをレンダリングする
- データを集計し、集計とブレークダウン ([グループ分け基準]) を再利用する
- データベースへの照会を減らす

構成テスト結果が 100 万件を超える場合は、標準レポートと一緒に集計レポートフレームワークを使用します。

必要なロール

このソリューションには、次のロールとタスクが関連付けられています。

- Now Platform アドミン (admin)：この プラットフォームアナリティクスソリューション をインストールしてアクティブ化し、システムのプロパティに必要な変更を加えます。
- パフォーマンスアナリティクス アドミン (pa_admin)：集計、ウィジェット、およびダッシュボードを確認します。データ収集を設定して開始します。適切なステークホルダーとダッシュボードを共有します。
- アドミン (sn_vul_cmn.admin)：集計を作成します。
- VR 書き込み (sn_vul_cmn.write)：集計および集計結果のデータを編集します。
- VR 読み取り (sn_vul_cmn.read)：集計および集計結果のデータを確認します。
- 脆弱性アナリスト [sn_vul.vulnerability_analyst]：集計結果を確認します。

関連情報

ソースデータの集計を構成する

複数の集計を同時に実行する

同時に実行できる集計の数を構成する

集計を使用してレポートを作成する

コンフィグレーションコンプライアンス の参照情報

コンフィグレーションコンプライアンス アプリケーションがアクティブ化されると、テーブル、スケジュール済みジョブ、ユーザーロールなど、いくつかのタイプのコンポーネントがインストールされます。

次のトピックでは、コンフィグレーションコンプライアンス にあるフォームやレコードのフィールドデータの他に、参照情報、トラブルシューティングについて説明します。

- コンフィグレーションコンプライアンスと一緒にインストールされるコンポーネント
- テスト結果フォームのフィールド
- コンフィグレーションコンプライアンス のインポートに関する問題を解決する
- Qualys PC 結果の開始日を変更する

コンフィグレーションコンプライアンスと一緒にインストールされるコンポーネント

いくつかのタイプのコンポーネント (テーブル、ユーザーロールなど) が、コンフィグレーションコンプライアンスプラグインのアクティブ化とともにインストールされます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

コンフィグレーションコンプライアンス の v15.1.5 以降、最も頻繁に使用されるシステムプロパティに コンフィグレーションコンプライアンス アプリケーション内でアクセスできるようになりました。これらのシステムプロパティを表示するには、次に移動します: **All** (すべて)コンフィグレーションコンプライアンスプロパティ.

注:
アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「アプリケーションとともにインストールされているコンポーネントの検索」を参照してください。

この機能ではデモデータを利用できます。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

アプリケーションとともにインストールされるコンポーネントのフィルター済みリストの表示

アプリケーションファイルテーブルをフィルタリングして、アプリケーションとともにインストールされたロール、スケジュール済みジョブ、およびテーブルのみを表示します。これらのコンポーネントを表示するアプリケーションは、そのファイルがインスタンスとメタデータテーブルにロードされるようにインストールする必要があります。アプリケーションファイルテーブルからフィルター済みリストを表示するには、次の手順に従います。

1. フィルターナビゲーターで、「**sys_metadata.list**」と入力してメタデータテーブルに移動します。
2. 条件ビルダー (フィルターアイコン) を選択し、次を選択します。 アプリケーション > 次の値に等しい その後にアプリケーションの名前が続きます。たとえば アプリケーション > 次の値に等しい > 脆弱性対応.
3. 条件ビルダーで 2 番目のフィルターを追加するには、[**AND**] を選択してから次を選択します。 クラス > は をクリックし、リストから [ロール]、[スケジュール済みジョブ]、または [テーブル] のいずれかのクラスを選択します。
4. **[Run** (実行)] を選択します。

選択したクラスの結果がフィルター済みリストに表示されます。

インストールされるロール

ロール タイトル [名前]	説明	含んでいるロール
コンフィグレーションコンプライアンス アドミニストレーター	コンフィグレーション コンプライアンスア	sn_vulc.write

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロール タイトル [名前]	説明	含んでいるロール
[sn_vulc.admin]	プリケーションのアプリケーションプロパティ、構成、更新ルール、統合を変更できます。v15.0 以降では、管理者ユーザーは エクスプロイト、CVE などのソースレコードを削除できません。	**注:** コンフィグレーションコンプライアンスアプリケーションのレコードの管理に必要なロールを継承します。
read [sn_vulc.read]	コンフィグレーションコンプライアンスでリストやレコードを読み取ります。 **重要:** 脆弱性対応 v24.0 以降、sn_vulc.read ロールにはVulnerability Manager ワークスペースにアクセスする権限があります。	• sn_sec_cmn.calc_read • sn_vul.view_manager_workspace
書き込み [sn_vulc.write]	Configuration Compliance でリストやレコードを書き込みます。	• sn_vulc.read • sn_vulc.remediation_owner
書き込みアサイン [sn_vulc.write_assignment	テスト結果のアサインフィールドに書き込みます。	sn_vulc.remediation_owner ロールに含まれています。
修復オーナー sn_vulc.remediation_owner	自分または自分のグループにアサインされたテスト結果の権限を表示および更新します。	itil ロールに含まれています。 次を含む： • sn_sec_cmn.read • sn_vulc.write_assignment • sn_vul.view_rem_workspace
CC.System sn_vulc.import_admin	コンフィグレーションコンプライアンスアプリケーションですべてのスケジュール済みジョブを実行します。	• sn_vulc.write • import_admin • sn_vul_tenable.read_integration

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロール タイトル [名前]	説明	含んでいるロール
	注: このユーザーは、コンフィグレーションコンプライアンスのすべてのスケジュール済みジョブのデフォルトの実行ユーザーです。	
VRCommon.System sn_vul_cmn.admin	脆弱性対応共通アプリケーションのすべてのスケジュール済みジョブのデフォルトの実行ユーザー。	• sn_vul_cmn.write • sn_sec_cmn.admin • report_admin
SecCommon.System sn_sec_cmn.admin	Security Support Common アプリケーションのバックグラウンドジョブ機能に使用される、すべてのスケジュール済みジョブのデフォルトの実行ユーザー	• sn_sec_cmn.int_write • sn_sec_cmn.write • workflow_admin • sn_sec_cmn.calc_write • sn_sec_core.read_dictionary • sn_sec_cmn.manage_approval_rules • sn_sec_int.admin • sn_sec_cmn.cap_email_write • sn_sec_cmn.manage_classification_rules • sn_sec_cmn.manage_background_job
V14.7：sn_vulc.edit_watch_topic	コンフィグレーションコンプライアンスの監視トピックを編集します。	sn_vulc.read_watch_topic
V14.7：sn_vulc.read_watch_topic	コンフィグレーションコンプライアンスの監視トピックを読み取ります。	cmdb_read
V14.7：sn_vulc.create_watch_topic	Configuration Compliance の監視トピックを作成します。	sn_vulc.read_watch_topic
sn_vulc.auditor	すべてのコンフィグレーションコンプライアンスモジュールの読み取りを許可	sn_vulc.read sn_vulc.advanced_read
sn_vulc.advanced_read	すべてのコンフィグレーションコンプライ	sn_vulc.read_auto_close_rules sn_vulc.read_exception_configuration

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロール タイトル [名前]	説明	含んでいるロール
	アンス管理モジュールの読み取りを許可	sn_vulc.read_assignment_rules sn_vulc.read_task_rules sn_vulc.read_auto_exception_rule sn_vulc.read_notifications sn_vulc.read_risk_score_configuration sn_vulc.read_test_criticality_mapping sn_sec_cmn.read_approval_rules sn_vulc.read_auto_delete sn_vulc.read_remediation_target_rules
sn_vulc.read_test_criticality_mapping	テスト重要度マッピングの読み取りを許可	
sn_vulc.read_task_rules	修復タスクルールの読み取りを許可	
sn_vulc.read_assignment_rules	アサインルールの読み取りを許可	
sn_vulc.read_risk_score_configuration	リスクスコア設定の読み取りを許可	
sn_vulc.read_auto_close_rules	自動クローズ構成の読み取りを許可	
sn_vulc.false_ positive_approver	クローズ時の修復タスクを誤検出として承認/却下できる	sn_vul.view_manager_workspace
sn_vulc.exception_approver	例外要求を承認または却下します。	sn_vul.view_manager_workspace
sn_vulc.delete	ソースレコードを削除	

自動翻訳

インストールされるスケジュール済みジョブ

スケジュール済みジョブ	説明
V15.0：構成テストでテストグループを更新	Tenable および Microsoft Defender ソースのテストに関するテストグループを更新します。これは 1 回限りのジョブです。
V15.0：既存のテスト結果フィールドへの入力	テスト結果テーブル、保存されたフィルター、およびモジュールに新しく追加された列 (経過時間、クローズした経過時間、アクティブなど) に値を更新します。これは 1 回限りのジョブです。
V15.0：脆弱性一致 CI テーブルの入力 - テスト結果の削除と再入力	[脆弱性一致 CI] テーブルの合計レコードを入力します。これは 1 回限りのジョブです。
バージョン 12.0	修復タスクレコードのステータスメトリクスの値を計算して更新します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みジョブ	説明
すべてのテスト結果グループの修復メトリクスを算出する	
バージョン 12.0： すべてのテスト結果の修復メトリクスを算出する	テスト結果レコードのステータスメトリクスの値を計算して更新します。
バージョン 12.0： 変更要求状況の同期	既存のすべての修復タスク (RT) の状況を変更要求 (CHG) と同期するオンデマンドジョブ。変更要求のライフサイクルが進むと、関連する修復タスクの状況も自動的に変化します。今後のステータスの同期を有効にします。
バージョン 11.1： テスト結果グループの保留を確認 有効期限	修復タスクが期限切れになった場合 (および 1 週間以内に期限切れになる場合) に通知を送信します。
Configuration Compliance CI 数	構成アイテム数 [sn_vulc_cc_configuration_item_count] テーブルに個別の構成アイテム (CI) 数と 90 日間ローリング平均を入力します。
バージョン 11.1：修復ターゲットの評価と通知	すべてのテスト結果の修復ターゲット日を設定または更新します。ルールに対する修復ターゲット日のステータスを決定します。通知を送信
V14.7：統一された修復タスクへのテスト結果グループの挿入	クラシック UI で作成されたすべての修復タスクを統一された修復タスク (sn_vul_remediation_task) に挿入するための 1 回限りのスケジュール済みジョブ。
バージョン 12.0： CR および CR-Parent の CR-TRG m2m を入力	修復タスクの変更要求を設定します。
v11.1 で削除：保留されたテスト結果グループを再オープン **注:** 11.1 より前のバージョンでは廃止されました。使用しないでください。	期日が過ぎたときに保留グループを再オープンします。
すべてのアサインルールを再適用	すべてのアサインルールを再適用します。
バージョン 14.3：アサインルールの再アサイン回数	毎日実行され、この機能によって特定のアサインルールに対してアサインされていないテスト結果と修復タスクの合計数を提示します。
テスト結果グループのステータスを再評価	**assess_state** が false であるエントリーに対して修復タスクのステータスを再評価します。15 分ごとに実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みジョブ	説明
テスト結果リスクスコアをテスト結果グループと構成にロールアップ test	1 時間ごとに実行され、変更された構成テストと修復タスクのロールアップスコアを計算します。 • sn_vulc_test_manifest のすべてのテストについてロールアップリスクスコアを計算し、完了時にマニフェストレコードを削除します。 • sn_vulc_result_group_manifest のすべてのテストについてロールアップリスクスコアを計算し、完了時にマニフェストを削除します。
バージョン 12.0： ポリシー修復メトリクスの更新	コンフィグレーションコンプライアンスの v15.0 以降では、このスケジュール済みジョブは「修復メトリクスの更新」に名前が変更されています。 • ポリシーレコードのステータスメトリクスの値を計算して更新します。 • 検出されたアイテムの CI のテスト結果コンプライアンスの % を計算します。
バージョン 14.3：保留数の設定	テスト結果または修復タスクが保留された回数を収集します。
テスト結果のリスク評価を更新	テスト結果のリスク評価を更新します。
クローズされていないすべての結果グループと構成テストのロールアップリスクスコアを更新	クローズされていないすべての結果グループと コンフィグレーションコンプライアンス テストのロールアップリスクスコアを更新します。

インストールされるテーブル

テーブル	説明
アサインルール [sn_vulc_assignment_rule]	テスト結果にアサイン先グループを設定するために評価される一連のルールが含まれます。
信頼できるソース [sn_vulc_auth_src]	インポートされた信頼できるソースを保存します。
算出 [sn_vulc_calculator_risk_score]	特定の条件が満たされたときに、特定のテスト結果フィールドを設定する算出が含まれます。
CC 構成アイテム数 [sn_vulc_cc_configuration_item_count]	構成アイテムの合計数が含まれます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
バージョン 12.0：変更要求の関連付け [sn_vulc_action_associate_cr]	変更要求を修復タスクに関連付けるために使用されるステージングテーブル。
バージョン 12.0：変更要求の作成 [sn_vulc_action_create_cr]	変更要求フォームの作成に使用されるステージングテーブル。
バージョン 12.0：変更要求のフォーム [sn_vulc_cr_form]	変更要求の管理用ベーステーブル。
引用 [sn_vulc_citation]	インポートされた引用が含まれます。
設定テスト [sn_vulc_test]	インポートされた構成テストデータが含まれます。
構成テストマニフェスト [sn_vulc_test_manifest]	ロールアップリスクスコアを算出する必要がある構成テストが含まれます。
バージョン 12.2 不足している資産テーブル [sn_vul_missing_asset]	一致しない資産を含むインポートされたコンフィグレーションコンプライアンスアセスメントデータに対応する一時的な資産レコードが含まれます。
設定テストテクノロジー [sn_vulc_test_technology]	インポートされた構成テストテクノロジーが含まれます。
修復タスクルール [sn_vulc_grouping_rule]	一連のテスト結果に対してグループを自動的に作成する基準を定義するルールが含まれます。
テストグループ [sn_vulc_policy]	インポートされたポリシーが含まれます。
ポリシー設定テスト [sn_vulc_policy_test]	インポートされたポリシー構成テストデータが含まれます。
修復ターゲットルール [sn_vulc_ttr_rule]	テスト結果の修復予定期間を定義します。
リスク算出 [sn_vulc_calculator_group]	コンフィグレーションコンプライアンス 算出のグループ化が含まれます。算出グループの順序によって最初に評価されるグループが決まり、各グループで最大 1 つの算出が使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
リスクスコアロールアップ算出 [sn_vulc_risk_score_rollup]	ロールアップ算出の構成が含まれます。
修復タスクを分割 [sn_vulc_action_split_trg]	修復タスクの分割に使用されるステージングテーブル。
ステート変更承認 [sn_vulc_state_change_approval]	承認ステータスのプロセスデータが含まれます。
テクノロジー [sn_vulc_technology]	インポートされたテクノロジーが含まれます。
重要度マップのテスト [sn_vulc_test_criticality_map]	重要度マップデータが含まれます。
テスト結果 [sn_vulc_result]	インポートされたテスト結果が含まれます。
修復タスク [sn_vulc_result_group]	インポートされた修復タスクが含まれます。
バージョン 12.0： 修復タスク変更要求	修復タスクの変更要求が含まれます。
修復タスクマニフェスト [sn_vulc_result_group_manifest]	ロールアップリスクスコアを算出する必要がある修復タスクが含まれます。
修復タスク [sn_vulc_m2m_result_result_group]	修復タスクデータが含まれています。
テスト結果の履歴 [sn_vulc_result_history]	インポートされたテスト結果履歴が含まれます。
テスト結果の修復ステータス	直近で適用された修復ターゲットルールに対するテスト結果のステータス。
V14.7：監視トピックテスト数	脆弱性マネージャーワークスペースの [個別の構成テスト] タブのキャッシュテーブル。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
[sn_vulc_wt_test_counts]	

コンフィグレーションコンプライアンス テストグループの表示

サードパーティスキャンの結果をインスタンスにインポートすると、テストグループレベルでテストのコンプライアンスを確認できます。そのテストグループと関連付けられているテストレコードの監査の前に、このビューを使用します。

始める前に
必要なロール：表示する場合、sn_vulc.read and sn_vulc.remediation_owner

このタスクについて
ポリシーはインポートされたレコードであり、コンフィグレーションコンプライアンス 内では編集できません。

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > テストグループ.
   テスト結果のリストが表示されます。コンフィグレーションコンプライアンス v15.0 以降では、[テスト結果のコンプライアンス率 **(%)**] 列に、テストグループにおいてテストに準拠しているテスト結果の割合が表示されます。

   テスト結果のコンプライアンス率 (%) = (テストグループでクローズされたテスト結果の数 / テストグループに関連付けられたテスト結果の合計数) x 100

2. 表示するテストグループの [簡単な説明] をクリックします。

コンフィグレーションコンプライアンス のテストグループフォームフィールド

フィールド	説明
ソース	サードパーティスキャナーのシステム名、または コンフィグレーションコンプライアンス との通信に使用される API の ServiceNow プラグインに入力された名前。
テクノロジー	サードパーティのスキャナーアプリケーションのテストグループに関連付けられているテクノロジーのリスト。
ソース ID	サードパーティスキャナーによってテストグループにアサインされた識別子。
ソース作成	サードパーティのスキャナーアプリケーションでテストグループが定義された日時。
ソース更新	サードパーティのスキャナーアプリケーションでテストグループが最後に変更された日時。
簡単な説明	サードパーティのスキャナーアプリケーションでテストグループにアサインされたサマリーの説明またはタイトル。
説明	サードパーティのスキャナーアプリケーションで定義されたテストグループの詳細な説明。
テスト	このテストグループを参照するテストのリスト。サードパーティのスキャナーからインポー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	トされます。必要に応じて、リストから特定のテストに関する詳細情報に移動できます。
修復ステータス (バージョン **12.0)**	
保留を除外する	これらの値には、保留されたテスト結果の CI は含まれません。 ○ [残りの **CI]**：このポリシーのアクティブなテスト結果 ([クローズ済み] 以外のステータス) のある構成アイテム (CI) の数 (カウント)。 ○ [修復された **CI** の割合 **(%)]**：このテストグループに準拠する CI の割合。この数には、保留されたテスト結果を持つ CI は含まれません。 ○ [合計 **CI]**：このテストグループによって影響を受ける CI の合計数。この数には、保留されたテスト結果は含まれません。
保留を含める	値は、すべてのアクティブなテスト結果 ([クローズ済み] 以外のステータス) の CI を表します。 ○ [残りの **CI]**：このテストグループが適用されているクローズ済みではない、1 つ以上のテスト結果に関連付けられた一意の CI の数。 ○ [修復された **CI** の割合 **(%)]**：このテストグループに準拠する CI の割合。 ○ [合計 **CI]**：このテストグループによって影響を受ける CI の合計数。

バージョン 12.0 以降では、これらの値をオンデマンドで更新するには、 [修復ステータス] タブで [ステータスを更新] 関連リンクをクリックします。データがリフレッシュされていることを示すメッセージが表示されます。[ステータスを表示] リンクをクリックして、更新の進捗状況を表示します。しばらくすると、前回のスケジュール済みジョブ以降に変更または更新されたデータがあれば、レコードをリフレッシュします。更新されたフィールド値がリフレッシュされます。

3. オプション: テストグループのテスト結果のインポートを無効化するには、[インポートを無効にする] ボタンを選択します。

   (Optional) [インポートが無効である] 列の値が *true* に変わります。テストグループのテスト結果は、次回の取り込みからインポートされません。

   > **注:**
   > [インポートを無効にする] ボタンは、Qualys スキャナーから取得したテスト結果でのみ使用できます。

   脆弱性対応 v23.0 以降：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- Vulnerability Manager ワークスペース で Qualys テストグループにおけるテスト結果のインポートを有効化または無効化することができます。詳細については、「Qualys テストグループのテスト結果のインポートを有効または無効にする」を参照してください。
- [廃止をマーク] ボタンの名前が [インポートを無効にする] に変更されました。
- [使用廃止] 列の名前が [インポートが無効である] に変更されました。

コンフィグレーションコンプライアンス の信頼できるソースの表示

このモジュールを使用して、信頼できる各ソースに関するサマリー情報を表示し、レコードの作成に使用されたソース公開を調査します。

始める前に

必要なロール：

- 更新する場合、sn_vulc.admin
- 表示する場合、sn_vulc.remediation_owner

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > サポートデータ > 信頼できるソース.
2. 表示する信頼できるソースの [簡単な説明] をクリックします。

コンフィグレーションコンプライアンス の信頼できるソースのフォームフィールド

フィールド	説明
数値	インポートプロセス中にインスタンスによって信頼できるソースにアサインされた ID 番号。
ソース	サードパーティのスキャナーアプリケーションのシステム名、または コンフィグレーションコンプライアンス と通信する API のスキャナープラグインに入力された名前。
ソース ID	サードパーティのスキャナーによって信頼できるソースにアサインされた識別子。
簡単な説明	サードパーティのスキャナーでこの信頼できるソースに与えられた名前。
パブリッシャー	この信頼できるソースの元の情報源である組織または公開の名前。
信頼できるソースコンテンツ	テスト結果に関する引用情報のリスト。サードパーティのスキャナーからインポートされます。必要に応じて、このリストから特定のテストに関する詳細情報に移動できます。

3. オプション: [公開者] を追加します。
4. [更新] をクリックします。
5. [削除] をクリックすると、このレコードを削除できます。
インスタンスからレコードを削除します。サードパーティ統合でまだ使用中の場合は、次のインポートで返されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンフィグレーションコンプライアンス テクノロジーの表示

このモジュールを使用して、信頼できる各ソースと引用 (Qualys では フレームワークとも呼ばれる) に関するサマリー情報を表示します。レコードの作成に使用されたソース公開を調査できます。

始める前に
必要なロール：

- 更新する場合、sn_vulc.admin
- 表示する場合、sn_vulc.remediation_owner

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > サポートデータ > テクノロジー.
2. 表示する信頼できるソースの [簡単な説明] をクリックします。

コンフィグレーションコンプライアンス の信頼できるソースのフォームフィールド

フィールド	説明
数値	インポートプロセス中にインスタンスによって信頼できるソースにアサインされた ID 番号。
ソース	サードパーティのスキャナーのシステム名、または コンフィグレーションコンプライアンス と通信する API のサードパーティのスキャナープラグインに入力された名前。
ソース ID	サードパーティのスキャナーによって信頼できるソースにアサインされた識別子。

3. [削除] をクリックすると、このレコードを削除できます。
インスタンスからレコードを削除します。サードパーティ統合でまだ使用中の場合は、次のインポートで返されます。

コンフィグレーションコンプライアンス のテストの表示

このモジュールを使用して、これらのテストに関する詳細情報を調べます。作成時に使用されたエキスパートソースの引用、それらが使用されているサードパーティの構成ポリシー、およびスキャンで取得された結果が含まれています。

始める前に
必要なロール：

- 更新する場合、sn_vulc.admin
- 表示する場合、sn_vulc.remediation_owner

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > コントロール.
2. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > テスト
3. リストから、表示するコントロール (コンプライアンステスト) を開きます。

バージョン 12.0 以降では、これらの値をオンデマンドで更新するには、 [修復ステータス] タブで [ステータスを更新] 関連リンクをクリックします。データがリフレッシュされていることを示すメッセージが表示されます。[ステータスを表示] リンクをクリックして、更新の進捗状況を表示します。しばらくすると、前回のスケジュール済みジョブ以降に変更または更新されたデータがあれば、レコードをリフレッシュします。[リスクスコア]、[リスク評価]、[修復ターゲット日]、[ステータス] などのフィールド値、および [修復ステータス] タブのフィールドが更新されます。

コンフィグレーションコンプライアンス のテストのフォームフィールド

フィールド	説明
数値	インポートプロセス時にコントロールにアサインされた番号。
結果	スキャンのステータス。合格または失敗。このテストが複数の修復タスクに属する場合、そのステータスは優先順位に従って決定されます。
ソース	サードパーティ統合アプリケーションのシステム名、または コンフィグレーションコンプライアンス との通信に使用される API のプラグインに入力された名前。
重要度	サードパーティ統合で定義された、コントロールに関連する構成の問題の重大度。重要度のレベルは、脆弱性対応 で利用可能な類似する脆弱性インジケーターの粒度に合わせて調整されます。次のレベルがあります。 重大 コントロールに関連する構成の問題は、1 つ以上の事業上重要な CI の中断を引き起こしています。 高 コントロールに関連する構成の問題は脅威ではありますが、重要なネットワークリソースのシャット

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	ダウンを引き起こしているわけではありません。 中 コントロールに関連する構成の問題はリスクではありますが、差し迫った脅威ではありません。 低 コントロールに関連する構成の問題は低レベルの脅威であり、よりリスクの高い CI を優先して無視できます。 マイナー コントロールに関連する構成の問題は軽微なリスクであり、必要に応じて無視できます。
ソース ID	サードパーティ統合によってコントロールにアサインされた識別子。
カテゴリ	サードパーティベンダーによってこのタイプのコントロールに付与された主要な分類カテゴリ。
リスクスコア	ロールアップリスクスコアです。このリスクスコアは、「クローズ済み」ではない ([オープン]、[調査中]、[実装待ち]、[保留中]、[解決済み]) すべてのテスト結果における最大リスクスコアから 85%、「クローズ済み」ではないテスト結果数の 15% のスコアで、重み付けされています。リスクスコア算出によって計算された値で、テスト結果のビジネス上の重要度とテストの重要度の各値に基づいているものです。
サブカテゴリ	サードパーティベンダーによってこのクラスのテストにアサインされたサブカテゴリ。
リスク評価	リスクスコア範囲に基づき、全体的なリスクを [1 - 重大] ～ [5 - なし] の 1 ～ 5 の数値スケールで評価します。このフィールドは、以前のバージョンの [Priority (優先度)] フィールドに代わるものです。
テクノロジー	このテストの対象となるテクノロジーのリスト。
ソース作成	サードパーティ統合でテストが最初に定義された日付。
ソース更新	サードパーティ統合でテストが最後に更新された日付。
簡単な説明	サードパーティ統合でテストに入力またはアサインされたサマリーの説明またはタイトル。
[修復ステータス **(v 12.0)**]	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
保留を除外する	これらの値には、保留されたテスト結果は含まれません。 ○ [オープンなテスト結果]：この構成テストのアクティブな ([クローズ済み] 以外のステータス) テスト結果の数 (カウント)。 ○ [修復されたテスト結果の割合]：このテスト結果グループの修復されたテスト結果の割合。 ○ テスト結果の合計数：この修復タスクのテスト結果の合計数。
保留を含める	これらの値には、保留されたテスト結果が含まれます。 ○ オープンなテスト結果：この修復タスクのすべてのアクティブな ([クローズ済み] 以外のステータス) テスト結果の数 (カウント)。 ○ [修復されたテスト結果の割合]：このテスト結果グループの修復されたテスト結果の割合。 ○ テスト結果の合計数：この修復タスクのテスト結果の合計数。
説明	テストの詳しい説明。Qualys Vulnerability Integration の場合、このフィールドは Qualys クラウドプラットフォーム カバーページのコンテンツがデフォルトとなります。
修復	非準拠を修復する方法を説明している手順。
[関連タブ]	
信頼できるソースコンテンツ	テストに関連付けられた信頼できるソースごとに入力された引用のリスト。
テストグループ	このテストを使用する コンフィグレーションコンプライアンス テストグループのリスト。
テスト結果	このテストに関連する構成の問題によって影響を受ける CI のリスト。必要に応じて、個々のテスト、ServiceNow 構成アイテム、または影響を受けるテクノロジーのリストにアクセスできます。
GRC ポリシーステートメント	GRC ポリシーとコンプライアンス管理 プラグインがインストールされている場合、このタブには関連する GRC ポリシーが含まれます。このリストを編集して、ポリシーステートメントを追加または削除できます。

コンフィグレーションコンプライアンス テスト結果の表示

監査と修復のために コンフィグレーションコンプライアンス テスト結果を表示します。テスト結果は、サードパーティの脆弱性統合のインポート時に自動的に作成されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

重要:
サードパーティの脆弱性統合のインポート中に作成されたテスト結果は、脆弱性マネージャーワークスペースで表示できます。詳細については、「のリストページ Vulnerability Manager ワークスペース」を参照してください。

始める前に
必要なロール：

- 表示する場合、sn_vulc.read
- 表示および更新する場合、sn_vulc.remediation_owner
- 削除する場合、sn_vulc.delete

このタスクについて
コンフィグレーションコンプライアンス はテスト結果を作成または更新しませんが、サードパーティ統合の一部としてインポートします。コンフィグレーションコンプライアンス で表示できるようになると、[テスト結果グループ] を使用して修正されます。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > テスト結果.
コンフィグレーションコンプライアンス v15.0 以降、テスト結果リストに次の列が表示されます。

テスト結果リスト

列	説明
アクティブ	テスト結果がアクティブかどうかを示します。テスト結果は次のようにマークされます。 ○ True：ステータスが [クローズ済み] でない場合。 ○ False：ステータスが [クローズ済み] の場合。
経過時間	テスト結果がオープンになって以降のアクティブ状態の期間。 テスト結果がクローズされた場合、このフィールドは空白になります。 形式：日付 HH:MM:SS

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

列	説明
	経過時間の計算をカスタマイズする方法の詳細については、 KB1703270 記事を参照してください。
クローズ経過時間	テスト結果が「クローズ済み」に移行する前にアクティブであった期間。テスト結果が [クローズ済み] に移行すると、[経過時間] 列の値が [クローズ所要時間] フィールドに表示されます。 テスト結果がアクティブの場合、このフィールドは空白になります。 形式：日付 HH:MM:SS [クローズ所要時間] の計算をカスタマイズする方法の詳細については、 KB1703270 記事を参照してください。
クローズ済み	テスト結果がクローズされたときのタイムスタンプ。 形式：YYYY-MM-DD HH:MM: SS
最終オープン日時	テスト結果がオープンになったときのタイムスタンプ ([アクティブ] フィールド値が *true* に変わったときなど)。

2. 表示するコントロールを開きます。

コンフィグレーションコンプライアンステスト結果のフォームフィールド

フィールド	説明
数値	インポートプロセス時にテストにアサインされた番号。
ソース	サードパーティ SCA アプリケーションのシステム名、または コンフィグレーションコンプライアンス との通信に使用される API のアプリケーションプラグインに入力された名前。
ソース ID	SCA アプリケーションによってコントロールにアサインされた識別子。
結果	合格、失敗、エラー、または不明。Qualys からインポートされます。
リスクスコア	このテストの算出結果。 コンフィグレーションコンプライアンス v15.0 より前の場合、合格したテスト結果のリスクスコアは「0」に設定されます。コンフィグレーションコンプライアンス v15.0 以降の場合、合格したテスト結果のリスクスコアは「0」に変更されないため、軽減されたリスクを評価できます。合格したテスト結果のリス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	クスコアは、修復タスクのリスクスコアの計算には含まれません。
リスク評価	リスクスコア範囲に基づき、全体的なリスクを [1 - 重大] ～ [5 - なし] の 1 ～ 5 の数値スケールで評価します。このフィールドは、以前のバージョンの [優先度] フィールドに代わるものです。
ステータス	テスト結果が属する修復タスクから計算されます。テスト結果が複数のグループに属する場合、優先順位をつけてステータスを決定します。
解決	テスト結果が属する修復タスクから計算されます。テスト結果が複数のグループに属する場合、優先順位をつけて解決策を決定します。
初回確認日	コンフィグレーションコンプライアンス に最初にインポートされた日付。 v13.1.1 以降、[初回確認日] フィールドにはスキャナーによって提供された日付が表示されます。それ以外の場合は、コンフィグレーションコンプライアンス に最初にインポートされた日付が表示されます。
最終確認日	コンフィグレーションコンプライアンス に最後にインポートされた日付。 v13.1.1 以降、[最終確認日] フィールドにはスキャナーによって提供された日付が表示されます。それ以外の場合は、コンフィグレーションコンプライアンス に最後にインポートされた日付が表示されます。
前回の合格	テスト結果が合格した最新の日付。
テスト	テストの名前
構成アイテム	テストに付けられた CI の名前。
テクノロジー	CI で実行されているソフトウェアのバージョン。
説明	テストの説明。
必要な値	Qualys で設定され、コンフィグレーションコンプライアンス によってインポートされた必要な値。この値は、true であると評価されるとテスト結果が [合格] になるブール式です。式は、論理演算子、セット演算子、または正規表現演算子の組み合わせにすることができます。
実際の値	テストによって返された値。これらの値は必要な値のブール式に代入されて、結果が合格か失敗かが決定されます。Qualys からインポートされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	コンフィグレーションコンプライアンス のバージョン 14.9 以降では、[詳細証拠 (Extended Evidence)] と [失敗の原因 (Cause of Failure)] の値が [実際の値] 列に追加されています。
修復	修復手順。
[関連タブ]	
修復タスク	このテスト結果に関連付けられている修復タスク。
テスト結果の履歴	同じ CI/テクノロジー/テストの合格/失敗の履歴を示すテスト結果の関連リスト。

修復タスクの表示

修復タスクを表示または作成して、修復を実行することができます。

重要:
修復タスクは、脆弱性マネージャーワークスペースで確認できます。詳細については、「のリストページ Vulnerability Manager ワークスペース」を参照してください。

始める前に
必要なロール：

- 更新または作成する場合、sn_vulc.admin
- 表示する場合、sn_vulc.remediation_owner

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

手順

1. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > 修復タスク.
2. リストから、表示するレコードをクリックします。
3. または、[新規] をクリックして新しい修復タスクを作成し、フィールドに入力します。

コンフィグレーションコンプライアンスの修復タスクフォームフィールド

フィールド	説明
数値	このレコードに対して自動的に生成された数値。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
状況	修復タスクの進捗状況。 ○ オープン ○ 調査中 ○ 実装待ち ○ 保留 ○ 解決済み ○ クローズ済み
リスクスコア	このスコアは、修復タスクにおけるすべてのアクティブなテスト結果のリスクスコアをロールアップした値です。このスコアは、修復タスクでテスト結果が修復されると変更されます。
アサイン先グループ	この修復タスクで作業するように選択されたグループ。
リスク評価	失敗したテスト結果がシステムにもたらすリスクの量を表します。これは、リスクを重大 (1) ～ なし (5) として評価する 1 ～ 5 の数値スケールによるリスクスコアの範囲に基づいています。
アサイン先	このタスクセットで作業するように選択されたアサイン先グループの個人。
修復ターゲット	テスト結果が最初に識別されてから、修復されるべき日付。
作成日時	この修復タスクが作成された日時。
修復ステータス	グループの修復のステータス。最も近い期日のテスト結果によって決定されます。 オープングループの状況には、[ターゲット内]、[ターゲット間近]、および [ターゲット経過] が含まれます。クローズ済みグループの状況には、[ターゲットなし]、[ターゲット達成]、[ターゲット経過] があります。 算出された修復ターゲット日について、修復タスクがクローズされている場合は、クローズ済みのすべてのテスト結果の全体的な修復ステータスが修復タスクに表示されます。それらによって、そのグループが日付を満みたしたか否かが判断されます。 クローズ済みの修復タスクの修復ステータスは、そのクローズ済み結果のどれにも修復ターゲット日がない場合、[ターゲットなし] になります。そのクローズ済み結果のいずれかがターゲット日を過ぎた場合、[ターゲット経過] になります。少なくとも 1 つのクローズ済み結果がターゲットを達成し、その他の結果が達成できなかった場合、[ターゲット達成] になります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
更新日時	このレコードが最後に変更された日時。
簡単な説明	この修復タスクの簡単な説明。
説明	この修復タスクに関連付けられたソフトウェアのリストを含む、修復タスクの長い説明。
テスト	この修復タスクに関連付けられた構成テスト。
修復ステータス (バージョン **12.0)**	
保留を除外する	これらの値には、保留されたテスト結果は含まれません。 ○ オープンなテスト結果：この修復タスクのアクティブな ([クローズ済み] 以外のステータス) テスト結果の数 (カウント)。 ○ [修復されたテスト結果の割合]：この修復タスクの修復された (クローズ済みの) テスト結果の割合。 ○ テスト結果の合計数：この修復タスクのテスト結果の合計数。
保留を含める	値は、すべてのアクティブなテスト結果 ([クローズ済み] 以外のステータス) を表します。 ○ オープンなテスト結果：この修復タスクのアクティブな ([クローズ済み] 以外のステータス) テスト結果の数 (カウント)。 ○ [修復されたテスト結果の割合]：この修復タスクの修復された (クローズ済みの) テスト結果の割合。 ○ テスト結果の合計数：この修復タスクのテスト結果の合計数。
グループ構成	修復タスクに対するテスト結果の選択に使用されるフィルタリングのタイプ。
グループ化の方法	使用されたメソッドの名前。
グループルール	使用されたグループルールの名前。
メモ	レコードに関連付けられたシステムメモ。
関連リンク	バージョン 12.0：ステータスリンクの更新。オンデマンドでテスト結果レコードの値を更新します。前回のスケジュール済みジョブ以降に変更または更新されたデータを表示します。
テスト結果	この修復タスクのテスト結果。
変更要求 **(v 12.0)**	この修復タスクに関連付けられた変更要求のリスト。
ステータス変更承認 **(v 12.0)**	この修復タスクに関連付けられた変更要求の承認に関するステータスと変更状況。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンフィグレーションコンプライアンスアプリケーションのテスト結果と修復タスクのステータス移行

テスト結果レコードが保留、解決、再オープンされ、他の修復作業 (RE) に転送されると、構成テストレコードおよび関連する修復タスク (RT) の状況が影響を受けます。

テスト結果と修復タスク間のステータス移行シナリオ

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

次の表は、構成テスト結果と修復タスクの間でステータスとサブステートがどのように移行するかを詳しく説明しています。

修復タスクのステータスが移行する場合...	...移行先ステータス/サブステート	関連するテスト結果のステータスの移行元...	...移行先ステータス/サブステート	説明
オープン	調査中	オープン	調査中	ステータスは双方向に移行します。
オープン	レビュー中	オープン	レビュー中	ステータスは双方向に移行します。
オープン	保留/解決のために選択された理由	オープン	保留	テスト結果では、修復タスクと同じ解決の理由が保持されます。
保留/解決の理由	オープン	テスト結果は保留されたまま		テスト結果では、修復タスクと同じ解決が保持されます。
オープン	[解決済み]/[修正済み]	オープン	解決済み	ステータス/サブステートは双方向に移行します。
オープン	[解決済み] および [解決済み] から [クローズ済み]/[修正済み]	オープン	解決済み	修復タスクが [クローズ済み]/[修正済み] に移行した場合、[オープン] に戻すことができます。タスクが [オープン] に移行した場合、関連するテスト結果は [解決済み] か

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクのステータスが移行する場合...	...移行先ステータス/サブステート	関連するテスト結果のステータスの移行元...	...移行先ステータス/サブステート	説明
				ら [オープン] に戻ります。
オープン	解決済み	オープン	解決済み	ステータス/サブステートは双方向に移行します。
オープン	[解決済み]/[キャンセル]	オープン	解決済み	ステータス/サブステートは双方向に移行します。
オープン	[解決済み] および [解決済み] から [クローズ済み]	オープン	解決済み	修復タスクが自動的に [クローズ済み] に移行した場合、関連するテスト結果は [オープン] に戻る可能性があります。
オープン	[解決済み] および [解決済み] から [クローズ済み]/[結果が無効]	オープン	[解決済み] および [解決済み] から [クローズ済み]/[結果が無効]	修復タスクが [解決済み] に移行した場合、[オープン] に戻すことができます。 修復タスクが [クローズ済み]/[結果が無効] に移行した場合、そのタスクとそれに関連するテスト結果は再オープンできません。
オープン	[クローズ済み]/[修正済み]	テスト結果はオープンのまま		

注:

- コンフィグレーションコンプライアンス v14.12 以降、[モーダルを閉じる] の [解決] フィールドで [無効な結果] オプションが削除されました。
- コンフィグレーションコンプライアンスの v14.12 以降では、[修復タスクステータスの承認 **(Remediation Task State Approval)]** ワークフローは廃止され、フローデザイナーのフロー [修復タスクステータスの承認 (Remediation Task State Approval)] に置き換えられました。

変更要求と修復タスク間のステータスの同期

コンフィグレーションコンプライアンスアプリケーションの修復タスクのステータスフィールドと変更要求 (CHG) のステータスフィールド間には、同期関係があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

変更要求のライフサイクルが進むと、関連する修復タスクのステータスも自動的に変化します。ステータスの同期は、v12.0 以降では、ServiceNow Store から コンフィグレーションコンプライアンス アプリケーションをダウンロードすると、デフォルトでシステムプロパティによってインスタンスで有効になります。

ステータスの同期を有効にすると、以下の場合に、CHG ステータスフィールドによって修復タスクのステータスフィールドが自動的に変更されます。

- 修復タスクに対して新しい変更要求が作成された場合、[実装待ち] でなければ、修復タスクのステータスは [実装待ち] に移行します。
- 修復タスクに既存の変更要求が関連付けられている場合、[実装待ち] でなければ、修復タスクのステータスは [実装待ち] に移行します。
- 変更要求のタスクが完了 ([実装済み]) し、CHG が [レビュー] ステータスに移行すると、修復タスクは [解決済み] に移行します。

ステータス同期の詳細と例については、次のセクションを参照してください。

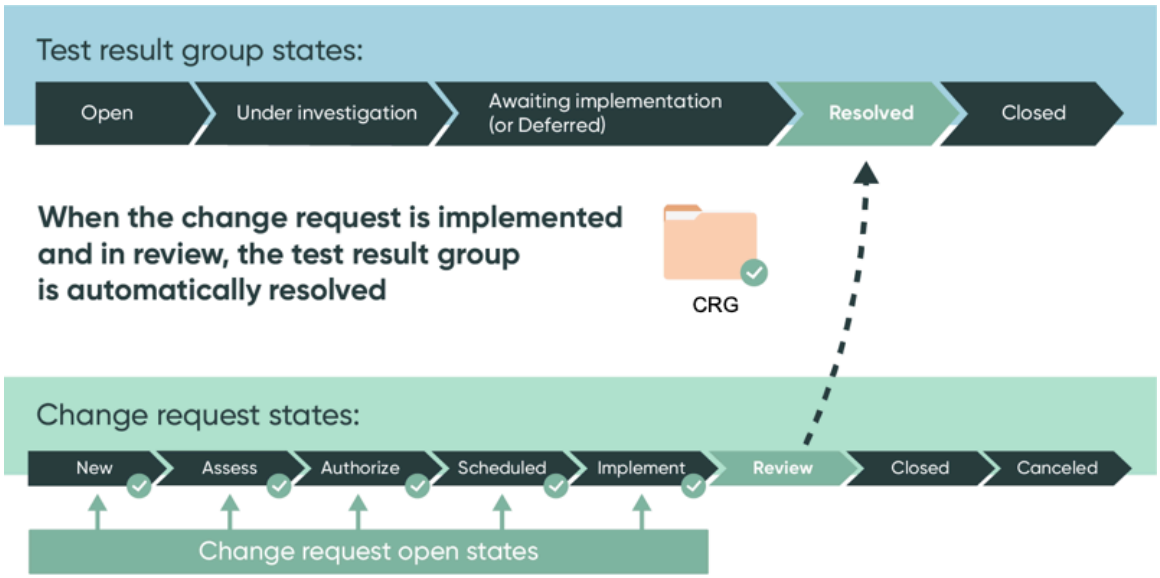
注:
ステータス同期を有効にした状態で、それぞれのレコードのライフサイクルのステータスを介して変更要求と修復タスクを引き続き手動で移行することはできますが、変更要求状況が変化したことをシステムが登録したり、各自が変更要求を追加したり、修復タスクから変更要求を削除したりすると、ステータス同期によって手動による介入が無効になる可能性があります。ただし、変更要求の状況により、修復タスクの状況が [クローズ済み] から自動的に移行されることはありません。

ステータスの順方向同期

次の図は、CHG ステータスが、修復タスクのステータスをライフサイクルの順方向、つまり [オープン] から [解決済み] に自動的に移行される様子を示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[解決済み] または [クローズ済み] 以外のステータスの任意の修復タスクに対して、新しい変更要求を作成できます。状況同期により、TRG は [オープン]、[調査中]、[実装待ち]、および [解決済み] 状況を介して自動的に双方向に移行します。この移行は、変更要求におけるステータスフィールドの特定の値に基づいています。変更要求と修復タスク間のステータス同期は、自動的に呼び出されます。ただし、チェックボックス (**[CR** に **CI** を追加]) がフォームに表示されており、それをオフにした場合は除きます。

CHG がオープンステータスの場合、修復タスクは [解決済み] には移行しません。CHG のライフサイクルにおいて、[レビュー] 以前の状況 ([新規]、[評価]、[許可]、[予約済み]、または [実装]など) にある CHG は、その CHG のオープン状況と見なされます。オープンステータスでは、CHG の調査またはタスクが完了していないため、修復タスクのステータスフィールドは移行されません。ステータス同期は、CHG が修復タスクに対して作成されるか関連付けられたとき、または CHG で既存の関係のステータスが変更されたときに呼び出されます。完了した CHG ステータスは、[レビュー] および正常に [クローズ済み] となります。CHG が正常にクローズされると、そのクローズ済みコードは [成功] または [成功したが問題あり] となるため、修復タスクは [解決済み] に移行します。

ステータスの逆方向同期

CHG はライフサイクル中に処理されるため、ある時点でキャンセルされる場合があります。この場合、CHG が [キャンセル] または [クローズ済み] (クローズコードは [不成功]) の場合、修復タスクは自動的に [調査中] に戻されます。脆弱性を修正するアクティブな計画がないため、修復タスクは [調査中] に戻されます。

修復タスクが [解決済み] 状況にある場合、新しい CHG を作成するか、初期オープン状況のいずれかで既存の CHG に関連付けると、修復タスクは自動的に [実装待ち] に戻されます。CHG にアサインされている作業が増えるため、修復タスクはこのステータスに戻されます。

複数の **CHG** を含む修復タスク

[実装待ち] の修復タスクに複数の CHG が関連付けられている場合、ステータスの同期は、そのライフサイクルの最も早期のステータスである CHG のステータスに基づいています。たとえば、次の表に示すように、修復タスクに CHG1、CHG2、CHG3、および CHG4 の 4 つの CHG が関連付けられているとします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CHG 番号	CHG ステータス
1	実装
2	キャンセル済み
3	クローズ済み (クローズコード [不成功])
4	クローズ済み (クローズコード [不成功])

この場合、CHG と修復タスク間のステータス同期は、4 つの CHG のうち最も早期のステータスである CHG1 ([実装]) に基づいています。この場合、修復タスクは [実装待ち] のままになります。

別の例では、修復タスクが [解決済み] ステータスにあり、実装済みで [レビュー] ステータスになっている既存の CHG があり、新しい CHG が作成された場合、修復タスクは [解決済み] から [実装待ち] に戻されます。ステータスの同期は、最も早期のステータスの CHG である [新規] ステータスの CHG に基づいています。

CHG 番号	CHG ステータス
1	レビュー
2	新規

また、修復タスクに複数の CHG がある場合、次の場合に修復タスクのステータスが自動的に移行します。

- CHG が [レビュー] に移行すると、修復タスクに関連付けられている他のすべての CHG が [レビュー] または [クローズ済み] 状況 (正常なクローズコードあり) であれば、修復タスクは [解決済み] に自動的に移行されます。キャンセルされたり、正常にクローズされていない他の関連する CHG は無視されます。
- CHG が [キャンセル] または [クローズ済み] (クローズコード [不成功]) に移行すると、修復タスクに関連付けられている他のすべての CHG が同じステータスであれば、修復タスクは自動的に [調査中] に戻されます。

修復タスクの状況と各状況で実行できる処理の詳細については、「コンフィグレーションコンプライアンス のステータス」を参照してください。

ドメインセパレーションと コンフィグレーションコンプライアンス

ドメインセパレーションは コンフィグレーションコンプライアンス でサポートされています。 ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	v14.9 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

サポートレベル：標準

- ベーシックレベルのサポートのすべての側面が含まれています。
- アプリケーションプロパティは、必要に応じてドメイン対応です。
- ビジネスロジック：サービスプロバイダー (SP) によって顧客ごとにプロセスを作成または変更できます。ユースケースには、単一のインスタンスでの複数のサービスプロバイダー顧客によるアプリケーションの正しい使用が反映されています。
- インスタンスのオーナーは、特定のアプリケーションに期待される通りに、テナントごとに MVP ビジネスロジックとデータパラメーターを設定できる必要があります。

サンプルユースケース：アドミンは、レコードを他のテナントに対してはクローズしないが、1 つのテナントに対してクローズする場合、コメントを必須にすることができる必要があります。

サポートレベルの詳細については、「アプリケーションでのドメインセパレーションのサポート)」を参照してください。

コンフィグレーションコンプライアンス におけるドメインセパレーションの仕組み

ドメインセパレーションによって、顧客ベース全体で (コンフィグレーションコンプライアンス) 手順を標準化し、運用コストの削減とサービス品質の向上を実現できます。

顧客データは、ワークフロー、ダッシュボード、レポートなどに別個の顧客ワークスペースを使用することで分離され、他のクライアントに公開されることはありません。

コンフィグレーションコンプライアンス におけるドメインセパレーションのサポート (バージョン別)

リリース	サポートレベル	メモ
Orland	標準	
Paris	標準	
Quebec-	標準	
Rome	標準	
サンディエゴ	標準	
東京	標準	
ユタ	標準	
Vancouver	標準	

コンフィグレーションコンプライアンス アプリケーションのドメインセパレーションは、次の製品機能をカバーしています。

- サードパーティのスキャナー (Qualys) のテスト結果を正しいドメインで取り込みます。

  データは、統合に使用される認証情報を持つ統合ユーザーと同じドメインに取り込まれます。

- 要求元のドメインの コンフィグレーションコンプライアンス から特定のホストを再スキャンします。
- CMDB CI ルックアッププロセスを使用して、スキャナーからの CI 情報が統合ユーザーのドメインの CMDB の CI と一致することを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 統合ユーザーと同じドメインで定義されたリスクスコア算出に従って、テスト結果レベルでリスクスコアを計算します。
- 修復タスクルールは、統合ユーザーと同じドメインで定義、アサイン、維持できます。
- 修復タスクルールを使用して作成された doc 修復タスクは、修復タスクルールが作成されたのと同じドメインに留まります。
- 保留ワークフローは、保留が要求された同じドメイン内の承認プロセスを通過します。
- レポートとダッシュボードには、テスト結果の経過時間、CI 別のオープンなテスト結果、影響度別のテスト結果などのテスト結果状況が、属しているドメイン内で表示されます。
- サードパーティのスキャナー (Qualys) からのナレッジをグローバルドメインに取り込み、複数のクライアント間でデータを共有できます。

注:
上記のすべてのケースでは、NOW Platform における分離されたドメインでの可視化の包括的な原則が適用されます。

ユースケース

コンフィグレーションコンプライアンス アプリケーションは、テスト結果のライフサイクルをエンドツーエンドで管理します。次のユースケースはドメインセパレーションに対応しています。

- Qualys からのテスト結果の [取り込み **(Ingest)**]
  - 複数のインスタンスからデータを取り込む
  - テスト結果の重複を排除する
  - CMDB CI と照合する
- リスクスコアによるテスト結果の [拡張]
  - 資産の拡張 (CMDB)
  - リスクスコア
- テスト結果を [グループ化 **(Group)**] して修復タスクをアサインする
  - テスト結果を自動的にグループ化する
  - 修復タスクを自動的にアサインする
- 修復
  - 修復タスクとしてアサインされた修復タスク
  - 包括的な修復ライフサイクル
  - 保留ワークフロー
- 組織のセキュリティ体制とコンプライアンス管理プログラムの [測定 **(Measure)**]
  - コンプライアンス、カテゴリ、重要度、およびテクノロジー別の結果の傾向
  - ポリシー、テスト、ホスト、テスト結果、およびリスクスコアのステータスと配布

セットアップ

コンフィグレーションコンプライアンス のドメインセパレーションを設定するには、追加の手順は必要ありません。インスタンスがドメインセパレーションされた後、すべての コンフィグレーションコンプライアンス テーブルで [ドメイン] 列が取得されます。テスト結果の統合インポートデータを特定のドメインに送信できます。詳細については、「統合のためのドメインセパレーションイン

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ポートの作成」を参照してください。その他の注意事項と設定の詳細については、「ドメインセパレーションの追加の設定」を参照してください 。

ドメインセパレーションデータ

データはドメインセパレーションできます。これは、次のことを意味します。

- サードパーティのスキャナーから取り込まれたテスト結果は統合ユーザーのドメインと同じドメインに留まり、他のドメインからはアクセスできません。
- あるドメイン内のテスト結果やホストを他のドメインから閲覧することはできません。
- リスクスコアアルゴリズムとテスト結果のグループルールは、ドメイン外のユーザーは閲覧できません。
- あるドメインで作成された保留ワークフローを別のドメインで見ることはできません。
- すべてのメール通知は、属しているドメイン内に含まれます。

コンプライアンスアナリストが自社のアプリケーションデータを管理する方法

- アナリストは、自分でアプリケーションインストール、マルチソースアプリケーション管理、および CI ルックアップルールを作成します。
- アナリストは、ドメイン内で使用するために特定の統合を構成できます。
- アナリストは、独自の保留および変更管理ワークフローを作成できます。
- アナリストは、独自の修復タスクルール、正確な結果の優先順位付けを行うリスクスコアロジック、修復タスクの自動アサイン、正しいアサイン先グループへのアサインを作成できます。
- ドメインユーザーは、手動修復タスクを作成し、クローズします。

インスタンスオーナーがドメインセパレーションできるビジネスロジックとプロセス

- コンフィグレーションコンプライアンス ユーザーとグループ
- コンフィグレーションコンプライアンス 統合 (Madrid リリースから)
- 完全なセットアップ構成 (ユーザーとグループの管理、アプリケーションのインストール、マルチソースアプリケーション管理、CI ルックアップルール、修復タスクルール、リスク算出など)
- 保留を含む完全な修復ライフサイクル

関連情報

サービスプロバイダーのドメインセパレーション

コンフィグレーションコンプライアンス の重要度マップ

コンフィグレーションコンプライアンス 重要度マッピングは、ソースの重要度フィールドを コンフィグレーションコンプライアンス のフィールドに変換します。

コンフィグレーションコンプライアンス ベースシステムには、標準の Qualys クラウドプラットフォーム から標準の ServiceNow へのマッピングが付属しています。重大度マップの作成または編集は、自分の環境におけるカスタマイズされたまたは非標準のサードパーティマッピングのみを対象としています。

コンフィグレーションコンプライアンス のステータス

コンフィグレーションコンプライアンス を使用すると、ステータスモデルを表示して、特定の時点での修復タスクのステータスを把握することができます。修復タスクのステータスは、優先順位に基づきテスト結果のステータスを制御します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

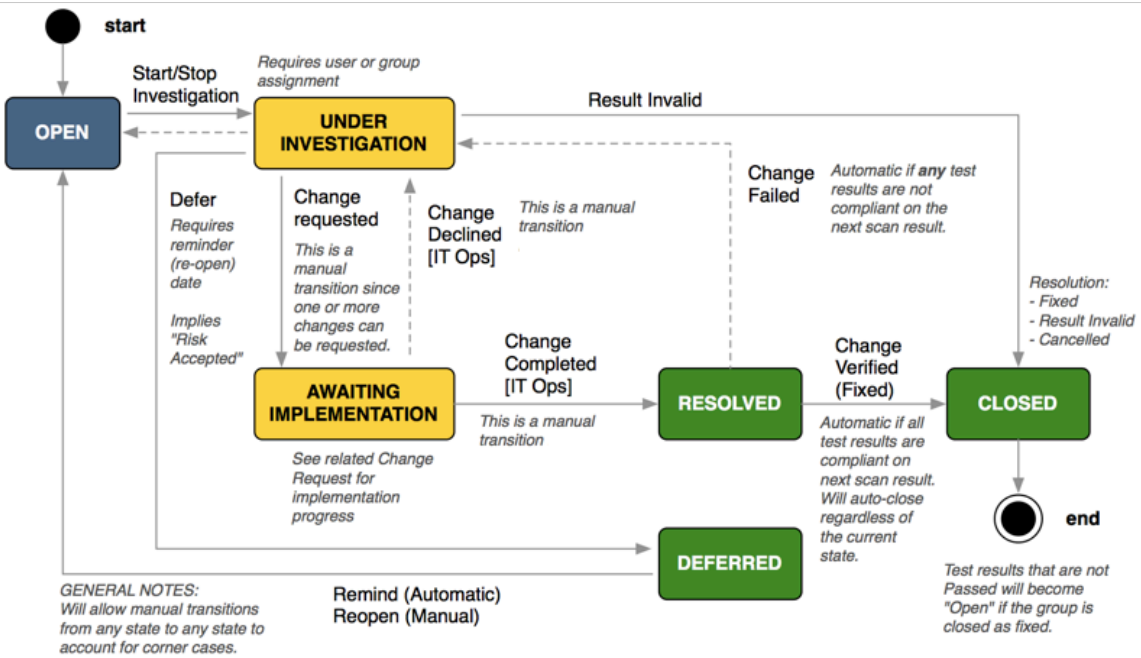
v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

修復タスクステータス

修復タスクには設定可能な状況が多数あります。次のスキャン結果に基づいて、[解決済み] ステータスからの自動移行が可能です。次のスキャンですべてのテスト結果が合格すると、その修復タスクはクローズされます。そうでない場合は、[調査中] ステータスに移行します。システムはこの [クローズ済み] ステータスを確認しますが、テスト結果が追加されるか、修復タスクから削除された場合は、修復タスクステータスを再評価します。作業メモは移行を反映して更新されます。

次の図は、修復タスクのステータスがどのように [オープン] ステータスから [クローズ済み] ステータスに移行するのかを示しています。

コンフィグレーションコンプライアンス状況フロー **(v15.0** より前)



注:

- 各修復タスクフォームには、ServiceNow タスクの標準である [フォロー] および [更新] ボタンが含まれています。
- コンフィグレーションコンプライアンス v15.0 以降、以下が削除されています。
  - [閉じる] ボタン
  - 解決モーダルの [解決] フィールド。

次の表に、コンフィグレーションコンプライアンス 状況を示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンフィギュレーションコンプライアンスの状況

状況	説明
オープン	作成時のステータス。
調査中	[調査を開始] ボタンによってトリガーされます。このステータスから、次のことができます。 変更要求の作成 詳細については、「コンフィグレーションコンプライアンスで変更要求を作成する」を参照してください。 例外の要求 理由を入力し、再オープン日を選択します。 削除 削除を確定します。修復タスクを削除します。 誤検出としてマーク 理由とメモを入力します。修復タスクを誤検出としてマークします。
保留	[保留] ボタンによってトリガーされます。このステータスから、次のことができます。 再オープン [オープン] ステータスに戻します。 削除 削除を確定します。グループを削除します。 [保留/クローズ] 関連タブの下に保留情報が表示されます。保留日に、グループは修復のために再オープンされます。
実装待ち	[実装待ち] ボタンによってトリガーされます。このステータスから、次のことができます。 セキュリティインシデントの作成 詳細については、「Create a security incident (セキュリティインシデントを作成する)」を参照してください。 変更要求の作成 詳細については、「コンフィグレーションコンプライアンスで変更要求を作成する」を参照してください。 解決 [解決メモ] に、修復タスクを解決する理由を追加します。 ステータスが [解決済み] になります。[解決] 関連タブの下にメモが表示されます。 削除 削除を確定します。修復タスクを削除します。
解決済み	[解決 **(Resolve)**] ボタンからトリガーされます。このステータスから、次のことができます。 セキュリティインシデントの作成

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンフィギュレーションコンプライアンスの状況 (続く)

状況	説明
	詳細については、「Create a security incident (セキュリティインシデントを作成する)」を参照してください。 再オープン [オープン] ステータスに戻します。 削除 削除を確定します。修復タスクを削除します。 [メモ] 関連タブの下にメモが表示されます。[解決] 関連タブの下に解決情報が表示されます。メモは、修復タスクに関連付けられているすべてのテスト結果の 作業メモ に反映されます。
クローズ済み	[クローズ] ボタンまたは [誤検出としてマーク] ボタンからトリガーされます。 コンフィグレーションコンプライアンス v14.12 以降、誤検出としてマークして修復タスクをクローズできます。 このステータスから、次のことができます。 再オープン [オープン] ステータスに戻します。 削除 削除を確定します。グループを削除します。 [保留/クローズ] 関連タブの下にクローズ情報が表示されます。メモは、修復タスクに関連付けられているすべてのテスト結果の 作業メモ に反映されます。

- 修復タスクが [クローズ済み] または [修復済み] としてマークされていて、追加されたテスト結果自体が [クローズ済み] または [修復済み] でない場合、テスト結果のステータスは変更されず、修復タスクのステータスは [オープン] に変更されます。
- 修復タスクを新規作成または分割すると、新 / 旧の修復タスクに対して [理由] および [期限] フィールドが再評価されることになります。すべてのテスト結果のステータスが [保留] の場合、[理由] および [期限] フィールドの値が修復タスクにロールアップされます。
  - 修復タスクのすべてのテスト結果が保留となり、理由 が同じ場合、修復タスクに同じ 理由がアサインされます。そうでない場合、[理由] フィールドは [なし] に変更されます。
  - [期限] フィールドの日付は、テスト結果が属するすべての修復タスクの中で最も近い日付で更新されます。

  注:
  この評価は、1 時間ごとに実行されるスケジュール済みジョブ [*Rollup test result values to test result group and configuration test*] によって行われます。

- [最終確認日] が解決済みのテスト結果の[解決日]よりも後の場合、テスト結果が再オープンされます。解決済みの修復タスクでは、取り込み中にテスト結果が 1 つでも再オープンされると、修復タスクのステータスが [調査中] に移行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テスト結果のステータス

修復タスクのステータスによって、関連するテスト結果のステータスも変更されます。このメカニズムには 2 つのケースがあります。

属する修復タスクが 1 つのみのテスト結果

結果は、次の 3 つの例外を除いて、修復タスクのステータスと一致します。

- 修復タスクのステータスが [クローズ済み] に、その解決策 (サブステート) が [修復済み] に変更された場合、アイテムはその変更を無視して [オープン] ステータスに戻ります。
- 修復タスクのステータスが [クローズ済み] に、その解決策 (サブステート) が [キャンセル] に変更された場合、アイテムはその変更を無視して [オープン] ステータスに戻ります。
- テスト結果のソースステータスが [修復済み] (スキャンまたはインポートによって更新) の場合、修復タスクのステータスが変更されると、修復タスクのステータスに関係なく、テスト結果のステータスが [クローズ済み (修復済み)] に変更されます。

複数の修復タスクに属するテスト結果

テスト結果は、自動的に修復タスクのステータスと一致するわけではありません。その代わりに、関連するすべてのグループを検索して、適用する優先順位が最も高いステータスを見つけます。優先されるステータスは次のとおりです。

クローズ済み (サブステート:結果が無効) > クローズ済み (サブステート:誤検出) > 保留 > 解決済み > 実装待ち > 調査中 > オープン

注:
[クローズ済み] (サブステート：[修正済み]) と [クローズ済み] (サブステート：[キャンセル]) は、2 つの特別なケースです。

注:
コンフィグレーションコンプライアンス v15.0 以降、[結果が無効] サブステートは廃止されました。

修復タスクステータスの例

たとえば、

修復タスクステータス	テスト結果のステータス
グループA: オープン > 調査中 グループ B：[オープン]	調査中 グループ A が [調査中]、グループ B が [オープン] の場合、検索の結果、グループ A とグループ B では、グループ A の方が優先順位が高いステータスであるため、テスト結果は [調査中] に変わります。
グループ A：[調査中] グループB: オープン > 調査中	[調査中] グループ B が [調査中]、グループ A が [調査中] の場合、検索の結果、グループ A とグループ B では、両グループの優先順位は同じであるため、テスト結果は [調査中] のままです。
グループ A：[調査中]	実装待ち

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクステータス	テスト結果のステータス
グループB: 調査中 > 実装待ち	グループ B が [実装待ち]、グループ A が [調査中] の場合、検索の結果、グループ A とグループ B では、グループ B の方が優先順位が高いステータスであるため、テスト結果は [実装待ち] に変わります。
グループA: 調査中 > 保留 グループB: 実装待ち	保留 グループ A が [保留]、グループ B が [実装待ち] の場合、検索の結果、アイテム 1 はグループ A とグループ B の間で、グループ A の方が優先順位が高いステータスであることがわかったため、テスト結果は [保留] に変わります。
グループA: 保留 グループB: 実装待ち > クローズ済み (結果が無効)	クローズ済み (結果が無効) > 保留 グループ B が [クローズ済み] でその解決策 (サブステート) が [結果が無効 (Result Invalid)]、グループ A が [保留] の場合、検索の結果、グループ A とグループ B では、グループ B の方が優先順位が高いステータスであるため、テスト結果は [クローズ済み (結果が無効) (Closed (Result Invalid))] に変わります。
グループA: 保留 グループB: クローズ済み (結果が無効) > オープン (再オープン経由)	保留 グループ B が再オープンして、ステータスが [オープン] に変わり、グループ A が [保留] の場合、検索の結果、グループ A とグループ B では、グループ A の方が優先順位の高いステータスであるため、テスト結果は [保留] に変わります。
グループ A：[保留] グループB: 実装待ち > クローズ済み (誤検出)	クローズ済み (誤検出) グループ B が [クローズ済み]、解決策 (サブステート) が [誤検出]、グループ A が [保留] の場合、検索の結果、グループ A とグループ B ではグループ B の方が優先順位の高いステータスであるため、テスト結果は [クローズ済み (誤検出) (Closed (False Positive))] に変わります。

テスト結果ステータスの特別な例

修復タスクステータス	テスト結果のステータス
グループA: 調査中 グループB: 実装待ち > クローズ済み (修正済みまたはキャンセル済み)	調査中 グループ B が [クローズ済み] (サブステート [修復済み] またはサブステート [キャンセル])、グループ A が [調査中] の場合、テスト結果は [実装待ち] (以前は最優先) から [調査中] (現在は最優先) に変わります。
グループ A：いずれかのステータス グループ B：いずれかのステータス	テスト結果のソースステータスが [修復済み] (スキャンまたはインポートによって更新) の場合、修復タスクの状況が変更されると、その他の関連付けられて

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テスト結果ステータスの特別な例 (続く)

修復タスクステータス	テスト結果のステータス
	いる修復タスクの状況に関係なく、テスト結果の状況が [クローズ済み (修復済み)] に変更されます。修復タスクステータスのテスト結果検索は行われません。

コンフィグレーションコンプライアンス のインポートに関する問題を解決する

サードパーティ統合のインポートに関する問題を解決します。

インポートに関する問題の解決

問題	解決
テスト結果がありません	**[Qualys PC** 結果] 統合で *Start Time* を確認します。 設定が不十分である可能性があります。「Qualys PC 結果の開始日を変更する」を参照してください。
統合が失敗しています	[脆弱性統合実行] ステータスをクリックします。 個々の統合プロセスエントリーには、インポートされた XML が保持されており、予期せぬ情報を調べることができます。 次のように移動する。 **Qualys Vulnerability Integration** > プライマリ統合 > **QualysPC** の結果 > 脆弱性統合実行 関連タブ。 最新の実行を選択します。 [脆弱性統合プロセス] 関連リストのエントリーのステータスやノートに異常がないか調べます。 。

Qualys PC 結果の開始日を変更する

Qualys PC 結果インポートに開始日のデータがない場合は、変更できます。

始める前に
必要なロール：sn_vul_qualys.admin

手順

1. 次のように移動する。 **All** (すべて) > **Qualys Vulnerability Integration** > アドミニストレーション > プライマリ統合.
2. **[Qualys PC** 結果] 統合をクリックします。
3. [統合の詳細] をクリックします。
4. [開始時間] フィールドを過去の値に設定すると、その時間以降にスキャンおよび検出されたすべてのテスト結果が検出されます。

> **注:**
> 日付が空欄の場合、最初の実行時にデータは返されません。過去最大 1 か月前の値を設定してください。この設定により、大量のデータで Qualys API レート制限を超えることがなくなり、実行タイムアウトがトリガーされなくなります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. [送信] または [更新] をクリックします。
6. オプション: [今すぐ実行] をクリックして、今すぐ実行します。

Microsoft Defender for Cloud Integration for セキュリティオペレーション と Palo Alto Prisma Cloud の CI ルックアップルール

Microsoft Defender for Cloud Integration と Palo Alto Prisma Cloud 統合の構成アイテム (CI) ルックアップルールを使用して、構成管理データベース (CMDB) で一般的に使用されるリソースタイプに正しく一致するものを見つけることができます。

概要

[CI ルックアップルール] モジュールには、構成管理データベース (CMDB) に一致するデータを持つフィールドを定義できるルールが含まれています。これらのルールを使用して、アプリケーションとアプリケーションリリースを識別できます。Microsoft Defender for Cloud Integration および Palo Alto Prisma Cloud のすべての資産は、 ServiceNow プラットフォームのオブジェクト ID、クラウドアカウント、および論理データセンターの組み合わせによって一意に識別されます。ServiceNow ディスカバリーは、CMDB の Object_id 列にリソース ID をさまざまなリソースタイプのさまざまな形式で入力します。 次の表は、検出サービスが CI の Object_id 列に入力するために使用する、一般的に使用されるリソースタイプのオブジェクト ID 形式を示しています。特定のリソースタイプの資産を検索するスキャナーは、適切なオブジェクト ID 形式を使用して検索する必要があります。対応する CMDB CI クラスのオブジェクト ID 列を調べて適切なオブジェクト ID の形式を確認し、スキャナーから受信した値を使用してオブジェクト ID を作成できます。

さまざまなリソースタイプのオブジェクト **ID** 形式

リソースタイプ	フォーマット
AWS::EC2::Instance	オブジェクト ID
AWS::ElasticLoadBalancing::LoadBalancer	ロードバランサー名
AWS::S3::Bucket	arn:aws:s3:::<Bucket Name>

ルックアップルールで同じ形式の object_id が使用されていない限り、テスト結果の CI 一致は 構成管理データベース (CMDB) では正確に検出されない可能性があります。ほとんどの場合、OOB CI ルックアップルールでは、Microsoft Defender for Cloud Integration および Palo Alto Prisma Cloudの最もよく使用されるリソースタイプの一致が検出されます。次の CI ルックアップルールで CMDB の CI をテスト結果に見つけられない場合は、リソースタイプの CI ルックアップルールを作成できます。CI ルックアップルールの作成方法の詳細については、「Create a CI lookup rule (CI ルックアップルールを作成する)」を参照してください。

CI ルックアップルール

次の CI ルックアップルールは、Microsoft Defender for Cloud Integration と Palo Alto Prisma Cloud に固有のものです。

S3 バケット

このルックアップルールは、arn:aws:s3::: とリソース名を連結して取得された値で、CMDB で CI の検索を試みます。取得された値は、cmdb_ci_cloud_object_storage テーブルの object_id 列で検索されます。このルックアップルールは、リソースタイプが AWS::S3::Bucket の場合にのみ適用されます。

名前

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このルックアップルールは、CMDB 内の CI の名前での検索を試みます。CI クラスの Object_id 列で検索される名前は、sn_capi_resource_type テーブルのリソースタイプに対応します。

注:
Palo Alto Prisma Cloud アプリケーションの場合、この CI ルックアップルールは AWS::RDS::DBInstance、 AWS::ElasticLoadBalancing::LoadBalancer、および AWS::CloudTail::Tail のリソースタイプに対してのみ実行されます。この CI ルックアップルールを実行するリソースタイプを追加できます。

リソース **ID**

このルックアップルールは、CMDB 内の CI のリソース ID での検索を試みます。CI クラスの Object_id 列で検索されるリソース ID は、sn_capi_resource_type テーブルのリソースタイプに対応します。

注:
[順序 **(Order)**] フィールドで CI ルックアップルールの優先順位を設定できます。最小の順序値の CI ルックアップルールが最初に実行されます。

脆弱性対応 ワークスペース

脆弱性対応ワークスペースは、機能の統合ビューを提供します。これにより、同じペイン内からマルチタスクを実行できるため、生産性が向上し、時間を節約できます。

脆弱性対応 ワークスペース

脆弱性マネージャー ワークスペース	**IT** 修復ワークスペース	脆弱性アセスメントのワークスペース
脆弱性マネージャー ワークスペースの詳細	IT 修復ワークスペースについて学ぶ	脆弱性アセスメントのワークスペースの詳細

事前準備

ワークスペースを使用する前に、次のことを行います。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- いくつかの構成タスクを実行する必要があります。詳細については、「脆弱性対応 ワークスペースの構成」を参照してください。
- 修復タスクおよび修復タスクルールの更新に関する重要な情報と、ワークスペースに関する主要な用語と概念を「脆弱性対応 ワークスペースおよび修復タスクと修復タスクのルールの最新情報」で確認します。

トラブルシューティングとサポート

- ServiceNow Community の Security Operations
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

脆弱性対応 ワークスペースの概要

脆弱性マネージャーのワークスペースと IT 修復ワークスペースでは、脆弱性対応、アプリケーション脆弱性対応、コンテナ脆弱性対応およびコンフィグレーションコンプライアンスがサポートされています。

脆弱性マネージャー、IT 修復、および脆弱性アセスメントのワークスペース

Vulnerability Manager ワークスペース

脆弱性マネージャーは、会社の資産をマルウェアや悪意のある攻撃から保護します。脆弱性対応アプリケーションを使用して、Now Platform 内の単一の作業領域から、脆弱性ライブラリやサードパーティのスキャナーデータアプリケーションからインスタンスにインポートされた現在の脆弱性データを使用して、重大な脆弱性と構成ミスを特定し、それらに優先順位を付け、修復タスクのリストを IT 部門に送信してスペシャリストが対応できるようにします。

IT 修復ワークスペース

IT スペシャリストは、脆弱性マネージャーから送信されたリストまたは修復タスク (RT) を使用して、自分または自分のグループにアサインされた重大な脆弱性を監視し、解決します。脆弱性一致アイテムのグループの修正をパッチ、ソリューション、脆弱性の再スキャン、変更の要求、例外、その他のツールで行い、脆弱性一致アイテムやテスト結果をすべて 1 か所で修正します。

脆弱性アセスメントのワークスペース

脆弱性イベントマネージャーは、エクスポージャーアセスメントを実行し、特にゼロデイイベントなどの重大な脆弱性イベント中に重大な脆弱性イベントを積極的に管理します。

主な機能

脆弱性対応のワークスペースには、以下の機能と拡張機能が含まれています。

- Vulnerability Manager ワークスペース の一括編集機能で、複数のレコードを同時に更新します。詳細については、「Vulnerability Manager ワークスペース での一括編集の使用」を参照してください。
- 脆弱性マネージャーワークスペースの [ダッシュボード] ページのネクストエクスペリエンス UI で、脆弱性管理 (PA)、脆弱性の承認、CISO、コンテナ脆弱性管理の概要 (Container Vulnerability Management Overview)、アプリケーションの脆弱性管理ダッシュボード、統一脆弱性対応 (Unified Vulnerability Response)、ヘルスダッシュボードを表示します。詳細については、「の [ダッシュボード] ページ Vulnerability Manager ワークスペース」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- IT 修復ワークスペースの [ダッシュボード] ページのネクストエクスペリエンス UI で、脆弱性修復ダッシュボードを表示します。詳細については、「の [ダッシュボード] ページ IT 修復ワークスペース」を参照してください。
- 修復タスク (VUL、AVUL、CVUL、CRG) を Vulnerability Manager ワークスペース と IT 修復ワークスペースで手動で作成します。詳細については、「で修復タスクを手動で作成する Vulnerability Manager ワークスペース」と「で修復タスクを手動で作成する IT 修復ワークスペース」を参照してください。
- 修復タスク (VUL、AVUL、CVUL、CRG) を Vulnerability Manager ワークスペース と IT 修復ワークスペース に分割します。詳細については、それぞれ「で修復タスクとレコードの例外を要求する Vulnerability Manager ワークスペース」と「IT 修復ワークスペースでの修復タスクの分割」を参照してください。
- 脆弱性マネージャーワークスペースと IT 修復ワークスペースで、脆弱性一致アイテム (VIT、AVIT、CVIT) と修復タスク (VUL、AVUL、CVUL、CRG) のポリシー例外を要求します。詳細については、それぞれ「で修復タスクとレコードの例外を要求する Vulnerability Manager ワークスペース」と「IT 修復ワークスペースで GRC: ポリシーとコンプライアンス管理 を使用して例外を要求する」を参照してください。
- 脆弱性危機管理 (VCM) で重大な脆弱性イベントを作成および追跡します。詳細については、「脆弱性アセスメントのワークスペースの詳細」を参照してください。
- Vulnerability Manager ワークスペースの補完コントロールライブラリに補完コントロールを追加します。詳細については、「補完コントロールをライブラリに追加する」を参照してください。
- IT 修復ワークスペースから、ホスト脆弱性一致アイテムや修復タスクのリスク削減を要求します。詳細については、「脆弱性一致アイテムまたは修復タスクのリスク削減の要求」を参照してください。
- Vulnerability Manager ワークスペース から、アプリケーションおよびコンテナ脆弱性一致アイテムのアジャイルな問題や Jira の問題を作成します。詳細については、「フォームアクションを使用して Agile の問題を手動で作成する」と「リストアクションを使用して Agile の問題を手動で作成する」を参照してください。

ファミリーリリースと互換性のあるバージョンについての詳細は、HI ナレッジベース記事「Vulnerability Response Compatibility Matrix and Release Schema Changes (脆弱性対応互換性マトリクスおよびリリーススキーマの変更点) [KB0856498]」を参照してください。

脆弱性対応 ワークスペースを使用したパッチオーケストレーション

脆弱性対応 を使用したパッチオーケストレーションによって、大規模な資産グループの重大な脆弱性に対するパッチとパッチ展開を管理できます。

ワークスペースでのパッチオーケストレーション

脆弱性対応 アプリケーションを使用したパッチオーケストレーションでは、サードパーティのソリューション統合、パッチベンダー、および脆弱性スキャナーからのスケジュール済みインポートが使用されます。

脆弱性対応 アプリケーションを使用したパッチオーケストレーションは、クラシック環境と 脆弱性対応 ワークスペースの両方でサポートされています。相関関係のあるデータは、ワークスペースとクラシック環境の両方でロールアップされて表示されます。クラシック環境での機能、要件、およびパッチオーケストレーションに関する情報の概要については、「脆弱性対応 を使用したパッチオーケストレーション」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- パッチベンダーとの統合のサポートの詳細については、「脆弱性対応 との HCL BigFix パッチオーケストレーション統合の概要」および「脆弱性対応 Patch Orchestration Integration with Microsoft SCCM の概要」を参照してください。
- ワークスペースでパッチフォームレコードをスケジュールする方法については、「Microsoft SCCM integration with 脆弱性対応 とのパッチスケージュール」および「脆弱性対応 Patch Orchestration Integration HCL BigFix のパッチのスケージュール」を参照してください。

パッチオーケストレーション統合に必要なアプリケーションと依存関係の利用可能なバージョン

脆弱性対応 のワークスペースでパッチオーケストレーションデータと利用可能な更新 (パッチ) を表示するには、次のアプリケーションが必要です。リストされているすべてのアプリケーションは ServiceNow Store で入手できます。一部のアプリケーションには別のサブスクリプションが必要です。「脆弱性対応 を使用したパッチオーケストレーション」を参照してください。

必要なロール

脆弱性対応 ワークスペースに必要な sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin ロールに加えて、ユーザーがデータを表示してパッチをスケジュールするために、使用しているパッチオーケストレーション統合に固有のロールが必要です。これらのロールの詳細については、次に示すサポートされている統合を参照してください。

「脆弱性対応 との HCL BigFix パッチオーケストレーション統合の概要」および「脆弱性対応 Patch Orchestration Integration with Microsoft SCCM の概要」を参照してください。

脆弱性対応 ワークスペース内のパッチデータ

IT 修復ワークスペースでは、ワークスペース内のパッチデータを表示できます。

- ホームビューでスコアカードをクリックすると、VI の優先ソリューション、脆弱な CI、および VI の優先パッチのレコードが表示されます。
- リストビューでは、すべてのパッチ更新レコード (VPU) と、自分にアサインされていてパッチがある脆弱性一致アイテムを利用可能なリンクから確認できます。

次のレコードからパッチをスケジュールできます。

- パッチ更新 (VPU)
- 修復タスク (RT)
- 検出されたアイテム (SDI)

関連エントリフォームで、 脆弱性マネージャーワークスペースでは、パッチを表示できます。

- ホームビューの [ウォッチトピック] の [脆弱性一致アイテム] タブで、優先パッチと潜在的なパッチ、パッチがスケジュールされている日付、その他の情報を確認できます。
- 修復作業レコードのリストビューで、[脆弱性一致アイテム] タブに VIT レコードのパッチデータを表示できます。

脆弱性対応 ワークスペースおよび修復タスクと修復タスクのルールの最新情報

修復タスクは、レコード (VIT、AVIT、CVIT、CTR) を 脆弱性対応 ワークスペースにバンドルします。

脆弱性対応 ワークスペースの主要な用語

脆弱性対応のワークスペース、またはワークスペース

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 は 脆弱性対応 ワークスペースをサポートしています。クラシック コア UI エクスペリエンスまたはワークスペースのいずれかを使用できます。

クラシック (レガシー) UI

コア UI エクスペリエンスを指します。一部のアクションの実行といくつかのリストの表示は、引き続きクラシック環境で行います。

脆弱性マネージャーのワークスペース

このワークスペースで、マネージャーはターゲットの脆弱性を監視し、最も関心のある VI とテスト結果を選択して IT チームにアサインします。

IT 修復ワークスペース

このワークスペースでは、IT チームはセキュリティによってアサインされた最も重要な脆弱性に集中できます。影響を受ける個別の構成アイテム (CI)、ソリューション、および修復の進捗状況を含む IT 中心の情報は、このワークスペースで修復オーナーが簡単に利用できます。

脆弱性アセスメントのワークスペース

このワークスペースでは、脆弱性アナリストがゼロデイ脆弱性の分析時に脆弱性アセスメントを実行できます。ゼロデイ脆弱性が特定されたら、この脆弱性に関連付けられている潜在的な影響とリスクを評価できます。アナリストは、影響を受けるシステム、アプリケーション、またはネットワークコンポーネントを分析して、組織内での重大度と発生する可能性がある攻撃ベクトルを把握できます。

監視トピック

ウォッチトピックでは、脆弱性マネージャーと脆弱性アナリストが脆弱性マネージャーワークスペースで監視する脆弱性一致アイテムのセグメントを定義します。ウォッチトピックには、傾向、CI、および脆弱性関連の統計情報を含む VI とテスト結果のセグメントに関連する、焦点を絞ったレポートの概要セットが表示されます。こうしたトピックのダッシュボードを使用して、傾向を監視できます。ダッシュボードは、マネージャーが以下を行うのにも役立ちます。

- 最重要アイテムの修復の進捗状況を表示する
- 重要なシステムの脆弱性の有無を判断する
- 新しいエクスプロイトが公開される時期を確認する
- 特定の一連の脆弱性を解決するために迅速な対応を促進する

修復作業 (RE)

修復作業は、ウォッチトピックに記載されている脆弱性を IT チームが修正する時であると脆弱性マネージャーが決定したときに作成されます。脆弱性マネージャーと脆弱性アナリストは、たとえばアサイン先グループや脆弱性別に修復タスクを作成する方法を選択できます。修復タスクは修復作業に含まれています。

修復タスク (VUL)

IT チームは、修復タスクを使用して、セキュリティによってアサインされた脆弱性を修復します。修復タスクは、脆弱性を修正するために必要なアクションのリストです。セキュリティマネージャーが修復作業を作成すると、修復タスクが自動的に作成されます。

ワークスペースの開発

以前のバージョンの 脆弱性対応 では、セキュリティおよび脆弱性アナリストが一連のレコード (VIT、AVIT、CVIT、CTR) を監視するには、次の 2 つのオプションがありました。

- すべての VI を要約する概要ダッシュボード
- 修復タスク

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性一致アイテムは、事前定義された修復タスクルールに従って自動的に修復タスクに分類されていました。修復タスクは、脆弱性一致アイテムの管理可能なチャンクを修正する IT チームをサポートするように設計されていました。

この自動化により、大量のレコードを自動的にグループ化して、一括アサインと修正を行うことが可能になりました。しかし、脆弱性アナリストと脆弱性マネージャーは、修復タスクからレコードのセット全体を監視することは困難であることがわかりました。大規模なグループにはパフォーマンスの問題があるのに加え、最も重大であると判断した脆弱性のみを除去する機能的な修復タスクのルールを作成することは困難です。

脆弱性対応 ワークスペースには、以下の機能があります。

- セキュリティマネージャーが、アクティブな VI とテスト結果を抽出して時間の経過とともに監視し、最も重要であると判断した脆弱性の修復を促進する。
- IT 中心の情報を 1 か所で IT チームに提供し、それを使用してセキュリティによってアサインされた脆弱性を修正できるようにする。

ワークスペースでの修復タスクの更新

脆弱性マネージャーワークスペースで、脆弱性アナリストと脆弱性マネージャーは、修復対象の VI を監視およびアサインするための 2 つの新しい方法として、ウォッチトピックと修復作業を使用します。

脆弱性グループの名前は「修復タスク」に変更されています。この変更は、従来の UI とワークスペースの両方にあるリスト、レコード、およびルールのラベルに適用されます。修復タスクは、IT チームが IT 修復ワークスペースで作業できるように設定されています。次のリストは、脆弱性マネージャーまたは脆弱性アナリストが脆弱性とテスト結果を監視し、フィルタリングしてアサインする方法を示しています。

1. 脆弱性マネージャーワークスペースでは、マネージャーはウォッチトピックのインポートされた脆弱性と構成ミスを監視します。マネージャーとアナリストは、ウォッチトピックを使用して、最も重要と思われるフィルタリングされたレコードの動的なセットを経時的に監視します。
2. ウォッチトピックを使用すると、セキュリティマネージャーは、修復作業 (RE) で VI を IT チームに渡すタイミングと VI の種類を決定できます。こうした RE は、セキュリティマネージャーが IT チームに修正を求めている VI の静的リストです。

   修復作業では、修復タスク (VUL、AVUL、CVUL、CRG) にレコードをバンドルする方法について、マネージャーには 4 つのオプションがあります。修復タスクは、レコードに元々関連付けられていたアサイン先グループに基づいて、自動的に IT チームにアサインされます。
3. IT チームは、すべてのレコードをソートしなくても、IT 修復ワークスペースで修復タスクを実行できます。

   修復タスクは、以前のバージョンの脆弱性対応での修復タスクと同じステータスに移行します。修復タスクのすべてのレコードがクローズされると、その修復タスクはクローズされ、 非アクティブに設定されます。

   修復の進捗状況は、ウォッチトピックと IT 修復ホームページの可視化されたデータで更新されます。

ワークスペースでの修復タスクルールの更新

脆弱性グループルールは、修復タスクルールと呼ばれます。この変更は、従来の UI とワークスペースの両方にあるリスト、レコード、およびルールのラベルに適用されます。

テーブル名 ([sn_vul_m2m_vul_group_item] など) は変更されません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

以前のバージョンの 脆弱性対応 で脆弱性グループルールを作成した場合でも、修復タスクルールとしてラベル付けできます。

ただし、ワークスペースでは、大量のレコードを修復タスクに整理するための主要な方法として、修復タスクルールが使用されなくなりました。ワークスペースに慣れたら、修復タスクルールを非アクティブにしておくことをお勧めします。

脆弱性対応 ワークスペースの使用を段階的に開始することもできます。

1. 以前のバージョンの 脆弱性対応 からアップグレードする場合、既存の修復タスクルールは保持されます。そうしたルールを引き続きワークスペースで使用できます。デフォルトのグループルールである [脆弱性] は、デフォルトでは非アクティブです。
2. アサインルールを設定し、必要に応じてリスクルールを設定してから、インポートを実行します。
3. 脆弱性マネージャーまたは脆弱性アナリストは、脆弱性マネージャーワークスペースのウォッチトピックから監視対象のセグメントを選択できます。ウォッチトピックはスタンドアロン機能として使用できます。レコードのサブセットを選択し、ダッシュボードを使用して傾向を監視します。それにより、修復作業を行う場所とタイミングを決定できます。
4. 脆弱性マネージャーまたは脆弱性アナリストは、レコードのサブセットを修復する時期であると判断したら、ウォッチトピックから修復作業を作成します。修復作業を作成するときに IT チームに渡すための修復タスクも自動的に作成されます。
5. 脆弱性マネージャーまたは脆弱性アナリストは、時間の経過とともに、修復タスクルールで自動的に処理できるルーチンパターンを発見することがあります。

修復タスクルールを表示するには、[すべて] メニューから [脆弱性対応]、[アプリケーション脆弱性対応]、[コンテナ脆弱性対応]、および [コンフィグレーションコンプライアンス] の各修復タスクルールモジュールに移動します。

脆弱性対応 ワークスペースのアサインルール、修復タスクルール、修復作業、および脆弱性一致アイテムの詳細

- 修復タスクレコードは、クラシック環境とワークスペースの両方でリストとレコードに表示されます。
- 修復タスクは、脆弱性グループと同じ状況に移行します。修復タスクのすべてのレコードがクローズされると、その修復タスクは [非アクティブ] ステータスに移行します。
- チームによる修復を支援するために、脆弱性一致アイテムは 1 回の修復作業にのみ含めることができます。修復作業に入ると、脆弱性一致アイテムは作成した他のどの修復作業にも追加されません。
- 修復作業を削除すると、その修復作業は非アクティブになり、アクティブな VI を新しい修復作業に使用できるようになります。
- レコード (VIT、AVIT、CVIT、CTR) は複数の修復タスクに含めることができます。
- 修復タスクは、修復作業内の脆弱性一致アイテムに関連付けられているアサイン先グループに基づいて、自動的に IT チームにアサインされます。オンデマンドで修復タスクを作成する場合は、アサイン先グループを選択します。
- 以前のバージョンの 脆弱性対応 からアップグレードする場合、アサインルールは従来の UI で保持されます。
- 以前のバージョンの 脆弱性対応 からアップグレードする場合、現在のユーザーとグループは継承され、ワークスペースでアクセスできます。

修復作業のライフサイクルの詳細については、「脆弱性対応ワークスペースの修復作業、修復タスク、およびレコードのライフサイクル」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 ワークスペースの構成とセットアップ

アサインルールと修復タスクルールの詳細については、「脆弱性対応 ワークスペースの構成」および「脆弱性対応 アサインルールの概要」を参照してください。

新規のお客様で、まだ追加していない場合は、必要な修復グループに脆弱性一致アイテムと修復タスクがアサインされるようにユーザーとグループを設定する必要があります。脆弱性対応アサインルールを使用して、作業をグループにアサインします。

脆弱性対応 ワークスペースの構成

ワークスペースを使用する前に、以下のセットアップタスクが完了していることを確認します。

始める前に

必要なロール：admin (ロールをユーザーとグループに、およびユーザーをグループにアサインする場合)。

sn_vul.vulnerability_admin (ルールの編集、作成、脆弱性対応 アプリケーションの構成を行う場合)。

以下のセットアップタスクが完了していることを確認します。これらのタスクを実行する方法の詳細については、リストの後の手順を参照してください。

タスク	説明
☐	まだアサインされていない場合は、適切なロールをユーザーとグループにアサインして、ワークスペースにアクセスできるようにします。 必要なロール：admin 詳細については、以下の手順を参照してください。
☐	脆弱性一致アイテムが修正のために適切なグループにアサインされるように、アサインルールをセットアップします。 必要なロール：sn_vul.vulnerability_admin。 アサインルールについては、「脆弱性対応 アサインルールの概要」を参照してください。クラシック環境でアサインルールを作成および編集します。
☐	(オプション)：修復タスクルールを編集または作成します。 必要なロール：sn_vul.vulnerability_admin。

自動翻訳

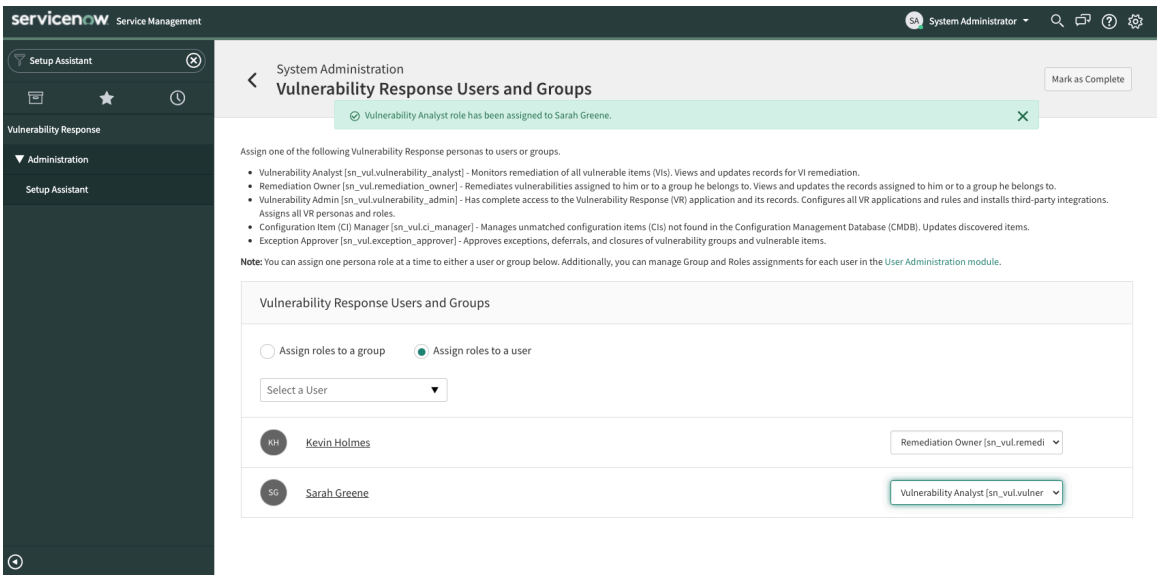
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスク	説明
	注: 機能的には、修復タスクルールは、以前のバージョンの 脆弱性対応 の修復タスクルールと同じように機能します。ただし、修復タスクルールから自動的に作成された脆弱性グループとは異なり、修復作業を作成すると修復タスクが作成されます。修復作業で脆弱性一致アイテムを修復タスクにバンドルするには、次のオプションがあります。 • アサイン先グループ別 (By Assignment group) • アサイン先グループと構成アイテム別 (By Assignment group and configuration item) • アサイン別グループと脆弱性 • なし：VI を修復タスクに手動で追加する場合は、このオプションを使用します。詳細については、「の修復作業から修復タスクをオンデマンドで作成する Vulnerability Manager ワークスペース」を参照してください。 クラシック環境で VI を自動的にグループ化する方法とグループルールを再適用する方法の詳細については、「脆弱性対応修復タスクとタスクルールの概要」を参照してください。
☐	修復ターゲットルールを編集します。 必要なロール：sn_vul.vulnerability_admin。 クラシック環境で修復ターゲットルールを追加します。修復ターゲットルールの詳細については、「脆弱性対応 修復ターゲットルールの作成または編集」を参照してください。

自動翻訳

手順

1. クラシック環境で admin ロールを持つユーザーとして 脆弱性対応 アプリケーションをインストールしてアクティブ化した後、次に移動します: **All** (すべて) > 脆弱性対応 > アドミニストレーション > セットアップアシスタント.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. セットアップアシスタントで、ユーザーを以下のグループにアサインします。

   注:
   脆弱性対応ワークスペースにおいてユーザーをアサインできるユーザーグループ数の上限は 1000 です。

   以下のグループは 脆弱性対応 アプリケーションで提供され、ワークスペースで使用されます。それらのグループにセットアップアシスタントでユーザーをアサインできます。

   - 修復オーナー：このグループは、IT 修復ワークスペース内の IT 修復オーナー用です。このロールを持つユーザーは、修復タスクで自分にアサインされた脆弱性を修正できます。

     注:

     修復オーナーが変更要求を作成および表示する場合、および IT 修復ワークスペースとクラシック環境において脆弱な構成アイテム (CI) データを表示できるようにする場合、修復オーナーに itil ロールをアサインします。itil ロールは、グループ内のすべてのメンバーにではなく、個々のユーザーにアサインすることをお勧めします。cmdb_read ロールは、ユーザーがワークスペース内の CI データを表示するためのオプションでもあります。

   - v16.1 以降は、IT 修復オーナーへのメールリマインダーを設定できるようになりました。ワークスペースへのメール通知を設定するには、「脆弱性対応 ワークスペースでのメール通知の設定」を参照してください。
   - 脆弱性アドミン：このグループは脆弱性マネージャー用です。このロールでは、セットアップアシスタントで 脆弱性対応 アプリケーションを構成できます。このロールには、例外と誤検出の要求を処理する権限もあります。
   - 脆弱性アナリスト：このグループは、脆弱性マネージャーワークスペース内のセキュリティマネージャー、脆弱性マネージャー、およびアナリスト用です。このロールでは、脆弱性の監視、ウォッチトピックと修復作業の作成、修正の進捗状況の監視を行うことができます。
   - 誤検出承認者：このグループのユーザーは、脆弱性一致アイテムまたは修復タスクの誤検出要求を処理できます。誤検出要求には、単一レベルの承認プロセスが必要です。このグループへのユーザーのアサインは、セットアップアシスタントの外部の [ユーザー管理] で管理できます。
   - 例外承認者：脆弱性一致アイテムまたは修復タスクの例外要求は、デフォルトの 2 レベルの承認ワークフローを使用して承認されます。例外要求には 2 つのレベルの承認者が必要です。例外承認者 - レベル 1 と例外承認者 - レベル 2 の両方の承認グループにユーザーを追加します。要求はレベル 1 の承認者によって承認された後、レベル 2 の承認者に送信されます。このグループへのユーザーのアサインは、セットアップアシスタントの外部の [ユーザー管理] で管理できます。

     注:
     誤検出および例外要求を送信する前に、ユーザーを承認グループに追加します。承認権限をユーザーにアサインする前に要求を作成すると、そのユーザーには要求が表示されない場合があります。

   または、[ユーザー管理] リンクをクリックし、以下の詳細ロールを管理してユーザーや既存のグループにアサインします。これらのロールにより、ユーザーは 脆弱性対応 アプリケーションとワークスペース内で特定のアクションを実行できるようになります。

   - sn_vul.vulnerability_admin
   - sn_vul.vulnerability_analyst
   - sn_vul.remediation_owner
   - IT 修復ワークスペースとクラシック環境において変更要求の作成や表示を行えるようにする場合は、 itil ロールをアサインします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ペルソナロールのユーザーへのアサインおよびユーザーのグループへのアサインの詳細については、「脆弱性対応 のペルソナと詳細なロール」および「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。

3. 修復タスクは、作成されると、処理に備えて IT 修正アサイン先グループに自動的に渡されます。
   - アサイン先グループ別 (By Assignment group)
   - アサイン先グループと構成アイテム別 (By Assignment group and configuration item)
   - アサイン別グループと脆弱性
   - なし：VI を修復タスクに手動で追加する場合は、このオプションを使用します。

     注:
     脆弱性対応 のバージョン 18.0 では、[なし] オプションは使用できません。

   脆弱性対応 の以前のバージョンからアップグレードする場合、アサイン先グループは保持されます。ただし、ウォッチトピックと修復作業に慣れるまで、こうしたグループを編集して、脆弱性一致アイテムが特定のアサイン先グループに関連付けられるようにすることをお勧めします。たとえば、製品または地域別にアサイン先グループを作成できますが、組織に最適な基準を使用できます。

   アサインルールを使用して、修復タスクをグループにアサインすることもできます。以下のアイテムに対しては、優先度の高いルールのみを実行することを推奨します。
   - 特別な処理が必要なアイテム
   - リスクが重要な意味を持つアイテム、または VI が規制コンプライアンスによる処理を必要とするアイテム

   アプリケーションに用意されている以下のアサインルールは、デフォルトで有効です。
   - 廃止された CI アサインルール
   - CI サポートグループにアサイン
   - ワークステーションアサインルール
   - データベースアサインルール
   - Web アプリケーションアサインルール
   - Windows Server アサインルール
   - 非 Windows Server アサインルール
   - すべてのアサインルールのキャッチ

   アサインルールについては、「脆弱性対応 アサインルールの概要」を参照してください。クラシック環境でアサインルールを作成および編集します。

4. オプション: 修復タスクルールを編集または作成します。

   (Optional) ワークスペースでは、修復作業を作成すると修復タスクが作成されます。修復作業で脆弱性一致アイテムを修復タスクにバンドルするには、次のオプションがあります。
   - アサイン先グループ別 (By Assignment group)
   - アサイン先グループと構成アイテム別 (By Assignment group and configuration item)
   - アサイン別グループと脆弱性

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- なし：VI を修復タスクに手動で追加する場合は、このオプションを使用します。詳細については、「の修復作業から修復タスクをオンデマンドで作成する Vulnerability Manager ワークスペース」を参照してください。

  注:
  脆弱性対応 のバージョン 18.0 では、[なし] オプションは使用できません。

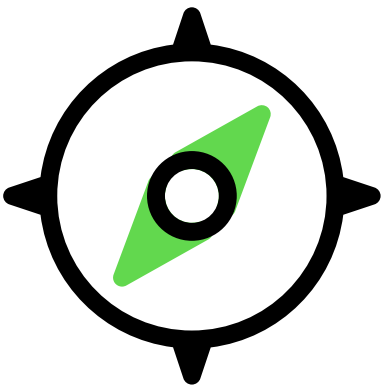
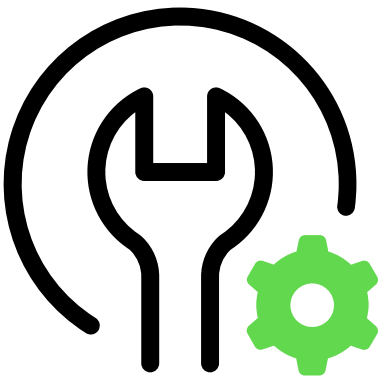
クラシック環境で VI を自動的にグループ化する方法とグループルールを再適用する方法の詳細については、「脆弱性対応修復タスクとタスクルールの概要」を参照してください。

Vulnerability Manager ワークスペース

この Vulnerability Manager ワークスペース により、脆弱性マネージャーと脆弱性アナリストは、最も関心のある脆弱性と構成ミスを監視し、修正のために IT チームに送信する脆弱性を戦略的に決定できます。

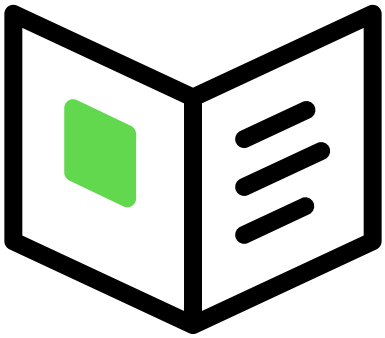
V18.0 脆弱性マネージャーのワークスペースのデモ

開始するには

探索	監視と管理	修復
		
の機能について学習する Vulnerability Manager ワークスペース	で脆弱性一致アイテム (VIT、AVIT、CVIT) とテスト結果を監視および管理する方法を学習する Vulnerability Manager ワークスペース	で脆弱性一致アイテム (VIT、AVIT、CVIT) とテスト結果を修復する方法を学習する Vulnerability Manager ワークスペース

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

	Reference (参照)  を使用するために必要な追加情報の詳細 Vulnerability Manager ワークスペース	

トラブルシューティングとサポート

- ServiceNow Community の Security Operations
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

Vulnerability Manager ワークスペース の探索

脆弱性マネージャーおよびアナリストは、Vulnerability Manager ワークスペースですべての脆弱性タイプの統合ビューを得られます。ホスト、アプリケーション、コンテナの脆弱性と構成の問題を確認し、これらの脆弱性と構成ミスに関する監視トピックを作成して、修復作業と修復タスクを作成できます。

注:
脆弱性対応 の v19.0 以降では、次の用語の名前が変更されました。

用語の変更

v19.0 より前の用語	**v19.0** 以降の用語
テスト結果グループ	修復タスク
構成の問題	構成テスト結果
ポリシー	テストグループ

Vulnerability Manager ワークスペースを表示するには、 ワークスペース > 脆弱性マネージャー ワークスペース.

この Vulnerability Manager ワークスペース は、次のページで構成されています。

ホームページ

ホスト脆弱性、アプリケーション脆弱性、コンテナ脆弱性、および構成テスト結果のサマリーを可視化するために使用される事前定義されたフィルターで構成されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ホームページの詳細については、「のホームページ Vulnerability Manager ワークスペース」を参照してください。

> **注:**
> 脆弱性対応の v21.0 以降、監視トピックは [監視トピック] ページに表示されます。

[監視トピック] ページ

ホスト脆弱性、アプリケーション脆弱性、コンテナ脆弱性、および構成テスト結果の 4 つのモジュールに分類される監視トピックのリストで構成されます。

監視トピックの詳細については、「の [監視トピック] ページ Vulnerability Manager ワークスペース」を参照してください。

ダッシュボードページ

脆弱性管理、脆弱性管理 (PA)、脆弱性の承認、CISO、コンテナ脆弱性管理の概要、アプリケーションの脆弱性管理、統一脆弱性対応、および健全性の各ダッシュボードで構成されます。

詳細については、「の [ダッシュボード] ページ Vulnerability Manager ワークスペース」を参照してください。

> **注:**
> ダッシュボードページは、脆弱性対応のバージョン 19.0 から表示されます。

リストページ

修復作業、修復タスク、ホスト脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、構成テスト結果、例外、承認、ライブラリについて、デフォルトおよびカスタマイズされたリストページで構成されます。

詳細については、「のリストページ Vulnerability Manager ワークスペース」を参照してください。

自動翻訳

Vulnerability Manager ワークスペースでワークフロー例を表示する

Vulnerability Manager ワークスペースのエンドツーエンドワークフローの例を表示します。脆弱性マネージャーまたは脆弱性アナリストがワークスペースを使用して重要なレコードを監視し、修復タスクを作成して IT に渡す方法を参照してください。

始める前に

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

手順

次のビデオをクリックすると、ワークフローのステップが表示されます。
Vulnerability Manager ワークスペース デモ

前ビデオには、次のタスクが含まれています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. ワークスペースの [監視トピック] ページの監視トピックをクリックして、ダッシュボードにデータを表示します。

b. フィルター条件を使用してウォッチトピックを作成し、一致するレコードをプレビューします。監視トピックの作成方法の詳細については、「で監視トピックを作成する Vulnerability Manager ワークスペース」を参照してください。

c. ウォッチトピックの [影響を受ける **CI]** タブで、レコードとその関連構成アイテムに関するデータを表示します。可視化の詳細については、「監視トピックの関連アイテムリストと可視化」を参照してください。

d. ウォッチトピックの [個別の脆弱性] タブで、脆弱性に関するデータを表示します。

e. 監視トピックの [脆弱性一致アイテム] タブまたは [構成テスト結果] タブで、監視トピックに関連付けられたレコードを表示します。右にスクロールして、[修復作業] 列で、どのレコードが既に修復作業に含まれているかを表示します。

f. 特定のタイプのレコードのタスクを作成し、修復のために IT にアサインする準備ができたら、ウォッチトピックで [修復作業の作成] を選択します。修復作業の作成方法の詳細については、「で修復作業を作成する Vulnerability Manager ワークスペース」を参照してください。

g. リストビューを選択すると、修復作業、修復タスク、レコード、例外、および承認のリストが表示されます。リストページの詳細については、「のリストページ Vulnerability Manager ワークスペース」を参照してください。

h. リストビューから アクティブな 修復作業リストを選択して修復作業レコードを開き、レコードのステータスと情報を表示します。詳細については、「のリストページ Vulnerability Manager ワークスペース」を参照してください。

i. 修復作業レコードの [修復タスク] タブを選択して、修復レコードに関連付けられた修復タスクを表示します。詳細については、「のリストページ Vulnerability Manager ワークスペース」を参照してください。

j. それぞれの修復作業レコードの [脆弱性一致アイテム] タブ、[アプリケーション脆弱性一致アイテム] タブ、[コンテナ脆弱性一致アイテム] タブ、または [構成テスト結果] タブを選択して、修復作業に関連付けられたレコードリストを表示します。詳細については、「のリストページ Vulnerability Manager ワークスペース」を参照してください。

k. レコードのサブセットの修復作業から新しい修復タスクをオンデマンドで作成する場合は、移動させるレコードを選択し、[修復タスクの作成] をクリックします。詳細については、「の修復作業から修復タスクをオンデマンドで作成する Vulnerability Manager ワークスペース」を参照してください。

のホームページ **Vulnerability Manager** ワークスペース

Vulnerability Manager ワークスペースのホームページには、リスク評価、修復の進捗状況、アサイン先グループへのアサイン、修復タスクのレコード、およびクラウドリソースからの脆弱性が可視化されて、アクティブなレコードの概要が表示されます。

ホームページでは、事前にフィルタリングされたホスト脆弱性一致アイテム、コンテナ脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、および構成テスト結果を可視化して表示できます。フィルターを作成して適用することで、目的のレコードセットの可視化を確認することもできます。フィルターを作成、更新、適用、削除する方法の詳細については、「アクティブなレコード (VIT、AVIT、CVIT、CTR) のサマリーを作成してフィルターを適用する」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ヒント:

sn_vul_cmn_ws.navigate_to_workspace システムプロパティがアドミンによって true に設定されている場合、[すべて] メニューから脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、およびテスト結果モジュールで事前定義されたフィルターリンクを選択すると、これらのリンクがVulnerability Manager ワークスペースのホームページで開き、対応する保存済みフィルターが自動的に選択されます。

たとえば、次の場所に移動して [高リスク] を選択した場合 **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテムの場合、このリンクは Vulnerability Manager ワークスペース のホームページにリダイレクトされ、[ホスト脆弱性] タブで [高リスク] フィルターが自動的に選択されます。

ホームページでは、次の操作を実行できます。

- データをドリルダウンし、可視化をクリックしてレコードリストを表示します。
- [クラシックリストを表示] リンクを選択して、クラシック UI のアクティブなレコードリストに移動します。
- [表示方法] ドロップダウンの横にあるアクティブなレコード数を選択して、Vulnerability Manager ワークスペース内のアクティブなレコードのリストを開きます。
- [選択した保存済みフィルターを更新] アイコンを選択して、可視化を更新します。
- ウィジェットの 3 点メニューの [リフレッシュ] オプションを選択して、最新情報を表示します。

ホスト脆弱性

[ホスト脆弱性] タブには、アクティブなホスト脆弱性の全体的な概要を示す可視化が含まれています。

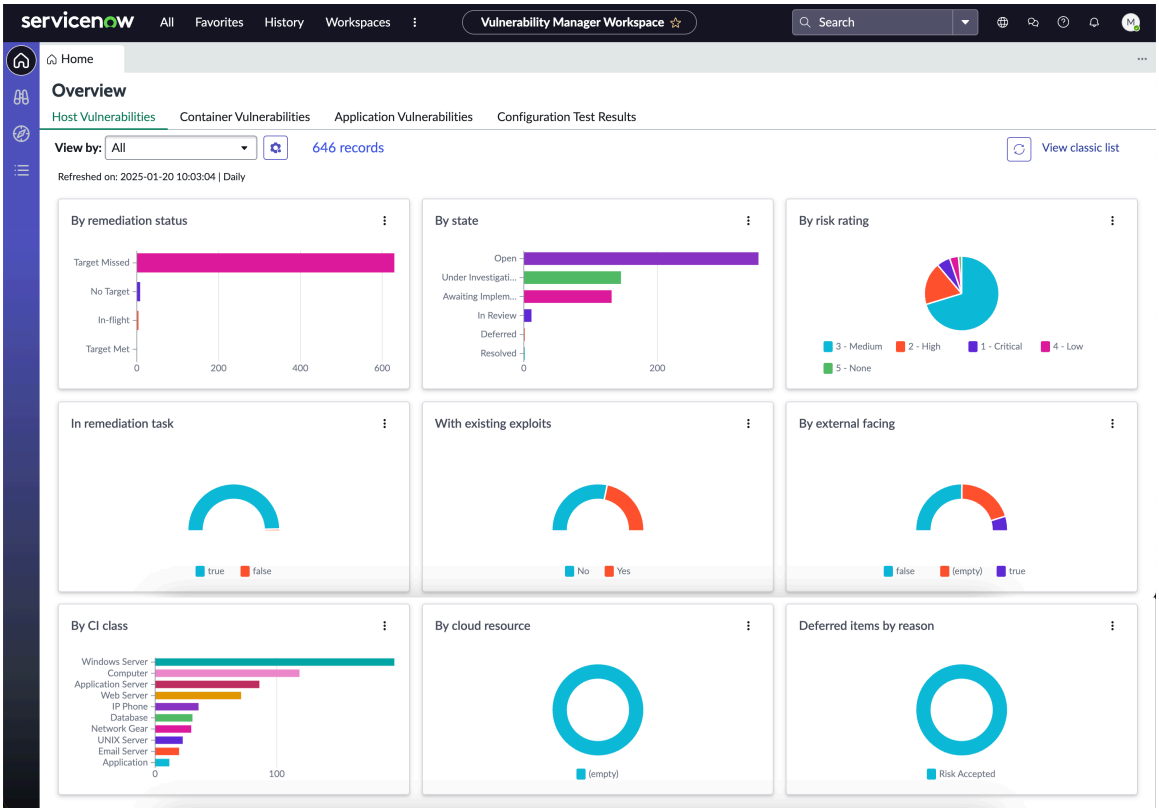
必要なロール：

- sn_vul.vulnerability_analyst および sn_vul.vulnerability_admin を使用して、フィルターを適用して可視化を表示し、フィルターを作成します。
- フィルターを適用して可視化を表示する sn_vul.read_all 詳細ロール。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[ホスト脆弱性] タブ



次の表では、ホームページの [ホスト脆弱性] タブに表示される可視化について説明します。これらの可視化を選択すると、対応するレコードのリストが表示されます。

ホームページの [ホスト脆弱性] タブの可視化

可視化	タイプ	説明
アサイン先グループと修復ステータス別	分布バー	修復ステータスごとにグループ化されたさまざまなアサイン先グループにアサインされたアクティブなレコード。
ステータス別	棒グラフ	さまざまな状況 (オープン、調査中、実装待ち、レビュー中、解決済み、保留) 別に分類されたアクティブなレコード。
リスク評価別	円グラフ	リスク評価 (1 - 重大、2 - 高、3 - 中、4 - 低、5 - なし) で分類されたアクティブなレコード
修復タスク中	半円ドーナツ	修復タスクの一部であるかないかにかかわらずアクティブなレコード。
既存のエクスプロイトあり	半円ドーナツ	既知のエクスプロイトの有無にかかわらずアクティブなレコード。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ホームページの [ホスト脆弱性] タブの可視化 (続く)

可視化	タイプ	説明
外向き別	半円ドーナツ	インターネットへの資産エクスポージャーによって分類されたアクティブなレコード。
CI クラス別	棒グラフ	CI クラス別に分類されたアクティブなレコード。
クラウドリソース別	ドーナツグラフ	さまざまなクラウドリソース別に分類されたアクティブなレコード。
理由別の保留アイテム	ドーナツグラフ	理由別にグループ化されたアクティブな保留レコード。

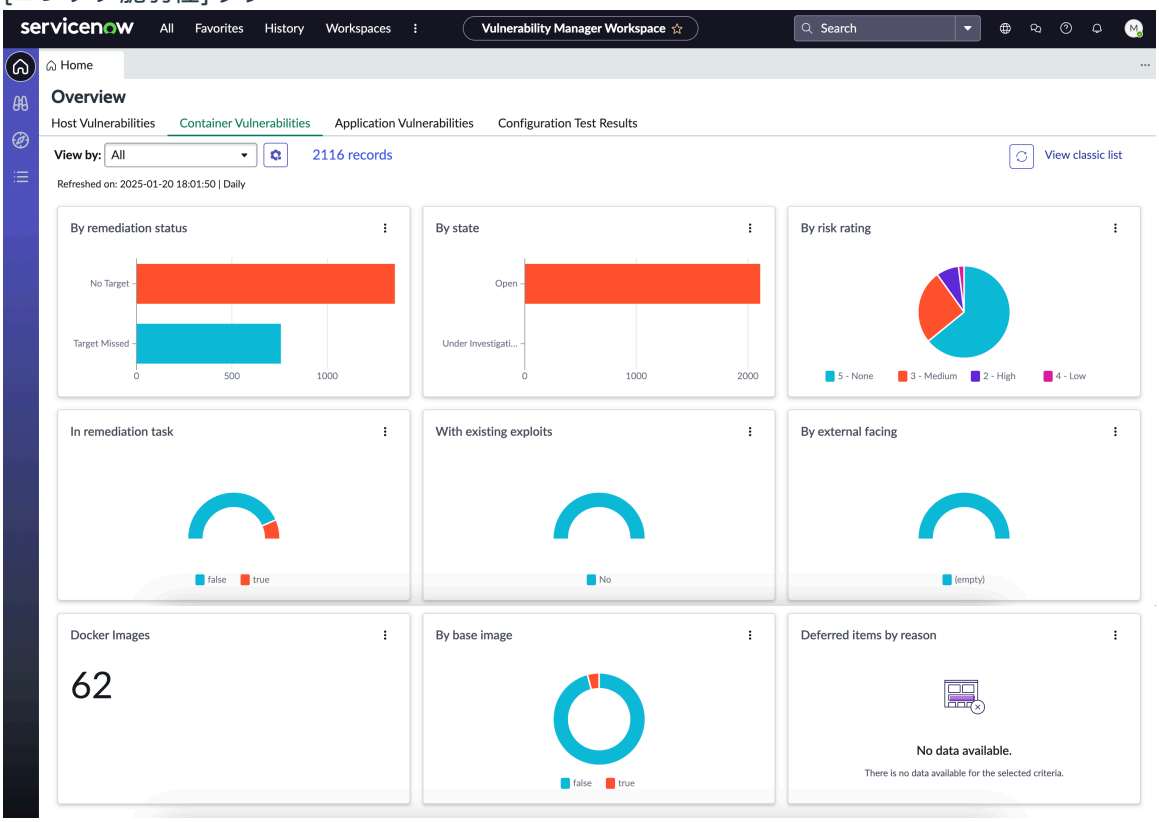
コンテナ脆弱性

[コンテナ脆弱性] タブには、アクティブなコンテナ脆弱性一致アイテムの全体的な概要を示す可視化が含まれています。

必要なロール：

- sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin:フィルターを適用して可視化を表示し、フィルターを作成します。
- フィルターを適用して可視化を表示する sn_vul_container.read_all 詳細ロール。

[コンテナ脆弱性] タブ



次の表では、ホームページの [ホスト脆弱性] タブに表示される可視化について説明します。これらの可視化を選択すると、対応するレコードのリストが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ホームページの [コンテナ脆弱性] タブの可視化

可視化	タイプ	説明
アサイン先グループと修復ステータス別	分布バー	修復ステータスごとにグループ化されたさまざまなアサイン先グループにアサインされたアクティブなレコード。
ステータス別	棒グラフ	さまざまな状況 (オープン、調査中、実装待ち、レビュー中、解決済み、保留) 別に分類されたアクティブなレコード。
リスク評価別	円グラフ	リスク評価 (1 - 重大、2 - 高、3 - 中、4 - 低、5 - なし) で分類されたアクティブなレコード
修復タスク中	半円ドーナツ	修復タスクの一部であるかないかにかかわらずアクティブなレコード。
既存のエクスプロイトあり	半円ドーナツ	既知のエクスプロイトの有無にかかわらずアクティブなレコード。
外向き別	半円ドーナツ	インターネットへの資産エクスポージャーによって分類されたアクティブなレコード。
Docker イメージ	カウント	一意の Docker イメージの数。
基本イメージ別	ドーナツグラフ	イメージのタイプ別に分類されたアクティブなレコード数。
理由別の保留アイテム	ドーナツグラフ	理由別にグループ化されたアクティブな保留レコード。

アプリケーション脆弱性

[アプリケーション脆弱性] タブには、アプリケーション脆弱性の全体的な概要を示す可視化が含まれています。

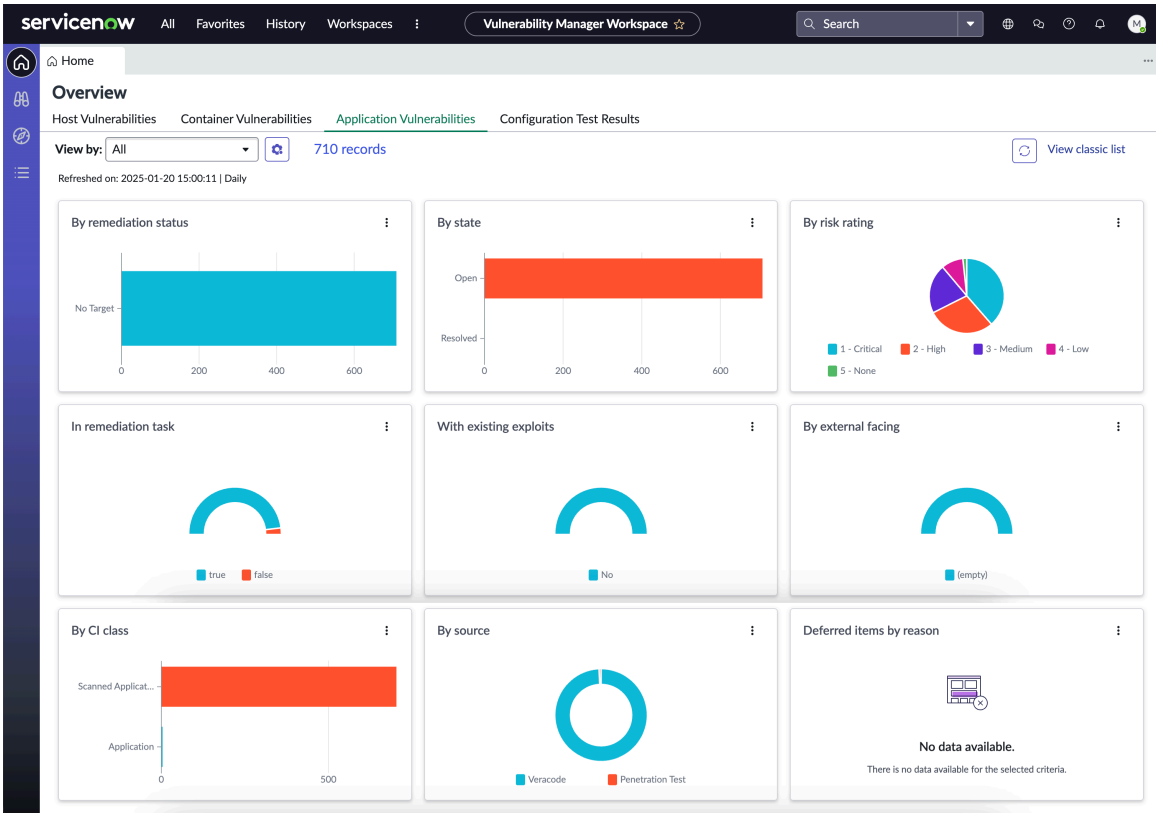
必要なロール：

- sn_vul.app_sec_manager を使用して、フィルターを適用して可視化を表示し、フィルターを作成します。
- フィルターを適用して可視化を表示する sn_vul.app_read_all 詳細ロール。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[アプリケーション脆弱性] タブ



次の表では、ホームページの [ホスト脆弱性] タブに表示される可視化について説明します。これらの可視化を選択すると、対応するレコードのリストが表示されます。

次の表では、ホームページの [アプリケーション脆弱性] タブに表示される可視化について説明します。

可視化	タイプ	説明
アサイン先グループと修復ステータス別	分布バー	修復ステータスごとにグループ化されたさまざまなアサイン先グループにアサインされたアクティブなレコード。
ステータス別	棒グラフ	さまざまな状況 (オープン、調査中、実装待ち、レビュー中、解決済み、保留) 別に分類されたアクティブなレコード。
リスク評価別	円グラフ	リスク評価 (1 - 重大、2 - 高、3 - 中、4 - 低、5 - なし) で分類されたアクティブなレコード
修復タスク中	半円ドーナツ	修復タスクの一部であるかないかにかかわらずアクティブなレコード。
既存のエクスプロイトあり	半円ドーナツ	既知のエクスプロイトの有無にかかわらずアクティブなレコード。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の表では、ホームページの [アプリケーション脆弱性] タブに表示される可視化について説明します。(続く)

可視化	タイプ	説明
外向き別	半円ドーナツ	インターネットへの資産エクスポージャーによって分類されたアクティブなレコード。
CI クラス別	棒グラフ	CI クラス別に分類されたアクティブなレコード。
クラウドリソース別	ドーナツグラフ	さまざまなクラウドリソース別に分類されたアクティブなレコード。
理由別の保留アイテム	ドーナツグラフ	理由別にグループ化されたアクティブな保留レコード。

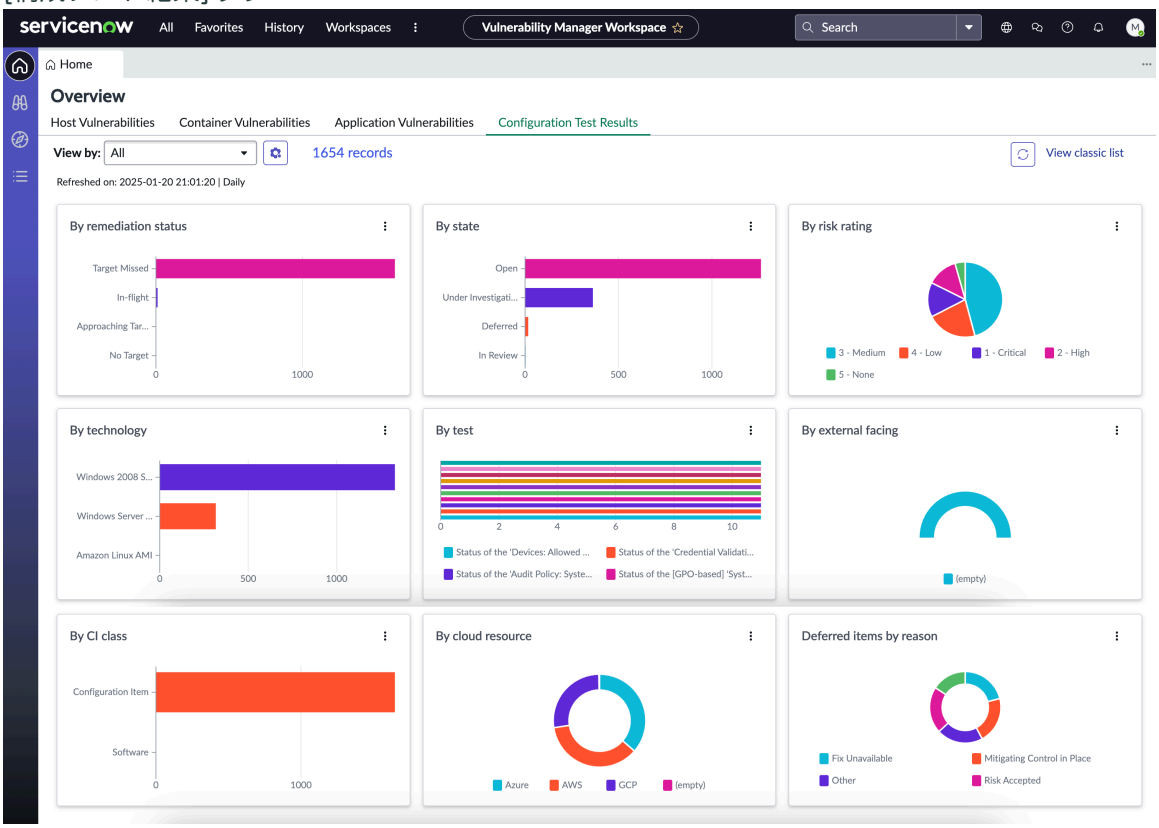
構成テスト結果

[構成テスト結果] タブには、組織内の資産のアクティブな構成ミスの全体的なサマリーを示す可視化が含まれています。

必要なロール：

- sn_vulc.admin を使用して、フィルターを適用して可視化を表示し、フィルターを作成します。
- フィルターを適用して可視化を表示する sn_vulc.read 詳細ロール。

[構成テスト結果] タブ



次の表では、ホームページの [構成テスト結果] タブに表示される可視化について説明します。これらの可視化を選択すると、対応するレコードのリストが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ホームページの [構成テスト結果] タブの可視化

可視化		説明
アサイン先グループと修復ステータス別	分布バー	修復ステータスごとにグループ化されたさまざまなアサイン先グループにアサインされたアクティブなレコード。
ステータス別	棒グラフ	さまざまな状況 (オープン、調査中、実装待ち、レビュー中、解決済み、保留) 別に分類されたアクティブなレコード。
リスク評価別	円グラフ	リスク評価 (1 - 重大、2 - 高、3 - 中、4 - 低、5 - なし) で分類されたアクティブなレコード
テクノロジー別	棒グラフ	テクノロジー別に分類されたアクティブなレコード数。
テスト別	棒グラフ	テスト別に分類されたアクティブなレコード数。
外向き別	半円ドーナツ	インターネットへの資産エクスポージャーによって分類されたアクティブなレコード。
CI クラス別	棒グラフ	CI クラス別に分類されたアクティブなレコード。
クラウドリソース別	ドーナツグラフ	さまざまなクラウドリソース別に分類されたアクティブなレコード。
理由別の保留アイテム	ドーナツグラフ	理由別にグループ化されたアクティブな保留レコード。

自動翻訳

の [監視トピック] ページ **Vulnerability Manager** ワークスペース

Vulnerability Manager ワークスペースの [監視トピック] ページでは、監視トピックを作成および編集できます。ウォッチトピックは一連のデータ可視化であり、組織にとって特に関心や優先度が高いと思われるダッシュボードで、フィルタリングされたレコードセット (VIT、AVIT、CVIT、CTR) を経時的に監視できます。

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

監視トピックの可視化された表示データは、インポート時に脆弱性データの変更に応じて動的に更新されます。ダッシュボードを使用して、選択したウォッチトピックの脆弱性と構成アイテムの傾向、範囲、タイプを監視します。この情報を使用して、各ウオッチトピックの脆弱性が環境に与える影響を判断できるようになります。[監視トピック] ページは、[ホスト脆弱性]、[コンテナ脆弱性]、[アプリケーション脆弱性]、[構成テスト結果]、および [非アクティブ] の 4 つのモジュールで構成されて

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

います。監視トピック内の関連アイテムのタブとその可視化の詳細については、「監視トピックの関連アイテムリストと可視化」を参照してください。

次の監視トピックは、[監視トピック] ページの [ホスト脆弱性] モジュールのベースシステムで提供されます。

- 外部向け資産の脆弱性
- エクスプロイトが可能な脆弱性
- Windows Server の脆弱性
- LINUX サーバーの脆弱性
- 期限を過ぎた重大な脆弱性
- 修復タスクに含まれない重大な脆弱性

注:
可視化されたデータでそのカテゴリのレコードがなくても、グラフアイコンをクリックするとレコードのリストが表示される場合は、表示されているリストでウォッチトピック名の列を確認します。監視トピックの列にリストされているすべてのレコードの値 (インターネット向けなど) が false であることを確認します。この例のこの値は、このウオッチトピックにインターネット接続のレコードがないことを示しています。

修正を開始すると判断した場合、または監視トピックにあるレコードに重大な必要性が生じた場合は、監視トピックから修復作業を作成できます。詳細については、「で修復作業を作成する Vulnerability Manager ワークスペース」を参照してください。

関連情報

監視トピックの関連アイテムリストと可視化

の使用 でトピックを監視する Vulnerability Manager ワークスペース

で監視トピックを作成する Vulnerability Manager ワークスペース

で監視トピックを編集または削除する Vulnerability Manager ワークスペース

監視トピックをアクティブ化または非アクティブ化する

監視トピックの関連アイテムリストと可視化

Vulnerability Manager ワークスペースの [監視トピック] ページでは、[ホスト脆弱性]、[コンテナ脆弱性]、[アプリケーション脆弱性]、および [構成テスト結果] の 4 つのモジュールに分類された監視トピックを作成できます。ウォッチトピックの関連アイテムタブは、モジュールごとに異なります。

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

[監視トピック] ページのナビゲーションペインには、次のモジュールが含まれています。

- ホスト脆弱性：ホスト脆弱性一致アイテムを含むウォッチトピックを表示します。
- コンテナ脆弱性：コンテナ脆弱性一致アイテムを含むウォッチトピックを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- アプリケーション脆弱性：アプリケーション脆弱性一致アイテムを含むウォッチトピックを表示します。
- 構成テスト結果：構成アイテムを含むウォッチトピックを表示します。
- 非アクティブ：4 つのモジュールすべてから非アクティブなウォッチトピックを表示します。

次の表は、さまざまなウォッチトピックモジュールで利用可能な関連アイテムタブを示しています。

ウォッチトピックとその関連アイテム

監視トピック	関連アイテムタブ
ホスト脆弱性	概要、影響を受ける CI、個別の脆弱性、および脆弱性一致アイテム
コンテナ脆弱性	概要、影響を受ける CI、個別の脆弱性、および脆弱性一致アイテム
アプリケーション脆弱性	概要と脆弱性一致アイテム
構成テスト結果	概要、影響を受ける CI、個別の構成テスト、および構成テスト結果

次の表にウォッチトピックの関連アイテムリストと可視化についての説明を示します。

ウォッチトピックの関連アイテムタブと可視化

関連アイテムタブと可視化	説明
概要	
経時的なアクティブな脆弱性一致アイテム	時間の経過に応じたアクティブな脆弱性一致アイテム (VI) の数。過去 30 日間のこのデータから傾向を監視できます。[資産カテゴリ] フィルターを使用してデータをフィルタリングすることもできます。
修復作業中の VI	既にアクティブな修復作業にある VI の合計数に対するアクティブな VI の数。
アクティブな修復作業	アクティブな修復作業のリスト。
影響を受ける **CI**	
個別の CI	これらの脆弱性の影響を受ける構成アイテム (CI) (資産) の数。
CI クラスごとの VI 数	各構成管理データベース (CMDB) CI クラスの脆弱性一致アイテム (VI) の数。 **注:** このウィジェットは、ホスト、アプリケーション、およびコンテナの脆弱性モジュールの監視トピックに対してのみ表示されます。
CI クラス別の構成の問題	各 構成管理データベース (CMDB) CI クラスの CI の数。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ウォッチトピックの関連アイテムタブと可視化 (続く)

関連アイテムタブと可視化	説明
	注: このウィジェットは、[構成の問題] モジュールの監視トピックに対してのみ表示されます。
インターネットに接続する VI	インターネットに公開されている資産の VI の合計数に対するアクティブな VI の数。 注: このウィジェットは、ホスト、アプリケーション、およびコンテナの脆弱性モジュールの監視トピックに対してのみ表示されます。
インターネットフェーシングの構成の問題	インターネットに公開されている資産の CI の合計数に対するアクティブな CI の数。 注: このウィジェットは、[構成の問題] モジュールの監視トピックに対してのみ表示されます。
個別の脆弱性	
既存のエクスプロイトを持つ VI	既知のエクスプロイトを持つアクティブな VI。
個別の脆弱性	資産に関連付けられている個々の脆弱性の数。個別の脆弱性は、問題タイプに基づいてフィルタリングできます。
PCI 脆弱性を持つ VI	ペイメントカード業界 (PCI) の脆弱性があるアクティブな VI を持つ個々の資産の数。
脆弱性一致アイテム	
ホスト脆弱性一致アイテム	すべてのホスト脆弱性一致アイテムのリスト。このリストをフィルタリングして、確認したいレコードのみを表示できます。 注: このリストは、ホスト脆弱性モジュールのウォッチトピックに対してのみ表示されます。
アプリケーション脆弱性一致アイテム	すべてのアプリケーション脆弱性一致アイテムのリスト。このリストをフィルタリングして、確認したいレコードのみを表示できます。 注: このリストは、アプリケーション脆弱性モジュールのウォッチトピックに対してのみ表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ウォッチトピックの関連アイテムタブと可視化 (続く)

関連アイテムタブと可視化	説明
コンテナ脆弱性一致アイテム	すべてのコンテナ脆弱性一致アイテムのリスト。このリストをフィルタリングして、確認したいレコードのみを表示できます。 **注:** このリストは、コンテナ脆弱性モジュールのウォッチトピックに対してのみ表示されます。
構成テスト結果モジュールのウォッチトピックの [概要] タブ	
アクティブな構成テストの経時的な結果	経時的なアクティブな構成テスト結果の数過去 30 日間のこのデータから傾向を監視できます。
修復作業の構成テスト結果	既にアクティブな修復作業にあるレコードの合計数に対する、アクティブな構成テスト結果の数。
アクティブな修復作業	アクティブな修復作業のリスト。
構成テスト結果モジュールの監視トピックの [個別の構成テスト] タブ	
テストの重要度別の構成テスト結果 (Configuration Test Results via Test Criticality)	問題の重要度に基づく構成テスト結果。
個別の構成テスト	個別の構成テストの数。
構成テスト結果モジュールのウォッチトピックの [構成テスト結果 **(Configuration Test Results)**] タブ	構成テスト結果のリスト。

[リフレッシュ] ボタンを選択することで、監視トピックの最新の詳細を取得できます。最新のリフレッシュステータスとタイムスタンプがウォッチトピック名の下に表示されます。ウォッチトピックをリフレッシュすると、チャートや修復作業など、ウォッチトピックのすべての詳細が更新されます。ウォッチトピックは、作成または更新されると自動的にリフレッシュされます。

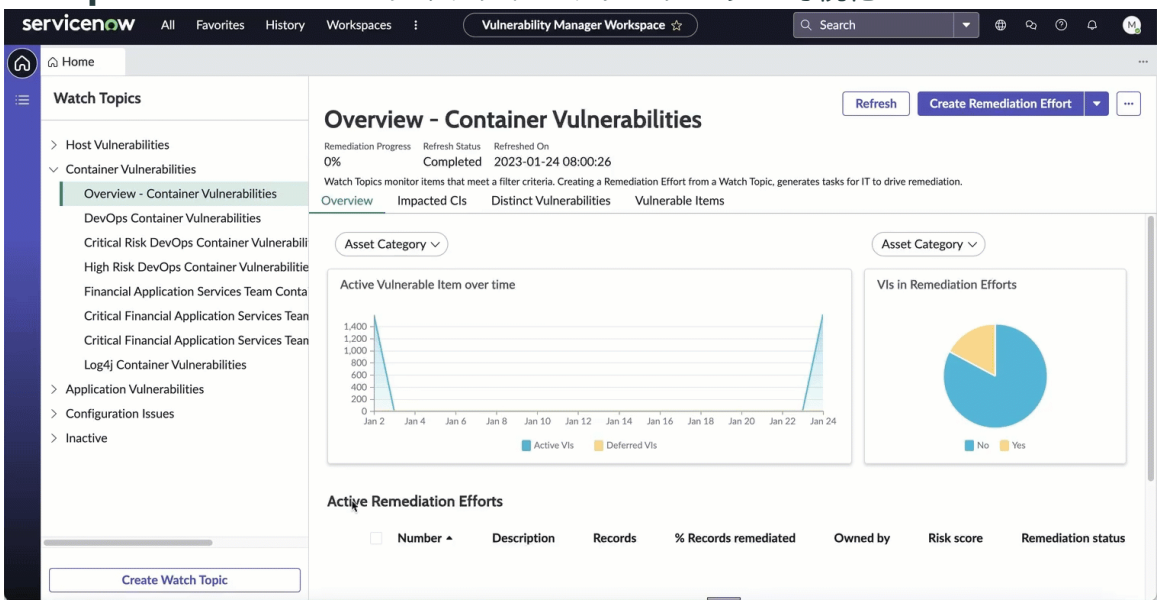
注:
非アクティブなウォッチトピックはリフレッシュできないため、非アクティブなウォッチトピックでは [リフレッシュ] ボタンはアクティブになりません。

ウィジェットのデータプロットをクリックすると、レコードに関する追加情報が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Example: バージョン **18.0** ウォッチトピックのデータの可視化



での修復作業 **Vulnerability Manager** ワークスペース

修復作業は、ウオッチトピックに関連付けられた一連のレコードです。修復作業にリストされているレコードは静的です。こうしたレコードは、新しいインポートデータによって、またウォッチトピックの変更によって更新されることはありません。

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

[リスト] ページの [修復作業] リストで [アクティブ] を選択した状態で、修復作業リンクをクリックして開きます。修復作業をホスト脆弱性一致アイテム (VIT)、アプリケーション脆弱性一致アイテム (AVIT)、コンテナ脆弱性一致アイテム (CVIT)、および構成テスト結果 (CTR) に分類するには、[レコードタイプ] 列の 3 つのドットメニューを選択し、[レコードタイプ別にグループ化] を選択します。

修復作業レコードの関連リストアイテムにより、関連するレコードの全体的な修正の進捗状況とステータスを表示できます。

- [概要] タブで、時間の経過とともにクローズされた、この修復作業に関連するレコードを監視します。レコードの右側にある、グラフのフィルターアイコンをクリックすると、データの可視化に適用されているフィルターが表示されます。
- [詳細] タブで、関連するウォッチトピックとステータス (アクティブまたは非アクティブ) をはじめとする、修復作業に関する詳細を表示します。このページから修復作業を非アクティブ化することができます。すべてのレコードをクローズする前に修復作業を非アクティブ化すると、アクティブなレコードを新しい修復作業に追加できるようになります。
- [修復タスク] タブで、この修復作業に関連する修復タスクを表示します。このタスクに関連付けられたレコードの、修正済みの割合を表示します。
- [脆弱性一致アイテム] タブで、この修復作業に関連するレコードを表示します。修復タスクのすべてのレコードが完了してクローズされると、その修復作業は [非アクティブ] に移行されます。修

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

復作業が非アクティブの場合、その修復作業に関連付けられたすべてのクローズ済みレコードは、新しい修復作業には追加できません。

> **注:**
> ホスト脆弱性、アプリケーション脆弱性、およびコンテナ脆弱性モジュールの監視トピックに関連付けられている修復作業に対して、[脆弱性一致アイテム] タブが表示されます。

- [構成テスト結果] タブで、修復作業に関連付けられた構成テスト結果を表示します。修復タスクのすべてのレコードが完了してクローズされると、その修復作業は [非アクティブ] に移行されます。修復作業が非アクティブの場合、その修復作業に関連付けられたすべてのクローズ済みレコードは、新しい修復作業には追加できません。

> **注:**
> [構成テスト結果] モジュールの監視トピックに関連付けられている修復作業に対して、[構成テスト結果] タブが表示されます。

詳細、および修復作業から実行できる UI アクションについては、「修復作業レコードを使用する」を参照してください。

関連情報

脆弱性対応ワークスペースの修復作業、修復タスク、およびレコードのライフサイクル

で修復作業を作成する Vulnerability Manager ワークスペース

の修復作業から修復タスクをオンデマンドで作成する Vulnerability Manager ワークスペース

で繰り返し修復作業を作成する Vulnerability Manager ワークスペース

の修復作業にレコードを転送する Vulnerability Manager ワークスペース

脆弱性対応ワークスペースの修復作業、修復タスク、およびレコードのライフサイクル

レコードが保留、解決、再オープンされ、他の修復作業 (RE) に転送されると、レコードおよび関連する修復タスク (RT) の状況が影響を受けます。

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

修復作業の作成

修復作業、修復タスク、およびレコードの状況とライフサイクルが受ける影響は、修復作業の作成方法、作成時期、および非アクティブ化されているかどうかによって異なります。

ウォッチトピックの右上にあるリストから、[修復作業の作成] または [繰り返し作業を作成] をクリックして、修復作業を作成できます。ウォッチトピックごとに 1 つの繰り返し修復作業を作成できます。繰り返し修復作業を作成すると、関連するウォッチトピックのそれ以降の修復作業は、設定した基準に基づいて自動的に作成されます。いずれの場合でも以下のようになります。

- 修復を容易にするために、アクティブなレコードのみが修復作業に追加されます。
- 新しい修復作業のすべてのレコードが新しい修復タスクに配置されます。レコードは複数の修復タスクに存在できますが、修復作業に関連付けることができるのは 1 つのレコードのみです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
アクティブなレコードがない場合、修復作業は自動的に非アクティブ化されます。

レコードの転送またはレコードの引き継ぎ

[他のアクティブな修復作業から一致するレコードを転送] チェックボックスをオンにすることで、修復作業を作成するときに、ある修復作業から別の修復作業にレコードを転送できます。レコードの転送方法の詳細については、「の修復作業にレコードを転送する Vulnerability Manager ワークスペース」を参照してください。レコードが、修復作業から転送される場合、または繰り返し修復作業に引き継がれる場合：

同じ監視トピック内の新しい修復作業へ

- 古い修復作業のすべての修復タスクが新しい修復作業に移動されます。
- 新しい修復タスクは、以前はどの修復タスクにも含まれていなかったレコードに対して選択されたグループ化基準に基づいて作成されます。
- 以前の修復作業は非アクティブ化されます。

異なる監視トピック内の新しい修復作業へ

古い修復作業のすべてのレコードが新しい修復作業に移動され、選択したグループ化基準に基づいて修復タスクが作成されます。

- 以前の修復作業に関連付けられた修復タスクのすべてのレコードが転送されると、これらの修復タスクはキャンセルしてクローズされます。
- レコードのサブセットのみが転送された場合、古い修復作業に関連付けられた修復タスクは分割され、アクティブなままになります。

古い修復作業に関連付けられたクローズ済み修復タスクは影響を受けません。

注:
繰り返し修復作業から新しい修復作業にレコードを転送することはできません。ただし、既存の繰り返さない修復作業から新しい修復作業にレコードを転送することはできます。レコードの転送の詳細については、「の修復作業にレコードを転送する Vulnerability Manager ワークスペース」を参照してください。

の [ダッシュボード] ページ **Vulnerability Manager** ワークスペース

Vulnerability Manager ワークスペース の [ダッシュボード] ページでは、ネクストエクスペリエンス UI でダッシュボードを表示し、これらのダッシュボードを使用して脆弱性を追跡および分析できます。

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

Vulnerability Manager ワークスペースのダッシュボードにアクセスするには、次の場所に移動します。 ワークスペース > 脆弱性マネージャーワークスペース [ダッシュボード] アイコンを選択します。ロールに応じてデフォルトのダッシュボードが表示されます。

次の表は、特定のロールに対して表示されるデフォルトのダッシュボードを示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

デフォルトのダッシュボード

デフォルトのダッシュボード	ロール
統一ダッシュボード (Unified Dashboard)	sn_vul_cmn_vulnerability_admin または sn_vul_cmn_vulnerability_analyst
脆弱性管理 (PA) ダッシュボード (Vulnerability PA Dashboard)	sn_vul_vulnerability_admin または sn_vul_vulnerability_analyst
アプリケーションの概要	sn_vul_app_sec_manager
コンテナの概要 (Container overview)	sn_vul_container_vulnerability_admin または sn_vul_container_analyst

[ダッシュボード] ページのドロップダウンから選択することで、実行するタスクの次のダッシュボードを表示できます。

Vulnerability Manager ワークスペースのダッシュボード

ダッシュボード	説明
脆弱性管理 (PA)	ホスト脆弱性の初期分析と検出から封じ込めや修復までのボリューム、パフォーマンス、および進捗状況を追跡します。詳細については、「脆弱性管理 (PA) ダッシュボード」を参照してください。
脆弱性の承認	承認済み、却下済み、および保留中の承認要求の数を表示します。詳細については、「デフォルトの 脆弱性対応 ダッシュボードを使用する」を参照してください。
CISO ダッシュボード	セキュリティの脆弱性やインシデントを含む、組織の全体的なセキュリティポスチャを表示します。詳細については、「脆弱性管理 CISO ダッシュボード」を参照してください。
コンテナ脆弱性管理の概要	コンテナ脆弱性の初期分析と検出から封じ込めや修復までのボリューム、パフォーマンス、および進捗状況を追跡します。詳細については、「コンテナ脆弱性対応 ダッシュボード」を参照してください。
アプリケーションの脆弱性管理ダッシュボード	アプリケーション脆弱性の初期分析と検出から封じ込めや修復までのボリューム、パフォーマンス、および進捗状況を追跡します。詳細については、「アプリケーション脆弱性管理 (PA) ダッシュボード」を参照してください。
統一脆弱性対応ダッシュボード	複数の脆弱性スキャナーとセキュリティツールからの情報を可視化して、組織の脆弱性とリスクを包括的に示します。詳細については、「統一脆弱性対応ダッシュボードのアナリティクスおよびレポートのソリューション」を参照してください。
脆弱性対応ヘルスダッシュボード	脆弱性対応アプリケーションの全体的なヘルススコアを表示します。詳細については、

自動翻訳

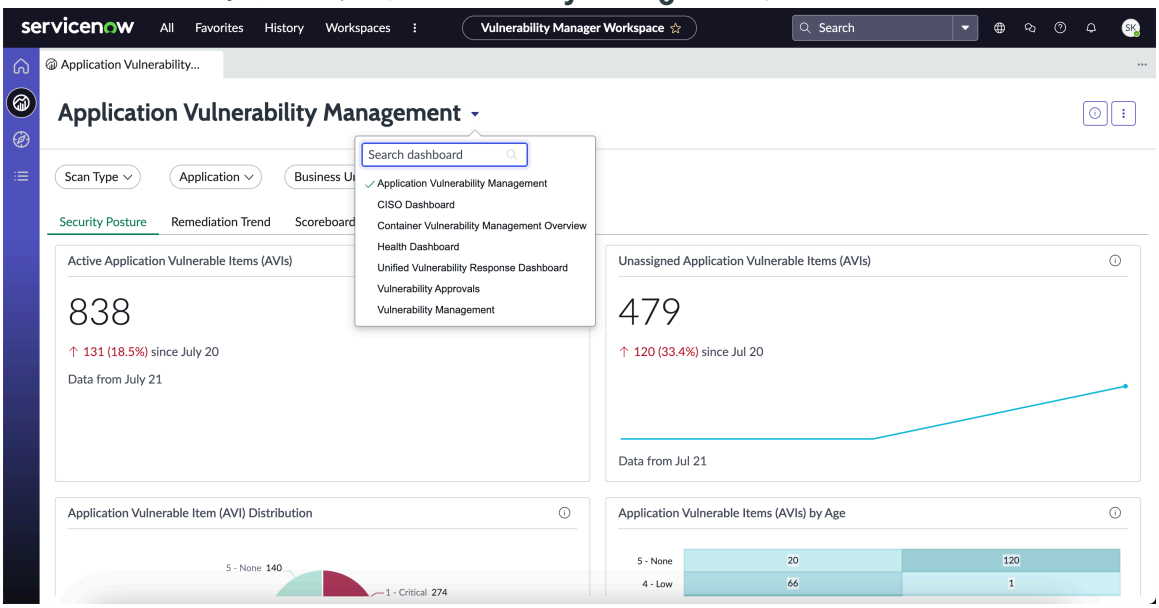
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Vulnerability Manager ワークスペースのダッシュボード (続く)

ダッシュボード	説明
	「SecOps 脆弱性対応ヘルスダッシュボード」を参照してください。

次の画像は、Vulnerability Manager ワークスペースの [ダッシュボード] ページを示しています。

バージョン **19.0** のダッシュボード **Vulnerability Manager** ワークスペース



[その他のオプション] アイコン (⋮)、[新しいダッシュボードを作成] の順に選択して、カスタムのダッシュボードを作成することもできます。

のリストページ **Vulnerability Manager** ワークスペース

Vulnerability Manager ワークスペースの [リスト] ページでは、脆弱性マネージャー/アナリスト、セキュリティマネージャー/アナリストは、レコードの修復の進捗状況を表示し、レコードにドリルダウンして、承認要求と例外のステータスを表示できます。

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

これらのリストとリンクを使用すると、レコードやタスクに簡単にアクセスできます。これには次の 2 つのタブがあります。

- [リスト] タブ:修復作業、修復タスク、脆弱性一致アイテム、構成テスト結果、ソリューション、例外、およびライブラリのデフォルトのリストが表示されます。
- [自分のリスト] タブ:[リスト] タブから名前を変更したリストと、作成したリストが表示されます。

  独自のリストを作成して、修正の進捗状況を監視することもできます。詳細については、「カスタマイズされたレコードリストの作成」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[リスト] タブ

次の表は、[リスト] ページの [リスト] タブで利用可能なリストを示しています。

ヒント:

アドミニストレーターが *sn_vul_cmn_ws.navigate_to_workspace* システムプロパティを true に設定している場合、[すべて] メニューから脆弱性対応、アプリケーション脆弱性対応、コンテナ脆弱性対応、およびコンフィグレーションコンプライアンスモジュールの事前定義フィルターリンクを選択すると、ロールに基づいてこれらのリンクが Vulnerability Manager ワークスペース のリストページで開きます。

たとえば、[所属グループにアサイン 済み] を選択した場合、 **All** (すべて) > 脆弱性対応 > 修復タスク > 所属グループにアサイン済みの場合、このリンクは Vulnerability Manager ワークスペースにリダイレクトされます。脆弱性アドミニストレーターまたはアナリストロールがある場合、修復タスクモジュールの [所属グループにアサイン済み] リストが脆弱性マネージャーワークスペースのリストページで開きます。ホスト修復タスクを表示するには、レコードタイプ別にタスクをグループ化します。

glide.ui.list.seismic.omit.count システムプロパティを使用して、リストのレコード数を非表示にすることができます。リストのレコード数のオン/オフを切り替える方法の詳細については、 KBB0010402 KB 記事を参照してください。

Lists (リスト)

リストアイテム	説明	モジュール	必要なロール
修復作業 (RE)	アクティブな RE とアサイン先グループにアサインされたすべての RE のリスト。 修復作業を レコードタイプ 別にグループ化し、ホスト脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、および構成テスト結果別に分類します。	脆弱性対応、 アプリケーション脆弱性対応、 コンテナ脆弱性対応、および コンフィグレーションコンプライアンス	• ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin • アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager • コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_a または sn_vul_container.vulnerability_admin • 構成テスト結果 (CTR) の sn_vulc.admin
修復タスク	次のリストが含まれています。 • アクティブ:すべてのアクティブなホスト、アプリケーション、コンテナ、およびテスト結果の修復タスクのリスト。	脆弱性対応、 アプリケーション脆弱性対応、 コンテナ脆弱性対応、および コンフィグレーションコンプライアンス	• ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin • アプリケーション脆弱性一致アイ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	モジュール	必要なロール
	• すべて:アクティブおよび非アクティブの両方のホスト、アプリケーション、コンテナ、およびテスト結果修復タスクのリスト。 • 自分にアサイン済み:修復のために自分にアサインされた修復タスクのリスト。 • 自分のグループにアサイン済み:修正のためにアサイン先グループにアサインされた修復タスク。 修復タスクを レコードタイプ 別にグループ化し、ホスト脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、および構成テスト結果別に分類します。 **注:** 修復タスクリストには、Vulnerability Manager ワークスペース での修復作業の作成中に生成されたタスクと、手動で作成されたタスク、およびクラシック UI の修復タスクルールやその他のプロセスによって作成されたタスクが含まれます。修復作業の一環として作成されなかった修復タスクについては、[修復作業] 列は空になります。		テム (AVIT) の場合、sn_vul.app_sec_manager • コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_a または sn_vul_container.vulnerability_admin • 構成テスト結果 (CTR) の sn_vulc.admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	モジュール	必要なロール
ホスト脆弱性一致アイテム	次のリストが含まれています • アクティブ:すべてのアクティブなホスト脆弱性一致アイテムのリスト。 • すべて:アクティブおよび非アクティブの両方のホスト脆弱性一致アイテムのリスト。 • [自分にアサイン済み (Assigned to me)]:修復のためにアサインされたホスト脆弱性一致アイテムのリスト。 • 自分のグループにアサイン済み:修復のためにアサイン先グループにアサインされたホスト脆弱性一致アイテムのリスト。	脆弱性対応	sn_vul.vulnerability_analyst、または sn_vul.vulnerability_admin
アプリケーション脆弱性一致アイテム	次のリストが含まれています。 • アクティブ:すべてのアクティブなアプリケーション脆弱性一致アイテムのリスト。 • すべて:アクティブおよび非アクティブの両方のアプリケーション脆弱性一致アイテムのリスト。 • [自分にアサイン済み (Assigned to me)]:修復のために自分にアサインされたアプリケーション脆弱性一致アイテムのリスト。 • 自分のグループにアサイン済み:修復のためにアサイン先グループにアサインさ	アプリケーション脆弱性対応	sn_vul.app_sec_manager

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	モジュール	必要なロール
	れたアプリケーション脆弱性一致アイテムのリスト。 [新規] ボタンを選択すると、新しいアプリケーション脆弱性一致アイテムを作成できます。		
コンテナ脆弱性一致アイテム	次のリストが含まれています。 • アクティブ:すべてのアクティブなコンテナ脆弱性一致アイテムのリスト。 • すべて:アクティブおよび非アクティブの両方のコンテナ脆弱性一致アイテムのリスト。 • [自分にアサイン済み (Assigned to me)]:修復のためにアサインされたコンテナ脆弱性一致アイテムのリスト。 • 自分のグループにアサイン済み:修復のためにアサイン先グループにアサインされたコンテナ脆弱性一致アイテムのリスト。	コンテナ脆弱性対応	sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
構成テスト結果	次のリストが含まれています。 • アクティブ:すべてのアクティブなテスト結果のリスト。 • すべて:アクティブなテスト結果と非アクティブなテスト結果の両方のリスト。 • 自分にアサイン済み:修復のために自分にアサインされたテスト結果のリスト。	コンフィグレーションコンプライアンス	sn_vulc.admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	モジュール	必要なロール
	• 自分のグループにアサイン済み:修復のためにアサイン先グループにアサインされたテスト結果のリスト。		
ソリューション	次のリストが含まれています。 • すべて:ホスト脆弱性一致アイテムを修正するために使用できるすべての利用可能なソリューションを表示します。 • 最高優先度:設定された優先ソリューションに使用されるすべてのソリューションを表示します。 • 脆弱性一致アイテムあり:脆弱性一致アイテムの優先ソリューションとして使用されているソリューションを表示します。	脆弱性対応	sn_vul.vulnerability_analyst、または sn_vul.vulnerability_admin
例外	アサイン先グループに関連付けられているすべての例外要求と誤検出要求の承認状況を表示します。 • すべて:VIT、AVIT、CVITとその修復タスク (VUL、AVUL、CVUL) に関連する例外、誤検出、およびアサイン解除承認要求のリスト。 • すべて (コンフィグレーションコンプライアンス):関連するテスト結果と修復タスク (CTR#) の例外、誤検出、およびアサイン解除承認要求のリスト。	脆弱性対応、 アプリケーション脆弱性対応、 コンテナ脆弱性対応、および コンフィグレーションコンプライアンス	• ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin • アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager • コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_a または sn_vul_container.vulnerability_admin • 構成テスト結果 (CTR) の sn_vulc.admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	モジュール	必要なロール
	例外を レコードタイプ別にグループ化し、ホスト脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、および構成テスト結果別に分類します。		
承認	[自分にアサイン済み]:処理のために自分にアサインされた承認要求を表示します。ワークスペースで承認を処理するには、「Vulnerability Manager ワークスペース で要求を承認または却下」を参照してください。	脆弱性対応、 アプリケーション脆弱性対応、 コンテナ脆弱性対応、および コンフィグレーションコンプライアンス	• ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin • アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager • コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_a または sn_vul_container.vulnerability_admin • 構成テスト結果 (CTR) の sn_vulc.admin
ライブラリー	次のリストで構成されます。 • CVE (NVD): 脆弱性対応、 アプリケーション脆弱性対応、コンテナ脆弱性対応のすべての共通脆弱性識別子 (CVE) のリスト。 • TPE:インスタンスにインポートされたサードパーティ脆弱性のリスト。関連する参照、脆弱性一致アイテム、エクスプロイト、および CVE のリストが含まれています。 • CWE: 脆弱性対応、アプリケーション脆	脆弱性対応、 アプリケーション脆弱性対応、 コンテナ脆弱性対応、および コンフィグレーションコンプライアンス	• ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin • アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager • コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_a または sn_vul_container.vulnerability_admin • 構成テスト結果 (CTR) の sn_vulc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	モジュール	必要なロール
	弱性対応、および コンテナ脆弱性対応 のすべての共通脆弱性タイプ一覧 (CWE) のリスト。 • アプリ脆弱性:すべてのサードパーティアプリケーション脆弱性エントリーのリスト。 • テストグループ: コンフィグレーションコンプライアンス すべてのテストグループのリスト。レコードビューのテストグループにおける CI およびテスト結果のコンプライアンス率を表示することができます。 • テスト: コンフィグレーションコンプライアンスからのすべてのテストのリスト。レコードビューのテストにおけるテスト結果のコンプライアンス率を表示することができます。 • 補完コントロール: リスク削減要求に使用できるすべての補完コントロールのリスト。補完コントロールを追加するには、[新規作成] をクリックします。補正コントロールを追加する方法の詳細については、「補完コントロールをライブラリに追加する」を参照してください。		
CMDB	次のリストが含まれています	脆弱性対応、 アプリケーション脆弱性対応、 コンテナ脆弱性対応、および コンフィグ	• ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	モジュール	必要なロール
	• 検出済みアイテム:検出されたすべてのアイテムのリスト。 • 検出されたコンテナイメージ:コンテナイメージのリスト。これらのコンテナーイメージは、レイヤー情報とともに、イメージ ID、Docker イメージ、およびイメージリポジトリに関する情報を提供します。	レーションコンプライアンス	• アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager • コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_a または sn_vul_container.vulnerability_admi • 構成テスト結果 (CTR) の sn_vulc.admin
ペネトレーションテストアセスメント要求	次のリストが含まれています。 • アクティブ:アクティブなペネトレーションテストアセスメント要求のリスト。 • すべて:アクティブと非アクティブの両方のペネトレーションテストアセスメント要求のリスト • 自分にアサイン済み:自分が作成したペネトレーションテストアセスメント要求のリスト。 • 自分のグループにアサイン済み:アサイン先グループのユーザーによって発生したペネトレーションテストアセスメント要求のリスト。 ペネトレーションテストアセスメント要求の作成方法については、「新しいペネトレーションテストアセスメント要求を作成します」を参照してください。	アプリケーション脆弱性対応	sn_vul.app_sec_manager

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	モジュール	必要なロール
ペネトレーションテスト結果	次のリストが含まれています。 • アクティブ:すべてのアクティブなペネトレーションテスト結果のリスト。 • すべて:アクティブと非アクティブの両方のペネトレーションテスト結果のリスト。 • [自分にアサイン済み (Assigned to me)]:修復のためにアサインされたペネトレーションテスト結果のリスト。 • 自分のグループにアサイン済み:修正のためにアサイン先グループにアサインされたペネトレーションテスト結果のリスト。 ペネトレーションテスト結果を作成する方法については、「アセスメントアンケートに基づくペネトレーションテスト結果の作成」を参照してください。	アプリケーション脆弱性対応	sn_vul.app_sec_manager
パッチ	すべて:ホスト脆弱性一致アイテムの修復に使用できるすべての利用可能なパッチのリスト。	脆弱性対応	sn_vul.vulnerability_analyst、または sn_vul.vulnerability_admin
サポートデータ	次のリストが含まれています。 • 信頼できる情報源:情報源の出版物の調査に役立つ要約情報を提供する信頼できる情報源のリスト。 • テクノロジー:信頼できる各ソースと引用に関するサマリー情報を提供するテク	コンフィグレーションコンプライアンス	sn_vulc.admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	モジュール	必要なロール
	ノロジーのリスト (Qualys ではフレームワークとも呼ばれます)。		

関連情報

Vulnerability Manager ワークスペースでリストビューを使用する

での一括編集 **Vulnerability Manager** ワークスペース

Vulnerability Manager ワークスペースでは、一括編集機能を使用すると、複数の脆弱性一致アイテム (VIT、AVIT、CVIT) または構成テスト結果 (TR) を同時に更新できるため、管理および修復プロセスが簡素化されます。

一括編集を使用すると、複数の脆弱性を選択して、修復オーナーのアサイン、ステータスの更新、作業メモの追加、例外の要求、誤検出の要求など、一貫性を持って変更を適用させることができるようになります。これにより、脆弱性一致アイテムを個別に編集する必要がなくなるので、時間や労力が節約され、効率的かつ一貫性のある脆弱性管理が促進されます。

一括編集機能は、次に対して有効です。

- 脆弱性対応 v21.0 以降のホスト脆弱性一致アイテム (VIT)。
- 脆弱性対応 v22.0 以降のアプリケーション脆弱性一致アイテム (AVIT) およびコンテナ脆弱性一致アイテム (CVIT)。
- 脆弱性対応 v23.0 以降のテスト結果 (TR)。

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

Vulnerability Manager ワークスペース の一括編集機能を使用して、次のタスクを実行できます。

- レコードをアサイン先グループに一括アサイン
- 脆弱性マネージャーワークスペースでの一括例外の要求
- ホスト脆弱性一致アイテムのアサインを一括解除する
- 脆弱性マネージャーワークスペースで誤検出を一括編集
- Vulnerability Manager ワークスペース でレコードを一括クローズ

リスク削減の補完コントロールについて

補完コントロールは、すぐにパッチを適用できない脆弱性によって引き起こされるリスクを軽減するために取られる手段です。これらは、エクスプロイトが成功する可能性または影響を軽減するために使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
補完コントロール機能は、ホストの脆弱性に対してのみ使用できます。

補完コントロールを適用すると、脆弱性のリスクを軽減するのに役立ちます。

次の表に、コントロールを補完するユースケースを示します。

補完コントロールのユースケース

ユースケース	補完コントロール
攻撃者が任意のコードを実行できる Web サーバーの脆弱性。	Web アプリケーションファイアウォール (WAF) を実装して、Web サーバーへの悪意のある要求をブロックします。
攻撃者が特権を root にエスカレーションすることを可能にするオペレーティングシステムの脆弱性。	ホストシステムでのアプリケーションの実行を制限するアプリケーションコントロールを実装します。
攻撃者が機密データにアクセスできるようにするデータベースサーバーの脆弱性。	ネットワークセグメンテーションを実装して、データベースサーバーを他のホストや重要なシステムから分離します。

補完コントロールが脆弱性一致アイテムと修復タスクのリスクスコアに与える影響の詳細については、「リスクスコアと有効期限に対する補完コントロールの影響」を参照してください。

関連情報

- 補完コントロールをライブラリに追加する
- リスク削減要求の CVE または TPE に補完コントロールを関連付ける
- CVE または TPE のリスク削減を無効または有効にする

統一脆弱性対応ダッシュボードのアナリティクスおよびレポートのソリューション

統一 Vulnerability Response ダッシュボード (Unified Vulnerability Response Dashboard) は、複数の脆弱性スキャナーとセキュリティツールからの情報を可視化する一元化的な集計ダッシュボードであり、組織の脆弱性とリスクを包括的に示します。

必要なロール

このソリューションには、次のロールとタスクが関連付けられています。レポートを表示および共有するために必要です。

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

関連情報

- アナリティクスおよびレポートのソリューション

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統一脆弱性対応ダッシュボード

統一脆弱性対応ダッシュボードは、組織の脆弱性とリスクを包括的に表示します。インフラストラクチャ、クラウド、アプリケーション、およびコンテナに関連する脆弱性を一元的なダッシュボードで表示して、可視化と修復を向上できます。

統一脆弱性対応ダッシュボードの詳細については、この 4 分間のビデオをご覧ください。

https://player.vimeo.com/video/1046083623?h=74c3349c9c&badge=0&autopause=0&player_id=0&app_id=58479

必要な **Now Platform** ロール

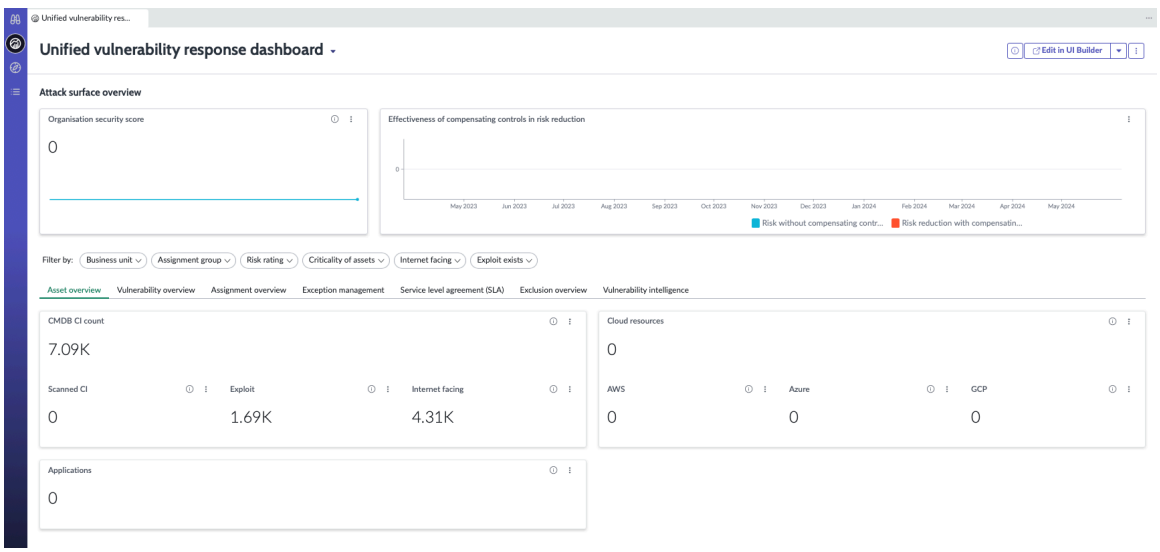
このソリューションには、次のロールが関連付けられています。レポートを表示、編集、および共有するために必要です。

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

[統一脆弱性対応ダッシュボード **(Unified Vulnerability Response Dashboard)**] へのアクセス

ダッシュボードを開くには、次のいずれかの場所に移動します。

- **All** (すべて) > 脆弱性対応 > 脆弱性マネージャーワークスペース をクリックし、[ダッシュボード] アイコンを選択します。ロールに応じてデフォルトのダッシュボードが表示されます。統一 脆弱性対応ダッシュボードを表示するには、ダッシュボード名の横にあるドロップダウンを選択します。
- ワークスペース > **Platform Analytics** (プラットフォームアナリティクス) ワークスペース > ダッシュボード > 統一脆弱性対応ダッシュボード.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ユースケース

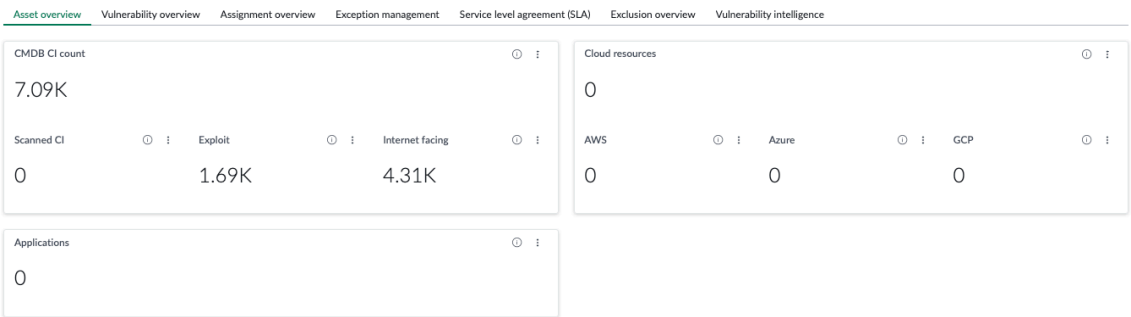
組織内のさまざまなユーザーがこのダッシュボードをどのように使用するかの例については、次のユースケースを参照してください。

ユーザー	ダッシュボードの使用法
• 脆弱性マネージャー • 脆弱性アナリスト	• インフラストラクチャ、アプリケーション、構成、およびコンテナに存在するリスクをリアルタイムで可視化し、。脆弱性マネージャーや脆弱性アナリストが、脆弱性をタイムリーに優先順位付けして修復できるようにします。 • 重要な資産の攻撃対象の概要を表示します。この概要を使用して、修復の進捗状況と作業を追跡できます。 • 事業部門 (BU) 全体のリスクの概要を表示します。必要に応じて、フィルターを使用して BU を選択し、進捗状況を比較してリソース再配分できます。ロールレベルのアクセス権を BU のリーダーに付与する必要があります。 • BU 別に潜在的な影響のヴィジビリティを提供します。共通脆弱性識別子 (CVE) フィルターを使用して、組織全体のエクスポージャーを特定できます。 • アプリケーション、ホスト、およびコンテナ脆弱性一致アイテムの CISA KEV カタログに存在する脆弱性一致エントリによって取得された EPSS スコアのヴィジビリティを提供します。

統一脆弱性対応 ダッシュボードのタブ

このダッシュボードでは、ホスト、クラウド、構成、アプリケーション、およびコンテナに存在する脆弱性または問題を確認できます。事業部門、アサイン先グループ、リスク評価、重要度、および脆弱性のエクスプロイトが存在するかどうかに基づいて、脆弱性を表示できます。

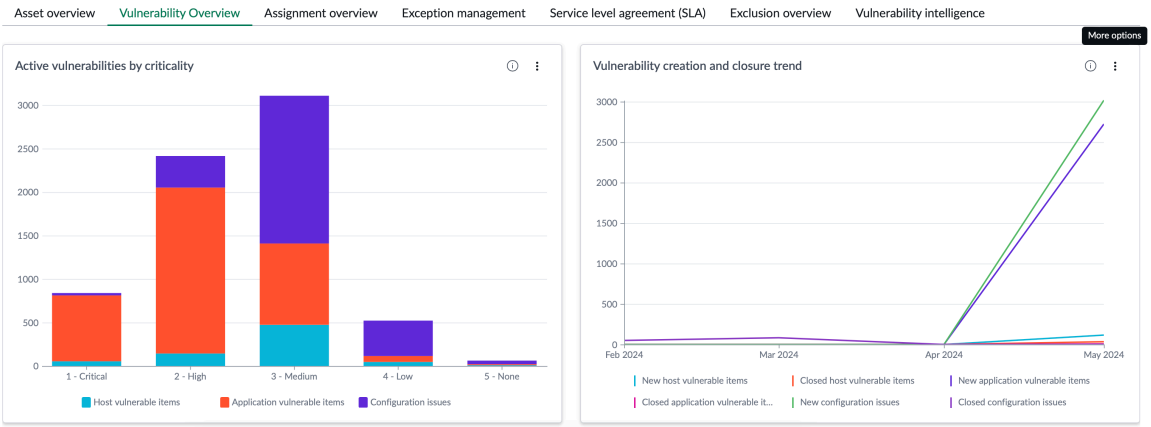
[資産の概要] タブには、システム内の構成アイテム (CI) の全体的なステータスが表示されます。



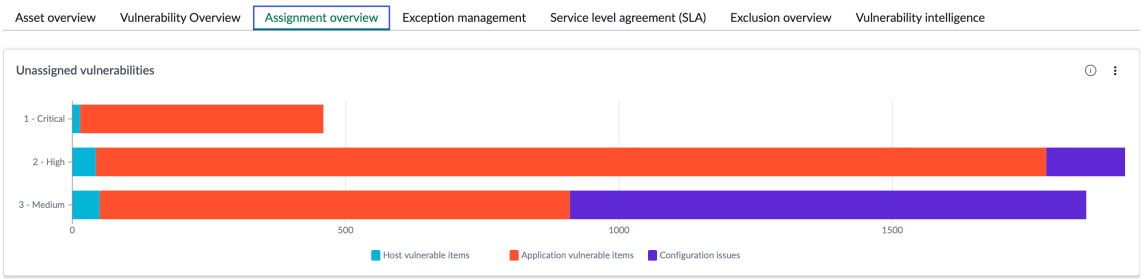
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

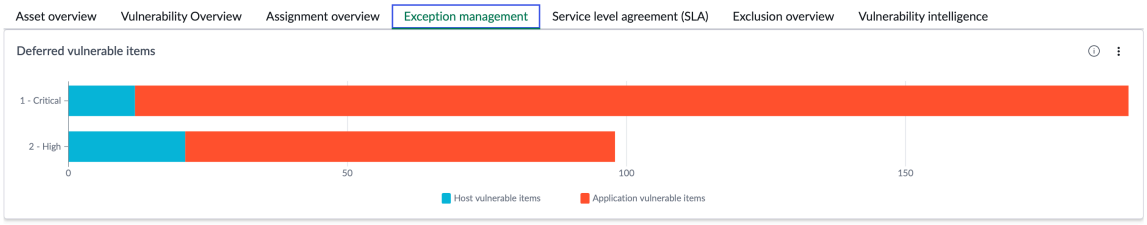
[脆弱性概要 **(Vulnerability Overview)]** タブには、ホスト、アプリケーション、コンテナなどの脆弱性のタイプに関するステータスが表示されます。



[アサインの概要 **(Assignment Overview)]** タブには、脆弱性のアサインのステータスが表示されます。



[例外管理 **(Exception Management)]** タブには、保留された脆弱性のステータスが表示されます。



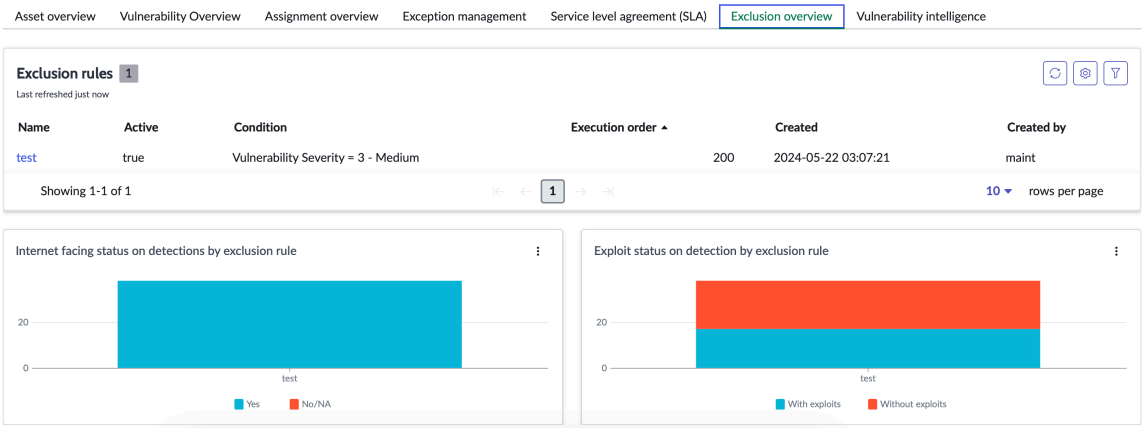
[Service Level Agreement (SLA)] タブには、さまざまなアサイン先グループが達成したサービスレベルアグリーメントのステータスが表示されます。

[除外の概要 **(Exclusion overview)]** タブには、作成した除外ルールのステータスだけでなく、「インターネットアクセス可」「有効なエクス

自動翻訳

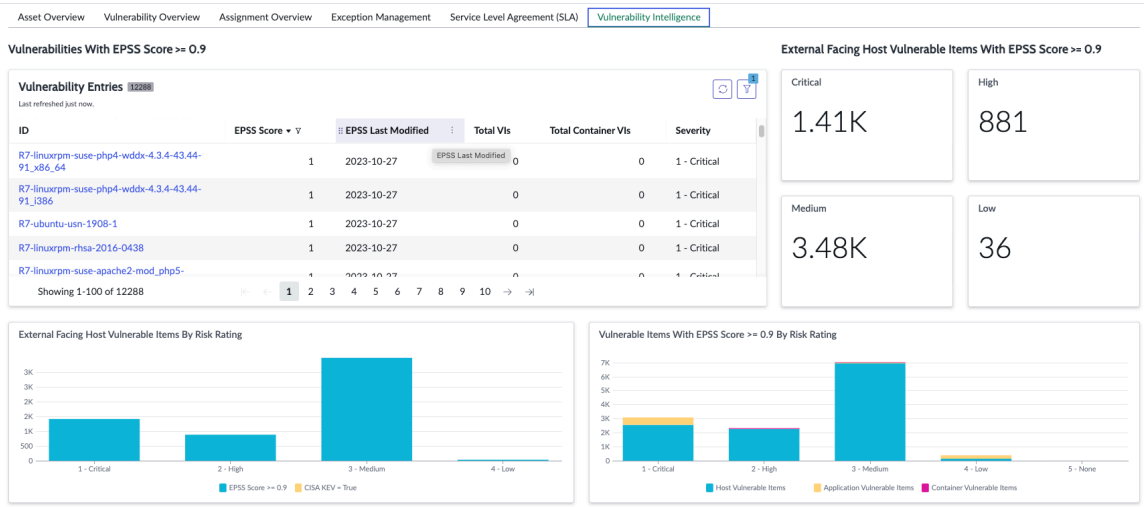
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロイトあり」の検出に影響を与えるルールのステータスも表示されま



す。

[脆弱性インテリジェンス **(Vulnerability Intelligence)**] タブには、アプリケーション、ホスト、およびコンテナ脆弱性一致アイテムの CISA KEV フラグが true および EPSS スコア >= 0.9 の脆弱性によって達成された EPSS スコアのステータスが表示されま



す。

フィルター

以下の条件に基づいてウィジェットをフィルタリングできます。

- 事業部門
- アサイン先グループ
- リスク評価
- 資産の重要度
- インターネットフェーシング
- エクスプロイト有無

フィルターを選択すると、すべてのウィジェットのデータが更新されます。ただし、フィルターがウィジェットに適用されない場合は、フィルター名の横に x 印が表示されます。

注:
Tokyo では、事業部門とアサイン先グループのフィルターのみが使用可能です。Utah 以降ではすべてのフィルターを使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インジケーター

スキャンされた資産

過去 60 日間にスキャンされた資産の式インジケーター。[スキャンされた検出済みアイテム資産 (Scanned Discovered item assets)]、[スキャンされたアプリケーションリリース資産 (Scanned Application release assets)]、[スキャンされた検出済みコンテナイメージ資産 (Scanned Discovered Container image assets)] が貢献インジケーターとして含まれています。☒

資産：エクスプロイトあり (Assets - Exploit exists)

脆弱性にエクスプロイトが存在する資産の式インジケーター。[ホスト資産：エクスプロイトあり (Host assets - Exploit exists)]、[アプリケーション資産：エクスプロイトあり (Application assets - Exploit exists)]、[コンテナ資産：エクスプロイトあり (Container assets - Exploit exists)] が貢献インジケーターとして含まれています。

インフラ資産：インターネットフェーシング (Infra Asset - Internet Facing)

インターネットに接続されている資産の数を取得するためのインジケーター。

クラウドリソースタイプに基づいて検出されたアイテム (Discovered items based on Cloud Resource type)

クラウドなどの資産カテゴリの資産の数を取得するためのインジケーター。☒

基本イメージ

基本イメージの数を取得するためのインジケーター 。

CISA KEV 資産タイプ (CISA KEVs Asset Type)

脆弱性の CISA KEV (BOD 22-01) フラグが true に設定されているコンテナ脆弱性一致アイテムおよびホスト脆弱性一致アイテムの数を示す式インジケーター。[CISA が存在する CVR (CISA exists CVR)] と [CISA が存在する脆弱性一致アイテム (CISA exists Vul Items)] が貢献インジケーターとして含まれています。

CISA が存在する脆弱性一致アイテム：未アサイン (CISA Exists Vulnerable Items – Unassigned)

脆弱性の CISA KEV (BOD 22-01) フラグが true に設定されているコンテナ脆弱性一致アイテムおよびホスト脆弱性一致アイテムの数を示す式インジケーター。脆弱性一アイテムは未アサインです。[未アサインのコンテナ脆弱性一致アイテム (Unassigned Container Vul Items)] と [未アサインのホスト脆弱性一致アイテム (Unassigned Host Vul Item)] が貢献インジケーターとして含まれています。

CISA が存在する脆弱性一致アイテム：ターゲット経過 (CISA Exists Vulnerable Items - Target Missed)

脆弱性の CISA KEV (BOD 22-01) フラグが true に設定されていて、脆弱性一致アイテムがターゲットを経過したコンテナ脆弱性一致アイテムおよびホスト脆弱性一致アイテムの数を示す式インジケーター。[CISA が存在する脆弱性一致アイテム (CISA exists Vul Items)] と [CISA が存在する CVR (CISA exists CVR)] が貢献インジケーターとして含まれています。

アクティブなホスト VIT (Active Host VITs)

アクティブなホスト脆弱性一致アイテム (VIT) の数。

アクティブなアプリケーション VIT (Active Application VITs)

アクティブなアプリケーション脆弱性一致アイテム (AVIT) の数。

アクティブなコンテナ VIT (Active Container VITs)

アクティブなコンテナ脆弱性一致アイテム (CVIT) の数。

新しい VIT (New VITs)

1 日にオープンされた VIT の数。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

新しい AVIT (New AVITs)

1 日にオープンされた AVIT の数。

新しい CVIT (New CVITs)

1 日にオープンされた CVIT の数。

新しいテスト結果 (New Test Results)

1 日に作成されたテスト結果 (TR) の数。

クローズ済み AVIT (Closed AVITs)

1 日にクローズされた VIT の数。

クローズ済み VIT (Closed VIT)

1 日にクローズされた AVIT の数。

クローズ済み CVIT (Closed CVITs)

1 日にクローズされた CVIT の数。

クローズされたテスト結果 (Closed Test Results)

1 日にクローズされた TR の数。

オープンな構成の問題 - テスト結果 (Open Config Issues - Test results)

失敗ステータスのすべてのオープンなテスト結果の数。

組織リスクスコア (Organization Risk Score)

ロールアップアプリケーションのリスクスコア (Rollup Application Risk Score) テーブルからの組織のリスクスコア。

未アサインのアプリケーション脆弱性一致アイテム (Unassigned Application Vul Item)

アサイン先グループまたはアサイン先がない AVIT。

未アサインのホスト脆弱性一致アイテム (Unassigned Host Vul Item)

アサイン先グループまたはアサイン先がない VIT。

未アサインのコンテナ脆弱性一致アイテム (Unassigned Container Vul Items)

アサイン先グループまたはアサイン先がない CVIT。

アサインされていない構成の問題 (Unassigned Config Issues)

アサイン先グループまたはアサイン先がない TR。

保留 VIT (Deferred VITs)

保留ステータスの VIT。

保留 AVIT (Deferred AVITs)

保留ステータスの AVIT。☒

保留 CVIT (Deferred CVITs)

保留ステータスの CVIT。

ホスト SLA：クローズ済み (Host SLA - Closed)

クローズ済み VIT の平均クローズ時間。

アプリケーション SLA：クローズ済み (Application SLA - Closed)

クローズ済み AVIT の平均クローズ時間。☒

コンテナ SLA：クローズ済み (Container SLA - Closed)

クローズ済み CVIT の平均クローズ時間。

テスト結果 SLA：合格 (Test Result SLA - Passed)

合格した TR の平均クローズ時間。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ホスト SLA：クローズ済み (重大および高) (Host SLA - Closed (Critical & High))

クローズ済み VIT (重大および高) の平均クローズ時間。

アプリケーション SLA：クローズ済み (重大および高) (Application SLA - Closed (Critical & High))

重大および高 AVIT の平均クローズ時間。☒

コンテナ SLA：クローズ済み (重大および高) (Container SLA - Closed (Critical & High))

クローズ済み CVIT (重大および高) の平均クローズ時間。

テスト結果 SLA：合格 (重大および高) (Test Result SLA - Passed (Critical & High))

合格した TR (重大および高) の平均クローズ時間。

集計 MTTR (Aggregate MTTR)

クローズ済み VIT、AVIT、CVIT、TR の平均クローズ時間。☒

SLA 欠落 (SLA Missed)

クローズ済みおよびターゲット経過 VIT、AVIT、CVIT、TR の平均クローズ時間。

EPSS スコア >= 0.9 の脆弱性

EPSS スコアが 0.9 以上の脆弱性エントリの数。

ブレークダウン

- VIT タイプ (統一) (VIT type (unified))
- インターネットフェーシング (統一) (Internet Facing (unified))
- リスク評価 (統一) (Risk Rating (unified))
- エクスプロイトあり (統一) (Exploit Exists (unified))
- 検出済みアイテムのクラウドリソースタイプ (統一) (Discovered Item Cloud Resource Type (unified))
- CISA あり (統一) (CISA Exists (unified))
- CMDB クラス (統一) (CMDB class (unified))
- 事業部門 (統一) (Business Unit (unified))
- ビジネス上の重要度 (統一) (Business Criticality (unified))
- 保留理由 (統一) (Deferred Reason (unified))
- アサイン先グループ (統一) (Assignment group (unified))
- 修復ステータス (統一) (Remediation Status (unified))

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データの可視化

[資産の概要] タブ

タイトル	タイプ	説明
攻撃対象領域の概要 (Attack Surface Overview)	単一スコア 	組織のセキュリティのアグリゲートスコアを表す数値。
CMDB CI カウント (CMDB CI Count)	単一スコア 	構成管理データベース (CMDB) に登録されており追跡される組織内の CI の数。次の CI のブレークダウンを示します。 • スキャンされた CI：スキャンされた CI の数 • エクスプロイト：利用可能なエクスプロイトの数 • インターネットフェイシング：インターネットに接続している CI の数
クラウドリソース	単一スコア 	クラウドなど資産カテゴリがある CI の数。次のクラウド資産のブレークダウンを示します。 • AWS • Azure • GCP
Docker イメージ	単一スコア 	基本イメージの数を含む Docker イメージの数

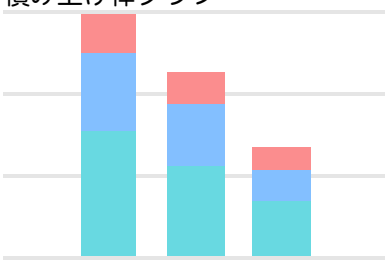
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[資産の概要] タブ (続く)

タイトル	タイプ	説明
アプリケーション	単一スコ ア	組織内のアプリケーションの数

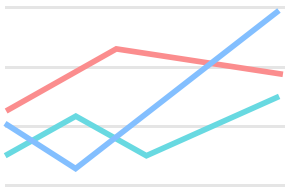
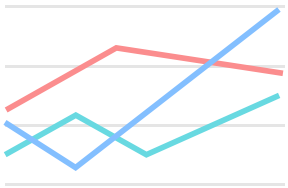
[脆弱性概要 **(Vulnerability Overview)]** タブ

タイトル	タイプ	説明
CISA KEV (CISA KEVs)	円グラフ	CISA カタログに関連付けられており、CISA フラグが true に設定されている脆弱性の数。 以下に基づくブレークダウンを示します。 • CISA 脆弱性 (CISA Vulnerability)：CISA フラグが true に設定されている脆弱性のタイプ • ホスト CI：インターネットに接続している CI • 未アサイン VIT (Unassigned VITs)：CISA フラグが true に設定されている未アサイン VIT • ターゲット欠落 VIT (VITs missed target)：CISA フラグが true に設定されているターゲットを経過した VIT
重要度別のアクティブな脆弱性 (Active Vulnerabilities by Criticality)	積み上げ棒グラフ 	重要度に基づくアクティブな VIT、AVIT、および CVIT の数。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

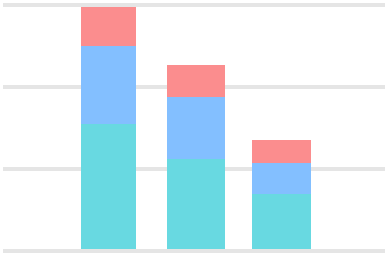
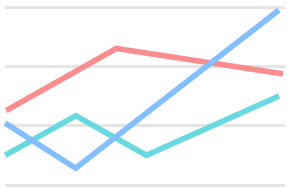
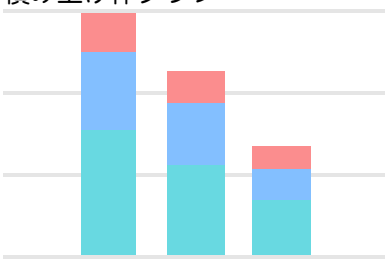
[脆弱性概要 **(Vulnerability Overview)**] タブ (続く)

タイトル	タイプ	説明
脆弱性の作成とクローズの傾向 (Vulnerability creation and closure trend)	複数折れ線グラフ 	すべてのアプリケーションの新規の脆弱性とクローズ済み脆弱性の数。過去 3 か月間の傾向を示します。
クラウドプラットフォーム別の構成ミス (Misconfiguration by cloud platform)	複数折れ線グラフ 	各クラウド資産のリスク評価に基づく構成の問題の数。
クラウドコンプライアンス (Cloud Compliance)	テーブル	資産カテゴリがクラウドであるリソースのリストと、次の詳細。 • リソース名 • クラス • 脆弱性の問題 (Vulnerability issues)：リスク評価に基づいて集計された、リソースに存在する問題の数。 • 構成の問題：構成の問題があるリソースの数とリスク評価。 • クラウドアカウント：クラウドアカウント ID。 • クラウドリージョン：クラウドリソースの場所。 • クラウドプロバイダー：クラウドプロバイダーの名前。

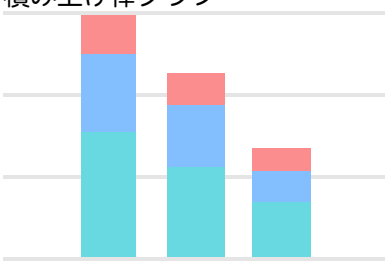
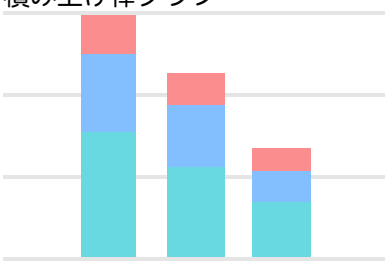
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[アサインの概要 **(Assignment Overview)**] タブ

タイトル	タイプ	説明
未アサイン VIT (Unassigned VITs)	積み上げ棒グラフ 	どのグループまたは個人にもアサインされていない脆弱性の数とリスク評価。
アサイン先グループ別 MTTR：上位 10 (MTTR by Assignment Group - Top 10)	複数折れ線グラフ 	アサイン先グループがセキュリティの脆弱性または問題を特定して修復するためにかかった平均時間。平均修復時間が最も長い上位 10 件のアサイン先グループが表示されます。
SLA が欠落している上位 10 のアサイン先グループ (脆弱性は重大および高) (Top 10 Assignment Groups missing SLA) (Critical & High Vulnerability)	積み上げ棒グラフ 	重大な脆弱性および高脆弱性の修復目標期日を経過した上位 10 件のアサイン先グループ。

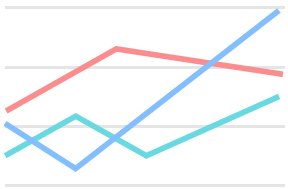
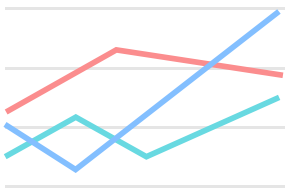
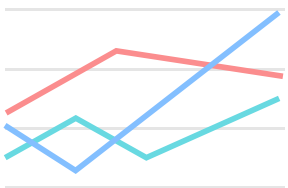
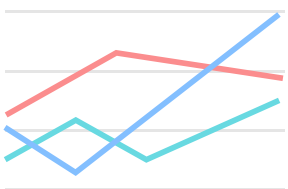
[例外管理 **(Exception Management)**] タブ

タイトル	タイプ	説明
保留 VIT (Deferred VITs)	積み上げ棒グラフ 	リスク評価に基づく保留ステータスの脆弱性の数。
アサイン先グループ別の重大および高保留 VIT (Critical and High Deferred VITs by Assignment Group)	積み上げ棒グラフ 	アサイン先グループに基づいて分類された、リスク評価が重大または高で保留ステータスの脆弱性の数。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[Service Level Agreement (SLA)] タブ

タイトル	タイプ	説明
ホスト脆弱性：アサイン先グループ別の SLA 達成 (Host Vulnerability: SLA attainment by assignment group)	複数折れ線グラフ 	アサイン先グループがホスト脆弱性を修復するために要した時間。過去 10 か月間の傾向を示します。
コンプライアンスの問題：アサイン先グループ別の SLA 達成 (Compliance Issues: SLA attainment by assignment group)	複数折れ線グラフ 	アサイン先グループがコンプライアンスの問題を修復するために要した時間。過去 10 か月間の傾向を示します。
アプリケーション脆弱性：アサイン先グループ別の SLA 達成 (Application Vulnerability: SLA attainment by assignment group)	複数折れ線グラフ 	アサイン先グループがアプリケーション脆弱性を修正するために要した時間。過去 10 か月間の傾向を示します。
コンテナ脆弱性：アサイン先グループ別の SLA 達成 (Container Vulnerability: SLA attainment by assignment group)	複数折れ線グラフ 	アサイン先グループがコンテナ脆弱性を修復するために要した時間。過去 10 か月間の傾向を示します。

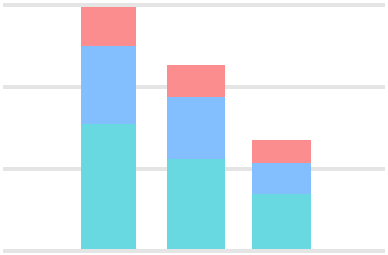
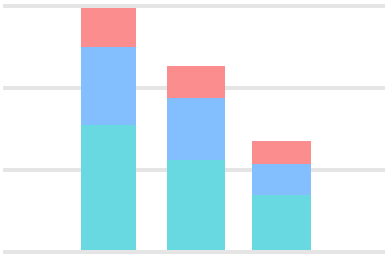
[除外の概要 **(Exclusion overview)]** タブ

タイトル	タイプ	説明
除外ルール	テーブル	作成したすべての除外ルールのリスト。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[除外の概要 **(Exclusion overview)**] タブ (続く)

タイトル	タイプ	説明
「インターネットアクセス可」に対する除外ルール	積み上げ棒グラフ 	「インターネットアクセス可」の資産に関する検出に影響を与える除外ルール。
「エクスプロイトの存在」に対する除外ルール	積み上げ棒グラフ 	「既存のエクスプロイトに対する脆弱性あり」の検出に影響を与える除外ルール。

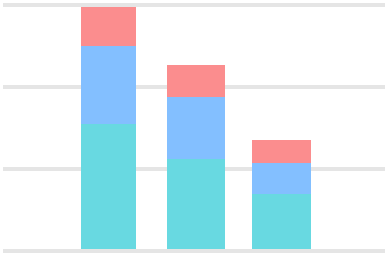
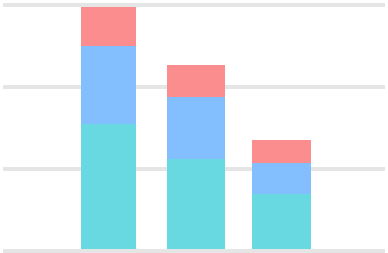
[脆弱性インテリジェンス **(Vulnerability Intelligence)**] タブ

タイトル	タイプ	説明
EPSS スコア >= 0.9 の脆弱性	テーブル	EPSS スコアが 0.9 以上のすべての脆弱性エントリ (CVE または TPE) の完全なリストビューと、次の詳細が表示されます。 • ID：脆弱性の CVE ID • EPSS スコア (EPSS Score) • EPSS 最終変更 (EPSS Last Modified) • CISA KEV BOD 22-01：エントリが CISA KEV BOD (拘束力のある運用指令 22-01) に存在するかどうかを示します • 合計 VI：この脆弱性エントリに存在する VI の合計数。 • 合計コンテナ VI：この脆弱性エントリに存在するコンテナ VI の合計数。 • 重大度

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[脆弱性インテリジェンス **(Vulnerability Intelligence)**] タブ (続く)

タイトル	タイプ	説明
EPSS スコア >= 0.9 の外部向けホスト脆弱性一致アイテム	単一スコア	EPSS スコアが 0.9 以上の外部向けホスト脆弱性一致アイテムの合計数を示す数。リスク評価の重大度でソートされた単一のスコアを提供します。
リスク評価別の外部向けホスト脆弱性一致アイテム	積み上げ棒グラフ 	リスク評価別の外部向けホスト脆弱性一致アイテムの数。積み上げ棒グラフは、EPSS スコア >= 0.9 および CISA KEV =True で分類されます。
リスク評価別 EPSS スコア >= 0.9 の脆弱性一致アイテム	積み上げ棒グラフ 	リスク評価でソートされた、EPSS スコアが 0.9 以上の脆弱性の数。ホスト脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、およびコンテナ脆弱性一致アイテム別のブレークダウンを提供します。

データ収集スケジュール済みジョブ

データ収集ジョブにより、自動インジケーターおよび自動ブレークダウンのスコアが自動的に収集されます。新しいデータのスコアを自動的に収集するために、次のスケジュール済みジョブが実行されます。

警告:
デフォルトでは、ベースシステムでは次のデータ収集ジョブは非アクティブです。

- 統一ダッシュボード日次データ収集 (Unified Dashboard Daily Data Collection)
- 統一ダッシュボード週次データ収集 (Unified Dashboard Weekly Data Collection)
- 統一ダッシュボードデータ収集 (Unified Dashboard Data Collection)

ジョブを有効にする前に、KB を参照してください。

スケジュール済みジョブ	頻度	説明
統一ダッシュボードデータ収集 (Unified Dashboard Data Collection)	1 回	既存のレコードのスコアとスナップショットを収集します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みジョブ	頻度	説明
統一ダッシュボード週次データ収集 (Unified Dashboard Weekly Data Collection)	週次	データを毎週収集します。
統一ダッシュボード日次データ収集 (Unified Dashboard Daily Data Collection)	日次	データを毎日収集します。
リスクスコアを組織にロールアップ (Rollup Risk scores to Organization)	日次	組織の集計リスクスコアを収集します。
クラウドコンプライアンスの日次カウントを入力 (Populate cloud compliance daily counts)	日次	クラウドコンプライアンスのデータを収集します。
EPSS 日次ジョブ	日次	First.org から EPSS データを収集します。

新しいテーブルであるロールアップアプリケーションのリスクスコア (Rollup Application Risk Score) [sn_vul_cmn_rollup_app_risk_score] が Vulnerability Common Scope に作成されます。このテーブルは、毎日のスケジュール済みジョブで次のロールアップ算出を使用して入力されます。

自動翻訳

ロールアップ算出名	説明
組織リスクスコアのロールアップ (Organization Risk Score Rollup)	組織内のすべての脆弱性一致アイテムと構成の問題のリスクスコアをロールアップします。これは組織の全体的なリスクスコアを示します。
脆弱性一致アイテムのロールアップ (Vulnerable Item Rollup)	組織内のすべての脆弱性一致アイテムのリスクスコアをロールアップします。これは組織の全体的なリスクスコアに寄与します。
アプリケーション脆弱性一致アイテムのロールアップ (Application Vulnerable Item Rollup)	組織内のすべてのアプリケーション脆弱性一致アイテムのリスクスコアをロールアップします。これは組織の全体的なリスクスコアに寄与します。
コンテナ脆弱性一致アイテムのロールアップ (Container Vulnerable Item Rollup)	組織内のすべてのコンテナ脆弱性一致アイテムのリスクスコアをロールアップします。これは組織の全体的なリスクスコアに寄与します。
テスト結果ロールアップ (Test Result Rollup)	組織内のすべてのテスト結果のリスクスコアをロールアップします。これは組織の全体的なリスクスコアに寄与します。
NVD から TPE に EPSS スコアをロールアップする	EPSS スコアを NVD から TPE にロールアップし、組織の全体的なリスクスコアに寄与します。

Vulnerability Manager ワークスペース での脆弱性一致アイテムとテスト結果の監視と管理

Vulnerability Manager ワークスペースにより、ウォッチトピックを使用して脆弱性一致アイテム (VIT、AVIT、CVIT) とテスト結果 (TR) を監視し、修復作業を作成することで修復の進捗状況を追跡および管理できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

で検索結果を開く **Vulnerability Manager** ワークスペース

アプリケーションスコープを変更することで、クラシック UI ではなく Vulnerability Manager ワークスペース で検索結果を開きます。

始める前に
必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst、sn_vul.vulnerability_admin、または sn_vul.read_all
- アプリケーション脆弱性一致アイテム (AVIT) の場合は sn_vul.app_sec_manager または sn_vul.app_read_all
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst、sn_vul_container.vulnerability_admin、または sn_vul_container.read_all
- 構成テスト結果 (TR) の場合、sn_vulc.admin または sn_vulc.read

このタスクについて
例:アプリケーションスコープを Vulnerability Manager ワークスペース に設定して、[検索] フィールドでホスト脆弱性一致アイテムをその番号で検索すると、VIT がVulnerability Manager ワークスペースのレコードビューで開きます。

手順

1. 統一ナビゲーションバーで、地球儀アイコン を選択します。
2. アプリケーションスコープを選択します。
3. スコープを 脆弱性マネージャーワークスペースに設定します。

次のタスク
VIT、修復タスク、ステータス変更承認などのレコードを検索すると、統一ナビゲーションバーの [検索] フィールドでレコードが Vulnerability Manager ワークスペースで開きます。

スコープがグローバルでない場合は、赤いリングが付いた [地球] アイコンが表示されます。 [。再度選択すると、スコープが変更されます。

アクティブなレコード (VIT、AVIT、CVIT、CTR) のサマリーを作成してフィルターを適用する

脆弱性マネージャーおよびアナリストは、目的のレコードをフィルタリングして、 Vulnerability Manager ワークスペースのホームページに概要を可視化できます。

始める前に
必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース > ホームページ.
2. 歯車アイコン 歯車 を選択し、[ホスト脆弱性]、[コンテナ脆弱性]、[アプリケーション脆弱性]、または [構成テスト結果] タブで [フィルターを作成] を選択します。
3. [フィルターを作成] ポップアップウィンドウで、フィールドに入力します。

[フィルターの作成] ポップアップウィンドウ

フィールド	説明
フィルター名	フィルターの名前。
条件	可視化するレコードのみを表示するための条件。
毎日更新	可視化情報を毎日更新します。

4. **[Save** (保存)] を選択します。
5. [表示基準] フィールドで新しいフィルターを選択して、フィルタリングされたレコードの可視化を表示します。
ヴィジェットの詳細については、「のホームページ Vulnerability Manager ワークスペース」を参照してください。
6. フィルターを更新または削除するには：

   a. 歯車アイコン を選択し、 フィルターの編集 を選択します。

   b. [保存済みフィルター] ポップアップウィンドウで、更新または削除するフィルターを選択します。

   c. フィルターを更新または削除します。

アクション	ステップ
フィルターを削除します。	[削除] を選択します。
フィルター名を変更	フィルター名を編集し、[更新] を選択します。
フィルター条件の変更	特定のレコードの情報のみを表示するように条件を編集し、[更新] を選択します。
毎日更新	可視化情報を毎日更新するかどうかを決定し、[更新] を選択します。

関連情報

のホームページ Vulnerability Manager ワークスペース

の使用 でトピックを監視する **Vulnerability Manager** ワークスペース

Vulnerability Manager ワークスペースのウォッチトピックを使用して、設定した条件からインポートされたデータからフィルタリングされた脆弱性と構成ミスを表示します。この情報を使用して、各ウォッチトピックの脆弱性と構成ミスが環境にどのように影響するかを判断します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

このタスクについて
[監視トピック] ページから、次のタスクを実行できます。

- 修復作業とレコード (VIT、AVIT、CVIT、TR) の数を監視して、脆弱性修復の進捗状況を確認します。
- 既存の監視トピックを編集または削除し、監視トピックを作成します。
- 修復作業を作成し、修正する必要がある脆弱性の修復タスクのみを IT チームに渡す。

注:
脆弱性対応 の v19.0 以降では、次の用語の名前が変更されました。

用語の変更

v19.0 より前の用語	**v19.0** 以降の用語
テスト結果グループ	修復タスク
構成の問題	構成テスト結果
ポリシー	テストグループ

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性マネージャーワークスペース.
2. 監視トピックアイコンを選択します。
3. [監視トピック] ページの [ホスト脆弱性]、[コンテナ脆弱性]、[アプリケーション脆弱性]、または [構成テスト結果] タブで監視トピックを選択します。

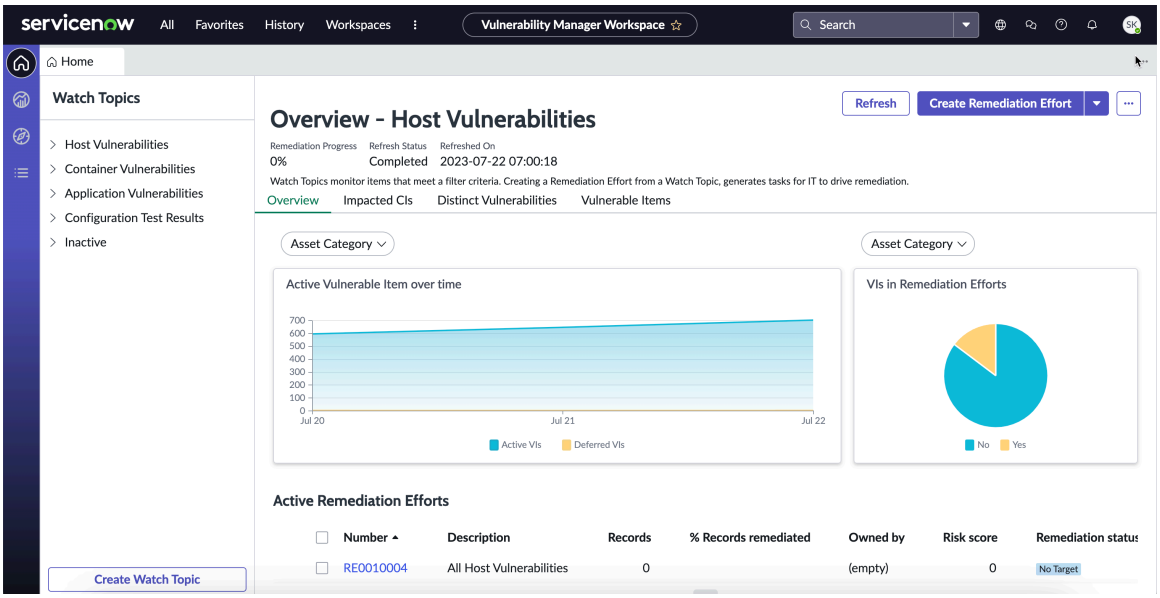
   ウォッチトピックを選択すると、デフォルトで [概要] タブが表示されます。

   監視トピックの詳細については、「の [監視トピック] ページ Vulnerability Manager ワークスペース」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

バージョン **19.0** の脆弱性マネージャーのワークスペースのホームページの [概要] タブ



ダッシュボードでは、インポート時に動的に新しい脆弱性データの更新が行われます。

4. 関連アイテムタブを選択して、さらにデータを表示します。

   ウォッチトピックの関連アイテムリストと可視化の詳細については、「監視トピックの関連アイテムリストと可視化」を参照してください。

5. [ウォッチトピック] ページで UI アクションを実行します。

6. オプション: レコードを選択すると、詳細が表示されます。

で監視トピックを作成する **Vulnerability Manager** ワークスペース

脆弱性マネージャーと脆弱性アナリストは、一連の条件を使用してウォッチトピックを作成し、監視するレコードのサブセット (VIT、AVIT、CVIT、CTR) を除外できます。

始める前に

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

このタスクについて

監視トピックの [概要] タブでは、他のレポートとともに夜間に更新されるトレンドレポートに、その監視トピックのレコードの現在のステータスが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
脆弱性対応 の v19.0 以降では、次の用語の名前が変更されました。

用語の変更

v19.0 より前の用語	**v19.0** 以降の用語
テスト結果グループ	修復タスク
構成の問題	構成テスト結果
ポリシー	テストグループ

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性マネージャーワークスペース > 監視トピック.
2. オプション: または、[修復作業の作成] ボタンの右側にある 3 つのドットの ... をクリックし、続いて [編集] をクリックして、既存のウォッチトピックを変更します。

   注:
   フィルタリングを変更した後、監視トピックに現在のデータが表示されるまでに遅延が発生する場合があります。

3. ページの左下にある [**Create Watch Topic**] を選択します。
4. 表示されるモーダルのフィールドに入力します。
   [トピックを作成] モーダルフィールドの詳細については、「[ウォッチトピックを作成] フォームのフィールド」を参照してください。
5. 選択したレコードカテゴリの条件を定義します。

   注:
   ウォッチトピックに条件を設定しない場合、データはダッシュボードに取り込まれません。

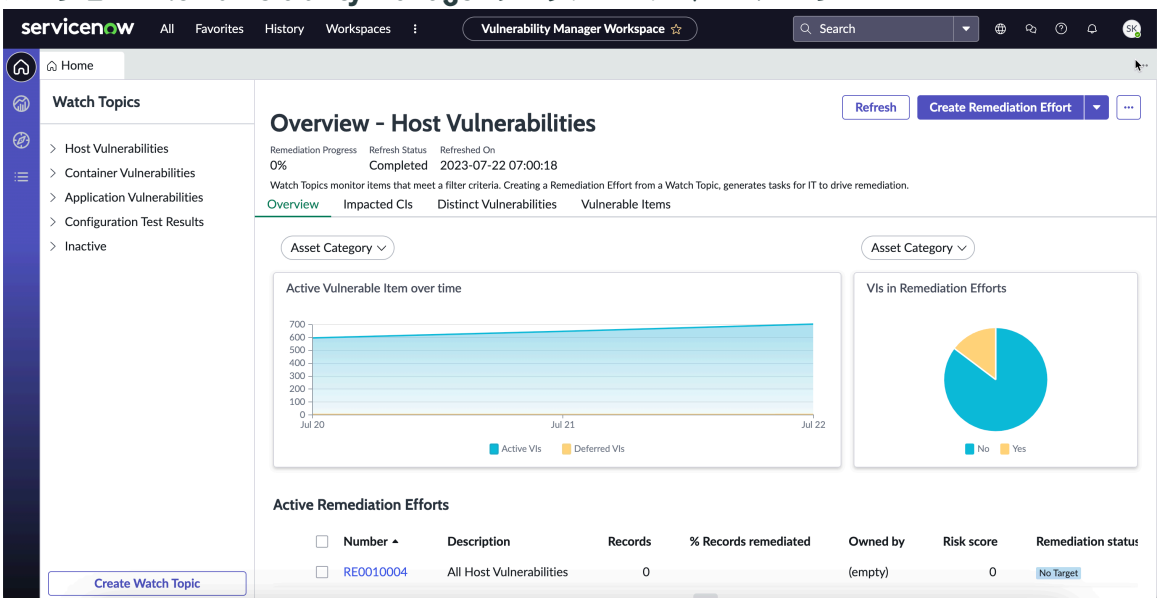
6. [送信] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

新しいウォッチトピックがホームランディングページに表示されます。ウォッチトピックナビゲーションペインでレコードタイプ別に分類されます。

バージョン **19.0 Vulnerability Manager** ワークスペース ホームページ



次のタスク
修復作業を作成します。

で監視トピックを編集または削除する **Vulnerability Manager** ワークスペース

Vulnerability Manager ワークスペース内の既存の監視トピックを編集または削除できます。

始める前に

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

このタスクについて

既存の監視トピックを編集する場合：

- ダッシュボードのデータが更新されて変更が反映されます。
- 既存の修復作業に現在含まれているレコードは変更されません。
- 修復作業に現在含まれていないレコードは、条件ビルダーに入力した条件に基づいて表示されます。

監視トピックのすべての関連レコードが修正される前に監視トピックを削除しても、その監視トピックとともに表示されるレコードは影響を受けません。

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース > 監視トピック.
2. 編集する監視トピックを開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 3 点の ... をクリックし、[編集] をクリックします。

   注:
   非アクティブなウォッチトピックを編集することはできません。

4. [監視トピックを編集] モーダルで、フィールドを変更します。
5. [**Submit** (送信)] を選択します。

   注:
   フィルタリングを変更した後、監視トピックに現在のデータが表示されるまでに遅延が発生する場合があります。

   既存の繰り返し修復作業も編集できます。ウォッチトピックに対する既存の繰り返し修復作業がある場合は、メニューから [繰り返し作業を編集] を使用できます。繰り返し作業を編集するには、このオプションを選択します。

   修復作業レコードに変更を加えて保存しても、ウォッチトピックから既に作成済みの他の修復作業には影響しません。

6. オプション: 監視トピックを削除するには、監視トピックの 3 点メニューの ... を選択し、[削除] を選択します。

監視トピックをアクティブ化または非アクティブ化する

脆弱性マネージャーワークスペースで、ウォッチトピックを非アクティブ化またはアクティブ化できます。

始める前に

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

このタスクについて

- すべての非アクティブなウォッチトピックは、ナビゲーションペインの [非アクティブ] モジュールに表示されます。
- 非アクティブなウォッチトピックに対して修復作業または繰り返し修復作業を作成することはできません。
- 非アクティブなウォッチトピックをリフレッシュすることはできません。
- 非アクティブなウォッチトピックとそれに関連する修復作業の詳細は更新されません。

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース > 監視トピック.
2. 非アクティブ化する監視トピックを開きます。
3. 3 つのドットをクリックし、[非アクティブ化] をクリックします。
   監視トピックが [非アクティブ] モジュールに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. 監視トピックをアクティブ化するには、[非アクティブ] モジュールで監視トピックを選択し、3 点メニューを選択して [アクティブ化] を選択します。
   アクティブ化されたウォッチトピックがナビゲーションペインの適切なモジュールに移動されます。

修復作業レコードを使用する

脆弱性マネージャーと脆弱性アナリストが修復作業 (RE) を作成すると、修復タスク (VUL、AVUL、CVUL、CRG) が修復のために IT チームに自動的にアサインされます。

始める前に

修復作業を使用して修復タスクの修正の進捗状況を監視するには、修復作業を作成する必要があります。

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

手順

1. 選択されていない場合は、左上の [リスト] アイコンをクリックします。

   アクティブな修復作業レコードを含むリストビューが表示されます。

2. [レコードタイプ] 列で、3 つのドットメニューを選択し、[レコードタイプ別にグループ化] を選択します。
   修復作業は、ホスト脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、および構成テスト結果に分類されます。
3. [リストビュー] ランディングページで、フィルター済みリストにおいて [アクティブな修復作業] が選択されている状態で、レコードをクリックして開きます。
   レコードが表示されます。選択した修復作業に関連付けられている修復タスクとレコードを表示できます。
4. 修復作業レコードで実行できるアクションについては、次の表を参照してください。

   レコードを作成した後、修復タスクと多数のレコードが表示されるまでに数分かかる場合があります。

UI アクション	説明
タグを追加する	ヘッダーの右側にある小さなタグアイコンをクリックします。このレコードを識別するのに役立つテキストを追加することもできます。たとえば、このレコードに PCI またはその他の重要なデータが含まれていることを示すタグを追加できます。
レコードに作業メモを追加する	画面の右端にあるアクティビティアイコン (稲妻アイコン) をクリックし、作業メモを入力します。。アイコンをクリックしてパネルを切り替えます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

UI アクション	説明
レコードを更新する	[詳細] タブで、編集可能なすべてのフィールドから 1 つをクリックして選択し、変更を加え、[保存] をクリックしてレコードを更新します。
フィルターアイコンが表示されている場合、それをクリックして、表示されたページのデータを絞り込む	[修復タスク] タブ、[脆弱性一致アイテム] タブ、[構成テスト結果 (Configuration Test Results)] タブのいずれかを選択した状態で、右端のフィルターアイコンをクリックすると、そのタブに適用されるフィルターが表示されます。 表示されるパネルで [詳細表示] をクリックし、ページ上のアイテムのフィルター条件を追加または変更します。[更新] をクリックして変更を保存します。 たとえば、[脆弱性一致アイテム] タブで [経過時間 (Age)] フィールドを追加し、範囲を入力して特定の期間のレコードのみが表示されるようにすることもできます。設定した条件に一致するレコードがリストに表示されます。
列内のアイテムのフィルターを絞り込む	列を選択し、縦 3 点メニューをクリックして展開し、列のデータを絞り込んでグループ化するための条件を入力します。
アイテムを除外する、または列内の行のアイテムと一致させる	たとえば、特定の脆弱性があるレコードのみを表示するとします。レコードのリストから、[サマリー] 列のレコードの行を選択します。表示される縦 3 点メニューをクリックし、次のいずれかを選択します。 ○ この値で絞り込み：この脆弱性がある他のすべてのレコードを表示します。 ○ この値を除外：この脆弱性がないすべてのレコードを表示します。

5. [修復タスク]、[脆弱性一致アイテム]、および [構成テスト結果] タブから、個々の修復タスク (VUL、AVUL、CVUL、CRG)、脆弱性一致アイテム (VIT、AVIT、CVIT) テスト結果 (CTR) レコードにそれぞれドリルダウンできます。

次のタスク

修正作業からオンデマンドで修復タスクを作成するには、「の修復作業から修復タスクをオンデマンドで作成する Vulnerability Manager ワークスペース」を参照してください。「カスタマイズされたレコードリストの作成」を実行して、修正の進捗状況を監視することもできます。

で修復作業を作成する **Vulnerability Manager** ワークスペース

修復作業レコードは、 Vulnerability Manager ワークスペースのウォッチトピックから作成するレコードの静的リストです。

始める前に

必要なロール：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

このタスクについて

修復作業を使用して、IT チームが脆弱性や構成ミスを修正するために使用するタスクを引き継ぎます。

- 既存の修復作業を編集できます。
- 設定した日時に自動的に作成される修復作業を作成します。
- 既存の修復作業から新しい修復作業にレコードを転送します。

バージョン 18.0 以降では、非アクティブなウォッチトピックに対して修復作業を作成できないため、[修復作業の作成] ボタンは非アクティブです。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性マネージャーワークスペース > 監視トピック.
2. [監視トピック] ページで、修復作業を作成する監視トピックを選択します。
3. 選択したウォッチトピックに関連付けられているレコードを表示するには、レコードヘッダーの下にある、それぞれのウォッチトピックの [脆弱性一致アイテム]、[アプリケーション脆弱性一致アイテム]、[コンテナ脆弱性一致アイテム]、または [構成テスト結果] タブをクリックします。

   レコードが表示されます。

   たとえば、[脆弱性一致アイテム] タブのヘッダーでは、このウォッチトピックに含まれるレコードの合計数を表示できます。

   以下の列とデータが表示されます。

[脆弱性一致アイテム] タブの列

列	説明
数値	レコードの番号。
まとめ	脆弱性の説明。
構成アイテム	脆弱性に関連付けられた資産。
リスク評価	レコードを [重大]、[高]、[中]、[低]、および [なし] に分類する数値化されたリスクスコア。
状態	レコードのステータス。
修復ステータス	レコードの修正ステータス。
アサイン先グループ	修正を担当するアサイン先グループ。グループへのレコードのアサインは、作成したアサインルールに基づいています。
修復作業	修復作業にアサインされている場合、各レコードにはアサインされた修復作業が一覧表示され

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

列	説明
	ます。修復作業に追加されると、レコードは作成した他のどの修復作業にも追加されません。
アサイン先グループ	修正を担当するアサイン先グループ。グループへのレコードのアサインは、作成したアサインルールに基づいています。
修復作業	修復作業にアサインされている場合、各レコードにはアサインされた修復作業が一覧表示されます。修復作業に追加されると、レコードは作成した他のどの修復作業にも追加されません。
修復タスク中	true の場合、この値はレコードが既に修復タスクにあることを示しています。レコードは複数の修復タスクに存在できますが、1 つの修復作業にしか追加できません。
エクスプロイト有無	レコードに既知のエクスプロイトが存在するかどうかを示します。
最終オープン日時	Now Platform でレコードが最後にオープンされた日付。レコードがクローズされてから再オープンされた場合は、レコードが最後に再オープンされた日付になります。

4. 修復作業を作成するには、[修復作業の作成] をクリックします。

   修復作業を作成すると、既存の修復作業にあるレコードは、このウォッチトピックから作成する新しい修復作業には追加されません。

   ウォッチトピックでレコードが更新されるか、新しいレコードが作成されると、修復作業を行うことができます。

5. または、で繰り返し修復作業を作成する Vulnerability Manager ワークスペースを実行できます。

   [編集] ボタンは、既存の修復作業のメニューで使用できます。選択によって、表示されるモーダルからフィールドと条件を変更できます。修復作業レコードに加えた変更は、ウォッチトピックからすでに作成済みの他の修復作業には影響しません。

6. [修復作業の作成] モーダルのステップ 1 で、フィールドに入力します。

   [簡単な説明] フィールドに、繰り返し修復作業を説明するテキストを入力すると、作業リストから修復作業を見つけて追跡できるようになります。

   [説明] フィールドに、修正作業のリストから簡単に見つけることができるように作業のコンテキストに関するテキストを入力します。

7. ステップ 2 のタスクの生成では、リストから 1 つのメソッドを選択して、作成後にこの修復作業から生成する修復タスクにレコードをバンドルします。

8. 重複するホスト脆弱性一致アイテムを自動的にリフレッシュするには、[作成された修復タスクの重複脆弱性一致アイテムを自動的にリフレッシュ する] チェックボックスをオンにする必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
このチェックボックスは、ホスト脆弱性に対してのみ使用できます。

9. ステップ 3 の [転送] で、修復作業に追加するレコードの数を確認し、他のアクティブな修復作業から転送できるレコードの数を確認します。

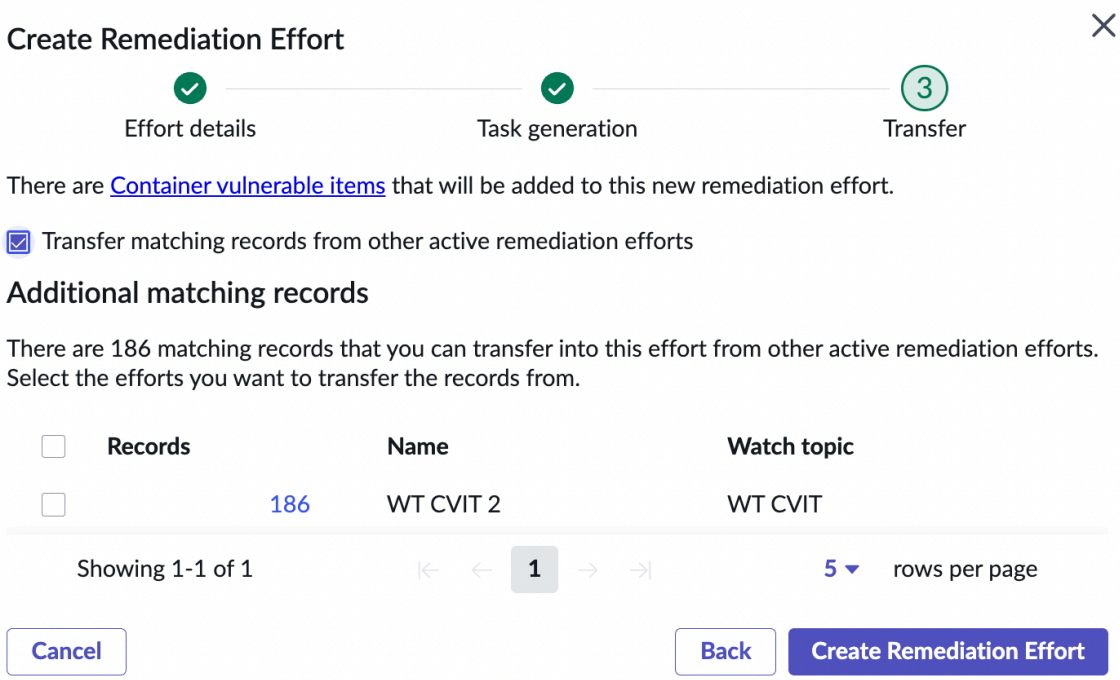
   追加する新しいアクティブなレコードがない場合は、次のテキストが表示されます。

   この新しい修復作業に追加できるアクティブな利用可能レコードがありません。(There are no available active records that you can add to this new remediation effort.)

   この作業に転送できる追加のレコードは、[追加の一致するレコード] の下に一覧表示されます。

   [他のアクティブな修復作業から一致するレコードを転送] チェックボックスをオンにしてから、他のアクティブな修復作業から転送するレコードのチェックボックスをオンにします。

   バージョン **18.0** の修復作業の作成



   [修復作業の作成] をクリックして、しばらくすると、新しい修復作業が表示されます。レコードの数によっては、新しいレコードの入力に時間がかかる場合があります。メッセージで、レコードがまだ入力中であるかどうかが示されます。

   新しい修復作業は、既存の作業から転送するために選択したレコードに加えて、作成に使用されたウォッチトピックから利用可能なレコードを使用して作成されます。

   既存の作業から転送するレコードを選択し、既存の作業のすべてのレコードを新しい作業に転送すると、レコードの移動元の修復作業はクローズされます。修復作業に関連付けられた修復タスクがレコード転送によってどのように影響を受けるかの詳細については、「脆弱性対応ワークスペースの修復作業、修復タスク、およびレコードのライフサイクル」を参照してください。

   注:
   ウォッチトピックからの利用可能なレコードがない場合や、転送用に選択されたレコードがない場合、[修復作業の作成] ボタンは非アクティブ化されます。

   Populate Efforts スケジュール済みジョブが 10 分ごとに実行され、選択した条件に基づいてウィジェットにデータが入力されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[修復の進捗状況] タブをクリックして、修正の進捗状況を表示します。任意のアイテムをクリックすると、レコードタイプ、リスクスコア、リスク評価、修正されたレコードの割合、保留/非保留ステータスのレコードと合計レコード数、ウォッチトピックで使用される条件、および修復ステータスなどの詳細が表示されます。修復ターゲットや修復ステータスなどの修復ステータス情報は、脆弱性一致アイテムテーブルからロールアップされます。最高のレコードリスクスコアは脆弱性算出テーブルからロールアップされ、リスクスコアは脆弱性算出テーブルからロールアップされます 脆弱性ロールアップ算出 > 修正作業をロールアップ.

[修復タスク] タブには、すべてのタイプの問題に関するタスクが表示されます。以下のスケジュール済みジョブが実行されると、フィールドに値が入力されます。ジョブは 15 分ごとに自動的に実行されます。

- アプリケーション脆弱性一致アイテムの値を脆弱性とグループにロールアップします。
- コンテナ脆弱性一致アイテムの値を脆弱性とグループにロールアップします。
- テスト結果値をテスト結果グループと構成テストにロールアップします。
- 脆弱性一致アイテムの値を脆弱性とグループにロールアップします。

リストビューでは、修復作業、修復タスク、脆弱性一致アイテム、構成テスト結果などを表示できます。修復タスクまたは脆弱性一致アイテムを開き、[詳細] ページを表示できます。[その他のアクション] (省略記号) をクリックし、[調査を開始] をクリックして修復タスクを解決します。

10. オプション: 既存の繰り返し修復作業も編集できます。

    (Optional) ウォッチトピックに既存の繰り返し修復作業がある場合は、ウォッチトピックの右上にあるメニューから [繰り返し作業を編集] を使用できます。繰り返し作業を編集するには、このオプションを選択します。

    修復作業レコードに加えた変更は、ウォッチトピックからすでに作成済みの他の修復作業には影響しません。

の修復作業から修復タスクをオンデマンドで作成する **Vulnerability Manager** ワークスペース

修復作業からオンデマンドで修復タスクを作成します。オンデマンドで修復タスクを作成する場合は、手動で追加するレコードを選択します。

始める前に

必要なロール：sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin

このタスクについて

脆弱性対応 のバージョン 18.0 では、修復作業のレコードビューから修復タスクを作成することはできません。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性マネージャーワークスペース.
2. ホームページが表示されているワークスペースの左上で、[リストビュー] アイコンを選択し、リストランディングページを表示します。
3. [修復作業] で、[アクティブ] または [すべて] をクリックします。
4. 表示されるリストから、レコードをクリックして開きます。
   レコードの [概要] タブが表示されます。
5. [脆弱性一致アイテム] タブをクリックします。
   レコードのリストが表示されます。
6. 新しい修復タスクを作成するには、[番号] 列で、追加するレコードを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. [修復タスクの作成] をクリックします。
8. 表示されるモーダルのフィールドに入力します。
9. [作成] をクリックします。
10. 新しい修復タスクが、選択したアクティブなレコードとともに表示されます。

で繰り返し修復作業を作成する **Vulnerability Manager** ワークスペース

設定した日時に自動的に生成される繰り返し修復作業を作成してスケジュールすることができます。

始める前に

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

このタスクについて

スケジュールに基づいて繰り返し修復作業を自動的に作成することで、発生する可能性があり、即時かつ継続的な注意が必要な脆弱性を追跡できます。

バージョン 18.0 以降では、非アクティブなウォッチトピックに対して繰り返し修復作業を作成できないため、[繰り返し作業を作成] オプションは非アクティブです。既に繰り返し作業がスケジュールされているウオッチトピックを非アクティブ化すると、そのウオッチトピックがアクティブ化されるまで新しい修復作業は作成されません。また、右上の [作業繰り返し **(Effort recurrence)]** と [次の繰り返し日 **(Next recurrence date)]** の詳細が表示されなくなります。ウォッチトピックをアクティブ化すると、今後のスケジュールで修復作業が作成されます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性マネージャーワークスペース > 監視トピック.
2. [監視トピック] ページで、繰り返し修復作業を作成する監視トピックを選択します。

   ウォッチトピックごとに 1 つの繰り返し修復作業を作成できます。

   > **注:**
   > 繰り返し修復作業から新しい修復作業にレコードを転送することはできません。ただし、既存の繰り返さない修復作業から新しい修復作業にレコードを転送することはできます。レコードの転送の詳細については、「の修復作業にレコードを転送する Vulnerability Manager ワークスペース」を参照してください。

3. [修復作業の作成 (Create Remediation Effort)] リストの右上にあるウォッチトピックで、[繰り返し作業を作成 **(Create Recurring Effort)]** を選択します。

   [繰り返し作業を作成] モーダルが表示されます。

4. ステップ 1 で、[作業の詳細] の必須フィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[簡単な説明] フィールドに、繰り返し修復作業を説明するテキストを入力すると、作業リストから修復作業を見つけて追跡するのに役立ちます。

[説明] フィールドに、修復作業のリストから簡単に見つけることができるように作業のコンテキストに関するテキストを入力します。たとえば、「外部向け資産の脆弱性」などとします。

5. [次へ] をクリックします。
タスク生成の詳細が表示されます。
6. ステップ 2 のタスクの生成では、リストから 1 つのメソッドを選択して、作成後にこの修復作業から生成する修復タスクに脆弱性一致アイテムをバンドルします。
   - アサイン先グループ別 (By Assignment group)
   - アサイン先グループと構成アイテム別 (By Assignment group and configuration item)
   - アサイン別グループと脆弱性
   - なし (修復タスクは作成されません)。この作業の修復タスクに手動でレコードを追加する場合は、この方法を使用します。「の修復作業から修復タスクをオンデマンドで作成する Vulnerability Manager ワークスペース」を参照してください。
7. 重複するホスト脆弱性一致アイテムを自動的にリフレッシュするには、[作成された修復タスクの重複脆弱性一致アイテムを自動的にリフレッシュ する] オプションを選択する必要があります。

   注:
   このチェックボックスは、ホスト脆弱性に対してのみ使用できます。

8. [次へ] をクリックして続行します。
9. ステップ 3 の [繰り返し (Recurrence)] で、頻度を選択します。

   a. 繰り返しスケジュールを定義します。

   リストを使用して、修復作業を作成する月/日/時間/分を選択します。スケジュール設定のタイムゾーンは、デフォルトでは各自のタイムゾーンです。

   注:
   脆弱性が多い場合は、作成を営業時間外に設定することをお勧めします。

   月の最終日にジョブを作成すると、スケジュール済みジョブで月の最終日に繰り返し修復作業が作成されます。31 日でない月の場合は、メッセージが表示されます。

   b. オプション: この修復作業におけるアクティブな脆弱性を、作成された後続の各修復作業に引き継ぐ場合は、[脆弱性を引き継ぐ] を選択します。

10. [繰り返しをスケジュール] をクリックします。
繰り返し修正レコードが作成されたことを示すメッセージが表示されます。新しい修復作業はすぐには表示されず、スケジュールしたときに作成されます。スケジュール済みジョブによって作成された後、リストに表示されます。

修復作業が作成される日付は、対応するウォッチトピックに表示されます。修復作業に関連付けられた修復タスクがレコード転送によってどのように影響を受けるかの詳細については、「 脆弱性対応ワークスペースの修復作業、修復タスク、およびレコードのライフサイクル」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

の修復作業にレコードを転送する **Vulnerability Manager** ワークスペース

既存の修復作業から Vulnerability Manager ワークスペースの新しい修復作業にレコードを転送できます。

始める前に
ゼロデイ脅威または迅速に解決したい非常に重大な脆弱性に直面した場合、この脆弱性に対して既に存在しているアクティブなレコードを 1 つの修復作業にまとめることができます。ただし、各レコードは 1 つの作業にしか含めることができませんが、レコードはウォッチトピック間で重複させることができます。したがって、それらをすべて収集するには、これらのレコードを複数の既存の作業から 1 つの修復作業に転送する必要があります。

たとえば、優先度の高い脆弱性が 1 つある修復作業を作成したとします。この脆弱性は広範囲に及んでおり、環境内の他の領域に影響を与える恐れがあるため、既存の修復作業において、この脆弱性が既にレコードに関連付けられている可能性があります。こうしたレコードすべてを 1 つの修復作業にまとめるために、既存の修復作業から新しい修復作業にレコードを転送できます。

注:
繰り返し修復作業から新しい修復作業にレコードを転送することはできません。詳細については、「で繰り返し修復作業を作成する Vulnerability Manager ワークスペース」を参照してください。

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性マネージャーワークスペース.
2. 監視トピックアイコンを選択します。
3. [監視トピック] ページで、繰り返し修復作業を作成する監視トピックを選択します。
4. [修復作業の作成] をクリックします。
   [修復作業の作成] モーダルが表示されます。
5. ステップ 1 で、[作業の詳細] の必須フィールドに入力します。

   [簡単な説明] フィールドに、繰り返し修復作業を説明するテキストを入力すると、作業リストから修復作業を見つけて追跡するのに役立ちます。

   [説明] フィールドに、修復作業のリストから簡単に見つけることができるように作業のコンテキストに関するテキストを入力します。たとえば、「Active Log4J Vulnerabilities」などを入力します。

   a. [名前] フィールドに新しい修復作業の名前を入力します。
      デフォルトでは、ウォッチトピック名が表示されます。

   b. [説明] フィールドに、この修正作業をリストから見つけやすくするためのテキストを入力します。

6. [次へ] をクリックします。

自動翻訳

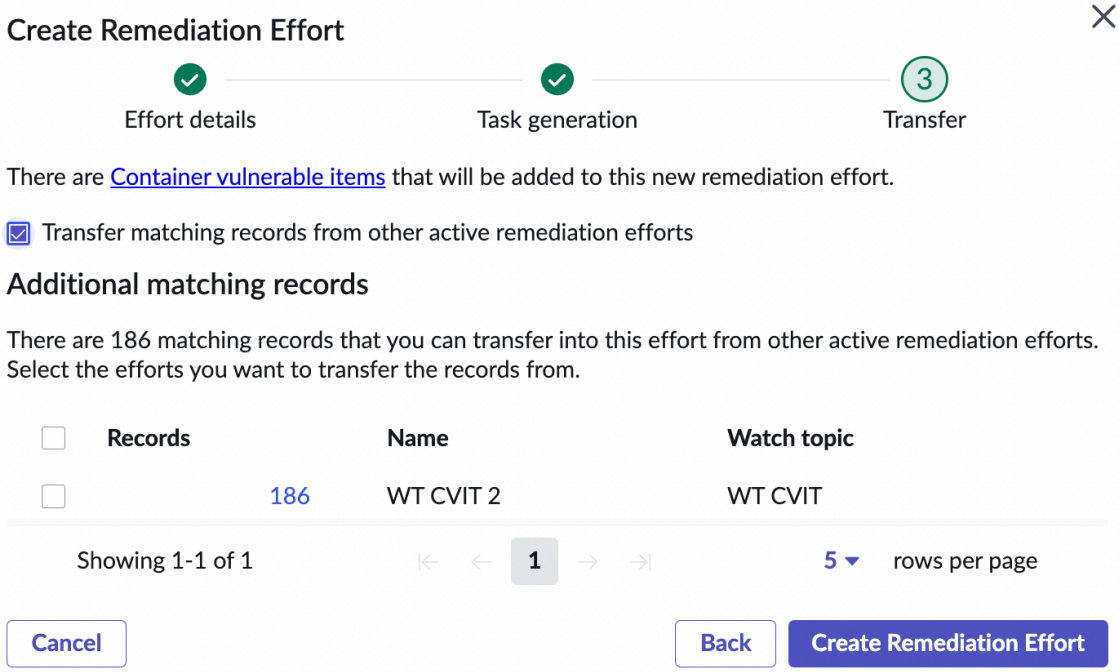
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスク生成の詳細が表示されます。

7. ステップ 2 のタスクの生成では、リストから 1 つのメソッドを選択して、作成後にこの修復作業から生成する修復タスクにレコードをバンドルします。
   - アサイン先グループ別 (By Assignment group)
   - アサイン先グループと構成アイテム別 (By Assignment group and configuration item)
   - アサイン別グループと脆弱性
   - なし (修復タスクは作成されません)。この作業の修復タスクに手動でレコードを追加する場合は、この方法を使用します。「の修復作業から修復タスクをオンデマンドで作成する Vulnerability Manager ワークスペース」を参照してください。
8. 重複する脆弱性一致アイテムを自動的にリフレッシュするには、 [作成された修復タスクの重複脆弱性一致アイテムを自動的にリフレッシュします] オプションを選択する必要があります。
9. [次へ] をクリックします。
10. ステップ 3 の [転送] で、修復作業に追加するレコードの数を確認し、他のアクティブな修復作業から転送できるレコードの数を確認します。
11. 他の作業からレコードを転送するには、リストで、必要なレコードのチェックボックスをオンにします。

    [一致するレコードを他のアクティブな修復作業から転送 する] チェックボックスをオンにして、他のアクティブな修復作業から転送するレコードのチェックボックスをオンにします。

バージョン **18.0** の修復作業の作成



12. [修復作業の作成] をクリックします。

    しばらくすると、新しい修復作業が表示されます。レコードの数によっては、時間がかかる場合があります。メッセージで、レコードが入力中であることが示されます。

    新しい修復作業は、既存の作業から転送するために選択したレコードに加えて、作成に使用されたウォッチトピックから利用可能なレコードを使用して作成されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

既存の作業から転送するレコードを選択し、既存の作業のすべてのレコードを新しい作業に転送すると、レコードの移動元の修復作業はクローズされます。

> **注:**
> ウォッチトピックからの利用可能なレコードがない場合や、転送用に選択されたレコードがない場合、[修復作業の作成] ボタンは非アクティブ化されます。

修復作業に関連付けられた修復タスクがレコード転送によってどのように影響を受けるのかに関する詳細については、「レコードの転送またはレコードの引き継ぎ」を参照してください。

補完コントロールをライブラリに追加する

脆弱性マネージャーまたはアナリストは、補完コントロールのリストを Vulnerability Manager ワークスペースの補完コントロールライブラリに追加します。補完コントロールは、ホスト脆弱性一致アイテムと修復タスクのリスク削減に適用できます。

始める前に
必要なロール：sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin

このタスクについて
よく使用されるいくつかの補完コントロールは、ベースシステムに付属しています。これらの補完コントロールを表示するには、次に移動します: ワークスペース > 脆弱性マネージャーワークスペース > **Lists** (リスト) > ライブラリー > 補完コントロール. 要件に応じて、これらの補完コントロールを有効または無効にすることができます。

> **注:**
> 補完コントロール機能は、ホストの脆弱性に対してのみ使用できます。

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース.
2. [リスト] ページの [ライブラリ] で、[補完コントロール] を選択します。
3. [新規] をクリックします。
4. [補完コントロールを作成 (Create Compensating Controls)] フォームで、各フィールドに入力します。

[補完コントロールを作成 **(Create Compensating Controls)]** フォームのフィールド

フィールド	説明
名前	[例外の要求] モーダルの [補完コントロール] ドロップダウンにオプションとして表示される、補完コントロールの名前。
説明	補完コントロールの詳細を示す簡単な情報。
有効	補完コントロールのステータス。アクティブなコントロールのみが、[例外の要求] モーダルの [補完コントロール] ドロップダウンに表示されます。

5. [保存] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [ライブラリ] の [補完コントロール] リストで、目的の補完コントロールを選択し、補完コントロールの [編集]、[アクティブ化]、または [非アクティブ化] を選択し、[保存] をクリックして補完コントロールを変更します。
すべてのアクティブな補完コントロールは、リスク削減要求の [例外の要求] モーダルの [補完コントロール] ドロップダウンのオプションとして表示されます。

次のタスク

脆弱性対応 v21.0 以降では、補完コントロールをライブラリに追加した後に、補完コントロールを CVE または TPE に関連付けることができます。補完コントロールを関連付ける方法の詳細については、「リスク削減要求の CVE または TPE に補完コントロールを関連付ける」を参照してください。

関連情報

- リスク削減の補完コントロールについて
- CVE または TPE のリスク削減を無効または有効にする
- リスク削減要求の CVE または TPE に補完コントロールを関連付ける
- リスクスコアと有効期限に対する補完コントロールの影響

リスク削減要求の **CVE** または **TPE** に補完コントロールを関連付ける

脆弱性マネージャーまたはアナリストは、関連する補完コントロールを Vulnerability Manager ワークスペースの共通脆弱性エントリ (CVE) またはサードパーティエントリ (TPE) に関連付けることができます。これにより、脆弱性によってもたらされるリスクを軽減するために使用できます。

始める前に

必要なロール：sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin

このタスクについて

- 補完コントロールを CVE または TPE に関連付けない場合、アクティブなすべてのコントロールが [例外の要求] フォームの [補完コントロールを選択] フィールドに表示されます。
- 補完コントロールを CVE に関連付けると、この補完コントロールは TPE に自動的に関連付けられ、その TPE が CVE にマッピングされます。

> **注:**
> 補完コントロール機能は、ホストの脆弱性に対してのみ使用できます。

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース.
2. リストページの [ライブラリ] で、コントロールを関連付ける次のいずれかを開きます。
   - CVE リストからの **CVE**。
   - TPE リストの **TPE**。
3. [コントロールの関連付け] を選択します。

   > **注:**
   > [コントロールの関連付け] ボタンは、CVE または TPE のリスク削減が有効になっている場合にのみ表示されます。つまり、CVE または TPE のリスク削減が有効になっている場合にのみ、補完コントロールを関連付けることができます。[コントロールの関連付け] ボタンが表示されていない場合は、[リスク削減の有効化] を選択します。

4. [コントロールの関連付け] モーダルで、リスク削減のために CVE または TPE に関連付けられた脆弱性に適用できる補完コントロールを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. [送信] を選択します。
   - 関連する補完コントロールは、CVE および TPE のレコードビューの [適用される補完コントロール] タブに表示されます。
   - 修復オーナーがリスク削減を要求している間、これらの関連する補完コントロールは、[例外の要求] モーダルの [補完コントロールを選択] フィールドに表示されます。

関連情報

リスク削減の補完コントロールについて

CVE または TPE のリスク削減を無効または有効にする

補完コントロールをライブラリに追加する

リスクスコアと有効期限に対する補完コントロールの影響

CVE または TPE のリスク削減を無効または有効にする

脆弱性マネージャーおよびアナリストは、Vulnerability Manager ワークスペース内の共通脆弱性エントリ (CVE) またはサードパーティエントリ (TPE) に関連付けられたホスト脆弱性のリスク削減要求を無効または有効にできます。

始める前に
必要なロール：admin

このタスクについて
CVE と TPE のリスク削減はデフォルトで有効になっています。

> **注:**
> 補完コントロール機能は、ホストの脆弱性に対してのみ使用できます。

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース.
   リストページの [ライブラリ] で、リスク削減要求を無効にする次のいずれかを開きます。
   - CVE リストからの **CVE**。
   - TPE リストの **TPE**。
2. [リスク削減の無効化] を選択します。
   修復オーナーは、この CVE または TPE に関連するホスト脆弱性一致アイテムのリスク削減を要求できません。つまり、[例外の要求] モーダルで [コントロールの緩和を実施] として [理由] が選択されている場合、[リスク削減の要求] チェックボックスは表示されません。
3. ホスト脆弱性一致アイテムのリスク削減要求を有効にするには、[リスク削減の有効化] を選択します。

関連情報

リスク削減の補完コントロールについて

補完コントロールをライブラリに追加する

リスク削減要求の CVE または TPE に補完コントロールを関連付ける

リスクスコアと有効期限に対する補完コントロールの影響

でのレコードと修復タスクの再スキャン Vulnerability Manager ワークスペース

スケジュールされたスキャンサイクル間で修復タスクとレコードが解決されたことを確認するには、Now Platform からオンデマンドで再スキャンを開始します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

必要なロール：sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin

再スキャンにより、修復アクティビティ、パッチ、およびその他のアクションによって構成アイテム (CI) の特定の脆弱性が正常に修正されたことを確認できます。

Rapid7 および Qualys スキャナーは、脆弱性対応 アプリケーションではデフォルトで無効になっています。これらのアプリケーションをソースとする脆弱性一致アイテムまたは修復タスクから再スキャンを実行しようとすると、[再スキャン] ボタンは使用できません。

これらのスキャナーをアクティブにするには、sn_vul.vulnerability_admin ロールのユーザーとして、次の操作を実行します。

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性スキャン > スキャナー.
2. アクティブ化するスキャナー製品を見つけ、レコードをクリックして開きます。
3. [アクティブ] チェックボックスをオンにします。
4. [更新] をクリックします。

   アクティブ化した製品は、次回のインポート後に脆弱性一致アイテムおよび修復タスクレコードの [ソース] フィールドに表示され、[再スキャン] が UI アクションとして使用可能になります。

再スキャンは、 Vulnerability Manager ワークスペース内の次の統合を使用したレコードおよび修復タスクでサポートされています。詳細は、以下のトピックを参照してください。

- 脆弱性対応 ワークスペースからの Rapid7 脆弱性一致アイテムの再スキャン
- 脆弱性対応 ワークスペースからの Qualys 脆弱性一致アイテムの再スキャン
- 脆弱性対応 ワークスペースからの Tenable.io および Tenable.sc 脆弱性一致アイテムの再スキャン

脆弱性一致アイテムおよび修復タスクレコードから Vulnerability Manager ワークスペース で再スキャンを開始するには、レコードにソースとしてサポートされているスキャナーが必要です。

ソース別にレコードを表示するフィルター済みリストを作成することをお勧めします。リストの作成方法の例については、「カスタマイズされたレコードリストの作成」を参照してください。

Vulnerability Manager ワークスペース でレコードの修復プロパティを再評価

Vulnerability Manager ワークスペース内の一連のレコード (VIT、AVIT、CVIT、TR) のアサイン、修復ターゲット日、修復タスク、例外、およびリスクスコアを評価します。

始める前に

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

このタスクについて

脆弱性対応 v.23.0 以前のバージョンでは、最新のアサイン、修復ターゲット日、リスクスコア、修復タスクを取得する場合、すべてのレコードにルールを適用する必要があり、時間を要するプロセスとなっていました。v.23.0 以降では、特定のレコードのプロパティを選択的に評価および更新できるため、処理時間を短縮できます。さらに、更新されたプロパティに基づいて修復プロセスを絞り込

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

むことができます。脆弱性対応の v24.0.6 以降では、 Vulnerability Manager ワークスペース内の選択したレコードの例外ルールを評価できます。

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース.
2. [リスト] ページより、次のいずれかのリストで [アクティブ] または [すべて] リストを開きます。
   - ホスト脆弱性一致アイテム
   - アプリケーション脆弱性一致アイテム
   - コンテナ脆弱性一致アイテム
   - 構成テスト結果
3. オプション: 目的のレコードのチェックボックスをオンにして、選択したレコードのみを更新するには、モーダルで [選択したアイテム] オプションを選択します。
4. [再評価] ボタンを選択します。
5. [修復プロパティの再評価と更新 (Re-evaluate and update remediation properties)] モーダルで、選択したレコードについて更新するプロパティを選択します。

   注:
   プロパティを選択すると、その依存プロパティが自動的に選択されます。

6. [適用] を選択します。

タスクの結果
選択したレコードのプロパティが更新されます。更新された修復プロパティの以前の値と最新の値は、レコードの作業メモで確認することができます。

Vulnerability Manager ワークスペースでリストビューを使用する

Vulnerability Manager ワークスペースのリストビューを使用すると、脆弱性マネージャー/アナリストおよびセキュリティマネージャー/アナリストは、レコードの修正の進捗状況を表示し、脆弱性対応レコードにドリルダウンし、承認要求と例外のステータスを表示できます。

始める前に
必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性マネージャーワークスペース.
2. ホームページが表示されているワークスペースの左上にある、[リスト] アイコンをクリックします。
3. オプション: [自分のリスト] をクリックして、リストを作成します。
   リストの作成方法の詳細については、「カスタマイズされたレコードリストの作成」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. リストページで実行できるアクションについては、次の表を参照してください。

UI アクション	説明
修復作業を開く	
リストが表示された状態での [番号] 列の左側で、行をロールオーバーし、レコードの小さな情報アイコン **[i]** をクリックします。	レコードの詳細がページの右側のパネルに表示されます。詳細には、以下が含まれています。 ○ アサイン先グループ ○ 脆弱性 ○ アサイン先 ○ 簡単な説明 ○ 説明 各フィールドは編集できます。[アクティブ] チェックボックスが表示されている場合は、レコードをアクティブ化または非アクティブ化することができます。[更新] をクリックして変更を保存します。
リストをリフレッシュする	ページの右上にあるリフレッシュアイコンを使用して、現在のページを再ロードします。
幅をリセット	歯車アイコンをクリックして、リストの列幅を調整します。元のリストのコピーが [あなたのリスト] に保存されます。
表示されたページの URL をコピーする	他の場所で使用するために URL をコピーします。
ページをエクスポートする	モーダルで、ファイルと配信タイプを入力し、[エクスポート] をクリックします。
ページ上のデータのフィルターを絞り込みます。	列を選択し、縦 3 点メニューを展開すると、列のデータをさらにフィルタリングするオプションが表示されます。 たとえば、アクティブな修復タスクリストの [アサイン先グループ] 列を特定のアサイン先グループでフィルタリングすることもできます。
アイテムを除外する、または列内の行のアイテムと一致させる	列のセルを選択し、次のいずれかを選択して表示されるデータを絞り込みます。 ○ この値で絞り込み：列内の選択したセルに一致するアイテムのみを表示します。 ○ 除外：列で選択したセルに一致する列のアイテムを除外します。

5. 右上の [新規] ボタンをクリックして、[*Application Vulnerable items*] の下の [アクティブ] または [すべて] リストからアプリケーション脆弱性一致アイテムを作成します。

カスタマイズされたレコードリストの作成

Vulnerability Manager ワークスペースでカスタマイズされたリストを作成できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース.
2. [リスト] アイコンを選択し、[自分のリスト] をクリックします。
3. [新規リスト] を選択します。
4. [新規リスト] モーダルで、[既存リストから作成] をクリックし、 [リスト] 選択リストから、テンプレートとして使用する既存のリストを検索します。
5. リスト名を編集します。
6. フィルターを追加します。
   たとえば、特定のスキャナー向けに、再スキャンに備えて監視するアクティブなレコードのリストを作成することができます。[アクティブ] [次の値に等しい] [true]、[ソース] [contains (次の値含む)] [(スキャナーの名前)] というフィルターを使用できます。
7. リストに表示する列を編集します。
8. [作成] をクリックします。
   新しいリストが表示されます。
9. または、[独自に作成 **(Create your own)]** をクリックし、名前を入力してから [ソースを選択 **(Select Source)]** をクリックします。
10. フィールドに入力し、新しいリストに表示されるソースから選択します。
11. [作成] をクリックします。
    新しいリストが表示されます。

    > **注:**
    > リストモジュールを終了すると、終了時に表示されるリストが、戻ったときに表示されるリストとなります。

12. リストを削除するには、リストを表示した状態で、ページの右上にある歯車アイコンをクリックします。

で修復タスクを手動で作成する **Vulnerability Manager** ワークスペース

脆弱性対応 の v25.0.4 以降、Vulnerability Manager ワークスペース の [リスト] ページにあるホスト脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、および構成テスト結果のリストから修復タスクを手動で作成できます。ホームページの可視化をクリックしたときに表示されるドリルダウンリストから修復タスクを作成することもできます。

始める前に
必要なロール：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.write_all、sn_vul.vulnerability_analyst、または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合は sn_vul.app_write_all または sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.write_all、sn_vul_container.vulnerability_analyst、または sn_vul_container.vulnerability_admin
- 構成テスト結果 (TR) の場合は sn_vulc.write または sn_vulc.admin

このタスクについて

Vulnerability Manager ワークスペース で修復タスク (RT) を手動で作成すると、レコード (VIT、CVIT、AVIT、TR) をリアルタイムで動的に修復タスクにグループ化できるため、修復タスク管理をきめ細かく制御できます。

次の場合は、修復タスクを手動で作成できます。

- 修復タスクルール基準以外の基準で脆弱性一致アイテムをグループ化します。たとえば、特定のマネージャーに対して、またはさまざまな脆弱性を含むランサムウェアなどのアクティブな新しいエクスプロイトに対して修復タスクを作成できます。
- グループ化されていないレコードをグループ化します。
- 修復タスクルールが非アクティブです。

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース > リスト.
2. [リスト] ページで、次のいずれかのリストから [アクティブ] または [すべて] リストを開きます。
   - ホスト脆弱性一致アイテム
   - アプリケーション脆弱性一致アイテム
   - コンテナ脆弱性一致アイテム
   - 構成テスト結果
3. オプション: 更新するレコードのチェックボックスをオンにし、[修復タスクの作成] モーダルの [レコード選択] フィールドで [選択したアイテム] オプションを選択します。
4. [修復タスクの作成] を選択します。
5. [修復タスクを作成] モーダルで、次の詳細を入力します。

修復タスクの作成モーダル

フィールド	説明
レコード選択	○ 選択したアイテム:選択したレコードのみを更新します。 ○ すべてのアイテム:リスト内のすべてのレコードを更新します。
簡単な説明	修復タスクに関する簡単なメモ。
グループ化クライテリア	選択肢は次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ アサイン先グループ:同じアサイン先グループを持つレコードは、1 つの修復タスクにグループ化されます。 ○ アサイン先グループと構成アイテム:同じアサイン先グループと構成アイテムを持つレコードは、1 つの修復タスクにグループ化されます。 ○ アサイン先グループと脆弱性:同じアサイン先グループと脆弱性を持つレコードは、1 つの修復タスクにグループ化されます。 ○ アサイン先グループとリスク評価:同じアサイン先グループとリスク評価を持つレコードは、1 つの修復タスクにグループ化されます。
他の修復タスクのレコードの管理	選択肢は次のとおりです。 ○ 新しい修復タスクのレコードをスキップ:他の修復タスクの一部であるレコードに対してアクションは実行されません。 ○ 新しい修復タスクに移動:他の修復タスクの一部であるレコードが新しい修復タスクに転送されます。 ○ 現在の修復タスクと新しい修復タスクの両方に保持:他の修復タスクの一部であるレコードは、古い修復タスクと新しい修復タスクの両方に保持されます。

6. **[Create remediation task** (修復タスクの作成)] を選択します。

タスクの結果
修復タスクは、グループ化基準に基づいて作成されます。アサイン先グループの修復オーナーにメール通知が送信され、修復タスクが作成されてグループにアサインされたことが通知されます。グループ化基準に基づいて修復タスクを作成する方法の例については、「 での修復タスク作成の例 Vulnerability Manager ワークスペース および IT 修復ワークスペース」を参照してください。

Qualys テストグループのテスト結果のインポートを有効または無効にする

脆弱性対応 の v23.0 以降では、テストグループのレコードビューにある [インポートの有効化/無効化 **(Enable/Disable import)]** ボタンを使用して、Qualys テストグループ内のテストのテスト結果のインポートを制御します。

始める前に
必要なロール：sn_vulc.admin

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース > **Lists** (リスト).
2. [ライブラリ] の [テストグループ] リストで、レコードビューで Qualys テストグループを開きます。
3. [インポートを無効にする **(Disable import)]** ボタンを選択して、Qualys テストグループに関連付けられたテスト結果のインポートを無効にします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

今後のデータの取り込みでは、Qualys テストグループのテスト結果はインポートされません。[インポートが無効である **(Is Import disabled)]** フィールドの値が *True* に変わります。

4. オプション: [インポートを有効にする **(Enable import)]** ボタンを選択して、テスト結果のインポートを有効にします。

Vulnerability Manager ワークスペース で要求を承認または却下

修復オーナーから送信された要求を承認または却下します。

始める前に
必要なロール：

各種の承認要求に必要な承認者ロール

承認タイプ	必要な承認レベル	承認者ロール	追加情報
誤検出の承認	1 つ	• 脆弱性一致アイテム (VIT) の sn_vul.false_positive_approver 詳細なロール。 • アプリケーション脆弱性一致アイテム (AVIT) の場合、「sn_vul.app_false_positive_approver」ロール • コンテナ脆弱性一致アイテム (CVIT) の場合、「sn_vul_container.false_positive_approver」ロール • 構成テスト結果の場合、「sn_vulc.false_positive_approver」 または 承認者は、誤検出承認者ユーザーグループに属している必要があります。	-
例外承認 (保留)	2	• 承認者 - レベル 1 グループには 1 人の承認者が必要です • 承認者 - レベル 2 グループには 1 人の承認者が必要です	レコードまたは修復タスクの例外要求は、デフォルトの 2 レベルの承認フローを使用して承認されます。例外要求には 2 つのレベルの承認者が必要です。要求はレベル 1 の承認者によって承認されると、レベル 2 の承認者に送信され、承認者 2

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

各種の承認要求に必要な承認者ロール (続く)

承認タイプ	必要な承認レベル	承認者ロール	追加情報
			のキューに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

各種の承認要求に必要な承認者ロール (続く)

承認タイプ	必要な承認レベル	承認者ロール	追加情報
承認をアサイン解除する	承認者 - レベル 1 グループには 1 人の承認者が必要です	• AVIT および VIT の sn_vul.unassign_appr • CVIT の sn_vul_container.unas • 構成の問題 (CI) の sn_vulc.unassign_app	**注:** デフォルトでは、承認構成が提供され、アサイン解除承認グループが作成されます。このグループのユーザー (アサイン解除承認者 - レベル 1) が要求を承認できます。デフォルトでは、このグループにはアサイン解除承認者ロール sn_vul.unassign_approver が含まれています。新しいグループを変更または作成し、承認構成を更新できます。承認ルールを構成するには、それぞれの承認ルールモジュールに移動し、次のいずれかの承認ルールを選択して、[承認構成] タブの承認構成に移動します。 • 脆弱性一致アイテム用の *Vulnerable item field change request*。 • 修復タスク用の *Vulnerability field change request*。 • アプリケーション脆弱性一致アイテム (AVIT) 用の *Application vulnerability field change request*。 • コンテナ脆弱性一致アイテム (CVIT) 用

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

各種の承認要求に必要な承認者ロール (続く)

承認タイプ	必要な承認レベル	承認者ロール	追加情報
リスク削減の承認	2	• 承認者 - レベル 1 グループには 1 人の承認者が必要です • 承認者 - レベル 2 グループには 1 人の承認者が必要です	リスク削減の承認フローは、例外承認 (保留) と同じです。

ペルソナロールのユーザーへのアサインおよびユーザーのグループへのアサインの詳細については、「脆弱性対応 のペルソナと詳細なロール」および「セットアップアシスタントを使用した 脆弱性対応 ペルソナロールのアサイン」を参照してください。

注:
承認要求を送信する前に、ユーザーを承認グループに追加します。承認グループにユーザーを追加する前に要求を作成すると、承認権限を持つユーザーに対して要求が表示されないことがあります。

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース.
   承認者がワークスペースへのアクセス権を持っていない場合は、次の URL で承認を処理できます 脆弱性対応 > 自分の承認 クラシック環境で
2. [リストビュー] アイコン ( ) を選択します。
   [リスト] ページが表示されます。
3. [承認] フィルター済みリストで、[自分にアサイン済み] を選択します。
4. 処理する要求を見つけて、 [ステータス] 列のリンクを選択します。
   脆弱性ステータス変更承認レコード (VCA#) が表示されます。
5. 要求を承認または却下するには、次のいずれかのオプションを選択します。

脆弱性対応 ワークスペースでのメール通知の設定

修復オーナーユーザーグループのユーザーに送信される自動メールリマインダーのユーザーを特定します。

始める前に

必要なロール：admin

この機能では、修復オーナーユーザーグループのユーザー用のメールダイジェストが自動的に生成されます。「脆弱性対応ワークスペースでのメールダイジェストの使用」の説明に従って、メール通知を受信するユーザーを追加します。

ユーザーレコードにアクティブなメールアドレスが入力されていること、およびそれが修復オーナーユーザーグループに追加されていることを確認します。

メールの配信の頻度、日付、または時刻を変更する場合、あるいは機能を非アクティブ化する場合は、次の手順を実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > スケジュール済みジョブ.
2. [修正ダイジェストを生成 **(Generate remediation digest)]** を見つけてクリックし、レコードを開きます。

   通知が送信されることを確認するまで、フィールドはデフォルト設定のままにしておくことをお勧めします。デフォルトでは、メールは、ジョブを実行しているインスタンスのタイムゾーンの毎週月曜日午前 9 時に送信されます。
3. フォームのフィールドを変更します。
   フォームフィールドの詳細については、「[修正ダイジェストを生成 (Generate remediation digest)] フォームのフィールド」を参照してください。
4. [更新] をクリックします。

次のタスク
以前にリストしたすべての情報が正しいことを確認し、修復オーナーユーザーグループにユーザーがいるのにメールが想定どおりに送信されない場合は、メール通知を受信するためのチャネルがアクティブ化されていることを確認します。「Create notification channels」を参照してください。

Vulnerability Manager ワークスペースでの脆弱性一致アイテムとテスト結果の修正

Vulnerability Manager ワークスペースでは、条件を定義して脆弱性一致アイテムとテスト結果を監視トピックに修復し、修復作業を作成することで修復の進捗状況を追跡できます。

Vulnerability Manager ワークスペース での一括編集の使用

Vulnerability Manager ワークスペース では、レコードのステータスを更新し、例外や誤検出を要求し、一括編集機能でレコードをアサイン先グループの複数の脆弱性一致アイテム (VIT、AVIT、CVIT) に同時にアサインすることができます。

一括編集機能は、次に対して有効です。

- 脆弱性対応 v21.0 以降のホスト脆弱性一致アイテム (VIT)。
- 脆弱性対応 v22.0 以降のアプリケーション脆弱性一致アイテム (AVIT) およびコンテナ脆弱性一致アイテム (CVIT)。
- 脆弱性対応 v23.0 以降のテスト結果。

Vulnerability Manager ワークスペース でレコードのステータスを一括更新

Vulnerability Manager ワークスペース の一括編集機能で、修正の進捗状況に応じて複数のレコード (VIT、AVIT、CVIT) のステータスを同時に更新します。

始める前に
必要なロール：

- ホスト脆弱性一致アイテムの場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin for host vulnerable items
- アプリケーション脆弱性一致アイテムの場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテムの場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース > リスト.
2. [リスト] ページより、次のいずれかのリストで [アクティブ] または [すべて] リストを開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- ホスト脆弱性一致アイテム
- コンテナ脆弱性一致アイテム
- アプリケーション脆弱性一致アイテム

3. 次のいずれかを実行します。
   - [レコード選択] フィールドで [選択されているアイテムのみ **(Only Selected Items)**] オプションを使用する場合は、各アイテムの横にあるチェックボックスをオンにします。
   - [レコード選択 **(Record Selection)**] フィールドの [フィルターと一致するすべての脆弱性一致アイテム **(All vulnerable items that match filter)**] オプションを使用する場合は、フィルターを適用します。
4. [一括編集] ボタンを選択します。
5. [一括編集] モーダルで、次のフィールドに入力してレコードのステータスを更新します。

[一括編集] モーダルのフィールド

フィールド	説明
レコード選択	更新するレコード。選択肢は次のとおりです。 ○ 選択したアイテムのみ：チェックボックスで選択したレコードを更新する場合は、このオプションを選択します。 ○ フィルターに一致するすべての脆弱性一致アイテム：フィルタリングされたレコードを更新する場合は、このオプションを選択します。 ○ 修復タスク：修復タスクのレコードを更新して、[修復タスク] フィールドで目的の修復タスクを選択する場合は、このオプションを選択します。 ○ 脆弱性エントリー：脆弱性エントリー (CVE) 固有のレコードを更新して、[脆弱性エントリー] フィールドで [CVE] を選択する場合は、このオプションを選択します。 **注:** 無効な CI または CI 廃止を含むレコードは更新されません。
ステータス	レコード内の ステータス の変更です。選択肢は次のとおりです。 ○ 更新しない ○ オープン ○ 調査中 ○ 実装待ち ○ 保留 詳しくは、「脆弱性マネージャーワークスペースでの一括例外の要求」を参照してください。 ○ クローズ済み 詳細については、「脆弱性マネージャーワークスペースで誤検出を一括編集」を参照してください。 ○ 解決済み

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: ステータス移行が有効なレコードのみ更新されます。
作業メモ	変更を説明するために入力するテキスト。

6. [編集] を選択します。

一括編集の非同期ジョブにより、選択したレコードが更新されます。

パッチやソリューションによるホスト脆弱性一致アイテムの一括編集

Vulnerability Manager ワークスペース の一括編集機能で複数のホスト脆弱性一致アイテムを同時に処理できるパッチやソリューションを推奨します。

始める前に
必要なロール：sn_vul.vulnerability_analyst、sn_vul.vulnerability_admin、および sn_vul.bulk_edit granular role の詳細なロールを含むロール。

このタスクについて
一括編集モーダルでは、推奨のソリューションやパッチを追加できるだけでなく、アサイン先グループに対するホスト脆弱性一致アイテム (VIT) のアサイン解除やアサインを複数同時に実行することもできます。

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース.

   注:
   選択するレコードのステータスは、[オープン]、[調査中]、[実装待ち] である必要があります。

2. [リスト] ページの [ホスト脆弱性一致アイテム] で、[アクティブ] または [すべて] のリストを開きます。
3. 次のいずれかを実行します。
   - [レコード選択] フィールドで [選択されているアイテムのみ **(Only Selected Items)]** オプションを使用する場合は、各アイテムの横にあるチェックボックスをオンにします。
   - [レコード選択 **(Record Selection)]** フィールドの [フィルターと一致するすべての脆弱性一致アイテム **(All vulnerable items that match filter)]** オプションを使用する場合は、フィルターを適用します。
   - 一括編集モーダルの [レコード選択 (Record Selection)] フィールドで [選択されているアイテムのみ **(Only Selected Items)]** オプションを使用する場合は、各アイテムの横にあるチェックボックスをオンにします。
   - 一括編集モーダルの [レコード選択 (Record Selection)] フィールドで [フィルターと一致するすべての脆弱性一致アイテム **(All vulnerable items that match filter)]** オプションを使用する場合は、フィルターを適用します。
4. [一括編集] ボタンを選択します。
5. 一括編集モーダルのフィールドを入力して、複数のホスト脆弱性一致アイテムに対するパッチやソリューションを推奨します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[一括編集] モーダルのフィールド

フィールド	説明
レコード選択	更新するレコード。選択肢は次のとおりです。 ○ 選択したアイテムのみ：チェックボックスで選択したレコードを更新する場合は、このオプションを選択します。 ○ フィルターに一致するすべての脆弱性一致アイテム：フィルタリングされたレコードを更新する場合は、このオプションを選択します。 ○ 修復タスク：修復タスクのレコードを更新して、[修復タスク] フィールドで目的の修復タスクを選択する場合は、このオプションを選択します。 ○ 脆弱性エントリー：脆弱性エントリー (CVE) 固有のレコードを更新して、[脆弱性エントリー] フィールドで [CVE] を選択する場合は、このオプションを選択します。 **注:** ○ 無効な CI または CI 廃止を含むレコードは更新されません。 ○ ステータスが [オープン]、[調査中]、[実装待ち] のレコード (VIT) のみが更新されます。
状態	ホスト脆弱性一致アイテムのステータスの変化。推奨のソリューションやパッチを追加できるのは、次のステータスを選択した場合のみです。 ○ 更新しない ○ オープン ○ 調査中 ○ 実装待ち
優先ソリューション	一括編集用に選択したすべての脆弱性一致アイテムの修正を対象としたソリューション。脆弱性一致アイテムの [優先ソリューション] フィールドに対する変更を選択します。選択した VIT で利用可能な優先ソリューションのルックアップリストからの選択肢があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: ○ 利用可能な優先ソリューションのセットは、選択したすべての VIT と、脆弱性のすべての見込みのある解決策との共通部分です。 ○ 選択時 レコード選択 > 脆弱性エントリー 一括編集の場合、脆弱性のすべての VIT が選択した優先ソリューションに設定されます。 **注:** この操作では脆弱性エントリーレベルで優先ソリューションが設定されません。脆弱性エントリレベルで優先ソリューションを設定すると、以降すべての新しい VIT に対して優先ソリューションが設定されます。一括編集では、現在の VIT セットのみが変更されます。 ○ 選択基準全体での個別の脆弱性は 500 に制限されています。500 を超える個別の脆弱性がある場合は、[優先ソリューション] の設定基準が異なる VIT を選択するように求める警告メッセージが表示されます。 ○ ルックアップリストに表示できるソリューションの合計数は 170 に制限されています。170 を超えるソリューションがある場合は、警告メッセージが表示されます。 更新された値は、脆弱性一致アイテムリストビューに表示されます。
優先パッチ	一括編集用に選択したすべての脆弱性一致アイテムの修正を対象としたパッチ。 **注:** ○ 優先パッチのリストを表示するには、パッチオーケストレーションをインストールする必要があります。 ○ 利用可能な優先パッチのセットは、選択したすべての VIT と、すべての見込みのあるパッチとの共通部分です。 ○ 選択基準全体での個別の脆弱性は 500 に制限されています。500 を超える個別の脆弱性がある場合は、[優先パッチ] の設定基準が異なる VIT を選択するように求める警告メッセージが表示されます。 ○ ルックアップリストに表示できるパッチの合計数は 170 に制限されています。170 を超えるパッチがある場合は、警告メッセージが表示されます。
アサイン解除	アサイン先グループおよび修復オーナーに対して選択したすべてのアイテムのアサインが解除されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: ○ このフィールドは、[ステータス] で [更新しない] を選択すると表示されます。 ○ レコードをアサイン解除すると、修復タスクが作成され、承認のために送信されます。詳細については、「ホスト脆弱性一致アイテムのアサインを一括解除する」を参照してください。
アサイン先グループ	レコードのアサイン先グループ。すべてのアクティブなアサイン先グループがこのフィールドに表示されます。 注: [アサイン解除] チェックボックスをオンにすると、このフィールドは非アクティブ化されます。
作業メモ	変更を説明するために入力するテキスト。

6. [編集] を選択します。

タスクの結果
一括編集の非同期ジョブにより、選択したホスト脆弱性一致アイテム (VIT) が更新されます。優先ソリューションとパッチが、関連するホスト脆弱性一致アイテム (VIT) に追加されます。ホスト脆弱性一致アイテムを開き、[詳細] タブの [修復] セクションで優先ソリューションとパッチを表示します。

レコードをアサイン先グループに一括アサイン

Vulnerability Manager ワークスペース の一括編集機能を使用して、複数のレコード (VIT、AVIT、CVIT、TR) をアサイン先グループに同時にアサインします。

始める前に
必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

手順
1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース > リスト.
2. [リスト] ページより、次のいずれかのリストで [アクティブ] または [すべて] リストを開きます。
   - ホスト脆弱性一致アイテム
   - コンテナ脆弱性一致アイテム
   - アプリケーション脆弱性一致アイテム
   - 構成テスト結果
3. 次のいずれかを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [レコード選択] フィールドで [選択されているアイテムのみ **(Only Selected Items)**] オプションを使用する場合は、各アイテムの横にあるチェックボックスをオンにします。
- [レコード選択] フィールドの [フィルターに一致するすべてのレコード] オプションを使用する場合は、フィルターを適用します。

4. [一括編集] ボタンを選択します。
5. フォームのフィールドに入力して、レコードをアサイン先グループにアサインします。

[一括編集] モーダルのフィールド

フィールド	説明
レコード選択	更新するレコード。選択肢は次のとおりです。 - 選択したアイテムのみ：チェックボックスで選択したレコードを更新する場合は、このオプションを選択します。 - フィルターに一致するすべてのレコード：フィルタリングされたレコードを更新する場合は、このオプションを選択します。 - 修復タスク：修復タスクのレコードを更新して、[修復タスク] フィールドで目的の修復タスクを選択する場合は、このオプションを選択します。 - 脆弱性エントリー：脆弱性固有のレコードを更新して、[脆弱性エントリー] フィールドで [CVE] または [TPE] を選択する場合は、このオプションを選択します。 **注:** このフィールドは、ホスト脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテムに対して表示されます。 - 構成テスト：テスト固有のテスト結果を更新して、[構成テスト] フィールドでテストを選択する場合は、このオプションを選択します。 **注:** このオプションは、構成テスト結果に対してのみ表示されます。 **注:** - 無効な CI または CI 廃止を含むレコードは更新されません。 - ステータスが [オープン]、[調査中]、[実装待ち]、[保留] のレコードのみが更新されます。
アサイン先グループ	レコードのアサイン先グループ。すべてのアクティブなアサイン先グループがこのフィールドに表示されます。 **注:** VIT の [アサイン解除] チェックボックスをオンにすると、このフィールドは非アクティブ化されます。
作業メモ	変更を説明するために入力するテキスト。

6. [編集] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスクの結果
アサイン先グループを更新したレコードを開いて [概要] タブに移動すると、レコードがアサインされているユーザーグループが [アサイン先グループ] フィールドに表示されます。

ホスト脆弱性一致アイテムのアサインを一括解除する

レコードが修復範囲外であると判断した場合、またはレコードが自分や自分のグループに誤ってアサインされていると思われる場合、ホスト脆弱性一致アイテム (VIT) や修復タスク (VUL) の [アサイン先] および [アサイン先グループ] のフィールドから自分または自分のグループを削除できます。

始める前に
必要なロール：sn_vul.vulnerability_analyst、sn_vul.vulnerability_admin

このタスクについて
[アサイン解除] 機能は、[クローズ済み] または [解決済み] を除くすべてのステータスのレコードに適用されます。一括編集機能でホスト脆弱性一致アイテムのアサインを解除すると、関連するレコードのみが更新されます。

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース.
2. [リスト] ページの [ホスト脆弱性一致アイテム] で、[アクティブ] または [すべて] のリストを開きます。
3. 次のいずれかを実行します。
   - [レコード選択] フィールドで [選択されているアイテムのみ **(Only Selected Items)]** オプションを使用する場合は、各アイテムの横にあるチェックボックスをオンにします。
   - [レコード選択 (Record Selection)] フィールドの [フィルターと一致するすべての脆弱性一致アイテム **(All vulnerable items that match filter)]** オプションを使用する場合は、フィルターを適用します。
4. [一括編集] ボタンを選択します。
5. フォームのフィールドに入力して、アサインを一括解除します。

[一括編集] モーダルのフィールド

フィールド	説明
レコード選択	更新するレコード。選択肢は次のとおりです。 ○ 選択したアイテムのみ：チェックボックスで選択したレコードを更新する場合は、このオプションを選択します。 ○ フィルターに一致するすべての脆弱性一致アイテム：フィルタリングされたレコードを更新する場合は、このオプションを選択します。 ○ 修復タスク：修復タスクのレコードを更新して、[修復タスク] フィールドで目的の修復タスクを選択する場合は、このオプションを選択します。 ○ 脆弱性エントリー：脆弱性エントリー (CVE) 固有のレコードを更新して、[脆弱性エントリー] フィールドで [CVE] を選択する場合は、このオプションを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: ○ 無効な CI または CI 廃止を含むレコードは更新されません。 ○ ステータスが [オープン]、[調査中]、[実装待ち]、[保留] のレコードのみが更新されます。
状態	ステータスを [更新しない] にします。
アサイン解除	選択した脆弱性一致アイテムはすべて、アサイン先グループおよび修復オーナーにおいてアサインが解除されます。 注: ○ このフィールドは、[ステータス] で [更新しない] を選択すると表示されます。 ○ レコードをアサイン解除すると、修復タスクが作成され、承認のために送信されます。
作業メモ	変更を説明するために入力するテキスト。

6. [編集] をクリックします。
   選択したホスト脆弱性一致アイテム (VIT) で修復タスクが作成されます。

   承認要求が送信され、承認者は承認要求のメール通知を受け取ります。

   ホスト脆弱性一致アイテム (VIT) と修復タスク (VUL) のステータスが [レビュー中] に移行します。修復タスクがこの機能で更新されると、関連するすべての VIT の [アサイン先] フィールドと [アサイン先グループ] フィールドも、要求の承認時にクリアされます。

タスクの結果

脆弱性マネージャーワークスペースのリストページで、次に移動します: 例外要求 > **All** (すべて) をクリックし、対応するステータス変更承認レコード (VCA#) を開き、[承認ステータス] 列で要求のステータスを確認します。

承認ステータス	結果
承認済み	すべてのホスト脆弱性一致アイテムにおいて [アサイン先] および [アサイン先グループ] フィールドがクリアされます。
却下	すべてのホスト脆弱性一致アイテムにおいて [アサイン先] および [アサイン先グループ] フィールドが更新されません。

レコードや修正タスクのアクティビティストリームでは、要求のワークフロー全体を表示できます。

脆弱性マネージャーワークスペースでの一括例外の要求

複数のレコード (VIT、AVIT、CVIT、TR) の例外を要求する際、手動で各レコードを選択するのではなく、一括編集機能で同時に行います。

始める前に

必要なロール：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

このタスクについて
一括編集モーダルから複数のレコードの例外を要求すると、選択したレコードで修復タスクが作成されます。

注:
[ServiceNow での例外の管理] パラメーターが [false] に設定されているスキャナーのアプリケーション脆弱性一致アイテム (AVIT) は更新されません。

- さまざまなスキャナーの AVIT を選択したときに、**[ServiceNow** での例外の管理] パラメーターの設定が [true] と [false] で混在している場合、**[ServiceNow** での例外の管理] パラメーターが [false] のスキャナーにリンクされている AVIT は更新されません。
- 選択した **AVIT** において、**[ServiceNow** での例外の管理] パラメーターが [false] のスキャナーとしかリンクしていない場合、[一括編集] モーダルの [ステータス] フィールドに [保留] オプションが表示されません。

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース.
2. [リスト] ページより、次のいずれかのリストで [アクティブ] または [すべて] リストを開きます。
   - ホスト脆弱性一致アイテム
   - コンテナ脆弱性一致アイテム
   - アプリケーション脆弱性一致アイテム
   - 構成テスト結果
3. 次のいずれかを実行します。
   - [レコード選択] フィールドで [選択されているアイテムのみ *(Only Selected Items)*] オプションを使用する場合は、各アイテムの横にあるチェックボックスをオンにします。
   - [レコード選択] フィールドの [フィルターに一致するすべてのレコード] オプションを使用する場合は、フィルターを適用します。
4. [一括編集] ボタンを選択します。
5. フォームより、次のフィールドに入力して、複数のレコード (VIT、AVIT、CVIT、TR) の例外を同時に要求します。

[一括編集] モーダルのフィールド

フィールド	説明
レコード選択	更新するレコード。選択肢は次のとおりです。 ○ 選択したアイテムのみ：チェックボックスで選択したレコードを更新する場合は、このオプションを選択します。 ○ フィルターに一致するすべてのレコード：フィルタリングされたレコードを更新する場合は、このオプションを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ 修復タスク：修復タスクのレコードを更新して、[修復タスク] フィールドで目的の修復タスクを選択する場合は、このオプションを選択します。 ○ 脆弱性エントリー：脆弱性 固有のレコードを更新して、[脆弱性エントリー] フィールドで [CVE] または [TPE] を選択する場合は、このオプションを選択します。 **注:** このフィールドは、ホスト脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテムに対して表示されます。 ○ 構成テスト：テスト固有のテスト結果を更新して、[構成テスト] フィールドでテストを選択する場合は、このオプションを選択します。 **注:** このオプションは、構成テスト結果に対してのみ表示されます。 **注:** ○ 無効な CI または CI 廃止を含むレコードは更新されません。 ○ ステータスが [オープン]、[調査中]、[実装待ち] のレコードのみが更新されます。
状態	選択したレコードの例外を要求するには、 [保留] ステータスを選択します。 **注:** ○ このオプションを選択すると、[理由]、[簡単な説明]、[期限]、[補足情報] フィールドが表示されます。 ○ レコードを保留すると、修復タスクが作成され、このタスクが承認のために送信されます。
理由	レコードを保留する理由： ○ メンテナンス期間待ち ○ 修正が利用不可 ○ リスクの受容 ○ コントロールの緩和を実施 ○ その他 **注:** [ステータス] で [保留] を選択すると、[理由] フィールドが表示されます。
簡単な説明	保留要求の理由を説明する簡単なメモ。この情報は、保留要求に対して作成された修復タスクの [説明] フィールドに反映されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: このフィールドは、[ステータス] で [保留] および [クローズ済み - 誤検出 (Closed-False positive)] を選択すると表示されます。
期限	レコードの保留状態が終了する日付。 注: このフィールドは、[ステータス] で [保留] を選択すると表示されます。
追加情報	その他の必要な情報。この情報は、保留要求およびクローズ済み誤検出要求に対して作成された修復タスクの [概要] タブにある [補足情報] フィールドに反映されます。保留要求が承認されると、この追加情報が VIT と修復タスクの両方の保留メモとして表示されます。 注: このフィールドは、[ステータス] で [保留] および [クローズ済み - 誤検出 (Closed-False positive)] を選択すると表示されます。
作業メモ	変更を説明するために入力するテキスト。

6. [編集] をクリックします。
7. [アンケートに回答] モーダルで、質問に回答し、[送信] をクリックします。

   選択したレコードを含む修復タスクが作成されます。承認要求が送信され、レコードのステータスが [レビュー中] に変わります。

   注:
   [アンケートに回答] モーダルは、例外管理フォームの例外要求においてアンケートが有効化されている場合にのみ表示されます。例外要求のアンケートの構成の詳細については、「脆弱性対応 の例外管理の設定」、「アプリケーション脆弱性対応 の例外管理の設定」、「コンテナ脆弱性対応 の例外管理の設定」、および「コンフィグレーションコンプライアンスの例外管理の概要」を参照してください。

   承認者は、承認要求のメール通知を受け取ります。

タスクの結果

脆弱性マネージャーワークスペースのリストページで、次に移動します: 例外 > **All** (すべて)で、対応するステータス変更承認レコード (VCA#) を開き、[承認ステータス] 列で要求のステータスを確認します。

承認ステータス	結果
承認済み	修復タスクのステータスが [保留] に移行し、示される [理由] がサブステートになります。ステータスや理由はレコードにロールダウンされます。
却下	修復タスクやレコードのステータスは変更されません。

レコードや修正タスクのアクティビティストリームでは、要求のワークフロー全体を表示できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脆弱性マネージャーワークスペースで誤検出を一括編集

各アイテムを手動で選択するのではなく、脆弱性マネージャーワークスペースの一括編集機能で複数のレコード (VIT、AVIT、CVIT、TR) を同時に誤検出としてマークします。

始める前に

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

このタスクについて

一括編集モーダルで 1 つ以上のレコードの誤検出を要求すると、選択したレコードにおいて修復タスクが作成されます。

注:
一括編集機能でアプリケーション脆弱性一致アイテム (AVIT) の誤検出を要求した場合、**[ServiceNow** で誤検出を管理する] パラメーターが [false] のスキャナーからの AVIT は更新されません。

- さまざまなスキャナーからの AVIT を選択したときに、**[ServiceNow** で誤検出を管理する] パラメーターの設定が [true] と [false] で混在している場合、**[ServiceNow** で誤検出を管理する] パラメーターが [false] のスキャナーにリンクされている AVIT は更新されません。
- **[ServiceNow** で誤検出を管理する] パラメーターが [false] のスキャナーからのみ AVIT を選択した場合、[一括編集] モーダルの [理由] フィールドに [誤検出] オプションは表示されません。

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース > リスト.

   注:
   選択するレコードのステータスは、[オープン]、[調査中]、[実装待ち] である必要があります。

2. [リスト] ページで、次のいずれかのリストから [アクティブ] または [すべて] のリストを開きます。
   - ホスト脆弱性一致アイテム
   - コンテナ脆弱性一致アイテム
   - アプリケーション脆弱性一致アイテム
   - 構成テスト結果
3. 次のいずれかを実行します。
   - [レコード選択] フィールドで [選択されているアイテムのみ *(Only Selected Items)]* オプションを使用する場合は、各アイテムの横にあるチェックボックスをオンにします。
   - [レコード選択] フィールドの [フィルターに一致するすべてのレコード] オプションを使用する場合は、フィルターを適用します。
4. [一括編集] ボタンを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. フォームのフィールドに入力して、複数のレコードの誤検出を要求します。

[一括編集] モーダルのフィールド

フィールド	説明
レコード選択	更新するレコード。選択肢は次のとおりです。 ○ 選択したアイテムのみ：チェックボックスで選択したレコードを更新する場合は、このオプションを選択します。 ○ フィルターに一致するすべてのレコード：フィルタリングされたレコードを更新する場合は、このオプションを選択します。 ○ 修復タスク：修復タスクのレコードを更新して、[修復タスク] フィールドで目的の修復タスクを選択する場合は、このオプションを選択します。 ○ 脆弱性エントリー：脆弱性 固有のレコードを更新して、[脆弱性エントリー] フィールドで [CVE] または [TPE] を選択する場合は、このオプションを選択します。 **注:** このフィールドは、ホスト脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテムに対して表示されます。 ○ 構成テスト：テスト固有のテスト結果を更新して、[構成テスト] フィールドでテストを選択する場合は、このオプションを選択します。 **注:** このオプションは、構成テスト結果に対してのみ表示されます。 **注:** ○ 無効な CI または CI 廃止を含むレコードは更新されません。 ○ ステータスが [オープン]、[調査中]、[実装待ち] のレコードのみが更新されます。
状態	[クローズ済み] ステータスを選択します。
理由	[理由] で [誤検出] を選択します。 **注:** ○ このオプションを選択すると、[簡単な説明] および [補足情報] フィールドが表示されます。 ○ レコードを誤検出としてマークすると、修復タスクが作成され、このタスクが承認のために送信されます。 **注:** [理由] フィールドは、[ステータス] で [保留] または [クローズ済み] を選択すると表示されます。
簡単な説明	クローズ済み誤検出要求の理由を説明する簡単なメモ。この情報は、クローズ済み誤検出要求に対して作成された修復タスクの [説明] フィールドに反映されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: このフィールドは、[ステータス] で [保留] や [クローズ済み誤検出] を選択すると表示されます。
追加情報	その他の必要な情報。この情報は、クローズ済み誤検出要求に対して作成された修復タスクの [概要] タブにある [補足情報] フィールドに反映されます。誤検出要求が承認されると、この追加情報が VIT と修復タスクの両方のメモとして表示されます。 注: このフィールドは、[ステータス] で [保留] や [クローズ済み誤検出] を選択すると表示されます。
作業メモ	変更を説明するために入力するテキスト。

6. [編集] をクリックします。
7. [アンケートに回答] モーダルで、質問に回答し、[送信] を選択します。
   選択したレコードを含む修復タスクが作成されます。承認要求が送信され、修復タスクのステータスが [レビュー中] に変わります。

   注:
   [アンケートに回答] モーダルは、例外管理フォームの誤検出要求においてアンケートが有効化されている場合にのみ表示されます。誤検出要求のアンケートの構成について、詳細は「脆弱性対応 の例外管理の設定」「アプリケーション脆弱性対応 の例外管理の設定」「コンテナ脆弱性対応 の例外管理の設定」を参照してください。

   承認者は、承認要求のメール通知を受け取ります。

タスクの結果

脆弱性マネージャーワークスペースのリストページで、次に移動します: 例外 > **All** (すべて)で、対応するステータス変更承認レコード (VCA#) を開き、[承認ステータス] 列で要求のステータスを確認します。

承認ステータス	結果
承認済み	修復タスクのステータスが [クローズ済み] に移行し、[理由] が [誤検出] になります。ステータスや理由はレコードにロールダウンされます。
却下	修復タスクやレコードのステータスは変更されません。

レコードや修正タスクのアクティビティストリームでは、要求のワークフロー全体を表示できます。

Vulnerability Manager ワークスペース でレコードを一括クローズ

Vulnerability Manager ワークスペース の一括編集機能を使用して、複数のレコード (VIT、AVIT、CVIT) を同時にクローズします。

始める前に

必要なロール：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーワークスペース > リスト.
2. [リスト] ページで、次のいずれかのリストから [アクティブ] または [すべて] のリストを開きます。
   - ホスト脆弱性一致アイテム
   - コンテナ脆弱性一致アイテム
   - アプリケーション脆弱性一致アイテム
3. 次のいずれかを実行します。
   - [レコード選択] フィールドで [選択されているアイテムのみ (Only Selected Items)] オプションを使用する場合は、各アイテムの横にあるチェックボックスをオンにします。
   - [レコード選択 **(Record Selection)]** フィールドの [フィルターと一致するすべての脆弱性一致アイテム (All vulnerable items that match filter)] オプションを使用する場合は、フィルターを適用します。
4. [一括編集] ボタンを選択します。
5. フォームのフィールドに入力して、選択したレコードをクローズします。

[一括編集] モーダルのフィールド

フィールド	説明
レコード選択	更新するレコード。選択肢は次のとおりです。 ○ 選択したアイテムのみ：チェックボックスで選択したレコードを更新する場合は、このオプションを選択します。 ○ フィルターに一致するすべての脆弱性一致アイテム：フィルタリングされたレコードを更新する場合は、このオプションを選択します。 ○ 修復タスク：修復タスクのレコードを更新して、[修復タスク] フィールドで目的の修復タスクを選択する場合は、このオプションを選択します。 ○ 脆弱性エントリー：脆弱性エントリー (CVE) 固有のレコードを更新して、[脆弱性エントリー] フィールドで [CVE] を選択する場合は、このオプションを選択します。 **注:** ○ 無効な CI または CI 廃止を含むレコードは更新されません。 ○ ステータスが [オープン]、[調査中]、[実装待ち] のレコードのみが更新されます。
状態	ステータスとして [クローズ済み] を選択します。
理由	レコードをクローズする理由：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ 誤検出 注: このオプションを選択してレコードを誤検出としてマークすると、[理由]、[簡単な説明]、[補足情報] フィールドが表示されます。誤検出の一括編集について、詳細は「脆弱性マネージャーワークスペースで誤検出を一括編集」を参照してください。 ○ キャンセル ○ 修正済み 注: CVIT の場合は [理由]、[キャンセル済み]、[修正済み] が適用されません。
作業メモ	変更を説明するために入力するテキスト。

6. [編集] をクリックします。

一括編集の非同期ジョブにより、関連のレコードが更新されます。

で修復タスクとレコードの例外を要求する **Vulnerability Manager** ワークスペース

脆弱性マネージャーと脆弱性アナリストは、 Vulnerability Manager ワークスペースから修復タスク (VUL、AVUL、CVUL、CRG) とレコード (VIT、CVIT、AVIT、CTR) の例外と誤検出を要求できます。修復タスクを分割して変更要求を作成することもできます。

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin
- アプリケーション脆弱性一致アイテム (AVIT) の場合、sn_vul.app_sec_manager
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin
- 構成テスト結果 (CTR) の sn_vulc.admin

注:
脆弱性対応 の v19.0 以降では、次の用語の名前が変更されました。

用語の変更

v19.0 より前の用語	**v19.0** 以降の用語
テスト結果グループ	修復タスク
構成の問題	構成テスト結果
ポリシー	テストグループ

Vulnerability Manager ワークスペースでは、レコードや修復タスクに対して次の操作を実行できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 修復タスク (VUL、AVUL、CVUL、CRG) を分割。
- レコード (VIT、AVIT、CVIT) または修復タスク (VUL、AVUL、CVUL、CRG) の例外を要求します。
- レコード (VIT、AVIT、CVIT) や修復タスク (VUL、AVUL、CVUL、CRG) のポリシー例外を要求。
- ホスト脆弱性一致アイテム (VIT) と修復タスク (VUL) のリスク削減の要求
- 修復タスク (VUL、CVUL、CRG) の変更要求を作成。
- レコード (VIT、AVIT、CVIT) や修復タスク (VUL、AVUL、CVUL、CRG) の誤検出を要求。

> **注:**
> 修復タスク (CRG) から、一連のテスト結果に対する誤検出要求を発生させることができます。

修復オーナーが IT 修復ワークスペース でタスクを実行するのと同じように、Vulnerability Manager ワークスペースでレコードから UI アクションを開始します。

詳細は、以下のトピックを参照してください。

- 脆弱性一致アイテムまたは修復タスクの誤検出を要求する
- IT 修復ワークスペースで例外を要求する
- 脆弱性一致アイテムまたは修復タスクのリスク削減の要求
- IT 修復ワークスペースでの修復タスクの分割
- IT 修復ワークスペースで変更要求を作成する
- IT 修復ワークスペースで GRC: ポリシーとコンプライアンス管理 を使用して例外を要求する
- 一連のテスト結果の誤検出を要求する

関連情報

例外管理の概要

コンフィグレーションコンプライアンス の例外管理の概要

脆弱性マネージャーワークスペースでの一括例外の要求

脆弱性マネージャーワークスペースで誤検出を一括編集

脆弱性マネージャーのワークスペースでの保留された脆弱性一致アイテムの延長の要求

保留された脆弱性一致アイテムがその保留された期限に達する前に、この脆弱性一致アイテムの延長を要求します。修復オーナーは、この要求を行うために保留期日まで待つ必要がなくなりました。

始める前に

必要なロール：sn_vul.vulnerability_admin または sn_vul.admin (非推奨)

このタスクについて

クラシック環境から延長を要求することもできます。

アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、テスト結果グループ、および修復タスクの延長を要求する場合には、同じ手順を使用します。

手順

1. 次のように移動する。 ワークスペース > 脆弱性マネージャーのワークスペース.
2. [リスト] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. [ホスト脆弱性一致アイテム] で [すべて] を選択します。
4. [ステータス] 列で [保留] を選択して、リストをフィルタリングします。
5. 保留されている脆弱性一致アイテムを選択します。

   注:
   [拡張を要求] ボタンは、脆弱性一致アイテムのステータスが [保留] の場合にのみ表示されます。

6. [拡張を要求 **(Request Extension)]** ボタンを選択します。
7. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
拡張期限	保留された脆弱性一致アイテムを修復のために延長する必要がある期限を選択します。
理由	問題を保留する理由を入力します。 次の選択肢があります。 ○ メンテナンス期間待ち ○ 修正が利用不可 ○ リスクの受容 ○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

8. [拡張を要求] を選択します。
   要求が送信され、承認者によって後続のアクションが実行されると、メールがトリガーされます。

   注:
   - 要求は 2 段階の承認を経過します。
   - 保留された脆弱性一致アイテムが再度延長されると、バックエンドで延長保留カウントが増加します。

9. 要求が承認されると、[期限]、[理由]、および [保留メモ] が更新されます。

Vulnerability Manager ワークスペース の参照情報

次のトピックでは、Vulnerability Manager ワークスペース にあるフォームやレコードのフィールドデータの他に、リンク、参照情報について説明します。

[store-future: BEGIN review]

[すべて] メニューから **Vulnerability Manager** ワークスペース にリダイレクトする

アドミニストレーターが *sn_vul_cmn_ws.navigate_to_workspace* システムプロパティを true に設定した場合、[すべて] メニューから [脆弱性対応]、[アプリケーション脆弱性対応]、[コンテナ脆弱性対応]、および [コンフィグレーションコンプライアンス] モジュールで事前定義されたフィルターリンクを選択すると、Vulnerability Manager ワークスペースにリダイレクトされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

のホームページへのリダイレクト **Vulnerability Manager** ワークスペース

sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin ロールを持つユーザーが、[脆弱性一致アイテム] モジュールで次の事前定義されたフィルターリンクを選択する場合、次の場所に移動します。 **All** (すべて) > 脆弱性対応 > 脆弱性一致アイテムの場合、 Vulnerability Manager ワークスペースのホームページでこれらのリンクが開き、[ホスト脆弱性] タブで対応する保存済みフィルターが自動的に選択されます。

- 重大なリスク
- 未達成ターゲット
- 複数の保留
- 90 日以上前
- アサイン解除済み
- 修復タスク未割り当て
- 高リスク
- 過去 90 日以内
- 廃止
- ターゲット間近
- エクスプロイト可能

sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin ロールを持つユーザーが、[コンテナ脆弱性一致アイテム] モジュールで次の事前定義されたフィルターリンクを選択する場合、次の場所に移動します。 **All** (すべて) > **Container Vulnerability Response** > コンテナ脆弱性一致アイテムの場合、 Vulnerability Manager ワークスペースのホームページでこれらのリンクが開き、[コンテナ脆弱性] タブで対応する保存済みフィルターが自動的に選択されます。

- アサイン解除済み
- 重大および高リスク
- エクスプロイト可能
- ターゲット間近
- 未達成ターゲット
- 複数の保留
- All (すべて)

sn_vul.app_sec_manager ロールを持つユーザーが、[アプリケーション脆弱性一致アイテム] モジュールで次の事前定義されたフィルターリンクを選択する場合、次の場所に移動します。 **All** (すべて) > アプリケーション脆弱性対応 > 脆弱性一致アイテムの場合、これらのリンクが Vulnerability Manager ワークスペースのホームページで開き、[アプリケーション脆弱性] タブで対応する保存済みフィルターが自動的に選択されます。

- アクティブ
- 未達成修復コミットメント日
- 複数の保留
- アサイン解除済み
- All (すべて)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

sn_vulc.admin ロールを持つユーザーが、[テスト結果] モジュールで次の事前定義されたフィルターリンクを選択する場合、 **All** (すべて) > コンフィグレーションコンプライアンス > テスト結果の場合、 Vulnerability Manager ワークスペースのホームページでこれらのリンクが開き、[構成テスト結果] タブで対応する保存済みフィルターが自動的に選択されます。

- 未トリアージのテスト結果
- テスト結果を開く
- ターゲット間近
- 未達成ターゲット
- 複数の保留
- アサイン解除済み
- All (すべて)

の [リスト] ページにリダイレクトする **Vulnerability Manager** ワークスペース

sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin ロールを持つユーザーが、脆弱性対応モジュールで次の事前定義フィルターリンクを選択する場合、次の場所に移動します。 **All** (すべて) > 脆弱性対応の場合、 Vulnerability Manager ワークスペースの [リスト] ページで次のリンクが開きます。

- 修復タスク:アクティブ、自分にアサイン済み、所属グループにアサイン済み、およびすべて
- 脆弱性一致アイテム:自分にアサイン済み、および所属グループにアサイン済み
- ライブラリ - NVD、CWE、サードパーティ、および脆弱なソフトウェア
- ソリューション:すべて、最高優先度、および脆弱性一致アイテムあり
- 自分の承認

sn_vul_container.vulnerability_analyst または sn_vul_container.vulnerability_admin ロールを持つユーザーが、Container Vulnerability Response モジュールで次の事前定義されたフィルターリンクを選択する場合、次の場所に移動します。 **All** (すべて) > **Container Vulnerability Response**の場合、これらのリンクは Vulnerability Manager ワークスペースのリストページで開きます。

- コンテナ修復タスク:アクティブ、自分にアサイン済み、所属グループにアサイン済み、およびすべて
- コンテナ脆弱性一致アイテム:自分にアサイン済み、所属グループにアサイン済み
- ライブラリ - NVD、CWE、およびサードパーティ
- 自分の承認

sn_vul.app_sec_manager ロールを持つユーザーが、アプリケーション脆弱性対応モジュールで次の事前定義されたフィルターリンクを選択する場合、次の場所に移動します。 **All** (すべて) > アプリケーション脆弱性対応の場合、 Vulnerability Manager ワークスペースの [リスト] ページで次のリンクが開きます。

- 修復タスク:アクティブ、自分にアサイン済み、所属グループにアサイン済み、およびすべて
- 脆弱性一致アイテム:自分にアサイン済み、所属グループにアサイン済み
- 自分の承認
- ライブラリ - NVD、CWE、およびサードパーティ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ペネトレーションテスト評価要求:アクティブ、すべて自分にアサイン済み、所属グループにアサイン済み
- ペネトレーションテスト結果:アクティブ、検証保留中、自分にアサイン済み、自分のグループにアサイン済み、すべて

sn_vul.app_sec_manager ロールを持つユーザーが、コンフィグレーションコンプライアンスモジュールで次の事前定義されたフィルターリンクを選択すると、次の場所に移動します。 **All** (すべて) > コンフィグレーションコンプライアンスの場合、 Vulnerability Manager ワークスペースの [リスト] ページで次のリンクが開きます。

- 修復タスク:自分のオープンタスク、すべてのオープンタスク、複数の保留、およびすべてのタスク
- テスト
- テストグループ
- サポートデータ - 信頼できるソースとテクノロジー

[End]

[ウォッチトピックを作成] フォームのフィールド

次の表では、 Vulnerability Manager ワークスペースの [ウォッチトピックを作成] フォームのフィールドについて説明します。

フィールド	説明
名前	ウォッチトピックの名前 (重要な VI など)。
オーナー	ウォッチトピックを所有するユーザーの名前。
表示順序	100 ～ 1000 の値を入力します。デフォルト値は 100 です。100 以降の小さい方の値からリストに昇順で表示されます。
所有グループ	ウォッチトピックを所有するグループの名前。
有効	ウォッチトピックをアクティブ化または非アクティブ化します。デフォルトでは選択されています (アクティブ)。
ウォッチリスト	通知を受信し、ウォッチトピックを表示できるユーザーの名前を追加します。
説明	ウォッチトピックを説明するテキスト。このウォッチトピックから修復作業を作成するときに、このテキストが [説明] フィールドに表示されます。
カテゴリ	ウォッチトピックが作成されているレコードのタイプ。

関連情報

で監視トピックを作成する Vulnerability Manager ワークスペース

[GRC 例外の要求 **(GRC request exception)]** フォームのフィールド

次の表に、[GRC 例外の要求 (GRC request exception)] フォームのフィールドの説明を示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[例外の要求] フォーム

フィールド	説明
ポリシー	例外を要求している脆弱性管理ポリシー。
コントロール目標	選択したポリシーに関連付けられているコントロール目標。ポリシーが選択されていない場合は、すべてのコントロール目標が一覧表示されます。
有効期限開始	例外が開始される日付。デフォルト値は現在の日付です。過去の日付にすることはできません。
有効期限	ポリシー例外が期限切れになり、脆弱性一致アイテムまたはグループのステータスが [保留] から [オープン] に変更される日付。 **注:** ポリシー例外が有効である日数を、ポリシーとコンプライアンスでポリシーに設定した [最大例外期間 (日数)] を超える日数に設定することはできません。詳細については、「ポリシーの作成」を参照してください。
理由	例外を要求する理由。
理由	この要求が行われている理由に関連する詳細情報。このフィールドは修復オーナーが入力する必要があります。

[修正ダイジェストを生成 **(Generate remediation digest)]** フォームのフィールド

次の表に、[修正ダイジェストを生成 (Generate remediation digest)] フォームのフィールドを示します。

[修正ダイジェストを生成 **(Generate remediation digest)]** のフィールド

フィールド	説明
[アクティブ] チェックボックス	このチェックボックスは、デフォルトでアクティブ化されています。メール通知を送信しない場合は、このフィールドを非アクティブ化します。
実行	デフォルトは [週次] です。リストからオプションを選択します。
曜日	デフォルトは [月曜日] です。リストからオプションを選択します。
時刻	メールを配信する時間を設定します。ジョブを実行するインスタンスで使用されているタイムゾーン以外のタイムゾーンを使用する場合は、タイムゾーンを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リスクスコアと有効期限に対する補完コントロールの影響

修復オーナーは、ホスト脆弱性一致アイテムまたは修復タスクのリスク削減を要求できます。脆弱性マネージャーまたはアナリストは、これらのリスク削減要求を承認できます。

リスク削減を要求し、リスク削減承認を行う方法の詳細については、「脆弱性一致アイテムまたは修復タスクのリスク削減の要求」および「Vulnerability Manager ワークスペース で要求を承認または却下」をそれぞれ参照してください。

リスク削減要求が承認されると、ステータス変更承認 (VCA#) レコードの [目標値] (リスク評価) に従ってリスクスコアが低下します。リスク削減要求が承認されると、目的のリスク評価の最も高いリスクスコアがレコードに割り当てられます。次の例は、補完コントロールが適用されたときに [リスクスコア] と [元のリスクスコア] がどのように更新されるかを示しています。次の例では、リスク評価のデフォルトの最高リスクスコアが使用されます。

リスクスコアと元のリスクスコアに対する補完コントロールの影響

シナリオ	リスク評価	リスクスコア	元のリスクスコア (計算されたリスクスコア)
v20.0 より前のデータ	2 - 高	80	このフィールドは v20.0 より前では使用できません。
v20.0 へのアップグレード後	2 - 高	80	Null
計算済みのリスクスコアが取り込み時に 90 に変更される	1 - 重大	90	Null
補完コントロールの適用時	3：中	69	90
計算済みのリスクスコアが取り込み時に 70 に変更される	3：中	69	70
計算済みのリスクスコアが取り込み時に 50 に変更される	3：中	50	50
計算済みのリスクスコアが取り込み時に 80 に変更される	3：中	50	80
補完コントロールが [リスク削減の期限日] に期限切れとなった場合	2 - 高	80	Null

修復タスクに対する補完コントロールの影響

リスク削減の要求が修復タスクに対して承認された場合、脆弱性一致アイテムに対する補完コントロールの影響は次のとおりです。

- 修復タスクに適用された補完コントロールは、修復タスクのステータス変更承認において [目標値 **(Desired value)]** に対応するリスクスコアよりもリスクスコアが高い脆弱性一致アイテム ([クローズ済み] ステータス以外) に適用されます。これらの脆弱性一致アイテムのリスクスコアは、[目標値] に従って削減されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- [リスク削減の期限日] は、補完コントロールが既に適用されている脆弱性一致アイテムについては変更されません。修復タスクの [リスク削減の期限日] では更新されません。
- リスク削減の期限日は、補完コントロールが以前に脆弱性一致アイテムに適用されていない場合にのみ、脆弱性一致アイテムにロールダウンされます。修復タスクに補完コントロールを再度適用すると、脆弱性一致アイテムの既存の [リスク削減の期限日] が優先されるため、[リスク削減の期限日] は脆弱性一致アイテムにロールダウンされません。
- 補完コントロールが既に適用されている修復タスクに新しい脆弱性一致アイテムが追加された場合、リスクは脆弱性一致アイテムにロールダウンされません。

脆弱性一致アイテムに対する補完コントロールの影響

脆弱性一致アイテムに対するリスク削減の要求が承認されている場合：

- 新しいリスクスコアが [リスクスコア] フィールドに表示され、古いリスクスコア (計算されたリスクスコア) が [元のリスクスコア] フィールドに移動します。この変更は、[リスク削減の期限日] フィールドで指定された日付まで保持されます。
- 取り込み時に、脆弱性一致アイテムに補完コントロールが既に適用されている場合：
  - 算出されたリスクスコアがリスクスコアより大きい場合、リスクスコアは同じままになり、元のリスクスコアは算出されたリスクスコアで更新されます。
  - 算出されたリスクスコアがリスクスコアより小さい場合、リスクスコアと元のリスクスコアの両方が算出されたリスクスコアで更新されます。
- 補完コントロールが既に適用されている脆弱性一致アイテムの構成アイテム (CI) が変更された場合:
  - *sn_sec_cmn.update_on_ci_change* システムプロパティが true に設定されていると、デフォルトで脆弱性一致アイテムに対して CI が更新されます。

    補完コントロールは引き続き脆弱性一致アイテムに適用されます。
  - *sn_sec_cmn.update_on_ci_change* システムプロパティが false に設定されている場合、脆弱性一致アイテムはクローズされ、新しい脆弱性一致アイテムが作成されます。

    古い脆弱性一致アイテムに適用された補完コントロールは、新しい脆弱性一致アイテムに適用され、[リスク削減の期限日]、[元のリスクスコア]、および [リスクスコア] は同じままです。
- 脆弱性一致アイテムがスキャナーによって再オープンし、補完コントロールが既に適用されている場合は、再オープン後に同じ補完コントロールが適用されます。

関連情報

リスク削減の補完コントロールについて

補完コントロールをライブラリに追加する

リスク削減要求の CVE または TPE に補完コントロールを関連付ける

CVE または TPE のリスク削減を無効または有効にする

#unique_135_Connect_42_li-risk-reduction-vmws

での修復タスク作成の例 **Vulnerability Manager** ワークスペース および **IT** 修復ワークスペース

Vulnerability Manager ワークスペースおよびIT 修復ワークスペースで修復タスクを手動で作成すると、選択したグループ化基準に基づいてレコードが修復タスクにグループ化されます。

修復タスクの作成対象として 10 件のレコードが選択されている次の例を考えてみましょう。レコード選択の詳細と簡単な説明を入力したら、要件に応じて グループ化基準 を選択し、既存の修復タスクに既に含まれているレコードの管理方法を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Example: グループ化基準に基づいた修復タスクの作成

修復タスクの作成対象として選択された脆弱性一致アイテム

脆弱性一致アイテム **ID**	既存の修復タスク	アサイン先グループ	構成アイテム **(CI)**	脆弱性	リスク評価
VIT10001	VUL10021、VUL10022	修復マネージャー	APSVR-NY-1672	CVE-2018-9024	10
VIT10002	-	脆弱性対応	DEV-IBM-NY-682	CVE-2018-9022	10
VIT10003	VUL10021	LDAP 管理者	DEV-IBM-NY-682	CVE-2012-5357	7
VIT10004	-	修復マネージャー	CRMBK-SD-4210	CVE-2013-1714	10
VIT10005	VUL10022	脆弱性対応	DEV-IBM-NY-682	CVE-2018-9022	10
VIT10006	-	修復マネージャー	CRMBK-SD-4210	CVE-2013-1712	10
VIT10007	-	LDAP 管理者	DEV-SAP-SD-9388	CVE-2013-3906	6
VIT10008	-	LDAP 管理者	DEV-IBM-NY-682	CVE-2013-3906	6
VIT10009	-	修復マネージャー	CRMBK-SD-4210	CVE-2013-1712	10
VIT10010	-	LDAP 管理者	DEV-SAP-SD-9388	CVE-2013-3904	6

次のリストは、修復タスクの作成時に選択されたグループ化基準に基づいて、レコードが修復タスクにどのようにグループ化されるかを示しています。

シナリオ 1:[グループ化基準] で [アサイン先グループ] が選択され、[他の修復タスクのレコードの管理 (Managing records in other remediation tasks)] で [新しい修復タスクのレコードをスキップ] が選択されている

同じアサイン先グループを持つレコードは、1 つの修復タスクにグループ化されます。既存の修復タスクに既に含まれているレコードは、新しい修復タスクに追加されません。ここでは、修復 マネージャー、 **LDAP** アドミン、 および脆弱性対応 アサイン先グループにアサインされたレコードを含む、3 つの修復タスクが作成されます。

シナリオ **1** で作成された修復タスク

作成された修復タスク	修復タスクのレコード
修復タスク 1:VUL10001	この修復タスクには、 修復マネージャーのアサイン先グループにアサインされたレコードが含まれています。 • VIT10004 • VIT10006 • VIT10009

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

シナリオ **1** で作成された修復タスク (続く)

作成された修復タスク	修復タスクのレコード
	VIT10001レコードはVUL10001修復タスクに移動されません。
修復タスク 2:VUL10002	この修復タスクには、 脆弱性対応 アサイン先グループにアサインされたVIT10002レコードが含まれています。 VIT10005レコードはVUL10002タスクに移動されません。
修復タスク 3:VUL10003	この修復タスクには、 **LDAP** アドミン アサイン先グループにアサインされたレコードが含まれています。 • VIT10007 • VIT10008 • VIT10010 VIT10003レコードはVUL10003修復タスクに移動されません。

シナリオ 2:[アサイン先グループと構成アイテム] として [グループ化基準] が選択され、[他の修復タスクのレコードの管理] が [新しい修復タスクにレコードを転送] として選択されている

同じアサイン先グループにアサインされている同じ構成アイテムを持つレコードは、修復タスクにグループ化されます。VIT10001、VIT10003、およびVIT10005レコードは古い修復タスクから削除され、新しい修復タスクに移動されます。ここでは、5 つの修復タスクが作成されます。

シナリオ **2** で作成された修復タスク

作成された修復タスク	修復タスクの一部を記録します
修復タスク 1:VUL10004	この修復タスクには、 修復オーナー アサイン先グループにアサインされ、**APSVR-NY-1672** 構成アイテムを持つレコードが含まれています。 • VIT10001 • [store-future: BEGIN review][End] VIT10001レコードがVUL10021から削除され、修復タスクがVUL10022されます。
修復タスク 2:VUL10005	この修復タスクには、 脆弱性対応 アサイン先グループにアサインされた、 **DEV-IBM-NY-682** 構成アイテムを含むレコードが含まれています。 • VIT10002 • VIT10005

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

シナリオ **2** で作成された修復タスク (続く)

作成された修復タスク	修復タスクの一部を記録します
	VIT10005レコードがVUL10022修復タスクから削除されます。
修復タスク 3:VUL10006	この修復タスクには、 **LDAP** アド ミン アサイン先グループにアサインされたレコードと 、DEV-**IBM-NY-682** 構成アイテムが含まれています。 • VIT10003 • VIT10008 VIT10003レコードがVUL10021修復タスクから削除されます。
修復タスク 4:VUL10007	この修復タスクには、 修復マネージャー のアサイン先グループと **CRMBK-SD-4210** 構成アイテムにアサインされたレコードが含まれています。 • VIT10004 • VIT10006 • VIT10009
修復タスク 5:VUL10008	この修復タスクには、 **LDAP** アド ミン アサイン先グループにアサインされたレコードと 、DEV-**SAP-SD-9388** 構成アイテムが含まれています。 • VIT10007 • VIT10010

シナリオ 3:グループ化クライテリアが [アサイン先グループと脆弱性] として選択され、[他の修復タスクのレコードの管理] が [現在の修復タスクと新しい修復タスクの両方のレコードを保持する] として選択されている

同じアサイン先グループにアサインされている同じ脆弱性を持つレコードは、修復タスクにグループ化されます。VIT10001、VIT10003、およびVIT10005レコードは、古い修復タスクから削除されることなく、それぞれの新しい修復タスクに追加されます。ここでは、5 つの修復タスクが作成されます。

シナリオ **3** で作成された修復タスク

作成された修復タスク	修復タスクの一部を記録します
修復タスク 1:VUL10009	この修復タスクには、 修復オーナー アサイン先グループにアサインされた、脆弱性が **CVE-2018-9020** のレコードが含まれています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

シナリオ **3** で作成された修復タスク (続く)

作成された修復タスク	修復タスクの一部を記録します
	• VIT10001 • [store-future: BEGIN review][End] VIT10001レコードはVUL10021の一部であり、修復タスクVUL10022残ります。
修復タスク 2:VUL10010	この修復タスクには、 脆弱性対応 アサイン先グループにアサインされた、**CVE-2018-9020** 脆弱性があるレコードが含まれています。 • VIT10002 • VIT10005 VIT10005レコードも修復タスクの一部として残りますVUL10022。
修復タスク 3:VUL10011	この修復タスクには、 **LDAP** アドミン アサイン先グループにアサインされた、**CVE-2012-5357** の脆弱性があるレコードが含まれています。 • VIT10003 • [store-future: BEGIN review][End] VIT10003レコードは、引き続きVUL10021修復タスクの一部になります。
修復タスク 4:VUL10012	この修復タスクには、 修復マネージャーのアサイン先グループにアサインされた、 **CVE-2013-1710** の脆弱性があるレコードが含まれています。 • VIT10004 • VIT10006 • VIT10009
修復タスク 5:VUL10013	この修復タスクには、 **LDAP** アドミン アサイン先グループにアサインされ、脆弱性が **CVE-2013-3906** のレコードが含まれています。 • VIT10007 • VIT10008 • VIT10010

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

シナリオ 4:グループ化クライテリアを [アサイン先グループとリスク評価] として、[他の修復タスクのレコードの管理] で [現在の修復タスクと新しい修復タスクの両方のレコードを保持する] が選択されている

同じアサイン先グループにアサインされた同じリスク評価のレコードは、修復タスクにグループ化されます。VIT10001、VIT10003、およびVIT10005レコードは、古い修復タスクから削除されることなく、それぞれの新しい修復タスクに追加されます。ここでは、5 つの修復タスクが作成されます。

シナリオ **4** で作成された修復タスク

作成された修復タスク	修復タスクの一部を記録します
修復タスク 1:VUL10014	この修復タスクには、 修復オーナー アサイン先グループにアサインされ、リスク評価が **4** のレコードが含まれています。 • VIT10001 • VIT10004 VIT10001レコードは引き続き VUL10021 の一部となり、修復タスクをVUL10022します。
修復タスク 2:VUL10015	この修復タスクには、 脆弱性対応 アサイン先グループにアサインされ、リスク評価が **2** のレコードが含まれています。 • VIT10002 • VIT10005 VIT10005レコードは引き続き修復タスクに含まれVUL10022。
修復タスク 3:VUL10016	この修復タスクには、 **LDAP** アドミン アサイン先グループにアサインされ、リスク評価が **1** つのレコードが含まれています。 • VIT10003 • VIT10007 • VIT10008 VIT10003レコードは引き続き修復タスクに含まれVUL10021。
修復タスク 4:VUL10017	この修復タスクには、 修復マネージャー のアサイン先グループにアサインされ、リスク評価が **2** のレコードが含まれています。 • VIT10006 • VIT10009

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

シナリオ **4** で作成された修復タスク (続く)

作成された修復タスク	修復タスクの一部を記録します
修復タスク 5:VUL10018	この修復タスクには、 **LDAP** アド ミンのアサイン先グループにアサインされ、リスク評価が **4** のレコードが含まれています。 • VIT10010 • [store-future: BEGIN review][End]

関連情報

で修復タスクを手動で作成する Vulnerability Manager ワークスペース

で修復タスクを手動で作成する IT 修復ワークスペース

で選択したレコードの例外を再評価しています **Vulnerability Manager** ワークスペース

Vulnerability Manager ワークスペースでは、[修復プロパティを再評価して更新] モーダルで一連のレコードの例外ルールを評価すると、最新の例外ルールに従って、保留ステータスと保留期限が更新されます。

シナリオ

Vulnerability Manager ワークスペースの [修復プロパティを再評価して更新] モーダルで選択したレコードセットの例外を評価すると、次のシナリオが発生する可能性があります。

シナリオ **1:** 選択したレコードが既に手動で保留されていて、例外ルールの条件に一致する場合、これらのレコードは変更されずに [保留] ステータスのままになります。

シナリオ **2:** 選択したレコードが例外ルールの条件に一致し、これらのレコードが保留以外のステータス ([オープン]、[レビュー中]、[調査中] など) である場合、これらのレコードは例外ルールで定義された日付まで保留されます。

シナリオ **3:** 選択したレコードが既に [保留] ステータス (例外ルール A を使用して保留されている) である場合、次のシナリオでは [保留] ステータスのままになります。

- 例外ルールの有効期限が切れ、レコードが条件と一致しません
- 例外ルールの有効期限が切れ、レコードが条件に一致する場合
- 例外ルール A の有効期限が切れ、レコードが別の例外ルール B の条件に一致する場合。

シナリオ **4:** 例外ルールを使用してレコードが保留されることを考慮してください。レコードの [保留] ステータスが無効になるように例外ルール条件を変更し、これらのレコードの例外ルールを再評価すると、次のようになります。

- レコードが [オープン] ステータスに移行します
- [期限日]、[保留日]、[保留数] などのフィールドが更新されます。

Example: 次のホスト脆弱性一致アイテム **(VIT)** の例外を評価していることを考慮してください

次の詳細を含む例外ルールを検討します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

例外ルールの詳細

フィールド	説明	値
名前	例外ルールの名前。	重要な VIT の保留
有効期限開始	このルールがアクティブになり、VI が保留される開始日付。	20-08-2024
有効期間終了日時	修復タスクが新しい VI の受け入れを停止する日付。	30-11-2024
理由	この例外ルールを作成する理由。	リスク受容
アサイン先グループ	保留された VI の追跡用に作成された修復タスクがアサインされているグループ。	修復グループ 1
補足情報	要求者が承認者に提供する追加情報。この情報は、修復タスクの説明フィールドに入力されます。	このルールは、重要な VIT を自動的に保留するために作成されました。
条件	VI の処理中に定義できる VI のフィルター条件。	リスク評価 = 5:重大
既存のデータで実行	このルールが初めて実行されるときに既存のデータでこのルールを実行できるようにするオプション。	要
状況	例外ルールのステータス。	承認済み
実行順序	各例外ルールの一意の順序。	100
保留期限	VUL および VI の保留期限となる日付。この日付になると、作成された VUL がクローズされ、すべての VI がグループから離脱し、グループルールが再適用されます。	2024-12-23 16:10:29

次の表は、例外ルールが複数の VIT に対して同時に再評価されたときにステータスがどのように変化するかを示しています。

例外が再評価されるレコード

VIT 番号	状況	リスク評価	例外の再評価後の更新されたステータス **-1**	期限日:1
VIT120067	オープン	2：低	オープン	-
VIT120068	レビュー中	3：中	レビュー中	-
VIT120069	調査中	5:重大	保留	2024-12-23 16:10:29
VIT120070	保留	5:重大	保留	2024-12-23 16:10:29

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

例外が再評価されるレコード (続く)

VIT 番号	状況	リスク評価	例外の再評価後の更新されたステータス -1	期限日:1
VIT120071	保留	2：低	保留	2024-10-02 16:10:29 (手動で保留)
VIT120072	クローズ済み	5:重大	クローズ済み	-

前の例外ルールの条件が [リスク評価] = 2 - [低] に変更され、[保留期限] が 2024-12-31 14:10:23 に変更されると、レコードは次のように更新されます。

例外が再評価されるレコード

VIT 番号	例外の再評価後の更新されたステータス -1	リスク評価	例外の再評価後の更新されたステータス - 2	終了日 - 2
VIT120067	オープン	2：低	保留	2024-12-31 14:10:23
VIT120068	レビュー中	3：中	レビュー中	-
VIT120069	保留	5:重大	保留	2024-12-23 16:10:29
VIT120070	保留	5:重大	保留	2024-12-23 16:10:29
VIT120071	保留	2：低	保留 (ステータスに変更なし)	2024-10-02 16:10:29 (終了日に変更はありません)
VIT120072	クローズ済み	5:重大	クローズ済み	-

関連情報

Vulnerability Manager ワークスペース でレコードの修復プロパティを再評価

例外ルールの概要

コンフィグレーションコンプライアンス の例外管理の概要

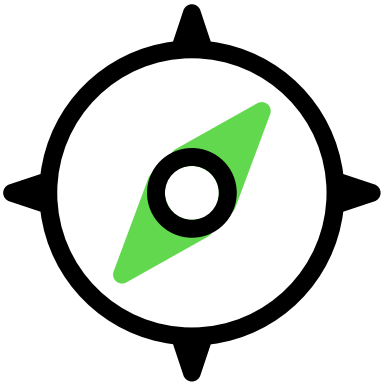
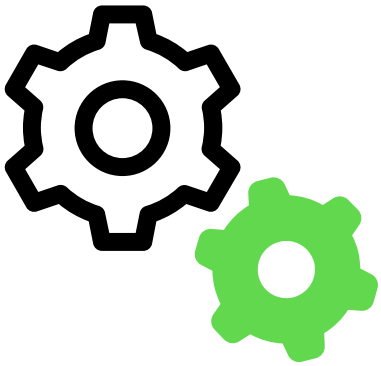
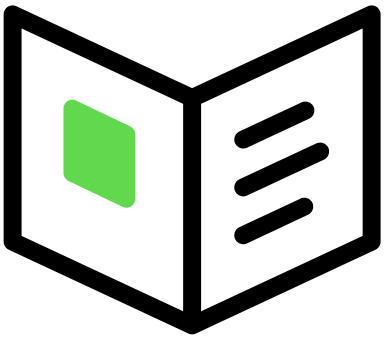
IT 修復ワークスペース

IT チームは、 IT 修復ワークスペース から簡単に変更要求を作成し、脆弱性一致アイテムを再スキャンし、例外要求を送信することで、IT 関連の脆弱性を解決する時間を節約できます。

v18.0 IT 修復ワークスペースのデモ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

開始するには

探索	修復	Reference (参照)
		
の詳細 IT 修復ワークスペース	から脆弱性と構成ミスを修復する方法を学習する IT 修復ワークスペース	構成と管理に使用する追加情報を取得します IT 修復ワークスペース

トラブルシューティングとサポート

- ServiceNow Community の Security Operations
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

IT 修復ワークスペース の探索

IT 修復ワークスペースは、IT 修復オーナーと IT グループを対象としています。このワークスペースは、ホームビューとリストビュー、およびクリックできる可視化データで構成されており、アサインされている修復タスクと、自分にアサインされた、ソリューションがあるレコードの数を確認できます。

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion
- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
脆弱性対応 の v19.0 以降では、次の用語の名前が変更されました。

用語の変更

v19.0 より前の用語	**v19.0** 以降の用語
テスト結果グループ	修復タスク
構成の問題	構成テスト結果
ポリシー	テストグループ

IT 修復ワークスペースは、次のページ、リスト、およびフォームで構成されています。

ランディング (ホーム) ページ

ホームページは、[アサインされた修復タスク] カード、[VI の優先ソリューション] カード、[影響を受ける CI] カード、[VI の優先パッチ] カード、および [修復タスク] リストで構成されます。ホームページの詳細については、「のホームページ IT 修復ワークスペース」を参照してください。

ダッシュボードページ

ダッシュボードページは、脆弱性修復ダッシュボードで構成されています。[ダッシュボード] ページの詳細については、「の [ダッシュボード] ページ IT 修復ワークスペース」を参照してください。

リストページ

このビューは、修復タスク、ホスト脆弱性一致アイテム、アプリケーション脆弱性一致アイテム、コンテナ脆弱性一致アイテム、自分にアサインされた構成テスト結果、ソリューション、例外要求などのデフォルトおよびカスタマイズされたリストで構成されています。[リスト] ページの詳細については、「 のリストページ IT 修復ワークスペース」を参照してください。このページで実行できる事柄の詳細については、「でリストを作成する IT 修復ワークスペース」を参照してください。

IT 修復ワークスペースでワークフロー例を表示する

IT 修復ワークスペースのエンドツーエンドワークフローの例を表示します。IT スペシャリストがワークスペースを使用して、重大な脆弱性一致アイテム (VIT、AVIT、CVIT) とテスト結果 (TR) を監視し、それらにアサインされた脆弱性を修正する方法を参照してください。

始める前に

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion
- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

手順

次の画像をクリックすると、ワークフローのステップが表示されます。
IT 修復ワークスペースのデモ

画像には、以下のタスクが含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ホームページ (IT 修復オーナーのランディングページ) から、自分にアサインされている修復タスクを表示します。自分と自分のグループにアサインされている作業を切り替えます。ソリューションがあるホスト修復タスクを確認します。ホームページの詳細については、「のホームページ IT 修復ワークスペース」を参照してください。
- リストビューを選択して、アサインされた作業のリストを表示します。
- [修復タスク] リストで [自分のグループにアサイン済み **(Assigned to my group**)] リストが選択されているリストビューから、作業を特定して自分にアサインします。[リスト] ページの詳細については、「 のリストページ IT 修復ワークスペース」を参照してください。
- 修復タスクをレコードタイプ別にグループ化する:[レコードタイプ] 列で 3 つのドットメニューを選択し、[レコードタイプ別にグループ化] を選択します。
- オープンな修復タスク (VUL、AVUL、CVUL、CRG) の場合:
  - [概要] タブを選択して、レコード (VIT、AVIT、CVIT、TR) と、レコードに関連付けられている影響を受ける構成アイテム (CI) を表示します。
  - [ソリューション] タブを選択して、ホスト修復タスクの優先ソリューションと見込みのあるソリューションを表示します。
  - [詳細] タブを選択して、[ステータス]、[アサイン先グループ]、[アサイン先]、[簡単な説明] などの編集可能なフィールドを変更し、修復タスクに対して実行されたアクションを表示します。
  - [ステータス変更承認] タブを選択して、承認ワークフローを追跡するのに役立つステータス変更承認レコード (CA#) を表示します。
  - [変更要求] タブを選択し、変更要求の承認ステータスを表示し、[新規] ボタンを選択して新しい変更要求を作成します。
  - UI アクションとして、[誤検出としてマーク]、[変更を作成]、[タスクを分割]、[ステータスを更新]、[例外を要求]、[削除] などを選択します。ダイアログの指示に従って修正を実行します。

のホームページ **IT** 修復ワークスペース

IT 修復ワークスペースのホームページには、自分と自分のアサイン先グループにアサインされたホスト、アプリケーション、コンテナ、およびテスト結果の修復タスクの統合リストが表示されます。

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion
- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

ホームページは、自分と自分のアサイン先グループにアサインされた次のカードと修復タスクのリストで構成されています。自分にアサインされたレコードにはソリューションがあります。

アサイン済み修復タスクカード

自分にアサインされたアクティブな修復タスクの数。タイルを選択すると、修復タスクのリストが表示されます。

VI カードの優先ソリューション

ホスト脆弱性一致アイテムを修正するために利用できる優先ソリューションの数。ソリューションリストは、Vulnerability Solution Management アプリケーションがインストールされている場合に表示されます。このカードには、脆弱性一致アイテムに関する、サードパーティベンダーからのソリューションデータ (見込みのある解決策と優先ソリューション) が表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

影響を受ける CI カード

自分または自分のグループにアサインされた VI を持つ構成アイテムの数。詳細については、「IT 修復ワークスペースで脆弱性のある構成アイテムを表示する」を参照してください。

VI カードの優先パッチ

ホスト脆弱性一致アイテムを修正するために使用できる優先パッチの数。

修復タスクリスト

自分と自分のアサイン先グループにアサインされた修復タスクのリスト。[自分にアサイン 済み] および [所属グループにアサイン 済み] オプションを選択すると、レコードをフィルタリングできます。

修復タスクをクリックすると、詳細を表示して調査を開始できます。リストビューでは、修復タスク、脆弱性一致アイテム、構成テスト結果などを表示できます。修復タスクを開き、[自分にアサイン] をクリックして自分にタスクをアサインし、調査を開始します。

注:
修復タスクで自分自身にタスクをアサインしないと、レコードレベルで UI アクションを表示することはできません。

[その他のアクション] (省略記号) をクリックし、[調査を開始] をクリックして修復タスクを解決します。

ホームページで実行できる操作の詳細については、「 IT 修復ワークスペースでの修復タスクレコードの使用」を参照してください。

の [ダッシュボード] ページ **IT** 修復ワークスペース

IT 修復ワークスペースのダッシュボードページは ネクストエクスペリエンス UI に [脆弱性の修復] ダッシュボードを提供します。これを使用して修復タスクと脆弱性一致アイテムにフォーカスできます。

修復オーナー (sn_vul.remediation_owner) は、次の場所に移動して 脆弱性修復 ダッシュボードにアクセスできます ワークスペース > **IT** 修復ワークスペース [ダッシュボード] アイコンを選択します。脆弱性修復ダッシュボードの詳細については、「デフォルトの 脆弱性対応 ダッシュボードを使用する」を参照してください。

カスタマイズされたダッシュボードを作成するには、[その他のオプション] アイコンを選択し、[新規作成] を選択します。 ⋮

のリストページ **IT** 修復ワークスペース

IT 修復ワークスペースのリストビューを使用すると、修復オーナーは自分とそのアサイン先グループにアサインされたレコード (VIT、AVIT、CVIT、TR) を表示し、これらの脆弱性と構成ミスを修正できます。ホスト脆弱性一致アイテム (VIT) の修正に推奨される優先ソリューションのリストを表示することもできます。これらのリストに加えて、自分が出した例外要求とペネトレーションテストアセスメント要求のリスト、ペネトレーションテストアセスメント要求に関連付けられたペネトレーションテスト結果、サポートされているライブラリ、およびその他のサポートされているデータを表示できます。

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

[リスト] ページのリストとリンクを使用すると、レコードやタスクに簡単にアクセスできます。これには次の 2 つのタブがあります。

- [リスト] タブ:修復作業、修復タスク、脆弱性一致アイテム (VIT、AVIT、CVIT)、ソリューション、例外、構成テスト結果 (TR) などのデフォルトリストを表示します。詳細については、次の表を参照してください。
- [自分のリスト] タブ:[リスト] タブから名前を変更したリストと、作成したリストが表示されます。

  独自のレコードリストを作成することもできます。詳細については、「でリストを作成する IT 修復ワークスペース」を参照してください。

ヒント:

sn_vul_cmn_ws.navigate_to_workspace システムプロパティがアドミニストレーターによって true に設定されている場合、[すべて] メニューの コンフィグレーションコンプライアンス脆弱性対応、アプリケーション脆弱性対応、コンテナ脆弱性対応、およびテスト結果モジュールで事前定義されたフィルターリンクを選択すると、これらのリンクがIT 修復ワークスペースのリストページで開きます。

たとえば、[所属グループにアサイン 済み] を選択した場合、 **All** (すべて) > 脆弱性対応 > 修復タスク > 所属グループにアサイン済みの場合、このリンクは IT 修復ワークスペースにリダイレクトされます。修復オーナーロールがある場合、IT 修復ワークスペースのリストページで、[修復タスク] モジュールの [自分のグループにアサイン済み] リストが開きます。ホスト修復タスクを表示するには、 レコードタイプ別にタスクをグループ化します。

glide.ui.list.seismic.omit.count システムプロパティを使用して、リストのレコード数を非表示にすることができます。リストのレコード数の表示をオン/オフにする方法の詳細については、 KBB0010402 KB 記事を参照してください。

[リスト] タブ

以下のリストが表示されます。

Lists (リスト)

リストアイテム	説明	必要なアプリケーション	必要なロール
修復タスク	修復タスクのリストを表示し、目的のタスクに移動して作業を開始します。次のリストが利用できます。 • [自分にアサイン済み **(Assigned to you)**]: 自分にアサインされているすべてのホスト、アプリケーショ	脆弱性対応、 アプリケーション脆弱性対応、 コンテナ脆弱性対応、および コンフィグレーションコンプライアンス	• ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner • アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	必要なアプリケーション	必要なロール
	ン、コンテナ、およびテスト結果の修復タスクを一覧表示します。 • 自分のグループにアサイン済み:自分が属するアサイン先グループにアサインされているすべてのホスト、アプリケーション、コンテナ、およびテスト結果修復タスクを一覧表示します。 タスクをレコードタイプ別にグループ化し、ホスト、アプリケーション、コンテナ、および構成テスト結果の修復タスクに分類します。クラシック UI の修復タスクルールによって作成された修復タスクには、空の修復作業があります。		• コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owne • 構成テスト結果 (CTR) の sn_vulc.remediation_owner
影響を受ける資産	影響を受ける資産のリストを表示します。次のリストが利用できます。 • あなたにアサイン済み:自分にアサインされた、影響を受ける構成アイテムのリスト • 自分のグループにアサイン済み:自分のアサイン先グループにアサインされた、影響を受ける構成アイテムのリスト。	脆弱性対応、 アプリケーション脆弱性対応、 コンテナ脆弱性対応、および コンフィグレーションコンプライアンス	• ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner • アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion • コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owne • 構成テスト結果 (CTR) の sn_vulc.remediation_owner
ホスト脆弱性一致アイテム	ホスト脆弱性一致アイテムのリストを表示し、目的のアイテムに移動して作業を開始します。このリストが利用可能です。	脆弱性対応	ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	必要なアプリケーション	必要なロール
	• [自分にアサイン済み **(Assigned to me)**]: 修復のためにアサインされたホスト脆弱性一致アイテムのリスト。 • 自分のグループにアサイン済み:自分が属するアサイン先グループにアサインされているホスト脆弱性一致アイテムのリスト。		
アプリケーション脆弱性一致アイテム	ホスト脆弱性一致アイテムのリストを表示し、目的のアイテムに移動して作業を開始します。次のリストが利用できます。 • [自分にアサイン済み **(Assigned to me)**]: 修復のために自分にアサインされたアプリケーション脆弱性一致アイテムのリスト。 • 自分のグループにアサイン済み:自分が属するアサイン先グループにアサインされているアプリケーション脆弱性一致アイテムのリスト。	アプリケーション脆弱性対応	sn_vul.app_security_champion
コンテナ脆弱性一致アイテム	コンテナ脆弱性一致アイテムのリストを表示し、目的のアイテムに移動して作業を開始します。このリストビューには次のものが含まれます。 • [自分にアサイン済み **(Assigned to me)**]: 修復のためにアサインされたコンテナ脆弱性一致アイテムのリスト。	コンテナ脆弱性対応	sn_vul_container.remediation_owner インシデントの事後レビューを行うために必要なアセスメントのリストを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	必要なアプリケーション	必要なロール
	• 自分のグループにアサイン済み:自分が属するアサイン先グループにアサインされているコンテナ脆弱性一致アイテムのリスト。		
構成テスト結果	テスト結果のリストを表示し、目的のレコードに移動して作業を開始します。このリストビューには次のものが含まれます。 • [自分にアサイン済み **(Assigned to me)**]: 修復のためにアサインされた構成テスト結果のリスト。 • 自分のグループにアサイン済み:自分が属するアサイン先グループにアサインされた構成テスト結果のリスト。	コンフィグレーションコンプライアンス	sn_vulc.remediation_owner
ソリューション	ソリューション管理アプリケーションのソリューションを一覧表示します。ソリューションリストは、Vulnerability Solution Management アプリケーションがインストールされている場合に表示されます。 • すべて:ホスト脆弱性一致アイテムの修正に使用する利用可能なソリューションをすべて表示します。 • 最高優先度:設定された優先ソリューションに使用されるすべてのソリューションを表示します。	脆弱性対応	sn_vul.remediation_owner

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	必要なアプリケーション	必要なロール
	• 脆弱性一致アイテムを使用:脆弱性一致アイテムの優先ソリューションとして使用されているソリューションを表示します。		
例外要求	• 自分の要求:ホスト、アプリケーション、およびコンテナの脆弱性一致アイテムとその修復タスクに対して自分が出したすべての例外、誤検出、およびアサイン解除承認要求のリスト。 • 自分の要求 (コンフィグレーションコンプライアンス):自分が作業しているテスト結果とその修復タスクに対して自分が出したすべての例外、誤検出、およびアサイン解除承認要求のリスト。	脆弱性対応、 アプリケーション脆弱性対応、 コンテナ脆弱性対応、および コンフィグレーションコンプライアンス	• ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner • アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion • コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owne • 構成テスト結果 (CTR) の sn_vulc.remediation_owner
ライブラリ	次のリストが含まれています。 • **NVD**:米国国立標準技術研究所 (NIST) によって管理されている脆弱性インテリジェンスの包括的なライブラリ。NVD によって検出された脆弱性のリストで、セキュリティチェックリスト、セキュリティ関連のソフトウェアの欠陥、不適切な構成、製品名、およびエクスプロイトを含む影響度メトリクスが含まれています。	脆弱性対応、 アプリケーション脆弱性対応、 コンテナ脆弱性対応、および コンフィグレーションコンプライアンス	• ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner • アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion • コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owne • 構成テスト結果 (CTR) の sn_vulc.remediation_owner

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	必要なアプリケーション	必要なロール
	• **CWE**:コミュニティで開発されたソフトウェアの脆弱性タイプのリスト。各 CWE レコードには、脆弱性を説明する関連するナレッジ記事も含まれています。 • アプリ脆弱性:すべてのサードパーティアプリケーション脆弱性エントリーのリスト。 • **TPE**:インスタンスにインポートされたサードパーティ脆弱性のリスト。関連する参照、脆弱性一致アイテム、エクスプロイト、および CVE のリストが含まれています。 • テスト:テスト結果が準拠する必要があるサードパーティ統合からインポートされたテスト。 • テストグループ:サードパーティ統合からインポートされたテストグループ/ポリシーのリスト。テストグループには、一連のテストが含まれています。		
CMDB	• 検出されたアイテム:検出されたすべてのアイテムのリスト。 • 検出されたコンテナイメージ:	脆弱性対応、 アプリケーション脆弱性対応、 コンテナ脆弱性対応、および コンフィグレーションコンプライアンス	• ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner • アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	必要なアプリケーション	必要なロール
			• コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owne • 構成テスト結果 (CTR) の sn_vulc.remediation_owner
ペネトレーションテストアセスメント要求	ビジネスアプリケーションのセキュリティアセスメントを実行するために、ユーザーがセキュリティチームに送信するペネトレーションテストアセスメント要求。このリストには次のものが含まれています。 • 自分にアサイン済み:自分が作成したペネトレーションテストアセスメント要求のリスト。 • 所属グループにアサイン済み:アサイン先グループのユーザーによって発生したペネトレーションテストアセスメント要求のリスト。	アプリケーション脆弱性対応	sn_vul.app_security_champion
ペネトレーションテスト結果	セキュリティチームによって実施されたペネトレーションテストアセスメント中に特定された脆弱性のリスト: • 自分にアサイン済み:修復のためにアサインされたペネトレーションテスト結果のリスト。 • 所属グループにアサイン済み:修正のためにアサイン先グループにアサインされたペネトレーションテスト結果のリスト。	アプリケーション脆弱性対応	sn_vul.app_security_champion

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Lists (リスト) (続く)

リストアイテム	説明	必要なアプリケーション	必要なロール
サポートデータ	このリストビューには次のものが含まれます。 • 信頼できるソース **(Authoritative Sources):** レコードの作成に使用されたソース公開の調査に役立つサマリー情報を提供する信頼できるソースのリスト。 • テクノロジー:信頼できる各ソースと引用に関するサマリー情報を提供するテクノロジーのリスト (Qualys ではフレームワークとも呼ばれます)。	コンフィグレーションコンプライアンス	sn_vulc.remediation_owner

関連情報

Vulnerability Manager ワークスペースでリストビューを使用する

IT 修復ワークスペースを使用する

IT 修復ワークスペースには、自分と自分のグループにアサインされたホスト脆弱性、アプリケーション脆弱性、コンテナ脆弱性、および構成ミスの統合リストが表示されます。このワークスペースを使用して、脆弱性や構成ミスを修正し、例外を要求できます。

で検索結果を開く IT 修復ワークスペース

アプリケーションスコープを変更してクラシック UI ではなくIT 修復ワークスペースで検索結果を開くには、アプリケーションスコープを [IT 修復ワークスペース] に設定します。

始める前に

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion
- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

このタスクについて

たとえば、アプリケーションスコープを IT 修復ワークスペース に設定して、[検索] フィールドでその番号を含むホスト脆弱性一致アイテムを検索すると、VIT がIT 修復ワークスペースのレコードビューで開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 統一ナビゲーションバーで、地球儀アイコン を選択します。
2. [アプリケーションスコープ] を選択し、スコープを **IT** 修復ワークスペースに設定します。

タスクの結果
VIT、修復タスク、ステータス変更承認などのレコードを検索すると、統一ナビゲーションバーの [検索] フィールドでレコードが IT 修復ワークスペースで開きます。

スコープがグローバルでない場合は、地球アイコンに赤いリングが表示されます。 。再度選択すると、スコープが変更されます。

脆弱性対応ワークスペースでのメールダイジェストの使用

メール通知を使用して、修正の進捗状況を表示し、タスクが SLA 期限に近づいているとき、または SLA 期限を過ぎたときにリマインダーを送信します。

始める前に
必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion
- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

このタスクについて
修復オーナーは、作業領域に移動し、作業の概要としてメール通知を確認します。達成した内容、近づいている内容、期限切れの内容を確認します。通知を使用すると、重要な修復アクションを整理して優先順位を付けることができます。メール内のリンクをクリックして、ワークスペースに直接移動します。通知によって、IT スペシャリストは作業のステータスを一目で確認できます。脆弱性マネージャーによって、IT スペシャリストは、修復タスクのためにメールサービスから直接 Platform にアクセスできます。

この機能の設定方法の詳細については、「脆弱性対応 ワークスペースでのメール通知の設定」を参照してください。

デフォルトでは、クローズしたタスク、自分と自分のグループにアサインされたアクティブなタスクの合計数、新しくアサインされた VIT (クローズ済み)、その他の情報が表示されます。

手順

1. メールに移動し、通知を見つけて、それをクリックして開きます。
   作業ステータスに関する情報を含む通知が表示されます。
2. [ワークスペースに移動 **(Go to workspace)]** をクリックして、作業領域に移動します。

でリストを作成する **IT** 修復ワークスペース

IT 修復ワークスペースのリストビューでは、自分と自分のグループにアサインされた修復タスクとレコードを確認できます。修復タスク (VUL、AVUL、CVUL、CRG)、脆弱性一致アイテム (VIT、AVIT、CVIT)、およびテスト結果 (TR) の例外と誤検出の要求を追跡し、ソリューションを表示することもできます。

始める前に
必要なロール：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion
- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > **IT** 修復ワークスペース.
2. [リスト] アイコン ( ) を選択します。
   リストビューが表示されます。
   - フィルター済みリストをクリックすると、自分または自分のグループにアサインされたアクティブな修復タスクまたはレコードの合計数が表示されます。こうしたレコードから実行できる処理の詳細については、「IT 修復ワークスペースでの修復タスクレコードの使用」を参照してください。
   - 自分または自分のグループにアサインされた、ソリューションのある VI の合計数を表示します。**[VI** の優先ソリューション] カードをクリックしてリストを表示します。
   - 自分と自分のグループにアサインされた脆弱性一致 CI が [脆弱性一致 **CI]** タブに、または自分と自分のグループにアサインされた脆弱性一致 CI がリストビューに表示されます。
3. [自分のリスト] タブを選択します。
4. [新しいリストを追加] を選択します。
5. 既存のリストまたは独自のセットアップに基づいてリストを作成します。
6. オプション: フィルター済みリストを作成します。
   a. [列の選択] フィールドで、表示しないフィールドを削除して、リストに表示する列を決定します。
   b. リストをフィルタリングする条件を指定します。
      (Optional) 複数の条件を追加するには、[新しい条件セット] を選択します。
      たとえば、監視するスキャナーのアクティブな脆弱性一致アイテムのリストを作成する場合は、条件 **[Active][is][true]** および **[Source][contains][scanner-name]** を入力します。
   c. **[Create** (作成)] を選択します。
      新しいリストが表示されます。

      注:
      リストモジュールを終了すると、終了時に表示されるリストが、戻ったときに表示されるリストとなります。作成したカスタムリストを削除するには、リストを表示した状態で、ペインの右側にある歯車アイコンを選択し、 削除 を選択します。
7. リストビューから実行できる操作については、次の表を参照してください。

IT 修復ワークスペースでレコードを使用する

レコードを使用すると、修復の進捗状況と、資産に対する脆弱性一致アイテムの影響を表示できるようになります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion
- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

手順

1. Now Platformインスタンスで、 ワークスペース > **IT** 修復ワークスペース.
   ホームランディングページが表示されます。
2. 脆弱性一致アイテムレコードに移動し、それをホームランディングページまたはリストビューで開きます。

   上部のフォームヘッダーの [詳細] タブには、脆弱性の性質に関連する情報 (「CVE-2013-5014 が LINUX-DAL-4331 で検出されました」など) が含まれています。フォームヘッダーの下に、[ステータス]、 [リスク評価]、 [修復ターゲット日] の値が表示されます。
3. 修復タスクレコードに対して実行できる UI アクションについては、次の表を参照してください。

で修復タスクを手動で作成する **IT** 修復ワークスペース

脆弱性対応 の v25.0.4 以降では、IT 修復ワークスペース の [リスト] ページにある [ホスト脆弱性一致アイテム]、[アプリケーション脆弱性一致アイテム]、[コンテナ脆弱性一致アイテム]、および [構成テスト結果] リストから修復タスクを手動で作成できます。

始める前に
必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.write_assigned または sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の場合は sn_vul.app_write_assigned または sn_vul.app_security_champion
- コンテナ脆弱性一致アイテム (CVIT) の場合、sn_vul_container.writer_assigned または sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

手順

1. 次のように移動する。 ワークスペース > **IT** 修復ワークスペース > リスト.
2. [リスト] ページより、次のいずれかのリストで [アクティブ] または [すべて] リストを開きます。
   - ホスト脆弱性一致アイテム
   - アプリケーション脆弱性一致アイテム
   - コンテナ脆弱性一致アイテム
   - 構成テスト結果
3. 更新するレコードのチェックボックスをオンにし、[修復タスクの作成] モーダルの [レコード選択] フィールドで [選択したアイテム] オプションを選択します。
4. [修復タスクの作成] を選択します。
5. [修復タスクを作成] モーダルで、次の詳細を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスクの作成モーダル

フィールド	説明
レコード選択	選択したアイテム:選択したレコードのみを更新します。
簡単な説明	修復タスクに関する簡単なメモ。
グループ化クライテリア	選択肢は次のとおりです。 ○ アサイン先グループ:同じアサイン先グループを持つレコードは、1 つの修復タスクにグループ化されます。 ○ アサイン先グループと構成アイテム:同じアサイン先グループと構成アイテムを持つレコードは、1 つの修復タスクにグループ化されます。 ○ アサイン先グループと脆弱性:同じアサイン先グループと脆弱性を持つレコードは、1 つの修復タスクにグループ化されます。 ○ アサイン先グループとリスク評価:同じアサイン先グループとリスク評価を持つレコードは、1 つの修復タスクにグループ化されます。
他の修復タスクのレコードの管理	選択肢は次のとおりです。 ○ 新しい修復タスクのレコードをスキップ:他の修復タスクの一部であるレコードに対してアクションは実行されません。 ○ 新しい修復タスクに移動:他の修復タスクの一部であるレコードが新しい修復タスクに転送されます。 ○ 現在の修復タスクと新しい修復タスクの両方に保持:他の修復タスクの一部であるレコードは、古い修復タスクと新しい修復タスクの両方に保持されます。

6. **[Create remediation task** (修復タスクの作成)] を選択します。

タスクの結果

修復タスクは、グループ化基準に基づいて作成されます。アサイン先グループの修復オーナーにメール通知が送信され、修復タスクが作成されてグループにアサインされたことが通知されます。グループ化基準とレコード管理基準に基づいて修復タスクを作成する方法の例については、「 での修復タスク作成の例 Vulnerability Manager ワークスペース および IT 修復ワークスペース」を参照してください。

IT 修復ワークスペースでの修復タスクレコードの使用

修復タスクが作成され、修復作業から自動的にアサインされます。IT 修復ワークスペース で、IT チームや修復オーナーは修復タスクを確認することができます。

始める前に

必要なロール：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion
- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

このタスクについて

脆弱性マネージャーと脆弱性アナリストが修復作業を作成して修正を推進すると、修復作業で レコードに関連付けられているグループに基づいて修復タスクが自動的に作成され、IT チームにアサインされます。

自分と自分のグループにアサインされた脆弱性一致 CI が [脆弱性一致 **CI]** タブに、または自分と自分のグループにアサインされた脆弱性一致 CI がリストビューに表示されます。

手順

1. Now Platformインスタンスで、 脆弱性対応 > **IT** 修復ワークスペース.
   ホームランディングページが表示されます。
2. [修復タスク] セクションで、修復タスクをクリックして開きます。
3. オプション: または、ホームページの左上にある [リスト] アイコンをクリックして、自分と自分のグループにアサインされたすべての修復タスク (VUL、AVUL、CVUL、CRG) とレコード (VIT、AVIT、CVIT、TR を表示することもできます。
   リストビューの使用方法の詳細については、「でリストを作成する IT 修復ワークスペース」を参照してください。
4. ホームページまたはリストビューから、修復タスクをクリックして開きます。

   [詳細] タブでは、アサイン先グループ、ステータス、簡単な説明など、レコードの情報の一部を更新できます。[保存] をクリックして変更を適用します。

5. 修復タスクレコードから実行できる UI アクションについては、次の表を参照してください。

   ホスト修復タスクの [ソリューション] タブには、修復タスクに関連付けられた脆弱性に最も一致する優先ソリューションと見込みのあるソリューションの両方の情報が表示されます。ソリューションとは、IT チームが脆弱性を解決するために適用するパッチのことです。

   Vulnerability Solution Management アプリケーションがインストールされている場合、優先ソリューションは、脆弱性一致アイテムに適用される最上位のソリューションです。ソリューションのリストは、ホスト修復タスクの脆弱性一致アイテムに基づいています。

   見込みのあるソリューションは、ホスト修復タスクの VIT で利用可能なすべてのソリューションのリストです。

   修復タスクでこの脆弱性の影響を受ける CI (資産) を表示するには、次に移動します: 概要 > 影響を受ける **CI**.

IT 修復ワークスペース で修復タスクやレコードを自分にアサインする

IT 修復ワークスペース ワークスペースの [リスト] ページから、修復タスク (VUL、AVUL、CVUL、CRG) やレコード (VIT、AVIT、CVIT、TR) を自分にアサインします。

始める前に

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

手順

1. 次のように移動する。 ワークスペース > **IT** 修復ワークスペース > リスト > 修復タスク > 自分のグループにアサイン済み.
2. 修復タスクリストから修復タスク (VUL、AVUL、CVUL、CRG) を開きます。
3. 右側の UI アクションボタンで、[自分にアサイン] をクリックします。

   [自分にアサイン] ボタンが利用できるのは、レコードがまだ自分にアサインされていない場合のみです。

   修復タスクは、リストビューの [修復タスク] の下の [自分にアサイン済み] リストに表示されます。

4. 同じ手順で、開いているレコードからレコード (VIT、AVIT、CVIT、TR) を自分にアサインすることもできます。
   [自分にアサイン] ボタンが利用できるのは、レコードがまだ自分にアサインされていない場合のみです。

IT 修復ワークスペースで脆弱性のある構成アイテムを表示する

脆弱性対応 アプリケーションのバージョン 16.1 では、以下の機能拡張が修復タスクに追加されました。

始める前に
必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion
- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

ワークスペース内の CI データを表示する場合は、itil または cmdb_read ロールも必要です。

このタスクについて
自分にアサインされた、脆弱性がある構成アイテム (CI) を表示します。[影響を受ける **CI** スコアカード] をクリックします。左上のフィルターリストをクリックして、[自分にアサイン済み] と [所属グループにアサイン済み] を切り替えます。リストビューから、リンクをクリックします。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > **IT** 修復ワークスペース.
   ホームランディングページが表示されます。
2. または、リストビューのリンクから、またはモジュールに移動して、これらのリストを表示することもできます。 **All** (すべて) > 脆弱性対応 > 修復タスク.
3. 1 つ選択して続行します。
   フィルター切り替えの選択内容に応じて、自分または自分のグループにアサインされている以下のレコードのリストが表示されます。

4. [影響を受ける **CI**] スコアカードをクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

CI レコードのリストが表示されます。

5. 構成アイテムをクリックしてそのレコードを開きます。
レコードが表示されます。

関連リストを使用すると、詳細とさまざまな関連レコードを表示できます。このリリースで新たに利用可能になった、このレコードのデータは、次のとおりです。

- このレコードの最近のアクティビティを示すタイムライン。
- この CI に関連付けられた変更要求。
- スコアカードに簡単に移動し、この CI に関連付けられた修復タスク、脆弱性一致アイテム、および優先ソリューションを表示します。
- スコアカードに移動して、この CI に関連付けられている優先パッチを表示することができます。優先パッチは、脆弱性一致アイテムに関連付けられたパッチです。関連リストの [パッチ] タブには、CI のインストール済みパッチと不足しているパッチが表示されます。
- クラス、場所、インターネット接続、環境、およびメンテナンススケジュールを含む CI に関する情報。

IT 修復ワークスペースで変更要求を作成する

修復タスク (VUL、AVUL、CVUL、CRG) から変更要求を作成します。または、既存の変更要求に修復タスクを追加します。

始める前に

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion
- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

注:
IT 修復ワークスペースから変更要求を送信する場合は、itli ロールが必要です。

このタスクについて

修復タスクの変更の要求を作成する理由はさまざまです。通常は、調査で脆弱性を修正するのに手動操作が必要になるためです。

変更要求およびクラシック環境からの変更要求の作成の詳細については、「脆弱性対応 の変更管理」を参照してください。

注:
脆弱性対応 の v19.0 以降では、次の用語の名前が変更されました。

用語の変更

v19.0 より前の用語	v19.0 以降の用語
テスト結果グループ	修復タスク
構成の問題	構成テスト結果
ポリシー	テストグループ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > **IT** 修復ワークスペース.
2. [リスト] アイコンを選択します。
3. [リスト] ページの [修復タスク] リストで、変更要求を作成する修復タスク (VUL、AVUL、CVUL、CRG) を見つけます。
4. 右側の UI アクションボタンで、リストを展開していずれかを選択します。
   - [変更を作成] をクリック
   - 既存の変更に追加
5. 新しい変更要求を作成するには、表示されるモーダルのフィールドに入力します。
   フォームフィールドの詳細については、「[変更要求の作成] フォームのフィールド」を参照してください。
6. [変更要求の作成 **(Create Change Request)]** を選択します。
   修復タスクレコードが表示され、メッセージで、変更要求が正常に作成されたことが示されます。

   レコードの [変更の要求] 関連リンクをクリックすると、レコードに関連付けられているすべての変更の要求が表示されます。
7. または、既存の変更要求にこの修復タスクを追加するには、次の手順を実行します。

   a. 下向き矢印をクリックして [変更を作成] ボタンのリストを展開します。

   b. [既存の変更に追加 **(Add to existing change)]** を選択します。

   c. 表示されるモーダルで、検索アイコンをクリックして、既存の変更要求のリストを表示します。

   d. 変更要求のリストを絞り込むためにリストに条件を追加するには、モーダルの右上にあるフィルターアイコン (じょうご) をクリックします。

   e. 表示される新しいペインで、[詳細表示] をクリックします。

   f. 条件ビルダーを使用して条件を作成します。

   g. [更新] を選択します。

   h. リストから変更の要求をクリックして選択します。
   更新されたモーダルが選択内容とともに表示されます。

   i. オプション: モーダルで、[CR に CI を追加] チェックボックスをオンにして、すべてのアクティブな脆弱性一致アイテムからの構成アイテムを、変更の要求に追加します。

   j. [変更を追加 **(Add change)]** を選択します。
   修正レコードが表示され、メッセージで、変更の要求が正常に作成され承認のために送信されたことが示されます。
      - メッセージ内の [変更を表示] リンクをクリックして、変更の要求 (CHG) レコードを開きます。
      - 修復タスクレコードの [変更の要求 **(Change Requests)]** 関連アイテムメニューリンクを選択すると、レコードに関連付けられているすべての変更要求が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

または、クラシック環境で、 セルフサービス > 自分の要求. 変更を送信してそれが実装されたら、ステータスの同期が有効になっていれば、修復タスクは自動的に [解決済み] に移行されます。変更要求の状況および状況同期の詳細については、「修復タスクからの変更要求の作成」を参照してください。

IT 修復ワークスペースでの修復タスクの分割

修復タスク (VUL、AVUL、CVUL、CRG) から、レコードのサブセットを特定し、それらの新しい修復タスクを作成します。

始める前に

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion
- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

このタスクについて

修復タスクの [概要] タブで個々のレコードを選択して、新しい修復タスクに移動できます。

既存の修復タスクのレコード (VIT、AVIT、CVIT、CTR) を新しいタスクに分割するユースケースには、次のような例が考えられます。

- 分割されたタスクに対して変更要求を作成する。
- 分割されたタスクをアサイン先グループの別のユーザーに再アサインする場合。
- 特定の構成アイテム (CI) に関する一部の脆弱性がターゲット日までに修正できないことがわかっているため、分割されたタスクの保留または例外を要求します。

クラシック環境および v15.0 より前のバージョンの 脆弱性対応 での変更の要求と修復タスクの分割の詳細については、「修復タスクの分割」を参照してください。

注:
脆弱性対応 の v19.0 以降では、次の用語の名前が変更されました。

用語の変更

v19.0 より前の用語	v19.0 以降の用語
テスト結果グループ	修復タスク
構成の問題	構成テスト結果
ポリシー	テストグループ

手順

1. 次のように移動する。 ワークスペース > **IT** 修復ワークスペース.
2. ホームページまたはリストページから修復タスク (VUL、AVUL、CVUL、CRG) を開きます。
3. [概要] タブで、新しい修復タスクに移動するレコード (VIT、AVIT、CVIT、CTR) を選択します。
4. [タスクを分割] をクリックします。
5. 表示されるダイアログに、リストから選択したレコードの数 (VIT、AVIT、CVIT、CTR) が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [タスクを分割] を再度クリックします。
   新しい修復タスクへのリンクを含む確認メッセージが表示されます。

   または、条件ビルダーを使用してレコード (VIT、AVIT、CVIT、CTR) をフィルタリングすることもできます。

7. 分割する修復タスクを見つけます。
8. 右側の UI アクションボタンで、[タスクを分割] をクリックします。
   しばらくすると、条件ビルダーが表示されます。
9. 表示されるモーダルで、条件ビルダーを使用して、新しい修復タスクに追加するレコードのサブセット (VIT、AVIT、CVIT、CTR) を特定します。
10. [タスクを分割] をクリックします。
    条件に一致するレコードがないというメッセージが表示された場合は、条件を調整して [タスクを分割] を再度クリックする必要があります。必要に応じて、[簡単な説明] フィールドを編集します。このフィールドは、新しい修復タスクを作成後に見つけるのに役立ちます。

    レコードが条件に一致する場合、一致するレコードの数がメッセージに表示されます。

11. オプション: [アイテムをプレビュー] リンクをクリックして、フィルター条件に一致するレコードを表示します。
    新しい修復タスクが新しいタブとして表示されます。

脆弱性一致アイテムまたは修復タスクの誤検出を要求する

IT 修復ワークスペース のホスト脆弱性一致アイテム (VIT)、アプリケーション脆弱性一致アイテム (AVIT)、コンテナ脆弱性一致アイテム (CVIT)、または修復タスク (VUL、AVUL、CVUL、CRG) の誤検出要求を示します。誤検出とは、誤った分類、不適切なロジック、スキャナーのアルゴリズムなどの状況が原因で、システムに脆弱性が存在することをスキャナーが誤って報告する状態です。

始める前に

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion
- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

このタスクについて

一連のテスト結果の誤検出を要求する方法については、「 一連のテスト結果の誤検出を要求する」を参照してください。

手順

1. 次のように移動する。 ワークスペース > **IT** 修復ワークスペース.
2. [リスト] アイコン ( ) を選択します。
3. 修復タスク (VUL、AVUL、CVUL、CRG) または脆弱性一致アイテム (VIT、AVIT、CVIT) を選択します。
4. [誤検出としてマーク] を選択します。
5. 要求に関する情報を入力します。
6. [承認を要求] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. 承認者に要求に関する追加情報を入力し、[送信] を選択します。

> **注:**
> [アンケートに回答] モーダルは、[例外管理構成] フォームで [誤検出をマークするアンケートを有効化] チェックボックスがオンの場合にのみ表示されます。詳細については「脆弱性対応 の例外管理の設定」「アプリケーション脆弱性対応 の例外管理の設定」「コンテナ脆弱性対応 の例外管理の設定」「コンフィグレーションコンプライアンス の例外管理の設定」を参照してください。

タスクの結果

脆弱性一致アイテム (IT、AVIT、CVIT) や修復タスク (VUL、AVUL、CVUL) のステータスが [レビュー中] に移行します。

承認要求が送信され、承認者は承認要求のメール通知を受け取ります。

要求が承認または却下されるとメール通知が届きます。

次のタスク

IT 修復ワークスペースのリストページで、次に移動します: 例外要求 > **My requests** (自分の要求) をクリックし、対応するステータス変更承認レコード (VCA#) を開き、[承認ステータス] 列で要求のステータスを確認します。

承認ステータス	レコード (VIT、AVIT、CVIT)	修復タスク (VUL、AVUL、CVUL、CRG)
承認済み	レコードのステータスが [クローズ済み] に移行し、[理由] が [誤検出] になります。	修復タスクのステータスが [クローズ済み] に移行し、[理由] が [誤検出] になります。ステータスが、適切に修復タスクのレコードにロールダウンされます。 修復タスクの [詳細] タブに移動し、必要に応じて [期限] フィールドで誤検出の有効期限を設定します。指定された日付後、修復タスクは [オープン] ステータスに戻り、ステータスがテスト結果にロールダウンされます。
却下	レコードのステータスは変わりません。	修復タスクやレコードのステータスが、前のステータスに戻ります。

レコードや修正タスクのアクティビティストリームでは、誤検出要求のワークフロー全体を表示できます。

関連情報

誤検出の概要

一連のテスト結果の誤検出を要求する

IT 修復ワークスペースの修復タスク内の一連のテスト結果に対して誤検出要求を発生させます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタスクについて

修復タスク内の一連のテスト結果の誤検出を要求するには、次の条件を満たす必要があります。

- 脆弱性対応 のバージョン 22.0 をインストールする必要があります。
- 選択したテスト結果のうち少なくとも 1 つはアクティブ状況である必要があります
- 修復タスクには、少なくとも 2 つのテスト結果が必要です
- 少なくとも 1 つのテスト結果が選択されていません

始める前に

必要なロール：sn_vulc.remediation_owner

手順

1. 次のように移動する。 ワークスペース > **IT** 修復ワークスペース.
2. [リスト] アイコン ( ) を選択します。
3. [リスト] ページで、 コンフィグレーションコンプライアンス 修復タスクを選択します。
4. [概要] 関連リストの [テスト結果] タブで、誤検出としてマークするテスト結果を選択します。
5. [構成テスト結果] タブの [誤検出としてマーク **]** ボタンを選択します。
6. 表示されるダイアログで、要求に関する情報を入力し、[承認要求] を選択します。
7. [アンケートに回答] モーダルで質問に回答して、要求に関する追加情報を承認者に提供し、[送信] を選択します。

> **注:**
> [アンケートに回答] モーダルは、[例外管理構成] フォームで [誤検出をマークするアンケートを有効化] チェックボックスがオンの場合にのみ表示されます。[アンケート構成] フォームの構成について、詳しくは「コンフィグレーションコンプライアンス の例外管理の設定」を参照してください。

タスクの結果

選択したテスト結果が新しい修復タスクに移動し、承認要求が送信されます。タスク番号は、古い修復タスクの アクティビティストリーム に表示されます。承認者は、承認要求のメール通知を受け取ります。

要求の承認または却下に関するのメール通知が届きます。テスト結果や修正タスクのアクティビティストリームでは、誤検出要求のワークフロー全体を表示できます。

次のタスク

1. IT 修復ワークスペースの [リスト] ページで、 例外要求 > **My requests** (自分の要求).
2. 対応するステータス変更の承認レコード (VCA#) を開き、[承認ステータス] 列で要求のステータスを確認します。

承認ステータス	結果
承認済み	新しい修復タスクのステータスが [クローズ済み] に移行し、[理由] が [誤検出] になります。
却下	新しい修復タスクのステータスが [オープン] に変わります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 要求が承認されたら、新しい修復タスクの [詳細] タブに移動し、必要に応じて [期限] フィールドで誤検出の有効期限を設定します。

   指定された日付後、修復タスクは [オープン] ステータスに戻り、ステータスがテスト結果にロールダウンされます。

IT 修復ワークスペースで例外を要求する

ホスト脆弱性一致アイテム (VIT)、アプリケーション脆弱性一致アイテム (AVIT)、コンテナ脆弱性一致アイテム (CVIT)、および修復タスク (VUL、AVUL、CVUL、CRG) の例外を IT 修復ワークスペースから要求します。

始める前に

必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion
- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

このタスクについて

脆弱性によっては、既存のパッチ、修正、またはソリューションがないこともあります。または、修復タスクをそのターゲット日までに解決できないと判断する場合があります。公開されている脆弱性管理やセキュリティポリシー、標準、指針に修正が準拠できない場合は、例外を要求できます。

自分にアサインされた IT 修復ワークスペース から、修復タスク (VUL、AVUL、CVUL、CRG) および脆弱性一致アイテム (VIT、AVIT、CVIT) の例外を要求できます。

注:
脆弱性対応 の v19.0 以降では、次の用語の名前が変更されました。

用語の変更

v19.0 より前の用語	**v19.0** 以降の用語
テスト結果グループ	修復タスク
構成の問題	構成テスト結果
ポリシー	テストグループ

バージョン 18.0 以降では、アプリケーション脆弱性一致アイテムとコンテナ脆弱性一致アイテムの例外を要求できます。

クラシック環境での例外の要求の詳細については、「修復タスクに対する例外の要求」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > **IT** 修復ワークスペース.
2. [リスト] アイコンを選択します。
3. [修復タスク] リストで、例外を要求する修復タスク (VUL、AVUL、CVUL、CRG) またはレコード (VIT、AVIT、CVIT) を開きます。
4. 右側の UI アクションボタンで、[例外の要求 **(Request Exception)]** をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. 表示されるダイアログで、例外の終了日を入力し、リストから理由を選択して、その他の必要な情報を追加します。
6. [例外の要求] をクリックします。
7. [アンケートに回答] モーダルで、質問に回答し、[送信] をクリックします。

   注:
   [アンケートに回答] モーダルは、[例外管理構成] フォームで [例外を要求するアンケートを有効化] チェックボックスがオンの場合にのみ表示されます。

   要求が承認を求めて正常に送信されたことを示すメッセージが表示されます。

   修復タスクの例外要求は、デフォルトの 2 レベルの承認フローを使用して承認されます。要求はレベル 1 の承認者によって承認されると、レベル 2 の承認者に送信されます。

   - 例外要求がオープンな間は、修復タスクまたはレコードは [レビュー中] に移行します。
   - 要求が承認されると、修復タスクまたはレコードは [保留] に移行されます。
   - 例外要求レコード (VCA#) は、例外要求が承認された後にクローズされます。

   承認要求のステータスを表示するには、リストページの [例外要求] で、[自分の要求] をクリックします。リストからレコードまたは修復タスクを開くと、要求の番号 (VCA#) が表示されます。

   - 要求が却下されると、要求レコード (VCA#) では、リストビューの [自分の要求] の下にある [承認ステータス] 列に [却下] と表示されます。
   - このアイテムを引き続き保留する場合は、新しい例外要求を送信する必要があります。

IT 修復ワークスペースで GRC: ポリシーとコンプライアンス管理 を使用して例外を要求する

ホスト脆弱性一致アイテム (VIT)、アプリケーション脆弱性一致アイテム (AVIT)、コンテナ脆弱性一致アイテム (CVIT)、または修復タスク (VUL、AVUL、CVUL、CRG) のポリシー例外を IT 修復ワークスペースから要求します。

始める前に
必要なロール：

- ホスト脆弱性一致アイテム (VIT) の場合、sn_vul.remediation_owner
- アプリケーション脆弱性一致アイテム (AVIT) の sn_vul.app_security_champion
- コンテナ脆弱性一致アイテム (CVIT) の sn_vul_container.remediation_owner
- 構成テスト結果 (CTR) の sn_vulc.remediation_owner

このタスクについて

注:
脆弱性対応 の v19.0 以降では、次の用語の名前が変更されました。

用語の変更

v19.0 より前の用語	v19.0 以降の用語
テスト結果グループ	修復タスク
構成の問題	構成テスト結果
ポリシー	テストグループ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 ワークスペース > **IT** 修復ワークスペース.
2. アプリケーションナビゲーターで、[リスト] アイコン ( )
3. [リスト] ページの [ホスト脆弱性一致アイテム]、[アプリケーション脆弱性一致アイテム]、[コンテナ脆弱性一致アイテム]、または [修復タスク (VUL、AVUL、CVUL、CRG)] で、例外を要求するレコードを選択します。
   選択するレコードは、[オープン]、[調査中]、または [実装待ち] ステータスである必要があります。
4. [例外の要求] ボタンを選択します。
5. フォームのフィールドに入力します。
   フォームフィールドの詳細については、「ポリシー例外の [例外の要求] フォームフィールド」を参照してください。
6. [例外の要求] ボタンを選択します。
7. [アンケートに回答] モーダルで、質問に回答して要求に関する追加情報を提供し、[送信] を選択します。

   注:
   [アンケートに回答] モーダルは、アンケートの詳細がそれぞれの統合レジストリに追加された場合にのみ表示されます。

   要求が承認を求めて正常に送信されたことを示すメッセージが表示されます。

   ポリシー例外統合および修復オーナーとコンプライアンスマネージャー間の引き渡しの詳細については、「ポリシーとコンプライアンス管理オプションのセットアップ」を参照してください。

脆弱性一致アイテムまたは修復タスクのリスク削減の要求

IT 修復ワークスペース内のホスト脆弱性一致アイテムまたは修復タスクのリスク削減を要求します。

始める前に

必要なロール： sn_vul.remediation_owner

このタスクについて

脆弱性対応 v21.0 以降では、次のアイテムについてのみリスク削減を要求できます。

- 修復タスクCVE に対してリスク削減が有効になっているかどうかに関係なく そのすべての脆弱性一致アイテムが 同じ共通脆弱性エントリ (CVE) 関連付けられている場合のみ 。
- リスク削減が有効になっているサードパーティ (TPE)。

注:
補完コントロール機能は、ホストの脆弱性に対してのみ使用できます。

手順

1. 次のように移動する。 ワークスペース > **IT** 修復ワークスペース.
2. [リスト] アイコン ( ) を選択します。
3. [リスト] ページで、ホスト脆弱性一致アイテムまたは修復タスクを開きます。
4. [その他のオプション] アイコンを選択し、[例外の要求] を選択します。
5. [例外の要求] フォームで、フィールドに入力します。
   フィールド値の説明については、「リスク削減の [例外の要求] フォーム」を参照して ください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [例外の要求] ボタンを選択します。
7. [アンケートに回答] モーダルが表示された場合は、質問に回答して要求に関する追加情報を提供し、[送信] を選択します。

> **注:**
> [アンケートに回答 (Take Questionnaire)] モーダルは、例外管理にアンケートが有効である場合にのみ表示されます。詳細については、「脆弱性対応 の例外管理の設定」を参照してください。

タスクの結果
要求が承認を求めて正常に送信されたことを示すメッセージが表示されます。要求についての通知が承認者に送信されます。

- 要求が延期とリスク軽減の場合:
  - 保留とリスク削減のために、2 つのステータス変更承認 (VCA#) が作成されます。
  - レコードのステータスが [レビュー中] に変更されます。
- 要求がリスク削減のみを目的としている場合:
  - ステータス変更承認 (VCA#) が作成されます。
  - ステータスは変わりません。

要求の承認または却下時には、通知が届きます。承認プロセスの詳細については、「Vulnerability Manager ワークスペース で要求を承認または却下」を参照してください。

リスク削減要求が承認されたときに、修復タスクと脆弱性一致アイテムの [リスク削減の期限日] がどのように更新されるかの詳細については、「リスクスコアと有効期限に対する補完コントロールの影響」を参照してください。

関連情報

リスク削減の補完コントロールについて

CVE または TPE のリスク削減を無効または有効にする

補完コントロールをライブラリに追加する

リスクスコアと有効期限に対する補完コントロールの影響

IT 修復ワークスペースでの脆弱性一致アイテムと修復タスクの再スキャン

スケジュールされたスキャンサイクル間で脆弱性一致アイテムが修正されたことを確認します。Now Platform の IT 修復ワークスペースからオンデマンドで再スキャンを開始します。

再スキャンにより、修復アクティビティ、パッチ、およびその他のアクションによって構成アイテム (CI) の特定の脆弱性が正常に修正されたことを確認できます。

再スキャンは、IT 修復ワークスペースの以下の統合でサポートされています。詳細は、以下のトピックを参照してください。

- 脆弱性対応 ワークスペースからの Qualys 脆弱性一致アイテムの再スキャン
- 脆弱性対応 ワークスペースからの Rapid7 脆弱性一致アイテムの再スキャン
- 脆弱性対応 ワークスペースからの Tenable.io および Tenable.sc 脆弱性一致アイテムの再スキャン

必要なロール：IT 修復ワークスペースの sn_vul.remediation_owner。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性対応 ワークスペースからの **Qualys** 脆弱性一致アイテムの再スキャン

スケジュールされたスキャンサイクル間で脆弱性一致アイテムが修正されたことを確認します。Now Platform インスタンスの IT 修復ワークスペース からオンデマンドで Qualys 製品の再スキャンを開始します。

始める前に
クラシック環境から Qualys 製品の再スキャンを開始するには、「Qualys 脆弱性統合の再スキャンの開始」を参照してください。

Qualys スキャナーは、脆弱性対応 アプリケーションではデフォルトで無効になっています。これらのアプリケーションをソースとする脆弱性一致アイテムまたは修復タスクから再スキャンを実行しようとすると、[再スキャン] ボタンは使用できません。

これらのスキャナーをアクティブにするには、sn_vul.vulnerability_admin ロールのユーザーとして、次の操作を実行します。

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性スキャン > スキャナー.
2. アクティブ化するスキャナー製品を見つけ、レコードをクリックして開きます。
3. [アクティブ] チェックボックスをオンにします。
4. [更新] をクリックします。

   アクティブ化した製品は、次のインポート後に脆弱性一致アイテムおよび修復タスクレコードの [ソース] フィールドに表示され、[再スキャン] は UI アクションとして使用できます。

Qualys スキャナーのセットアップの詳細については、「スキャナーアプライアンスのセットアップ」および「詳細な Qualys 構成と変更」を参照してください。

- Now Platform の IT 修復ワークスペース から、Qualys 製品をソースとする脆弱性一致アイテムおよび修復タスクの再スキャンをオンデマンドで開始できます。
- 修復タスクレコードでは、レコードは [クローズ済み] を除くあらゆるステータスをとることが可能ですが、関連する VI はすべてソースが Qualys 製品である必要があります。
- 脆弱性一致アイテムおよび修復タスクレコードから IT 修復ワークスペースで再スキャンを開始するには、これらのレコードがアサインされている必要があります。

必要なロール：

- IT 修復ワークスペース の sn_vul.remediation_owner。
- sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin (脆弱性マネージャーのワークスペースから)。

手順

1. 割り当てられた脆弱性一致アイテムまたは修復タスクに移動して開きます。

   注:
   再スキャンを開始する修復タスクを選択すると、そのレコードに関連付けられているすべての VI がスキャンされます。

2. レコードの右上にある [再スキャン] をクリックします。
3. [再スキャン] モーダルで、オプションプロファイルを選択します。
   Now Platform から Qualys スキャンを開始する場合は、オプションプロファイルが必要です。オプションプロファイルには Qualys スキャン設定が含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [再スキャン] モーダルで、[再スキャンを要求] をクリックします。
   「スキャン要求を処理しています」というメッセージが表示されます。
5. メッセージの [ステータスを表示] リンクをクリックして、スキャンの進行状況を表示します。

   スキャンレコード (VSCAN#) が表示されます。スキャン番号を含むレコードヘッダーの下の関連アイテムリストに次の情報が表示されます。

   - [詳細] リストには、親スキャンのスキャン番号、スキャナーソース、およびステータスが表示されます。完了したスキャンと失敗したスキャンは [スキャンサマリー] セクションに表示されます。
   - [スキャン] リストには、子スキャンとその状況が表示されます。すべての子スキャンが完了すると、親スキャンのステータスが [完了] に移行します。
   - [ソース] リストには、スキャンに使用された脆弱性一致アイテム、関連する構成アイテムと脆弱性、VI のステータス、およびその修復ステータスが表示されます。

   Now Platform® インスタンスは、正常に完了するか設定された追跡期間がタイムアウトするまで、再スキャンステータスを追跡します。

   タイムアウトしてもスキャンは停止しません。タイムアウトは、実際の再スキャンが停止したときではなく、Now Platform® が再スキャンステータスの追跡を停止したときです。

   [クローズ済み]/[修正済み] に移行した、または移行する予定のすべての VI は、Qualys 統合の次のスケジュール済みインポートとともにインポートされます。

脆弱性対応 ワークスペースからの **Rapid7** 脆弱性一致アイテムの再スキャン

スケジュールされたスキャンサイクル間で脆弱性一致アイテムが修正されたことを確認します。Now Platform インスタンスの IT 修復ワークスペースからオンデマンドで Rapid7 製品の再スキャンを開始します。

始める前に

クラシック環境から製品の再スキャンを開始するには、「Rapid7 脆弱性統合の再スキャンの開始」を参照してください。このトピックには、Rapid7 統合インスタンスで統合パラメーターを使用してスキャンをスケジュールする方法に関する情報も含まれています。

Rapid7 スキャナーは、脆弱性対応 アプリケーションではデフォルトで無効になっています。Rapid7 アプリケーションをソースとする脆弱性一致アイテムまたは修復タスクから再スキャンを実行しようとすると、[再スキャン] ボタンは使用できません。

これらのスキャナーをアクティブにするには、sn_vul.vulnerability_admin ロールのユーザーとして、次の操作を実行します。

1. 次のように移動する。 **All** (すべて) > 脆弱性対応 > 脆弱性スキャン > スキャナー.
2. アクティブ化するスキャナー製品を見つけ、レコードをクリックして開きます。
3. [アクティブ] チェックボックスをオンにします。
4. [更新] をクリックします。

   アクティブ化した製品は、次のインポート後に脆弱性一致アイテムおよび修復タスクレコードの [ソース] フィールドに表示され、[再スキャン] は UI アクションとして使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- Now Platform の IT 修復ワークスペースから、Rapid7 InsightVM 製品をソースとする脆弱性一致アイテムおよび修復タスクの再スキャンをオンデマンドで開始できます。
- 修復タスクレコードでは、レコードは [クローズ済み] を除くあらゆるステータスをとることが可能ですが、関連する VI はすべてソースが Rapid7 製品である必要があります。
- 脆弱性一致アイテムおよび修復タスクレコードから IT 修復ワークスペースで再スキャンを開始するには、これらのレコードがアサインされている必要があります。

必要なロール：

- IT 修復ワークスペースの sn_vul.remediation_owner
- sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin (脆弱性マネージャーのワークスペースから)

手順

1. 割り当てられた脆弱性一致アイテムまたは修復タスクに移動して開きます。

   注:
   再スキャンを開始する修復タスクを選択すると、そのレコードに関連付けられているすべての VI がスキャンされます。

2. レコードの右上にある [再スキャン] をクリックします。
3. [再スキャンを確認] モーダルで、[再スキャンを要求] をクリックします。
   「スキャン要求を処理しています」というメッセージが表示されます。
4. メッセージの [ステータスを表示] リンクをクリックして、スキャンの進行状況を表示します。

   スキャンレコード (VSCAN#) が表示されます。スキャン番号を含むレコードヘッダーの下の関連アイテムリストに次の情報が表示されます。

   - [詳細] リストには、親スキャンのスキャン番号、スキャナーソース、およびステータスが表示されます。完了したスキャンと失敗したスキャンは [スキャンサマリー] セクションに表示されます。
   - [スキャン] リストには、子スキャンとその状況が表示されます。すべての子スキャンが完了すると、親スキャンのステータスが [完了] に移行します。
   - [ソース] リストには、スキャンに使用された脆弱性一致アイテム、関連する構成アイテムと脆弱性、VI のステータス、およびその修復ステータスが表示されます。

   Now Platform® インスタンスは、正常に完了するか設定された追跡期間がタイムアウトするまで、再スキャンステータスを追跡します。

   タイムアウトしてもスキャンは停止しません。タイムアウトは、実際の再スキャンが停止したときではなく、Now Platform® が再スキャンステータスの追跡を停止したときです。

   [クローズ済み]/[修正済み] に移行した、または移行する予定のすべての VI は、Rapid7 統合の次のスケジュール済みインポートとともにインポートされます。

脆弱性対応 ワークスペースからの **Tenable.io** および **Tenable.sc** 脆弱性一致アイテムの再スキャン

スケジュールされたスキャンサイクル間で脆弱性一致アイテムが修正されたことを確認します。Now Platform インスタンスの IT 修復ワークスペースからオンデマンドで Tenable.io および Tenable.sc 製品の再スキャンを開始します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
脆弱性対応 のクラシック環境から Tenable.io および Tenable.sc 製品の再スキャンを開始するには、「Tenable.sc 統合の再スキャンの開始」および「Tenable.io 統合の再スキャンの開始」を参照してください。

Now Platform から再スキャンを実行するには、Tenable 認証情報が必要です。Tenable.io および Tenable.sc のスキャナーを設定し、Tenable から認証情報をインポートする方法の詳細については、「セットアップアシスタントを使用した Tenable 脆弱性統合の構成」を参照してください。

- Now Platform の IT 修復ワークスペースから、Tenable.io または Tenable.sc 製品をソースとする脆弱性一致アイテムおよび修復タスクの再スキャンをオンデマンドで開始できます。
- 修復タスクレコードでは、レコードは [クローズ済み] を除くあらゆるステータスをとることが可能ですが、関連する VI はすべてソースが Tenable.io または Tenable.sc 製品である必要があります。
- 脆弱性一致アイテムおよび修復タスクレコードから IT 修復ワークスペース で再スキャンを開始するには、これらのレコードがアサインされている必要があります。

必要なロール：
- IT 修復ワークスペース の sn_vul.remediation_owner
- sn_vul.vulnerability_analyst または sn_vul.vulnerability_admin (脆弱性マネージャーのワークスペースから)

手順
1. 割り当てられた脆弱性一致アイテムまたは修復タスクに移動して開きます。

   注:
   再スキャンを開始する修復タスクを選択すると、そのレコードに関連付けられているすべての VI がスキャンされます。

2. レコードの右上にある [再スキャン] をクリックします。
   再スキャンのインスタンスとスキャナーへのアクセスに使用するスキャナー認証情報を選択するように求められます。表示される認証情報は、Tenable.io および Tenable.sc スキャン認証情報統合によってインポートされた認証情報です。
3. モーダルで、検索アイコンをクリックします。

   表示される [スキャン認証情報を選択] モーダルで、列見出しのフィルターを使用して、名前、インスタンス (1 つまたは複数)、使用する認証情報タイプを選択します。

   詳細については、次の表を参照してください。

4. 更新された [再スキャン] モーダルで、[再スキャンを要求] をクリックします。
   「スキャン要求を処理しています」というメッセージが表示されます。
5. メッセージの [ステータスを表示] リンクをクリックして、スキャンの進行状況を表示します。

   スキャンレコード (VSCAN#) が表示されます。スキャン番号を含むレコードヘッダーの下の関連アイテムリストに次の情報が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [詳細] リストには、親スキャンのスキャン番号、スキャナーソース、およびステータスが表示されます。完了したスキャンと失敗したスキャンは [スキャンサマリー] セクションに表示されます。
- [スキャン] リストには、子スキャンとその状況が表示されます。すべての子スキャンが完了すると、親スキャンのステータスが [完了] に移行します。
- [ソース] リストには、スキャンに使用された脆弱性一致アイテム、関連する構成アイテムと脆弱性、VI のステータス、およびその修復ステータスが表示されます。

Now Platform® インスタンスは、正常に完了するか設定された追跡期間がタイムアウトするまで、再スキャンステータスを追跡します。

タイムアウトしてもスキャンは停止しません。タイムアウトは、実際の再スキャンが停止したときではなく、Now Platform® が再スキャンステータスの追跡を停止したときです。

[クローズ済み]/[修正済み] に移行した、または移行する予定のすべての VI は、Tenable.io または Tenable.sc 統合の次のスケジュール済みインポートとともにインポートされます。

IT 修復ワークスペース の参照情報

次のトピックでは、IT 修復ワークスペース にあるフォームやレコードのフィールドデータの他に、リンク、参照情報について説明します。

[store-future: BEGIN review]

[すべて] メニューから IT 修復ワークスペース にリダイレクトする

アドミニストレーターが *sn_vul_cmn_ws.navigate_to_workspace* システムプロパティを true に設定した場合、[すべて] メニューから [脆弱性対応]、[アプリケーション脆弱性対応]、[コンテナ脆弱性対応]、および [コンフィグレーションコンプライアンス] モジュールで事前定義されたフィルターリンクを選択すると、IT 修復ワークスペースにリダイレクトされます。

の [リスト] ページにリダイレクトする IT 修復ワークスペース

sn_vul.remediation_owner ロールを持つユーザーが、脆弱性対応モジュールで次の事前定義されたフィルターリンクを選択する場合、次の場所に移動します。 **All** (すべて) > 脆弱性対応の場合、これらのリンクは IT 修復ワークスペースのリストページで開きます。

- 修復タスク:自分にアサイン済み、所属グループにアサイン済み
- 脆弱性一致アイテム:自分にアサイン済み、所属グループにアサイン済み
- ライブラリ - NVD、CWE、およびサードパーティ
- ソリューション:すべて、最高優先度、および脆弱性一致アイテムあり
- 自分の承認

sn_vul_container.remediation_owner ロールを持つユーザーが、Container Vulnerability Response モジュールで次の事前定義されたフィルターリンクを選択する場合、次の場所に移動します。 **All** (すべて) > **Container Vulnerability Response**の場合、これらのリンクは IT 修復ワークスペースのリストページで開きます。

- コンテナ修復タスク:アクティブ、自分にアサイン済み、所属グループにアサイン済み、およびすべて
- コンテナ脆弱性一致アイテム:自分にアサイン済み、所属グループにアサイン済み
- 自分の承認
- ライブラリ - NVD、CWE、およびサードパーティ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

sn_vul.app_security_champion ロールを持つユーザーが、アプリケーション脆弱性対応モジュールで次の事前定義されたフィルターリンクを選択する場合、次の場所に移動します。 **All** (すべて) > アプリケーション脆弱性対応の場合、これらのリンクは IT 修復ワークスペースのリストページで開きます。

- 修復タスク:アクティブ、自分にアサイン済み、所属グループにアサイン済み、およびすべて
- 脆弱性一致アイテム:自分にアサイン済み、所属グループにアサイン済み
- 自分の承認
- ライブラリ - NVD、CWE、およびサードパーティ
- ペネトレーションテストアセスメント要求:アクティブ、すべて自分にアサイン済み、所属グループにアサイン済み
- ペネトレーションテスト結果:アクティブ、検証保留中、自分にアサイン済み、自分のグループにアサイン済み、すべて

sn_vulc.remediation_owner ロールを持つユーザーが、コンフィグレーションコンプライアンスモジュールで次の事前定義されたフィルターリンクを選択する場合、次の場所に移動します。 **All** (すべて) > コンフィグレーションコンプライアンスの場合、これらのリンクは IT 修復ワークスペースのリストページで開きます。

- 修復タスク:自分のオープンタスク、すべてのオープンタスク、複数の保留、およびすべてのタスク
- テスト
- テストグループ
- サポートデータ - 信頼できるソースとテクノロジー

[End]

[変更要求の作成] フォームのフィールド

次の表に、[変更要求の作成 (Create change request)] フォームのフィールドとその説明を示します。

フィールド	説明
変更タイプ	通常 (Normal)：デフォルトです。 標準 (Standard)：次の 2 つの追加フィールドが表示されます。 標準的な変更カテゴリ：リストからカテゴリを選択します 標準的な変更テンプレート：この変更要求に使用するテンプレートを選択リストから選択します 緊急 (Emergency)：重要な優先度
CI を変更要求に追加	デフォルトでは有効です。有効にすると、変更要求により、この修復作業のアクティブな脆弱性一致アイテムに属する構成アイテム (CI) がこの変更要求に追加されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
優先度	[高] がデフォルトです。リストから優先度を選択します。
アサイン先グループ	アサイン先グループは、デフォルトではウォッチトピックから取得されます。検索アイコンをクリックし、モーダルから別のアサイン先グループを選択します。
終了予定日	カレンダーのアイコンをクリックして、終了予定日を選択します。
アサイン先	デフォルトでは現在のユーザーが修復タスクにアサインされます。検索アイコンをクリックし、モーダルから別のユーザーを選択します。
簡単な説明	簡単な説明は修復タスクから取得されます。テキストをクリックして編集します。
説明	説明は修復タスクから取得されます。テキストをクリックして編集します。
理由	修復タスクから取得された根拠。テキストをクリックして編集します。
実装計画	優先ソリューション情報が事前入力されています (利用可能な場合)。ソリューションを表示するか、正当化の計画を入力します。

関連情報

IT 修復ワークスペースで変更要求を作成する

ポリシー例外の [例外の要求] フォームフィールド

次の表は、ポリシー例外の [例外の要求] フォームで入力する必要があるフィールドを示しています。

[例外の要求] フォーム

フィールド	説明
ポリシー	例外を要求している脆弱性管理ポリシー。
コントロール目標	選択したポリシーに関連付けられたコントロール目標。ポリシーが選択されていない場合は、すべてのコントロール目標が一覧表示されます。
有効期限開始	例外が開始される日付。デフォルト値は現在の日付です。過去の日付にすることはできません。
有効期限	ポリシー例外が期限切れになり、脆弱性一致アイテムまたはグループのステータスが [保留] から [オープン] に変更される日付。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[例外の要求] フォーム (続く)

フィールド	説明
	注: ポリシー例外が有効である日数は、ポリシーに設定した [最大例外期間 (日数)] フィールドの値を超えることはできません。詳細については、「ポリシーの作成」を参照してください。
理由	例外を要求する理由。
正当性	この例外が要求されている理由に関連する詳細。このフィールドは修復オーナーが入力する必要があります。

関連情報

IT 修復ワークスペースで GRC: ポリシーとコンプライアンス管理 を使用して例外を要求する

リスク削減の [例外の要求] フォーム

次の表は、リスク削減要求の [例外の要求] フォームで入力する必要があるフィールドを示しています。

[例外の要求] フォーム

フィールド	説明
理由	例外要求の理由。リスク削減要求に対して [コントロールの緩和を実施] を選択します。 理由の新しい選択肢を追加する方法については、「ポリシー理由のマッピングの定義」を参照してください。
保留の要求	レコードを保留します。デフォルトでは、このフィールドが選択されます。 注: このフィールドは、[理由] フィールドで [コントロールの緩和を実施] オプションが選択されている場合にのみ表示されます。
リスク削減の要求	リスクスコア削減を要求できます。 注: このチェックボックスは、[理由] フィールドで [コントロールの緩和を実施] オプションが選択されている場合にのみ表示されます。
現在のリスク評価	現在のリスクの重大度。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[例外の要求] フォーム (続く)

フィールド	説明
	注: このフィールドは、[リスク削減の要求] チェックボックスがオンになっている場合にのみ表示されます。
望ましいリスク評価	レコードに割り当てる新しいリスク評価。 要求が承認されると、このリスク評価範囲内の最も高いリスクスコアがレコードに適用されます。 **注:** このフィールドは、[リスク削減の要求] チェックボックスがオンになっている場合にのみ表示されます。
補完コントロールの選択	リスク評価の引き下げを要求する理由。
期限	保留またはリスク削減要求の有効期限が切れる日付。 例外要求の有効期限が切れると、次のようになります。 • レコードが [オープン] ステータスに戻ります。 • 補完コントロールの有効期限が切れます。 • 計算済みスコアは、引き下げられたスコアの代わりになります。
正当性に関するメモ	この要求が行われている理由に関連する詳細情報。

関連情報

脆弱性一致アイテムまたは修復タスクのリスク削減の要求

脆弱性アセスメントのワークスペースの詳細

脆弱性アセスメントのワークスペースは、脆弱性イベントマネージャー用に設計されており、エクスポージャーアセスメントを実行し、特にゼロデイイベントなどの重大な脆弱性イベント中に重大な脆弱性イベントを積極的に管理します。

重大な脆弱性が特定されたら、脆弱性イベントマネージャーはこの脆弱性に関連付けられている潜在的な影響とリスクを評価できます。アナリストは、影響を受けるシステム、アプリケーション、またはネットワークコンポーネントを分析して、組織内での重大度と発生する可能性がある攻撃ベクトルを把握できます。

脆弱性アセスメントのワークスペースには、次のものが含まれています。

[エクスポージャーアセスメント] ページ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性や脆弱なソフトウェアにさらされている資産の詳細なヴィジビリティを提供します。エクスポージャーアセスメント機能は、以下を提供します。

- 脆弱性の影響を受ける資産と影響を受けるソフトウェアのヴィジビリティ
- 単一の CVE または脆弱なソフトウェアに対してスタンドアロン評価を実行する機能
- CISA の既知の悪用された脆弱性 CVE の影響を受ける資産のヴィジビリティ
- 追加のディスカバリーモデルと資産からのエクスポージャーについてのヴィジビリティ
- 脆弱性一致アイテムの作成機能

[脆弱性アセスメント] ページ

[脆弱性危機管理]ワークフローを使用して、アセスメントから解決までの脆弱性危機イベントを処理できる [脆弱性アセスメント] ページ。ワークフローを使用すると、関心対象の脆弱性イベントを追跡し、それらに関連するリスクを分析し、複数のインベントリ (ソフトウェアインストールインベントリなど) にわたってエクスポージャーアセスメントを実行し、それを危機として宣言して応答エンゲージメントを昇格させることができます。その後、脆弱性アセスメントレコードを重大なセキュリティインシデントに関連付けて、セキュリティインシデント応答チームが危機に対応できるようになります。

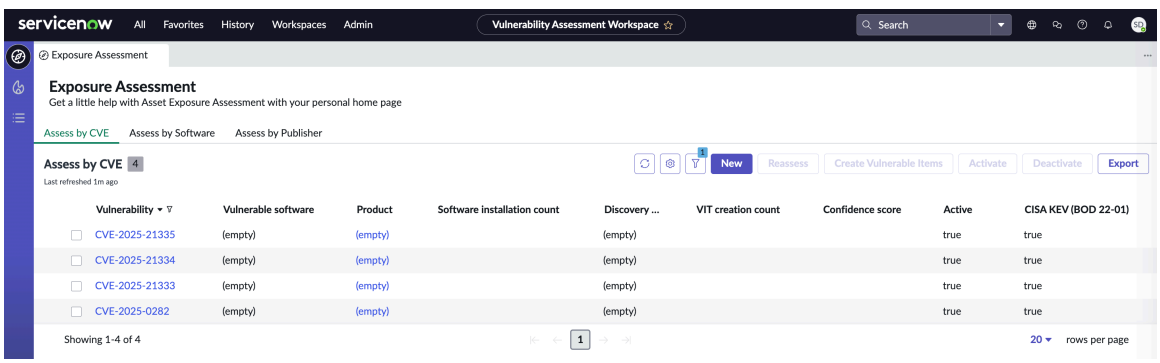
- 重大な脆弱性イベントの脆弱性アセスメントを作成および変更する
- 脆弱性の主要な属性を記録してリスクを計算する
- 脆弱性アセスメントを実行して、エクスポージャーレベルと優先度を決定する
- 脆弱性アセスメントを重大なイベントとして宣言する
- 脆弱性アセスメントを重大なセキュリティインシデントにリンク、提案、または昇格させて、脆弱性アセスメントを重大なセキュリティインシデントに関連付けます。

リストページ

[リスト] ページは、以下を含むライブラリで構成されています。

- CVE
- TPE
- CWE

次の画像に、脆弱性アセスメントのワークスペースのホームページを示します。



エクスポージャーアセスメントの概要

エクスポージャーアセスメントでは、共通脆弱性識別子 (CVE) システムの一部である共通プラットフォーム一覧 (CPE) フレームワークを使用して、脆弱なソフトウェアに対する資産の脆弱性エクスポージャーを評価します。このアセスメントは、ソフトウェアディスカバリーモデルを使用して実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

照合アルゴリズムを使用することで、関連する CPE がソフトウェアディスカバリーモデルに関連付けられてマッピングされ、潜在的なエクスポージャーを特定できるようになります。

CVE またはソフトウェアによるエクスポージャーアセスメントを使用して、次のシナリオでの潜在的な脆弱性へのエクスポージャーを特定できます。

- 従来のスキャナーでは特定できない可能性がある脆弱性
- スキャナーが脆弱性検出の署名を提供する前のゼロデイ脆弱性

エクスポージャーアセスメントは、これらの脆弱性を修復し、脆弱性管理プログラムの成熟度を向上させるための早期警告を提供します。

エクスポージャーアセスメントの前提条件

利用可能バージョン

アプリケーション	バージョン
脆弱性危機管理プラグイン	1.0
脆弱性対応	20.0
脆弱性対応 with NVD	1.3
Vulnerability Response Integration with CISA	1.2
NVD の脆弱性対応統合 **注:** 詳細については、「NVD 統合の概要」を参照してください。	1.3
ソフトウェア資産管理	ソフトウェア資産管理の基盤プラグイン または ソフトウェア資産管理プロ プラグイン

ユースケース

脆弱性アナリスト組織が脆弱性エクスポージャーアセスメントワークスペースを使用する方法の例については、次のユースケースを参照してください。

アセスメントタイプ	使用
CVE による評価	ソフトウェア資産管理 (SAM) とディスカバリーデータを使用して、CVE ごとに脆弱性を評価し、影響を受けるシステムの影響とエクスポージャーを完全に把握します。手動 VIT を作成して修復オーナーにアサインすることで、迅速な修復アクションを実行します。スキャナーは影響を受けるすべてのシステムを検出するわけではないのに対し、通常は攻撃対象領域にあるほとんどのソフトウェアを識別するため、CVE による評価 ディスカバリー 有益です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アセスメントタイプ	使用
ソフトウェアによる評価	CVE が利用できない場合のソフトウェアによる影響を評価して、ソフトウェアがインストールされている CI の数を特定します。ソフトウェアで評価することで、手動で VIT を作成し、正式に公開される前、またはスキャナーで識別される前に修復オーナーにアサインすることで、ゼロデイ脆弱性または重大な脆弱性に積極的に対処できます。
パブリッシャーによる評価	ソフトウェアベンダーによる脆弱性を評価して、ベンダーが公開した CVE について影響を受けるシステムの影響とエクスポージャーを期間内に把握します。公開者による評価は、ベンダーリスクと重大な脆弱性を評価し、プロアクティブな修復を可能にするのに役立ちます。

互換性とシステム要件

脆弱性対応 アプリケーションは ServiceNow Store から入手可能です。エクスポージャーアセスメントモジュールには ITSM ソフトウェア資産管理 アプリケーション (com.snc.asset_management) が必要です。このアプリケーションはすべての資産とソフトウェアライセンスを管理します。このアプリケーションの SAM の基盤 バージョンは、ServiceNow Store からダウンロードする脆弱性対応アプリケーションに含まれています。

重要:
エクスポージャーアセスメントアプリケーションは、次のプラグインと連携します。

- ソフトウェア資産管理の基盤プラグイン (com.snc.sams)
- ソフトウェア資産管理プロ (com.snc.pa.samp)
- ソフトウェア資産管理プラグイン (com.snc.software_asset_management)

SAM の基盤アプリケーションがインスタンスにインストールされていることを確認するには、 システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて) 「com.snc.asset_management」を検索します。アプリケーションがインストールされていない場合は、[インストール] を選択します。脆弱性エクスポージャーアセスメントアプリケーションは Now Platform インスタンスの資産データにアクセスする必要があるため、資産管理アプリケーションには参照するデータが必要です。ソフトウェアディスカバリーモデルテーブル (cmdb_sam_sw_discovery_model) とソフトウェアインストール (cmdb_sam_sw_install) にはデータが必要です。

ソフトウェアディスカバリーモデルの一致するアルゴリズムフィールド

ソフトウェア資産管理プロ アプリケーションでは、ソフトウェアディスカバリーモデルを編集して、[ソフトウェアディスカバリーモデル] フォームで完全に正規化されていない (部分的に正規化済み、公開者が正規化済み、または一致が見つからない) 検出されたソフトウェアを手動で正規化し、調整可能にすることができます。脆弱性対応バージョン 20.0 以降では、ソフトウェア資産管理プロから取得される正規化されたディスカバリーモデルがサポートされています。以下のフィールドは、ソフトウェアディスカバリーモデルの照合アルゴリズムに使用されます。

CPE (ソフトウェアモデル)	**SAM Foundations**	**SAM Professional**
ベンダー	プライマリキー	プライマリキー

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

CPE (ソフトウェアモデル)	SAM Foundations	SAM Professional
製品	表示名	表示名
バージョン	検出されたパブリッシャー	検出されたパブリッシャー
エディション	検出された製品	検出された製品
	検出されたバージョン	検出されたバージョン
		正規化済みパブリッシャー
		正規化済み製品
		正規化されたバージョン

注:
SAM Professional アプリケーションは ServiceNow Store のコア 脆弱性対応 製品には含まれておらず、別途サブスクリプションが必要です。

システムプロパティ

エクスポージャーアセスメントのために CISA で悪用された脆弱性を自動的に処理するには、システムプロパティ *sn_vul_analyst.enable_exposure_for_cisa* を *true*に設定します。デフォルト値は *false* です。

スケジュール済みジョブ

スケジュール済みジョブは次のとおりです。

スケジュール済みジョブの名前	説明
潜在的な脆弱性エクスポージャーのチェック (Check potential vulnerability exposure)	デルタ CVE、ソフトウェア、およびインストールを処理して、エクスポージャーを取得します。 **注:** このスケジュール済みジョブは 12 時間ごとに実行されます。他のスケジュール済みジョブよりも長時間実行されます。
CISA で悪用された CVE をエクスポージャー構成に挿入 (Insert CISA exploited CVE to exposure config)	オンデマンド。エクスポージャー構成 (Exposure Configuration) テーブルに CISA CVE を挿入してエクスポージャーを計算します。
構成済み CVE のエクスポージャーアセスメントの実行 (Run exposure assessment for configured CVEs)	オンデマンド。エクスポージャー構成 (Exposure Configuration) テーブル内のすべての CVE レコードのエクスポージャーを計算します。
ソフトウェアエクスポージャーの実行 (Run software exposure)	オンデマンド。エクスポージャー構成 (Exposure Configuration) テーブル内のすべてのソフトウェアレコードのエクスポージャーを計算します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

主要な用語

- 信頼スコア：信頼スコアは、フィールドの推奨事項を提供する際の信頼性の測定値です。スコアが高いほど、推奨事項の信頼性が高いことを示します。計算の例については、「信頼スコア計算の例」を参照してください。
- ソフトウェアインストール数：脆弱性の影響を受けるソフトウェア資産の数。
- ソフトウェアモデル：製品に関連付けられているソフトウェアモデル。ソフトウェアモデルの結果を確認するには、ソフトウェアモデルをドリルダウンします。詳細については、「Software Asset Management Foundation plugin discovery models and software installations」を参照してください。

[ソフトウェアインストール数] フィールドには、ディスカバリーモデルのステータス (アクティブ / 非アクティブ) に関係なく、ソフトウェアインストールの合計数が表示されます。脆弱性対応 v22.0 以降、新しいシステムプロパティ *sn_vul.filter_inactive_sw_installs* が導入され、非アクティブなソフトウェアのインストールをエクスポージャーアセスメントや[store-future: BEGIN review]脆弱性危機管理 (VCM)[End] から除外するかどうか決めることができます。デフォルトでは、このプロパティはベースシステムで有効になっています。フィルターを有効化すると、アクティブなインストールのみが表示されます。

[ディスカバリーモデル] フィールドには、アクティブなソフトウェアのインストール数が明確に表示されます。これは、[ソフトウェアディスカバリーモデル] テーブルのフィルターがデフォルトで「active=true」であることに基づいて非アクティブなソフトウェアが除外されるためです。このフィールドの数は、[ソフトウェアインストール数] フィールドに表示されるフィルタリング後の数と一致します。[ソフトウェアインストール] フィールドの数は、システムプロパティが更新されても保持されます。更新された数を取得するには、スケジュール済みジョブの *Run exposure assessment for configured CVEs* と *Run software exposure that updates the count* を実行する必要があります。

CVE によるエクスポージャーアセスメント

エクスポージャーアセスメントでは、共通脆弱性識別子 (CVE) を使用して、ソフトウェアディスカバリーモデルを使用した資産のエクスポージャーの評価を行います。CVE によるエクスポージャーアセスメントを使用して、潜在的な脆弱性へのエクスポージャーを特定できます。

CVE によるエクスポージャーの評価については、以下を参照してください。

- エクスポージャー評価のための CVE の追加
- エクスポージャーアセスメントのための CVE の VI の作成
- エクスポージャーアセスメントのための CVE のアクティブ化または非アクティブ化
- エクスポージャーアセスメントのための影響を受ける CI のエクスポート
- 信頼スコア計算の例

エクスポージャー評価のための **CVE** の追加

新しい脆弱性またはゼロデイ脆弱性の影響を評価するために、共通脆弱性識別子 (CVE) をエクスポージャーアセスメントの CVE のエクスポージャー構成リストに追加します。

始める前に

必要なロール：sn_vul_analyst.vul_event_manager

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース > エクスポージャーアセスメント > **CVE** による評価.
2. [**Add**] を選択します。
3. [CVE を追加 (Add CVE)] ダイアログボックスで、リストに追加する CVE を選択して [追加] オプションを選択します。
   既にリストに含まれている CVE が再度追加されることはありません。その他の CVE は CVE のリストに追加されます。

   注:
   フィルターアイコンを選択して [詳細表示] に移動し、表示する CVE を指定します。

4. 既にリストに含まれている CVE の影響を評価するには、次の手順を実行します。

   a. 再評価する CVE のチェックボックスをオンにします。

   b. [再評価] ボタンを選択します。
      更新された詳細情報が各列に表示されます。

エクスポージャーアセスメントのための **CVE** の **VI** の作成

[エクスポージャーアセスメント] ページでの脆弱性アイテム (VI) の作成脆弱性イベントマネージャーはこの VI のリストを分析し、IT チームがこれらの脆弱性にパッチを適用するのに役立つソリューションとパッチを推奨します。

始める前に
必要なロール：sn_vul_analyst.vul_event_manager

このタスクについて
エクスポージャーの評価後に、潜在的なアセスメントのリストが、構成アイテム (CI) の数とともにエクスポージャーアセスメントレコードに表示されます。レコードを選択し、リストアクションで [脆弱性一致アイテムを作成] を選択します。これにより、共通脆弱性識別子 (CVE) がある脆弱なソフトウェアが存在する CI の脆弱性一致アイテム (VI) を作成できます。VI はバックグラウンドで作成されます。このプロセスには時間がかかることがあります。アイテムが作成されたら、VI テーブルに移動して作成されたレコードを確認できます。

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース > エクスポージャーアセスメント > **CVE** による評価.
2. 必要な CVE を選択し、[脆弱性一致アイテムを作成 **(Create Vulnerable Items)]** オプションを選択します。
3. [脆弱性一致アイテムを作成 (Create vulnerable items)] ダイアログボックスで、[脆弱性一致アイテムを作成 **(Create vulnerable items)]** オプションを選択します。
4. [ステータスの表示] リンクを選択して、VI の作成に使用されているバックグラウンドジョブのステータスを表示します。

エクスポージャーアセスメントのための **CVE** のアクティブ化または非アクティブ化

CVE のデルタ処理のために、CVE をアクティブ化できます (CVE のアクティブリストにその CVE が追加されます)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_vul_analyst.vul_event_manager

> **注:**
> 脆弱性エクスポージャーアセスメントのバージョン 4.0.1 以降では、共通脆弱性エントリー (CVE) が更新されていないか、過去 30 日間に脆弱性一致アイテム (VIT) が作成されている場合、その CVE のエクスポージャーアセスメントレコードは自動的に非アクティブとしてマークされます。ただし、これらのレコードを手動でアクティブ化または非アクティブ化することはできます。さらに、スケジュール済みジョブ *Check potential vulnerability exposure* 継続的に実行され、そのような CVE をスキャンして非アクティブとして指定します。

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース > エクスポージャーアセスメント > **CVE** による評価.
2. 必要なアクティブ CVE を選択し、[非アクティブ化 **(Deactivate)]** オプションを選択します。CVE が非アクティブ化されます。

   > **注:**
   > ソフトウェアをアクティブ化するには、同じプロセスに従って [アクティブ化] オプションを選択します。

3. ページを更新します。更新されたステータス (false) が [アクティブ] 列に表示されます。

エクスポージャーアセスメントのための影響を受ける **CI** のエクスポート

エクスポージャーアセスメントレコードに関連する構成アイテム (CI) を Excel シートにエクスポートすることで、新しい CVE の影響を受ける資産のリストを追跡できます。このシートを使用して、資産の詳細と所有者を共有し、ゼロデイ脆弱性の影響を受ける既知の資産でインシデントを作成できます。

始める前に
必要なロール：sn_vul_analyst.vul_event_manager

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース > エクスポージャーアセスメント > **CVE** による評価.
2. CI をエクスポートするレコードのディスカバリーモデルを選択します。
   [ソフトウェアインストール] タブには、ソフトウェアレコードに関連するアクティブな CI が含まれています。これらの CI は [インストール先] 列に格納されます。
3. [エクスポート] オプションを選択します。
4. [エクスポート] ダイアログボックスで、ファイルタイプとデリバリタイプを選択して、関連する CI をエクスポートします。
5. [エクスポート] オプションを選択します。

信頼スコア計算の例

共通脆弱性識別子 (CVE) 情報に基づいてゼロデイ脆弱性の信頼度を計算する例。

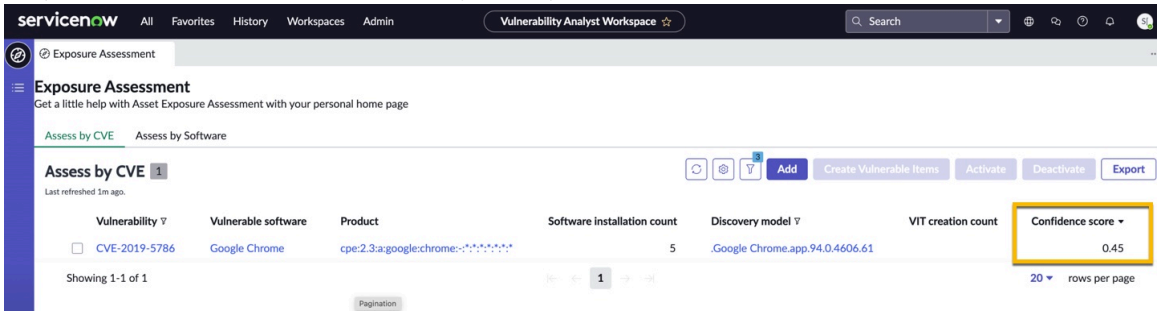
CVE-2019-5786 の共通プラットフォーム一覧 (CPE) 情報から信頼スコアを計算する例を以下に示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

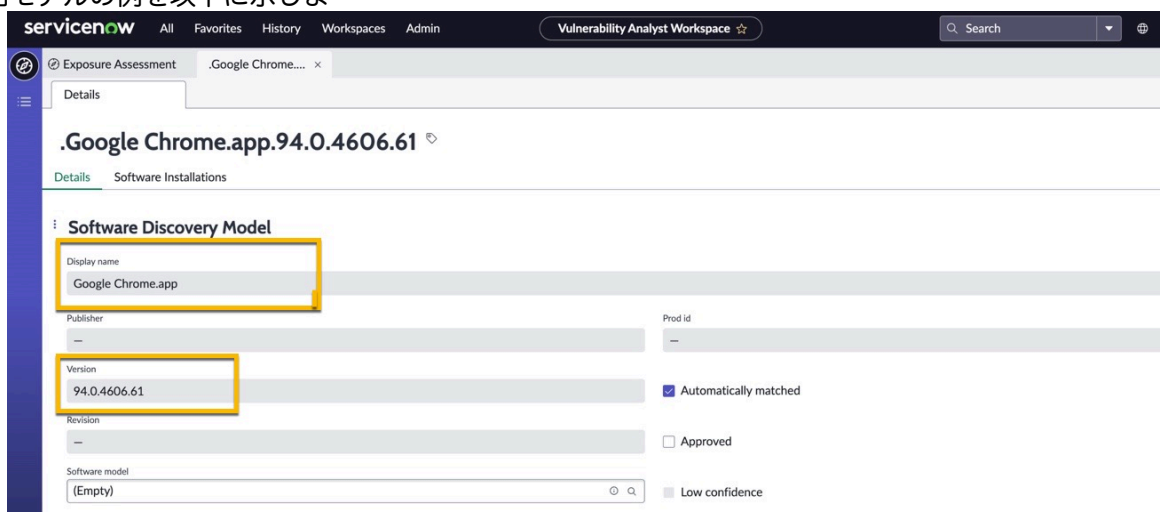
注:
CPE を確認するには、[脆弱性] 列を脆弱性に基づいてグループ化できます。脆弱なソフトウェアの詳細を表示する方法の詳細については、「脆弱なソフトウェアの詳細の表示」を参照してください。

エクスポージャーアセスメントレコードの例を以下に示しま



す。

検出モデルの例を以下に示しま



す。

信頼スコアの計算方法

信頼スコアの範囲は 0 ~ 1 です。信頼スコアは、CPE 情報に基づいて次の式で計算されます。

```
((BASE SCORE) + (publisher score) +(product score) + (version score) + (edition score) + (display name score)) / 100
```

=

```
((25) + (10) + (10)) / 100
```

=

```
45 / 100
```

=

```
.45
```

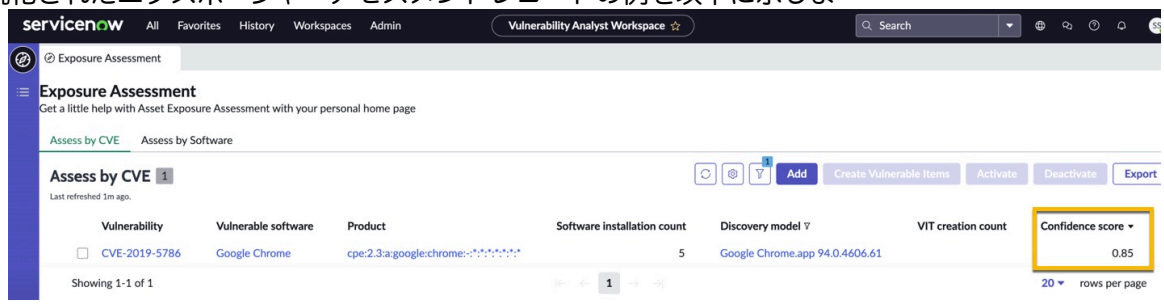
注:
信頼スコアの計算に使用される値を参照するには、「エクスポージャーアセスメントの信頼スコア参照テーブル」を参照してください。

ソフトウェアモデルが正規化された検出モデルに一致した場合の信頼スコアの計算

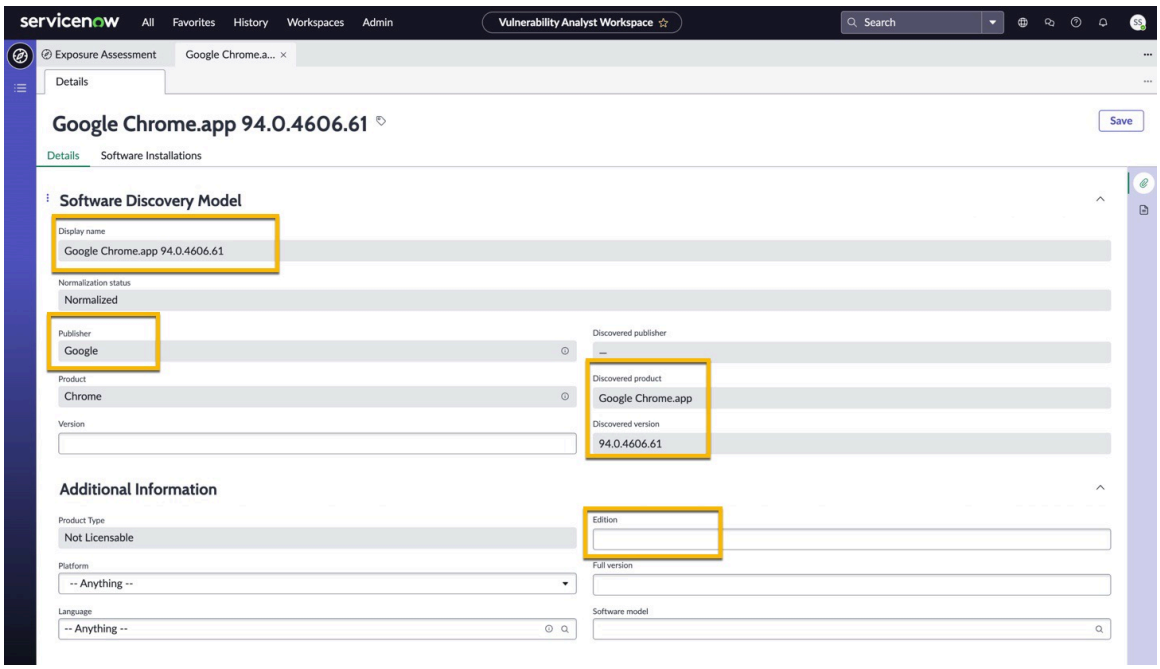
正規化された検出モデルを使用している場合は、ソフトウェアディスカバリーモデルで利用可能な追加情報により、信頼スコアが拡張されます。計算の例を次に示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

正規化されたエクスポージャーアセスメントレコードの例を以下に示しま


す。

正規化された検出モデルの例を以下に示します。


((BASE SCORE) + (publisher score) + (product score) + (version score) + (edition score) + (display name score)) / 100

=

((25) + (20) + (15) + (15) + (0) + (10)) / 100

=

85 / 100

=

.85

注:
信頼スコアの計算に使用される値を参照するには、「エクスポージャーアセスメントの信頼スコア参照テーブル」を参照してください。

脆弱なソフトウェアの詳細の表示

脆弱なソフトウェア (この場合は Google Chrome) の詳細を表示します。これは、検出モデルおよび共通プラットフォーム一覧 (CPE) と照合されます。この CPE バージョンは、すべての Google Chrome バージョンに影響します。

始める前に
必要なロール：sn_vul_analyst.vul_event_manager

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. [すべて] に移動して「*sn_vul_software.LIST*」と入力します。
2. 脆弱なソフトウェアのリストで **cpe:2.3:a:google:chrome:-:*:*:*:*:*:*:*** を検索し、情報を表示します。

エクスポージャーアセスメントの信頼スコア参照テーブル

信頼スコアの計算に使用される参照値。

参照テーブル

信頼スコア計算参照テーブル

脆弱なソフトウェアセグメント	検出モデルセグメント	スコア	検出モデル完全一致セグメント	完全一致スコア
パブリッシャー	表示名	15	パブリッシャー	5
モデル	表示名	15	モデル	5
バージョン	表示名	10	バージョン	5
Edition (エディション)	Display name (表示名)	3	正規化版	2
Display name (表示名)	表示名	10	表示名	5

信頼スコアサマリーテーブル

スコア	値
すべてのスコアの合計	75
基本スコア **注:** 一致したすべてのディスカバリーモデルに与えられる最小スコア。	25
合計スコア	100

ソフトウェアによるエクスポージャーアセスメント

資産または構成アイテムの共通脆弱性識別子 (CVE) が利用できない場合の、ゼロデイ脆弱性のエクスポージャーアセスメント。ソフトウェアディスカバリーモデルを使用したエクスポージャーの評価に、ソフトウェア情報を使用します。

ソフトウェアによるエクスポージャーアセスメントの詳細については、以下を参照してください。

- エクスポージャーアセスメントのためのソフトウェアの追加
- エクスポージャーアセスメントのためのソフトウェアの VI の作成
- エクスポージャーアセスメントのためのソフトウェアのアクティブ化または非アクティブ化
- 脆弱性アセスメントのワークスペースでソフトウェアの影響を受ける CI をエクスポートする

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エクスポージャーアセスメントのためのソフトウェアの追加

新しい脆弱性またはゼロデイ脆弱性の影響を評価するために、新しいソフトウェアを [エクスポージャーアセスメント] モジュールに追加します。

始める前に
必要なロール：sn_vul_analyst.vul_event_manager

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース > エクスポージャーアセスメント > ソフトウェアによる評価 > 追加.
2. フォームのフィールドに入力します。

フィールド	説明
パブリッシャー	ソフトウェアの公開者。
製品	このソフトウェアの製品名。
バージョン	ソフトウェア製品のバージョン。
エディション	ソフトウェアのエディション。

> **注:**
> テーブルに存在しており、ステータスが「false」のソフトウェアのエクスポージャーを追加しようとすると、重複するレコードは作成されません。既存のソフトウェアのステータスが「true」に更新されます。

3. [追加] オプションを選択します。
4. 既にリストに含まれているソフトウェアの影響を評価するには、次の手順を実行します。
   a. 再評価するソフトウェアのチェックボックスをオンにします。
   b. [再評価] ボタンを選択します。
   更新された詳細情報が各列に表示されます。

エクスポージャーアセスメントのためのソフトウェアの **VI** の作成

[エクスポージャーアセスメント] ページでの脆弱性アイテム (VI) の作成脆弱性イベントマネージャーはこの VI のリストを分析し、IT チームがこれらの脆弱性にパッチを適用するのに役立つソリューションとパッチを推奨します。

始める前に
必要なロール：sn_vul_analyst.vul_event_manager

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース > エクスポージャーアセスメント > ソフトウェアによる評価.
2. VI を作成するレコードを選択します。
3. [脆弱性一致アイテムを作成] オプションを選択します。
4. [脆弱性一致アイテムを作成 (Create vulnerable items)] ダイアログボックスで、次のいずれかを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 既存の脆弱性
- 新しい脆弱性

5. [脆弱性一致アイテムを作成] オプションを選択します。

エクスポージャーアセスメントのためのソフトウェアのアクティブ化または非アクティブ化

ソフトウェアの今後のデルタ処理を停止するには、ソフトウェアを非アクティブ化します (ソフトウェアのアクティブリストからそのソフトウェアが削除されます)。

始める前に
必要なロール：sn_vul_analyst.vul_event_manager

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース > エクスポージャーアセスメント > ソフトウェアによる評価.
2. 非アクティブ化するには、必要なアクティブなソフトウェアを選択してから [非アクティブ化 **(Deactivate)]** オプションを選択します。
   ソフトウェアが非アクティブ化されます。

   > **注:**
   > ソフトウェアをアクティブ化するには、同じプロセスに従って [アクティブ化] オプションを選択します。

3. ページを更新します。更新されたステータス (false) が [アクティブ] 列に表示されます。

脆弱性アセスメントのワークスペースでソフトウェアの影響を受ける **CI** をエクスポートする

エクスポージャーアセスメントレコードに関連する構成アイテム (CI) を Excel シートにエクスポートすることで、新しいソフトウェアの影響を受ける資産のリストを追跡できます。このシートを使用して、資産の詳細と所有者を共有し、ゼロデイ脆弱性の影響を受ける既知の資産でインシデントを作成できます。

始める前に
必要なロール：sn_vul_analyst.vul_event_manager

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース > エクスポージャーアセスメント > ソフトウェアによる評価.
2. CI をエクスポートするレコードのディスカバリーモデルを選択します。
   [ソフトウェアインストール] タブには、ソフトウェアレコードに関連するアクティブな CI が含まれています。これらの CI は [インストール先] 列に格納されます。
3. [エクスポート] オプションを選択します。
4. [エクスポート] ダイアログボックスで、ファイルタイプとデリバリタイプを選択して、関連する CI をエクスポートします。
5. [エクスポート] オプションを選択します。

パブリッシャーソフトウェアによるエクスポージャーアセスメント

資産または構成アイテムの共通脆弱性識別子 (CVE) が利用できない場合の、ゼロデイ脆弱性のエクスポージャーを評価します。ソフトウェアディスカバリーモデルを使用したエクスポージャーの評価に、ソフトウェア情報を使用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソフトウェアによるエクスポージャーアセスメントの詳細については、以下を参照してください。

- エクスポージャーアセスメントのための公開者別ソフトウェアの追加
- エクスポージャーアセスメントのために公開者別にソフトウェアの VI を作成する
- エクスポージャーアセスメントのための公開者によるソフトウェアのアクティブ化または非アクティブ化
- 脆弱性アセスメントのワークスペースで、公開者によってソフトウェアの影響を受ける CI をエクスポートする

エクスポージャーアセスメントのための公開者別ソフトウェアの追加

公開者のソフトウェアをエクスポージャーアセスメントモジュールに追加して、新しい脆弱性またはゼロデイ脆弱性の影響を評価します。

始める前に

必要なロール：sn_vul_analyst.vul_event_manager

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース > エクスポージャーアセスメント > パブリッシャーによる評価 > 新規.
2. 新しいアセスメント ウィンドウで、アセスメントを実行する公開者を選択します。
3. **[CVE** の公開元] フィールドで日付を選択します。
   選択した日付以降に、ソフトウェアに関連する共通脆弱性エントリ (CVE) のいずれかが変更された場合、そのソフトウェアはエクスポージャーアセスメントの対象と見なされます。
4. [**CVE** 重大度] セクションで CVE の重大度レベルを選択します。
5. [アセスメントの開始] を選択します。
   ジョブが完了すると、選択したレコードが作成されます。

エクスポージャーアセスメントのために公開者別にソフトウェアの **VI** を作成する

[エクスポージャーアセスメント] ページから脆弱性一致アイテム (VI) を作成して VI のリストを分析し、IT チームが脆弱性にパッチを適用するのに役立つソリューションとパッチを推奨します。

始める前に

必要なロール：sn_vul_analyst.vul_event_manager

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース > エクスポージャーアセスメント > パブリッシャーによる評価.
2. VI を作成するレコードを選択します。
3. [脆弱性一致アイテムを作成] オプションを選択します。
4. [脆弱性一致アイテムを作成 (Create vulnerable items)] ダイアログボックスで、次のいずれかを選択します。
   - 既存の脆弱性
   - 新しい脆弱性
5. [脆弱性一致アイテムを作成] オプションを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エクスポージャーアセスメントのための公開者によるソフトウェアのアクティブ化または非アクティブ化

公開者がソフトウェアをアクティブ化または非アクティブ化して、ソフトウェアのデルタ処理を停止し、ソフトウェアのアクティブリストからソフトウェアを削除します。

始める前に
必要なロール：sn_vul_analyst.vul_event_manager

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース > エクスポージャーアセスメント > パブリッシャーによる評価.
2. 非アクティブ化するには、公開者によって必要なアクティブなソフトウェアを選択し、[再評価] ボタンの下にある [非アクティブ化] オプションを選択します。
   パブリッシャーが非アクティブ化されます。

   > **注:**
   > 公開者がソフトウェアのライセンス認証を行うには、同じプロセスに従って [ライセンス認証] オプションを選択します。

3. ページを更新します。更新されたステータス (false) が [アクティブ] 列に表示されます。

脆弱性アセスメントのワークスペースで、公開者によってソフトウェアの影響を受ける **CI** をエクスポートする

エクスポージャーアセスメントレコードに関連する構成アイテム (CI) を Excel シートにエクスポートすることで、新しいソフトウェアの影響を受ける資産のリストを追跡できます。このシートを使用して、資産の詳細と所有者を共有し、ゼロデイ脆弱性の影響を受ける既知の資産でインシデントを作成できます。

始める前に
必要なロール：sn_vul_analyst.vul_event_manager

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース > エクスポージャーアセスメント > パブリッシャーによる評価.
2. CI をエクスポートするレコードのディスカバリーモデルを選択します。
   [ソフトウェアインストール] タブには、ソフトウェアレコードに関連するアクティブな CI が含まれています。これらの CI は [インストール先] 列に格納されます。
3. [エクスポート] オプションを選択します。
4. [エクスポート] ダイアログボックスで、ファイルタイプとデリバリタイプを選択して、関連する CI をエクスポートします。
5. [エクスポート] オプションを選択します。

脆弱性アセスメントの詳細

脆弱性アセスメントのワークスペースは、脆弱性イベントマネージャーが特にゼロデイ脆弱性分析時に、脆弱性イベントを作成して脆弱性アセスメントを実行できるように設計されています。

脆弱性アセスメントのワークスペースを使用して、次のような重大な脆弱性を管理できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 「重大」または「高」の重大度のゼロデイ脆弱性
- 脆弱性に対して特定された新しい脅威インテリジェンス
- 「重大」または「高」の重大度の脆弱性の悪用の急速な発生

脆弱性アセスメントのワークスペースと脆弱性危機管理

脆弱性イベントマネージャーは、関心対象の脆弱性の脆弱性イベントレコードを特定して作成します。脆弱性一致イベントを作成すると、リスクアセスメントを実行し、リスク属性を手動で更新して、リスクスコアを自動的に計算できます。脆弱性アセスメントのワークスペースを使用して、脆弱性危機イベントを発生から解決まで処理するために、次のアクションを実行できます。

- 脆弱性アセスメントレコードの作成
- 脆弱性アセスメントレコードを変更する
- 脆弱性アセスメントの実行
- アセスメントの詳細の確認
- 脆弱性アセスメントレコードに優先度とエクスポージャーレベルをアサインする
- 影響を受ける CI をアセスメントレコードに追加する
- 影響を受ける CI または影響を受けるソフトウェアコンポーネントの脆弱性一致アイテムを作成する
- 脆弱性アセスメントを重大セキュリティインシデント管理で重大なセキュリティインシデントにリンクする

脆弱性アセスメントの前提条件

利用可能バージョン

アプリケーション	バージョン
脆弱性危機管理プラグイン	1.0
脆弱性対応	20.0
脆弱性対応 with NVD **注:** 詳細については、「NVD 統合の概要」を参照してください。	1.4.2
Vulnerability Response Integration with CISA	1.2
Data Model for SBOM	1.1.2
ソフトウェア部品表 コア	2.0.2
ソフトウェア資産管理	ソフトウェア資産管理の基盤プラグイン または ソフトウェア資産管理プロ プラグイン
重大セキュリティインシデント管理	2.2.5

スケジュール済みジョブ

スケジュール済みジョブは次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みジョブの名前	説明
脆弱性アセスメント	脆弱性一致アイテム (VIT または AVIT) がアセスメント後に作成された場合、影響を受ける構成アイテムテーブルと CI のソースを更新します。 **注:** このスケジュール済みジョブは毎日実行されます。他のスケジュール済みジョブよりも長時間実行されます。

関連情報

脆弱性危機管理

脆弱性アセスメントレコードの作成

関心対象の脆弱性のアセスメントレコードを作成します。アセスメントを作成した後、初期リスクアセスメントを開始し、レコードを手動で更新して、リスクスコアを自動的に計算できます。

始める前に

脆弱性アセスメントに関連付けられたタスクを実行できるようにするには、ベースシステムの脆弱性アセスメントイベントマネージャーのアサイン先グループの一員である必要があります。必要なロール：sn_vul_analyst.vul_event_manager

このタスクについて

イベントレコードをプライマリ CVE または影響を受ける製品に関連付けることで、関心対象の脆弱性の脆弱性アセスメントレコードを作成できます。

手順

1. 次のように移動する。 **All** (すべて) > ワークスペース > 脆弱性アセスメントのワークスペース.
2. [脆弱性アセスメント] アイコンを選択します。
3. [新規] を選択します。
4. [タイトル] フィールドに適切なタイトルを入力します。
5. オプション: 新しいアセスメントレコードに関連付けるプライマリ CVE を [プライマリ **CVE**] フィールドから選択します。

   注:
   アセスメントレコードのすべての予備的な詳細は、選択または作成した製品、またはレコードに関連付けるプライマリ CVE に基づいて入力されます。

6. [送信] を選択します。
   入力したタイトルの脆弱性アセスメントレコードが作成され、新しい [脆弱性アセスメント] タブに表示されます。デフォルトでは、脆弱性アセスメントレコードは [詳細] タブに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
デフォルトでは、関連付けられた/マッピングされたプライマリ CVE の詳細が表示されます。

- 脆弱性アセスメントイベントレコードの作成時にプライマリ CVE が選択されていない場合は、デフォルトのレコードが作成されます。
- プライマリ CVE に CVE が関連付けられている場合は、関連する CVE が [脆弱性エントリ] タブに入力されます。[脆弱性エントリ] タブから、関連する CVE をさらに追加できます。

7. [影響を受ける製品] タブに移動します。

a. [新規] を選択します。

b. フォームのフィールドに入力します。

フィールド	説明
パブリッシャー	ソフトウェアの公開者。 このフィールドは必須です。
製品	このソフトウェアの製品名。 このフィールドは必須です。
バージョン	ソフトウェア製品のバージョン。
エディション	ソフトウェアのエディション。

注:
テーブルに存在しており、ステータスが「false」のソフトウェアの脆弱性を追加しようとすると、重複するレコードは作成されません。既存のソフトウェアのステータスが「true」に更新されます。

c. [OK] を選択します。

8. [保存] を選択します。

脆弱性アセスメント自動フラッシュレコードを更新する

脆弱性アセスメント自動フラッシュレコードを更新します。

始める前に
必要なロール：sn_vul_analyst.vul_event_manager

このタスクについて
ベースシステムでは、脆弱性アセスメントレコードの保存期間は 6 か月に設定されています。いずれかの脆弱性アセスメントレコードのステータスがクローズ済みの場合、脆弱性アセスメントレコードは定義された保持期間までのみ保存され、そのアセスメントの関連レコードは 6 か月後にすべての関連テーブルから削除されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 自動フラッシュ.
2. レコードをテーブル sn_vul_analyst_vulnerability_assessment で開きます。
3. [アクティブ] チェックボックスをオンにして、脆弱性アセスメントレコードの自動フラッシュオプションをアクティブ化します。
4. [更新] をクリックします。

脆弱性アセスメントレコードを変更する

脆弱性アセスメントレコードを作成後に更新します。フィールドの値に基づいて、リスクスコアを計算できます。

始める前に

必要なロール：sn_vul_analyst.vul_event_manager

このタスクについて

プライマリ CVE が脆弱性アセスメントに追加されると、レコードは [処理待ちのアセスメント] ステータスに移行します。[脆弱性エントリ] タブで他の関連 CVE をさらに追加したり、[影響を受ける製品] タブからこの脆弱性の影響を受ける製品を追加したりできます。[リスクアセスメント] フィールドにさらに変更を加えると、アセスメントレコードの [リスクスコア] がそれに応じて自動的に更新されます。

手順

1. 次のように移動する。 **All** (すべて) > 脆弱性アセスメントのワークスペース > 脆弱性アセスメント.
2. [詳細] タブで、フィールドを更新します。

フィールド	説明
タイトル	脆弱性イベントのレコードを説明するタイトル。
プライマリ CVE	イベントレコードに関連付けたプライマリ CVE。
状態	イベントレコードの現在のステータス。
優先度	1 ～ 5 段階でのイベントレコードの優先度。
アラートソース	潜在的な脆弱性イベントのソース。
リスクスコア	自動計算されたリスクスコア。 デフォルトでは編集できません。
エクスポージャーレベル	1 ～ 5 段階での脆弱性イベントのエクスポージャーレベル。
アサイン先グループ	イベントレコードがアサインされているアサイン先グループ。
アサイン先	イベントレコードが割り当てられているユーザー。
説明	イベントレコードの詳細な説明。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [脆弱性エントリ] タブに移動して、関連付けられた、または関連する CVE を追加します。
   a. [新規] を選択します。
   b. [脆弱性エントリ] フィールドでレコードを検索します。
   c. アセスメントレコードに関連付ける脆弱性レコードを選択します。
   d. オプション: [参照] をクリックし、ファイルを参照して添付します。
   e. [保存] を選択します。
   選択した脆弱性レコードがアセスメントレコードに追加され、[脆弱性エントリ] タブに表示されます。
4. オプション: 影響を受ける製品を追加します。
5. アセスメントレコードに関連リンクを追加する。
6. 脆弱性アセスメントイベントレコードに関連付けられたプライマリ CVE の [リスク属性] を変更します。

フィールド	説明
メモリ破損	このイベントレコードによってメモリが破損する可能性があるかどうかを示します。
リモートコード実行可能ファイル	リモートのコード実行が可能かどうかを示します。
ローカル特権エスカレーション	ローカルの特権エスカレーションの脆弱性が存在するかどうかを示します。
不正アクセス	不正アクセスの脆弱性が存在するかどうかを示します。
DDOS	潜在的なイベントに分散サービス拒否が関係している可能性があるかどうかを示します。
攻撃の複雑さ	攻撃の複雑さを示します。 オプションは、[低]、[中]、または [高] です。
攻撃ベクトル	攻撃の潜在的な経路または方法を示します。 オプションは、[ネットワーク]、[隣接ネットワーク]、[ローカル]、[物理]、[なし] です。
必要な権限	攻撃者が脆弱性を悪用するために必要とする特権のレベルを示します。 オプションは、[なし]、[低]、または [高] です。
ユーザーのインタラクション	脆弱性を悪用するためにユーザーのインタラクションが必要かどうかを示します。
機密性に及ぼす影響度	脆弱性の機密性に対する潜在的な影響の尺度を示します。 オプションは、[なし]、[低]、または [高] です
スコープの変更	アセスメントが変更された場合にスコープかどうかを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
可用性に及ぼす影響度	悪用が成功して脆弱性が誤用された場合に可用性に及ぶ可能性がある影響を示します。可用性とは、情報リソースのアクセシビリティを指します。 オプションは、[なし]、[低]、または [高] です
完全性に及ぼす影響度	悪用が成功して脆弱性が誤用された場合に完全性に及ぶ可能性がある影響を示します。完全性とは、情報の信頼性と保証された正確性を指します。 オプションは、[なし]、[低]、または [高] です
修復レベル	脆弱性の修復のステータスまたは可用性を示します。 オプションは、[公式の修正]、[一時的な修正]、[ワークアラウンド]、[利用不可]、[未定義] です。
コード成熟度を利用します	既存の悪用技術とコードの可用性の状況に基づいて、脆弱性が悪用される可能性を示します。 選択肢は、[未確認]、[概念実証]、[機能的]、[高]、[未定義] です。
信頼度をレポート	脆弱性が存在する確信度を示します。

7. 関連するコメントを [作成 **(Compose)]** フィールドに入力します。
   - [作業メモ (プライベート)] フィールドに作業メモを入力します。
   - [コメント] フィールドにコメントを入力します (全員に表示されます)。
8. [保存] をクリックしてアセスメントレコードを保存します。
   アセスメントレコードに関連付けられたプライマリ CVE または影響を受ける製品の [リスク属性] フィールドに加えた更新に基づいて、[リスクスコア] フィールドが自動的に更新されます。

   注:
   ベースシステムのリスクスコア算出ルールまたは基準を変更するには、次に移動します: **All** (すべて) > 脆弱性アセスメントの算出 > 脆弱性アセスメントリスクの算出 > 脆弱性アセスメントリスクルール. 必要に応じて、基準を追加し、フィールドレベルの重み付けを既存の基準に変更できます。

次のタスク
イベントレコードの初期アセスメントを実行します。

脆弱性アセスメントレコードから関連 **CVE** または影響を受ける製品を削除する

不要になった脆弱性イベントレコードを削除します。

始める前に
必要なロール：sn_vul_analyst.vul_event_manager

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
脆弱性アセスメントレコードに関連付けられた CVE または影響を受ける製品を削除できます。脆弱性エントリ/関連する CVE または影響を受ける製品が [新規] または [処理待ちのアセスメント] 状況である場合にのみ、それらを削除できます。

手順
1. 次のように移動する。 **All** (すべて) > ワークスペース > 脆弱性アセスメント.
2. 脆弱性アセスメントレコードを選択します。
3. [脆弱性エントリ] タブまたは [影響を受ける製品] タブを選択します。
4. 関連する CVE または影響を受ける製品レコードを選択します。
5. [削除] を選択します。

> **注:**
> [削除] ボタンは、[新規] または [処理待ちのアセスメント] 状況のアセスメントレコードに対してのみ表示されます。

アセスメントレコードに関連リンクを追加する

アセスメントレコードに関連するリンクと情報をさらに追加します。

始める前に
必要なロール：sn_vul_analyst.vul_event_manager

手順
1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース.
2. アセスメントレコードエントリを選択します。
3. [関連リンク] タブを選択します。
4. [説明] フィールドに関連する説明を入力します。
5. [リンク **]** フィールドに URL を入力します。
6. **[OK]** を選択します。
   関連リンクが追加され、[関連リンク] タブにリストされます。

アセスメントの実行

脆弱性アセスメントレコードを作成し、リスク属性フィールドを更新した後、イベントレコードのアセスメントを実行します。

始める前に
必要なロール：sn_vul_analyst.vul_event_manager

このタスクについて
関心対象の脆弱性のイベントが作成され、システムとデータにリスクがあると判断されたら、初期アセスメントを実行します。このアクティビティの目的は、リスクアセスメントを詳細なエクスポージャーアセスメントで更新することにより、脅威をさらに分析することです。

手順
1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース > 脆弱性アセスメント.
2. 脆弱性アセスメントイベントレコードのリストから関連するレコードを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [評価] を選択して、脆弱性評価を実行します。
   脆弱性対応 - 脆弱性アセスメントイベントの処理バックグラウンドジョブが開始され、関連する通知が表示されます。
4. 通知の [ステータスを表示 **(View Status)]** を選択して、実行中のジョブのステータスを表示します。
5. [保存] を選択します。

   [アセスメント] タブには、アセスメントの詳細が表示されます。アセスメントが処理されると、脆弱性エントリまたは CVE に関連付けられた VIT または AVIT が [脆弱性一致アイテム] または [アプリケーション脆弱性一致アイテム] タブに表示されます。

タスクの結果

- 関連付けられた CVE に関連する脆弱性一致アイテムまたは TPE は、アセスメント中にフェッチされます。脆弱性一致アイテムに関連する CI も特定され、[影響を受ける構成アイテム] テーブルに表示されます。
- 影響を受ける CI テーブルに関連する CI が存在しない場合、識別された CI がテーブルに追加され、[脆弱性一致アイテムあり] フィールドの値が **True** に設定され、[ソース] フィールドの値が [スキャナー] に設定されます。
- 影響を受ける CI テーブルに CI が既に存在する場合は、[脆弱性一致アイテムあり] フィールド値のみが **True** に設定され、CI の [ソース] フィールドの値はアセスメントレコードが作成されたときと同じままです。
- アセスメント後に脆弱性一致アイテムが作成されると、脆弱性アセスメントのスケジュール済みジョブが実行され、影響を受ける CI テーブルと CI のソースが更新されます。

次のタスク

- 脆弱性アセスメントレコードに優先度とエクスポージャーレベルをアサインする
- 影響を受ける CI をアセスメントレコードに追加する
- 影響を受ける CI または影響を受けるソフトウェアコンポーネントの脆弱性一致アイテムを作成する
- アセスメントレコードに関連リンクを追加する

関連情報

[アセスメント] タブ

[概要] タブ

[アセスメント] タブ

[アセスメント] タブでアセスメント結果を確認します。脆弱性イベントのアセスメントを実行すると、レコードは ソフトウェア部品表 および ソフトウェア資産管理 からのデータと関連付けられ、ビジュアル化されて表示されます。

[アセスメント] タブは、作成したアセスメントレコードに基づいてデータを入力し (入手可能な場合)、CMDB 内のアセスメント ソフトウェア資産管理 および ソフトウェア部品表 コンポーネントデータと詳細を関連付けます。

アセスメントの仕組み

[評価] ボタンを選択すると、ソフトウェア資産管理 データと SBOM データの両方を使用して、関連するすべての CVE と影響を受ける製品の評価が開始されます。バックグラウンドジョブがトリガーされ、アセスメントが処理されると、脆弱性エントリまたは CVE に関連付けられた VIT または

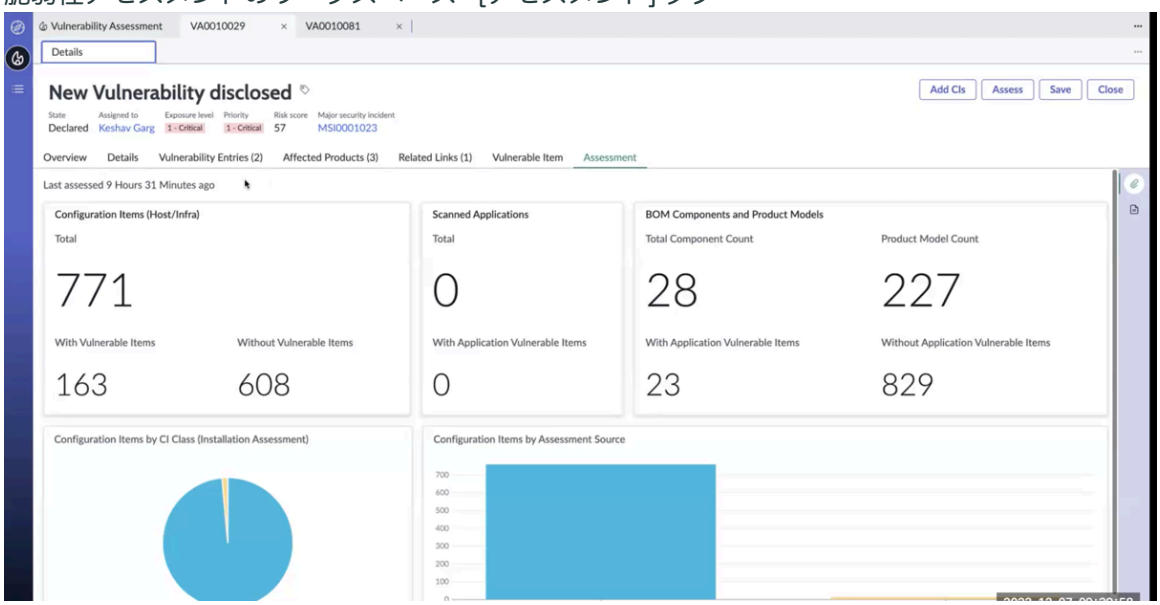
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

AVIT が [脆弱性一致アイテム] タブおよび [アプリケーション脆弱性一致アイテム] タブに表示されます。

- CVE に関連するすべての脆弱性一致アイテムまたは TPE が特定されます。
- 脆弱性一致アイテムに関連する構成アイテム (CI) も特定され、影響を受ける構成アイテムテーブルに表示されます。
- 影響を受ける CI テーブルに CI が存在しない場合、識別された CI がテーブルに追加され、[脆弱性一致アイテムあり] フラグが true に変わり、[ソース] フィールドの値が [スキャナー] に設定されます。
- 影響を受ける構成アイテムテーブルに CI が既に存在する場合は、[脆弱性一致アイテムあり] フラグのみが true に設定され、[ソース] はアセスメントレコードが作成された時点から変更されません。
- アセスメント後に脆弱性一致アイテムが作成されると、脆弱性アセスメントのスケジュール済みジョブが実行され、影響を受ける CI テーブルと CI のソースが更新されます。
- アセスメントワークスペースでは、タイムスタンプを表示して、イベントの最後のアセスメントを確認できます。[アセスメント] タブは、新しいアセスメントが作成された場合にのみ表示されます。アセスメントが進行中状態である場合、アセスメントの進行に伴い、アセスメントの最終ステータスが表示されます。更新されたアセスメントステータスを表示するには、ページをリフレッシュする必要があります。アセスメントが完了すると、ユーザーはそのアセスメントのすべての関連タブを表示できるようになります。

脆弱性アセスメントのワークスペース - [アセスメント] タブ



次のウィジェットのアセスメントの詳細が表示されます。

- 構成アイテム（ホスト/インフラ）
- スキャン済みアプリケーション
- BOM コンポーネントと製品モデル
- CI クラス別の構成アイテム（インストールアセスメント）
- アセスメントソース別の構成アイテム – 影響を受ける構成アイテムのリストを表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データの可視化

名前	タイプ	説明
構成アイテム（ホスト/インフラ）	単一スコア	VI ありと VI なしの CI の数を表示します。 [構成アイテム] ウィジェットには、アセスメントレコードに関連付けられていることが判明した CI の合計数が表示されます。ウィジェットはさらに、脆弱性一致アイテムがある構成アイテムと、脆弱性一致アイテムがない構成アイテムを表示します。
スキャン済みアプリケーション	カウント	AVIT でスキャンされたアプリケーションの合計数。 **注:** プライマリ CVE とセカンダリ CVE の両方について、スキャンされたアプリケーションの数を表示できます。
BOM コンポーネントと製品モデル	単一スコア	コンポーネントの合計数、製品モデルの数、アプリケーション脆弱性一致アイテムあり、アプリケーション脆弱性一致アイテムなしの数。
アセスメントソース別の構成アイテム	積み重ねバー	アセスメントソースによってスタックされた影響を受ける構成アイテム。
CI クラス別の構成アイテム（インストールアセスメント）	円グラフ	CI クラス別にスタックされた構成アイテム。

[概要] タブ

アセスメントの詳細の概要が [概要] タブに表示されます。最初のアセスメントを実行すると、レコードは ソフトウェア部品表 および ソフトウェア資産管理 からのデータと関連付けられ、 ビジュアル化されて表示されます。

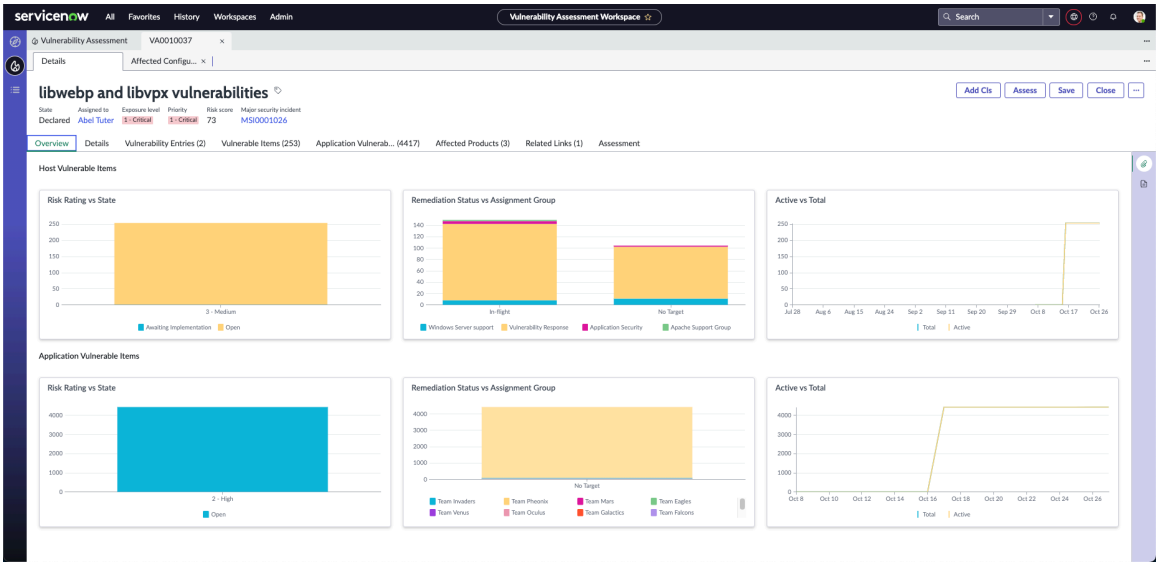
[概要] タブ

[概要] タブは、作成したアセスメントレコードに基づいてデータを入力し (入手可能な場合)、CMDB 内のアセスメント ソフトウェア資産管理 および ソフトウェア部品表 データと詳細を関連付けます。-

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性アセスメント - [概要] タブ



次のウィジェットのアセスメントの詳細が表示されます。

- ホスト脆弱性一致アイテム (ホスト/インフラ)
  - リスク評価とステータス
  - 修復ステータスとアサイン先グループ
  - アクティブと合計
- アプリケーション脆弱性一致アイテム
  - リスク評価とステータス
  - 修復ステータスとアサイン先グループ
  - アクティブと合計

データの可視化

ホスト脆弱性一致アイテム

名前	タイプ	説明
リスク評価とステータス	積み重ねバー	リスク評価別にスタックされた脆弱性一致アイテムのステータス。
修復ステータスとアサイン先グループ	積み重ねバー	アサイン先グループによってスタックされた脆弱性一致アイテムの修復ステータス。
アクティブと合計	リストと折れ線グラフ	このエントリに関連付けられた脆弱性一致アイテムの合計数とアクティブな脆弱性一致アイテム数の比較。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション脆弱性一致アイテム

名前	タイプ	説明
リスク評価とステータス	積み重ねバー	リスク評価別にスタックされたアプリケーション脆弱性一致アイテムのステータス。
修復ステータスとアサイン先グループ	積み重ねバー	アサイン先グループによってスタックされたアプリケーション脆弱性一致アイテムの修復ステータス。
アクティブと合計	リストと折れ線グラフ	このエントリに関連付けられたアプリケーション脆弱性一致アイテムの合計数とアクティブな脆弱性一致アイテム数の比較。

脆弱性アセスメントレコードに優先度とエクスポージャーレベルをアサインする

脆弱性アセスメントレコードに優先度とエクスポージャーレベルを手動でアサインします。

始める前に

必要なロール：sn_vul_analyst.vul_event_manager

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース.
2. 脆弱性アセスメントレコードを選択します。
3. [詳細] タブの [リスク属性] に移動します。
4. オプションのリストから [優先度] を選択します。
5. オプションのリストから [エクスポージャーレベル **(Exposure Level)]** を選択します。
6. [保存] を選択します。

影響を受ける **CI** をアセスメントレコードに追加する

脆弱性アセスメントレコードに関連付ける必要があると思われるものの、初期アセスメント後に影響を受ける CI に表示されないようにする、組織の CI を手動で追加します。

始める前に

必要なロール：sn_vul_analyst.vul_event_manager

このタスクについて

影響を受けている可能性があるが、アセスメント完了後には表示されないことがわかっている CI を追加します。CI を追加できるのは、アセスメントレコードが [宣言済み] または [処理待ちのアセスメント] ステータスの場合のみです。

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース.
2. リストから必要なアセスメントレコードを選択します。
3. **[CI** を追加 **(Add CIs)]** を選択します。
4. [構成アイテム] ダイアログボックスから構成アイテムを選択します。
5. **[CI** を追加 **(Add CIs)]** を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

「脆弱性対応 - イベントに構成アイテムを追加」バックグラウンドジョブが開始され、関連する通知が表示されます。

6. 通知の [ステータスを表示 **(View Status)**] を選択して、実行中のジョブのステータスを表示します。

タスクの結果

レコードが [影響を受ける構成アイテム] テーブルに追加され、[ソース] が [手動] になります。

次のタスク

[アセスメント] タブに移動し、[構成アイテム (ホスト/インフラ) **(Configurations Items (Host/Infra))**] ウィジェットを更新して、追加した CI を表示します。

影響を受ける **CI** または影響を受けるソフトウェアコンポーネントの脆弱性一致アイテムを作成する

脆弱性アセスメントのワークスペースから脆弱性一致アイテム (VI) またはアプリケーション脆弱性一致アイテム (AVIT) を作成します。脆弱性アナリストは VI のリストを分析し、IT チームがこれらの脆弱性にパッチを適用するのに役立つソリューションとパッチを推奨します。

脆弱性イベントマネージャーは、エクスポージャー検索結果の 1 つ、多数、またはすべてを選択して、脆弱性一致アイテムを作成できる必要があります。

- AVIT が関連付けられていない SBOM アセスメント結果のアプリケーション脆弱性一致アイテム
- VIT が関連付けられていない構成アイテムの脆弱性一致アイテム
- プライマリ CVE を脆弱性一致アイテムに関連付けます。

脆弱性一致アイテムが関連付けられていない構成アイテムの **VI** を作成する

脆弱性アセスメントによって特定されたが、レコードに関連付けられた VIT がない構成アイテムに対して、脆弱性一致アイテム VIT を作成します。

始める前に

必要なロール：admin

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース > アセスメント.
2. VIT を作成する必要があるアセスメントレコードを選択します。
3. [アセスメント **(Assessment)**] タブを選択します。
4. [構成アイテム (ホスト/インフラ) **(Configuration Items (Host Infra))**] ウィジェットから [構成アイテムなし **(Without Configuration Items)**] カウントを選択します。
5. VIT を作成する構成アイテムを [影響を受ける構成アイテム] リストから選択します。
6. [脆弱性一致アイテムを作成] を選択します。
   [脆弱性対応 - 手動 VITs Vul アセスメントを作成 (VIT Vulnerability Response - Create Manual VITs Vul Assessment)] バックグラウンドジョブが開始され、関連する通知が表示されます。
7. 通知の [ステータスを表示 **(View Status)**] を選択して、実行中のジョブのステータスを表示します。
   選択した影響を受ける構成アイテムの脆弱性一致アイテムが作成されます。

   [構成アイテム (ホスト/インフラ) **(Configuration Items (Host Infra))**] ウィジェットの [脆弱性一致アイテムを使用] の数に同じ CI が表示されるようになりました。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション脆弱性一致アイテムが関連付けられていない、影響を受ける製品モデルまたはコンポーネントのアプリケーション脆弱性一致アイテム **(AVI)** を作成する

脆弱性アセスメントによって特定されたが、レコードに関連付けられた AVIT がない、影響を受ける製品またはコンポーネントアイテムに対して、アプリケーション脆弱性一致アイテム (AVIT) を作成します。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース > アセスメント.
2. VIT を作成する必要があるアセスメントレコードを選択します。
3. [アセスメント **(Assessment)]** タブを選択します。
4. **[BOM** コンポーネントと製品モデル] ウィジェットから [アプリケーション脆弱性一致アイテムを使用しない] カウントを選択します。
5. [影響を受ける製品モデル] リストから、その AVIT を作成する、影響を受ける製品モデルを選択します。
6. [アプリケーション脆弱性一致アイテムを作成] を選択します。
   [脆弱性対応 - 手動 VITs Vul アセスメントを作成 (VIT Vulnerability Response - Create Manual VITs Vul Assessment)] バックグラウンドジョブが開始され、関連する通知が表示されます。
7. 通知の [ステータスを表示 **(View Status)]** を選択して、実行中のジョブのステータスを表示します。
   選択した影響を受ける製品モデルのアプリケーション脆弱性一致アイテムが、レコードに関連付けられたプライマリ CVE に対して作成されます。

   [BOM コンポーネントと製品モデル] ウィジェットで、同じ製品モデルまたはコンポーネントが [アプリケーション脆弱性一致アイテムを使用] のカウントに表示されるようになりました。

脆弱性アセスメントを重大セキュリティインシデント管理で重大なセキュリティインシデントにリンクする

重大セキュリティインシデント管理アプリケーションへのアクセス権を持っている場合は、アセスメントレコードを重大セキュリティインシデントにリンク、提案、または昇格することができます。

始める前に
必要なロール：sn_vul_analyst.vul_event_manager、sn_si.analyst、sn_msi.workspace_admin

このタスクについて
アセスメントレコードを移動して、既存の重大なセキュリティインシデントに関連付けたり、アセスメントレコードから新しい MSI を作成したり、脆弱性アセスメントレコードを重大なセキュリティインシデントに昇格させたりすることができます。Microsoft Teams や Microsoft SharePoint との統合など、重大セキュリティインシデント管理 の機能を活用します

脆弱性一致アイテムの脆弱性マネージャーのワークスペースで、重大なセキュリティインシデントへのリンクを表示することもできます。MSIM リンクは脆弱性一致アセスメントに関連付けられ、脆弱性一致アイテムとの他の脆弱性対応のワークスペースに表示されます。

手順

1. 次のように移動する。 ワークスペース > 脆弱性アセスメントのワークスペース.
2. 重大なセキュリティインシデントにリンクするアセスメントレコードを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [詳細] タブで、[その他のアクション] アイコンを選択します。
4. 次のいずれかを選択します。

オプション	説明
重大なセキュリティインシデントへのリンク	重大なセキュリティインシデントのリストから既存の MSI レコードを選択します。 脆弱性アセスメントレコードは、既存の重大なセキュリティインシデントにリンクされています。
重大なセキュリティインシデントとして提案	次の詳細を入力し、[提案] を選択します。 ○ 検出日 ○ 正当性 ○ 潜在的な影響
重大なセキュリティインシデントとして昇格	次の詳細を入力し、[昇格 **(Promote)]** を選択します。 ○ 検出日 ○ 推定解決日 ○ 正当性 ○ 潜在的な影響

5. [保存] を選択します。

次のタスク
MSI レコードを選択して、重大セキュリティインシデント管理ビューでレコードを開きます。

関連情報

- 重大セキュリティインシデント へのリンク
- 重大セキュリティインシデント として提案する
- 重大セキュリティインシデント への昇格

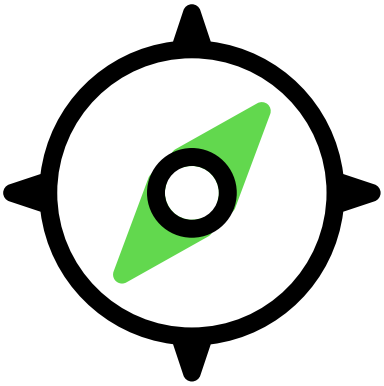
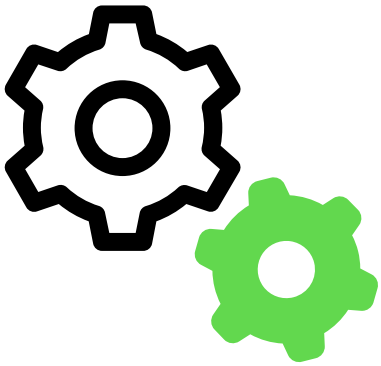
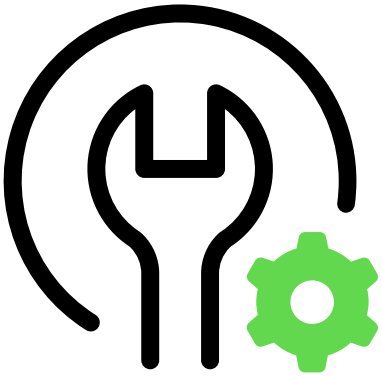
ソフトウェア部品表

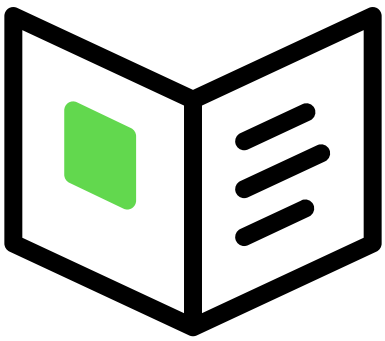
アプリケーション開発で使用しているオープンソースおよびサードパーティのソフトウェアコンポーネントのリストを表示します。インスタンスにアップロードする ソフトウェア部品表 (SBOM) ファイルで、ソフトウェアライセンス、バージョン情報、およびコンポーネントの既知の脆弱性に関するインサイトを取得します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

開始するには

探索	構成	使用
		
SBOMの概念と機能について説明します。	SBOMアプリケーションを設定します。	SBOMコンポーネントをインポートし、ワークスペースでデータを表示する方法について説明します。

Reference (参照)

SBOMフォーム、フィールド、テーブル、プロパティの詳細を取得します。

トラブルシューティングとサポート

- セキュリティオペレーションコミュニティ
- CycloneDX - Software bill of Materials (SBOM) (CycloneDX - ソフトウェア部品表 (SBOM))。
- SPDX。
- 既知のエラーポータルで既知のエラー記事を検索する。
- 連絡先 カスタマーサービス & サポート.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソフトウェア部品表 の詳細

インスタンスにアップロードする ソフトウェア部品表 (SBOM) ファイルから、組織のアプリケーションで使用されているコンポーネントを特定します。オープンソースソフトウェアの使用に関連するリスクを理解して、潜在的なエクスポージャーを判断し、ライセンスコンプライアンスを表示し、脆弱性を修正するのに役立ちます。

ソフトウェア部品表の概要

サードパーティおよびオープンソースのコンポーネントには、ソフトウェアプロジェクトを迅速に作成してリリースするための多くのメリットがあります。ただし、場合によっては、公開されているコンポーネントの使用に関連する次のようなリスクがあります。

- コンポーネントの完全性の可視化の欠如
- オープンソースソフトウェアの脆弱性
- オープンソースソフトウェアのパッケージインテリジェンス
- 非準拠ソフトウェアライセンス

ソフトウェア部品表ファイルは、API を介して、または手動でアップロードできます。エンティティとしてインポートしたファイルを表示します。これは、ソフトウェアで使用されているサードパーティコンポーネントライブラリのインベントリです。これには、推移的な依存関係や利用可能なライセンス情報が含まれます。

CycloneDX および SPDX SBOM のソフトウェアインベントリに含まれるものの詳細については、「CycloneDX - ソフトウェア部品表 (SBOM)」および「SPDX」を参照してください。

ソフトウェア部品表ユーザー

ユーザー

ユーザー	説明
脆弱性マネージャーと脆弱性アナリスト	ソフトウェア部品表 (SBOM) ワークスペースでは、アップロードされたソフトウェア部品表ファイルをレコードで表示したり、データの可視化を行ったり、拡張脆弱性インテリジェンスを作成したりできます。 脆弱性マネージャーと脆弱性アナリストは、この情報を使用して、ソフトウェアライセンスのコンプライアンスと、オープンソースソフトウェアを使用した場合の潜在的なリスクエクスポージャーを判断するのに役立ちます。
以下のユーザーが含まれますが、これらに限定されません。 • テクノロジーまたはソフトウェア弁護士 • IT マネージャー • 監査人 • ソフトウェア資産マネージャーとチーム	アップロードした SBOM ファイルのコンポーネントについて、アップロードされた独自のソフトウェアライセンスとオープンソースのソフトウェアライセンスを表示します。 コンポーネントのプロプライエタリおよびオープンソースのソフトウェアライセンスのデータベースを構築します。 内部ポリシーまたは規制ポリシーに従って、情報が不足しているライセンスをレビューして分類します。 コンポーネントをライセンスに一致させ、全体的なライセンスコンプライアンスを判断し、禁止、制限、または欠落したライセンスに対する潜在的なリスクエクスポージャーを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソフトウェア部品表 のワークフロー

SBOM アプリケーションを使用すると、ファイルをアップロードし、ソフトウェア部品表 (SBOM) ワークスペースでエンティティ、コンポーネントインベントリ、脆弱性、およびソフトウェアライセンス情報の詳細を表示できます。

- API を使用して、または手動で SBOM ファイルをアップロードします。
- SBOMワークスペースにアップロードしたSBOMファイルのコンポーネントを確認します。
- アップロードされた SBOM ファイルからコンポーネントライセンス情報を確認し、それらを分類して、制限付きまたは禁止されたライセンスへのエクスポージャーを特定するのに役立ちます。
- リスクエクスポージャーを評価し、脆弱性が関連付けられているコンポーネントの脆弱性一致アイテムを作成します。
- SBOMワークスペースのホームページで、レポートとダッシュボード、およびアップロードされたSBOMコンポーネントの全体的なライセンスコンプライアンスを表示します。

ソフトウェア部品表 のメリット

次の 3 つのソフトウェア部品表アプリケーションを使用すると、ソフトウェアコンポーネントと関連するリスクの正確なインベントリを表示できます。

- SBOMデータモデル
- SBOM Core
- SBOM Response

互換性情報については、「KB0856498 Vulnerability Response 互換性マトリクスおよびリリーススキーマの変更」を参照してください。

SBOM のメリット

ベネフィット	アプリケーション	サポート対象のバージョン
このアプリケーションは、 SBOM データを格納するために使用されるテーブルを提供します。このアプリケーションは必須です。SBOM データを読み取るために必要なテーブル、ACL、およびロールが含まれています。	SBOMデータモデル	v4.0、v3.0、v2.0
このアプリケーションは必須です。SBOM ドキュメントをアップロードするために必要な API と、それらのドキュメントからデータを解析してインスタンスにインポートするために必要なビジネスロジックが含まれています。ワークスペースでソフトウェアコンポーネントのインベントリを表示できます SBOM が、ランディングページでデータの可視化を表示することはできません。 CycloneDX および SPDX 標準でソフトウェア部品表ファイルをアップロード、解析、および処理します。これらの製品でサポートされているファイル形式とバージョンについては、「サポートされているバージョン」列を参照してください。部品表 (BOM) エンティティとソフトウェアコンポーネントのインベントリを表示し	SBOM Core	v6.0、v5.0、v4.0 バージョン 4.0 以降、SBOM Core は以下をサポートしています。 • CycloneDX の XML および JSON バージョン 1.0 から 1.6 まで。 • SPDX の JSON バージョン 2.2 ～ 2.3。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SBOM のメリット (続く)

ベネフィット	アプリケーション	サポート対象のバージョン
ます。BOM エンティティは、SBOM ファイルのルートレベルコンポーネントです。たとえば、CycloneDX SBOMの場合、メタデータにリストされているコンポーネントは BOM エンティティと見なされます。		
• SBOMSBOM ワークスペースのランディングページの機能とデータの可視化にアクセスする場合は、応答が必要です。 • SBOM 応答には 脆弱性対応 アプリケーションが必要です。 • コンポーネントのインベントリを表示し、SBOM ワークスペースでリスクエクスポージャーを評価します。アプリケーション脆弱性一致アイテム (AVIT) を自動的に作成し、 アプリケーション脆弱性対応 ワークフローで修復するためのルールを設定します。 • ライセンス管理モジュールで、SBOMファイルとともにアップロードされたコンポーネントライセンス情報を表示します。アプリケーション脆弱性対応ファイルでアップロードしたコンポーネントを分類して解決 (照合) し、全体的なライセンスコンプライアンスの状態を確認できるようにします。 • 応答のバージョン 4.0 以降 アプリケーション脆弱性対応 、 SBOM ワークスペースで利用可能な Policy as Code Engine (PaCE) インターフェイスで、「古い」と識別されたコンポーネントまたは破棄されたコンポーネントを ワークスペースで表示できます。 • OSV.dev と Deps.dev の統合は、SBOM Response のインストール時に組み込まれます。 ◦ OSV.dev は、パッケージまたはライブラリの特定のバージョンの脆弱性インテリジェンス情報を提供するオープンソース API です。 ◦ Deps.dev は、特定のパッケージまたはライブラリのバージョンリストを提供し、 古い ステータスと 破棄 されたステータスのコンポーネントを識別するオープンソース API です。 詳細については、「の Deps.dev、OSV.dev、および PaCE 統合の	SBOM Response	v6.0、v5.0、v4.0

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SBOM のメリット (続く)

ベネフィット	アプリケーション	サポート対象のバージョン
構成 ソフトウェア部品表」を参照してください。 PaCE および PaCE ポリシーの詳細については、 Integrating PaCE with other applications を参照してください。		
継続的インテグレーションと継続的デプロイの開発サイクル全体を通じて、ソフトウェアの ソフトウェア部品表 (SBOM) ファイルを生成してアップロードします。	SBOM Response	• SBOM のデータモデル:v1.4 以降。 • SBOM コア:v3.0 以降。 • SBOM 応答:v4.0 以降。

次に探索する内容

ソフトウェア部品表を構成して使用する方法の詳細については、以下を参照してください。

- でサポートされているアプリケーションの探索 ソフトウェア部品表
- ソフトウェア部品表の構成
- SBOMワークスペースでのSBOMファイルのアップロードと表示
- ソフトウェア部品表ワークスペースでのレポートとダッシュボードの表示

でサポートされているアプリケーションの探索 ソフトウェア部品表

サードパーティの脆弱性インテリジェンスや、 ソフトウェア部品表 アプリケーションとのその他の統合により、アップロードしたファイルのデータを拡張できます。

サポートされているアプリケーションのメリット

サードパーティの脆弱性インテリジェンスや ソフトウェア部品表 アプリケーションとのその他の統合により、古いと見なされて破棄されたコンポーネントの数と、コンポーネントに関連する脆弱性を修正できるかどうかに関する情報を表示できます。

次のテーブルにリストされている ServiceNow® アプリケーションとサードパーティ統合は、SBOM アプリケーションによってサポートされています。これらのアプリケーションは、SBOM ファイルに関連する脆弱性の表示と優先順位付けに役立つ、拡張された脆弱性データ、脆弱性インテリジェンス、およびその他の重要な情報を提供します。これらのアプリケーションと統合はすべて、ServiceNow® Store から入手できます。

サポートされているアプリケーションとサードパーティの統合

ベネフィット	アプリケーション	サポート対象のバージョン	ユーザー
脆弱性対応 は、SBOM Response アプリケーションをイ	脆弱性対応	互換性情報については、「 KB0856498 Vulnerability	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サポートされているアプリケーションとサードパーティの統合 (続く)

ベネフィット	アプリケーション	サポート対象のバージョン	ユーザー
ンストールする場合に必要です。SBOM Response をインストールする前に、 脆弱性対応 アプリケーションをインストールします。 アプリケーション脆弱性対応 機能は 脆弱性対応 とともにインストールされます。これらの機能を使用すると、 脆弱性対応 アプリケーションの脆弱性マネージャーワークスペースと脆弱性ワークフローにアクセスして、アプリケーション脆弱性一致アイテム (AVIT) の修復に役立てることができます。		Response 互換性マトリクスおよびリリーススキーマの変更」を参照してください。	
拡張された NVD 脆弱性と重大度のデータを表示します。NVD と CWE の統合からインポートされたデータを表示して、SBOM データにある可能性のある脆弱性データを拡張します。 詳細については、「NVD と CWE の統合によるデータのインポートとサードパーティライブラリの管理」を参照してください。	NVD および SBOM Response との脆弱性対応の統合	互換性情報については、「 KB0856498 Vulnerability Response 互換性マトリクスおよびリリーススキーマの変更」を参照してください。	
Veracode 脆弱性統合を使用してソフトウェア部品表ファイルをインポートします。この Veracode 脆弱性統合 には、 Veracode SBOM ファイルに関する次の機能拡張が含まれています。	Veracode 脆弱性統合と SBOM Response	Veracode 脆弱性統合のバージョン 4.3 以降。 Veracode 脆弱性統合 が既にインストールされている場合は、SBOM Core のバージョン v3.0 以降、CycloneDX	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サポートされているアプリケーションとサードパーティの統合 (続く)

ベネフィット	アプリケーション	サポート対象のバージョン	ユーザー
• SBOM Response がインストールされている場合は、アップロードするSBOMファイルにSBOM で検出された脆弱性を含めることができます。 • SBOM は、アップロードする SBOM SBOM ファイルの部品表 [sn_sbom_doc] テーブルにあるレコードの [ソース] フィールドにマッピングされます。 詳細については、「Veracode 脆弱性統合」を参照してください。		(JSON および XML) および SPDX (XML) 形式でインポートされたVeracode SBOMデータをアップロードすることもできます。 互換性情報については、「 KB0856498 Vulnerability Response 互換性マトリクスおよびリリーススキーマの変更 」を参照してください。	
GitHub リポジトリから Now Platform に SBOM ファイルをアップロードします。CI/CD (継続的統合および継続的デリバリ/展開) パイプラインで生成された SBOM ファイルが Now Platform インスタンスで正常にキューに入れられているかどうかを確認します。 GitHub 環境から開始する GitHub Actions を使用して、ソフトウェア開発サイクル中に潜在的に有害なコンポーネントから環境を保護します。	GitHub Marketplace で SBOM アップロードに必要な GitHub Actions を取得します。	SBOM Core のバージョン 4.0 以降。	

ソフトウェア部品表の構成

SBOMファイルをアップロードする前に、ソフトウェア部品表 (SBOM) アプリケーションに必要なアプリケーションをダウンロードしてアクティブ化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

構成の概要

1. 必要な SBOM アプリケーションと、必要な追加のサポート対象アプリケーションと統合を ServiceNow Store から ServiceNow インスタンスにダウンロードします。サポートされているアプリケーションの詳細については、「 ソフトウェア部品表 の詳細 」と「 ServiceNow Store からのアプリケーションの初回ダウンロード 」を参照してください。

   SBOM Response には脆弱性対応アプリケーションが必要です。SBOM Responseをインストールする前に、脆弱性対応アプリケーションをインストールします。

2. ダウンロードした SBOM アプリケーションを見つけて [インストール] を選択し、次の順序で依存関係とともにアクティブ化します。「ソフトウェア部品表でサポートされているアプリケーションのインストール」を参照してください。

   - 脆弱性対応とその依存関係
   - NVD の脆弱性対応統合
   - SBOM データモデル
   - SBOM Core
   - SBOM 応答には、OSV.dev と Deps.dev の統合、SBOM ワークスペースの Policy as Code Engine (PaCE) の機能へのアクセスが含まれます。

3. Deps.dev と OSV.dev の統合を構成します。これらの統合は SBOM Response アプリケーションに含まれており、自動的にインストールされてアクティブ化されます。統合レコードから OSV.dev 統合 - 包括的オンデマンドを開始する必要があります。詳細については、「 の Deps.dev、OSV.dev、および PaCE 統合の構成 ソフトウェア部品表 と ソフトウェア部品表 の詳細 」を参照してください。

   Deps.dev 統合は、SBOMファイルにアップロードするパッケージまたはライブラリの特定のバージョンで、古い状態および破棄状態のコンポーネントに関する情報を提供します。

   OSV.dev は、 SBOM ファイルにアップロードするパッケージまたはライブラリのバージョンについて、オープンソースデータベースから脆弱性データをプルします。

4. インストールした追加のサポート対象アプリケーションと統合を構成するには、製品ドキュメントを参照してください。「脆弱性対応 の統合」および「他のアプリケーションとの アプリケーション脆弱性対応 の統合」を参照してください。

ソフトウェア部品表でサポートされているアプリケーションのインストール

ファイルをアップロードする前に、 ソフトウェア部品表 (SBOM) アプリケーションに必要なアプリケーションをダウンロードしてアクティブ化します。

始める前に

必要なロール：すべてのアプリケーションのダウンロード、インストール、およびアクティブ化と、インスタンスでロールのアサインを行うアドミン。

このタスクについて

手順

1. ServiceNow Store から必要な SBOM アプリケーションを ServiceNow インスタンスにダウンロードします。

   これらのアプリケーションを使用すると、SBOM ファイルをインスタンスにアップロードおよびインポートできます。SBOM Core がインストールされている場合は、SBOMワークスペースで BOM エンティティおよびコンポーネントデータを表示できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SBOM Response がインストールされている場合は、SBOMワークスペースで BOM エンティティ、コンポーネントデータ、およびデータの可視化を表示できます。

- SBOMデータモデル
- SBOM Core

アプリケーションのダウンロードとアクティブ化の詳細については、「」を参照してください。

- Install a ServiceNow Store application
- Install an update to a ServiceNow Store application

2. オプション: SBOMワークスペースでSBOMデータを表示し、インポートされたサードパーティの脆弱性インテリジェンスを表示し、リスクエクスポージャーを評価して、アプリケーション脆弱性対応および脆弱性対応ワークフローで脆弱性を修正する場合は、次のアプリケーションをダウンロードします。
   - 脆弱性対応 とその依存関係
   - NVD の脆弱性対応統合
   - SBOM Response

   これらおよびその他のサポートされている SBOM アプリケーションの詳細については、「ソフトウェア部品表 の詳細」を参照してください。

3. アプリケーションをダウンロードしたら、 **All** (すべて) > システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて).

4. ダウンロードした SBOM アプリケーションを見つけ、[インストール] を選択して、それぞれの依存関係とともにアクティブ化します。

   アプリケーションが正常にアクティブ化されると、メッセージが表示されます。以下の順序でプラグインを有効にします。

   - 脆弱性対応 とその依存関係
   - NVD の脆弱性対応統合
   - SBOM データモデル
   - SBOM Core
   - SBOM 応答。OSV.dev と Deps.dev の統合が含まれ、 SBOM ワークスペースの Policy as Code Engine (PaCE) インターフェイスをサポートします。

   SBOM 応答のインストール後におけるこれらの統合アプリケーションの構成について、詳細は の Deps.dev、OSV.dev、および PaCE 統合の構成 ソフトウェア部品表 を参照してください。

5. オプション: に移動して統合をアクティブ化 **All** (すべて) > システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて) をクリックし、[インストール] を選択します。

   (Optional) これらの統合と提供される機能の詳細については、「ソフトウェア部品表 の詳細」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- Vulnerability Response Integration with Veracode。詳細については、「ServiceNow Vulnerability Response Integration with Veracode のインストール」を参照してください。
- NVD の脆弱性対応統合は、アップロードされたコンポーネントに関連付けられている脆弱性の拡張データを表示する場合に必要です。詳細については、「NVD 統合の概要」を参照してください。
- CWE Comprehensive 2000 Integration。このスケジュール済みジョブのアクティブ化の詳細については、「CWE レコードの更新のためのスケジュール済みジョブの構成および実行」を参照してください。

アプリケーションが正常にアクティブ化されると、メッセージが表示されます。

6. ユーザーに次のロールを割り当てます。
   - sn_sbom_dm.app_create
   - sn_sbom_dm.app_read
   - sn_sbom_dm.app_write
   - sn_sbom_core.sbom_ingest
   - sn_sbom_core.admin
   - sn_sbom_resp.sbom_analyst
   - sn_sbom_resp.manage_avi_rule
   - sn_sbom_response.managelicense
   - sn_sbom_response.licenseResolver
7. オプション: インポートされた SBOM データの脆弱性に対するアプリケーション脆弱性一致アイテムを作成する場合は、ユーザーをアプリセキュリティマネージャーグループにアサインします。

   (Optional) アプリセキュリティマネージャーグループにアサインされたユーザーは、アプリケーション脆弱性一致アイテムに優先順位を付けて管理します。このグループのユーザーは、レコードの読み取りと編集、およびアプリケーションとその修復ワークフローでサポートされている アプリケーション脆弱性対応 アプリケーションの設定に必要な多くのロールを継承します。
8. オプション: クローズ済み AVIT を自動的に [オープン] ステータスに戻さない場合は、[検出された場合は AVIT を再オープン (*sn_sbom_resp.reopen_avits_if_detected*)] システムプロパティを無効にします。

   (Optional) 次の条件が存在する場合、脆弱性が関連付けられているコンポーネントの クローズ済みの アプリケーション脆弱性一致アイテム (AVIT) が自動的に再オープン ([オープン] に設定) され、SBOM ワークスペースに表示されます。
   - 脆弱性が関連付けられている AVIT がサードパーティ統合の脆弱性スキャンによって再度検出されたか、脆弱性のあるコンポーネントが後続の SBOM アップロードの一部となっている場合。
   - [検出された場合は AVIT を再オープン (*sn_sbom_resp.reopen_avits_if_detected*)] システムプロパティを無効にしていません。このシステムプロパティはデフォルトで有効になっています。
   - クローズ済み AVIT のサブステートが、[緩和コントロールを実施]、[影響を受けていない]、または [誤検出] のいずれでもない。これらのサブステートを持つ AVIT は、システムプロパティによって再オープンされません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のタスク
SBOM ファイルをアップロードします。詳細については、「ソフトウェア部品表ファイルを手動でアップロードする」と「REST API を使用したソフトウェア部品表ファイルのアップロード」を参照してください。

の Deps.dev、OSV.dev、および **PaCE** 統合の構成 ソフトウェア部品表

Deps.dev および OSV.dev 統合のパラメーターを一部編集することができます。これらの統合には、内部ワークフローにのみ使用される 2 つのコードトリガーバージョンもあります。これらの統合をオンデマンドで開始しないでください。さらに、ポリシー・アズ・コード・エンジン (PaCE) を使用してポリシーを作成するためのスケジュール済みジョブをアクティブ化できます。

内部ワークフローのコードトリガー統合

SBOM Response v3.2 以降では、パフォーマンスが強化され、2 つの OSV.dev および Deps.dev コードトリガー統合が追加されました。

- OSV 統合 (オンデマンドコードトリガー)
- Deps.dev 統合 (オンデマンドコードトリガー)

これらの統合は、内部ワークフローにより自動的に開始され、内部でのみ使用されます。それらを見つけることはできますが、統合レコードから [今すぐ実行] ボタンを使用してこれらの統合をオンデマンドで開始することはできません。

Deps.dev 統合の実行スケジュールの構成

スケジュールを変更するには、次に移動します: **All** (すべて) > 脆弱性対応 > アドミニストレーション > 統合 > **Deps.dev** 統合. この統合のスケジュールを編集するには、sn_vul.app_configure_integrations ロールが必要です。

この Deps.dev 統合は、 古い ステータスと 破棄 ステータスのコンポーネントを識別するために使用されます。現在のコンポーネントバージョンは、最新のものより 2 年以上遅れており、メジャーバージョンが 2 つ遅れています。破棄されたコンポーネントが 2 年以上更新されていません。2 年と 2 つのバージョンのしきい値は、システムプロパティを使用して編集できます。これらのパラメーターを編集するには、 **All** (すべて) > システムプロパティ > すべてのプロパティ をクリックし、次のレコードを見つけます。

- sn_sbom_resp.pkg_abandoned_threshold
- sn_sbom_resp.pkg_stale_threshold
- sn_sbom_resp.pkg_stale_version_threshold

Deps.dev 統合 SBOM応答とともにインストールされます。統合はデフォルトで有効になっており (統合レコードで [アクティブ] チェックボックスが選択されている)、毎週実行されるようにスケジュールされています。これはオンデマンドの Deps.dev コードトリガー統合ではなく、統合レコードからスケジュールを編集し、スケジュール済みジョブをオンデマンドで開始できることに注意してください。 。

破棄および古いしきい値は月単位です。バージョンのしきい値は数値です。

インポートされたデータは、ワークスペースのホームページと BOM キューモジュールで表示できます。インポートされたデータは、パッケージグループ [sn_sbom_pkg_group] テーブルに保存されます。

OSV.dev 統合 - 包括的の構成と開始

OSV.dev 統合 - 包括的 統合は、 SBOM 応答とともにインストールされます。統合はデフォルトでアクティブ化されています (統合レコードの [アクティブ] チェックボックスが選択されています)。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

これはオンデマンドの OSV.dev コードトリガー統合ではなく、統合レコードからオンデマンドで開始する必要があることに注意してください。

この統合を構成して開始するには、次に移動します: **All** (すべて) > 脆弱性対応 > アドミニストレーション > 統合 > **OSV.dev** 統合 - 包括的. sn_vul.app_configure_integrations ロールが必要です。

インポートされたデータは、ワークスペースのホームページの [脆弱性] タブ、エンティティリストのレコード、およびライブラリモジュールで表示できます。インポートされたデータは、アプリケーション脆弱性エントリ [sn_vul_app_vul_entry] テーブルと脆弱性情報データベース エントリ [sn_vul_nvd_entry] テーブルに格納されます。

注:
OSV.devの *batchSize* 統合パラメータは、次の場所にある オープン・ソース脆弱性インスタンス の「統合パラメータ」タブで構成できます **All** (すべて) > 脆弱性対応 > アドミニストレーション > 統合 > 脆弱性統合 > オープンソース脆弱性インスタンス. デフォルトは、API 呼び出し当たり 75 Purl です。

この値はデフォルト設定のままにしてください。値を変更すると、パフォーマンスに影響を及ぼす可能性があります。

PaCE のアクティブ化

応答のバージョン 4.0 以降 SBOM 、 SBOM ワークスペースで利用可能な Policy as Code Engine (PaCE) インターフェイスで、「古い」と識別されたコンポーネントまたは破棄されたコンポーネントを ワークスペースで表示できます。

- *Run PaCE policies for SBOM Response* スケジュール済みジョブで、コンポーネントが古くなっているか破棄されているかを判断します。このスケジュール済みジョブは、デフォルトでは非アクティブです。
- SBOMワークスペースで利用可能かつ表示される PaCE インターフェイスで、「古い」または「非準拠」として破棄されたコンポーネントを表示します。

PaCE および PaCE ポリシーの詳細については、 Integrating PaCE with other applications を参照してください。

SBOMワークスペースでのSBOMファイルのアップロードと表示

SBOM アプリケーションを使用すると、ファイルをアップロードし、エンティティ、コンポーネントインベントリ、ライセンス情報、その他の詳細をソフトウェア部品表ワークスペースに表示できます。

SBOMファイルのアップロードの概要

ソフトウェア部品表ファイルは、API を介して、または手動でアップロードできます。エンティティとしてインポートしたファイルを表示します。これは、ソフトウェアで使用されているサードパーティコンポーネントライブラリのインベントリであり、推移的な依存関係を含みます。

- REST API を使用したソフトウェア部品表ファイルのアップロード.

  アップロード API は、 SBOM ファイル (CycloneDX/SPDX) をインスタンスにアップロードして取り込むために使用されます。

- ソフトウェア部品表ファイルを手動でアップロードする.

  ソフトウェア部品表ファイルを手動でアップロードします。ファイルのアップロードに使用する方法は、SBOM Core アプリケーションをインストールしているか SBOM Response アプリケーションをインストールしているかによって異なります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- DevOps SBOM ファイルの ソフトウェア部品表 のアップロード.

  継続的インテグレーションと継続的デプロイの開発サイクル全体を通じて、ソフトウェアの SBOM ファイルを生成してアップロードします。

- ライセンス管理モジュールでコンポーネントライセンスを分類して解決します。

  内部ポリシーまたは規制ポリシーに従って、SBOMファイルにアップロードするコンポーネントのライセンス情報をレビュー、分類、解決 (アサイン) します。コンポーネントをライセンスに一致させ、全体的なライセンスコンプライアンスを判断して、禁止、制限、または欠落したライセンスに対する潜在的なリスクエクスポージャーを確認できます。

- ソフトウェア部品表ワークスペースでのレポートとダッシュボードの表示

  脆弱性アナリストと脆弱性マネージャーは、アップロードされたソフトウェア部品表ファイルとレコード内の重要なデータ、データの可視化、および拡張脆弱性インテリジェンスとライセンス情報を ソフトウェア部品表 (SBOM) ワークスペースで表示できます。

  注:
  ワークスペース SBOM ランディング (ホーム) ページでデータの可視化を表示する場合は、Response をインストールする必要があります。

REST API を使用したソフトウェア部品表ファイルのアップロード

API を使用してソフトウェア部品表ファイルをアップロードする前に、次の情報を確認してください。

REST API の使用

API を使用して SBOM をアップロードするには、sn_sbom_core.sbom_ingest ロールが必要です。

アップロード API。

この API は、SBOM ファイル (CycloneDX / SPDX) をインスタンスにアップロードして取り込む際に使用されます。

SBOM Core v4.0 では、以下がサポートされています。

- CycloneDx の XML と JSON (バージョン 1.0～1.6)。
- SPDX の JSON (バージョン 2.2～2.3)

- **注:**
  32 MB 以上のファイルの場合、正しく読み込まれない場合があります。

HTTP メソッド：(POST)

API URL：`<host_name>/api/sbom/core/upload`

注:
`<host_name>` は ServiceNow インスタンス名です。

以下の要求パラメーターはすべてオプションです。要求本文は SBOM ファイルのコンテンツとなります。開発プロセスの一環で DevOps を使用している場合、「requestedBy」の値を「devops」にする必要があります。DevOps の一般的な情報については、「DevOps SBOM ファイルの ソフトウェア部品表 のアップロード」を参照してください。「requestedby」の値が「devops」(開発運用) の場合、次のパラメーターが必須となります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- buildId
- lifecycleStage

さらに、「requestedBy」が「devops」の場合、「fetchVulenrabilityInfo」と「fetchPackageInfo」のデータが含まれます。

- buildId：送信する文字列
- lifecycleStage：2 つの値 (「production」または「pre_production」)
- fetchVulenrabilityInfo：t/f
- fetchPackageInfo：t/f

要求パラメーター	可能な値	説明
productModelId	Sys ID	指定された SBOMのルートアプリケーションでマッピングする製品モデルの Sys ID。
businessApplicationId	Sys ID	指定された SBOM のルートアプリケーションでマッピングするビジネスアプリケーションの Sys ID。
businessApplicationName (非推奨)	ビジネスアプリケーション名	指定された SBOMのルートアプリケーションでマッピングするビジネスアプリケーションの名前。
sbomSource	たとえば、 Veracodeなどの製品	SBOMファイルのソース。
requestedBy	メソドロジーツールやメソドロジー名。「Jenkins」など。「devops」を使用する場合、「buildId」と「lifecycleStage」は必須です。	アップロード要求者
buildId	要求者が送信する文字列。	SBOMビルドのビルド ID。
lifecycleStage	「production」または「pre_production」	エンティティのライフサイクルステージ。
fetchVulenrabilityInfo	t/f (正/誤)	「true」の場合、脆弱性インテリジェンス統合がトリガーされます。
fetchPackage 情報	t/f (正/誤)	「true」の場合、パッケージインテリジェンス統合がトリガーされます。

アップロード API 応答:「status」の成功/失敗、「message」(文字列)、「bomRecordId」(アップロード API を介して返される SBOM の Sys ID) が含まれていました。

```
{

"result": {

"status": "success",
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
"message": "Queued for processing.",
"bomRecordId": "f207059b4393c290629aa597cbb8f247"
}
}
```


ステータス API

この API を使用して、取り込みのキューに入れられている SBOM のステータスやサマリーを取得します。

- API URL：`/api/sbom/core/upload/status`
- HTTP メソッド (GET)

要求パラメーター	可能な値	説明
bomRecordId	Sys ID	アップロード API を介して返される SBOM レコード ID です。これにより SBOM アップロードが正常に行われます。

ステータス API のデフォルトの応答例。


```
{
  "result": {
    "bomRecordId": "0407c0fea3e70a505df340f5251e617e",
    "uploadStatus": "processed",
    "additionalInfoStatus": "not_requested",
    "uploadSummary": {
      "components": {
        "added": 0,
        "removed": 0,
        "total": 70
      }
    }
  }
}
```


追加のパラメーターを使用したステータス API 応答の例。当該 SBOM の fetchVulenrabilityInfo を要求した場合、応答の一部として脆弱性のブレークダウンを取得できます。


```
{
 "result": {
  "bomRecordId": "93af349b4393c290629aa597cbb8f258",
  "uploadStatus": "processed",
  "additionalInfoStatus": "complete",
  "uploadSummary": {
```


自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
  "components": {
   "added": 0,
   "removed": 0,
   "total": 3
  },
  "vulnerabilityInfo": {
   "critical": 0,
   "high": 0,
   "medium": 0,
   "low": 0,
   "none": 0
  }
 },
 "buildId": "1"
}
}
```


当該 SBOM の fetchPackageInfo を要求した場合、応答の一部として「古い」および「破棄」カウントを取得できます。

SBOM が正常に処理された後、アップロードされたレコードを表示する場所は、使用しているアプリケーションにより異なります。

- SBOM Response を使用している場合、BOM エンティティレコードは、SBOM ワークスペースの BOM キューモジュールの [SBOM 取り込みステータス] リストに表示されます。
- SBOM Core を使用している場合は、次に移動します: **SBOM Core** > **BOM** 取り込みステータス.

サポートされている **SBOM** 標準と一般的な使用情報の強化

SBOM Core v4.0 では、以下がサポートされています。

- CycloneDx の XML と JSON (バージョン 1.0～1.6)。
- SPDX の JSON (バージョン 2.2～2.3)

- **注:**
  32 MB 以上のファイルの場合、正しく読み込まれない場合があります。

SBOM Core v4.0 以降、v1.0～1.6 の CycloneDx 標準をサポートするために、次の機能が拡張されました。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- CycloneDX SBOM ファイルの追加情報を (sn_sbom_core.collect_properties) プロパティでインポートします。このプロパティはデフォルトで非アクティブ化されています。一般的にサポートされていない情報をインポートするには、このプロパティを有効にします。これらのプロパティからインポートされた情報は、次の SBOM コンポーネントプロパティ [sn_sbom_comp_property] テーブルにアップロードされます。
  - アップロードされた SBOM ファイル
  - メタデータ
  - 個々の脆弱性
  - コンポーネント
- CycloneDX v1.4 以降、SBOM ファイルの宣言および締結ライセンスに関するインポート済みのコンポーネントデータが、次の 2 つの新しいライセンスフィールドに表示されます。
  - 宣言済み
  - 締結
- SBOM 構文解析のサポートが、以下の CycloneDX コンポーネントタイプに拡張されました。
  - バージョン 1.5：プラットフォーム、データ、デバイス ドライバー、機械学習モデル
  - バージョン 1.6：暗号化

SBOM Core v3.0 では、以下がサポートされています。

- CycloneDx の XML と JSON (v1.4 以前)
- SPDX の JSON (v2.3 以前)

呼び出し元ユーザーが適切に認証されており、ServiceNow インスタンスで sn_sbom_core.sbom_ingest ロールを持っている場合は、インスタンスの外部から API にアクセスして SBOM データをアップロードすることができます。

データはアップロードされた後、解析されます。データの解析前に、次の要件が検証されます。

- 受信データにおいて、JSON または XML が有効であることを確認します。
- BOM 形式がサポートされている。SBOM Core v2.1 以降、CycloneDX (JSON や XML) および SPDX (XML) 形式がサポートされています。
- データを解析できるように、最小限のフィールドが利用可能である。

これらのチェックの検証後に、部品表 [sn_sbom_doc] テーブルにエントリが作成され、受信 SBOM データが添付ファイルとして含まれます。

*Process BOM file*ビジネスルールは、レコードの挿入とデータの解析の結果として自動的にトリガーされます。

注:
このビジネスルールは、SBOM Core のインストール時にデフォルトでアクティブになります。

SBOM にリストされているすべてのコンポーネントには、type が定義されています。

- SBOM ファイルがアップロードされているコンポーネントは、BOM エンティティと見なされます。
- type=library としてリストされているコンポーネントは、サードパーティコンポーネントと見なされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連情報

ソフトウェア部品表ファイルのアップロードステータスを表示

ソフトウェア部品表ワークスペースでのレポートとダッシュボードの表示

ソフトウェア部品表ファイルを手動でアップロードする

ソフトウェア部品表 (SBOM) ファイルを手動でアップロードする

始める前に
バージョン 4.0 以降、SBOM Core は以下をサポートしています。

- CycloneDX のバージョン 1.0 から 1.6 の XML と JSON。
- SPDX のバージョン 2.2 ～ 2.3 の JSON。

必要なロール：sn_sbom_core.sbom_ingest

手順

1. ファイルを手動でアップロードする

   ファイルのアップロードに使用する方法は、SBOM Core アプリケーションをインストールしているか SBOM Response アプリケーションをインストールしているかによって異なります。

2. オプション: Veracode 脆弱性統合 によってインポートされた SBOM ファイルをアップロードします。

   注:
   Veracode ファイルを CycloneDX (JSON や XML) および SPDX (XML) 形式でアップロードできるのは、アプリケーション脆弱性対応 との Veracode 統合をインストールしてアクティブ化している場合のみです。詳細については、「Veracode 脆弱性統合」を参照してください。

タスクの結果
SBOM が正常に処理された後、アップロードステータスを表示する場所は、使用しているアプリケーションにより異なります。

- SBOM Response を使用している場合、BOM エンティティレコードは、SBOM ワークスペースの BOM キューモジュールの [SBOM 取り込みステータス] リストに表示されます。
- SBOM Core を使用している場合は、 **SBOM Core** > **BOM** 取り込みステータス.

関連情報

REST API を使用したソフトウェア部品表ファイルのアップロード

DevOps SBOM ファイルの ソフトウェア部品表 のアップロード

継続的統合と継続的展開の開発サイクル全体を通じて、ソフトウェアの ソフトウェア部品表 SBOM ファイルを生成してアップロードします。

DevOps ファイルと **SBOM** ファイル

SBOM ファイルは、ソフトウェアの継続的統合や継続的展開 (CI/CD) の 開発ライフサイクル全体を通して、さまざまな段階で生成されます。多くの場合、組織のソフトウェア開発運用 (DevOps) では、リリース後に表面化する可能性のあるバグに対して、一種の CI/CD プロセスで特定したり防止したりして、コストのかかる対応をしています。DevOps では、CI/CD パイプライン全体を通じて SBOM ファイルを生成し、脆弱性やリスクのあるコンポーネントを先回りしてチェックできるよ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

うになります。こうしたチェックにより、組織はソフトウェアの品質を向上させ、後のメンテナンスによるコストの発生を回避できるようになります。SBOM ファイルの生成は、CI/CD 開発時にビルド評価を正常に実装し、正確に自動化するうえで非常に重要となります。

開発パイプラインからの SBOM ファイルのアップロードは、次のバージョン以降の SBOM アプリケーションでサポートされています。

サポートされているバージョン

アプリケーション	サポートされているバージョン
SBOMデータモデル	v3.0、v2.0
SBOM Core	v5.0、v4.0、v3.0
SBOM Response	v5.0、v4.0、v3.2、3.1

ユースケース

DevOps ビルドパイプラインの一環で SBOM ファイルを生成し、SBOM アップロード API を介して送信すると、以下に関するカウントが表示され、パイプラインの成功や失敗を判断することができます。

- 追加されたコンポーネント
- 削除されたコンポーネント
- 脆弱性情報
- パッケージ情報 (破棄済み / 古いコンポーネント)

パイプラインの成功や失敗に関する DevOps ポリシーおよびルールは、SBOM ステータス API から受信した脆弱性の数や、「古い」「破棄済み」コンポーネントの数のしきい値によって定義される場合があります。

パイプラインの失敗の場合、DevOps ユーザーは ServiceNow® インスタンスの失敗ビルドに関する情報にアクセスすることで、脆弱性の根本原因や発生元をより深く理解できるようになります。

アップロード API や ステータス API の (POST) および (GET) パラメーターや URL について、詳細は「REST API を使用したソフトウェア部品表ファイルのアップロード」を参照してください。

ドメインセパレーション

SBOM アプリケーション内のテーブルはすべてドメインセパレーションされています。

ソフトウェア部品表ワークスペースでのライセンスの分類とコンポーネントライセンスの解決

ライセンスを分類してコンポーネントに解決 (照合) するか、 SBOM ワークスペースのライセンス管理モジュールでライセンスを作成します。ライセンスを分類してコンポーネントに一致させることで、 SBOM ファイルにアップロードするプロプライエタリ、オープンソース、ベンダー提供のソフトウェア コンポーネントのライセンス コンプライアンスを判断できます。

ライセンスデータとサードパーティソフトウェア

組織が独自のソフトウェアアプリケーションを構築するが増えるにつれて、オープンソースコンポーネントとベンダーが提供するソフトウェアを使用しています。サードパーティおよびオープンソースのコンポーネントを使用すると、ソフトウェアプロジェクトを迅速に作成してリリースするための多くの利点がありますが、これらのコンポーネントを使用するとライセンスのリスクが伴います。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- オープンソースおよびベンダー提供のソフトウェアコンポーネントは、他のコンポーネントに依存することがあり、各コンポーネントには独自のライセンス要件がある場合があります。
- アプリケーションのコンポーネントとソフトウェアのライセンス条件に準拠していない場合、内部ポリシーと規制ライセンス要件に違反するコードを誤って出荷する可能性があります。

ライセンス管理モジュール

SBOM ワークスペースのライセンス管理モジュールでは、次のタスクを実行できます。

- SBOMファイルとともにアップロードするコンポーネントに対して、ライセンスを必要とするライセンスを分類します。
- 分類した各ライセンスを特定のコンポーネントに解決します。
- 使用しているコンポーネントの何パーセントがコンプライアンス違反であるかを、ホームページのデータ可視化で確認します。この情報を使用して、全体的なセキュリティ体制と潜在的なリスクエクスポージャーを判断できます。

アップロードする SBOM ファイルにライセンス情報が含まれている場合、各 SBOM アップロードで一意のライセンスが確認されると、ライセンスデータベースが自動的に拡張されます。各 SBOM アップロードで、アップロードされたライセンスのデータベースを構築し、必要に応じて SBOM Workspace のライセンス管理モジュールで分類できます。ライセンスのインベントリを作成し、ライセンスを次のいずれかのカテゴリに分類した後、コンポーネントに割り当てることができるようにします。

- 許可
- Restricted (制限付き)
- 禁止
- 未分類

法務担当者、ライセンスマネージャー、コンプライアンス、および規制マネージャーは、ライセンス管理モジュールでタスクを実行します。

アップロードされたライセンスデータの表示

コンポーネントとともにアップロードしたライセンス情報を SBOM ワークスペースで表示するには、次のオプションがあります。

- 次のように移動する。 ワークスペース > **SBOM** ワークスペース > コンポーネント.

  [コンポーネント] ページの [コンポーネントのライセンス分類] カードには、次のカテゴリに対する全体的なライセンスコンプライアンスが可視化されて表示されます。

Category (カテゴリ)	説明
禁止	ライセンスの使用は許可されていません。
分類が必要	ライセンスはまだ分類されておらず、レビューが必要です。
許可	ライセンスの使用は制限なしで許可されます。
Restricted (制限付き)	特定のユースケースでは、ライセンスの使用は許可されていません。

  このスナップショットでは、ライセンス管理モジュールに入力した分類と解決済みのライセンス情報を使用して、全体的なライセンスコンプライアンスを計算します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このリストからコンポーネントレコードを選択すると、[ステータス] フィールドに他の情報とともにコンポーネントのライセンス情報を表示できます。

- または、 ワークスペース > **SBOM** ワークスペース > ライセンス管理 > ライセンスの分類.

  このページでは、アップロードした SBOM ファイルから検出された一意のライセンスの合計数を追跡します。また、ページの上部にある次のカテゴリのカードでもフィルタリングされます。

  - 未分類:ライセンスにはレビューと分類が必要です。
  - 禁止:ライセンスの使用は許可されていません。
  - 制限付き:特定のユースケースではライセンスは許可されません。
  - 許可:ライセンスの使用は制限なしで許可されます。
  - すべてのライセンス:ライセンスの合計数。

  組織内のすべてのコンポーネントが、このページに記載されているいずれかのライセンスを使用しています。SBOM アップロードから新しいライセンスが検出されると、レコードが作成されて SBOM ライセンス [sn_sbom_license] テーブルに保存され、このリストに追加されます。デフォルトの分類は [分類が必要] です。このステータスのライセンスレコードは、全体的なライセンスコンプライアンスを正確に計算するために、コンポーネントに解決 (照合) する前に確認して分類する必要があります。

  ライセンスの分類方法については、「 インポートされたライセンスを ソフトウェア部品表 ワークスペースに分類」を参照してください。

ロール

新しいライセンスは、sn_sbom_response.managelicense ロールを持つユーザーが分類する必要があります。このユーザーは、アップロードされたライセンス情報を表示し、許可されているライセンスと禁止されているライセンスを決定します。このロールを持つユーザーは、sn_sbom_response.licenseresolver ロールを持っていない限り、コンポーネントライセンス解決モジュールを表示できません。

分類後、全体的なライセンスコンプライアンスを判断できるように、sn_sbom_response.licenseresolver ロールを持つユーザーがライセンスを解決する必要があります。このユーザーは、ライセンスをコンポーネントに解決します。このロールを持つユーザーは、sn_sbom_response.managelicense ロールを持っていない限り、ライセンス分類モジュールを表示できません。

新しいライセンス情報の分類は進行中のプロセスです。[未分類] カードに表示される合計数は低く抑えることをお勧めします。ライセンスマネージャーは、SBOM ファイルをアップロードした後に、数日ごとに分類が必要なライセンスを確認することをお勧めします。

ライセンス リゾルバーとして、数日ごとに更新された分類されたライセンスを確認することをお勧めします。

インポートされたライセンスを ソフトウェア部品表 ワークスペースに分類

ライセンス分類機能を使用して、 SBOM ファイルとともにアップロードするコンポーネントライセンスを分類します。

始める前に

新しいライセンス情報の分類は進行中のプロセスです。[未分類] カードに表示される合計数は低く抑えることをお勧めします。ライセンスマネージャーは、SBOM ファイルをアップロードした後に、数日ごとに分類が必要なライセンスを確認することをお勧めします。

必要なロール:sn_sbom_response.managelicense

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > **SBOM** ワークスペース > ライセンス管理 > ライセンスの分類.

   注:
   sn_sbom_response.licenseresolver ロールも持っていない限り、[ライセンスの分類] タブのみが表示されます。

2. オプション: カードを選択して、分類でライセンスをフィルタリングします。
3. ライセンスを分類するには、ライセンスを 1 つ選択します。
4. ライセンスを分類したら、 分類されたライセンスをコンポーネントに解決する準備が整います。

ソフトウェア部品表ワークスペースのコンポーネントに対するライセンスの解決

コンポーネントライセンス解決機能を使用して、分類されたライセンスを特定のコンポーネントに解決 (アサイン) します。情報が不足しているコンポーネントやライセンス情報が正しくないコンポーネントにライセンスをアサインするか、新しいライセンスを作成して、全体的なライセンスコンプライアンスを計算できるようにします。

始める前に
必要なロール:sn_sbom_response.licenseresolver

手順

1. 次のように移動する。 ワークスペース > **SBOM** ワークスペース > ライセンス管理 > コンポーネントライセンス解決.

   注:
   sn_sbom_response.managelicense ロールも持っていない限り、[コンポーネントライセンス解決] タブのみが表示されます。

   このページでは、アップロードした SBOM ファイルから検出された一意のライセンスの合計数とライセンスの合計が一目でわかるビューで追跡されます。このページに表示されるライセンスは、コンポーネントに関連するため、大きく 2 つのカテゴリに分類されます。

   - コンポーネントのすべてのインスタンスがライセンスに同意します。
   - 1 つのライセンスについて意見の相違があり、1 つのコンポーネントに複数のライセンスがある場合。

   2 番目のケースでは、1 つのライセンスが 1 つのコンポーネントに解決されるように、これらのライセンスを調整する必要があります。ライセンスコンプライアンスは、コンポーネントごとに 1 つの解決済みライセンスに基づいて計算されます。

   このページのライセンスは、解決に役立つ次のカテゴリにフィルタリングされています。

値	説明
未解決のライセンスを持つコンポーネント	コンポーネントにライセンスが割り当てられておらず、解決が必要です。(空) は、これらのコンポーネントの [解決済みのライセンス] 列に表示されます。不足しているライセンスと複数

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

値	説明
	のライセンスの両方の合計は、このカテゴリの一部としてリストされます。
ライセンスのないコンポーネント。	解決が必要な、ライセンス情報が不足しているコンポーネント。
複数のライセンスを持つコンポーネント	異なるライセンスを持ち、解決が必要な複数のエンティティに表示されるコンポーネント。
すべてのコンポーネント	組織内で追跡されているコンポーネントの合計リスト。このフィルター済みリストからライセンスを変更できます。

2. カードを選択します。
3. いずれかを選択してライセンスを解決します。

4. SBOM ワークスペースのホームページに移動して、[コンポーネントのライセンス分類] 可視化で使用しているコンポーネントの割合がコンプライアンス違反であるかどうかを確認します。
この可視化のデータは、[BOM コンポーネントのライセンスブレークダウン] スケジュール済みジョブによって毎日更新されます。このジョブは、毎日実行される SBOM レポートデータコレクターのスケジュール済みジョブの一部です。

ソフトウェア部品表ワークスペースでのレポートとダッシュボードの表示

脆弱性アナリストは、ソフトウェア部品表 (SBOM) ワークスペースでレコード内のアップロードされたソフトウェア部品表ファイル、データの可視化、および拡張脆弱性インテリジェンスを表示します。

SBOM Core

ホーム (ランディング) ページと SBOM Workspace のコンポーネントモジュールで、BOM エンティティとアップロードしたコンポーネントのリストを表示できます。

SBOM Response

SBOM Response アプリケーションは、SBOM ワークスペースのホーム (ランディング) ページにおいて、データを可視化して、BOM エンティティ、脆弱性のあるエンティティ、アクティブなアプリケーション脆弱性一致アイテムに関する詳細情報を提供します。SBOM Response を有するワークスペースには、次のモジュールが含まれています。

- ホームページ - データの可視化と拡張された脆弱性の詳細。
- コンポーネント - コンポーネントのバージョンと修正情報、 およびコンポーネントのライセンス分類。
- AVIT (アプリケーション脆弱性一致アイテム) 作成ルール - アプリケーション脆弱性一致アイテム (AVIT) が作成される場合の条件。
- BOM キュー - ファイルのアップロードステータスと履歴。
- リスト - 脆弱なコンポーネントとライブラリの AVIT レコード (NVD、CWE、およびアプリケーション脆弱性)。

次のトピックでは、ソフトウェア部品表ワークスペース内のコンポーネントの詳細を見つける方法について詳しく説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ソフトウェア部品表ワークスペースのホームページを確認する
- ソフトウェア部品表ワークスペースの [コンポーネント] モジュールの確認
- ソフトウェア部品表ファイルのアップロードステータスを表示
- ソフトウェア部品表エンティティの脆弱性のチェック
- ソフトウェア部品表ワークスペースでのライセンスの分類とコンポーネントライセンスの解決

ソフトウェア部品表ワークスペースのホームページを確認する

アップロードされたデータは、ソフトウェア部品表 (SBOM) ワークスペースのランディング (ホーム) ページの可視化にロールアップされます。ファイルのアップロード後にデータが変更されるため、脆弱性アナリストは傾向を確認し、コンポーネントに関する現在の情報を確認できます。

始める前に

必要なロール:sn_sbom_resp.sbom_analyst

手順

1. 次のように移動する。 ワークスペース > **SBOM** ワークスペース.
   デフォルトでは、ランディングページ (ホーム) が表示されます。

   モジュールに表示されるアプリケーションは、インストールしたアプリケーションによって異なります。

   インポートされたデータは、ライブクエリによって計算および入力されません。[ホーム] および [コンポーネント] ページのスコアは毎日 1 回更新され、レポートのパフォーマンスが強化されています。この機能拡張により、 SBOM ワークスペースの [ホーム] および [コンポーネント] モジュールのスコアカードにおけるロード時間が短縮される可能性があります。

   データの保存方法や保存場所への影響はありません。

インストール済みアプリケーション	説明
SBOM Core をインストールしている場合	すべての BOM エンティティ。リストには、各エンティティの名前、分類子 (アプリケーション、コンテナ、ライブラリなど)、およびコンポーネント数が含まれます。BOM エンティティは、SBOMドキュメントが生成およびアップロードされたSBOMファイルのルートレベルのコンポーネントを参照します。 ワークスペースのホームページに移動して 、BOM エンティティのリストを表示します。
SBOM Response をインストールしている場合	次のデータの可視化が表示されます。 ○ すべての BOM エンティティ:タイプ (アプリケーション、コンテナ、ライブラリ、およびその他) 別の BOM エンティティのブレークダウン。BOM エンティティは、SBOMドキュメントが生成およびアップロードされたSBOMファイルのルートレベルのコンポーネントを参照します。 ○ 脆弱性のある BOM エンティティ - 依存するコンポーネントに脆弱性が関連付けられて

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インストール済みアプリケーション	説明
	いるエンティティ。エンティティの依存関係に 重大な 脆弱性が 1 つある場合、エンティティの重大度は重大と見なされます。 ○ アクティブな AVI:毎日作成されるアプリケーション脆弱性一致アイテム (AVI) の数の傾向。 データの可視化には、過去 30 日間のデータが表示されます。30 日間の範囲は編集できません。このデータは、アプリケーション脆弱性一致アイテムの作成ルールを確認して設定した後に利用可能になります。詳細については、「ソフトウェア部品表ワークスペースでアプリケーション脆弱性一致アイテムのルールを作成する」を参照してください。

2. データ可視化カードを選択すると、そのレコードリストが表示されます。
3. [ホーム] タブを選択してランディングページに戻ります。
4. または、[**BOM** エンティティ] リストでレコードを選択します。

   エンティティ名とバージョンがレコードの上部に表示されます (例：SNC-SECOPS-SIR2.0)。

   > **注:**
   > ライセンス管理モジュールでは、エンティティとライセンスの関係はこのリストに表示されません。コンポーネントが使用されているエンティティを表示するには、コンポーネントモジュールに移動し、コンポーネントレコードを開きます。コンポーネントレコードでは、[ステータス] (未解決または未分類) を表示できます。

5. エンティティレコードのタブを選択して、データを確認します。

   a. 選択されていない場合は、[概要] タブを選択します。

      データを確認します。このレコードのフィールドにデータが入力されていない場合、アップロードした SBOM ファイルにデータが含まれていません。

名前	説明
名前	エンティティ名。
分類子	エンティティタイプ (アプリケーション、コンポーネント、ライブラリなど)。
バージョン	エンティティのバージョン番号。
サプライヤー	エンティティを提供した製品。
製品モデル	既存の製品モデルがない場合、または API を介した SBOM アップロード時に製品モデルを含めない場合は、作成されます。エンティティの名前は、製品モデルレコードに使用されます (SNC-SECOPS-SIR2.0 など)。

   b. [依存先] タブを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このエンティティのすべての依存関係と分類子 (ライブラリなど) が一覧表示されます。バージョン番号、 ライセンス、およびその他の情報が表示されます。

このリストのリンクを選択すると、レコードが開きます。そのタブは、[ホーム] タブと [エンティティレコード] タブの下に表示されます。開いたレコードには、概要、ハッシュ、BOM エンティティ、脆弱性、およびアプリケーション脆弱性一致アイテム (AVIT) のレビュー可能な関連リストが含まれている場合があります。

[BOM エンティティ] 関連リストには、この表示アイテムが使用されているすべてのエンティティが表示されます。

c. [脆弱性] タブを選択して、このエンティティの依存関係に関連付けられている脆弱性を確認します。

表示されるエンティティの脆弱性の詳細については、「ソフトウェア部品表ファイルのアップロードステータスを表示」を参照してください。

d. [AVI] タブを選択して、このエンティティに対するアプリケーション脆弱性一致アイテムがあるかどうかを表示します。

6. オプション: レコードを確認した後、1 つ以上の BOM エンティティレコードが不要になったと判断した場合は削除できます。

> **注:**
> BOM エンティティレコードを削除すると、それらとそのコンポーネント関係が完全に削除されます。BOM エンティティに関連付けられているすべてのアプリケーション脆弱性一致アイテム (AVIT) は [クローズ済み] に移行されます。削除したレコードとコンポーネントの関係を BOM エンティティリストに戻し、ワークスペースで使用できるようにすることを後で決定した場合は、これらの BOM エンティティを再度アップロードする必要があります。

a. ホームページに表示されていない場合は、[ホーム] タブを選択して戻ります。

b. [**BOM** エンティティ] リストで、削除するレコードを選択します。

c. [削除] を選択します。

ソフトウェア部品表ワークスペースの [コンポーネント] モジュールの確認

ソフトウェア部品表 (SBOM) ワークスペースの [コンポーネント] モジュールには、インポートしたコンポーネントの脆弱性、古い、破棄された、および高リスクの組み合わせに関する現在の情報が表示されます。

コンポーネントモジュールの表示

必要なロール:sn_sbom_resp.sbom_analyst

次のように移動する。 ワークスペース > **SBOM** ワークスペース > コンポーネント.

モジュールに表示されるアプリケーションは、インストールしたアプリケーションによって異なります。

インポートされたデータは、ライブクエリによって計算および入力されません。[ホーム] および [コンポーネント] ページのスコアは毎日 1 回更新され、レポートのパフォーマンスが強化されています。この機能拡張により、 SBOM ワークスペースの [ホーム] および [コンポーネント] モジュールのスコアカードにおけるロード時間が短縮される可能性があります。

データの保存方法や保存場所への影響はありません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

インストール済みアプリケーション	説明
SBOM Core をインストールしている場合	次の情報を含むアップロードされたすべてのコンポーネントのインベントリ。 • 名前 • 説明 • バージョン • BOM エンティティ数
SBOM Response をインストールしている場合	グラフまたはグラフ上の数値を選択すると、関連レコードのリストが表示されます。 すべてのコンポーネント [古い] コンポーネントと [放棄]されたコンポーネントのリスト、および合計コンポーネント数に少なくとも 1 つの脆弱性があるコンポーネントのリスト。これらの数は、注意が必要なコンポーネントを特定するのに役立ちます。すべてのコンポーネントがこれらのカテゴリに当てはまらない可能性があるため、これらのコンポーネントのサブセットはコンポーネントの合計数と一致しない場合があります。 • 現在のコンポーネントバージョンは、最新のものより 2 年以上遅れており、メジャーバージョンが 2 つ遅れています。 • 破棄されたコンポーネントが 2 年以上更新されていません。 • 脆弱性一致コンポーネントとは、重大度が [高] 以上の脆弱性があるコンポーネントのことです。 高リスクの組み合わせ リスクの高いコンポーネントには、早急な対応が必要な場合があります。SBOM Response アプリケーションのインストール時にインストールされる Deps.dev 統合は、ステータスが [古い] および [破棄] のコンポーネントのパッケージインテリジェンスを提供します。 インポートされたリスクの高い組み合わせは、更新、交換、または別のタイプの修復で修正できる、

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インストール済みアプリケーション	説明
	少なくとも 1 つの重大な ([重大] または [高]) 脆弱性を持つ古いコンポーネントと放棄されたコンポーネントで構成されています。[完全に修正可能 **(Completely fixable)**] ステータスは、コンポーネントに修正可能なバージョンがあることを意味します。修正可能なバージョンを持つ高リスクコンポーネントの合計数の割合が表示されます。 脆弱なコンポーネントの修正可能性 [重大]、[高]、[中]、[低] の脆弱性があるコンポーネントの合計とブレークダウン、およびそれらの脆弱性の一部またはすべてを修正できるかどうか。コンポーネントに複数の脆弱性がある場合は、最も重大な脆弱性が優先されます。 修正可能性ステータス： • 完全 - コンポーネントの現在のバージョンに関連付けられているすべての脆弱性の修正バージョンがあります。 • 部分的 - コンポーネントの現在のバージョンに関連付けられている修正バージョンが少なくとも 1 つありますが、すべての脆弱性ではありません。 コンポーネントのライセンスの分類 ライセンス分類別のコンポーネントの合計とブレークダウン。 ビジュアル化の下の [コンポーネントリスト] では、名前、説明、バージョン、エンティティ数を確認できます。右側のパネルでは、バージョン履歴を表示できます。バージョン履歴で現在のバージョンが強調表示されます。[共通脆弱性識別子 (**CVE**)] 列と [修正可能性 **(Fixability)**] 列も表示されます。

脆弱性インテリジェンスによるリスク評価

ワークスペースで脆弱性インテリジェンスデータを確認する方法の詳細については、「ソフトウェア部品表エンティティの脆弱性のチェック」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ライセンスコンプライアンスによるリスクの評価

コンポーネントを使用してインポートしたデータにライセンスを付与する方法と、ワークスペースで全体的なライセンスコンプライアンスを表示する方法の詳細については、 ソフトウェア部品表ワークスペースでのライセンスの分類とコンポーネントライセンスの解決 を参照してください。

ソフトウェア部品表ワークスペースでアプリケーション脆弱性一致アイテムのルールを作成する

ソフトウェア部品表 (SBOM) ワークスペースでアプリケーション脆弱性一致アイテム (AVIT) を表示するには、AVIT を作成する条件を設定しておく必要があります。

SBOM ワークスペースの AVIT

SBOM Response アプリケーションをインストールしてアクティブ化している場合、インポートされたデータのいずれかが既存の AVIT 作成ルールの条件に一致すると、 SBOM ファイルの AVIT が作成されます。

SBOM Response および 脆弱性対応 アプリケーションでは、アプリケーション脆弱性一致アイテム (AVIT) を自動的に作成し、アプリケーション脆弱性対応 ワークフローで修復するためのルールを設定する必要があります。詳細については、「ソフトウェア部品表 の詳細」を参照してください。

sn_sbom_resp.manage_avi_rule ロールを持つユーザーは、取り込まれたSBOMデータで見つかった脆弱性の AVIT を作成する前に、SBOMワークスペースに AVIT 作成ルールを追加する必要があります。AVIT を使用すると、アプリケーションで使用されているサードパーティコンポーネントの完全性を評価できます。脆弱性が関連付けられているコンポーネントとアプリケーションが一致したときに、インスタンスに AVIT が作成されます。

SBOM ワークスペースでは、SBOM AVIT のみを表示できます。ただし、脆弱性対応 の脆弱性マネージャーワークスペースでは、SBOM AVIT を他のタイプの脆弱性一致アイテムとともに表示できます。リストモジュールの SBOM ワークスペースで作成されたすべての AVIT を表示できます。リストモジュールには、すべての NVD エントリーおよび CWE エントリーとアプリケーション脆弱性も含まれています。

脆弱性情報データベース (NVD) などの既知の脆弱性リストからの推奨事項に基づいて、修復のために AVIT をアサインすることもできます。スケジュール済みジョブがトリガーされ、取り込まれたデータが作成ルールの条件と一致すると、AVIT が作成されます。

カスタマイズされたルールを設定することで、AVIT を追跡および修復できます。

ルールの作成方法については、「ソフトウェア部品表ワークスペースでアプリケーション脆弱性一致アイテムルールを作成する」を参照してください。

脆弱性対応の**Vulnerability Manager** ワークスペースでの **SBOM AVIT**

アクセスできる場合は、Vulnerability Manager ワークスペースの SBOM ワークスペースで作成された SBOM AVIT を表示できます。

注:
すべての AVIT ではなく脆弱性マネージャーのワークスペースでVulnerability Manager ワークスペースリストからの SBOM AVIT のみを表示するには、アプリケーション脆弱性一致アイテム [sn_vul_app_vulnerable_item] テーブルで条件 [ソース] [は次の値に等しい **(=)] [SBOM] AND** [スキャンタイプ] [は次の値に等しい **(=)] [SBOM-SCA]** を設定します。テーブルを表示するには、インスタンスで [すべて] に移動し、フィルターナビゲーターに「**sn_vul_app_vulnerable_item.list**」と入力します。

脆弱性マネージャーのワークスペースの詳細、監視トピックの表示方法、アプリケーションの修復作業、およびVulnerability Manager ワークスペースで脆弱性対応アプリケーションから構成された AVIT のアプリケーション修復タスクルールの詳細については、「の使用 でトピックを監視する Vulnerability Manager ワークスペース」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復タスク (AVUL) は AVIT から作成され、アサインルールに基づいて修復のためにグループに自動的にアサインされます。これらのルールの作成方法の詳細については、以下のトピックを参照してください。

- 脆弱性対応 アサインルールの作成または編集
- 脆弱性対応 修復タスクルールの作成または編集 および で修復作業を作成する Vulnerability Manager ワークスペース。

SBOM 応答でのアプリケーション脆弱性一致アイテムの再オープン

次の条件が存在する場合、脆弱性が関連付けられているコンポーネントの クローズ済みの アプリケーション脆弱性一致アイテム (AVIT) が自動的に再オープンされ、 SBOM ワークスペースに表示されます。

- 脆弱性が関連付けられている AVIT がサードパーティ統合の脆弱性スキャンによって再度検出されたか、脆弱性のあるコンポーネントが後続の SBOM アップロードの一部となっている場合。
- [検出された場合は AVIT を再オープン (*sn_sbom_resp.reopen_avits_if_detected*)] システムプロパティを無効にしていません。このシステムプロパティはデフォルトで有効になっています。
- クローズ済み AVIT のサブステートが、[緩和コントロールを実施]、**[**影響を受けていない]、または [誤検出] のいずれでもない。これらのサブステートを持つ AVIT は、システムプロパティによって再オープンされません。

このシステムプロパティは、 クローズ済み AVIT を自動的に再オープンしない場合にのみ非アクティブ化してください。

ソフトウェア部品表ファイルのアップロードステータスを表示

ソフトウェア部品表 (SBOM) ワークスペースの BOM キューモジュールにアップロードするソフトウェア部品表 (SBOM) ファイルのアップロードステータスを確認します。正常にアップロードされたファイル、アップロード履歴、およびエラーを追跡します。

始める前に

必要なロール:sn_sbom_resp.sbom_analyst

手順

1. アップロードステータスを表示します。

   アップロードステータスの表示に使用する方法は、インストールしたアプリケーションによって異なります。

オプション	説明
SBOM Core	a. 次のように移動する。 **All** (すべて) > **SBOM Core** > **BOM** 取り込みステータス. b. [部品表] リストで、[ステータス]、**[BOM** 生成時刻]、および [作成済み] 列で詳細を確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
SBOM Response	**a.** 次のように移動する。 **All** (すべて) > **SBOM** ワークスペース > **BOM** キュー. **b.** 可視化カードを選択して、アップロードしたファイルのカテゴリに関する次の詳細を確認します。 ▪ 過去 30 日間の BOM の更新 - 過去 30 日間に正常にアップロードおよび解析された BOM エンティティの合計数。 ▪ ソースのアップロード - 正常にアップロードされた SBOM ファイルの合計数と、SBOM を取り込むために使用した方法 (API または手動) のブレークダウン。 ▪ カテゴリ別のアップロードエラー - アップロードエラーの上位 5 つのカテゴリ。この可視化にデータが表示されない場合は、すべての SBOM ファイルが正常にアップロードされています。

部品表テーブル [sn_sbom_doc_list] と BOM キューモジュールのステータス情報には、BOM 形式、取り込みステータス、および BOM 生成時刻の両方が含まれます。BOM 取り込みの [ステータス] 列には、次のステータスが含まれます。

- キューに格納 - SBOM データがアップロードされました。
- 処理中 - コンポーネントデータはインポートの一部として処理されています。
- 処理済み - データの取り込みが正常に完了しました。
- エラー - 処理中にエラーが発生しました。

アップロードされたファイルのステータスに加えて、BOM エンティティレコードを選択することで、取り込んだコンポーネントのリストを表示できます。

2. オプション: 歯車アイコン (⚙) を選択し、[エラーカテゴリ] や [エラーの詳細] などのフィールドを追加して、 エラーとアップロードステータスに関する詳細情報にアクセスします。

ソフトウェア部品表エンティティの脆弱性のチェック

アップロードされたソフトウェア部品表 (SBOM) ファイル内のコンポーネントに脆弱性が関連付けられているかどうかを判断します。

脆弱性と拡張脆弱性データを表示するには、次のアプリケーションをインストールしてアクティブ化する必要があります。

- SBOM Response
- NVD の脆弱性対応統合および CWE ジョブ
- 脆弱性対応

詳細については、「ソフトウェア部品表 の詳細」を参照してください。

必要なロール:sn_sbom_resp.sbom_analyst

1. 次のように移動する。 **All** (すべて) > **SBOM** ワークスペース > コンポーネント.
2. 脆弱性情報は、可視化またはコンポーネントレコードのいずれかを使用して表示できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

メソッド	アクション
脆弱性がある BOM エンティティの可視化	脆弱性がある **BOM** エンティティの可視化グラフを選択します。 ○ 脆弱性がコンポーネントに関連付けられている場合、合計数はリストの [CVE] 列と [CWE] 列にが表示されます。コンポーネントには複数の脆弱性が存在する可能性があります。利用可能な場合は、このリストの [修正可能性] 列でエントリを確認できます。 ○ このコンポーネントに脆弱性が関連付けられていない場合、これらの列には 0 が表示されるか、コンポーネントの値が表示されません。 [CVE]、[CWE]、および [修正可能性 (Fixibilty)] 列が表示されない場合は、ページの右上にある歯車アイコン と [列を編集] を選択して、それらをページに追加できます。[利用可能] 列の一覧からそれらを選択し、**[OK]** を選択します。
コンポーネントレコード	**a.** [可視化] の下にあるリストからレコードを選択します。 **b.** レコードの [脆弱性] タブを選択します。 **i.** データが表示されない場合、レポートされた脆弱性はレコードに関連付けられません。 **ii.** データが表示された場合は、「ソフトウェア部品表ワークスペースの [コンポーネント] モジュールの確認」を参照し、脆弱性に対処するためのアプリケーション脆弱性対応の修復ワークフローの手順に従ってください。 詳細については、「アプリケーション脆弱性対応 の脆弱性を修復する」を参照してください。

脆弱性インテリジェンスによるリスク評価

コンポーネントレコードの SBOM Response を使用して、さらに拡張された脆弱性データを表示します。「サポートされているアプリケーション」で説明されている SBOM Response アプリケーション、脆弱性対応、脆弱性情報データベース (NVD) 統合および共通脆弱性タイプ一覧 (CWE) のスケジュール済みジョブをインストールしてアクティブ化する必要があります。

1. [すべてのコンポーネント] の画像を選択して、関連するレコードのリストを表示します。
2. [名前] 列のリンクを選択してレコードを開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[古い]、 [放棄]、[脆弱] などのステータスがコンポーネント名の下に表示されます。コンポーネントは、これらの状況を任意に組み合わせることができます。ステータスが表示されない場合、コンポーネントは古くなく、放棄されておらず、脆弱でもありません。

現在のバージョンと最新の公開バージョンをレビューします。右側のパネルでは、バージョン履歴を表示できます。現在のバージョンはバージョン履歴で強調表示され、リスト内のその場所によって、コンポーネントが [古い]、[放棄]、[脆弱] である理由に関するインサイトが得られる場合があります。たとえば、古いバージョンのコンポーネントを使用している可能性があります。

3. レコードの [概要]、[ハッシュ]、**[BOM** エンティティ]、[脆弱性]、および **[AVI]** 関連タブを選択します。
   - 概要：コンポーネント詳細のサマリー。
   - BOM エンティティ：このコンポーネントに関連付けられているエンティティのリスト。
   - ハッシュ - インポートした場合、ハッシュが表示されます。
   - 脆弱性 - このコンポーネントに関連する既知の脆弱性に関する情報。このリストが空の場合、既知の脆弱性はありません。

     リストに入力されている場合は、タブを選択して、このレコードに関連付けられた共通脆弱性識別子 (CVE) および共通脆弱性タイプ一覧 (CWE) データの脆弱性 ID、サマリー、およびその他の脆弱性情報を表示します。CVE は重大度別にブレークダウンされ、CWE はコンポーネントが悪用される可能性によってブレークダウンされます。脆弱性 ID リンクを選択すると、脆弱性対応アプリケーションまたはアプリケーション脆弱性対応アプリケーションの拡張脆弱性レコードを表示できます。

   - AVI (AVIT) - コンポーネントを既知の脆弱性に照合する AVIT 作成ルールを作成した場合、このコンポーネントに関連付けられたアプリケーション脆弱性一致アイテム。アプリケーション脆弱性対応アプリケーション (AVR) は脆弱性をアプリケーションに関連付けて AVI レコードを作成します。詳細については、「ソフトウェア部品表ワークスペースでアプリケーション脆弱性一致アイテムのルールを作成する」を参照してください。

自動翻訳

ソフトウェア部品表 アプリケーションとともにインストールされるコンポーネント

ソフトウェア部品表アプリケーションが有効になると、いくつかのタイプのコンポーネント (テーブル、ユーザーロール、スケジュール済みジョブなど) がインストールされます。

インストールされるロール

ロール タイトル [名前]	説明	含まれるロール
sn_sbom_response.managelicense	このロールは、SBOM Response アプリケーションと一緒にインストールされます。 このロールでは、コンポーネントのライセンスを解決することができます。	なし
sn_sbom_response.licenseResolver	このロールは、SBOM Response アプリケーションと一緒にインストールされます。	なし

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロール タイトル [名前]	説明	含まれるロール
	このロールでは、アップロードされたライセンス情報を表示し、許可するライセンスと禁止するライセンスを決定することができます。	
SBOM の書き込み [sn_sbom_dm.app_write]、SBOM の作成 [sn_sbom_dm.app_create]、SBOM の読み取り [sbom_dm.app_read]	これらのロールは、SBOM データモデルアプリケーションと一緒にインストールされます。 これらのロールにより、SBOM テーブルのレコードの読み取り、作成、および編集が許可されます。	なし
SBOM Core の取り込み [sn_sbom_core.sbom_ingest] と SBOM Core アドミン [sn_sbom_core.admin]	これらのロールは、SBOM Core アプリケーションと一緒にインストールされます。 sn_sbom_core.sbom_ingest ロールでは、手動および REST API 経由での SBOM のアップロードが許可されます。sn_sbom_core.admin ロールでは、SBOM の作成、読み取り、編集、およびアップロードが許可されます。 このロールでは、インスタンス内で SBOM Core のモジュールにもアクセスできます。SBOM データモデルアプリケーションからロールを継承します。	• sn_sbom_dm.app_write • sn_sbom_dm.app_create • sn_ sbom_dm.app_read
SBOM アナリスト [sn_sbom_resp.sbom_analyst]	このロールは、SBOM Response アプリケーションと一緒にインストールされます。 sn_sbom_core.admin ロールを継承し、SBOM ワークスペースにアクセスできるようにします。	• sn_sbom_core.admin • sn_sbom_dm.app_write • sn_sbom_dm.app_create • sn_ sbom_dm.app_read • sn_sbom_resp.manage_avi_rule • sn_sbom_config_rule テーブル

SBOM アプリケーションとともにインストールされるテーブル

次のテーブルにリストされているテーブルは、SBOM アプリケーションのデータモデルと一緒にインストールされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SBOM データモデルのテーブル

テーブル	説明
SBOM ドキュメント [sn_sbom_doc]	アップロードした BOM エンティティが含まれます。
SBOM コンポーネント [sn_sbom_component]	インポートされた SBOM コンポーネント、分類子、および親コンポーネントに含まれるバージョンが含まれます。
SBOM コンポーネントの関係 [sn_sbom_comp_relationship]	コンポーネントとその依存関係が含まれます。
SBOM m2m bom コンポーネント [sn_sbom_m2m_bom_comp]	BOM コンポーネントマッピングが含まれます。
SBOM ライセンス [sn_sbom_license]	コンポーネントに使用されるオープンソースのライセンス ID が含まれます。
SBOM サプライヤー [sn_sbom_supplier]	コンポーネントを提供した組織 (製造元、販売業者、再梱包業者など) が含まれます。
SBOM コンポーネント ID [sn_sbom_comp_id]	コンポーネント識別子が含まれます。
SBOM コンポーネントのプロパティ [sn_sbom_comp_property]	コンポーネントの名前と値のプロパティが含まれます。
SBOM ハッシュ [sn_sbom_hash]	コンポーネントのハッシュアルゴリズムが含まれます。
SBOM 連絡先 [sn_sbom_contact]	サプライヤーの連絡先情報が含まれます。
SBOM 外部参照 [sn_sbom_comp_external_ref]	関連する可能性があるが SBOM に含まれていないシステム、サイト、および情報を文書化したコンポーネント、コンポーネントタイプ、および外部 URL が含まれます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SBOM データモデルのテーブル (続く)

テーブル	説明
SBOM パッケージグループ [sn_sbom_pkg_group]	すべてのコンポーネントのパッケージグループ情報が含まれます。複数のバージョンのライブラリをアプリケーション間で使用できます。同じデータが複数回プルされることを避けるために、同じコンポーネントのバージョンがグループ化されてこのテーブルに追加されます。

次のテーブルにリストされているテーブルは、SBOM Response アプリケーションと一緒にインストールされます。

SBOM Response テーブル

テーブル	説明
SBOM 作成ルール構成 [sn_sbom_config_rule]	SBOM ワークスペースで使用される AVIT 作成ルールが含まれます。
SBOM m2m コンポーネントの脆弱性 [sn_sbom_m2m_comp_vuln]	コンポーネントと関連する脆弱性が含まれます。
コンポーネント脆弱性修正情報 [sn_sbom_comp_vuln_fix_info]	コンポーネントのバージョンに関連付けられた各サードパーティ脆弱性の修正バージョンが含まれています。
コンポーネントレポートインサイト [sn_sbom_comp_report_insight]	コンポーネントの古いデータ、破棄されたデータ、および修正可能性データに関するインサイトが含まれます。
Deps 統合インポート [sn_sbom_deps_integration_import]	特定のパッケージまたはライブラリのインポートされたバージョンリスト情報が含まれます。
OSV 統合インポート [sn_sbom_osv_integration_import]	パッケージまたはライブラリの特定のバージョンの脆弱性インテリジェンス情報が含まれています。
コンポーネントバージョンリスト [sn_sbom_st_version_list]	コンポーネントのバージョン情報と公開日が含まれます。

スケジュール済みジョブ

ジョブ	説明
コンポーネントの修正可能性と脆弱性の計算	脆弱性があるコンポーネントを修正する方法と、コンポーネントを修正できる可能性に関する情報を計算します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ジョブ	説明
OSV 統合の新しいコンポーネント	前回の統合実行後にインポートされたパッケージ (ライブラリ) に関連付けられた、すべての公開されている脆弱性を取得します。
包括的 OSV 統合	インポートされたすべてのパッケージに関連付けられた、公開されているすべての脆弱性を取得します。
Deps.dev 統合	パッケージの公開されているすべてのバージョンを取得し、 [古い] ステータスと [破棄] ステータスのコンポーネントを識別するために使用されます。
BOM コンポーネントの vuln_based_criticality の更新	脆弱性があるコンポーネントの重要度を更新します。

ソフトウェア部品表ワークスペースでアプリケーション脆弱性一致アイテムルールを作成する

ソフトウェア部品表 (SBOM) ワークスペースの AVI 作成ルールモジュールでアプリケーション脆弱性一致アイテム (AVIT) が自動的に作成される条件を設定します。

始める前に

アプリケーション脆弱性一致アイテムを作成する場合は、SBOM Response アプリケーションが必要です。詳細については、「ソフトウェア部品表 の詳細」を参照してください。

必要なロール：sn_sbom_resp.manage_avi_rule

手順

1. 次のように移動する。 **SBOM** ワークスペース > **AVI** 作成ルール.
2. **[New** (新規)] を選択します。
3. フィールドに入力します。

フィールド	説明
名前	ルールの名前。
有効	作成ルールがアクティブになっているかどうかを示します。
実行順序	このルールが評価される順番。最も低い数値のルールが最初に実行されます。 たとえば、特別な処理が必要なアイテムや、リスクが重大なアイテムに対して優先度の高いルールを作成して、それらが最初に実行されるようにすることができます。次に、特別な処理を必要としないアイテムの一般的なルールを作成します。最後に、脆弱性があるコンポーネントを検出するためのデフォルトルールを作成します。
説明	他のルールと区別するのに役立つルールの説明。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
条件	アプリケーション脆弱性一致アイテム (AVI) が作成される条件を作成します。 たとえば、[脆弱性 > 重大度][次の値に等しい]**[1 - 重大]** を選択して、高リスクでユーザーに重大な影響を与える可能性のある脆弱性があるコンポーネントの AVIT を作成できます。 さらに条件を追加できることに注意してください。

4. [保存] を選択します。
   作成ルールは次回のアップロード後に自動的に実行され、条件に一致するコンポーネントの AVI を作成します。[今すぐ実行] を選択して、AVI 作成ルールモジュールからルールをオンデマンドで実行することもできます。

タスクの結果
作成された後、AVI レコードの [ソース] フィールドと [スキャンタイプ] フィールドの値を確認することで、SBOM データ専用の AVIT が作成されたことを確認できます。

フィールド	値
ソース	SBOM
スキャンタイプ	SBOM-SCA

自動翻訳

エンタープライズセキュリティケース管理のアプリケーション

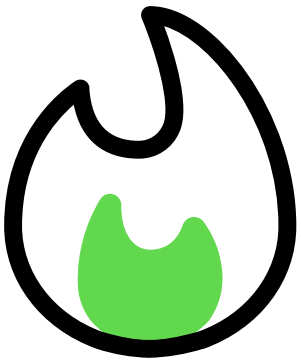
エンタープライズセキュリティケース管理のアプリケーションには、企業のセキュリティオペレーションを最適化およびオーケストレーションしながら、進化する脅威に迅速に対応できるセキュリティオーケストレーションと自動化対応 (SOAR) ソリューションであるセキュリティインシデントレスポンスが含まれます。これにより、システム、チーム、および責任間での手動の引き継ぎに内在するエラーや摩擦が解消されます。

開始するには

次のセキュリティインシデントレスポンスアプリケーションは、ServiceNow® Store の別のサブスクリプションで利用できます。アプリを検索してエンタイトルメントを取得し、インスタンスにダウンロードする方法の詳細については、「セキュリティオペレーション および ServiceNow Store」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Security Incident Response (セキュリティインシデントレスポンス)



Security Incident Response アプリケーションの詳細

重大セキュリティインシデント管理

重大セキュリティインシデント管理アプリケーションの詳細

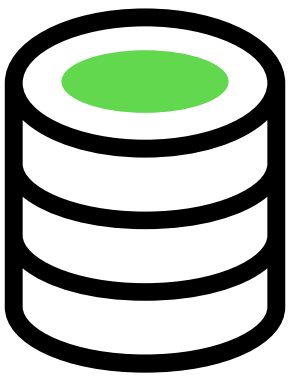
脅威インテリジェンス

脅威インテリジェンスアプリケーションの詳細

脅威インテリジェンスセキュリティセンター

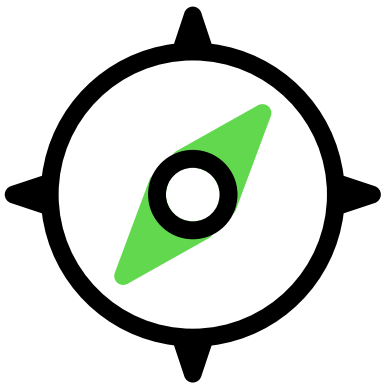
脅威インテリジェンスセキュリティセンターアプリケーションの詳細

Data Loss Prevention Incident Response



Data Loss Prevention アプリケーションの詳細

セキュリティインシデントレスポンスアプリケーションの共有機能



セキュリティインシデントレスポンスアプリケーション間で共有される機能について説明します

自動翻訳

トラブルシューティングとサポート

- セキュリティオペレーションリソースライブラリ
- セキュリティオペレーションコミュニティ
- 既知のエラーポータルで既知のエラー記事を検索する
- 連絡先 カスタマーサービス & サポート

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

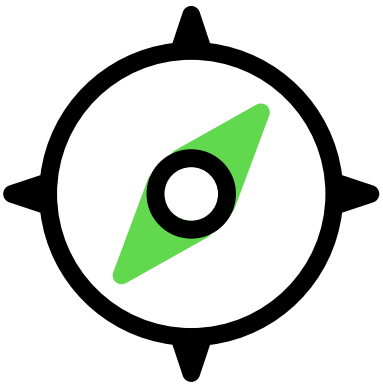
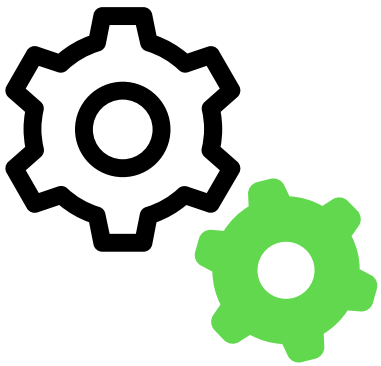
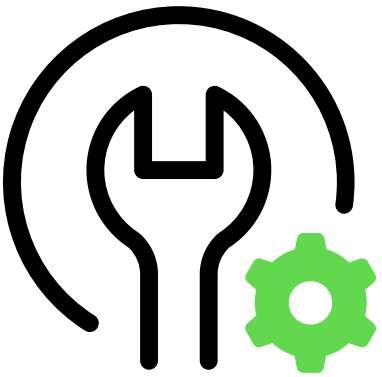
セキュリティインシデントレスポンス

ServiceNow® セキュリティインシデントレスポンス アプリケーションは、検出と初期分析から、封じ込め、根絶、復旧、および最終的なインシデントの事後レビュー、ナレッジベース記事の作成、およびクローズに至るまで、セキュリティインシデントの進捗状況を追跡します。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

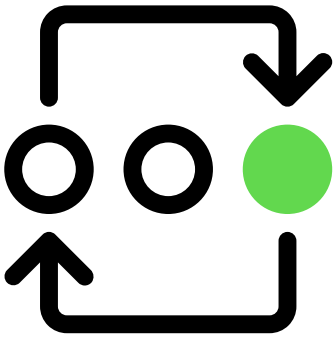
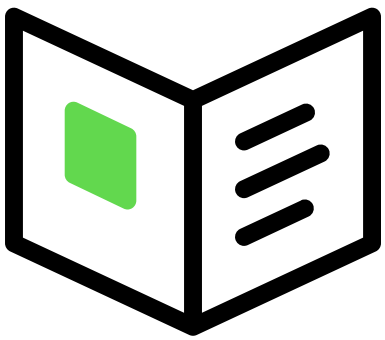
セキュリティインシデントレスポンス

探索	セットアップと構成	管理
		
セキュリティインシデントレスポンスの機能について学ぶ	セキュリティインシデントレスポンスアプリケーションをインストールして設定する	セキュリティインシデントの管理とカスタマイズ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンス (続く)

統合	セキュリティインシデントレスポンスワークスペースの使用	アナリティクスとレポート
		
他のアプリケーションと統合することでセキュリティインシデントレスポンスを拡張します。	セキュリティインシデントレスポンスワークスペースと IT 修復ワークスペースの使用方法を学習する	修復の進捗状況を監視
		
	セキュリティインシデントレスポンスに関する追加情報を取得	

ストアで セキュリティオペレーション アプリを要求する

Londonパッチ 6 以降を使用している新規の セキュリティオペレーション のお客様の場合は、ServiceNow Store Web サイトでは、利用可能なすべてのアプリを表示し、ストアに要求を送信する方法を確認できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

トラブルシューティングとサポート

- セキュリティオペレーションリソースライブラリ
- セキュリティオペレーションコミュニティ
- 既知のエラーポータルで既知のエラー記事を検索する
- 連絡先 カスタマーサービス & サポート

セキュリティインシデントレスポンス の概要

セキュリティインシデントレスポンス (SIR) を使用すると、初期分析から封じ込め、除去、復旧までのセキュリティインシデントのライフサイクルを管理できます。セキュリティインシデントレスポンスを使用すると、アナリストが実行するインシデント応答手順を包括的に把握し、分析主導型のダッシュボードとレポートでそれらの手順の傾向とボトルネックを理解できます。

アプリケーションの使用を開始する方法を示すセキュリティインシデントレスポンスの概要。

セキュリティインシデントレスポンス を使用して攻撃を阻止し、セキュリティインシデントレスポンス エクスプローラーでセキュリティアクティビティを確認する SIR プロセスについては、この 9 分間のビデオをご覧ください。

サードパーティのサイバーセキュリティソリューションとのビルトイン統合と、ServiceNow Store にあるパートナーが開発した統合により、セキュリティの自動化とオーケストレーションが可能になり、効率的で正確なインシデント応答を実現できます。

調査を保護し、セキュリティインシデントを非公開にするために、セキュリティインシデントレスポンス は、システムへのアクセスを特定のセキュリティ関連のロールと ACL に制限する手段を提供します。明示的に許可しない限り、セキュリティアドミニストレーター以外のユーザーによるアクセスを制限できます。

注:
IT システムアドミニストレーター [admin] は、ServiceNow ユーザーの代理操作を行うことができます。ただし、セキュリティインシデントレスポンスのアプリケーションアドミニストレーターロールを持つユーザーの代理操作を行う場合、アドミニストレーターは、そのロールによって付与された機能 (セキュリティインシデントやプロファイル情報など) にはアクセスできません。ナビゲーションバーのモジュールとアプリケーションへのアクセスも制限されます。さらに、セキュリティインシデントレスポンスのアプリケーションアドミニストレーターロールを持つユーザーのパスワードをアドミニストレーターが変更することもできません。

セキュリティインシデントレスポンスの情報フロー

セキュリティインシデントレスポンスでは、次に示す統合から調査、解決とレビューまでの情報フローを使用します。

注:
これはインタラクティブインフォグラフィックです。画像内のアイコンやステップをクリックすると、該当のプロセスやタスクについて詳しく知ることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. SIR 統合について、詳細はこの画像をクリック
2. セキュリティインシデントの作成について、詳細はこの画像をクリック
3. 脅威インテリジェンスについて、詳細はこの画像をクリック
4. SIR ワークスペースについて、詳細はこの画像をクリック
5. MITRE 攻撃機能について、詳細はこの画像をクリック
6. インシデント後のレビューアクティビティについて、詳細はこの画像をクリック

ディスカバリー

セキュリティインシデントは、次の方法で記録または作成されます。

- セキュリティインシデントフォームから
- 内部で生成されたイベント、またはアラートルールを介した外部モニタリングまたは脆弱性トラッキングシステムによって作成されたイベントから、または手動
- 外部モニタリングまたはトラッキングシステムから
- サービスカタログから

分析

セキュリティインシデントフォームには、選択したビュー (デフォルト、非 IT セキュリティ、セキュリティ ITIL など) に応じて、影響を受ける CI および影響を受ける CI グループの脆弱性、インシデント、変更、問題、タスクの任意の組み合わせを表示できます。このシステムは、米国国立標準技術研究所 (NIST) のデータベースまたはその他のサードパーティ製の検出ソフトウェアを相互参照することで、マルウェア、ウイルス、およびその他の脆弱性領域を特定できます。セキュリティインシデントが解決されたら、後で参照できるように、任意のインシデントを使用してセキュリティナレッジベース記事を作成できます。

ビジネスサービスマップを使用して詳細な分析を実行し、感染している可能性のある他の影響を受けるシステムまたはビジネスサービスを特定します。

封じ込め、除去、復旧

脆弱性を監視して分析するときに、タスクを作成して他の部門に割り当てることができます。ビジネスサービスマップを使用して、影響を受けるすべてのシステム、ドキュメント、アクティビ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ティ、SMS メッセージ、ブリッジコールなどに対して、タスク、問題、または変更を作成できます。

レビュー

インシデントが解決された後、クローズする前に他のステップを実行できます。インシデントの事後レビューを実行できます。ナレッジベース記事を作成すると、将来の類似のインシデントに役立ちます。重大なインシデントの場合は、インシデント後の解決策のレビューが必要になる場合があります。このレビューは、いくつかの形式で行うことができます。例：

- 会議を実施してインシデントについて話し合い、応答を収集します。
- インシデントのカテゴリまたは優先度ごとに設計された解決策レビューの質問のリストを作成して、インシデントを処理したチームに配布します。
- インシデントマネージャーは、自分でレポートを作成して情報を収集できます。

以下を含むインシデント解決策レビューレポートを自動的に生成できます。

1. 実行された処理の概要
2. タイムライン
3. 発生したセキュリティインシデントのタイプ
4. すべての関連するインシデント、変更、問題、タスク、CI グループ
5. 解決策の詳細

さらに、自動化されたセキュリティインシデント解決策レビューシステムが利用可能です。このシステムは、セキュリティインシデントに割り当てられたすべてのユーザーの名前を収集し、カスタマイズされたサーベイを送信して、インシデントの処理に関するデータを収集します。このデータは、生成されたセキュリティインシデントレビューレポートで確認でき、これを編集して最終ドラフトを作成できます。同様のデータをナレッジベース記事に追加して、得られた教訓と今後同様の問題を解決するためのステップを含めることができます。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

セキュリティインシデントレスポンスの用語

セキュリティインシデントレスポンス では次の用語が使用されます。

用語	定義
有効	クローズまたはキャンセルステータスでないすべてのセキュリティインシデント。
アドミンのロックダウン	セキュリティインシデントレスポンス へのアクセスをセキュリティ関連のロールと ACL を持つ担当者に制限する機能。
受信セキュリティ要求	新しい電子バッジの要求など、影響度の低いセキュリティデマンドのために送信された要求。
インシデントの事後アクティビティの管理	セキュリティインシデントの作成元と処理のレビュー。最終的な成果物は、実行されたすべてのアクションとその理由が記録されたインシデントの事後レポートです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

用語	定義
応答タスク	脅威に対するアクションを追跡するためにセキュリティインシデントに割り当てられたタスク。
セキュリティインシデント算出の理解	事前定義された条件が満たされたときにレコード値を更新するために使用される算出。
セキュリティインシデントツリーマップ	ネストされた矩形の形式でセキュリティインシデントデータを階層的に表示するチャートタイプ。
脅威のルックアップ	マルウェアについてファイル、URL、および IP アドレスをスキャンするためにセキュリティインシデントカタログから送信される要求。
脆弱性スキャン	脆弱性について影響を受けるリソース (サーバー、コンピューター、およびその他の構成アイテム) をスキャンするための、セキュリティインシデントフォームから開始される要求。

ドメインセパレーションと セキュリティインシデントレスポンス

ドメインセパレーションは セキュリティインシデントレスポンス でサポートされています。 ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル：標準

- ベーシックレベルのサポートのすべての側面が含まれています。
- アプリケーションプロパティは、必要に応じてドメイン対応です。
- ビジネスロジック：サービスプロバイダー (SP) によって顧客ごとにプロセスを作成または変更できます。ユースケースには、単一のインスタンスでの複数のサービスプロバイダー顧客によるアプリケーションの正しい使用が反映されています。
- インスタンスのオーナーは、特定のアプリケーションに期待される通りに、テナントごとに MVP ビジネスロジックとデータパラメーターを設定できる必要があります。

サンプルユースケース：アドミンは、レコードを他のテナントに対してはクローズしないが、1 つのテナントに対してクローズする場合、コメントを必須にすることができる必要があります。

サポートレベルの詳細については、「アプリケーションでのドメインセパレーションのサポート)」を参照してください。

概要

セキュリティインシデントレスポンス アプリケーションでは、サービスプロバイダー (SP) は、ドメインセパレーションによって、顧客ベース全体で SOC (Security Operations Center) および セキュリティインシデントレスポンス (SIR) 手順を標準化し、運用コストの削減とサービス品質の向上を実現できます。顧客データは、ワークフロー、ダッシュボード、レポートなどに別個の顧客ワークスペースを使用することで分離され、他のクライアントに公開されることはありません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

バージョンリリースごとのセキュリティインシデントレスポンスでのドメインセパレーションのサポート

リリース	サポートレベル	メモ
Geneva、Helsinki	サポートはありません	データレベルのドメインセパレーションの開始
Istanbul	データのみ	
Jakarta	レベル 2 (データ、要求者、履行者)	新機能：単一の統合インスタンスでのレベル 2 ドメインセパレーションによるサードパーティ統合のサポート (脅威インテリジェンス統合を含む)
Kingston	レベル 2 (データ、要求者、履行者)	新機能：SIR のサイティング検索統合は複数のインスタンスで有効になりますが、すべてのインスタンスは引き続き単一のドメインの下で動作します。例：Splunk Integration の 2 つのインスタンス (SplunkCLOUD および SplunkCORP) が構成されている場合は、実装が最初に構成された単一のドメインでのインシデント応答アクティビティにその両方が引き続き利用されます。
London	レベル 2 (データ、要求者、履行者)	新機能：すべての統合を複数のドメインに配置できます。
Madrid	レベル 2 (データ、要求者、履行者)	すべての統合を複数のドメインに配置できるようになりました。上記の例では、SplunkCloud を domain1 に配置し、SplunkCORP を domain2 に配置できます。
New York	レベル 2 (データ、要求者、履行者)	すべての統合を複数のドメインに配置できます。
Orland	標準	すべての統合を複数のドメインに配置できます。
Paris	標準	すべての統合を複数のドメインに配置できます。

セキュリティインシデントレスポンス アプリケーションのドメインセパレーションは、次の製品機能をカバーしています。

- セキュリティアラートは、インシデントがその ID/認証情報/スコープで生成され、セキュリティインシデントとして登録されているユーザーの適切なドメインに送信されます。
- アラートは、ステートフルなプロパティまたは測定可能なイベントを表す「観測事象」を生成します。セキュリティインシデントのドメイン内のセキュリティワークフローを使用して、応答を調整します。
- 統合は、応答の自動化のためにセキュリティインシデントのドメイン内で構成されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 機能は、応答の自動化のためにセキュリティインシデントのドメイン内で構成されます。機能には、次のものが含まれます (Kingston リリース時点)。
  - 脅威のルックアップ
  - 観測事象を拡張
  - 構成アイテムを拡張
  - 実行中のプロセスを取得
  - ネットワーク統計情報を取得
  - ブロック要求
  - ホストを隔離
  - サイティング検索
  - メールの検索と削除
  - ウォッチリストに公開
- 応答の自動化の結果 (脅威のルックアップやサイティング検索など) は、セキュリティインシデントのドメインに保存されます。
- 他のセキュリティインシデントは、観測事象の共有セットに基づいて、セキュリティインシデントの同じドメイン内で相互参照されます。
- 他のユーザーは、セキュリティインシデントのドメイン内で相互参照されます。
- 構成アイテムは、セキュリティインシデントと同じドメイン内で相互参照されます。
- 手動応答タスクは、セキュリティインシデントのドメインに追加されます。
- ナレッジベース記事と Runbook は、セキュリティインシデントのドメイン内で参照されます。
- ドメイン内のインシデントに関連するセキュリティインシデントレスポンスメトリクスは、ダッシュボードとレポートに表示されます。

注:
上記のケースでは、NOW Platform の分離されたドメインでの可視化の包括的な原則が適用されます。通常どおり、親ドメインのインシデントは子ドメインのアーティファクトを参照できますが、その逆はできません。

セキュリティインシデントレスポンスにおけるドメインセパレーションの仕組み

セキュリティインシデントレスポンス アプリケーションは、セキュリティインシデントのライフサイクルをエンドツーエンドで管理します。次のユースケースはドメインセパレーションに対応しています。

- 顧客の SOC または MSP のアナリストが応答するセキュリティインシデントを作成するためのイベントとアラートの取り込み：
  - メールパーサー (プラットフォームベース、ユーザーから報告されたフィッシング、カスタム)
  - インシデント作成前の重複排除イベント/アラート
  - 観測事象の自動抽出
  - サードパーティ SIEM ストアにあるアプリケーション
- インシデントに関連するアーティファクトの拡張 (IP、URL、ドメイン、ファイルハッシュ)：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 資産の拡張 (CMDB)
- ユーザー (プラットフォーム)
- 自動化：観測事象の拡張 (例：WhoIs)

- アーティファクトとその評判または既知の脅威との関連付けを使用したインシデントの調査
  - 調整：プレイブックとナレッジベース記事
  - 自動化：脅威のルックアップ (例：VirusTotal)、サイティング検索 (例：Splunk)、実行中のプロセスを取得 (例：Carbon Black)
- 実行された調査に基づく、インシデントに関連する脅威関連のアーティファクトの根絶
  - 調整：プレイブックとナレッジベース記事
  - 自動化：メールの検索と削除 (例：Microsoft Exchange)、IP のブロック (例：Palo Alto ファイアウォール)
- 効率性またはインシデント応答操作の測定
  - パフォーマンスアナリティクスダッシュボード：生産性とインシデントの傾向
  - 作業メモからのインシデント調査ステップの再ビルド
  - インシデントの事後レビュー

ドメインセパレーションのセットアップ

セキュリティインシデントレスポンス のドメインセパレーションを設定するには、追加の手順は必要ありません。インスタンスがドメインセパレーションされた後、すべての セキュリティインシデントレスポンス テーブルで [ドメイン] 列が取得されます。

ドメインセパレーションデータ

データはドメインセパレーションできます。これは、次のことを意味します。

- あるドメイン内のセキュリティインシデントを他のドメインから表示することはできません。
- セキュリティインシデントから抽出された観測事象は同じドメインに配置され、他のドメインから表示することはできません。
- Kingston リリースまで、構成されたサードパーティ統合はグローバルドメインに存在し、インスタンス内の他のすべてのドメインからアクセスできます。
- Madrid リリースでは、サードパーティ統合をドメインごとに構成してアクティブ化できます。これは、あるドメインでアクティブ化および構成された統合を別のドメインで活用できないことを意味します。
- (脅威の調査、封じ込め、または根絶のために) サードパーティ統合を使用して観測事象で実行される自動化では、結果がセキュリティインシデントのドメインに配置され、別のドメインから結果を表示することはできません。
- あるドメインで作成されたオーケストレーションワークフローを別のドメインで表示することはできません。
- 呼び出される機能 (前の機能のリストに記載) は、呼び出される機能のドメイン固有の実装により、ドメイン全体で汎用的なままになります。たとえば、IP のサイティング検索で、あるドメインで Splunk 実装を呼び出し、別のドメインで QRadar 実装を呼び出すことができます。

構成

製品構成のすべての側面は、ドメインセパレーションされた環境で自己完結型です。セットアップは、個々のドメインに合わせてカスタマイズできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
ビジネスロジックと下記の #2 ～ 5 のプロセスは、テナントドメイン内で管理できます。

次のタスクを構成する必要があります。

1. システム管理
   - ユーザーおよびユーザーのグループへのロールの割り当て：セキュリティインシデントレスポンスとともにインストールされるユーザーロール)
   - セキュリティインシデントレスポンス と統合する 1 つ以上のサードパーティ統合プラグインのインストール：セキュリティインシデントレスポンス の統合
2. セキュリティインシデントレスポンス 管理
   - ロールの追加またはレビュー：セキュリティインシデントレスポンス とともにインストールされるコンポーネント
   - グループとユーザーの設定：セキュリティインシデントグループの作成
   - インシデントエスカレーションの設定：セキュリティインシデントのエスカレーション
   - セキュリティインシデントリスクスコア算出の設定：セキュリティインシデント算出の理解
   - サービスレベルアグリーメントの設定：セキュリティインシデントレスポンス SLA の作成
   - セキュリティインシデントプロセス定義の設定：セキュリティインシデントレスポンスプロセス定義の概要
   - インシデント後のレビュープロセスの設定：インシデントの事後アクティビティの管理
3. セキュリティインシデントメールの設定
   - メール解析機能付き受信箱の設定：セキュリティオペレーション メール解析
   - アラート取り込み用メールパーサーの設定：Security Operations でのメールパーサーの作成
   - ユーザーから報告されたフィッシングに対するメール一致ルールの設定：ユーザーから報告されたフィッシング攻撃を検証するためのルールの作成
   - 受信メールアクションの設定：受信メールアクション
4. セキュリティインシデントプレイブックの設定
   - Runbook ドキュメントのレビューおよび設定：セキュリティインシデントレスポンス Runbook の作成
   - セキュリティインシデントワークフローの設定：セキュリティオペレーション の共通機能
5. 機能の設定
   - ブロック要求：Security Operations Integration - ブロック要求機能
   - メールの検索と削除：Security Operations Integration - [メールの検索と削除] 機能
   - 構成アイテムを拡張：Security Operations Integration - [CI を拡張] 機能
   - 観測事象を拡張：Security Operations Integration - [観測事象を拡張] 機能
   - ネットワーク統計情報を取得：Security Operations Integration - [ネットワーク統計情報を取得] 機能
   - 実行中のプロセスを取得：Security Operations Integration - [実行中のプロセスを取得] 機能
   - ホスト隔離：Security Operations Integration - [ホストを隔離] 機能
   - ウォッチリストに公開：Security Operations Integration - [ウォッチリストに公開] 機能
   - サイティング検索：Security Operations Integration - [サイティング検索] 機能
   - 脅威のルックアップ：[Security Operations Integration - 脅威のルックアップ] 機能

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テナントドメインが独自のアプリケーションデータを管理する方法

- テナントドメインオーナーは、セキュリティインシデントを取り込むための独自のメール解析ルールを作成します。
- テナントドメインオーナーは、ドメイン内で使用するために特定の統合を構成できます。
- テナントドメインオーナーは、独自のインシデント応答ワークフローを作成できます。
- テナントドメインオーナーは、独自のインシデントカテゴリ、インシデント応答のナレッジベース記事、および Runbook を作成して、インシデント応答ワークフローに関連付けることができます。
- テナントドメインユーザーは、独自のセキュリティインシデントを作成し、クローズします。

インスタンスオーナーがドメインセパレーションできるビジネスロジックとプロセス

- セキュリティインシデントレスポンス ユーザーとグループ
- セキュリティインシデントレスポンス 統合 (Madrid リリースから)
- インシデント作成のためのメール解析ルール
- 複数のイベントまたはアラートをセキュリティインシデントに統合するビジネスルール
- インシデント応答オーケストレーションのワークフロー
- セキュリティインシデントリスクスコア算出
- セキュリティインシデントのエスカレーションパス
- セキュリティインシデント SLA
- セキュリティインシデントプロセス定義
- セキュリティインシデントのインシデント後のレビュープロセス

関連情報

サービスプロバイダーのドメインセパレーション

セキュリティインシデントレスポンス のセットアップ

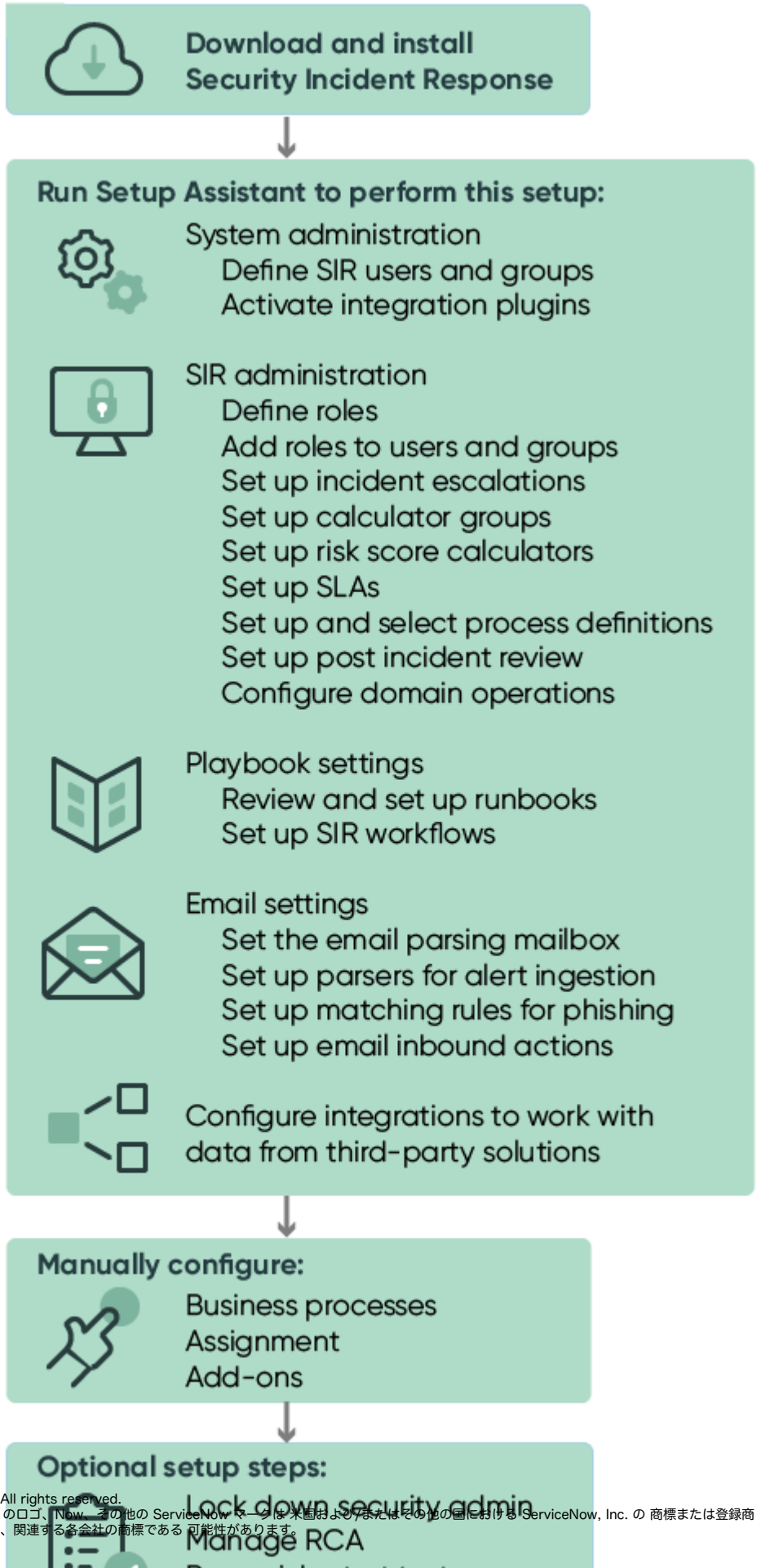
セキュリティインシデントレスポンス のセットアップには、特定の要件に応じて、いくつかの必須のステップといくつかのオプションのステップが含まれます。セキュリティインシデントレスポンスから ServiceNow Store をダウンロードしてインストールすると、セットアップアシスタントを実行して、セキュリティインシデントレスポンス とサードパーティの統合の基本構成を行うことができます。

セキュリティインシデントレスポンス のセットアッププロセス

次の図は、セットアッププロセスを示しています。セットアッププロセスは、セキュリティインシデントレスポンスアプリケーションのダウンロードと構成の 2 つのサブプロセスに分かれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは、米国および/または他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

最初のセットアップステップでは、 をダウンロードする セキュリティインシデントレスポンス アプリケーションから ServiceNow Store. ダウンロードが完了すると、セットアップアシスタントを含むいくつかの依存アプリケーションがロードされ、セキュリティインシデントレスポンス を構成するために使用できるようになります。

セットアップアシスタント

セキュリティインシデントレスポンス セットアップアシスタントは、ベース セキュリティインシデントレスポンス インスタンスのセットアップをステップバイステップでガイドする、ウィザードに似たアプリケーションです。

セットアップステップはとても分かりやすいものですが、追加の説明が必要な場合は、セットアップアシスタントのリファレンスで追加の説明を見つけることができます。セットアップアシスタントを使用してセットアップを完了した後、必要に応じて他のオプションのセットアップ手順を実行できます。これらの手順には、以下に関するオプションが含まれています。

- 要求ライフサイクルの設定
- カタログと要求の作成
- 通知の構成
- 手動アサインと自動アサインの設定
- ナレッジベース、ドキュメント管理、およびタスクアクティビティの有効化

改善された新しいセキュリティインシデントレスポンスワークスペースを利用できます。詳細については、「セキュリティインシデントレスポンスワークスペース」を参照してください。

セキュリティインシデントレスポンス のインストールと構成

インスタンスで セキュリティインシデントレスポンス を実行する前に、ServiceNow Store からダウンロードして、構成ステップを完了する必要があります。

始める前に

必要なロール：admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重要:

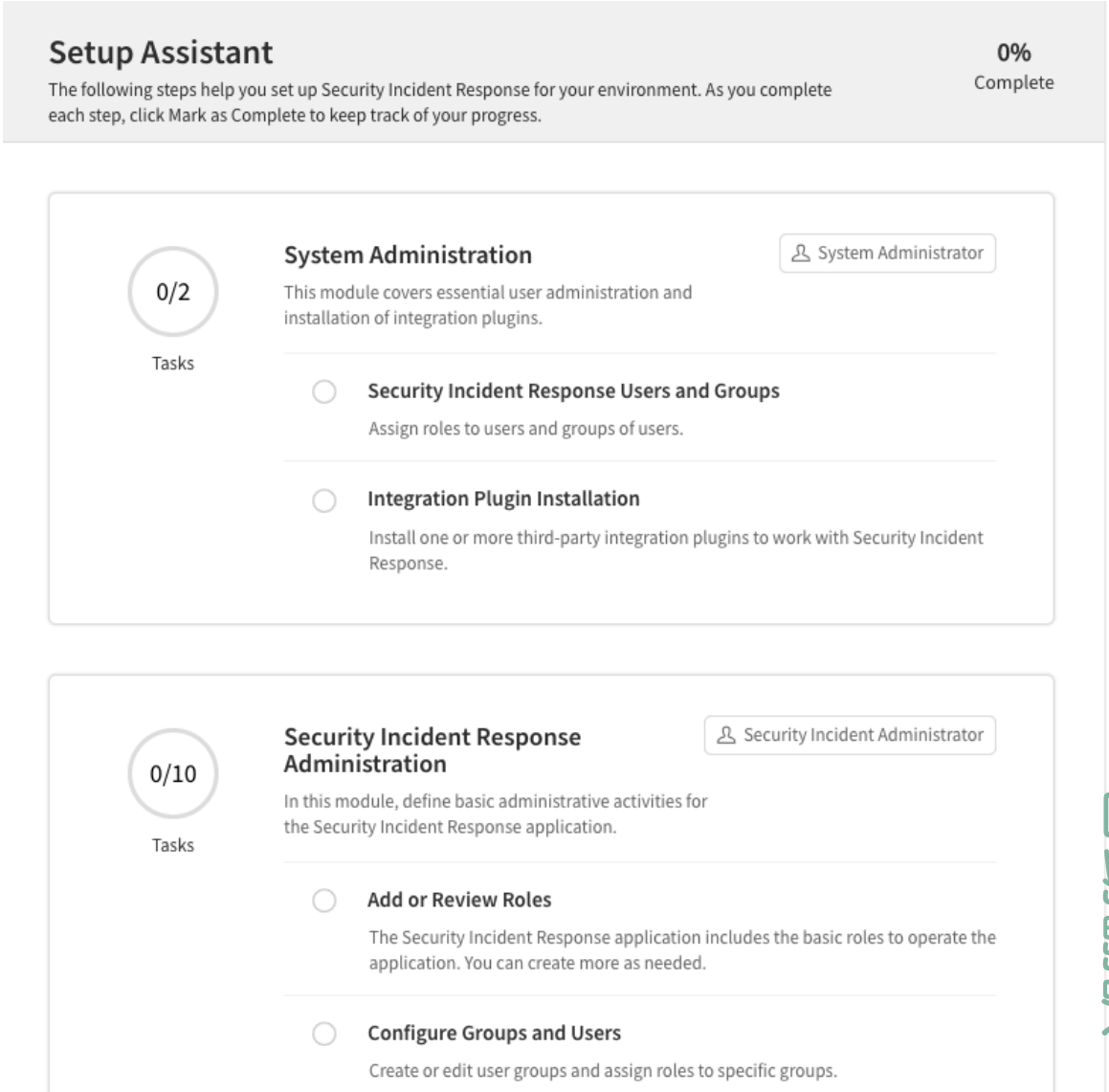
- ServiceNow Store から セキュリティインシデントレスポンス の 13.4.5 バージョン以降をインストールすると、デフォルトで セキュリティインシデントレスポンスワークスペース (sn_si_aw) 1.5.1 バージョン以降が自動的にインストールされます。依存アプリケーションの詳細については、「SIR ワークスペース プラグインおよびロール」セクションを参照してください。
- セキュリティインシデントレスポンスワークスペースバージョン 1.5.1 以降は、セキュリティインシデントレスポンスのインストール/アップグレードによってのみインストール/アップグレードでき、個別にインストールすることはできません。
- セキュリティインシデントレスポンスの最新機能は、セキュリティインシデントレスポンスワークスペースでのみ利用できます。シフト引き継ぎ、リスクスコア算出などの機能にアクセスして活用するには、最新の セキュリティインシデントレスポンス または セキュリティインシデントレスポンスワークスペース バージョンをインストールまたはアップグレードしてください。

手順

1. の指示に従ってください からのアプリケーションのダウンロード ServiceNow Store.
2. セキュリティインシデントレスポンスアプリケーションとそのすべての依存アプリケーションをダウンロードしたら、 セキュリティインシデント > アナリストワークスペースのセットアップ > セットアップアシスタント.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

3. フォームの指示に従って、セキュリティインシデントレスポンス ベースシステムを構成します。より複雑なセットアップタスクの詳細については、必要に応じて「セットアップアシスタントの参考情報」を参照してください。

セキュリティアナリストワークスペースのダウンロードとインストール

インスタンスで セキュリティインシデントレスポンス 新規 UI を実行する前に、ServiceNow® Store からダウンロードしてインストールする必要があります。

始める前に

スムーズにインストールできるように、インスタンスに必要な ServiceNow ロールがあることを確認します。インストール、構成、および予想される結果の検証には、次のロールが必要です。

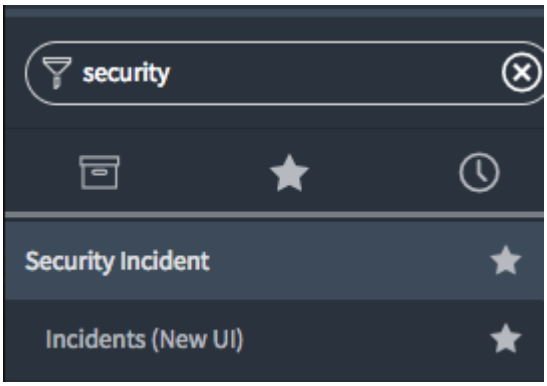
- まだアサインされていない場合、システムアドミニストレーター [admin] は、アプリケーションをインストールし、セキュリティインシデントレスポンスアドミン [sn_si.admin] ロールをアサインします。
- セキュリティインシデントレスポンスアドミン [sn_si.admin] は構成を監視し、期待される結果を検証します。

必要なロール：admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. の指示に従ってください からのアプリケーションのダウンロード ServiceNow Store をクリックし、 セキュリティインシデントレスポンス **UI** アプリケーションをインストールします。
2. インストールが完了したら、次の場所に移動して [セキュリティアナリストワークスペース] を開くことができます セキュリティインシデント > インシデント (新規 **UI)**



セキュリティインシデントレスポンス とともにインストールされるコンポーネント

セキュリティインシデントレスポンス アプリケーションをダウンロードしてアクティブ化すると、ユーザーロール、テーブル、プロパティ、スケジュール済みジョブなど、いくつかのタイプのコンポーネントがインストールされます。

注:
アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「アプリケーションとともにインストールされているコンポーネントの検索」を参照してください。

この機能ではデモデータを利用できます。

インストールされるプロパティ

システムアドミニストレーター [admin] ロールを持つユーザーは、プロパティを表示できます。セキュリティアドミニストレーター [sn_si.admin] ロールを持つユーザーは、それらを変更できます。

プロパティ	使用法
ワークスペース内の [関係グラフ] タブに表示されるデフォルトのカテゴリノード。デフォルト値は、関連レコードに対応するテーブル名を表します。 sn_si_aw.defaultCategories	• タイプ：文字列 • デフォルト値:sn_ti_m2m_task_observables、sn_si_m2m_task_affected_us
スケジュールが設定されていない場合のすべてのエージェントに対するデフォルト開始時間 (形式：08:00) sn_si.default.start.time	• タイプ：文字列 • デフォルト値：08:00 • [**Location** (場所)]： セキュリティインシデント > アドミニストレーティ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	使用法
スケジュールが設定されていない場合のすべてのエージェントに対するデフォルト終了時間 (形式：17:00) sn_si.default.end.time	• タイプ：文字列 • デフォルト値：17:00 • [**Location** (場所)]： セキュリティインシデント > アドミニストレーティ
セキュリティインシデントのユーザーおよび CI 関係性に他のコンテキストタイプの観察事項とともに宛先タイプ観察事項を含めます sn_si.link_dest_ip	コンテキストタイプが [宛先] のセキュリティインシデント観測事象または [影響を受けるユーザー] タブに表示するかどうかを決定します。は、宛先コンテキストタイプの観測事象は除外されます。観測事象をい] を選択します。
セキュリティインシデントから問題または変更要求を作成するときにカスタマイズを許可します sn_si.popup	このプロパティは、問題または変更を作成するときに要求を変更するプウィンドウを開きます。 これらのプロパティを **false** に設定した場合、問題または変更要求にティインシデントと同じ優先度、簡単な説明、および説明が表示されフィールドを追加または編集するオプションは表示されません。 • タイプ：true | false • デフォルト値：true • [**Location** (場所)]： セキュリティインシデント > アドミニストレーティ
サイティング検索の結果を CMDB 内の CI に関連付けます。 sn_si.associate_ci_with_sighting_search	true に設定した場合、CMDB にある関連する構成アイテムがサイテに含まれます。 • タイプ：true | false • デフォルト値：true • [**Location** (場所)]： セキュリティインシデント > アドミニストレーティ
範囲のリスクスコアは緑色でハイライト表示され、0 ～ 49 の形式で示されます sn_si.risk.score.green	[セキュリティインシデント] リストで、リスクスコアが 0 ～ 49 のセシデントは緑色の点でマークされます。
範囲のリスクスコアはオレンジでハイライト表示され、50 ～ 79 の形式で示されます sn_si.risk.score.orange	[セキュリティインシデント] リストで、リスクスコアが 50 ～ 79 のシデントはオレンジ色の点でマークされます。
範囲内のリスクスコアは赤でハイライト表示され、80 ～ 100 の形式で示されます sn_si.risk.score.red	[セキュリティインシデント] リストで、リスクスコアが 80 ～ 100 のンシデントは赤色の点でマークされます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	使用法
このパラメーターは、この機能を実装したサイティング検索構成を有効または無効にします。 sn_si.enable_sighting_search	true に設定した場合、アクティブ化された統合でサイティング検索を • タイプ：true | false • デフォルト値：true • [**Location** (場所)]： セキュリティインシデント > アドミニストレーティ
サイティング検索が実行されたときに保存される生データの行数。0 ～ 100 の範囲 sn_si.sighting_search_raw_data_rows	このプロパティのデフォルトは 50 行の生データです。結果行の半分から報告され、半分は検索期間の終わりから報告されます。したがっした場合、検索期間の開始から 25 行、検索期間の終わりから 25 行
応答タスクが「対応中」に進むと、インシデント状況が「含む」に自動的に進みます sn_si.rollup_task_state	フローまたはワークフローを使用する場合は、このプロパティを **fals**を検討してください。これにより、フローまたはワークフロー内から制御できます。また、あるインシデント状況から別のステータスに的な競合を回避するのにも役立ちます。 • タイプ：true | false • デフォルト値：true • [**Location** (場所)]： セキュリティインシデント > アドミニストレーティ
セキュリティインシデントレスポンスのアサインプロパティ	
場所の重み sn_si.location.weight	セキュリティアナリストの自動アサインに使用する基準を計算すると価。たとえば、タスクに対して場所が考慮される場合、場所の重み付ティアナリストの評価に追加されます。 • タイプ：整数 • デフォルト値：10 • [**Location** (場所)]： セキュリティインシデント > アドミニストレーティ
スキルの重み sn_si.skills.weight	セキュリティアナリストの自動アサインに使用する基準を計算すると価。たとえば、タスクに対してスキルが考慮される場合、スキルの重リティアナリストの評価に追加されます。 • タイプ：整数 • デフォルト値：10 • [**Location** (場所)]： セキュリティインシデント > アドミニストレーティ
自動アサインによって一度に処理される最大セキュリティアナリスト数を設定 sn_si.max.agents.processed	システムに設定されているセキュリティアナリスト数の絶対上限は 3を超える値を指定すると、値はそのレベルに設定されます。システムる値よりも多くのセキュリティアナリストが含まれているディスパッてタスクを自動ディスパッチすることはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	使用法
	• タイプ：整数 • デフォルト値：100 • [**Location** (場所)]： セキュリティインシデント > アドミニストレーティ
タイムゾーンの重み sn_si.timezone.weight	セキュリティアナリストの自動アサインに使用する基準を計算すると価。たとえば、タスクに対してセキュリティアナリストのタイムゾー合、タイムゾーンの重み付け値がセキュリティアナリストの評価に追 • タイプ：整数 • デフォルト値：10 • [**Location** (場所)]： セキュリティインシデント > アドミニストレーティ
タスクの最後から次の移動開始までの時間(分)。 sn_si.work.spacing	有効な時間値の例は 10 です。 • タイプ：整数 • デフォルト値：0 • [**Location** (場所)]： セキュリティインシデント > アドミニストレーティ
コンテンツを HTML として表示する `code` タグを含む、指定されたジャーナルフィールド。 sn_si.journal_field.html_enabled	• タイプ：文字列 • デフォルト値：work_notes, comments • [**Location** (場所)]： セキュリティインシデント > アドミニストレーティ
影響を受けるサービスをバックグラウンドで計算します。 sn_si.refresh_impacted.event	[影響を受けるサービス/影響を受けた CI] 関連リストは、イベントをす。有効にすると、リフレッシュがバックグラウンドで実行され、セインシデントに追加されます。 操作をバックグラウンドで実行するには、値を **[true]** に設定します。 • タイプ：true | false • デフォルト値：false • [**Location** (場所)]： セキュリティインシデント > アドミニストレーティ
事前計算済みデータから重要なサービスを取得します。 sn_si.critical_service.calculator.use_cache	構成アイテムの事前計算済みデータを、重要なサービス算出で使用です。 事前計算済みデータからルックアップするには、値を **[true]** に設定し

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	使用法
	• タイプ：true | false • デフォルト値：false • [**Location** (場所)]： セキュリティインシデント > アドミニストレーティ

インストールされているロール

ロール タイトル [名前]	説明	含んでいるロール
セキュリティインシデントアドミン [sn_si.admin]	すべての セキュリティインシデントレスポンス データを完全に制御します。また、必要に応じてテリトリとスキルを管理します。 **注:** ベースシステムでは、アドミニストレーターは sn_si.admin にもアクセスできます。セキュリティインシデントレスポンス は、少なくとも 1 人の他のユーザーにセキュリティアドミンロールがアサインされている限り、アドミニストレーターによるアクセスを制限できます。	• assessment_admin • catalog_admin • decision_table_admin • decision_table_reader • filter_admin • flow_designer • pd_author • pd_content_author • pd_operator • skill_admin • skill_model_admin • sn_si.analyst • sn_si.knowledge_admin • sn_si.manager • sn_sec_cmn.admin • sn_si.restriction_access_manager • sn_si.special_access_read_manager • sn_si.special_access_write_manager • sn_ti.malicious_attachment_access • sn_ti.observable.admin • tags_admin • template_admin • territory_admin • treemap_admin • user_admin
セキュリティインシデントアナリスト	セキュリティインシデントを管理します。基本的なセキュリティア	• pd_operator • snc_platform_rest_api_access

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロール タイトル [名前]	説明	含んでいるロール
[sn_si.analyst]	クセスの基礎となるロール。このロールを持つユーザーは、セキュリティインシデント、要求、タスクの他、各自のインシデントに関連する問題、変更、および機能停止を作成したり更新したりできます。	• sn_msi.promoter • sn_msi.proposer • sn_si.basic • sn_ti.malicious_attachment_access
セキュリティインシデントの基本 (Security Incident Basic) [sn_si.basic]	基本的なセキュリティアクセスの基礎となるロール。このロールを持つユーザーは、セキュリティインシデント、要求、タスクの他、各自のインシデントに関連する問題、変更、および機能停止を作成したり更新したりできます。	• canvas_user • document_management_user • email_composer • flow_operator • inventory_user • pa_viewer • service_fullfiller • skill_user • sn_sec_cmn.write • sn_si.read • sn_ti.observable.read • sn_ti.observable.write • sn_ti.read • task_activity_writer • task_editor • treemap_user
最高情報セキュリティ責任者 (CISO) [sn_si.ciso]	CISO ダッシュボードを表示および操作します。また、脆弱性対応 プラグインが有効になっている場合、このロールを持つユーザーは、脆弱性重要度定義ツリーマップをダッシュボードに追加できます。セキュリティインシデントレスポンス プラグインでも同じことができます。	• pa_viewer • sn_si.basic • sn_si.read
セキュリティインシデント (外部) (Security Incident External) [sn_si.external]	特定のグループに属するセキュリティインシデントを表示します。	service_fulfiller

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロール タイトル [名前]	説明	含んでいるロール
	注: 次の 2 つのルールは、スコープ指定されたアドミニストレーターまたはスコープアプリに関係なく、ServiceNow 全体に適用されます。 • グループにユーザーを追加すると、そのグループにもロールが割り当てられます。同様に、グループからユーザーを削除すると、継承されたロールも削除されます。 • すべてのロールは、優先順位の高いロールによってアサイン可能です。	
Security Incident Integration ユーザー (Security Incident Integration User) [sn_si.integration_user]	外部ツールは、新しいセキュリティインシデントレコードを提供し、セキュリティインシデントレコードを更新できます。	import_transformer
セキュリティインシデントナレッジアドミニストレーター (Security Incident Knowledge Administrator) [sn_si.knowledge_admin]	セキュリティインシデントナレッジベースの情報を管理、更新、削除します。	• knowledge_admin • sn_si.read
セキュリティインシデントマネージャー [sn_si.manager]	セキュリティアナリストと同じアクセス権。	• pd_author • pd_operator • sn_si.basic
セキュリティインシデント読み取り (Security Incident Read) [sn_si.read]	セキュリティインシデントを読み取ります。	• canvas_user • sn_sec_cmn.read • sn_templated_snip.template_snippet_reade

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロール タイトル [名前]	説明	含んでいるロール
		• sn_ti.observable.read • workspace_user
セキュリティ制限アクセスマネージャー (Security Restriction Access Manager) [sn_si.restriction_access_manager]	ユーザーまたはグループがセキュリティインシデントに「制限を適用」できるようにします。これはフィールドの変更にのみ適用されます。	該当なし
セキュリティインシデント特別アクセス (Security Incident Special Access) sn_si.special_access	Security Operations 組織外のユーザーに特定のセキュリティインシデントへのアクセス権を付与します。	該当なし
セキュリティ特別アクセスイネーブラー (Security Special Access Enabler) [sn_si.special_access_enabler]	Security Operations 組織外のユーザーに特定のセキュリティインシデントへの特別アクセスロールを付与します。	該当なし
セキュリティインシデント特別アクセス読み取りマネージャー (Security Incident Special Access Read Manager) [sn_si.special_access_read_manager]	セキュリティインシデント特別アクセス (Security Incident Special Access) [sn_si.special_access] ロールを管理します。セキュリティインシデントフォームの [読み取りアクセス] フィールドを変更するには、このロールを使用します。sn_si.admin がこのロールをアサインできます。	sn_si.special_access_enabler
セキュリティインシデント特別アクセスライターマネージャー (Security Incident Special Access Writer Manager) [sn_si.special_access_write_manager]	セキュリティインシデント特別アクセス (Security Incident Special Access) [sn_si.special_access] ロールを管理します。セキュリティインシデントフォームの [特権アクセス] フィールドを変更するには、このロールを使用します。sn_si.admin がこのロールをアサインできます。	sn_si.special_access_enabler

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インストールされたスケジュール済みジョブ

スケジュール済みジョブ	説明
セキュリティインシデント観測事象のルックアップ	ユーザー定義のスケジュールで観測事象のルックアップを実行します。

インストールされるテーブル

テーブル	説明
ニュースフィード設定 [sn_si_feed_configuration]	セキュリティインシデントのニュースフィードに表示されるコンテンツを定義するために使用される設定レコード。
インシデントの事後レビューのアサインルール [sn_si_pir_condition]	セキュリティインシデントをクローズしたときのインシデントの事後レビューサーベイの参加者の選択を自動化します。
セキュリティインシデント [sn_si_incident]	セキュリティインシデント、インシデントへの応答、このセキュリティインシデントに関連付けられたすべてのリンクされたタスク、変更、問題、およびインシデントを保存します。
セキュリティインシデント攻撃ベクトル [sn_si_attack_vector]	攻撃ベクトルのオプション。
セキュリティインシデントの監査ログ [sn_si_audit_log]	セキュリティインシデント拡張の監査ログを保存します。
セキュリティインシデント算出 [sn_si_calculator]	特定の条件が満たされたときに特定のセキュリティインシデントフィールドを設定する算出。
セキュリティインシデント算出グループ [sn_si_calculator_group]	セキュリティインシデント算出をグループ化したもの。算出グループの順序によって最初に評価されるグループが決まり、各グループで最大 1 つの算出が使用されます。
セキュリティインシデント拡張ファイアウォール [sn_si_enrichment_firewall]	ベーステーブル (sn_sec_cmn_enrichment_data_base) から拡張され、Palo Alto Networks ファイアウォールに固有のすべての拡張レコードを含みます。
セキュリティインシデント拡張マルウェアの結果 [sn_si_enrichment_malware]	ベーステーブル (sn_sec_cmn_enrichment_data_base) から拡張され、マルウェアに固有のすべての拡張レコードを含みます。
セキュリティインシデント拡張ネットワーク統計 [sn_si_enrichment_network_statistics]	ベーステーブル (sn_sec_cmn_enrichment_data_base) から拡張され、ネットワーク統計に固有のすべての拡張レコードを含みます。
セキュリティインシデント拡張の実行中のプロセス	ベーステーブル (sn_sec_cmn_enrichment_data_base) から拡

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
[sn_si_enrichment_running _processes]	張され、実行中のプロセスに固有のすべての拡張レコードを含みます。
セキュリティインシデント拡張の実行中のサービス [sn_si_enrichment_running_service]	ベーステーブル (sn_sec_cmn_enrichment_data_base) から拡張され、実行中のサービスに固有のすべての拡張レコードを含みます。
セキュリティインシデントメール検索 [sn_si_m2m_incident_email_search]	メール検索レコードをセキュリティインシデントにマッピングします。
セキュリティインシデントのインポート [sn_si_incident_import]	セキュリティインシデントのインポートテーブル。外部システムからセキュリティインシデントを作成するために使用されます。
セキュリティインシデントプロセス定義 [sn_si_process_definition]	セキュリティインシデントプロセスフローの構成を保存します。
セキュリティインシデントプロセス定義セレクタ [sn_si_process_definition_selector]	セキュリティインシデントに使用するセキュリティインシデントプロセス定義を保存します。
セキュリティインシデントに関連したカスタマーサービスケース [sn_si_m2m_incident_customerservice_case]	カスタマーサービスケースとセキュリティインシデントをマッピングします。
セキュリティインシデントに関連した拡張データ [sn_si_m2m_incident_enrichment]	セキュリティインシデントと関連する拡張データレコードをマッピングします。
セキュリティインシデントレスポンス タスク [sn_si_task]	セキュリティインシデントの処理に関連するサブタスクを管理します。これらのタスクをセキュリティ担当者または他の部門のユーザーにアサインして、部門間のコミュニケーションとタスクの追跡を管理できます。
セキュリティインシデントレスポンス タスクテンプレート [sn_si_task_template]	セキュリティインシデントレスポンス タスクを作成するために使用されます。これらのテンプレートは、特定のタイプのセキュリティインシデントに対する一連の適切なサブタスクを自動的に作成するために、カタログエントリーでよく使用されます。
セキュリティインシデント Runbook ドキュメント [sn_si_runbook_document]	セキュリティインシデントの条件またはフィルターをナレッジ記事に関連付けます。セキュリティインシデント修復の Runbook 手順を指定するために使用されます。
セキュリティインシデントテンプレート [sn_si_incident_template]	セキュリティインシデントを作成するために使用されます。これらのテンプレートは、事前ビルドされたセキュリティインシデントを作成するためにカタログエントリーでよく使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
セキュリティの要求 [sn_si_request]	セキュリティチームへのセキュリティ関連の要求。
セキュリティスキャンの要求 [sn_si_scan_request]	脅威のルックアップの要求。
重大度算出 sn_si_severity_calculator	セキュリティインシデントの重大度、影響度、リスク、および重要度の値を定義します。
タスクの影響を受けるユーザー [sn_si_m2m_task_affected_user]	セキュリティインシデントを影響を受けるユーザーに関連付ける多対多のテーブル。
ワークフロー動作結果評価テンプレート [sn_si_wf_activity_outcome_evaluator]	評価スクリプトを使用して機能をマッピングします。新しいサブフローをテンプレートワークフローに追加して、アナリストが手動で設定することなく応答タスクの結果を設定できます。

その他の追加の セキュリティインシデントレスポンス セットアップタスク

グローバルドメインのアドミニストレーターは、セキュリティインシデントレスポンス が日常業務をどのように処理するかを構成します。

始める前に

必要なロール：sn_si.admin

注:

これらのオプションは、多くのサービス管理アプリケーションにとって標準であるため、サービス管理の用語を使用します。たとえば、要求はメインタスク (つまりセキュリティインシデント) に使用され、タスクはサブタスクまたは応答タスクに使用されます。

グローバルドメインより下位のドメインのアドミンの場合、[構成] 画面を表示することはできますが、設定を変更することはできません。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > アドミニストレーション > 構成.
   アプリケーションを設定するためのオプションは、次のタブに整理されています。
   - [ビジネスプロセス] タブには、要求ライフサイクルの設定、カタログおよび要求の作成、通知の設定に関するオプションが含まれています。
   - [アサインメント] タブには、手動および自動アサインの設定に関するオプションが含まれています。
   - [アドオン] タブには、ナレッジベースの有効化、ドキュメント管理、およびタスクアクティビティに関するオプションが含まれています。
2. [ビジネスプロセス] タブのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[構成] 画面 – [ビジネスプロセス] タブ

フィールド	説明
ライフサイクル	
作業メモは、要求またはタスクをクローズしたりキャンセルしたりするときに必要です	このオプションを有効にすると、ユーザーは、作業メモを入力してからでないと、セキュリティインシデントまたは応答タスクをクローズまたはキャンセルできなくなります。
タスク作業メモを要求へコピー	このオプションを有効にすると、応答タスク作業メモがセキュリティインシデントの作業メモと同期されます。したがって、タスクに作業メモが追加されると、同じ作業メモが親セキュリティインシデントに表示されます。
カタログと要求の作成	
受信メールによって要求を作成または更新	このオプションを有効にすると、セキュリティインシデントを受信メールから作成または更新できます。
次のものを使用して、要求が作成されました：	[カタログまたは通常のフォーム] を選択すると、カタログがアクティブ化され、セキュリティインシデントテンプレートのカタログへの自動公開が有効になります。 [通常のフォームのみ] を選択すると、カタログが非アクティブ化され、セキュリティインシデントテンプレートのカタログへの自動公開が無効になります。
テンプレートによる専用のカタログアイテムの作成	このオプションを有効にすると、アプリケーションのカタログアイテムの自動公開がアクティブ化されます。
通知	
要求またはタスクの場合、選択したフィールドが変更されたときに受信者に通知を送信する (For a request or task, when the selected field changes, send notification to recipients)	セキュリティインシデントや応答タスクの選択したフィールドが変更されたときに、特定の受信者に送信される通知を設定できます。 **a.** [テーブル] から、[要求] (セキュリティインシデント) または [タスク] (応答タスク) を選択します。 **b.** [フィールド] から、通知の生成に使用するフィールドを選択します。選択したフィールドに変更が加えられると、識別された受信者に通知が送信されます。 **c.** [受信者] から受信者を 1 人または複数選択します。 **d.** [特定ユーザー] または [特定グループ] を選択すると、ユーザーまたはグループを選択するように求められます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	e. その他のフィールド、または受信者を使用してさらに通知を定義するには、次の一連の通知設定で、ここまでの手順を繰り返します。 **f.** 通知を削除するには、通知の右にある ⊖ アイコンをクリックします。

3. [アサイン] タブをクリックし、フィールドに入力します。

[構成] 画面 - [アサイン] タブ

フィールド	説明
要求に対する割り当て方法	セキュリティインシデントを割り当てる方法を選択します。 ○ 自動割り当ての使用：セキュリティインシデントが自動的に割り当てられます。 ○ ワークフローを使用：セキュリティインシデントは、選択したワークフローによって割り当てられます。 ○ 手動：セキュリティインシデントは手動で割り当てられます。
このワークフローを使用して、要求をアサインします	セキュリティインシデントをディスパッチするワークフローを選択します。このフィールドは、[要求に対する割り当て方法] リストから [ワークフローを使用] を選択した場合に表示されます。
タスクの割り当てメソッド	応答タスクを割り当てる方法を次から選択します。 ○ 自動割り当ての使用：応答タスクは自動的に割り当てられます。 ○ ワークフローを使用：応答タスクは、選択したワークフローによって割り当てられます。 ○ 手動：応答タスクは手動で割り当てられます。
タスクの割り当てにこのワークフローを使用	応答タスクを割り当てるワークフローを選択します。このフィールドは、[タスクの割り当てメソッド] リストから [ワークフローを使用] を選択した場合に表示されます。
アサイン先グループのカバー範囲に基づく要求またはタスクの割り当て	このオプションを有効にすると、セキュリティインシデントと応答タスクのアサイン先を、タスクの場所に対応できるグループに制限できます。
スケジューリング	
エージェントの自動選択にタスクのタイムゾーンを考慮 (Auto-selection of agents consider time zone for tasks)	タスクの割り当てにエージェントのタイムゾーンを考慮する場合は、このオプションを有効にします。このフィールドは、セキュリティインシデントまたは応答タスクに対して自動割り当てが選択されている場合に表示されます。
追加のファクター	
エージェントの自動選択にエージェントの場所を考慮 (Auto-selection of agents consider location of agents)	このオプションを有効にすると、タスクをアサインするときに、タスクの場所に近いエージェントが優先されます。このフィールドは、セキュリティインシデントまたは応答

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	タスクに対して自動割り当てが選択されている場合に表示されます。
タスクごとのエージェント自動選択ではそのスキルを有するエージェントのみを選択	自動割り当ての決定時にエージェントのスキルがどの程度タスクに適合している必要があるかを選択します。 ○ タスクを割り当てるエージェントに、タスクを実行するすべてのスキルを求める場合は、[すべて] を選択します。スキルが 1 つでも不足すると、そのエージェントは除外されます。 ○ タスクを実行するスキルの大部分をエージェントに求める場合は、[一部] を選択します。 ○ スキルを考慮せずエージェントを自動割り当てする場合は、[なし] を選択します。このフィールドは、セキュリティインシデントまたは応答タスクに対して自動割り当てが選択されている場合に表示されます。
自動選択で要求内のすべてのタスクに同じエージェントのアサインを試行 (Auto-selection attempt to assign the same agent to all tasks in a request)	あるセキュリティインシデントのすべての応答タスクのを同じエージェントに自動割り当てするには、このオプションを有効にします。

4. [アドオン] タブをクリックし、フィールドに入力します。

[構成] 画面 - [アドオン] タブ

フィールド	説明
ドキュメント	
専用ナレッジベースの有効化	セキュリティインシデントレスポンス のナレッジベースをアクティブにするには、このオプションを有効にします。
ドキュメント管理の有効化	ドキュメント管理に関連リストを追加するには、このオプションを有効にします。
タスクアクティビティの有効化	電話やメールメッセージなど、タスクのインタラクションと通信をログに記録するには、このオプションを有効にします。

5. [保存] をクリックします。

セキュリティアドミニストレーターのロックダウン

調査を保護し、セキュリティインシデントを非公開にするために、セキュリティインシデントレスポンス のアクセスをセキュリティ固有のロールと ACL に制限することができます。明示的に許可しない限り、セキュリティアドミニストレーター以外のユーザーによるアクセスを制限できます。

始める前に

セキュリティインシデントレスポンス アプリケーションがアクティブになると、システムアドミニストレーターユーザーにはデフォルトで sn_si.admin ロールが付与されます。システムアドミニストレーターは、セキュリティグループとユーザーを設定できる唯一のアドミンです。

セキュリティインシデントレスポンス の機能とレコードにアクセスするには、セキュリティロールが必要です。

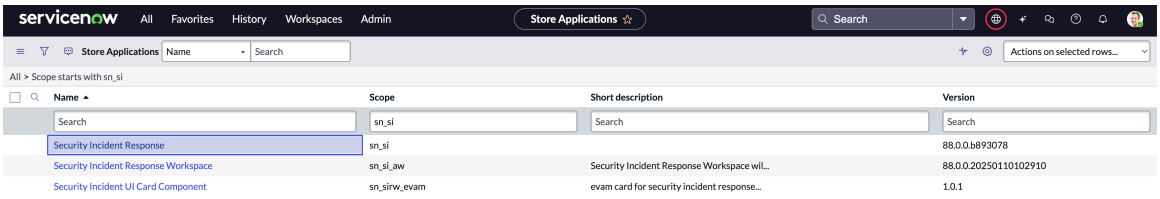
必要なロール：sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. セキュリティインシデントレスポンス プラグインがアクティブ化された後、admin ロールを持つユーザーが、スコープ指定アドミン (sn_si.admin) ロールを少なくとも 1 人のユーザーにアサインします。
2. admin ロールを持つユーザーがセキュリティインシデントスコープに変更されます。
3. 次のように移動する。 **All** (すべて) > **sys_store_app.list**.
4. [スコープ] フィールドに「sn_si」と入力します。



5. [セキュリティインシデントレスポンス] をクリックします。
6. [関連リンク] まで下にスクロールし、[アドミニストレーターが付与したロールから削除] をクリックします。
7. ログアウトして、再度ログインします。
アドミンユーザーは セキュリティインシデントレスポンス アプリケーションにアクセスできません。

関連情報

アプリケーション管理

制限付き発信者アクセスの管理

アドミニストレーターは、制限付き発信者アクセス (RCA) 機能を使用して、アプリケーションまたはアプリケーションリソースへのクロススコープアクセスを定義し、アクセス要求を許可または拒否できます。 セキュリティインシデントレスポンス ではこの機能がデフォルトで有効になっているため、セキュリティアナリストは機密性の高いセキュリティ関連情報を保護できます。

セキュリティインシデントレスポンス のすべてのテーブルとスクリプトインクルードに [発信者アクセス **(Caller access)**] と呼ばれるフィールドが追加されています。このフィールドは、デフォルトで [発信者追跡 **(Caller Tracking)**] に設定されます。この設定は、アプリケーションスコープが セキュリティインシデントレスポンス テーブルおよびスクリプトインクルードにアクセスできることを意味します。ただし、レコードごとにトラッキングレコードが作成され、制限付き発信者アクセス権限 [sys_restricted_caller_access] テーブルに格納されます。

注:
[発信者追跡 **(Caller Tracking)**] から [発信者制限 **(Caller Restricted]** にレコードを変更する場合は注意してください。アドミニストレーターが手動でアクセスを許可するまで、このステータスのレコードにアクセスすることはできません。アドミニストレーターは、次の場所に移動する必要があります システムアプリケーション > アプリケーションの制限付き発信者アクセスで、アクセスが要求されたテーブルまたはスクリプトインクルードを見つけて、[ステータス] フィールドを [要求済み] から [許可] に変更します。

関連情報

制限付き発信者アクセス特権の設定

アプリケーションスコープ、アプリケーションリソース、およびイベントへのアクセスの設定

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

セキュリティインシデントレスポンス のクイックスタートテストの実行

アップグレードの適用やアプリケーションの開発などの構成変更を行った後も、セキュリティインシデントレスポンス が変わらず正常に動作するかを検証します。自分のインスタンスに固有のデータを使用するときは、それが成功するように、これらのクイックスタートテストをコピーしてカスタマイズします。

セキュリティインシデントレスポンス クイックスタートテストではセキュリティインシデントレスポンスプラグイン (com.snc.security_incident) をアクティブ化して、デモデータをロードする必要があります。

セキュリティインシデントレスポンス テスト

テスト	説明	リリースバージョン
SIR：セキュリティインシデントの作成	ユーザーがセキュリティインシデントフォームからセキュリティインシデントを正常に作成できるかどうかを判断します。	Yokohama
SIR：セキュリティインシデントカタログからセキュリティインシデントを作成する	ユーザーがカタログからセキュリティインシデントを正常に作成できるかどうかを判断します。	Yokohama
SIR：セキュリティインシデントライフサイクル	ポリシー違反ワークフローの対応タスクを検証します。	Yokohama
SIR：脅威のルックアップ	脅威のルックアップ機能を検証します。	Yokohama
SIR：PIR アセスメント OOTB 構成	このテストを使用して、PIR アセスメントとベースシステム構成を検証します。	Yokohama
SIR：PIR アセスメントの条件付き構成	インシデントの事後アセスメントを完了せずに、必須の条件付きルールに一致するセキュリティインシデントがクローズされていないことを確認します。 インシデントの事後アセスメントを完了せずに、オプションの条件付きルールに一致するセキュリティインシデントがクローズされていないことを確認します。 ルールに一致しないセキュリティインシデントに対してアセスメントが生成されていないことを確認します。	Yokohama
SIR：PIR 実行時間検証	新しい設計に従って PIR レポートが構成され、セキュリティインシデントに添付されていることを検証します。	Yokohama
SIR：PIR デザイン時間セットアップ検証	アドミニストレーターの構成に基づいて、セキュリティインシ	Yokohama

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンス テスト (続く)

テスト	説明	リリースバージョン
	デントがレポートテンプレートにマップされていることを検証します。	
SIR：セキュリティインシデントを既存の重大なセキュリティインシデントにリンク	セキュリティインシデントを既存の重大なセキュリティインシデントにリンクし、重大なセキュリティインシデントにロールアップされたセキュリティインシデントからのデータを検証します。	Yokohama
SIR：セキュリティインシデントを重大なセキュリティインシデントとして昇格	セキュリティインシデントを重大なセキュリティインシデントとして昇格し、重大なセキュリティインシデントにロールアップされたセキュリティインシデントのデータを検証します。	Yokohama
SIR：重大なセキュリティインシデントとしてセキュリティインシデントを提案	セキュリティインシデントを重大なセキュリティインシデントとして提案し、重大なセキュリティインシデントにロールアップされたセキュリティインシデントからのデータを検証します。	Yokohama
[制限の適用] がオンになっていると、許可されたメンバーのみがセキュリティインシデントにアクセスできることを確認します。	[制限の適用] が有効になると、許可されたメンバーのみがセキュリティインシデントにアクセスできることを確認します。	Yokohama
[制限の適用] がオンになっていると、許可されたグループのみがセキュリティインシデントにアクセスできることを確認します。	[制限の適用] が有効になると、許可されたグループのみがセキュリティインシデントにアクセスできることを確認します。	Yokohama
読み取りアクセスを検証する	表示アクセスを検証します。	Yokohama
書き込みアクセスを検証する	編集アクセスを検証します。	Yokohama
SIR ワークスペース:読み取りアクセス	読み取りアクセスユーザーが、ワークスペースでもセキュリティロールがなくてもセキュリティインシデントを表示できることを確認する	Yokohama
SIR ワークスペース:書き込みアクセス	書き込みアクセスユーザーがセキュリティロールなしでセキュリティインシデントを更新できることを確認する	Yokohama
SIR ワークスペース:新規セキュリティインシデントの作成	ワークスペースから新しいセキュリティインシデントを作成	Yokohama

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンス テスト (続く)

テスト	説明	リリースバージョン
SIR ワークスペース:対応タスクの作成	既存のセキュリティインシデントから新しい応答タスクを作成する	Yokohama

関連情報

クイックスタートテスト

セットアップアシスタントの参考情報

セットアップアシスタントは、セキュリティインシデントレスポンス ベースシステムを設定するために実行する必要がある手順をガイドします。このセクションでは、さらに説明が必要な、複雑な手順について追加情報を提供します。

セキュリティインシデントレスポンス プロセス定義の作成

プロセス定義を作成して、セキュリティインシデントを 1 つのステータスから次のステータスに移行する方法を定義できます。プロセス定義は、サービスデスクとエンドユーザーがライフサイクル全体で問題を追跡するのに役立ちます。

始める前に

必要なロール：sn.si_admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > アドミニストレーション > プロセス定義.
2. [**New**] をクリックします。
3. 必要に応じてフィールドに入力します。

プロセス定義の作成

フィールド	説明
名前	スクリプトインクルードファイルでエンコードされたプロセスを説明するレコードの名前。名前は、[プロセス定義セレクター **(Process Definition Selector)**] リストの選択肢として表示されます。
スクリプトインクルード	プロセスの定義を含むスクリプトインクルードの名前 (sn_si. プリフィックスを含む)。スクリプトは、セキュリティインシデント (sn_si) アプリケーションスコープ内にある必要があります。詳細については、「カスタムの セキュリティインシデントレスポンス プロセス定義スクリプトインクルードの作成」を参照してください。このフィールドに有効なスクリプトインクルード名が含まれていない場合は、デフォルトの ProcessDefinition_NIST_Stateful 定義が使用されます。
説明	スクリプトインクルードに関する有用な情報。
順序	プロセス定義リスト内の位置を決定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
有効	オンにすると、このプロセス定義が [プロセス定義セレクター **(Process Definition Selector)**] ページから選択可能になります。

4. [送信] をクリックします。

関連情報

- セキュリティインシデントレスポンスプロセスの選択
- セキュリティインシデントレスポンスプロセス定義の概要

セキュリティインシデントレスポンスプロセス定義の概要

セキュリティインシデントレスポンス プロセス定義 は、状況フローを置き換え、エンドユーザーとサービスデスクに問題のステータスを提供します。プロセス定義は、問題のライフサイクル全体を追跡するのに役立ちます。セキュリティインシデントレスポンス はサービス管理 (SM) アプリケーションで、独自の状況セットを持ちます。無効な状況は プロセスの選択 の一部として報告されます。

セキュリティインシデントレスポンスプロセス定義

デフォルトのプロセス定義 (NIST Stateful) では、次のインシデント状況が定義されます。

注:
使用可能な状況は、インシデントの現在の状況によって異なります。

セキュリティインシデントプロセス定義の状況

状況	説明
ドラフト	要求のイニシエータが、セキュリティインシデントに関する情報を追加します。ただし、この段階では処理する準備がまだ整っていません。
分析	インシデントがアサインされ、問題が分析されます。
封じ込め	問題が特定され、セキュリティスタッフが問題の封じ込めとダメージコントロールを実行しています。これらのアクションには、サーバーのオフライン化、インターネットからの機器の切断、バックアップの存在の確認が含まれます。
根絶	問題が封じ込められ、セキュリティスタッフが問題を解決するための措置を講じています。
復旧	問題が解決され、対象システムの運用準備状況が検証されています。
レビュー	セキュリティインシデントが完了し、すべてのシステムが通常の機能に戻りました。ただし、インシデントの事後レビューがまだ必要です。
クローズ済み	インシデントが完了しました。ただし、セキュリティインシデントをクローズする前に、[クローズ情報] タブに情報を入力する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントタスクプロセス定義

セキュリティインシデントタスクには、次のプロセス定義が使用されます。

タスクプロセス定義状況

状況	説明
準備完了	タスクがエージェントにアサインされると、処理する準備が整います。
アサイン済み	タスクがエージェントにアサインされています。
対応中	アサインされたエージェントがタスクを処理しています。
完了	タスクが完了しました 。
キャンセル済み	タスクがキャンセルされました。

NIST は次の 2 つのモデルをサポートしています。

- **NIST Stateful**

  このプロセス定義により、アナリストはステップをスキップすることなく、各ステータスを順に移行できます。たとえば、アナリストが [ドラフト] ステータスで開始した場合、このプロセス定義の順序は [ドラフト] > [分析] > [封じ込め] > [根絶] > [復旧] になります。したがって、NIST ステートフルプロセス定義は単方向であり、アナリストは順方向でのみ状況を順方向にのみ移動できます。

  もう 1 つの例として、アナリストが [分析] ステータスで開始した場合、このプロセス定義の順序は [分析] > [封じ込め] > [根絶] > [復旧] になります。

- **NIST Open**

  このプロセス定義により、アナリストはステータス間を順方向と逆方向の両方で移行できます。もう 1 つの例として、アナリストが [分析] ステータスで開始した場合、このプロセス定義の順序は [分析] > [封じ込め] > [根絶] > [復旧] または [分析] > [ドラフト] になります。したがって、NIST オープンプロセス定義は双方向であり、アナリストは要件に応じて順方向または逆方向で状況間を移行できます。

セキュリティインシデントレスポンスプロセスの選択

セキュリティインシデントレスポンスプロセスの選択では、セキュリティインシデントと応答タスクに対して無効な状態のプロセスが一覧表示されます。

アドミニストレーターは、手動またはスクリプトを使用して、インシデントまたはタスクを有効な状況に修正できます。空の (インシデントもタスクもない) 関連リストは、すべてのアクティブなタスクが有効なステータスであることを示します。使用可能な状況は、インシデントの現在の状況によって異なります。詳細については、「プロセス定義を使用して無効なセキュリティインシデントまたはタスクのステータスを修正する」を参照してください。

セキュリティインシデントレスポンス プロセス定義の選択

会社のセキュリティインシデントおよび応答タスクの適切な状況に使用するプロセス定義を選択できます。

始める前に
必要なロール：admin および sn_si.admin

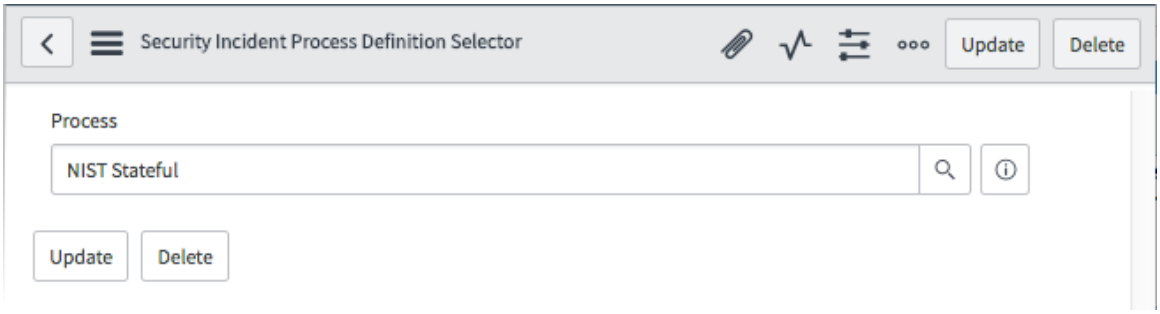
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて

手順

1. 次のように移動する。 **All** (すべて) > **Security Incident Response** (セキュリティインシデントレスポンス) > アドミニストレーション > プロセスの選択.
2. 検索アイコンをクリックすると、利用可能なプロセス定義のリストが表示されます。



3. プロセス定義を選択します。
4. [更新] をクリックします。

カスタムの セキュリティインシデントレスポンス プロセス定義スクリプトインクルードの作成

会社のセキュリティインシデントおよび応答タスクの適切な状況用のカスタムのプロセス定義スクリプトを作成します。

始める前に
必要なロール：sn_si.admin

このタスクについて
sn_si.ProcessDefinition メインスクリプトインクルードは、プロセス定義を制御します。[プロセス定義] は、使用される定義を決定します ([プロセスの選択] を使用)。適切なスクリプトインクルードファイルを呼び出して、セキュリティインシデントおよび応答タスクの両方の初期状況と移行を決定します。

手順

1. 次のように移動する。 **All** (すべて) > システム定義 > スクリプトインクルード.
2. [**New**] をクリックします。
3. 必要に応じてフィールドに入力します。

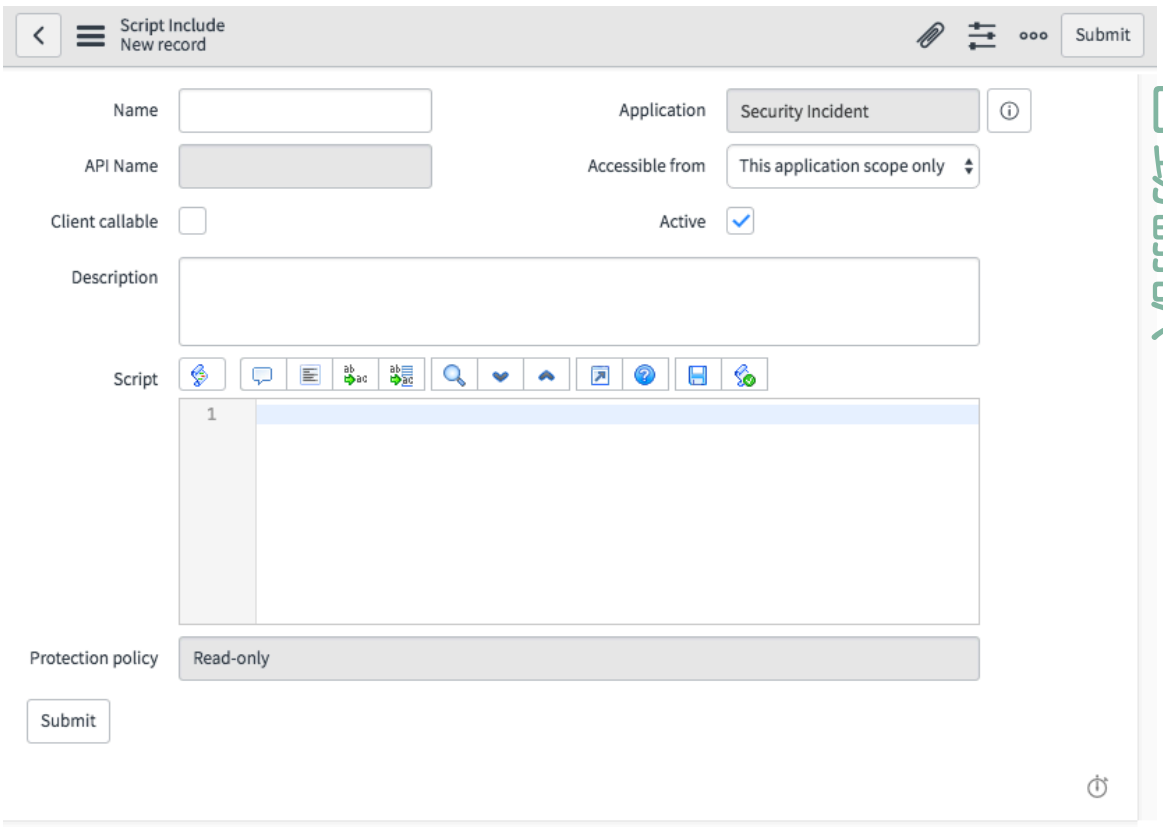
プロセス定義の作成

フィールド	説明
名前	このスクリプトインクルードの名前です。
API 名	スクリプトインクルードの名前に基づいて作成されます。
クライアント呼び出し可能	スクリプトインクルードをクライアントスクリプト、リストとレポートフィルター、参照修飾子で使用できるようにするか、指定されている場合は URL の一部として使用できるようにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
アプリケーション	セキュリティインシデント
アクセス可能	[このアプリケーションスコープのみ] を選択します。
有効	オンにすると、このスクリプトインクルードが [プロセス定義] ページから選択可能になります。
説明	スクリプトインクルードに関する有用な情報。
スクリプト	他のスクリプトから呼び出されたときに実行するサーバーサイドスクリプトを定義します。 スクリプトは、単一の JavaScript クラスまたはグローバル関数を定義する必要があります。クラス名または関数名は [名前] フィールドと一致する必要があります。 スクリプトのコンテンツの詳細については、「プロセス定義スクリプトインクルード」を参照してください。



自動翻訳

4. [送信] をクリックします。

関連情報

プロセス定義スクリプトインクルード

プロセス定義スクリプトインクルード

プロセス定義スクリプトインクルードは、プロセス定義を定義するためのメソッドを提供します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ここで説明されている定数、属性、アレイ、およびメソッド呼び出しを実装して、プロセス定義スクリプトインクルードをカスタマイズします。

使用する状況

このスクリプトインクルードを使用して、プロセス定義を作成します。

スクリプトインクルードの本文

スクリプトインクルードの本文は、次の 3 つのセクションで構成されます。

- 定数：初期ステータスの定義
- セキュリティインシデントと応答タスク：プロセス定義のアレイ
- メソッド呼び出し：情報の取得

定数

定数は、セキュリティインシデントと応答タスクの初期状況を定義するために使用されます。

定数の使用はオプションですが、読みやすくするため使用することをお勧めします。例：

```
INITIAL_INCIDENT_STATE: 10,
INITIAL_TASK_STATE: 1,
```

後続のメソッドで次のように使用されます。

```
getInitialIncidentState: function() {
return this.INITIAL_INCIDENT_STATE;
},
getInitialTaskState: function() {
return this.INITIAL_TASK_STATE;
},
```

次の定数セットは、セキュリティインシデントと応答タスクの両方の状況を定義します。

各アレイには、インシデントまたはタスクが特定の状況にあるときに使用できる状況の定義も含まれています。

例：

```
TASK_STATES: [{state:1, label:"Draft", choice:[1, 10]},
 {state:10, label:"Ready", choice:[10, 16]},
 {state:16, label:"Assigned", choice:[16, 18]},
 {state:18, label:"Work in Progress", choice:[18, 3]},
 {state:3, label:"Close Complete", choice:[]},
 {state:7, label:"Cancelled", choice:[]},
 ],
```

この例は、オブジェクトのアレイです。各オブジェクトは、状況および可能な移行状況を定義します。

ステータスのオブジェクトの順序によって、フローの必要な順序が決まります。

タスクが [ドラフト] 状況 (値 1) の場合、可能なステータスは 1 (ドラフト、変更なし) および 10 (準備完了、プロセスの次のステップ) です。

ステータスからの移行回数に制限はありません。[完了してクローズ] 状況および [キャンセル] 状況は最終状況であるため、状況の移行はできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オブジェクト内の属性の順序は重要ではありません。定義が明確になる場合は、最初にラベルを配置します。

属性

ステータス定義オブジェクトに必要な属性は次のとおりです。

- state：ステータスの数値
- label：ステータスに関連付けられた分かりやすいテキスト
- choice：ステータスが移行できるステータス値のアレイ (ステータスドロップダウンの内容を決定)

オプションの属性は次のとおりです。

- mandatory：このステータスで必須になるフィールド ID のリスト
- readonly：このステータスで読み取り専用になるフィールド ID のリスト
- visible：このステータスで表示されるフィールド ID のリスト
- notmandatory：このステータスで任意になるフィールド ID のリスト
- notvisible：このステータスで表示されなくなるフィールド ID のリスト

注:

オプションの属性を使用する場合、状況間で適切にフィールドが表示/非表示、必須/非必須、または読み取り専用になっていることを確認するのは作成者の責任です。

たとえば、「visible」属性を使用しない限り、あるステータスでフィールドを非表示にすると、後で別のステータスで表示されることはありません。

プロセスフロー定義のアレイ

プロセスフローフォーマッター (セキュリティインシデントおよび応答タスクフォームの上部にあるバー) に表示される情報を定義するには、各ステータスの表示内容に関する情報がシステムに必要です。

例：

```
TASK_PF: [{label:"Draft", condition:"state=1^EQ", description:"<p>Security Incident Response Task is in draft</p>"},
{label:"Ready", condition:"state=10^EQ", description:"<p>Security Incident Response Task is ready to be assigned</p>"},
{label:"Assigned", condition:"state=16^EQ", description:"<p>Security Incident Response Task is assigned</p>"},
{label:"Work in Progress", condition:"state=18^EQ", description:"<p>Work has started on this Security Incident Response Task</p>"},
{label:"Closed", condition:"state=3^ORstate=4^ORstate=7^EQ", description:"<p>Security Incident Response Task is complete</p>"},
],
```

TASK_PF アレイは、プロセスフォーマッターバーに表示されるテキスト (順序とアクティビティを含む) を決定するために使用されるラベル、条件、および説明のコレクションです。

この例では、「準備完了」というテキストが 2 番目に表示されます。タスクが条件「state=10^EQ」を満たした場合にハイライト表示されます。

ポインターをテキストの上に置くと、「セキュリティインシデントレスポンスタスクをアサインする準備ができました」という説明が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

状況は、単一のフォーマッター状況に結合できます。

この例では、[完了してクローズ] 状況と [キャンセル] 状況の両方がトップバーに [クローズ済み] として表示されます。

メソッド呼び出し

次のメソッドは sn_si.ProcessDefinition で使用されるため、スクリプトインクルードに存在する必要があります。

戻り値の型	メソッドの概要	説明
文字列	getInitialIncidentState: function()	初期インシデント状況の数値を返す
文字列	getInitialTaskState: function():	初期タスクステータスの数値を返す
文字列のアレイ	getIncidentStates: function():	インシデント状況のアレイを返す
文字列のアレイ	getTaskStates: function():	タスクステータスのアレイを返す
オブジェクトのアレイ	getIncidentProcessFlows: function():	インシデントプロセスフロー定義アレイを返す
オブジェクトのアレイ	getTaskProcessFlows: function():	タスクプロセスフロー定義アレイを返す

次の一連のメソッドは、インシデントまたはタスクが更新されるたびに呼び出され、特定の変更移行に対してアクションを実行できるようにします。

戻り値の型	メソッドの概要	説明
なし	performIncidentStateChange: function(current, previous)	例では、このメソッドを使用して SM 関連の値を設定し、誰かがインシデントにアサインされると、インシデントが [ドラフト] から進むようにします。
なし	performTaskStateChange: function(current, previous)	例では、このメソッドを使用してタイムスタンプ (アサイン時とクローズ時) を更新し、assigned_to フィールドが入力されるとタスクを [準備完了] から [アサイン済み] に進めます。

これら 2 つのメソッドで実行される同じアクションは、ビジネスルールを使用して実行できます。スクリプトインクルードで定義することで、プロセス定義の切り替えが容易になります。

プロセス定義を使用して無効なセキュリティインシデントまたはタスクのステータスを修正する

アドミニストレーターは、手動またはスクリプトを使用して、セキュリティインシデントまたはタスクを有効な状況に修正できます。使用可能な状況は、インシデントの現在の状況によって異なります。

始める前に
必要なロール：admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

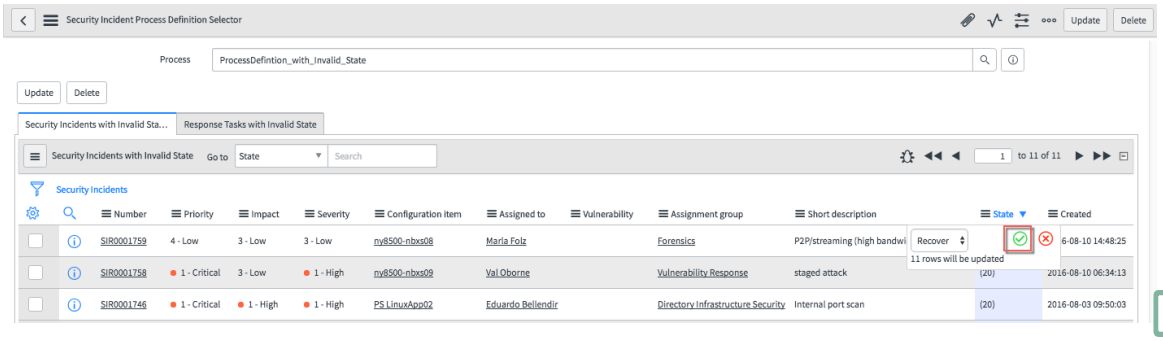
このタスクについて

プロセス定義を切り替えた後、新しい定義で古いステータスの一部がサポートされない可能性があります。孤立したインシデントまたはタスクの状況を修正するには、プロセス定義を変更するか、スクリプトインクルードを編集するか、各インシデントまたはタスクを手動で開いて状況を更新します。一般に、ステータスの更新 (一括で実行可能) が最も簡単な解決策です。

一括で状況を変更するには、次の手順を実行します。

手順

1. 次のように移動する。 **All** (すべて) > プロセスの選択.
2. 変更するインシデントまたはタスクの [ステータス **(State)**] フィールドをハイライト表示します。
3. 最初のレコードの [ステータス **(State)**]フィールドをダブルクリックし、新しい [ステータス **(State)**] を選択し、緑色のチェックマーク ( ) をクリックして、変更を完了します。



4. [更新] をクリックします。

セキュリティインシデントグループの作成

セキュリティインシデントグループをセットアップし、適切なロールとユーザーをグループにアサインします。

始める前に

必要なロール：

- user_admin ロールを持っている場合は、セキュリティインシデントアサイン先グループを作成できます。
- sn_si.admin ロールを持っている場合は、セキュリティインシデントアサイン先グループの作成と編集ができます。

このタスクについて

グループに属するユーザーはグループのロールを継承するため、各ユーザーに個別にロールをアサインする必要はありません。
組織に必要な数だけグループを作成することをお勧めします。アドミン用に 1 つのグループを作成し、そのグループのみに admin ロールをアサインすることもお勧めします。

手順

1. 次のように移動する。 **All** (すべて) > ユーザー管理 **(User Administration)** > グループ または セキュリティインシデント > セットアップ > グループ.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

詳細については、「ユーザーグループの作成」を参照してください。

4. このグループには、[セキュリティインシデント] タイプを選択してください。
   a. [タイプ] フィールドが表示されていない場合は、フォームを構成して追加します。
   b. [タイプ] フィールドの横にあるロックアイコンをクリックします。
   c. 参照ルックアップアイコン () をクリックします。
   d. [セキュリティインシデント] タイプを検索して選択します。
5. フォームヘッダーを右クリックし、[保存] を選択します。
6. [ロール] 関連リストで、このグループの各メンバーが受け取るロールを追加します。
   たとえば、セキュリティインシデントレスポンス チームメンバーのグループを作成する場合は、sn_si.analyst を追加します。セキュリティインシデントレスポンス アドミンのグループを作成する場合は、sn_si.admin を追加します。
7. [グループメンバー] 関連リストで、このグループにユーザーを追加します。
8. [更新] をクリックします。

セキュリティインシデント算出グループの作成

セキュリティインシデント算出グループは、算出をグループ化するために使用されます。

始める前に
必要なロール：sn_si.admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > セットアップ > セキュリティインシデント算出グループ.
2. **[New]** をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
名前	セキュリティインシデント算出の名前
アプリケーション	このレコードを含んでいるアプリケーション。
順序	セキュリティインシデント算出が実行される順番。順序エントリーが 100 の算出は、順序エントリーが 200 の算出の前に実行されます。
説明	この算出グループの説明。
作成者	作成したユーザーの名前を入力します。

4. **[Submit]** をクリックします。

セキュリティインシデント算出の作成

セキュリティインシデント算出を使用すると、事前定義された式に基づいてセキュリティインシデントの重大度を計算できます。必要に応じて、独自のセキュリティインシデント算出を定義できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_si.admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > セットアップ > セキュリティインシデント算出グループ.
2. 算出を作成するグループの名前をクリックするか、算出グループを作成します。
3. [新規] をクリックします。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
名前	セキュリティインシデント算出の名前
算出グループ	この算出が属するグループの名前 **注:** [名前] と [テーブル] に入力した後、算出グループの作成または変更ができるようになります。
テーブル	この算出で使用するテーブルを選択します。 脆弱性 [sn_vul_vulnerability] や脆弱性一致アイテム [sn_vul_vulnerable_item] 以外のテーブルに算出を追加する場合は、これらのテーブルにビジネスルールと UI アクションを追加する必要があります。例を表示するには： ○ 次のように移動する。 システム定義 > ビジネスルールをクリックし、脆弱性一致アイテム [sn_vul_vulnerable_item] テーブルで **[Calculate Severity**] ビジネスルールを見つけます。 ○ 次のように移動する。 システム **UI** > **UI** アクションをクリックし、脆弱性一致アイテム [sn_vul_vulnerable_item] テーブルで [重大度の計算] UI アクションを見つけます。 また、脆弱性アドミンロールには、算出で使用されるすべてのテーブルに対する完全な読み取り/書き込み (または save_as_template) 機能を付与し、テンプレートに適用する値を正しく表示できるようにする必要があります。
アプリケーション	算出が属するスコープ対象のアプリケーション。
順序	セキュリティインシデント算出が実行される順番。順序エントリーが 100 の算出は、順序エントリーが 200 の算出の前に実行されます。
有効	計算機をオンまたはオフにします。
説明	この算出の説明。

5. フォームヘッダーを右クリックし、[保存] を選択します。
[条件] および [適用する値 **(Values to Apply)]** タブが表示されます。
6. 必要に応じて、[条件] タブのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
フィルタグループを使用	事前定義フィルターグループを使用するか、または新しいフィルターグループを作成して算出基準を定義する場合は、このチェックボックスをオンにします。
フィルターグループ	算出の定義に使用するフィルターグループを選択します。 このフィールドは、[フィルターグループを使用] チェックボックスをオンにした場合のみ表示されます。
詳細条件を使用	このチェックボックスをオンにすると、スクリプト条件を使用して、この算出が適用されるタイミングを決定できます。チェックボックスをオンにすると、[詳細条件] スクリプトフィールドが表示されます。 [フィルターグループを使用] チェックボックスをオンにした場合、このフィールドは非表示になります。 **注:** 詳細条件を定義し、セキュリティインシデント算出を適用するタイミングを決定するスクリプトを記述する前に、[セキュリティインシデント算出] リストに戻ります。ベースシステムに付属している算出レコードを確認します。
条件	算出を使用するかどうかを決める基本的なフィルター条件を定義します。 [フィルターグループを使用] または [詳細条件を使用] チェックボックスをオンにした場合、このフィールドは非表示になります。

7. [適用する値 **(Values to Apply)]** タブをクリックし、必要に応じてフォームのフィールドに入力します。
算出に適用する値を定義するためのスクリプトを作成するか、選択したテーブルのフィールドに基づいてテンプレートを定義するかを選択できます。

フィールド	説明
スクリプト値の使用	スクリプトでフィールド値を定義するには、このチェックボックスをオンにします。
スクリプト値	計算を適用する値を定義します。 このフィールドは、[スクリプト値の使用] チェックボックスをオンにした場合のみ表示されます。
テンプレート	フォームヘッダーを右クリックし、[保存] を選択します。計算機に使用するフィールドと値を選択します。

8. すべての入力が完了したら、[送信] をクリックします。

セキュリティインシデント算出の理解

セキュリティインシデント算出は、事前定義された条件が満たされたときにレコード値を更新するために使用されます。算出は、レコードの更新方法を決定するために使用される基準に基づいてグループ化されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンス ベースシステムには、次のセキュリティインシデント算出グループと算出が含まれています。各グループ内で、条件に一致する最初の計算が実行されます。

ベースシステムのセキュリティインシデント算出

セキュリティインシデント算出のグループ名	グループに含まれる算出	説明
ビジネスインパクト	重大度算出から集計	この算出では、その他のフィールドの値を重み付けすることにより重要度を決定する Security Criticality Calculator に委任します。
重大度	影響を受ける事業	この重大度算出では、シンプルな条件ビルダーを使用して選択基準を定義します。
	影響を受けた重要サービス	この重大度算出では、詳細条件を使用して選択基準を定義します。 セキュリティインシデントの構成アイテムが重要性の高いビジネスサービスに関連付けられている場合、[リスクスコア]、[ビジネスインパクト]、および [優先度] フィールドは、算出で定義されたとおりに昇格されます。
	重要なサービス変更	この重大度算出では、詳細条件を使用して選択基準を定義します。 セキュリティインシデントが条件を満たしている場合、スクリプトが実行され、フィールドがどのレベルに昇格されるかを定義します。セキュリティインシデントの構成アイテムが最も重大またはやや重要なビジネスサービスに関連付けられている場合、[リスクスコア]、[ビジネスインパクト]、および [優先度] フィールドは、算出で定義されたとおりに昇格されます。
	複数攻撃ベクトル	この重大度算出では、シンプルな条件ビルダーを使用して選択基準を定義します。 セキュリティインシデントの構成アイテムが Web、メールおよび代理操作の攻撃ベクトルに関連付けられている場合、[リスクスコア]、[ビジネスインパクト]、および [優先度] フィールドは、算出で定義されたとおりに昇格されます。
	カテゴリとサービスを使用して優先度を設定	この重大度算出では、詳細条件ビルダーを使用して選択基準を定義します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ベースシステムのセキュリティインシデント算出 (続く)

セキュリティインシデント算出のグループ名	グループに含まれる算出	説明
		次の条件が満たされた場合、セキュリティインシデントの優先度は **[1 -** 重大] に設定されます。 • 影響を受けるサービスがセキュリティインシデントに関連付けられており、そのうちの 1 つが重大である。 • セキュリティインシデントのカテゴリが次のいずれかである。 ○ サービス拒否 ○ スピアフィッシング ○ 悪意のあるコードアクティビティ **注:** この算出は、Starter Security Operations の価格階層がある場合にベースシステムで使用できます。
	観測可能項目の優先度を設定	この重大度算出では、詳細条件ビルダーを使用して選択基準を定義します。 次の条件が満たされた場合、セキュリティインシデントの優先度は **[1 -** 重大] に設定されます。 • 影響を受けるサービスがセキュリティインシデントに関連付けられており、そのうちの 1 つが重大である。 • セキュリティインシデントのカテゴリが次のいずれかである。 ○ サービス拒否 ○ スピアフィッシング ○ 悪意のあるコードアクティビティ • 関連する観測事象またはインジケーターの 1 つのサイティング回数が、アクティブなインジケーターによる 2 回のサイティングを超えています (複数のソースからの観測事象またはインジケーターが不適切であると確認されています)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

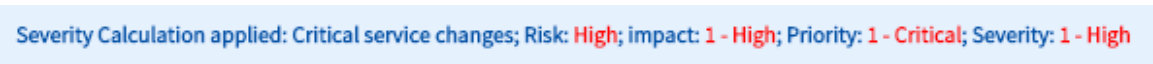
ベースシステムのセキュリティインシデント算出 (続く)

セキュリティインシデント算出のグループ名	グループに含まれる算出	説明
		注: この算出をベースシステムで使用できるのは、Advanced Security Operation の価格階層があり、Threat Feeds プラグインをアクティブ化している場合です。
ユーザー重要度	ユーザー重要度を取得	この重大度算出では、シンプルな条件ビルダーを使用して選択基準を定義します。 この重大度算出では、[部門] フィールドが [経理] に変更されたときに、ユーザーのビジネス上の重要度が **[1 - 重大]** に変更されます。
	ユーザーグループ重要度を取得	この重大度算出では、詳細条件ビルダーを使用して選択基準を定義します。 この重大度算出は、関連リストのデータで実行される算出の例です。

重大度算出

セキュリティインシデントを作成すると、[リスクスコア]、[ビジネスインパクト]、および [優先度] フィールドにデフォルト値が入力されます。インシデントを保存すると、ビジネスルールによって、アクティブな重大度算出で定義された条件に照らしてセキュリティインシデントの情報が自動的に検証されます。これらは、各算出の [順序] フィールドで定義された順序で、一度に 1 つずつセキュリティ算出が検証されます。セキュリティインシデントの情報がいずれかの算出で定義された条件と一致する場合、重大度フィールドの値は算出で設定されたルールに従って更新されます。

たとえば、影響を受ける CI のセキュリティインシデントを作成し、その CI の重要性が高いとします。セキュリティインシデントが保存されると、CI 情報が重大度算出で定義された条件と比較されます。[影響を受けた重要サービス] の重大度算出に照らしてセキュリティインシデントが検証されると、重大度フィールドが自動的に更新され、次のようなメッセージがセキュリティインシデントの上部に表示されます。



これらの重大度算出をそのまま使用することも、ビジネスのニーズに細かく合わせて編集することもできます。たとえば、経理の事業部門に固有の Web およびメールの脅威を特定する場合は、[複数攻撃ベクトル] 算出の条件を変更できます。

- [攻撃ベクトル] [含む] [Web]
- [攻撃ベクトル] [含む] [メール]
- [事業部門] [含む] [経理]

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レコードを開き、[重大度の計算] 関連リンクをクリックすることで、既存のセキュリティインシデントの重大度の値をいつでも更新することもできます。

セキュリティインシデントリスクスコア算出

[カテゴリとサービスを使用して優先度を設定] および [観測可能項目の優先度を設定] 算出は、セキュリティインシデントのリスクスコアを計算するために使用されます。

ユーザー重要度算出

[ユーザー重要度] グループの 2 つの算出 ([ユーザー重要度を取得] および [ユーザーグループ重要度を取得]) では、ユーザーレコードで定義された基準またはユーザーが属するグループに基づいて重要度をどのように算出できるかの例を示します。

これらは、必要に応じて編集したり、新しいユーザー重要度算出を作成したりできます。

[ユーザー重要度を取得] 算出では、[部門] フィールドが [経理] に変更されたときに、ユーザーのビジネス上の重要度が **[1 - 重大]** に変更されます。

[ユーザーグループ重要度を取得] 算出では、ユーザーが [データベース] グループに追加されたときに、ユーザーのビジネス上の重要度が **[1 - 重大]** に変更されます。

注:
[ユーザーグループ重要度を取得] は、関連リスト内のデータに対して実行される算出の 1 つです。重要度の変更を開始するグループをさらに追加する場合は、スクリプトの最初の行にグループ sys_id のカンマ区切りリストを追加します。例：var CRITICAL_GROUPS = [group1_sys_id, group2_sys_id, group3_sys_id]。

セキュリティインシデントリスクスコア算出

リスクスコアは、セキュリティインシデントの優先度、セキュリティインシデントのタイプ (サービス拒否、スピアフィッシング、または悪意のあるコードアクティビティ)、およびインジケーター上の否定的な評価スコアの要因となったソース数に基づくリスクを表す算術平均として計算されます。

リスクスコアは、アナリストのセキュリティインシデント作業の優先順位付けに役立ちます。

重要:
新しいリスクスコア算出を使用する場合は、「新しいリスクスコア算出ルールの定義」を参照してください。

[カテゴリとサービスを使用して優先度を設定] および [観測事象の優先度を設定] セキュリティインシデント算出は、セキュリティインシデントのリスクスコアを計算するために使用されます。さらに、次のビジネスルールによってリスクスコアの自動計算がトリガーされます。

- 重大度の計算
- リスクスコアの更新
- SI リスクスコアの更新

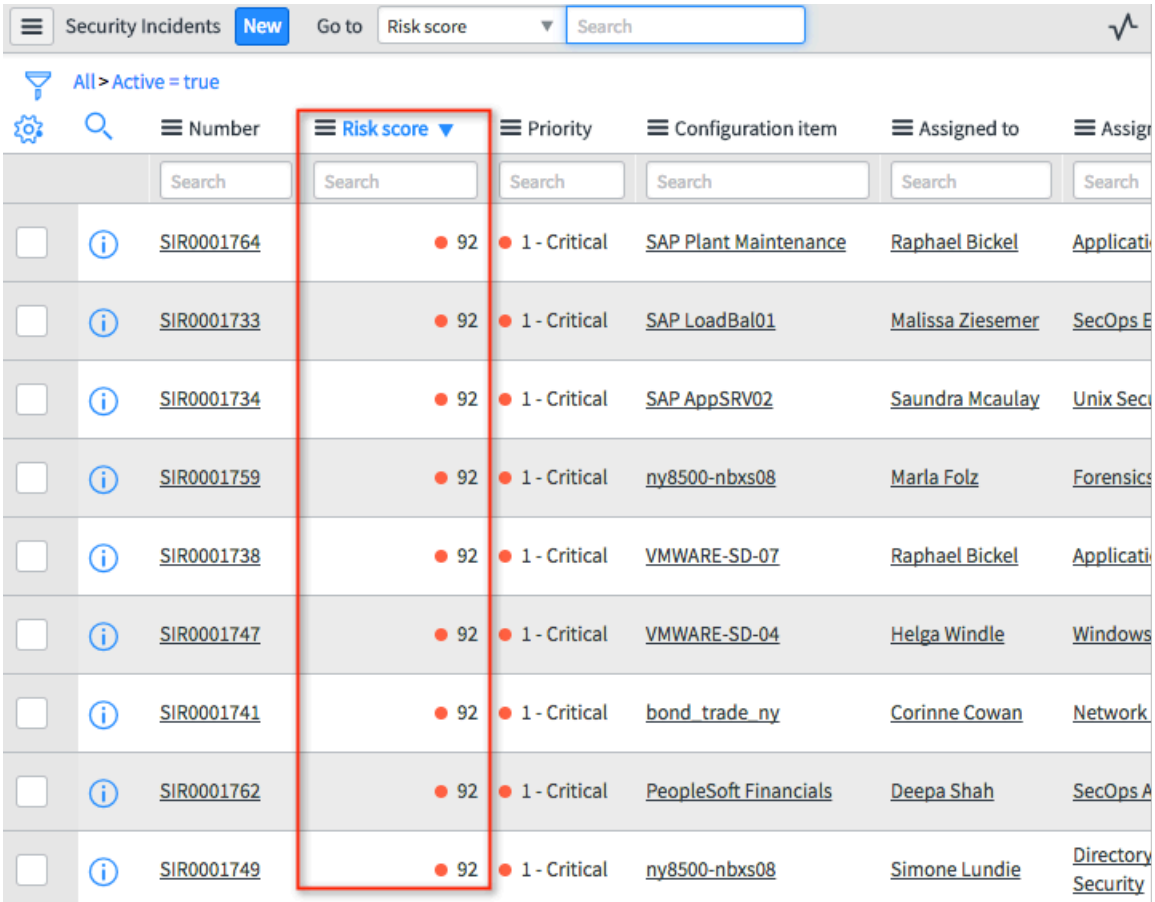
注:
ベースシステムで利用できるリスク算出は、Security Operations の価格階層によって異なります。

ベースシステムのセキュリティインシデントのリストを表示すると、[リスクスコア] 列があることを確認できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

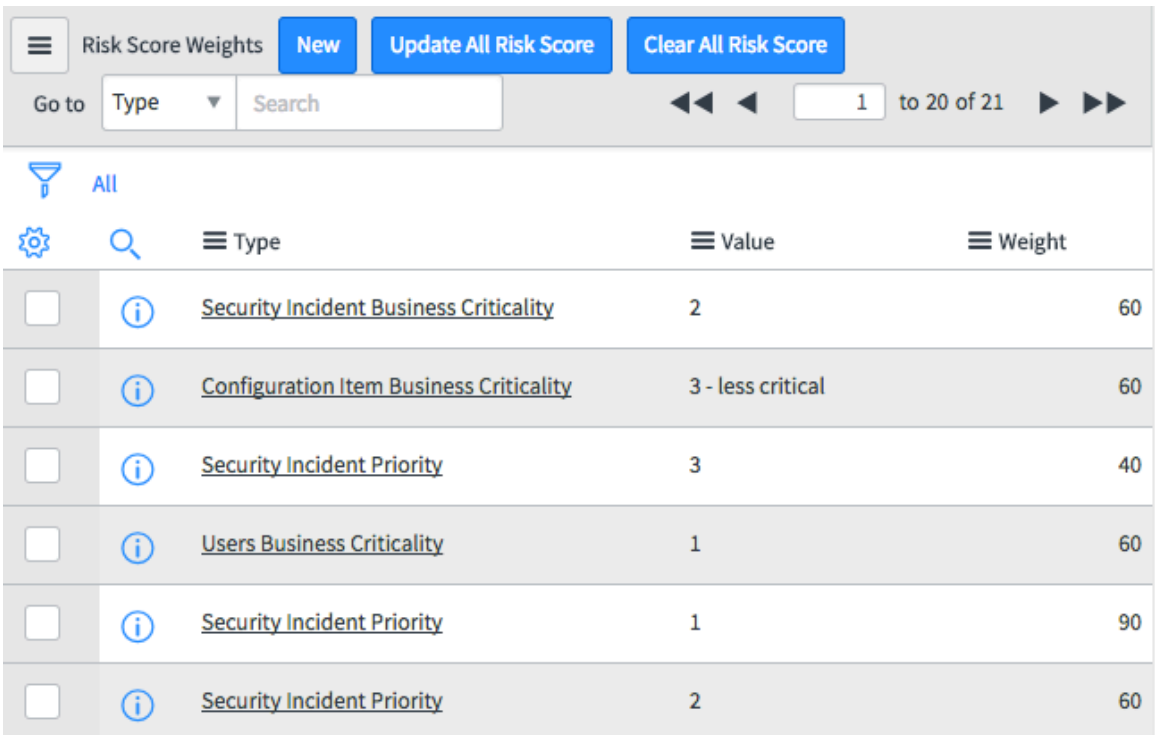
セキュリティインシデント



Number	Risk score	Priority	Configuration item	Assigned to	Assig
SIR0001764	92	1 - Critical	SAP Plant Maintenance	Raphael Bickel	Applicati
SIR0001733	92	1 - Critical	SAP LoadBal01	Malissa Ziesemer	SecOps E
SIR0001734	92	1 - Critical	SAP AppSRV02	Saundra Mcaulay	Unix Secu
SIR0001759	92	1 - Critical	ny8500-nbxs08	Marla Folz	Forensics
SIR0001738	92	1 - Critical	VMWARE-SD-07	Raphael Bickel	Applicati
SIR0001747	92	1 - Critical	VMWARE-SD-04	Helga Windle	Windows
SIR0001741	92	1 - Critical	bond_trade_ny	Corinne Cowan	Network
SIR0001762	92	1 - Critical	PeopleSoft Financials	Deepa Shah	SecOps A
SIR0001749	92	1 - Critical	ny8500-nbxs08	Simone Lundie	Directory Security

リスクスコアは、リスクスコア設定で定義された重み付けを使用して計算されます。

リスクスコア設定



Type	Value	Weight
Security Incident Business Criticality	2	60
Configuration Item Business Criticality	3 - less critical	60
Security Incident Priority	3	40
Users Business Criticality	1	60
Security Incident Priority	1	90
Security Incident Priority	2	60

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

たとえば、セキュリティインシデントの [ビジネスインパクト] が **[2 -** 高い] に設定され、[優先度] が **[3 -** 中] に設定されている場合、[リスクスコアの重み付け] テーブル内のそれぞれの重み付けは、次のようにルックアップおよび計算されます。

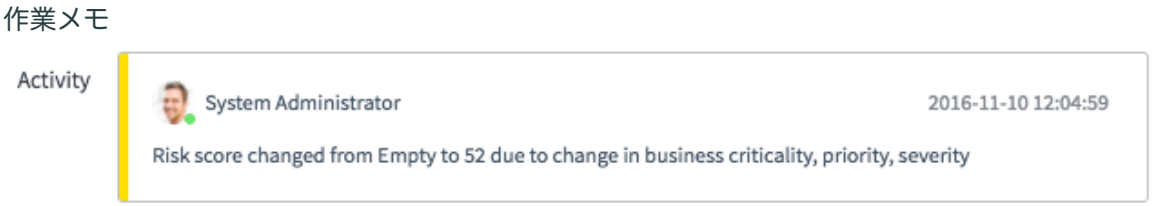
セキュリティインシデントのビジネスインパクトが 2 の場合、重み付けは 60 です。

セキュリティインシデントの優先度が 3 の場合、重み付けは 40 です。

(60 + 40)/2 = リスクスコア 50。

セキュリティインシデントリスト内のセキュリティインシデントの位置は、更新されたリスクスコアに基づいて並べ替えられます。

上記の例で、セキュリティインシデントのビジネスインパクトまたは優先度が変更されると、リスクスコアが再計算され、変更が作業メモに反映されます。



作業メモは、次のフィールドが変更されてリスクスコアが更新されたときに更新されます。

- セキュリティインシデントフォームの [ビジネスインパクト]
- セキュリティインシデントフォームの [優先度]
- セキュリティインシデントフォームの [重大度] (デフォルトでは非表示)
- [影響を受けるユーザー] 関連リストの [ビジネスインパクト]
- [影響を受けるサービス] 関連リストの [ビジネスインパクト]
- [脆弱性一致アイテム] 関連リストの [ビジネスインパクト]

さらに、作業メモは、次の状況で更新されます。

- 影響を受けるユーザーとセキュリティインシデントの関連付けが作成または変更されたとき
- 影響を受けるサービスとセキュリティインシデントの関連付けが作成または変更されたとき
- 脆弱性一致アイテムとセキュリティインシデントの関連付けが作成または変更されたとき

また、作業メモは、[リスクスコアの重み付け] フォームで [すべてのリスクスコアを更新] および [すべてのリスクスコアをクリア] がクリックされるたびに更新されます。

リスクスコアの重み付けの管理

セキュリティインシデントのリスクスコアの計算に使用されるリスクスコアの重み付けは、個別に削除または更新できます。すべてのセキュリティインシデントに対して削除または更新することもできます。セキュリティインシデントからの重み付けの削除機能は、重み付けの値を変更する場合に役立ちます。

始める前に
必要なロール：sn_sec_cmn.admin

注:
sn_si.read ロールを持つユーザーは、セキュリティインシデントレスポンス でリスクスコア構成を表示できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > セットアップ > リスクスコアの設定.

   > **注:**
   > sn_si.read ロールを持つユーザーは、次の場所に移動してリスクスコア構成を表示できます。 セキュリティインシデント > アラートとイベント > リスクスコア設定.

2. 新しいリスクスコアの重み付けを追加するには、[新規] をクリックし、フィールドに情報を入力します。

フィールド	説明
タイプ	定義するリスクスコアのタイプを選択します。
値	選択したタイプに関連付けられた値を指定します。タイプで複数の値が利用可能な場合は、複数のリスクスコア重み付けレコードを定義することもできます。例：セキュリティインシデント優先度の値が 1、セキュリティインシデント優先度の値が 2 などです。
重み付け	選択したタイプ/値のペアに関連付けられた重み付け。有効なエントリーは 0 ～ 100 で、0 が最小の重み付け、100 が最大です。

3. **[Submit]** をクリックします。
4. 必要に応じて、次の手順を実行します。
   - リスクスコアの重み付けレコードをクリアするには、リストからレコードを開いて、[削除] をクリックします。
   - すべてのリスクスコアの重み付けレコードをクリアするには、[すべてのリスクスコアをクリア] をクリックします。
   - すべてのリスクスコアの重み付けレコードを更新するには、[すべてのリスクスコアを更新] をクリックします。

セキュリティインシデントレスポンス **SLA** の作成

セキュリティインシデントレスポンス の Service Level Agreement (SLA) を定義できます。

始める前に
必要なロール：sn_si.admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > セットアップ > **SLA**.
2. [**New**] をクリックします。
   フィールドの説明と詳細な手順については、「Create an SLA definition」を参照してください。

セキュリティインシデント **SLA** の修理

SLA のタイミングと期間の情報が正確になるように、SLA レコードを修理することができます。

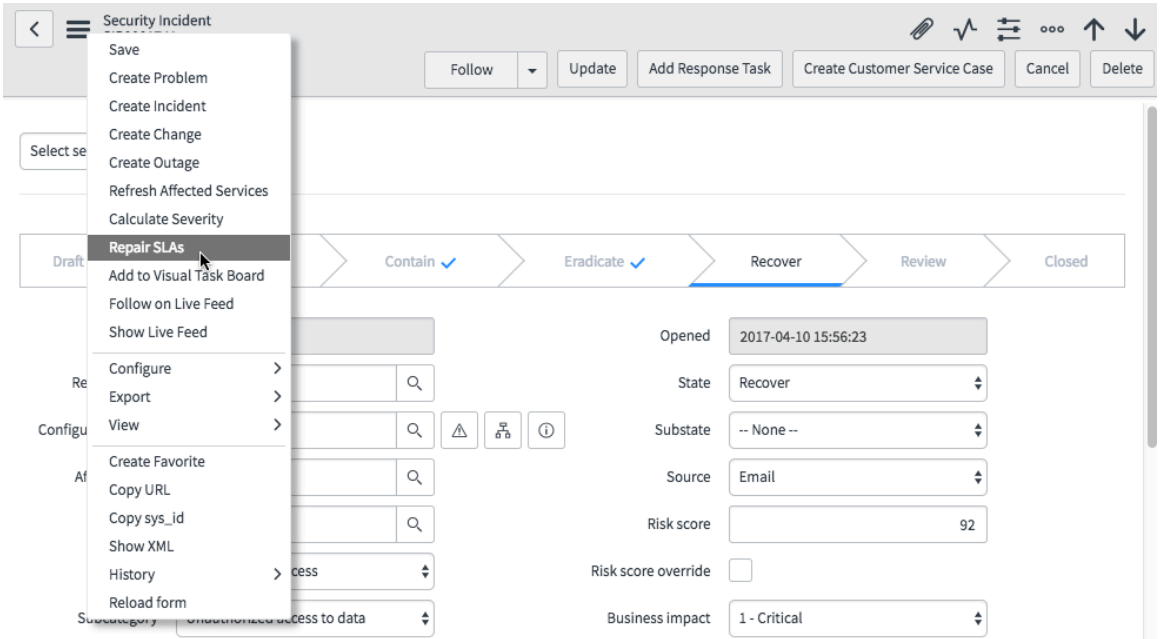
始める前に
必要なロール：sn_si.basic

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. SLA を修理するセキュリティインシデントがまだ開いていない場合は、これを開きます。
2. フォームヘッダーのコンテキストメニューをクリックし、**[SLA** の修理] を選択します。



3. 警告の確認ボックスで **[OK]** をクリックします。
   詳細については、「SLA の修理」を参照してください。

セキュリティインシデントレスポンス **Runbook** の作成

Runbook は、公開されたナレッジ記事と特定のタスクとの関連付けです。タスクを実行している間、Runbook のナレッジ記事が自動的に開き、タスクに関連する情報が提供されます。

始める前に

セキュリティインシデントレスポンス Runbook ナレッジベースにナレッジ記事が存在している必要があります。セキュリティインシデントナレッジ記事を作成するときは、必ず [ナレッジベース] フィールドで [セキュリティインシデントレスポンス **Runbook]** を選択します。記事を公開した後、**[Runbook** を作成] ボタンをクリックできます。

必要なロール：sn.si.knowledge_admin

このタスクについて

セキュリティインシデントまたは応答タスクの作成プロセス中に Runbook を使用するか、または Runbook のナレッジベース記事をプレイブックのタスクに関連付けることができます。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > 手動 **Runbook** > 新しい **Runbook** を作成.
2. 必要に応じて、フィールドに入力します。

フィールド	説明
ナレッジ記事	Runbook に含めるナレッジ記事を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
有効	[フィルターナビゲーター] から Runbook を利用できるようにするには、このボックスをオンにします。
フィルタグループを使用	事前定義フィルターグループを使用するか、または新しいフィルターグループを作成して Runbook 基準を定義する場合は、このチェックボックスをオンにします。
フィルターグループ	Runbook の定義に使用するフィルターグループを選択します。 このフィールドは、[フィルターグループを使用] チェックボックスが選択されている場合にのみ表示されます。
テーブル	セキュリティインシデント [sn_si_incident] または セキュリティインシデントレスポンス タスク [sn_si_task] を選択します。 [フィルターグループを使用] チェックボックスをオンにしてフィルターグループを選択した場合、このフィールドは、選択したフィルターグループに関連付けられたテーブルにデフォルトで設定されます。
条件	この Runbook をインシデントまたはタスクに関連付ける条件を設定します。 [フィルターグループを使用] チェックボックスをオンにしてフィルターグループを選択した場合、[条件] フィールドは表示されません。

3. フォームヘッダーを右クリックし、[保存] を選択します。
   [ナレッジ記事の詳細] タブと一連のボタンが表示されます。
4. Runbook の詳細を表示するには、[ナレッジベースの詳細 **(Knowledge Base Details)]** タブをクリックします。
5. ユーザーに表示されるナレッジ記事を表示するには、[記事の表示] をクリックします。
6. 終了 ナレッジ記事の詳細を編集するには、[記事の編集] をクリックします。

ユーザーから報告されたフィッシング攻撃を検証するためのルールの作成

従業員がフィッシング攻撃と思われるメールを受信した場合、フィッシングメールアドレスを使用して報告を受けることができます。不審なメールは、組織で定義されたルールを使用して検証されます。

始める前に

メール一致ルールを使用して潜在的なフィッシング攻撃を特定する前に、従業員から転送されるメールを処理するための送信先メールアドレスを定義します。このメールアドレスを定義する場合には、次のオプションがあります (会社のメールドメインが acme.com である場合)。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- **acme+phishing@service-now.com** などのメールアドレスを定義します。**+phishing** タグは、フィルタリングを有効にするよう SMTP でサポートされており、インスタンスはそこに送信されたメールを受信できます。
- **phishing@acme.com** (Exchange メールボックス) などのメールアドレスを定義し、このアドレスから **acme+phishing@service-now.com** (メール転送ルールによって定義されたインスタンスメールボックス) に転送されるようにします。

必要なロール：sn_sec_cmn.write

このタスクについて
従業員が不審なメールを見つけた場合は、それを添付ファイルとしてフィッシングメールアドレスに転送する必要があります。添付されたメールが脅威を定義するルールに一致する場合、セキュリティインシデントが作成されます。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > メール処理 > ユーザーから報告されたフィッシング.
2. [**New**] をクリックします。
3. 必要に応じて、フィールドに入力します。

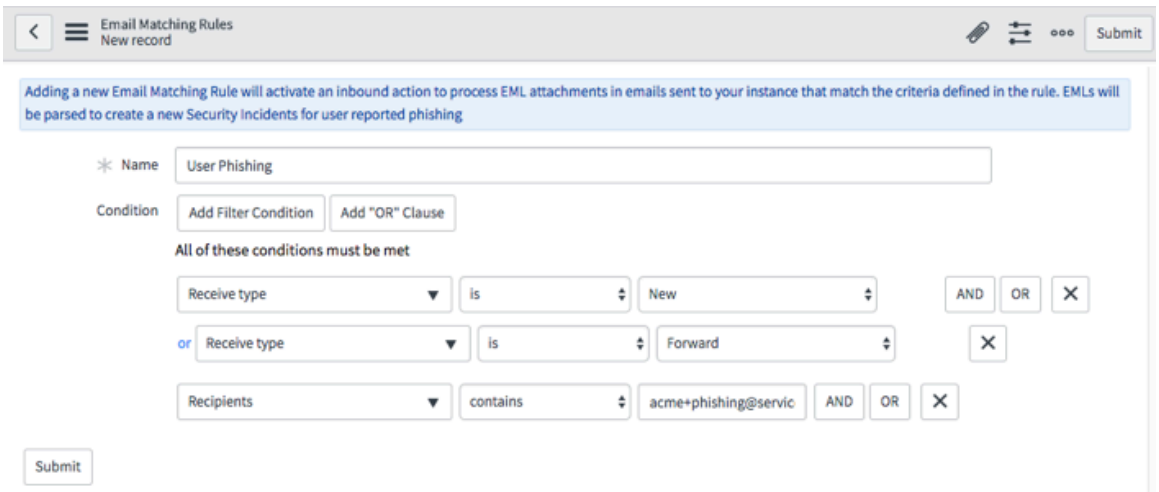
メール一致ルールフォーム

フィールド	説明
名前	このメール一致ルールの名前。たとえば、「ユーザーから報告されたフィッシング」などです。
条件	次を使用： 会社のフィッシングメールアドレスに送信されたメールがフィッシング攻撃かどうかを検証する条件ビルダー。以下の例を参照してください。

4. **[Submit]** をクリックします。

Example:
この例は、ユーザーから報告されたフィッシングを処理するための一致ルールを示しています。

メール一致ルールの例



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティアナリストワークスペース の構成

セキュリティアナリストワークスペースのインシデントレコードのユーザーインターフェイスを構成して、表示するフィールドを指定します。

始める前に

必要なロール：sn_si.analyst

このタスクについて

インシデントレコードに表示するフィールドと、[セキュリティインシデント] フォームおよび [応答タスク] フォームにフィールドを表示する順番を指定します。表示するフィールドの数に制限を設定することもできます。

注:
特定のフォームに使用するビューを決定するルールを作成できます。[デフォルト] および [SIR 新規 UI (SIR New UI)] ビューを含むいくつかのビューがベースシステムに含まれています。[その他すべて] 応答タスクルールを含むいくつかのビュールールもベースシステムに付属しています。このルールは、ビュールールに指定された条件が満たされたときに、[応答タスク] フォームにデフォルトビューを適用します。セキュリティアナリストワークスペースは [SIR 新規 UI (SIR New UI)] ビューを使用します。セキュリティアナリストワークスペースに表示されるフォームフィールドがクラシック環境のフォームフィールドと一致しない場合、多くの場合、ビュールールが適用されます。フォームに **[SIR 新規 UI (SIR New UI)]** ビューを使用するには、ビュールールを無効にする必要があります。詳細については、「Control when the system displays a view (システムがビューを表示するタイミングの制御)」を参照してください。

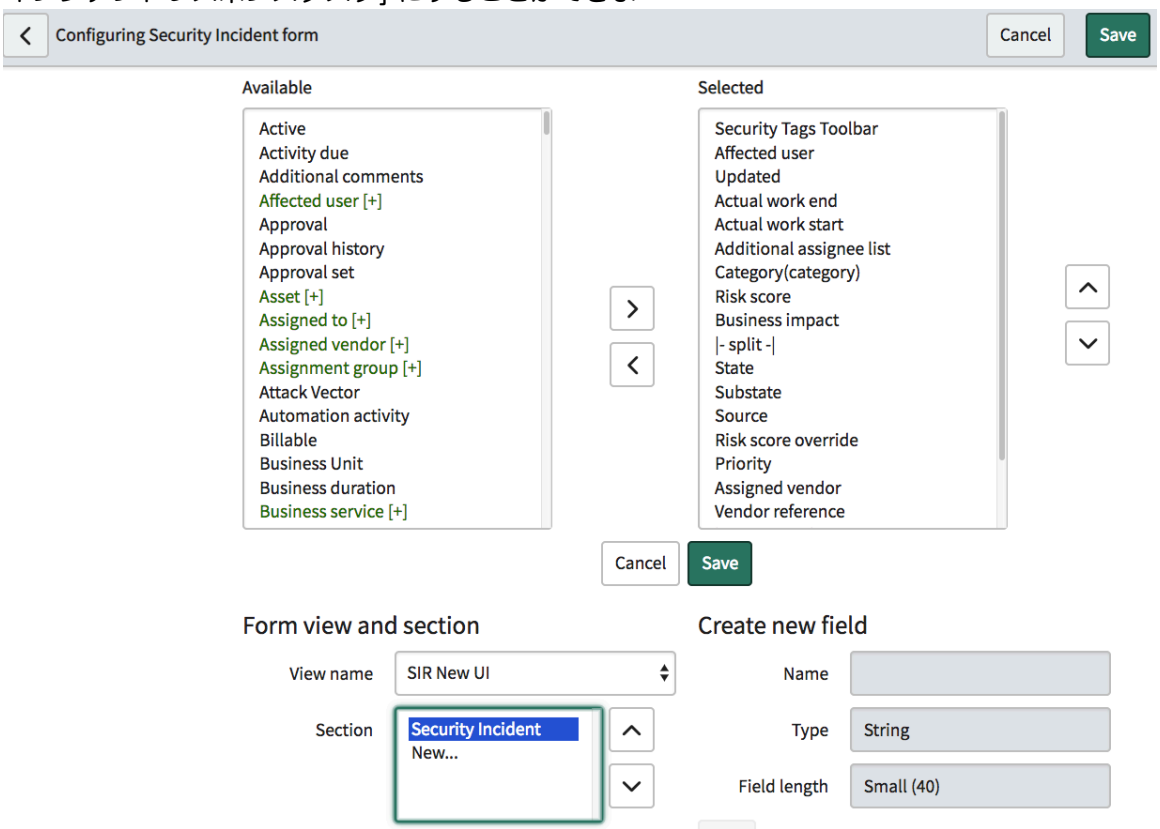
手順

1. 任意のセキュリティインシデントリスト (例: **All** (すべて) > セキュリティインシデント > インシデント > すべてのインシデントを表示) を開きます。
2. セキュリティインシデントレコードを開くには、セキュリティインシデントのリンクをクリックします。
3. [セキュリティインシデントの設定] フォームページに移動するには、 メニューアイコンをクリックして、 構成 > フォームレイアウト.
4. [ビュー名] リストから **[SIR 新規 UI (SIR New UI)]** を選択します。
5. [セクション] フィールドで、適切なセクションを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

これは、[セキュリティインシデント] または [セキュリティインシデントレスポンスタスク] にすることができます。



6. 新規 UI のインシデントバナーに表示するフィールドとその順番を選択します。
7. [保存] をクリックします。

   注:

   - 特定のフィールドは、インシデントおよび応答タスクバナーでデフォルトで非表示になっています。「セキュリティアナリストワークスペースのプロパティ」で説明されているように、sn_app_secops_ui.form.excluded_fields.incident および sn_app_secops_ui.form.excluded_fields.response_task プロパティを変更することで、表示/非表示にするフィールドを変更できます。
   - 次のプロパティを設定して、インシデントおよび応答タスクバナーとインシデントバナーの最初の行に表示できるフィールドの数を指定します。
     - sn_app_secops_ui.task_summary.single_summary.limit.incident
     - sn_app_secops_ui.task_summary.single_summary.limit.response_task
     - sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line

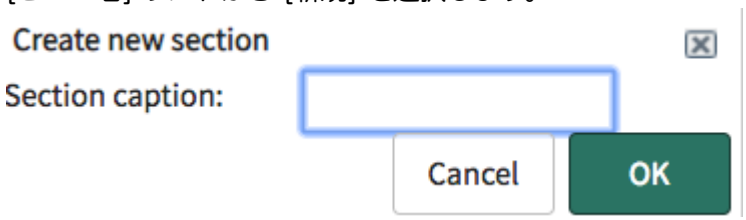
8. インシデントレコードのフィールド値の横に表示される点線の円のスタイル (など) を設定するには、 システム **UI** > フィールドスタイル をクリックし、特定のテーブルとフィールド名のスタイルレコードを変更または新規作成します。
   スタイルレコードの [スタイル] フィールドのプロパティ background-color によって、ドットサークル色が決まります。
9. 更新されたインシデントバナーを表示するには、次をクリックします セキュリティインシデント > インシデント (新規 **UI)** をクリックして セキュリティアナリストワークスペース 内のインシデントレコードに移動し、ページを更新して更新されたインシデントバナーを表示します。
10. インシデントレコードで応答タスクバナーを設定するには、 セキュリティインシデント > 対応タスク > すべてのタスクを表示 をクリックし、手順を繰り返します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

11. ベースの [セキュリティインシデントレスポンスタスク] テーブルを拡張して新しいタスクテーブルを作成する場合は、[SIR 新規 UI (SIR New UI)] ビューもテーブルに追加する必要があります。

    a. [ビュー名] リストから [新規] を選択します。



    b. [新規ビューの作成] ウィンドウに「**SIR New UI**」と入力し (大文字と小文字は区別されます)、**[OK]** をクリックします。

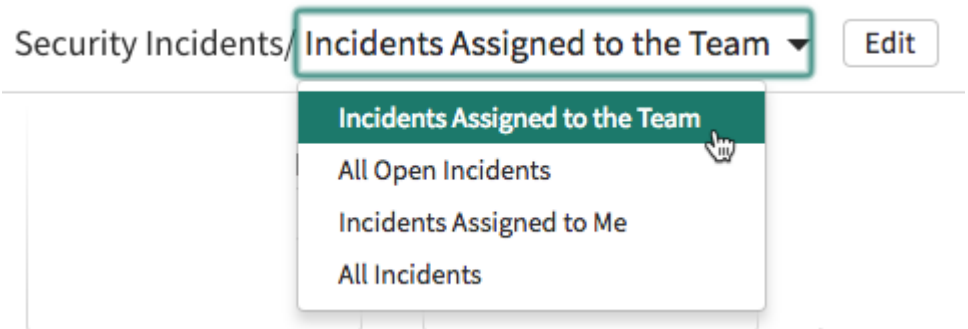
タスクの結果
セキュリティインシデントと応答タスクのバナーが セキュリティアナリストワークスペース で更新されます (「セキュリティアナリストワークスペース を使用したセキュリティ上の脅威の管理」)。

セキュリティアナリストワークスペースのプライマリフィルターとセカンダリフィルターの設定

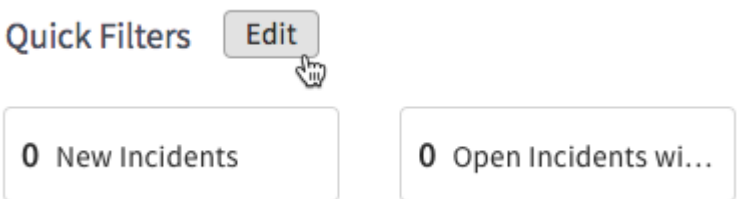
セキュリティアナリストワークスペースベースシステムには、分析するセキュリティインシデントのリストを絞り込むための一連のプライマリフィルター (自分に割り当てられたセキュリティインシデント用、すべてのオープンインシデント用など) と、(新規インシデント、オープンインシデント、重大なインシデントのみなどで) リストをさらに絞り込むための一連のクイック (セカンダリ) フィルターが含まれています。

始める前に
クラシック環境を使用して、追加のプライマリフィルターとセカンダリフィルターを定義できます。

セキュリティアナリストワークスペースで使用するフィルターを定義するときに、そのフィルターをプライマリまたはセカンダリフィルターとして使用できるかどうかを示すタグを割り当てることができます。プライマリフィルターは、セキュリティインシデントリストの一番上に表示されます。



[クイックフィルター] オプションの横にある [編集] をクリックして、セカンダリ (クイック) フィルターを選択します。



必要なロール：admin または sn_sec_cmn.write

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

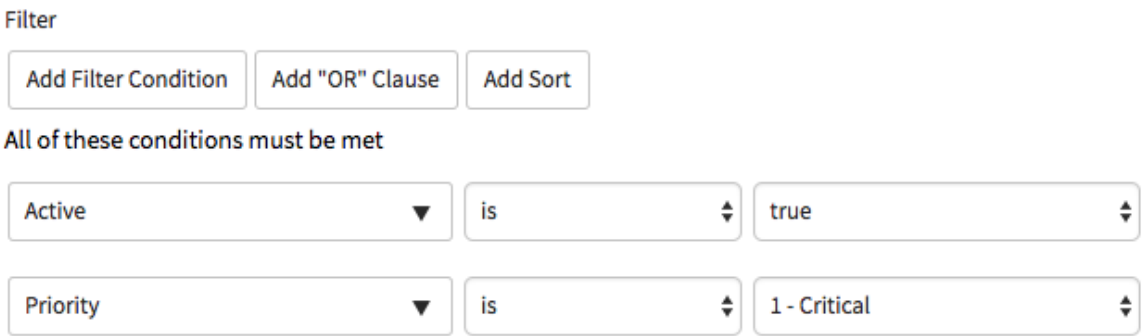
手順

1. 次のように移動する。 **All** (すべて) > システム定義 > フィルター.
2. [新規] をクリックして、次の手順を実行します。

   a. [タイトル] を入力します。

   b. [テーブル] 選択リストから [セキュリティインシデント **[sn_si_incident]]** を選択します。

   c. フィルター条件を追加します。
   たとえば、[優先度が [最重要] のオープンインシデント] フィルターでは、次の条件を使用します。



   d. **[Submit]** をクリックします。

3. フィルターリストに [タグ] 列が表示されていない場合は、歯車アイコンをクリックし、ビューをカスタマイズして追加します。
4. 作成したフィルターを見つけ、セキュリティアナリストワークスペースにフィルターを表示する方法を示す次のいずれかのタグを追加します。
   - **SN_SI_Primary**：このタグを選択した場合、セキュリティアナリストワークスペースのプライマリフィルタースラッシュバケットからフィルターを選択できます。
   - **SN_SI_Primary_OOB**：このタグを選択した場合、フィルターはデフォルトで、プライマリフィルタースラッシュバケットの [選択済み] 側に表示されます。
   - **SN_SI_Secondary**：このタグを選択した場合、フィルターは、セカンダリ (クイック) フィルタースラッシュバケットから選択できます。
   - **SN_SI_Secondary_OOB**：このタグを選択した場合、フィルターはデフォルトで、プライマリフィルタースラッシュバケットの [選択済み] 側に表示されます。

関連情報

フィルターの作成と編集

セキュリティアナリストワークスペースのプロパティ

次のシステムプロパティは、セキュリティアナリストワークスペースの構成に使用されます。

次の 2 つのタイプのプロパティがあります。

- sys_id や製品キーなど、通常は変更されないプロパティ。
- 長いポーリング間隔やユーザーインターフェイス構成など、必要に応じて変更されるプロパティ。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
セキュリティアナリストワークスペースのプロパティは、次の場所にあります。 セキュリティインシデント > アナリストワークスペースのセットアップ > アナリストワークスペースのプロパティ.

セキュリティアナリストワークスペースのプロパティ

プロパティ名	説明
対応タスクバナーでデフォルトで非表示になっているフィールド。 sn_app_secops_ui.form.excluded_fields.response_task	• タイプ：文字列 • デフォルト値： ◦ number ◦ short description ◦ comments ◦ work_notes ◦ comments_and_work_notes ◦ work_notes_list ◦ automation_activity
インシデントバナーでデフォルトで非表示になっているフィールド。 sn_app_secops_ui.form.excluded_fields.incident	• タイプ：文字列 • デフォルト値： ◦ number ◦ short description ◦ comments ◦ work_notes ◦ comments_and_work_notes ◦ work_notes_list ◦ automation_activity ◦ security_tags
背景色スタイルは、ここにリストされているフィールドに適用されます。 sn_app_secops_ui.form.color_coded_fields	• タイプ：文字列 • デフォルト値： ◦ business criticality ◦ impact ◦ priority ◦ risk_score ◦ severity

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティアナリストワークスペースのプロパティ (続く)

プロパティ名	説明
true である場合、sn_si_task ベース対応タスクテーブルから拡張されたテーブルも、ベース対応タスクテーブル用に作成されたメールテンプレートにアクセスできるようになります。 sn_app_secops_ui.extend.base.response_task.email_templates	• タイプ：true | false • デフォルト値：true
各対応タスクバナーの各サマリフィールドの幅を設定します。 sn_app_secops_ui.task_summary.single_summary.width.response_task	• タイプ：整数 • デフォルト値：10
各インシデントバナーの各サマリフィールドの幅を設定します。 sn_app_secops_ui.task_summary.single_summary.width.incident	• タイプ：整数 • デフォルト値：15
インシデントバナーで許可されるサマリフィールド数の制限を設定します。 sn_app_secops_ui.task_summary.single_summary.limit.incident	• タイプ：整数 • デフォルト値：12
対応タスクバナーで許可されるサマリフィールド数の制限を設定します。 sn_app_secops_ui.task_summary.single_summary.limit.response_task	• タイプ：整数 • デフォルト値：12
インシデントバナーの最初の行で許可されるサマリフィールド数の制限を設定します。 sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line	• タイプ：整数 • デフォルト値：3

ユーザーの写真を含めることができるフィールドのカンマ区切りリスト。
 	
sn_app_secops_ui.form.user_fields
	• タイプ：文字列
	• デフォルト値：
	  ○ affected_user
	  ○ caller
	  ○ sys_updated_by
	  ○ sys_created_by
	  ○ opened_by
	  ○ closed_by
	  ○ submitted_by

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティアナリストワークスペースのプロパティ (続く)

プロパティ名	説明
各インシデントピークビューの各サマリフィールドの幅を設定します。 sn_app_secops_ui.task_summary.single_summary.width.incident_peek	• タイプ：整数 • デフォルト値：13.5
時間を表示するフィールドのカンマ区切りリスト。 sn_app_secops_ui.form.time_fields	• タイプ：文字列 • デフォルト値： ○ open_at ○ sys_created_on ○ sys_updated_on
サイティング検索結果が更新される頻度 (ミリ秒) を制御します。 sn_app_secops_ui.poller_interval.search_action	• タイプ：整数 • デフォルト値：30000 最小：15000
カウントまたはクエリデータが更新される頻度 (ミリ秒) を制御します。 sn_app_secops_ui.poller_interval.related_list	• タイプ：整数 • デフォルト値：30000 最小：15000
(Playbook の) 結果データが更新される頻度 (ミリ秒) を制御します。 sn_app_secops_ui.poller_interval.playbook_tasks	• タイプ：整数 • デフォルト値：30000 最小：15000
Security Operations Integration の ID - ホストワークフローを隔離。 sn_app_secops_ui.workflow.id.isolate_host	• タイプ：文字列 • デフォルト値： d72041f1ff203200c68c84648e94fa5e
Security Operations Integration の ID - ウォッチリストワークフロー。 sn_app_secops_ui.workflow.id.publish_to_watchlist	• タイプ：文字列 • デフォルト値： 35800c0eff343200c68c84648e94fa85
Security Operations Integration の ID - ブロック要求ワークフロー。 sn_app_secops_ui.workflow.id.block_request	• タイプ：文字列 • デフォルト値： 11a6a5270b9032008f9108e3c5673a24

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティアナリストワークスペースのプロパティ (続く)

プロパティ名	説明
sn_si_analyst ユーザーロールの ID。 sn_app_secops_ui.roles.id.sn_si.write	• タイプ：文字列 • デフォルト値：66878663ff123100158bfffffffff8d
sn_si_read ユーザーロールの ID。 sn_app_secops_ui.roles.id.sn_si.read	• タイプ：文字列 • デフォルト値：ae878663ff123100158bfffffffff8e
sn_si_admin ユーザーロールの ID。 sn_app_secops_ui.roles.id.sn_si.admin	• タイプ：文字列 • デフォルト値：22878663ff123100158bfffffffff8d
Microsoft Exchange の ID - メールの検索と削除ワークフローの実行。 sn_app_secops_ui.email.phishing.manual.workflow	• タイプ：文字列 • デフォルト値：ed9f289cc310220031fbdccdf3d3aeb4
セキュリティアナリストワークスペースの [探索] タブにある [拒否リストに追加 (Add to Deny list)] カスタムアクションの ID。 sn_app_secops_ui.explore.action.direct.id.deny_list	• タイプ：文字列 • デフォルト値：DENY_e9bd0ac50b632200263a089b37673a0b
セキュリティアナリストワークスペースの [探索] タブにある [許可リストに追加 (Add to Allow list)] カスタムアクションの ID。 sn_app_secops_ui.explore.action.direct.id.allow_list	• タイプ：文字列 • デフォルト値：ALLOWLIST_e9bd0ac50b632200263a089b37673a0b
[脅威のルックアップを実行] UI アクションの ID。 sn_app_secops_ui.explore.action.id.run_threat_lookup	• タイプ：文字列 • デフォルト値：da5ff4420b540300263a089b37673ae7
[脅威のルックアップ] 統合機能の ID。 sn_app_secops_ui.explore.capability.id.threat_lookup	• タイプ：文字列 • デフォルト値：39344d4f0b273200263a089b37673ab1
セキュリティアナリストワークスペースの [探索] タブにある [観測事象の拡張] カスタムアクションの ID。	• タイプ：文字列 • デフォルト値：OBS_ENRICHMENT_54e2f5d60b5003009f66e94685673

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティアナリストワークスペースのプロパティ (続く)

プロパティ名	説明
sn_app_secops_ui.explore.action.id.observable_enrichment	
[観測事象を拡張] 統合機能の ID。 sn_app_secops_ui.explore.capability.id.observable_enrichment	• タイプ：文字列 • デフォルト値：9ad183640b1003009f66e94685673af4
[ウォッチリストに公開] UI アクションの ID。 sn_app_secops_ui.explore.action.id.publish_to_watchlist	• タイプ：文字列 • デフォルト値：8ee94002ff743200c68c84648e94faf9
[ブロック要求] UI アクションの ID。 sn_app_secops_ui.explore.action.id.block_request	• タイプ：文字列 • デフォルト値：7158f6e40b2032008f9108e3c5673adf
[サイティング検索を実行] UI アクションの ID。 sn_app_secops_ui.explore.action.id.sightings_search	• タイプ：文字列 • デフォルト値：43f91a6f0b032200b97c67d985673a2c
[子のセキュリティインシデントの作成] UI アクションの ID。 sn_app_secops_ui.explore.action.id.create_child_incident	• タイプ：文字列 • デフォルト値：5a6882645363530099d5ddeeff7b1272
[セキュリティ注釈を追加] UI アクションの ID。 sn_app_secops_ui.explore.action.id.add_security_annotation	• タイプ：文字列 • デフォルト値：1e3a3e723b5332005a9149a4d2efc4eb
セキュリティアナリストワークスペースの [探索] タブにある [CI 拡張] カスタムアクションの ID。 sn_app_secops_ui.explore.action.id.ci_enrichment	• タイプ：文字列 • デフォルト値：CI_ENRICHMENT_54e2f5d60b5003009f66e94685673a1
[ホストを隔離] UI アクションの ID。 sn_app_secops_ui.explore.action.id.isolate_host	• タイプ：文字列 • デフォルト値：d6244e0aff203200c68c84648e94fad3

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティアナリストワークスペースのプロパティ (続く)

プロパティ名	説明
[複数の観測事象を追加] UI アクションの ID。 sn_app_secops_ui.explore.action.id.multiple_observable	• タイプ：文字列 • デフォルト値： 138de478d78322007a6de294de6103aa
ag-Grid-Enterprise の製品キー。 sn_app_secops_ui.ag-grid-license	• タイプ：文字列 • デフォルト値： ServiceNow_ServiceNow_5Devs2_August_2018__MTUzM

追加のセキュリティアナリストワークスペースの構成

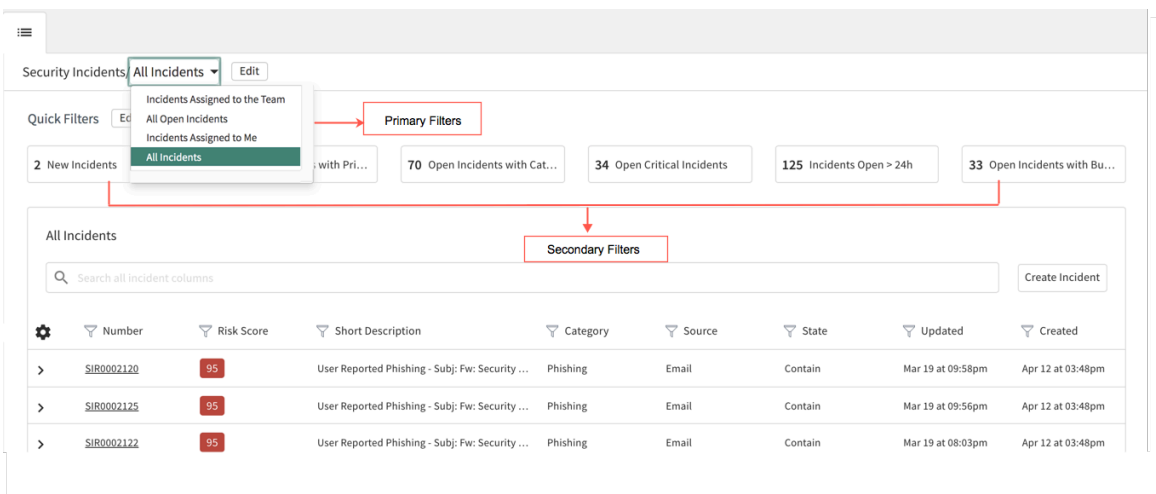
セキュリティアナリストワークスペース を構成し、フィルター、UI アクション、および関連リストを定義します。

- ランディングページのフィルター構成
- 有効な UI アクション
- フォーム UI アクション
- 関連リストの構成
- 関連リスト UI アクション
- フォーム構成システムプロパティ
- アナリスト向け Playbook の有効化

ランディングページのフィルター構成

セキュリティアナリストワークスペース に表示される新しいフィルターを追加したり、既存のフィルターを変更したりすることができます。

セキュリティアナリストワークスペース にはセキュリティインシデントのリストをフィルタリングするためのプライマリフィルターとセカンダリフィルターが用意されているため、分析するセキュリティインシデントをすばやく見つけることができます。詳細については、「セキュリティアナリストワークスペース を使用したセキュリティ上の脅威の管理」を参照してください。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィルターの新規作成

1. 次のように移動する。 セキュリティインシデント > アナリストワークスペースセットアップ (新規 **UI)** > ランディングページのフィルター構成.
2. [**New**] をクリックします。
3. フィルターのタイトルを入力し、フィルター条件を指定して、[送信] をクリックして前のページに戻ります。

   新しく追加されたフィルターがページに表示されます。
4. このフィルターに対し、これがプライマリフィルターかセカンダリフィルターかを示すタグを追加します。次のタグを使用できます。
   - SN_SI_Primary
   - SN_SI_Secondary

既存のフィルターの編集

次の操作も実行できます。

- 既存のフィルターを変更する：既存のフィルターのタイトルをクリックします。タイトルとフィルター条件を変更し、[更新] をクリックします。
- タグを変更する：フィルターを選択し、ランディングページのフィルター構成の [タグ] 列をクリックします。既存のタグを削除するか、フィルターに新しいタグを追加することができます。

有効な **UI** アクション

UI アクションを構成するには、UI アクションを セキュリティアナリストワークスペース で構成できるように事前に特定のステップを実行して有効化する必要があります。

> **注:**
> UI アクションを変更するには、次のロールを持つユーザーとしてログインします。
> - ui_action_admin
> - ui_page_admin
> - web_service_admin

セキュリティアナリストワークスペース に構成できる UI アクションには 2 つのタイプがあります。

- ダイアログベースの UI アクション
- サーバー側 UI アクション

ダイアログベースの **UI** アクション

セキュリティアナリストワークスペース でダイアログベースの UI アクションを有効化するには、それぞれの標準 UI アクションに関連付けられた UI ページに次の変更を加えます。

1. **HTML** セクション：HTML セクションを変更して、*react* 入力タグを含めます。*react* 入力タグ値は、UI ページが セキュリティアナリストワークスペース から起動されたかどうかを識別するためにクライアントスクリプトセクションで使用されます。例を次に示します。

```
<input id="react" name="react" type="hidden"
value="${JS,HTML:sysparm_react}" />
```

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

2. クライアントスクリプト：*react* フラグが true の場合、クライアントスクリプトに追加のロジックを記述する必要があります。これは、ダイアログウィンドウの一部として表示される [送信] および [キャンセル] ボタンのイベントを処理するために必要です。
   a. onCancel () イベントハンドラーは、セキュリティアナリストワークスペース から「SIR_WORKBENCH_POPUP_CANCEL」イベントをディスパッチする必要があります。
   b. onSubmit () イベントハンドラーは、セキュリティアナリストワークスペース から「SIR_WORKBENCH_POPUP_SUBMIT」イベントをディスパッチする必要があります。
3. *react* 入力タグの値が true のときは false を返すように「onSubmit」アクションを変更したため、処理スクリプトの実行は セキュリティアナリストワークスペース のコンテキストからスキップされます。処理スクリプトのロジックは、(GlideAjax API を介して呼び出される) クライアント呼び出し可能スクリプトまたは REST リソースエンドポイントのいずれかを介して処理する必要があります。

詳細については、次のサンプルの UI ページを参照してください。

- 関連リストの UI アクションの例：ウォッチリストに公開 (UI ページ名：publish_to_watchlist)
- フォームの UI アクションの例：問題の作成 (UI ページ名：create_prb_change_inc)

サーバー側 **UI** アクション

サーバー側 UI アクションを有効化するには、次の操作を行う必要があります。

標準 UI アクションスクリプトのロジックは、スクリプト化された REST リソースの一部として処理する必要があります。

詳細については、次のサンプルフォームの UI アクションを参照してください。

- 機能停止の作成
- キャンセル

フォーム **UI** アクション

セキュリティアナリストワークスペース に表示される UI アクションを構成できます。

必須条件：

UI アクションを構成するには、UI アクションを セキュリティアナリストワークスペース で構成できるように事前に特定のステップを実行して有効化する必要があります。詳細については、「有効な UI アクション」を参照してください。

セキュリティアナリストワークスペース のフォームの UI アクションを構成するには、次のステップを実行します。

1. 次のように移動する。 セキュリティインシデント > アナリストワークスペースセットアップ (新規 **UI)** > フォーム **UI** アクション.
2. 以下の詳細を入力します。

フィールド名	説明
アクション	選択リストから UI アクションを選択します。
タイプ	アクションのタイプを選択します。次のいずれかを選択できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド名	説明
	○ ダイアログベースのアクション：このタイプのアクションは、特定のビジネスロジックを実行するためにユーザーインタラクションまたは入力が必要な場合に使用します。 ○ サーバー側のアクション：このアクションは、追加のユーザー入力なしで必要なビジネスロジックを実行します。 **注:** UI アクションを構成するには、UI アクションを セキュリティアナリストワークスペース で構成できるように事前に特定のステップを実行して有効化する必要があります。詳細については、「有効な UI アクション」を参照してください。
アプリケーション	UI アクションが追加されるアプリケーションスコープの名前 (セキュリティインシデントレスポンス UI) がここに表示されます。
ダイアログベースのアクション [タイプ] フィールドで [ダイアログベースのアクション] を選択した場合は、次の詳細を入力します。	
UI ページ	アクションに関連付けられた UI ページを選択します。
ダイアログタイトル	ダイアログアクションのタイトルを入力します。
ダイアログの幅と高さ (Dialog Width and Height)	ダイアログの高さと幅をピクセル単位で入力します。
スクリプト	選択した UI ページについて、ここで追加のクエリパラメーターを指定できます。ベースシステムで提供されるテンプレートでは、sysparm_sys_id パラメーターのみが構成され、返されます。ここで別のパラメーターを指定することで、これを上書きできます。
サーバー側のアクション [タイプ] フィールドで [サーバー側のアクション] を選択した場合は、次の詳細を入力します。	
スクリプト化済み REST リソース	アクションを定義するスクリプト化済みの REST リソースを選択します。 **注:** **SIR UI ANALYST** ACL を REST リソースに追加する必要があります。

3. [**Submit** (送信)] を選択します。
4. 次のように移動する。 セキュリティインシデント > インシデント (新規 **UI)** ページ
5. セキュリティインシデントレコードを表示するには、セキュリティインシデント番号をクリックします。ページの上部に新しい UI アクションが表示されます。

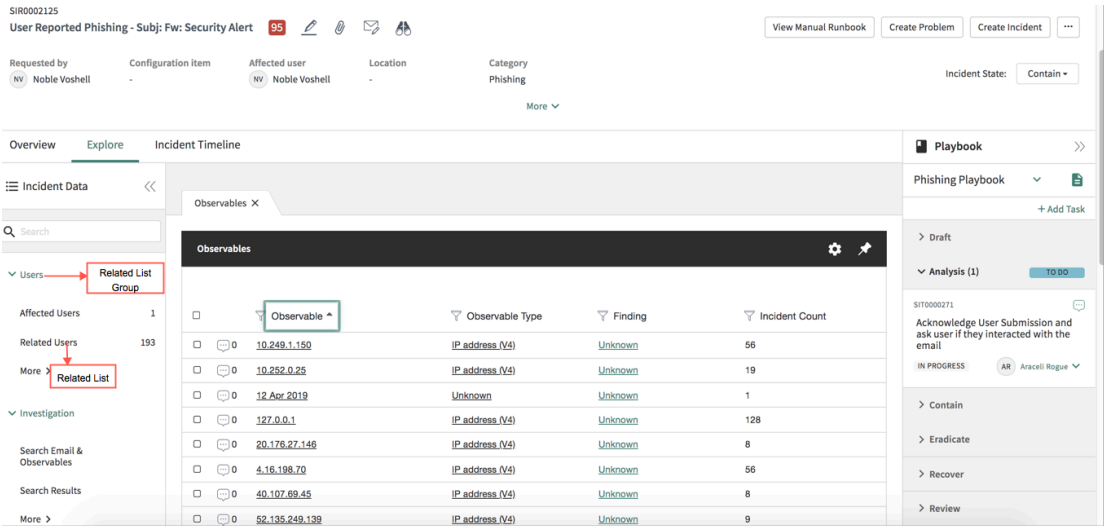
既存のフォーム UI アクションを変更するには、アクション名をクリックして [フォーム UI アクション] ページに移動します。選択したタイプに基づいて、[アクション名]、[タイプ]、および残りのフィールドを変更できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

関連リストの構成

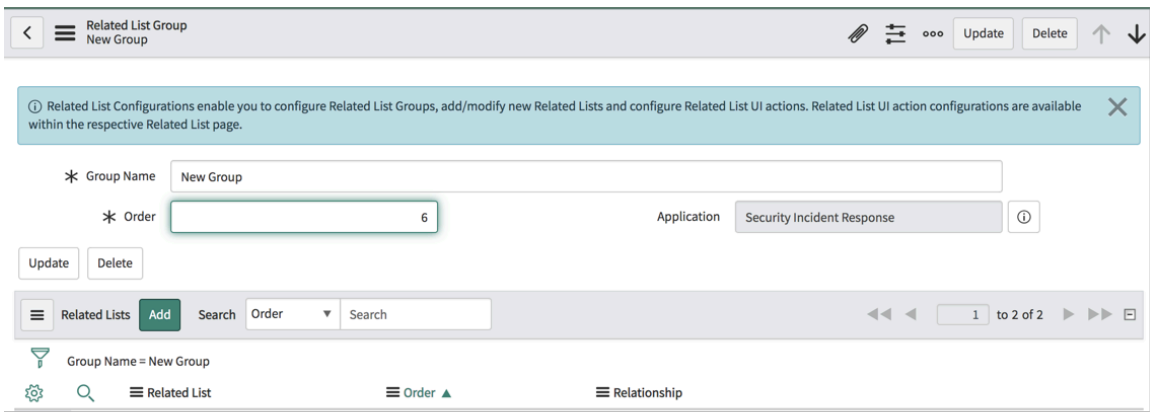
新しい関連リストまたは新しい関連リストグループを追加し、セキュリティアナリストワークスペース に表示される既存のグループまたは関連リストを変更できます。



関連リストグループの追加

関連リストグループを追加するには、次のステップを実行します。

1. 次のように移動する。 セキュリティインシデント > アナリストワークスペースセットアップ (新規 **UI)** > 関連リストの構成.
2. [新規] をクリックして、新しい関連リストグループを追加します。[インシデント (新規 UI)] ページに表示するグループ名とその順番を入力します。
3. **[Submit]** をクリックします。新しく追加されたグループが [関連リストグループ] ページに表示されます。



関連リストの追加

新しい関連リストを追加するには、次のステップを実行します。

1. [関連リストグループ] リンクをクリックします。
2. [関連リスト] セクションで、[追加] をクリックして新しい関連リストを追加します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[追加] ボタンが表示されない場合は、関連リストグループと同じアプリケーションスコープに設定されているかどうかを確認してください。

3. グループに含める関連リストを選択します。

   注:
   特定の関連リストが表示されない場合は、次の操作を実行します。

   a. 次のように移動する。 システム **UI** > 関連リスト をクリックし、 *sn_si_incident* テーブルに存在する関連リストを検索します。

   b. **[SIR** 新規 **UI]** ビューに関連付けられている *sn_si_incident* テーブルをクリックします。

   c. [関連リストエントリー] セクションで、[新規] をクリックして、**[SIR** 新規 **UI]** ビューに関連リストを追加します。

4. 表示する順序を指定し、[送信] をクリックします。

   追加した関連リストが セキュリティアナリストワークスペース に表示されます。

既存の関連リストグループを変更するには、グループ名をクリックして [関連リストグループ] ページに移動します。グループ名と順序を変更したり、グループの関連リストを追加または削除したりできます。

関連リスト **UI** アクション

セキュリティアナリストワークスペースに表示される関連リストに新しい UI アクションを追加できます。

必須条件：

UI アクションを構成するには、UI アクションを セキュリティアナリストワークスペース で構成できるように事前に特定のステップを実行して有効化する必要があります。詳細については、「有効な UI アクション」を参照してください。

新しい関連リスト UI アクションを追加するには、次のステップを実行します。

1. 次のように移動する。 セキュリティインシデント > アナリストワークスペースセットアップ (新規 **UI)** > 関連リストの構成.
2. グループ名をクリックします。[関連リストグループ] 設定ページが表示されます。
3. UI アクションを追加する関連リストをクリックします。
4. [関連リスト UI アクション] セクションで [追加] をクリックします。
5. 以下の詳細を入力します。

フィールド名	説明
アクション	選択リストから UI アクションを選択します。
タイプ	アクションのタイプを選択します。次のいずれかを選択できます。 ○ ダイアログベースのアクション：このタイプのアクションは、特定のビジネスロジックを実行するためにユーザーインタラクションまたは入力が必要な場合に使用します。 ○ サーバー側のアクション：このアクションは、追加のユーザー入力なしで必要なビジネスロジックを実行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド名	説明
	注: UI アクションを構成するには、UI アクションを セキュリティアナリストワークスペース で構成できるように事前に特定のステップを実行して有効化する必要があります。詳細については、「有効な UI アクション」を参照してください。
アプリケーション	UI アクションが追加されるアプリケーションスコープの名前 (セキュリティインシデントレスポンス UI) がここに表示されます。
ダイアログベースのアクション [タイプ] フィールドで [ダイアログベースのアクション] を選択した場合は、次の詳細を入力します。	
UI ページ	アクションに関連付けられた UI ページを選択します。
ダイアログタイトル	ダイアログアクションのタイトルを入力します。
ダイアログの幅と高さ (Dialog Width and Height)	ダイアログの高さと幅をピクセル単位で入力します。
スクリプト	選択した UI ページについて、ここで追加のクエリパラメーターを指定できます。ベースシステムで提供されるテンプレートでは、sysparm_incident_id、sysparm_record_table、および sysparm_related_sys_ids パラメーターのみが構成され、返されます。ここで別のパラメーターを指定することで、これらを上書きできます。
サーバー側のアクション [タイプ] フィールドで [サーバー側のアクション] を選択した場合は、以下を指定します。	
スクリプト化済み REST リソース	アクションを定義するスクリプト化済みの REST リソースを選択します。 注: **SIR UI ANALYST** ACL を REST リソースに追加する必要があります。

6. [**Submit** (送信)] を選択します。
7. 次のように移動する。 セキュリティインシデント > インシデント (新規 **UI)** ページ
8. セキュリティインシデントレコードを表示するには、セキュリティインシデント番号をクリックします。それぞれの関連リストを起動して、新しい UI アクションを表示します。

フォーム構成システムプロパティ

これらのシステムプロパティは、プレイブックタスクのフォーム更新間隔を定義します。

これらのプロパティを設定するには、次に移動します: アナリストワークスペースセットアップ (新規 **UI)** > アナリストワークスペースのプロパティ.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

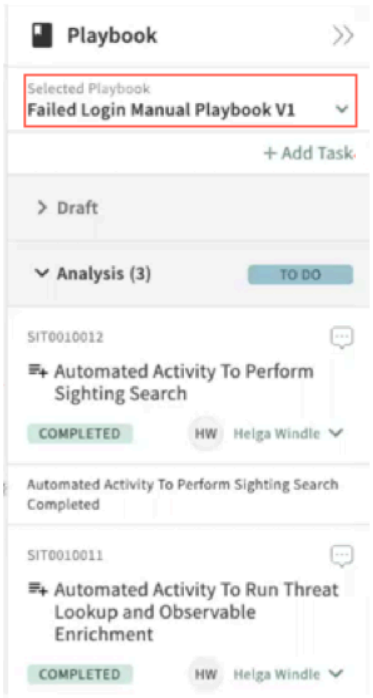
自動翻訳

プロパティ	デフォルト値	説明
sn_app_secops_ui.poller_interval_playbook_tasks	10,000 ミリ秒	すべての構成済みの時間間隔に対して応答タスクを更新するためにプレイブックコンポーネントが使用する時間間隔。
sn_app_secops_ui.poller_interval_count.playbook_tasks	9	プレイブックコンポーネントが応答タスクをポーリングする回数。
sn_app_secops_ui.poller_interval_related_list	30,000 ミリ秒	すべての構成済みの時間間隔に対して プレイブックコンポーネントがその関連リストを更新するために使用する時間間隔。

アナリスト向け **Playbook** の有効化

新しいプレイブックをプレイブック選択リストに追加します。

セキュリティアナリストワークスペース でセキュリティインシデントを調査するための適切なプレイブックを選択できます (「セキュリティアナリストワークスペース を使用したセキュリティ上の脅威の管理」)。プレイブック選択オプションでは、フローデザイナーを使用して設計されたプレイブックのみがサポートされます。



フローデザイナーを使用してプレイブックを作成した後、次のステップに従って [選択されたプレイブック] 選択リストに含めます。

1. *sys_hub_flow* テーブルに移動します。
2. フローデザイナーを使用して作成した新しいプレイブックを検索します。
3. [選択されたプレイブック] 選択リストに含めるプレイブックに **sir_playbook** タグを追加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
ワークフローからフローデザイナーに移行されていない古いプレイブックがある場合、それらはリストに表示されません。ただし、ワークフローを使用して作成されたプレイブックが、トリガー条件または手動選択 (クラシック環境の [オーケストレーションを実行] オプションを使用) のいずれかによってセキュリティインシデントに割り当てられている場合、セキュリティアナリストワークスペースでセキュリティインシデントを開くと、このプレイブックが起動されます。

セキュリティインシデントレスポンスのトラブルシューティング

このセクションでは、セキュリティインシデントレスポンスに関連する重要なトラブルシューティングのヒントとよくある質問について説明します。

アクセス制御ルールの問題

アクセス制御ルールでは、次の 3 つの条件すべてが満たされている場合に、指定されたリソースへのアクセスが許可されます。

- ユーザーが [ロール] リストに指定されたいずれかのロールを持っているか、リストが空である。
- [条件] フィールドの条件が True と評価されているか、条件が空である。
- [スクリプト] フィールド (詳細) のスクリプトが、True と評価されているか、変数 **answer** が True に設定されているか、空である。

アクセス制御ルールの詳細については、「Exploring Access Control Lists」を参照してください。

重要:
セキュリティインシデントテーブルの [アドミン優先] オプションがオフになっており、アドミニストレーターがセキュリティインシデントテーブルにアクセスできる場合は、KB1444673 を参照してください。

セキュリティインシデントレスポンス プラットフォームアナリティクスソリューション

プラットフォームアナリティクスソリューション には事前構成済みのダッシュボードが含まれます。ダッシュボードには、新しいセキュリティインシデントやオープンセキュリティインシデントの平均経過時間など、セキュリティインシデントレスポンス プロセスを分析する上で重要なメトリクスが表示されます。

プラットフォームアナリティクス データの可視化では、 パフォーマンスアナリティクス インジケーター データを使用してデータを経時的に表示し、ビジネスプロセスの分析や改善が必要な領域の特定に役立ちます。プラットフォームアナリティクスソリューション を使用すると、最小限のセットアップで パフォーマンスアナリティクス からアプリケーションに関する値を取得できます。いつでも独自のオブジェクトを作成することもできます。

重要:
本番で有効にする前に、非本番インスタンスで プラットフォームアナリティクスソリューション を設定してテストします。

セキュリティインシデントレスポンス パフォーマンスアナリティクス ソリューションは ServiceNow Storeから入手できます。このアプリケーションのダウンロードとインストールに関する詳細については、「Security Operations and the ServiceNow Store (Security Operations と ServiceNow Store)」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
機能を評価するには、パフォーマンスアナリティクス のライセンスのないインスタンスで パフォーマンスアナリティクス ソリューションおよびフォーム内アナリティクスをアクティブにします。ただし、次の制限があります。

- 新しいインジケーターを作成できない。
- 180 日以上経過した古いデータを収集できない。

完全な機能を利用するには、パフォーマンスアナリティクス のライセンスを取得してください。詳細については、「パフォーマンスアナリティクスサブスクリプションのアクティブ化」を参照してください。

重要:
デフォルトでは、パフォーマンスアナリティクスの `(com.snc.pa.dc.max_records)` プロパティのデータ収集制限は 5,000 レコードに設定されています。ただし、要件に応じてこの制限を増やすことができます (50,000 レコードなど)。ただし、この制限を増やすと、データ収集時や、スナップショットテーブルで操作を実行する際のパフォーマンスに影響する可能性があります。パフォーマンスアナリティクスのプロパティの詳細については、「Performance Analytics properties」を参照してください。

関連情報

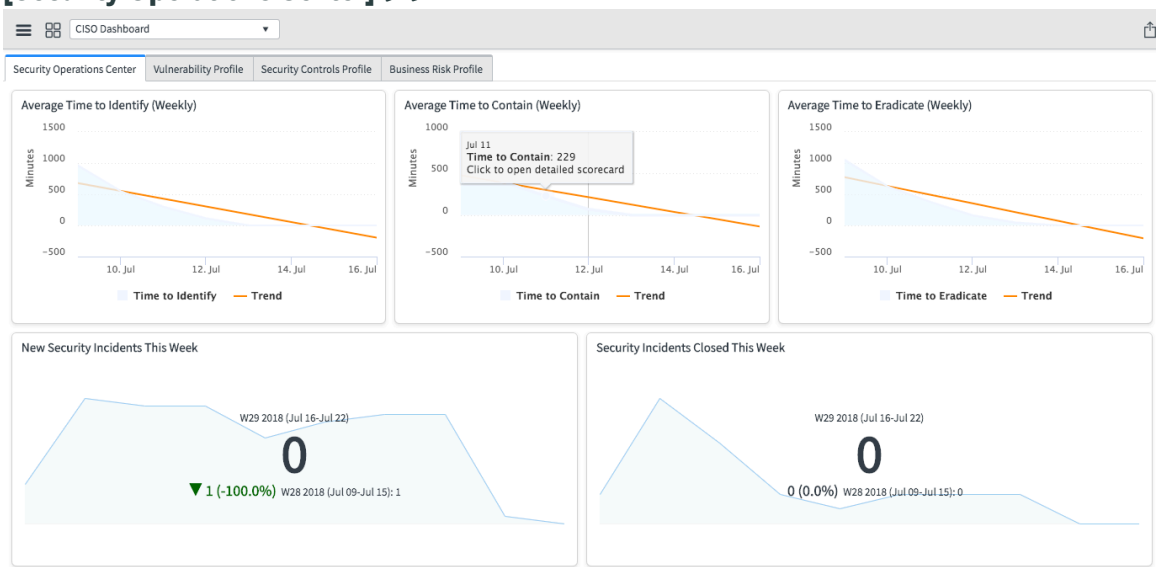
プラットフォームアナリティクスソリューション

パフォーマンスアナリティクスサブスクリプションのアクティブ化

CISO ダッシュボード

このダッシュボードには、セキュリティの脆弱性やインシデントを含む、組織の全体的なセキュリティ体制が表示されます。

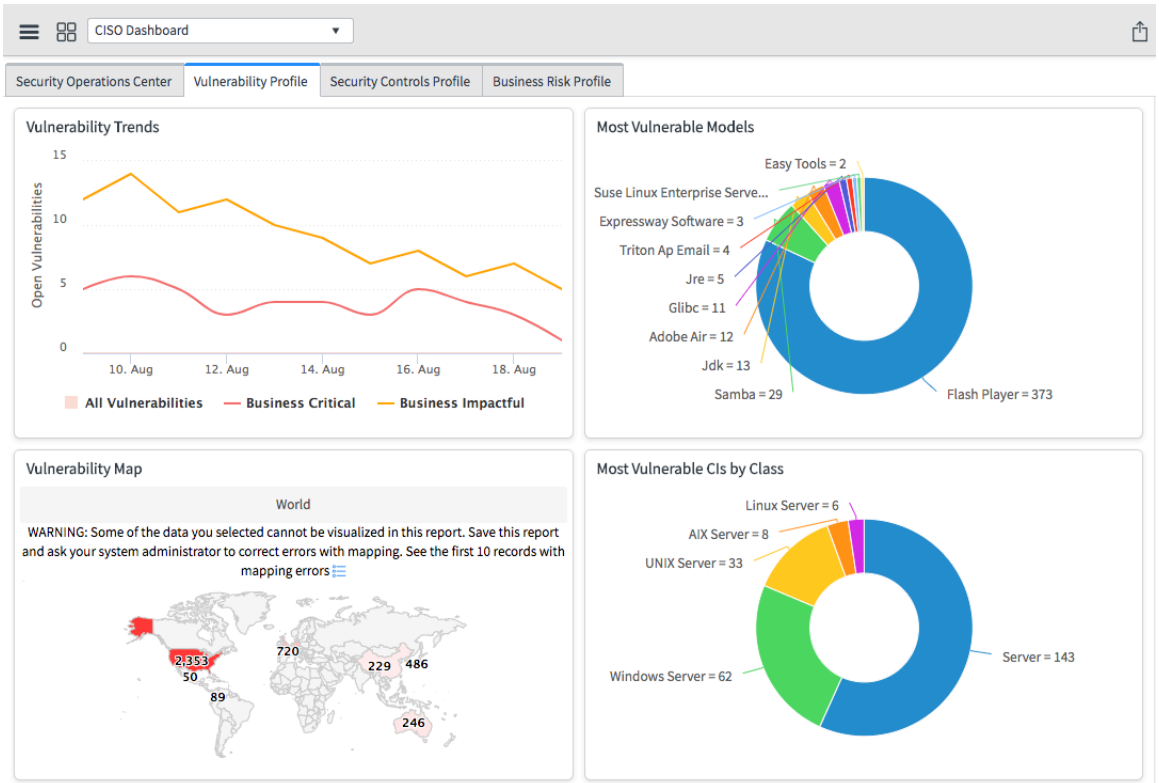
[Security Operations Center] タブ



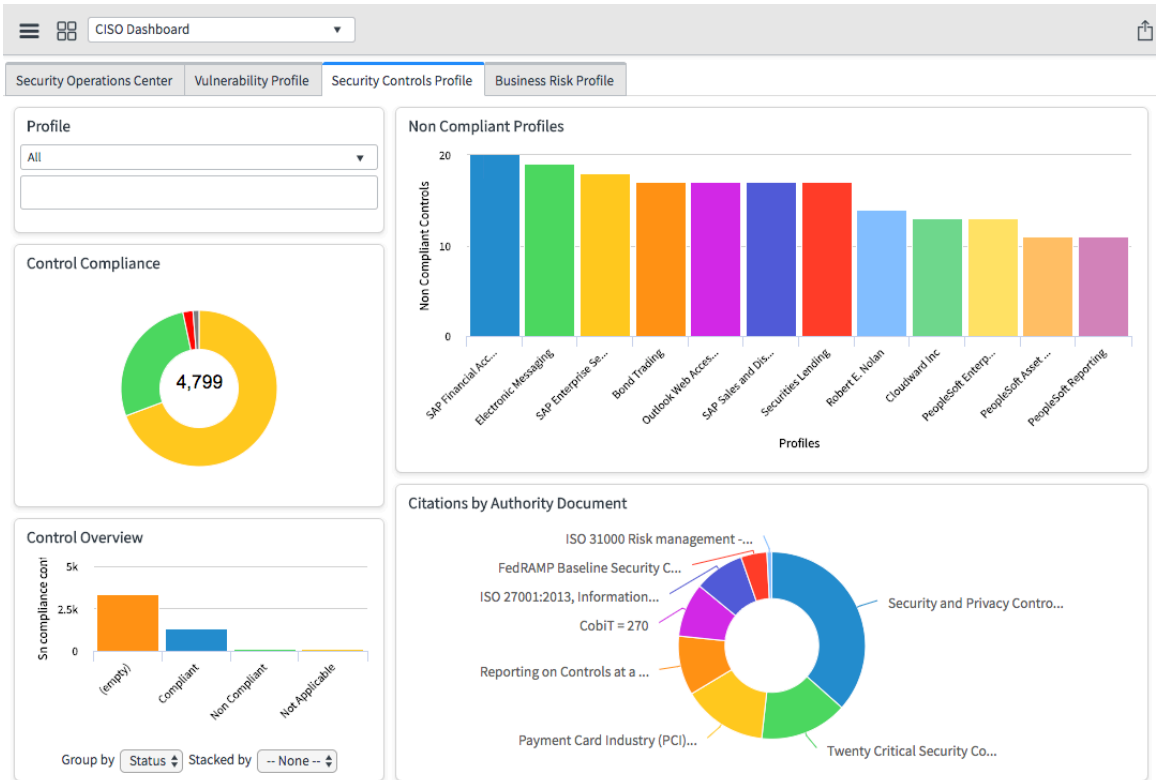
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[脆弱性プロファイル] タブ



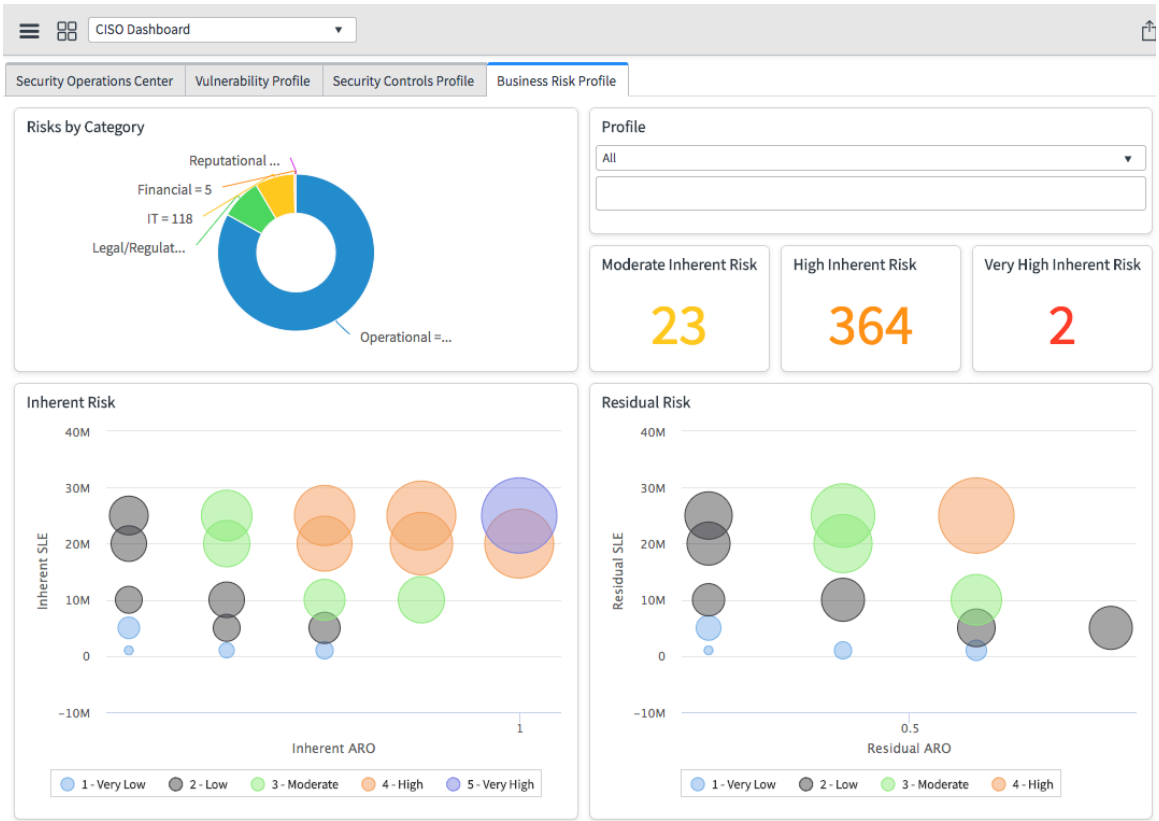
[セキュリティコントロールプロファイル] タブ



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[ビジネスリスクプロファイル] タブ



エンドユーザーとロール

エンドユーザーと目標	必要なロール
CISO：組織全体の現在のセキュリティ体制を明確に把握する必要がある	sn_si.ciso

CISO ダッシュボードのインジケーター

CISO ダッシュボードには、次の重要業績評価指標が表示されます。

SI - 平均識別時間

セキュリティインシデントの識別にかかる 7 日間の平均時間 (分)。毎日計算されます。

平均封じ込め時間

セキュリティインシデントの封じ込めにかかる 7 日間の平均時間 (分)。毎日計算されます。

平均除去時間

セキュリティインシデントの除去にかかる 7 日間の平均時間 (分)。毎日計算されます。平均封じ込め時間と平均除去時間は、どちらもインジケーター [SI - 平均期間] (セキュリティインシデントのステータス別) に基づいています。

今週の新規セキュリティインシデント

日次の新規セキュリティインシデント数のスコアを週別に合計したインジケーター。

クローズされたセキュリティインシデント (週次)

日次のクローズされたセキュリティインシデント数を 7 日間分合計したインジケーター。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

優先度別の新規セキュリティインシデント

新規セキュリティインシデント数を日別にブレークダウンした優先度別のインジケーター。

新規 対 クローズされたセキュリティインシデント (週次) の量

新規インシデント数を 7 日間分合計したインジケーターが、クローズされたインシデント数を 7 日間分合計したインジケーターに対してグラフ化されます。

セキュリティインシデントヒートマップ

各国のオープンセキュリティインシデントの数を示すグローバルマップ。

セキュリティインシデントツリーマップ

インタラクティブツリーマップでは、以下を表示するよう選択できます。

- ビジネスサービスごとのセキュリティインシデント (ビジネス上の重要度別)
- インシデントのカテゴリまたはサブカテゴリ別のセキュリティインシデント
- アサイン先グループごとまたはアサイニーごとのセキュリティインシデント
- 影響を受けるリソースまたは影響を受けるユーザーごとのセキュリティインシデントの「被害者統計情報」

ブレークダウン

ダッシュボードのインジケーターは、次のように分析されます。

- ビジネス上の重要度
- セキュリティグループ
- セキュリティインシデントの経過時間
- セキュリティインシデントカテゴリ
- セキュリティインシデントクローズコード
- セキュリティインシデント優先度
- セキュリティインシデントのステータス
- SI - ビジネスサービス
- 脆弱性

データの可視化

ダッシュボードには、以下の可視化が含まれています。

タイトル	タイプ	説明
30 日を超えてオープン中のセキュリティインシデント (アサイン先グループおよびステータス別) (Security Incidents Open for More Than 30 Days by Assignment Group and State)	ヒートマップ	最も脆弱なアイテムを含むモデルを表示します。
カテゴリ別のリスク (Risks by Category)	ドーナツグラフ	再オープンされた脆弱性一致アイテムの経過時間をリストします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タイトル	タイプ	説明
信頼できるソースによる引用 (Citations by Authority Document)	ドーナツグラフ	アクティブな脆弱性の数
アクティブでないアサイニーのセキュリティインシデント (Security Incidents With Assignee That is not Active)	ヒートマップ	脆弱性に関連付けられたオープンな脆弱性一致アイテムの数 (共通の脆弱性タイプの一覧 (CVE) レコード) を多い順に表示します。
30 日を超えて更新されていないセキュリティインシデント (アサイン先グループおよびステータス別) (Security Incidents Not Updated for More Than 30 Days by Assignment Group and State)	ヒートマップ	最も脆弱なアイテムを含む公開者を表示します。
脆弱性マップ (Vulnerability Map)	マップ	場所別の脆弱性を示す世界地図
最も脆弱なモデル	ドーナツグラフ	脆弱性が最も多いアプリケーション
クラス別の最も脆弱な CI	ドーナツグラフ	サーバータイプ別の CI
重大な脆弱性があるサービス (Services with Critically Significant Vulnerabilities)	List	
非準拠プロファイル (Non-compliant profiles)	棒グラフ	非準拠コントロール (プロファイル別)
コントロールの概要	棒グラフ	準拠しているコントロールと準拠していないコントロールの数
ポリシー例外	List	優先度、所有者、および簡単な説明を含むポリシーの例外
カテゴリ別のリスク (Risks by Category)	ドーナツグラフ	リスクの各カテゴリにおけるリスクの数
固有のリスク	バブル	固有 SLE と固有 ARO

自動翻訳

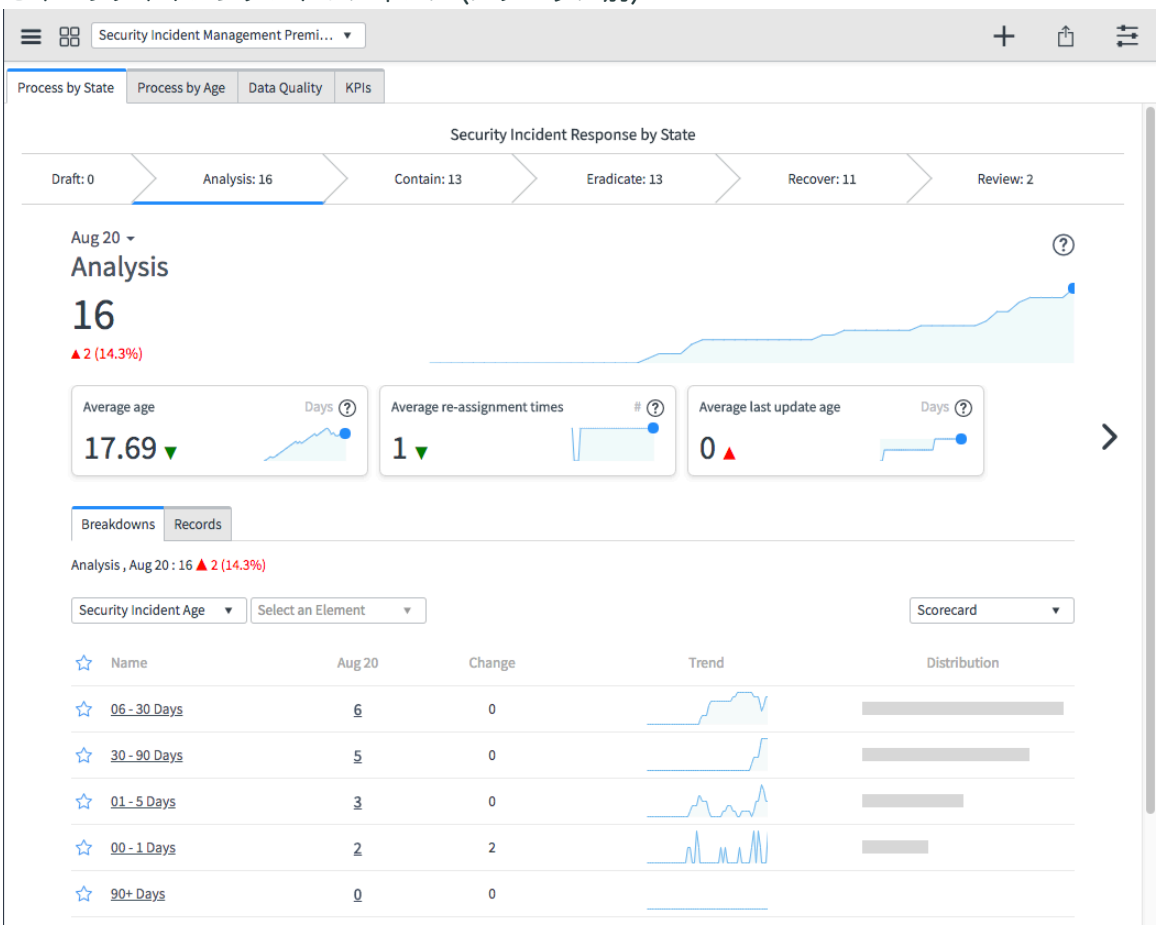
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タイトル	タイプ	説明
残存リスク	バブル	残存 SLE と残存 ARO
中リスク、高リスク、非常に高いリスク (Moderate, High, and Very High Risks)	スコア	それぞれ中リスク、高リスク、非常に高いリスクの数
プロファイル別のリスク (Risk by Profile)	積み上げ棒グラフ	リスクの数 (グループ化する項目、積み上げる項目を選択できます)

セキュリティインシデント管理 (プレミアム) ダッシュボード

このダッシュボードでは、高度な プラットフォームアナリティクス の可視化を使用して、セキュリティマネージャーが初期分析/検出から封じ込め、除去、復旧までのセキュリティインシデントのボリューム、パフォーマンス、および進捗状況を追跡できるようにします。パフォーマンスアナリティクス のライセンスバージョンが必要です。

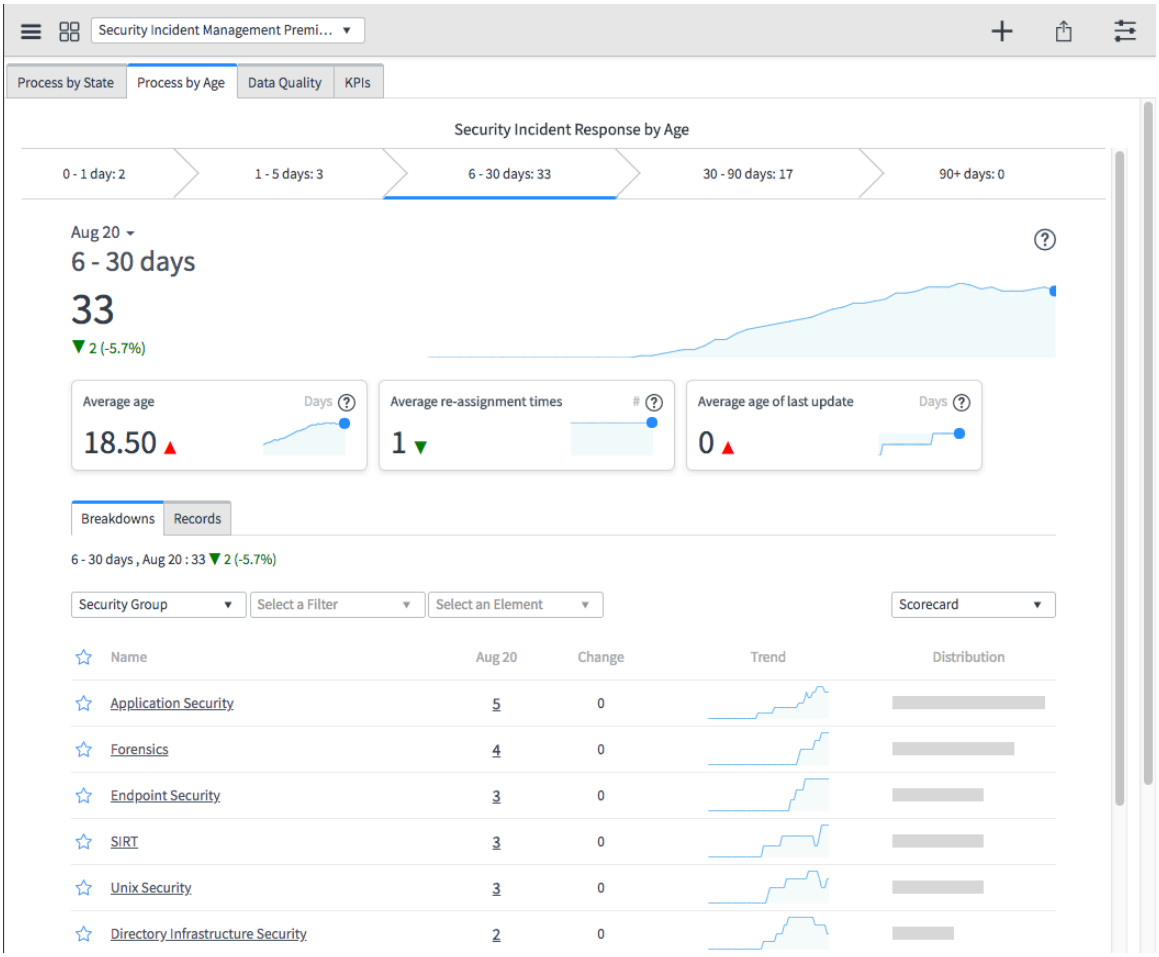
セキュリティインシデントレスポンス (ステータス別)



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンス (経過時間別)



エンドユーザーとロール

エンドユーザーと目標	必要なロール	利点
セキュリティ応答マネージャー：アプリケーションとサービスに関連するセキュリティインシデントの全体的なステータスとボリュームを明確に把握する必要があります。	sn_si.manager	アサイン先グループのメンバーを調整する機能を使用して、全体的なセキュリティ体制を確認できます。
セキュリティ応答アドミン：懸念事項を迅速に特定し、必要に応じてテリトリとスキルを管理しながら、すべてのセキュリティインシデントレスポンスデータを制御する必要があります。	sn_si.admin	リスク計算パラメーターを調整することで、組織に最も関連する脆弱性一致アイテムが最初に対処されるようにすることができます。
セキュリティ応答アナリスト：組織にとっての重要度に基づいて、どの脆弱性に焦点を当てるかを迅速に優先順位付けする必要があります。	sn_si.analyst	階層 1 および 2 のセキュリティアナリストがセキュリティインシデントに対応します。セキュリティインシデント、要求、タスクの他、各自のインシデントに関連する問題、変更、

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エンドユーザーと目標	必要なロール	利点
		および機能停止を作成したり更新したりできます。

セキュリティインシデント管理 (プレミアム) インジケーター

[プロセス - ステータス] タブと [プロセス - 経過時間] タブには、次のインジケーターを備えたワークベンチウィジェットが含まれています。

平均経過時間

オープンセキュリティインシデントの平均経過時間インジケーターは、計算式 [[オープンセキュリティインシデントの合計経過時間]] / [[オープンセキュリティインシデントの数]] / 24 を使用して日単位で結果を返します。

平均再アサイン回数

オープンセキュリティインシデントの平均再アサイン回数インジケーターは、計算式「オープンセキュリティインシデントの再アサイン回数合計 / オープンセキュリティインシデントの数」を使用します。

最終更新の平均経過時間

セキュリティインシデントの前回の更新の平均経過時間インジケーターは、計算式「オープンセキュリティインシデントの前回の更新の経過時間合計 / オープンセキュリティインシデントの数 / 24」を使用して日単位で結果を返します。

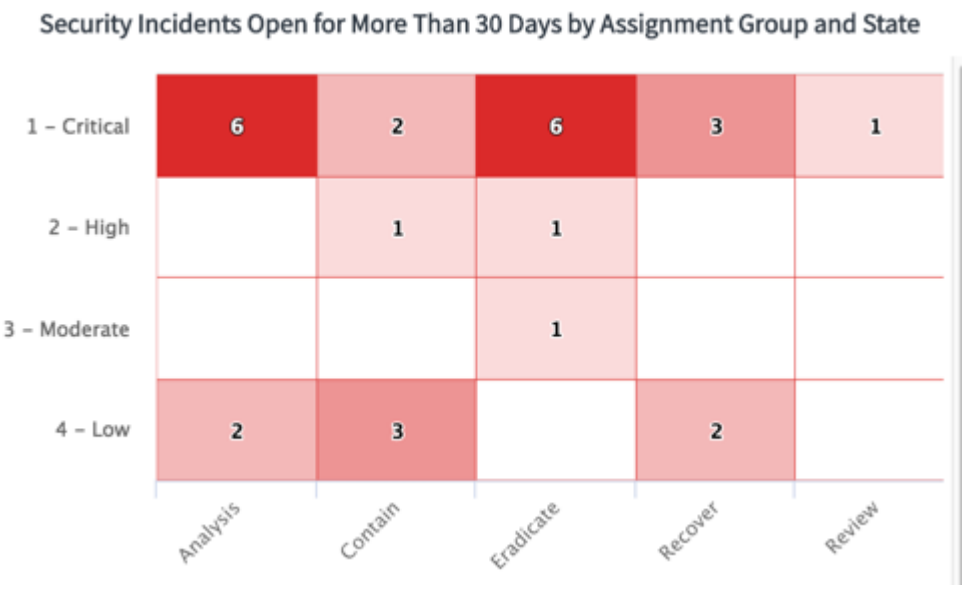
5 日間更新されていない割合

過去 5 日間更新されていないオープンセキュリティの割合インジケーターは、計算式 ([[過去 5 日間更新されていない未解決セキュリティインシデントの数]] / [[オープンセキュリティインシデントの数]]) * 100 を使用します。

[データ品質] タブには、セキュリティインシデントの [カテゴリ] と、[リスク]、[優先度]、および [重大度] のレベルのインタラクティブフィルターがあります。これらのフィルターは、次のインジケーターに同時に適用されます。

30 日を超えてオープン中のセキュリティインシデント (アサイン先グループおよびステータス別) (Security Incidents Open for More Than 30 Days by Assignment Group and State)

30 日間でフィルタリングされ、アサイン先グループとステータス別に分類されたオープンセキュリティインシデントの数。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクティブでないアサイニーのセキュリティインシデント (Security Incidents With Assignee That is not Active)

アサイニーがいない、またはアサイニーがアクティブでないオープンセキュリティインシデントの数。

30 日を超えてオープン中のセキュリティインシデント (アサイン先グループおよびステータス別) (Security Incidents Open for More Than 30 Days by Assignment Group and State)

アサイン先グループとステータス別に分類された、過去 30 日間更新されていないオープンセキュリティインシデント数インジケーター。

[KPI] タブには、次の追加のインジケーターがあります。

- 重大な新規セキュリティインシデントの割合
- オープンセキュリティインシデントの平均経過時間
- セキュリティインシデントの平均クローズ所要時間
- 再度割り当てられたセキュリティインシデントの割合
- 最初のアサイン先によりクローズされたセキュリティインシデントの割合
- セルフサービスによりクローズされたセキュリティインシデントの割合
- 未解決のセキュリティインシデントの割合
- セキュリティインシデントタスクの平均クローズ所要時間

ブレークダウン

ダッシュボードのインジケーターは、次のように分析されます。

- セキュリティグループ
- セキュリティインシデントの経過時間
- セキュリティインシデントカテゴリ
- セキュリティインシデント優先度
- セキュリティインシデントのステータス

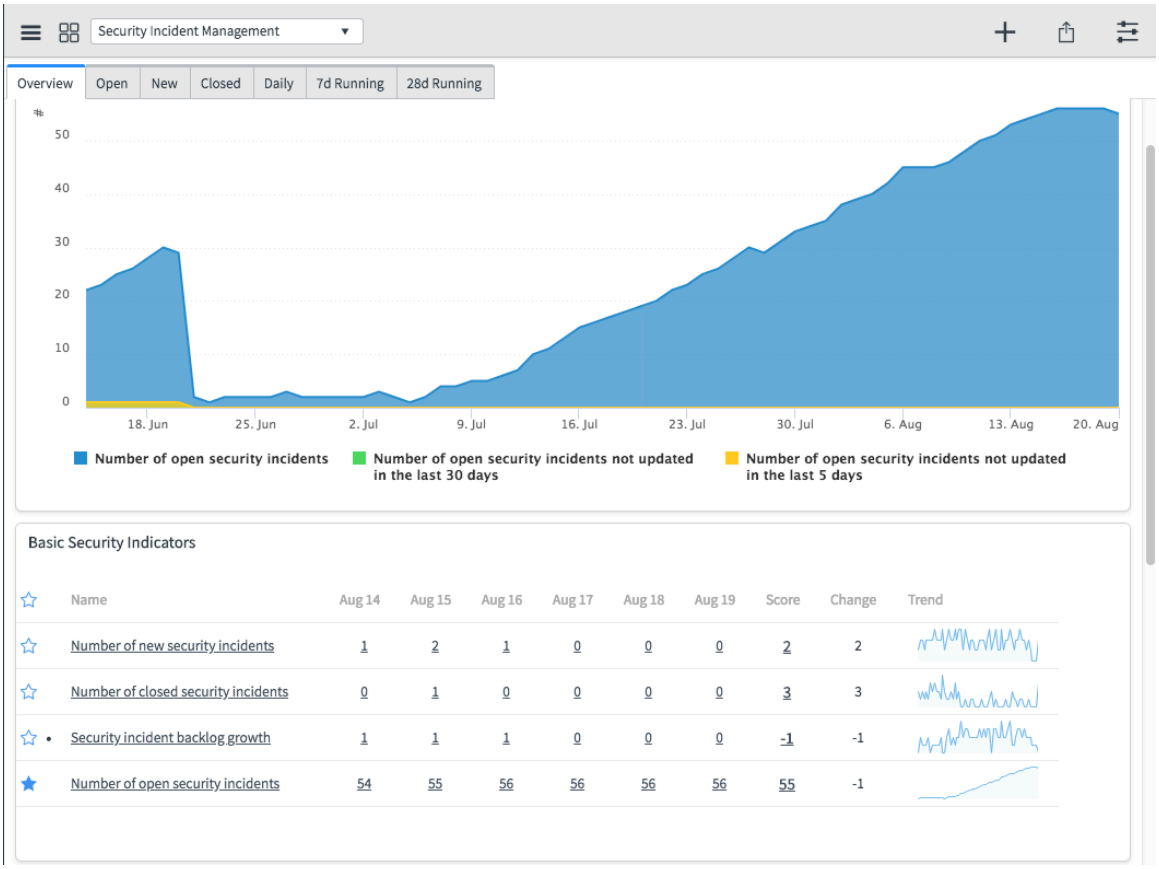
[Major Security Incident] ダッシュボード

セキュリティマネージャーは、このダッシュボードを使用して、初期分析/検出から封じ込め、除去、復旧までのセキュリティインシデントのボリューム、パフォーマンス、および進捗状況を簡単に追跡できます。

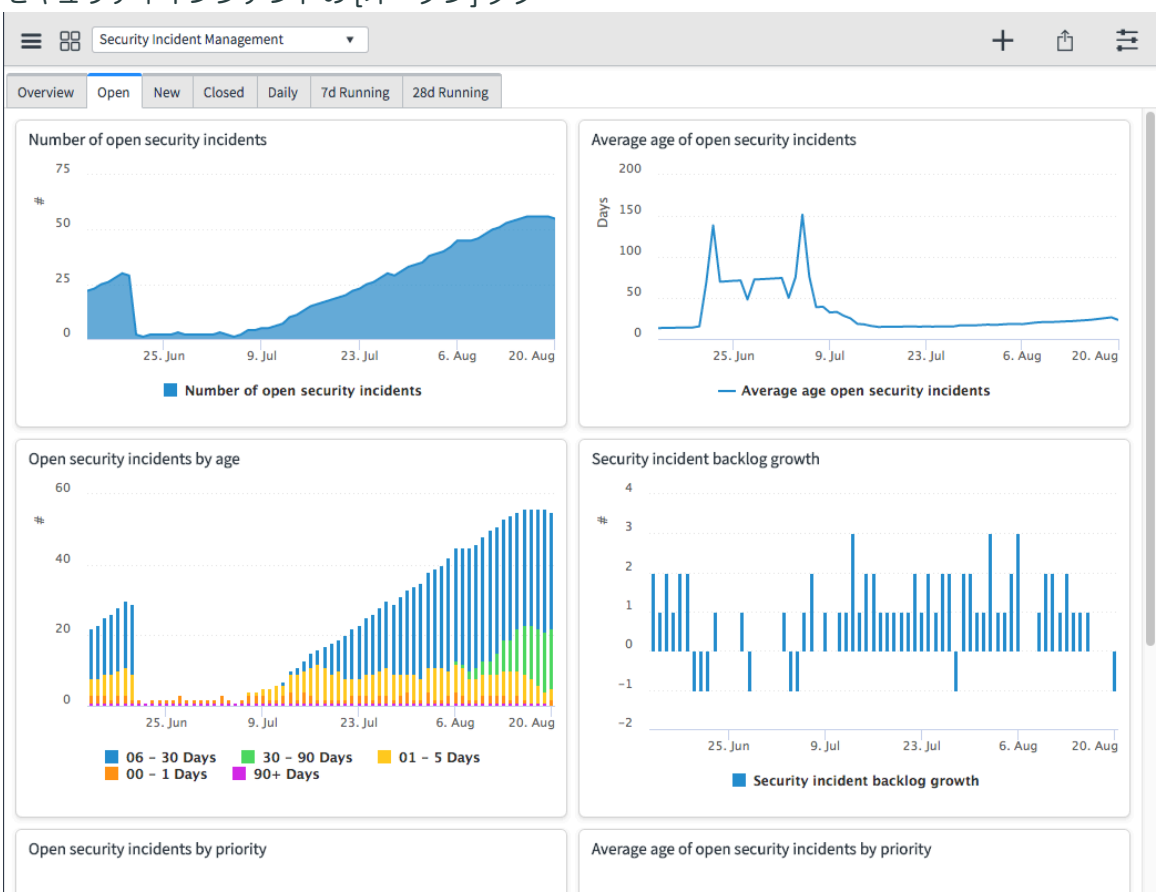
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[概要] タブ



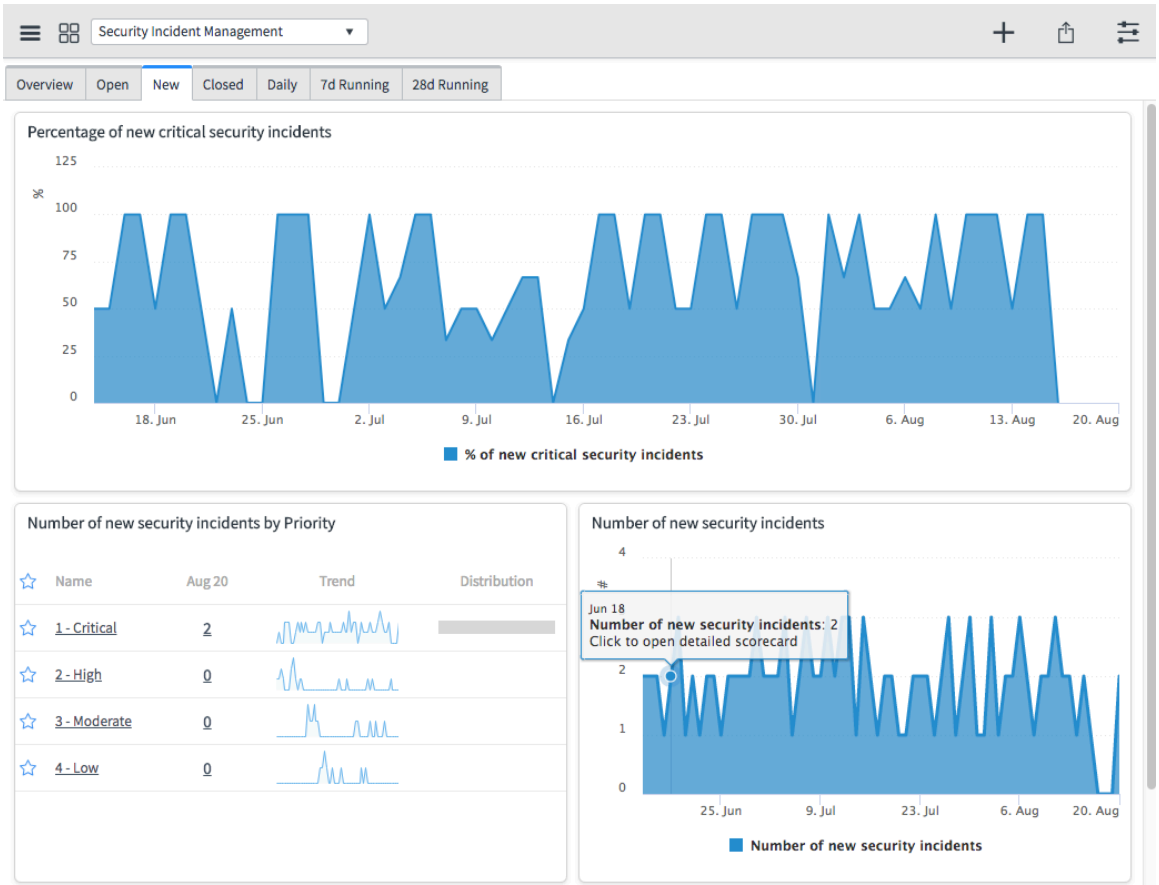
セキュリティインシデントの [オープン] タブ



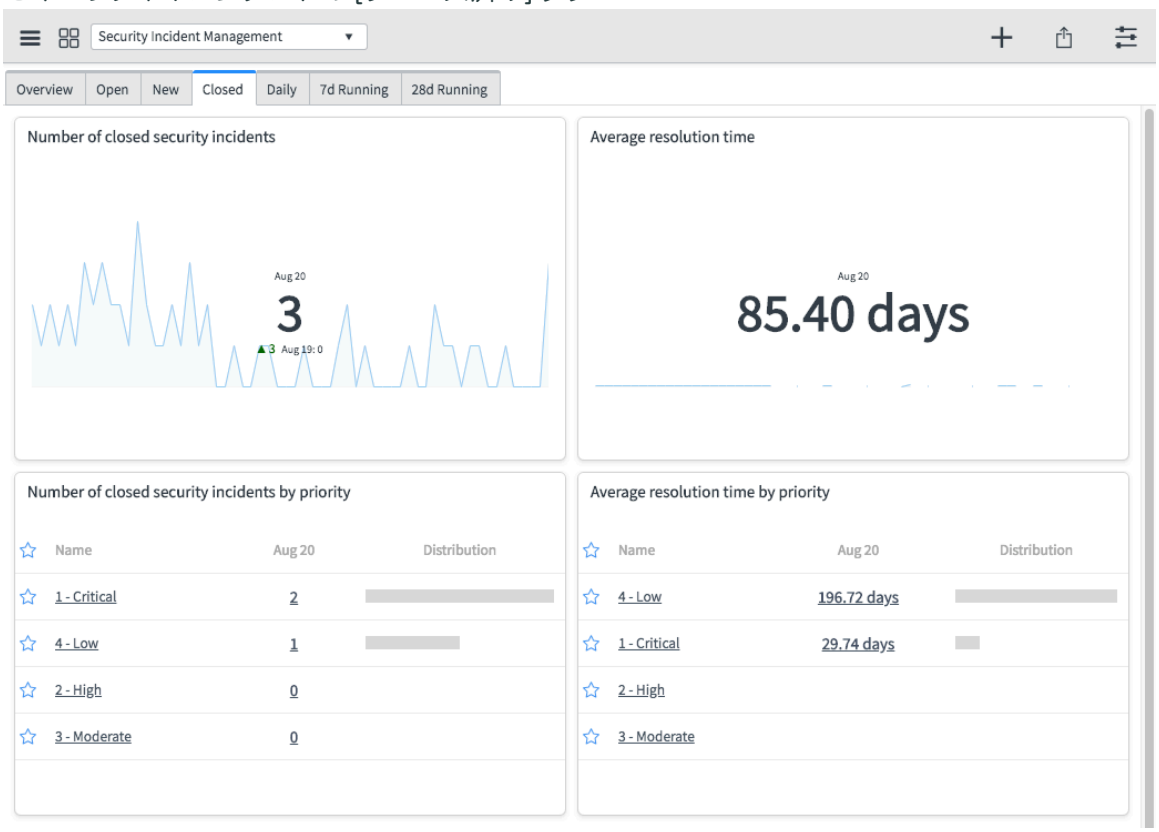
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントの [新規] タブ



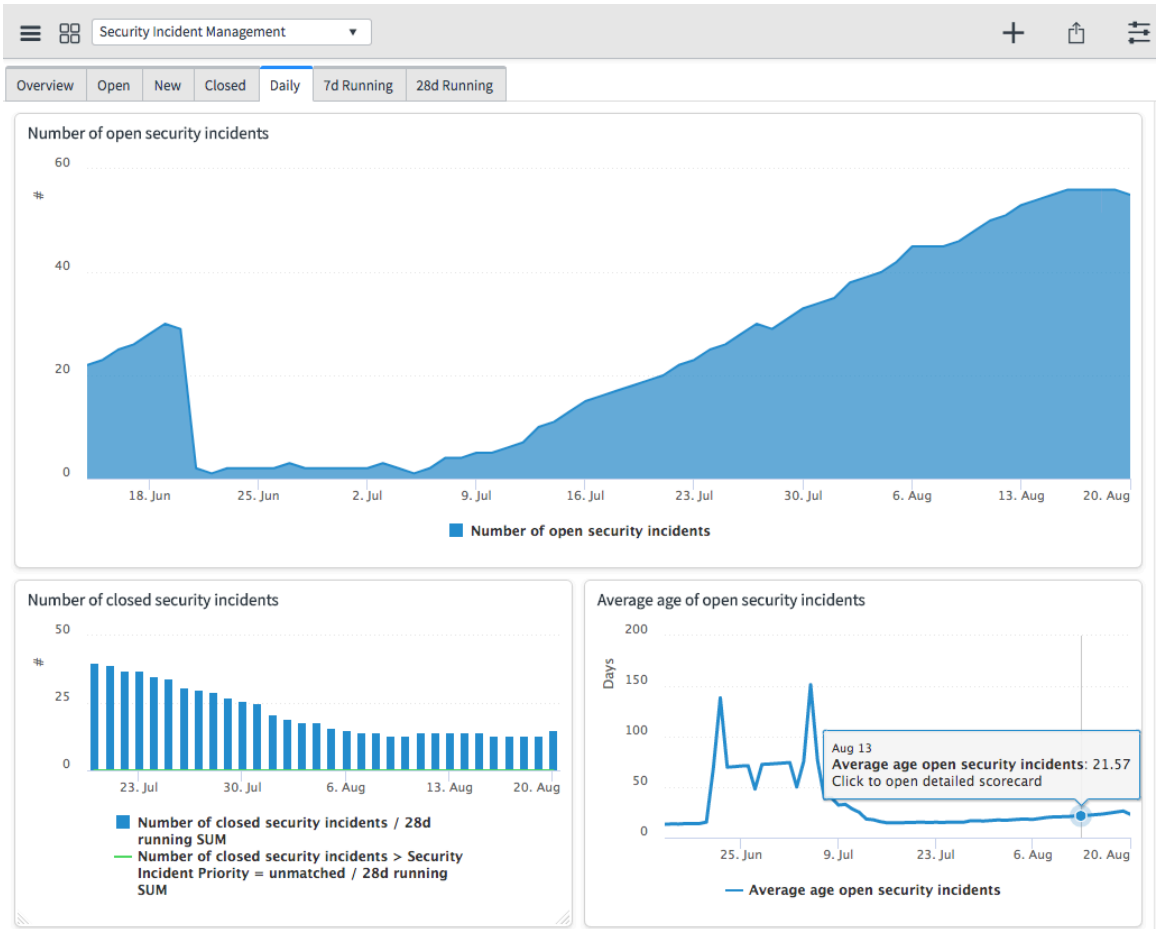
セキュリティインシデントの [クローズ済み] タブ



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントの [日次] タブ



[7 日間移動合計] タブおよび **[28** 日間移動合計] タブは、[日次] タブの形式に従います。

エンドユーザーとロール

エンドユーザーと目標	必要なロール	利点
セキュリティ応答マネージャー：アプリケーションとサービスに関連するセキュリティインシデントの全体的なステータスとボリュームを明確に把握する必要があります。	sn_si.manager	アサイン先グループのメンバーを調整する機能を使用して、全体的なセキュリティ体制を確認できます。
セキュリティ応答アドミン：懸念事項を迅速に特定し、必要に応じてテリトリとスキルを管理しながら、すべてのセキュリティインシデントレスポンスデータを制御する必要があります。	sn_si.admin	リスク計算パラメーターを調整することで、組織に最も関連する脆弱性一致アイテムが最初に対処されるようにすることができます。
セキュリティ応答アナリスト：組織にとっての重要度に基づいて、どの脆弱性に焦点を当てるかを迅速に優先順位付けする必要があります。	sn_si.analyst	階層 1 および 2 のセキュリティアナリストがセキュリティインシデントに対応します。セキュリティインシデント、要求、タスクの他、各自のインシデントに関連する問題、変更、

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エンドユーザーと目標	必要なロール	利点
		および機能停止を作成したり更新したりできます。

セキュリティインシデント管理インジケーター

[Major Security Incident] ダッシュボードには、次の重要業績評価指標が表示されます。

新規セキュリティインシデント

新規セキュリティインシデント数のチャート。

オープンセキュリティインシデント

オープンセキュリティインシデントの数、過去 30 日間更新されていないオープンセキュリティインシデントの数、過去 5 日間更新されていないオープンセキュリティインシデントの数を比較できるチャート。

基本セキュリティインジケーター

新規セキュリティインシデント数インジケーター、クローズ済みセキュリティインシデント数インジケーター、セキュリティインシデントバックログの増加インジケーター、およびオープンセキュリティインシデント数インジケーターを示す過去 6 日間のスコア。

優先度別の新規セキュリティインシデント

優先度別の新規セキュリティインシデントの数。

ブレークダウン

ダッシュボードのインジケーターは、次のように分析されます。

- セキュリティグループ
- セキュリティインシデントの経過時間
- セキュリティインシデントカテゴリ
- セキュリティインシデント優先度
- セキュリティインシデントのステータス

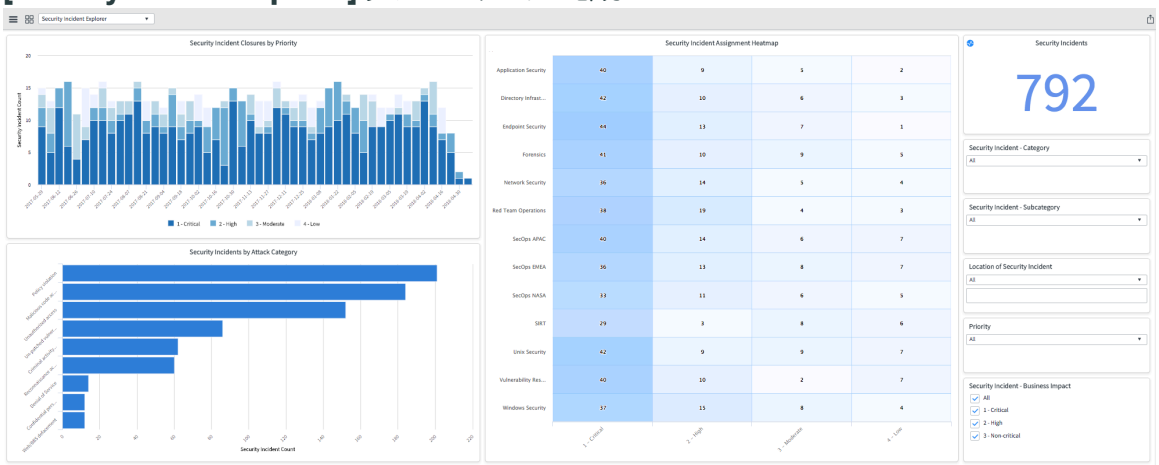
Security Incident Explorer ダッシュボード

セキュリティマネージャーは、このダッシュボードを使用して、カテゴリ、サブカテゴリ、場所、優先度、およびビジネスインパクト別に集計されグループ化されたセキュリティインシデントを表示できます。これらのビューにより、アドミニストレーターは、攻撃の発生頻度と影響を受けるビジネスサービスをすばやく把握できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[Security Incident Explorer] ダッシュボードの部分ビュー



エンドユーザーとロール

エンドユーザーと目標	必要なロール	利点
セキュリティ応答マネージャー：アプリケーションとサービスに関連するセキュリティインシデントの全体的なステータスとボリュームを明確に把握する必要があります。	sn_si.manager	アサイン先グループのメンバーを調整する機能を使用して、全体的なセキュリティ体制を確認できます。
セキュリティ応答アドミン：懸念事項を迅速に特定し、必要に応じてテリトリとスキルを管理しながら、すべてのセキュリティインシデントレスポンスデータを制御する必要があります。	sn_si.admin	リスク計算パラメーターを調整することで、組織に最も関連する脆弱性一致アイテムが最初に対処されるようにすることができます。
セキュリティ応答アナリスト：組織にとっての重要度に基づいて、どの脆弱性に焦点を当てるかを迅速に優先順位付けする必要があります。	sn_si.analyst	階層 1 および 2 のセキュリティアナリストがセキュリティインシデントに対応します。セキュリティインシデント、要求、タスクの他、各自のインシデントに関連する問題、変更、および機能停止を作成したり更新したりできます。

Security Incident Explorer インジケーター

[Security Incident Explorer] ダッシュボードには、次の重要業績評価指標が表示されます。

セキュリティインシデント

オープンセキュリティインシデントおよび処理待ちのセキュリティインシデントの合計数。

優先度別のセキュリティインシデントのクローズ

優先度別のクローズ済みセキュリティインシデントの数。

攻撃別のセキュリティインシデントカテゴリ

カテゴリ別のオープンセキュリティインシデントの数。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントアサインヒートマップ

アサイン先グループと優先度別のオープンセキュリティインシデント数の 2 段階のブレークダウン。

セキュリティインシデントヒートマップ

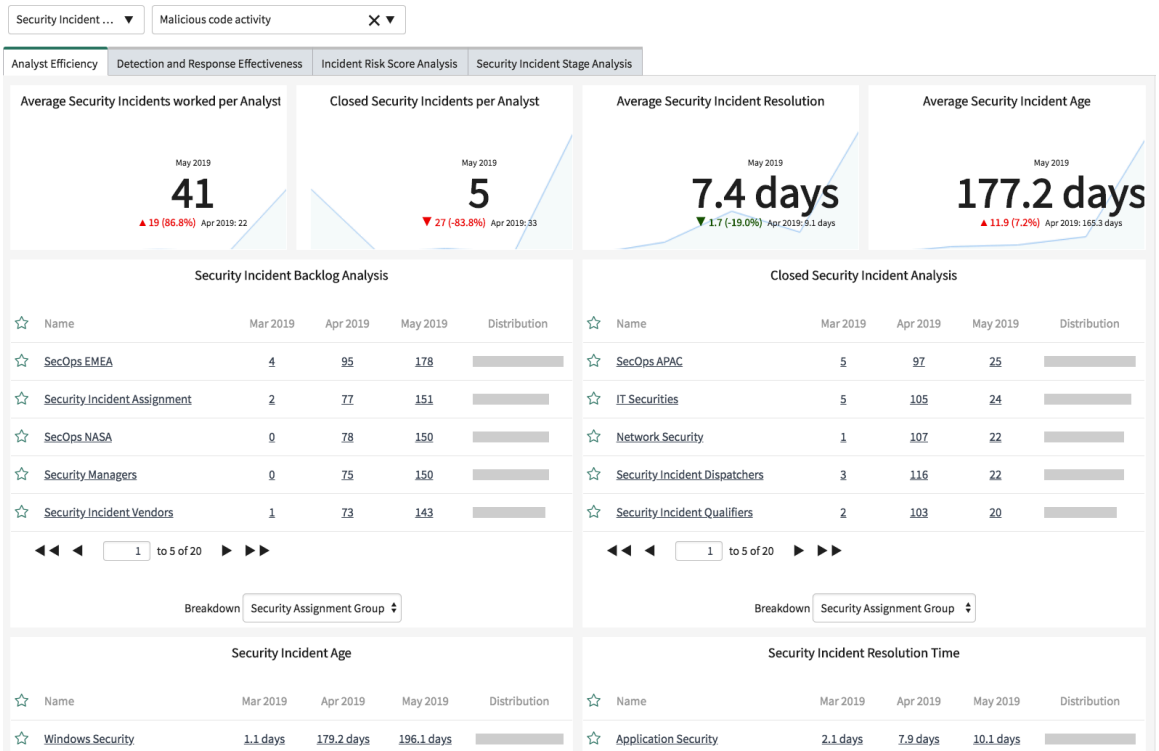
各国のオープンセキュリティインシデントの数を示すグローバルマップ。

Security Operations 効率ダッシュボード

Security Operations Center (SOC) のマネージャーは、全体的な効率メトリクスを表示し、組織内の SOC チームメンバーの個々のパフォーマンスを測定できます。

SOC のマネージャーは、パフォーマンスアナリティクスダッシュボードを使用して、効率を向上させ、時間の経過とともに一般的な領域と特定の領域の両方で SOC のパフォーマンスを把握できます。

[アナリストの効率] タブ

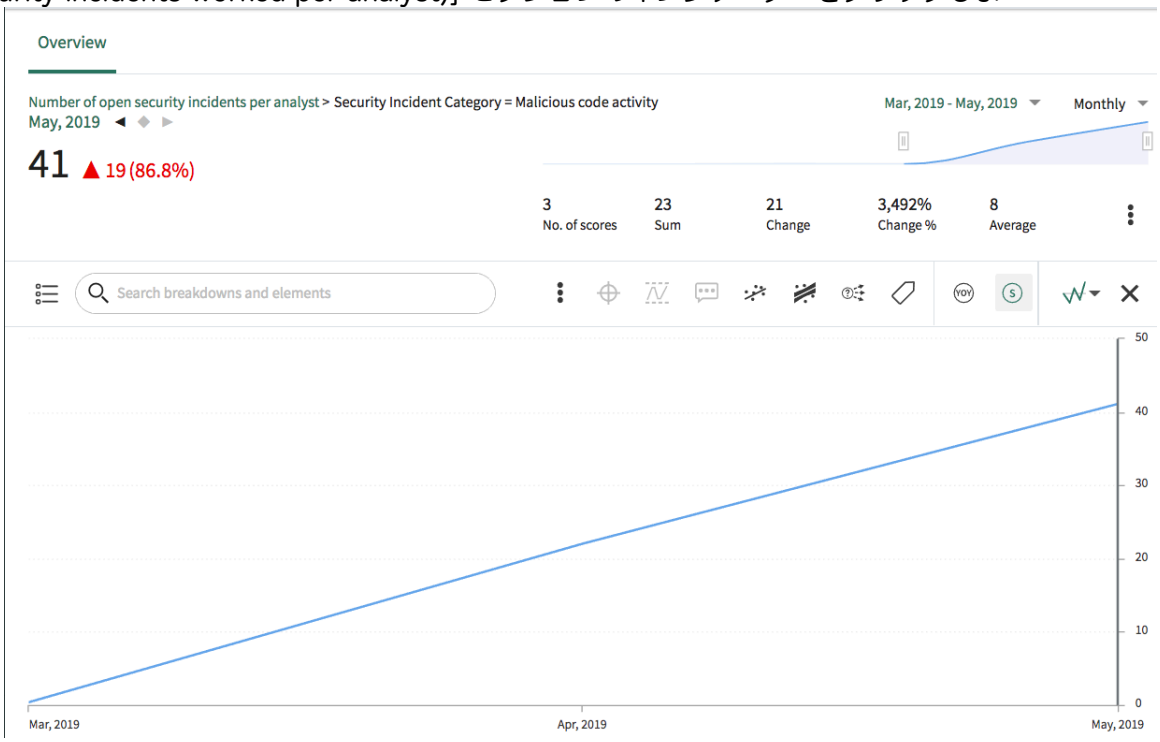


ドリルダウンして詳細を表示するには、いずれかのインジケーターをクリックします。たとえば、[アナリストごとの処理完了セキュリティインシデント数の平均 (Average

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

security incidents worked per analyst)] セクションのインジケーターをクリックしま



す。

グラフは、オープンセキュリティインシデントの数が 3 月から 5 月にかけて 0 から 40 を超えて増加したことを示しています。ヘッダーに表示されるデータに注目してください。

- 傾向インジケーター：データが収集された最新の期間のオープンインシデント数の変化を示します。このチャートは、2019 年 3 月から 2019 年 5 月までのデータを表し、オープンインシデントの数が 5 月に 19 増加していることを示しています。オープンインシデントの数が一定期間にわたって減少している場合は、アナリストの効率が高いことを示します。
- スコア数 (No. of scores)：データが収集された期間 (2019 年 3 月から 5 月)。
- 合計：3 月から 5 月までの新規オープンインシデントの数。
- 変更：3 月から 4 月までの新規オープンインシデントの数。
- 平均：選択された期間のアナリストごとのオープンインシデント数の平均。

[アナリストの効率] タブ

インジケーター	説明
アナリストごとの作業済みセキュリティインシデント数の平均 (Average security incidents worked per analyst)	指定された期間のアナリストごとのオープンインシデント数の平均。使用される式：[[Number of open security incidents / By month AVG +]]/[[Number of Security Agents]]
アナリストごとのクローズ済みセキュリティインシデント	指定された期間に選択されたカテゴリの各アナリストによってクローズされたインシデントの合計数。使用される式：[Number of closed security incidents > Security Incident Category = <category_name> / By month SUM +]]/[[Number of Security Agents / By month AVG +]]
セキュリティインシデントの平均解決時間 (Average security incident resolution)	指定された期間に各アナリストがセキュリティインシデントをクローズするのにかかった平均時間。結果を日数で表示するために使用される式：([[Summed duration of closed security incidents > Security Incident Category = <category_name> / By month AVG +]] /

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

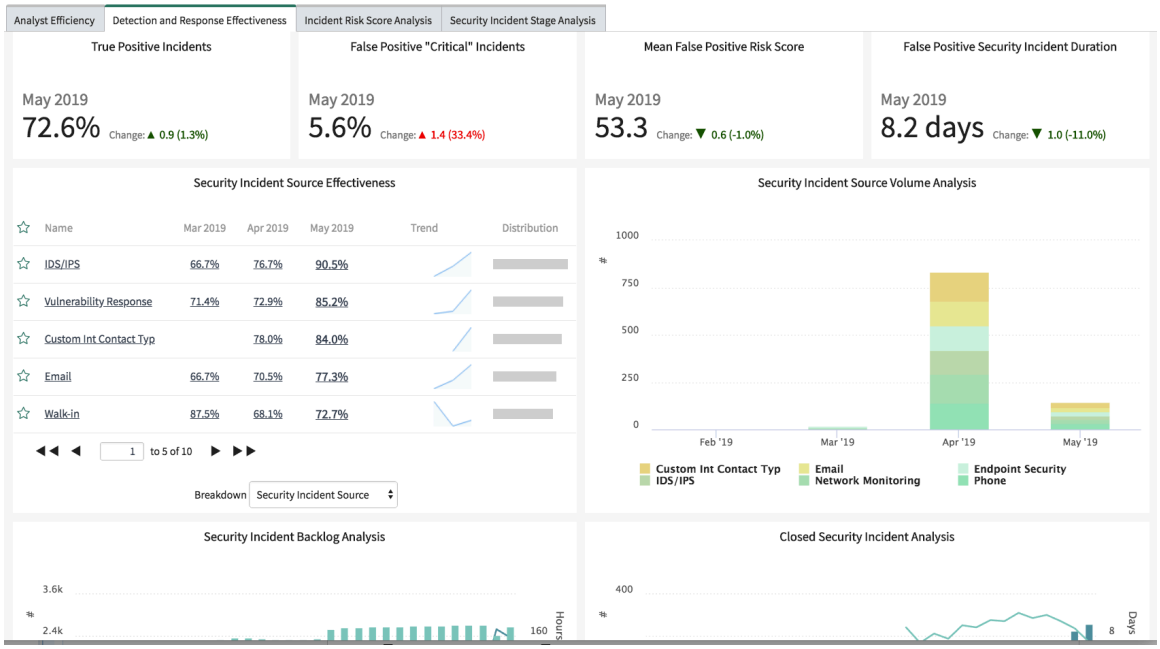
[アナリストの効率] タブ (続く)

インジケーター	説明
	[[Number of closed security incidents > Security Incident Category = <category_name> / By month AVG +]]) / 24
セキュリティインシデントの平均経過時間 (Average security incident age)	アナリストごとの、セキュリティインシデントがオープン状態になっていた平均日数。結果を日数で表示するために使用される式：([[Summed age of open security incidents > Security Incident Category = <category_name> / By month AVG +]]/ [[Number of open security incidents > Security Incident Category = <category_name> / By month AVG +]]) / 24
セキュリティインシデントバックログアナリティクス	指定された期間のオープンセキュリティインシデントの合計数。[ブレークダウン] リストからオプションを選択して、各アナリスト、セキュリティグループ、優先度のバックログを表示します。選択した 2 つの月の間でオープンセキュリティインシデントの数を比較することもできます。
クローズ済みセキュリティインシデント分析	指定された期間にクローズされたセキュリティインシデントの合計数。[ブレークダウン] リストからオプションを選択して、各アナリスト、セキュリティグループ、優先度のカウントを表示します。選択した 2 つの月の間でクローズされたセキュリティインシデントの数を比較することもできます。
セキュリティインシデントの経過時間	指定された期間にセキュリティインシデントがオープン状態であった平均日数。[ブレークダウン] リストからオプションを選択して、各アナリスト、セキュリティグループ、優先度のセキュリティインシデントの経過時間を表示します。結果を日数で表示するために使用される式：([[Summed age of open security incidents > Security Incident Category = <category_name> > Security Assignment Group = <group_name> / By month AVG +]]/ [[Number of open security incidents > Security Incident Category = <category_name> > Security Assignment Group = <group_name> / By month AVG +]]) / 24
セキュリティインシデントの解決時間	指定された期間にセキュリティインシデントを解決するのにかかった平均日数。[ブレークダウン] リストからオプションを選択して、各アナリスト、セキュリティグループ、優先度のセキュリティインシデントの解決時間を表示します。結果を日数で表示するために使用される式：([[Summed duration of closed security incidents > Security Incident Category = Malicious code activity > Security Assigned To = John Ashby / By month AVG +]] / [[Number of closed security incidents > Security Incident Category = Malicious code activity > Security Assigned To = John Ashby / By month AVG +]]) / 24

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[検出と応答の有効性] タブ



[検出と応答の有効性] タブ

インジケーター	説明
真陽性インシデント	指定された期間の選択されたカテゴリでの真陽性セキュリティインシデントの割合。使用される式：(1-([[Number of false positive security incidents > Security Incident Category = Malicious code activity / By month SUM +]] / [[Number of closed security incidents > Security Incident Category = Malicious code activity / By month SUM +]])) * 100
重大な誤検出インシデント	指定された期間の選択されたカテゴリでの誤検出の重大セキュリティインシデントの割合。使用される式：([[Number of false positive security incidents > Security Incident Risk Score = Critical Risk > Security Incident Category = Malicious code activity / By month SUM +]] / [[Number of closed security incidents > Security Incident Category = Malicious code activity / By month SUM +]]) * 100 **注:** Closed code = Invalid vulnerability or False positive であるすべてのセキュリティインシデントが誤検出インシデントとして扱われます。
平均誤検出リスクスコア (Mean false positive risk score)	誤検出インシデントとして識別されたクローズ済みセキュリティインシデントの平均月次リスクスコア。リスクスコアが低いほど、セキュリティアナリストが誤検出インシデントの分析に

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

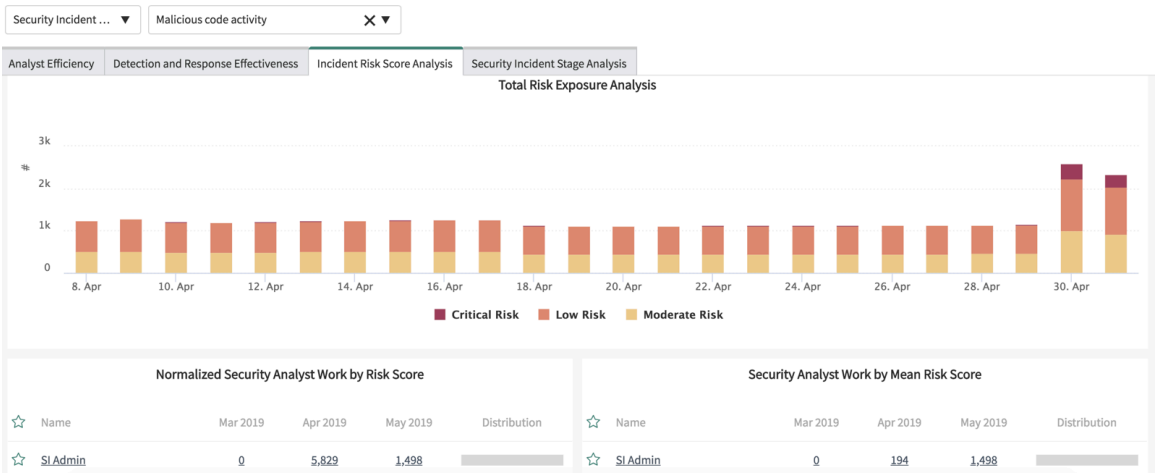
[検出と応答の有効性] タブ (続く)

インジケーター	説明
	費やした時間が少ないことを示します。使用される式：([[Number of false positive security incidents > Security Incident Risk Score = Critical Risk > Security Incident Category = Malicious code activity / By month SUM +]] / [[Number of closed security incidents > Security Incident Category = Malicious code activity / By month SUM +]]) * 100
誤検出セキュリティインシデントの期間	セキュリティアナリストが誤検出インシデントの調査に費やした平均日数。使用される式：([[Summed duration of false positive security incidents]] / [[Number of false positive security incidents]]) / 24
セキュリティインシデントソースの有効性	指定された期間に特定のソースによって識別された真陽性セキュリティインシデントの割合。ソースには、メール、ネットワークアクティビティ、カスタマーサポートなどがあります。このデータは、セキュリティインシデントソースの有効性を測定するのに役立ちます。使用される式： (1-([[Number of false positive security incidents > Security Incident Category = Malicious code activity > Security Incident Source = IDS/IPS / By month SUM +]] / [[Number of closed security incidents > Security Incident Category = Malicious code activity > Security Incident Source = IDS/IPS / By month SUM +]])) * 100
セキュリティインシデントソースボリューム分析	それぞれのセキュリティインシデントソースの当月のクローズ済みセキュリティインシデントの数。選択した 2 つの月の間で各ソースタイプのセキュリティインシデントの数を比較することもできます。
セキュリティインシデントバックログアナリティクス	指定された期間のオープンセキュリティインシデントの合計数と、インシデントがオープン状態であった平均日数。選択した 2 つの月の間でオープンセキュリティインシデントの数を比較することもできます。平均バックログ期間の計算に使用される式：([[Summed age of open security incidents > Security Incident Category = Malicious code activity]]/ [[Number of open security incidents > Security Incident Category = Malicious code activity]]) / 24
クローズ済みセキュリティインシデント分析	指定された期間のクローズ済みセキュリティインシデントの合計数と、これらのインシデントの平均解決時間。平均解決時間の計算に使用される式： ([[Summed duration of closed security incidents > Security Incident Category = Malicious code activity]] / [[Number of closed security incidents > Security Incident Category = Malicious code activity]]) / 24

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[インシデントリスクスコア分析] タブ



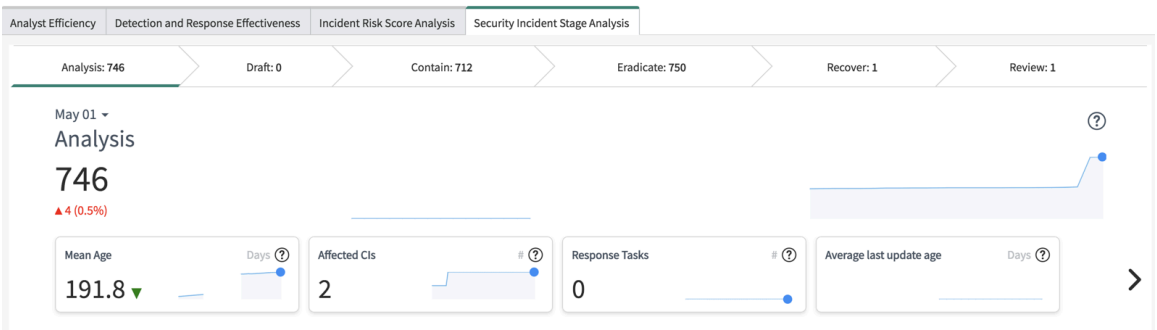
[インシデントリスクスコア分析] タブ

インジケーター	説明
合計リスクエクスポージャー分析	指定された期間の各リスクカテゴリ (低、中、重大) のオープンインシデントの合計数。2 つの月の間でさまざまなリスクカテゴリのインシデントの数を比較することもできます。
リスクスコア別の正規化されたセキュリティアナリストの作業 (Normalized security analyst work by risk score)	指定された期間の各セキュリティアナリストの合計リスクスコア。これは、セキュリティアナリストがクローズした真陽性セキュリティインシデントの数に基づいて計算されます。使用される式： [[Summed Risk Score of Closed Security Incidents > Security Incident Category = Malicious code activity > Security Assigned To = SI Admin / By month SUM +]] - [[Summed Risk Score of False Positive Security Incidents > Security Incident Category = Malicious code activity > Security Assigned To = SI Admin / By month SUM +]]
平均リスクスコア別のセキュリティアナリストの作業	指定された期間の各セキュリティアナリストの平均リスクスコア。使用される式： [[Summed Risk Score of Closed Security Incidents > Security Incident Category = Malicious code activity > Security Assigned To = SI Admin / By month AVG +]] - [[Summed Risk Score of False Positive Security Incidents > Security Incident Category = Malicious code activity > Security Assigned To = SI Admin / By month AVG +]]

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[セキュリティインシデントステージ分析] タブ



特定の日のオープンインシデントの数と、これらのインシデントのステータス ([分析]、[ドラフト]、[封じ込め]、[根絶]、[復旧]、または [レビュー) を確認できます。各ステージでは、平均経過時間、影響を受ける CI、応答タスクなどを表示できます。リンクをクリックすると、これらのインシデントの追加の詳細またはブレークダウンが表示されます。

セキュリティインシデントレスポンスワークスペース

ServiceNow® セキュリティインシデントレスポンスワークスペースは刷新されたインターフェイスで、セキュリティアナリストと SOC マネージャーに次世代のユーザーエクスペリエンスを提供します。セキュリティアナリストは、このインターフェイスを使用して、初期分析から封じ込め、除去、復旧までのセキュリティインシデントのライフサイクルを管理できます。

SIR ワークスペース を開始するには

タイルを選択して開始します。

ワークスペースを探索

SIR ワークスペースの概念と機能について学ぶ

ワークスペースを使用するアドミン

SIR ワークスペースと機能の構成

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ワークスペースを使用するアナリスト

アナリストが SIR ワークスペースを使用する方法を学ぶ

SIR ダッシュボードを表示

SIR ワークスペースダッシュボードの表示

ストアでアプリを要求

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアに要求を送信する方法について確認してください。リリースされたすべてのアプリのリリースメモ情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

重要:

- ServiceNow Store から セキュリティインシデントレスポンス の 13.4.5 バージョン以降をインストールすると、デフォルトで セキュリティインシデントレスポンスワークスペース (sn_si_aw) 1.5.1 バージョン以降が自動的にインストールされます。依存アプリケーションの詳細については、「SIR ワークスペース プラグインおよびロール」セクションを参照してください。
- セキュリティインシデントレスポンスワークスペースバージョン 1.5.1 以降は、セキュリティインシデントレスポンスのインストール/アップグレードによってのみインストール/アップグレードでき、個別にインストールすることはできません。

その他のリソース

ServiceNow コミュニティ で、セキュリティインシデントレスポンス のフォーラム にアクセスしてください。

SIR ワークスペース の概要

セキュリティインシデントレスポンスワークスペース の概要を確認し、改善されたユーザーエクスペリエンスを使用して、セキュリティアナリストとマネージャーがどのように日常業務、全インシデント調査を行い、セキュリティアナリストやチームにアサインされたセキュリティインシデント、応答タスク、および SLA の概要を把握するかを理解します。

このセクションでは、以下について説明します。

- SIR ワークスペース プラグインおよび必要なロール
- SIR ワークスペース の主な機能

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SIR ワークスペース プラグインおよびロール

セキュリティインシデントレスポンスワークスペース (sn_si_aw) プラグインを使用するには、次のアプリケーションが必要です。

アプリケーション

セキュリティインシデントレスポンスアプリケーションのバージョン 13.4.5 以降をインストールすると、セキュリティインシデントレスポンスワークスペース と次のアプリが自動的にインストールされます。

- エンタープライズセキュリティケース管理 PAD 共通 [sn_escm_pad_cmn]
- Security Operations Common Workspace [sn_escm_ws_cmn]
- Security Incident UI Card Component [sn_sirw_evam]
- Security Operations スポーク [sn_sec_spoke]

重要:

- ServiceNow Store から セキュリティインシデントレスポンス の 13.4.5 バージョン以降をインストールすると、デフォルトで セキュリティインシデントレスポンスワークスペース (sn_si_aw) 1.5.1 バージョン以降が自動的にインストールされます。依存アプリケーションの詳細については、「SIR ワークスペース プラグインおよびロール」セクションを参照してください。
- セキュリティインシデントレスポンスワークスペースバージョン 1.5.1 以降は、セキュリティインシデントレスポンスのインストール/アップグレードによってのみインストール/アップグレードでき、個別にインストールすることはできません。

エンタープライズセキュリティケース管理 **PAD** 共通にはプレイブックエクスペリエンス [playbook_experience] プラグインが必要です。

セキュリティインシデントレスポンス のロール、テーブル、プロパティ、およびスケジュール済みジョブの詳細については、「セキュリティインシデントレスポンス とともにインストールされるコンポーネント」を参照してください。

SIR ワークスペースの機能

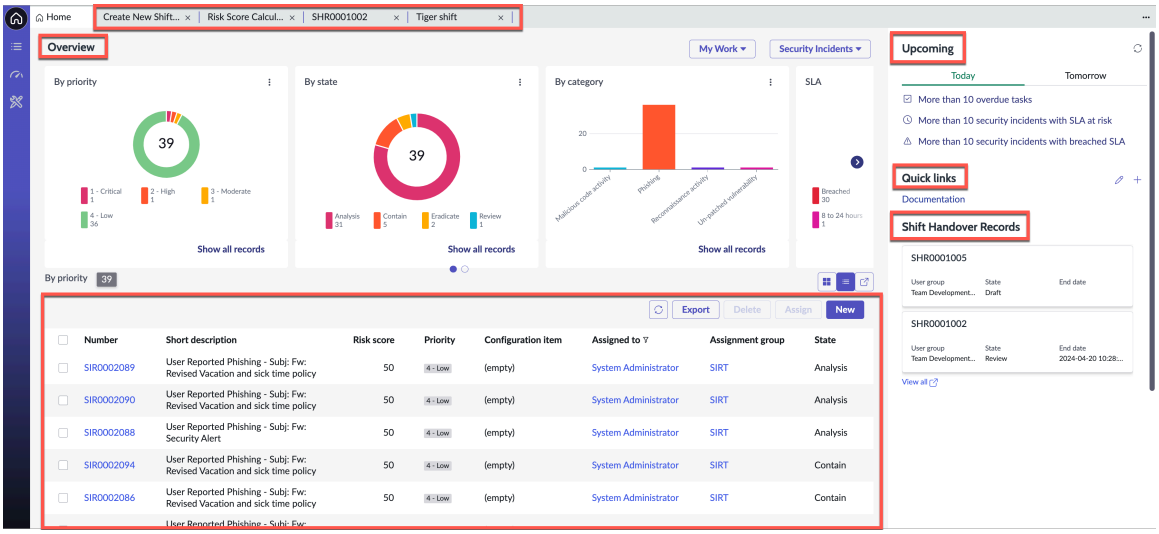
セキュリティインシデントレスポンスワークスペース は、主に次の機能で構成されています。

- [概要] セクション
- [予定] セクション
- [クイックリンク] セクション
- [シフト引継ぎレコード] セクション
- リストビュー
- 複数のセキュリティインシデントを開くことができるマルチタブインターフェイス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SIR ワークスペースの主な機能



SIR ワークスペース インターフェイスの概要

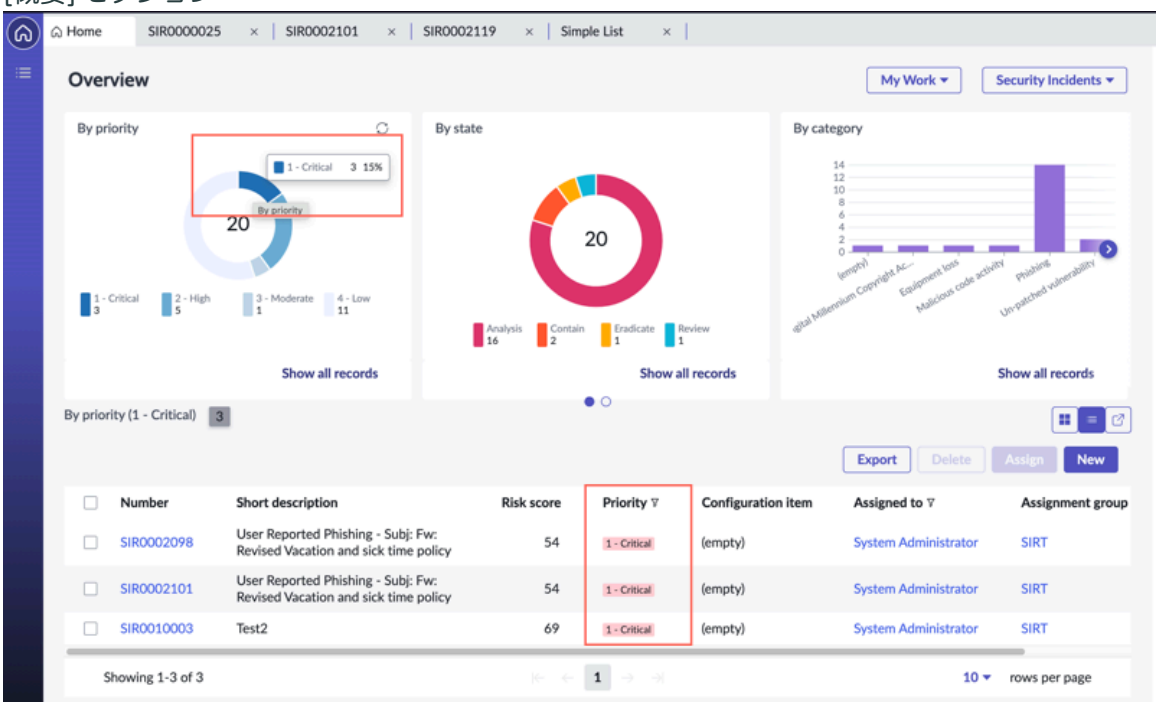
[SIR ワークスペース の概要] ページは、セキュリティアナリストとそのチームの管理下にあるセキュリティインシデントおよび応答タスクの詳細で構成されています。

各フィルターの下には、セキュリティアナリストのキューおよびセキュリティアナリストチームのキューにある、優先度、カテゴリ、ステータス、および SLA 別にグループ化されたさまざまなウィジェットがあります。

ウィジェットでフィルターを適用すると、概要ページの下半分に、対応するセキュリティインシデントまたは応答タスクがカードまたはリストアイテムとして表示されます。アナリストは、必要に応じてカードビューとリストビューを切り替えることができます。

たとえば、[優先度] ウィジェットで最重要のインシデントまたは応答タスクをすべて選択する場合は、ウィジェットの [重要] セグメント (以下は一例のスクリーンショットです) をクリックすると、重要なインシデントまたは応答タスクがリストまたはカードビューに表示されます。

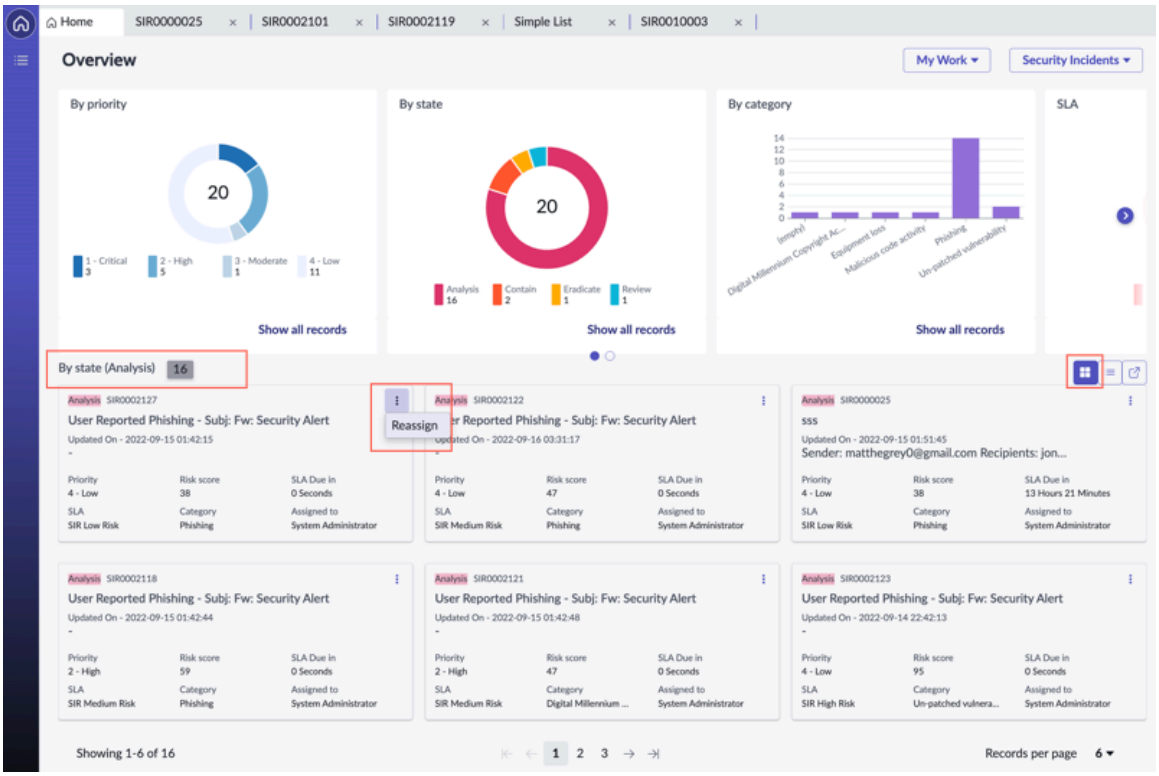
[概要] セクション



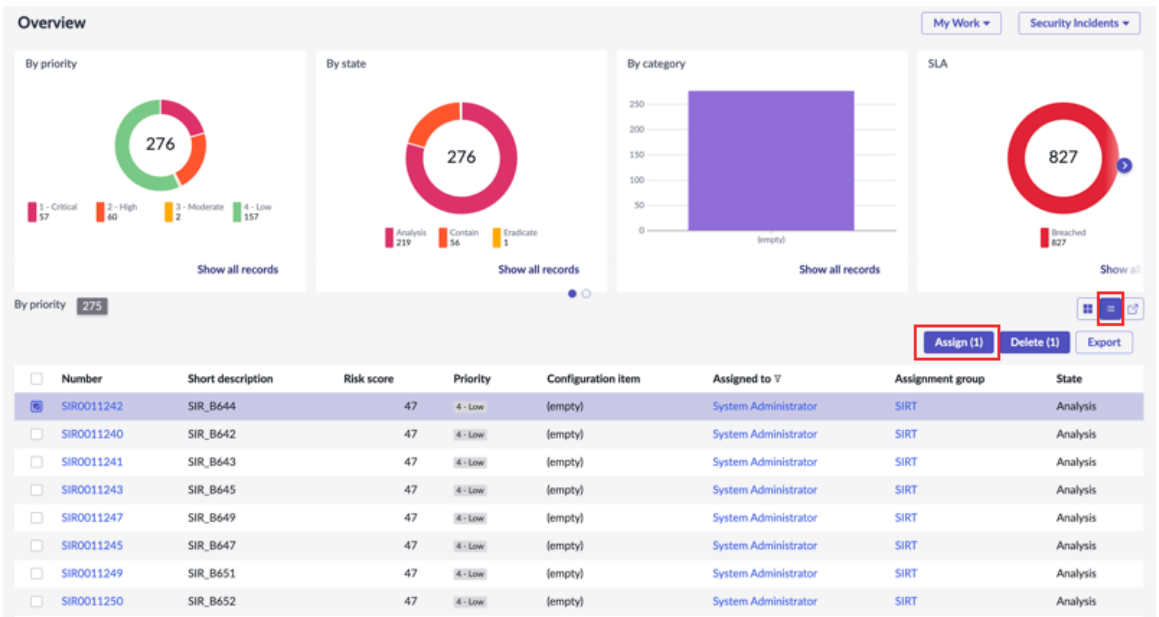
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントまたは応答タスクをこのビューから直接アサインするか再アサインするには、省略記号アイコンをクリックし、[アサイン] (カードビューのオプション) を選択するか、 [アサイン] ボタン (リストビューのオプション) を直接選択してインシデントをアサインします。

カードビューと再アサインの例



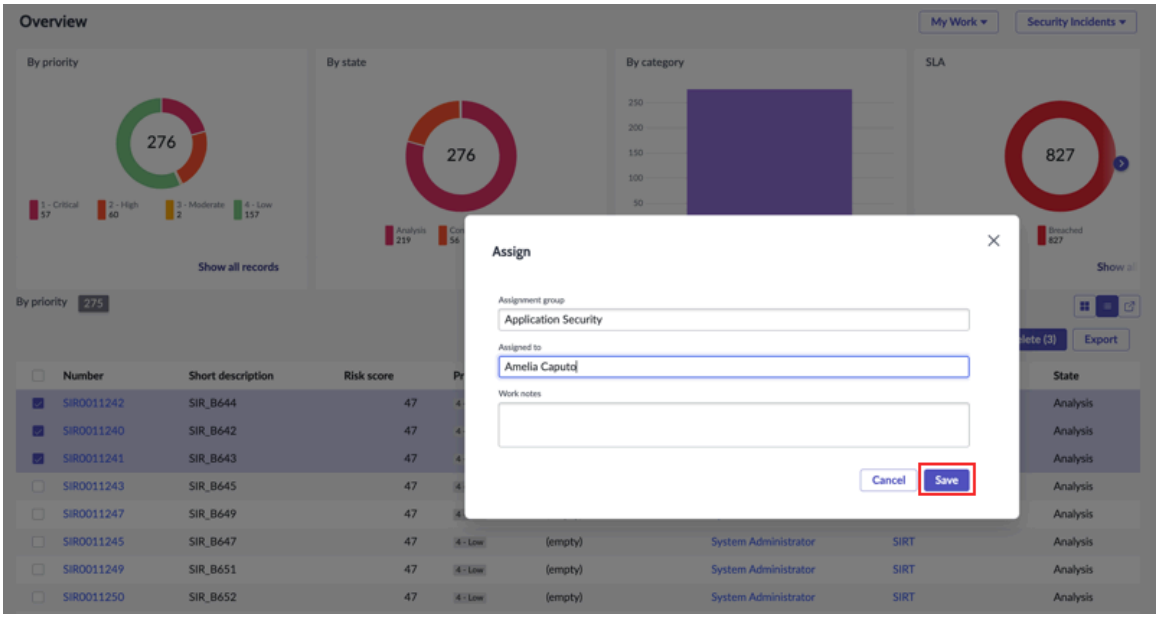
インシデントをアサイン



リストビューの例を次に示します。ユーザーは、リストビューからインシデントをアサインすることもできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インシデントをアサイン



必要に応じて、[アサイン先グループ] や [アサイン先]、[作業メモを追加] などのアサイニーの詳細を [追加] または変更します。

注:
1 つ以上のセキュリティインシデントまたは応答タスクをアサイン先グループにアサインすることができます。選択した番号が [アサイン] ボタンに表示されます。

ユーザーはこのビューからセキュリティインシデントを削除できます。[削除] ボタンをクリックしてセキュリティインシデントを削除すると、レコードがリストビューから削除されます。

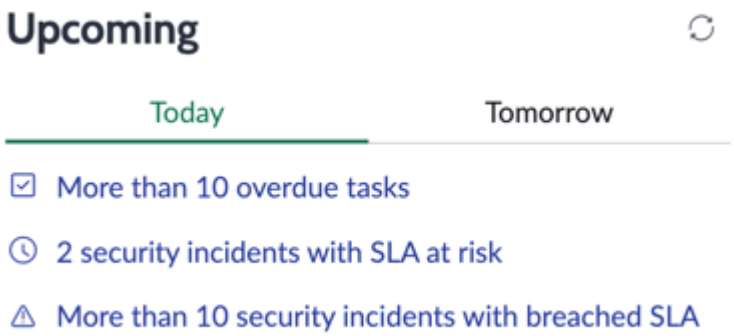
ユーザーはリストのコンテンツをエクスポートすることもできます。[エクスポート] ボタンをクリックして、リストを目的の形式でエクスポートします。

[予定] セクション

このセクションには、当日および翌日に期限切れになるセキュリティインシデントや応答タスクなどの今後のタスクが表示されます。

表示されるセキュリティインシデントと応答タスクのリストは、それらのレコードに定義された日付フィールドと SLA 定義に基づいています。

このセクションに複数のセキュリティインシデントまたは応答タスクが含まれている場合、インシデントまたはレコードはそれらのすべてのレコードを新しいタブで開きます。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

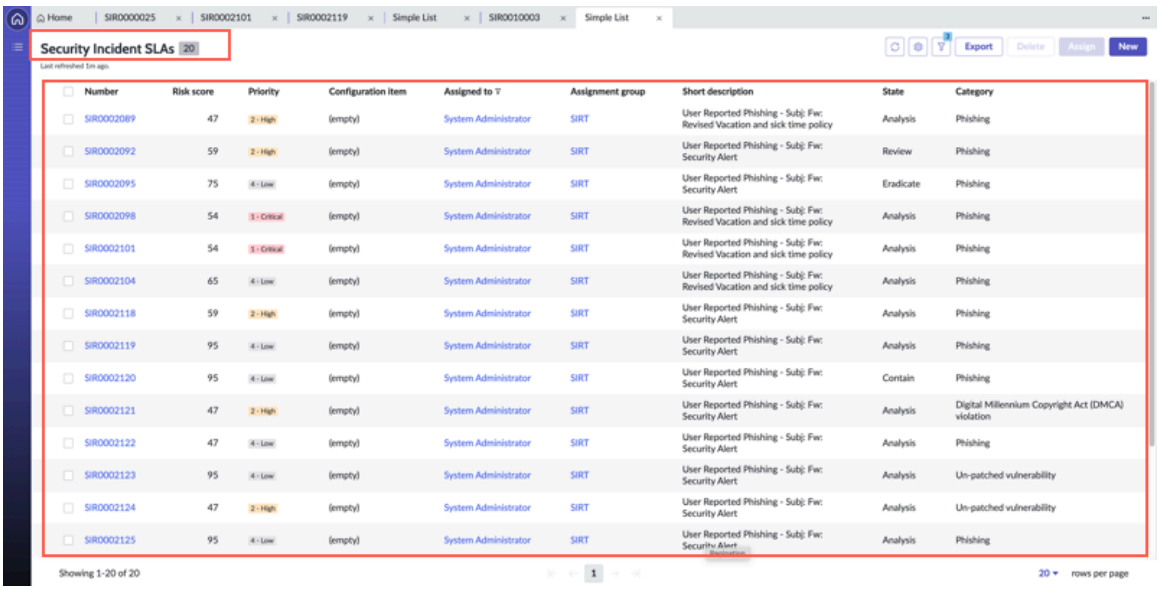
予定されているタスクの表示

セキュリティアナリストは、期限付き、期限切れ、または定義された SLA に違反しているセキュリティインシデントおよび応答タスクに関連する今後のタスクを表示できます。

始める前に
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > 予定.
2. [今日] タブをクリックすると、その日に期限が切れるタスクが表示されます。
3. [明日] タブを選択すると、次の日に期限が切れるタスクが表示されます。
   次のセクションには、期日に基づいて期限切れになり、SLA 定義に違反したセキュリティインシデントまたは応答タスクが一覧表示されます。
4. [予定] セクションのリストを更新するには、[リフレッシュ] アイコンをクリックします。
   たとえば、**[SLA** 違反がある **10** 件を超えるセキュリティインシデント **(More than 10 security incidents with breached SLA)]** リンクをクリックすると、SLA 違反のインシデントのリストがワークスペース内の新しいタブに表示されます。



> **注:**
> 任意のリストビューから、新規、アサイン、エクスポート、および削除の操作を実行できます。

[クイックリンク] セクション

クイックリンクはブックマークリンクのように機能します。外部 URL を追加して、ワークスペース内からすばやくアクセスできます。

クイックリンクの操作

簡単に参照できるようにクイックリンクを追加します。

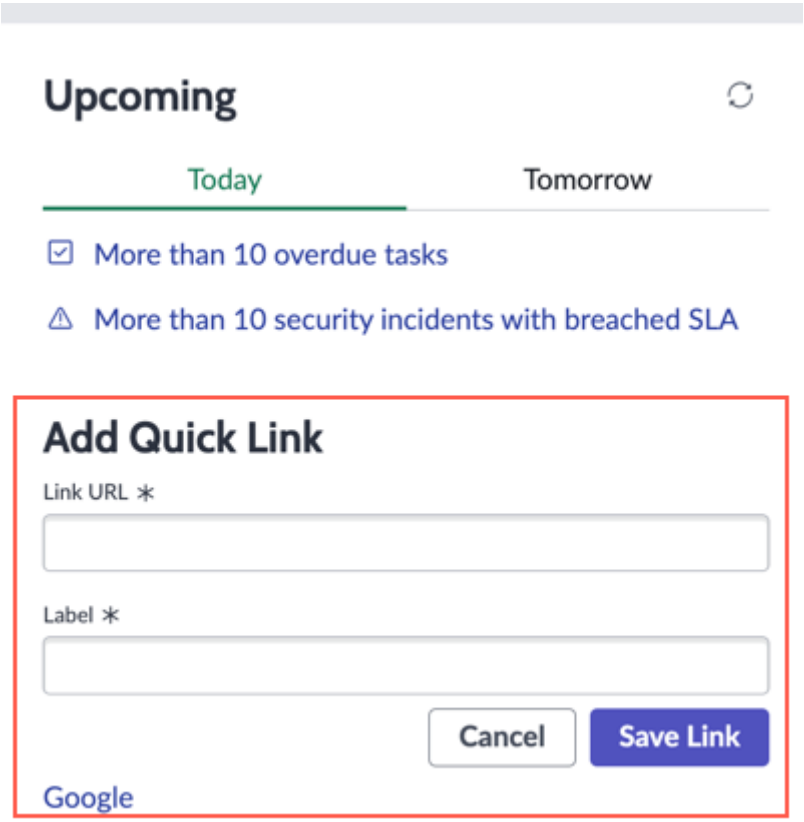
始める前に
必要なロール：sn_si.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
便利なクイックリンクを追加および変更し、インシデントの解決に役立つリンクをブックマークすることができます。

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > クイックリンク.
2. [クイックリンクを追加] アイコンをクリックしてリンクを追加します。
3. URL とラベルへのリンクを入力します。
4. [リンクを保存] をクリックします。



新しいリンクがクイックリンクのセクションの下に追加されます。

5. リンクを変更または削除するには：

   a. [リンクを編集] アイコンをクリックします。

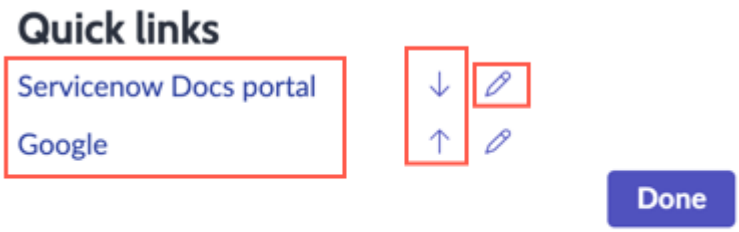
   b. URL のラベルである目的のリンクまたは表示テキストを変更します。

   c. [保存] をクリックします。

   d. [完了] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



e. 上向き矢印と下向き矢印を使用して、リンクの位置を動かします。

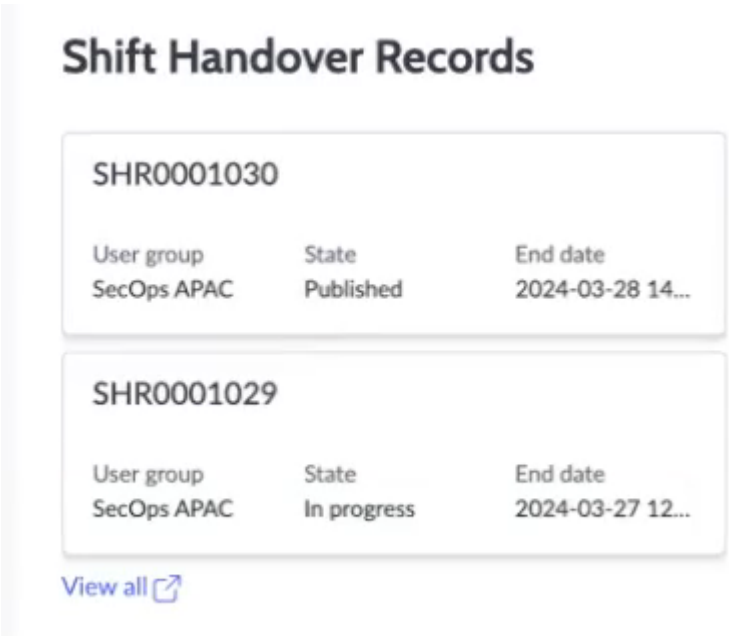
f. [削除] をクリックすると、編集中にブックマークされたリンクが削除されます。

[シフト引継ぎレコード] セクション

このセクションには、セキュリティインシデントレスポンスワークスペースのシフト引き継ぎレコードのリストが表示されます。

セキュリティインシデントレスポンスワークスペースの [シフト引き継ぎレコード] セクションには、これらのレコードに定義された [終了日]、[ステータス]、および [ユーザーグループ] フィールドに基づいて、最新の 2 つのシフト引き継ぎレコードが表示されます。すべてのシフト引き継ぎレコードを表示するには、[すべて表示] を選択します。

[シフト引継ぎレコード] セクション



SIR ワークスペース でのリストビュー

リストビューは、セキュリティインシデント、応答タスク、フィッシングメール、およびアセスメントで構成されています。

リストビューには、[自分にアサイン済み]、[チームにアサイン済み]、[未割り当て]、[オープンステータス]、[すべて] などのフィルターが事前に適用されています。

アナリストは、これらのリストカテゴリとフィルター済みリストを使用して、作業する必要があるセキュリティインシデントと応答タスクのレコードをすばやく見つけることができます。

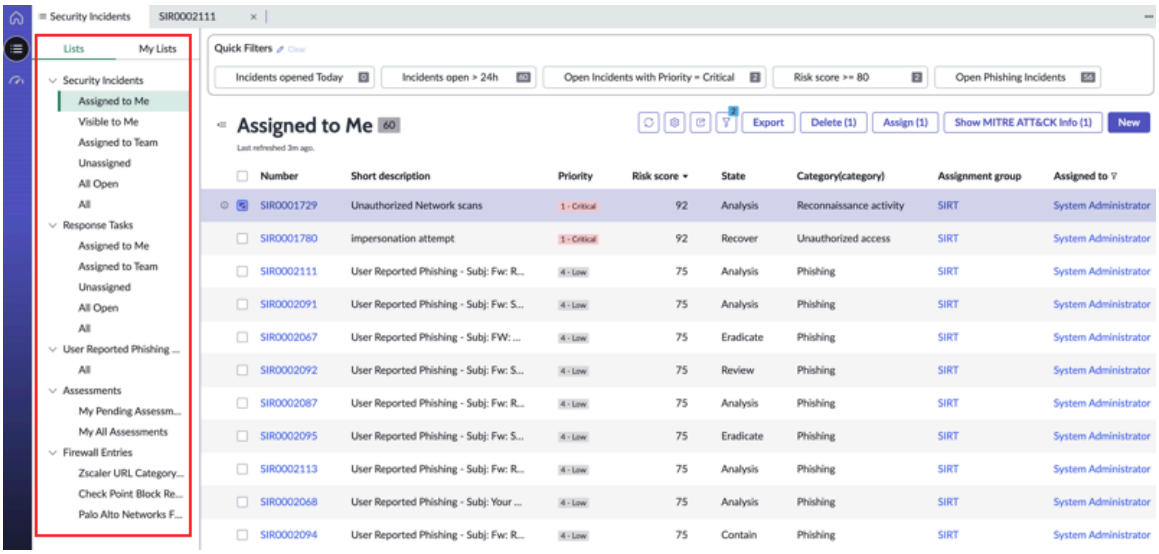
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リストビューにアクセスするには、リストアイコン ( ) をクリックする必要があります。リストビューでレコードをクリックすると、レコードが新しいタブで開きます。

リストタイプ

リストのビューの例を次に示します。



リストペインには次のセクションがあります。

リスト

リストアイテム	説明	機能
セキュリティインシデント	セキュリティインシデントのリストを表示し、目的のインシデントに移動して作業を開始します。次のリストが利用できます。 • 閲覧可能なインシデント：ログインしているユーザーに表示されるセキュリティインシデント • 自分にアサイン済み：アナリストにアサインされたセキュリティインシデント • チームにアサイン済み **(Assigned to the Team)**：アナリストが属する全チームにアサインされたセキュリティインシデント • 未割り当て：未割り当てのセキュリティインシデントのリスト	• リストビューで、アナリストはインシデント列の上にある歯車アイコンをクリックして列のリストを構成できます。 • アナリストは、1 つ以上のセキュリティインシデントを選択し、それらのインシデントを他のユーザーにアサインすることができます。 • アナリストはセキュリティインシデントを削除できます。 • アナリストは新しいセキュリティインシデントを作成できます。 • アナリストはクイックフィルターを適用できます。高度な [フィルター] オプションを使用する代わりに、[クイックフィルター] オプションをクリックしてフィルターを適用します。クイックフィルターを使用すると、緊急の対応が必要なセキュリティインシデ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リスト (続く)

リストアイテム	説明	機能
	• オープンステータス：すべてのオープンセキュリティインシデントのリスト • すべて：すべてのセキュリティインシデントのリスト。	ントのリストをすばやくフィルタリングできます。詳細については、「クイックフィルターの使用」を参照してください。 • アナリストはインシデントのリストを更新できます。 • アナリストは、リストビューを Excel 形式、CSV 形式、JSON 形式、および PDF 形式にエクスポートできます。
シフト引継ぎレコード	シフト引き継ぎレコードのリストを表示します。次のリストが利用できます。 • チームにアサイン済み **(Assigned to the Team)**：アナリストが属するすべてのチーム/ユーザーグループにアサインされているシフト引き継ぎレコード。 • すべて：すべてのセキュリティインシデントのリスト。	シフト引き継ぎは、次の 3 つのロールをサポートしています。 • admin：シフトオーナーロール • セキュリティアナリスト：シフトアナリストロール • セキュリティマネージャー：シフトオーナーロールですが、シフト引き継ぎレコードがアサインされているユーザーグループへのアクセス権がありません。 • アクティブなシフトのユーザーグループに属するシフトオーナー/アナリストロールを持つユーザーは、ドラフトステータスのシフト引き継ぎレコードでコンテンツを追加または変更できます。 • シフトオーナー/アナリストロールを持たないユーザー、またはアクティブなシフトのユーザーグループに含まれていないユーザーは、シフト引き継ぎレコードのコンテンツのみを表示できます。
対応タスク	対応タスクのリストを表示し、目的の対応タスクに移動して作業を開始します。リストビューには次のものが含まれます。	• リストビューで、アナリストはインシデント列の上にある歯車アイコンをクリックして列のリストを構成できます。 • アナリストは、1 つ以上の応答タスクを選択し、それらの

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リスト (続く)

リストアイテム	説明	機能
	• 自分にアサイン済み：アナリストにアサインされた応答タスク • チームにアサイン済み **(Assigned to the Team)**：アナリストが属するチームにアサインされた応答タスク • 未割り当て：未アサインの応答タスクのリスト • オープンステータス：すべてのオープンな応答タスクのリスト • すべて：すべての応答タスクのリスト	インシデントを他のユーザーに割り当てることができます。 • アナリストは新しい応答タスクを作成できます。 • アナリストはクイックフィルターを適用できます。高度な [フィルター] オプションを使用する代わりに、[クイックフィルター] オプションをクリックしてフィルターを適用します。クイックフィルターを使用すると、緊急の対応が必要な応答タスクのリストをすばやくフィルタリングできます。 • アナリストは応答タスクのリストを更新できます。 • アナリストは、リストビューを Excel 形式、CSV 形式、JSON 形式、および PDF 形式にエクスポートできます。詳細については、「セキュリティインシデントまたは応答タスクのエクスポート」を参照してください。
フィッシングメール	すべてのフィッシングメールのリストを表示します。リストビューは最終更新日時に基づいてソートされます。	• フィッシングメールを報告します。詳細については、「フィッシングメールを報告」でフィッシングメールを報告する方法を参照してください。 • フィッシングメールを削除します。 • フィッシングメールのリストビューを Excel 形式、CSV 形式、JSON 形式、および PDF 形式でエクスポートします。
アセスメント	インシデントの事後レビューを行うために必要なアセスメントのリストを表示します。	アセスメントを実施します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リスト (続く)

リストアイテム	説明	機能
	• 自分の処理待ちのアセスメント：処理待ちのアセスメントのリスト • 自分のすべてのアセスメント：すべてのアセスメントのリスト	

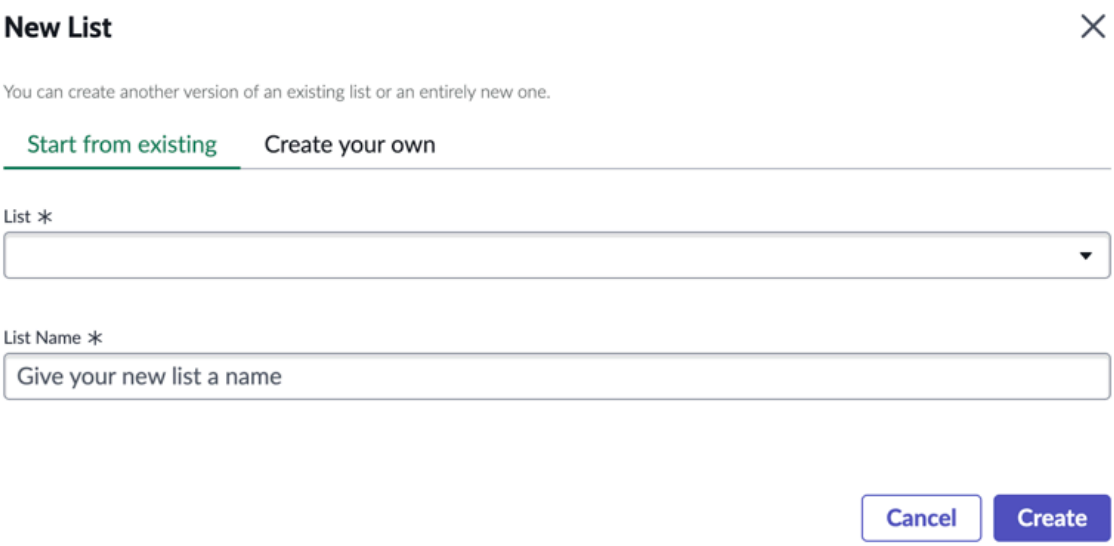
リストのカスタマイズ

セキュリティアナリストまたはマネージャーは、個々の設定に基づいて、セキュリティインシデントまたは応答タスク、フィッシングメールのカスタムリストビューをカスタマイズできます。

始める前に
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. [リストビュー] をクリックします。
3. クリックします マイリスト.
4. [自分のリスト **(My Lists)**] ビューの下部にある [新しいリストを追加] をクリックします。



セキュリティアナリストは、既存のリストの別のバージョンまたはカスタマイズしたまったく新しいリストのいずれかを作成できます。

5. 既存のリストビューから作成するには：

   a. [既存リストから作成] リンクをクリックします。

   b. ドロップダウンリストから [リスト] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

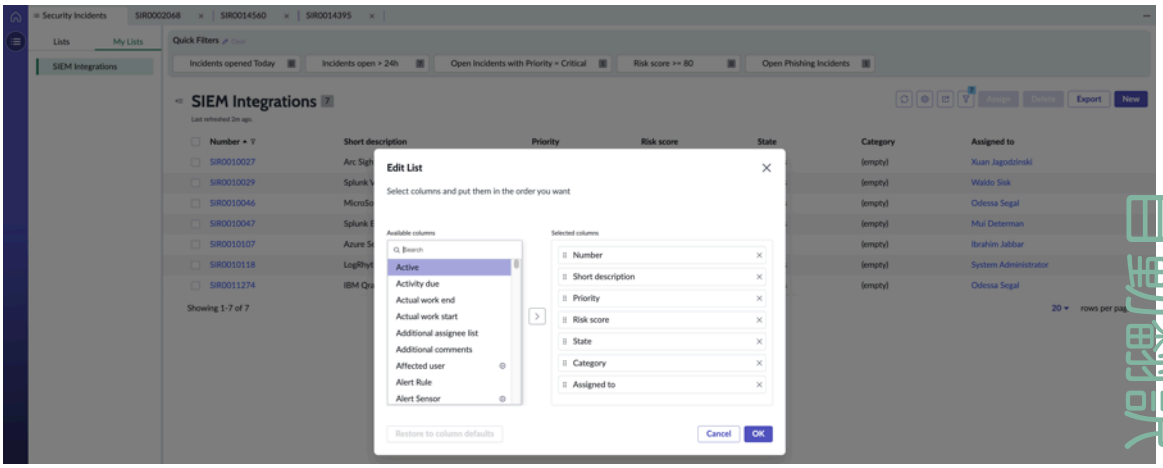
> **注:**
> ドロップダウンリストからどのリストを選択しても、リスト名はメインリストのコピーとなります。たとえば、[セキュリティインシデント] セクション内で [自分にアサイン済み] を選択した場合、リスト名は [セキュリティインシデント] セクションの [自分にアサイン済みコピー **(Assigned to Me Copy)]** になります。

c. カスタマイズする列を選択し、フィルターを追加します。
フィールド、演算子、および値を含む条件を追加して、フィルターを作成します。

d. [作成] をクリックします。

> **注:**
> カスタム列やフィルターを追加し、条件を設定して、必要に応じて順序をソートすることで、独自のリストビューをカスタマイズすることができます。

e. カスタマイズされたリストビューを作成したら、歯車アイコンをクリックし、[列を編集] オプションを選択して列を編集し、希望する順序に配置します。



以下も実行できます。

- カスタマイズしたリストビューで [名前の変更] を行います。
- カスタマイズしたリストビューを [削除] します。
- [名前を付けて保存] オプションを使用して、カスタマイズしたリストビューを必要に応じて保存します。
- リストビューの [幅をリセット] します。

> **注:**
> 提供されているリストビューのアサイン、削除、エクスポートなどの他の [アクション一覧] ボタンを使用して、これらの操作を直接実行することもできます。

6. 独自のリストを作成するには：

a. [独自に作成する] リンクをクリックします。

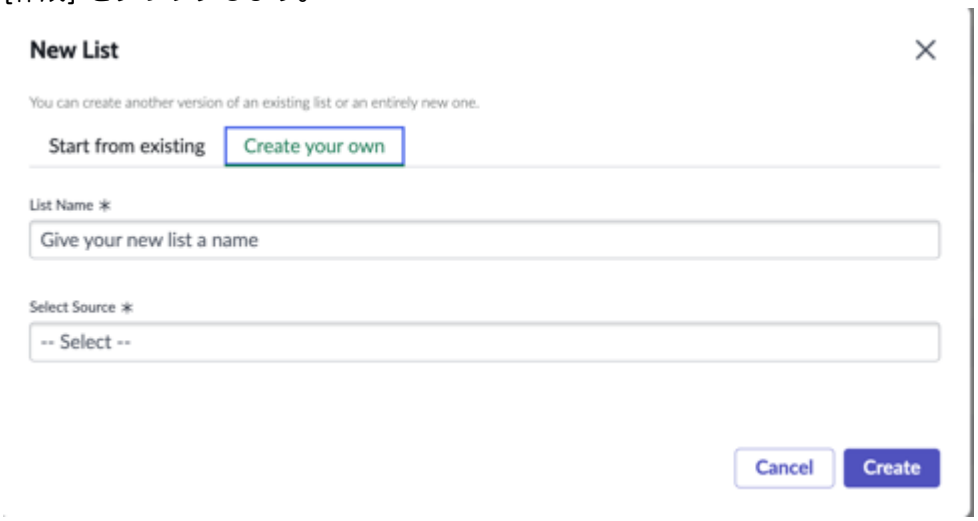
b. [リスト名] を入力します。

c. [ソース] および [列] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

d. フィルターを追加します。
条件を追加してフィルターをビルドし、リストを表示する順序を指定します。

e. [作成] をクリックします。



[自分のリスト **(My Lists)**] セクションの下に、定義およびカスタマイズした新しいリストが作成されます。

> **注:**
> 位置を移動することで、カスタマイズしたビューの順序を変更することができます。

セキュリティインシデントのアサイン

セキュリティインシデントをアサインします。

始める前に

必要なロール：sn_si.basic

手順

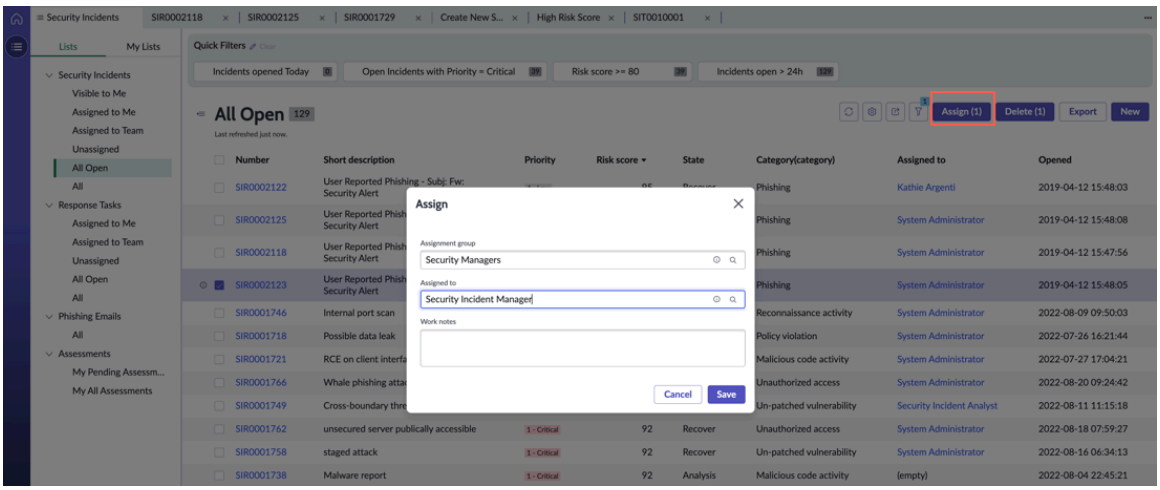
1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. リスト ( ) アイコンをクリックします。
3. [リスト] をクリックします。
4. たとえば、 セキュリティインシデント > オープンステータス.
5. セキュリティインシデントを 1 つ以上選択します。
6. [アサイン] をクリックします。
7. 必要に応じて、[アサイン先グループ] や [アサイン先]、[作業メモを追加] などの詳細を入力します。
   その後、インシデントがユーザーにアサインされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

8. [保存] をクリックします。

セキュリティインシデントを 1 つ以上アサインします。



応答タスクのアサイン

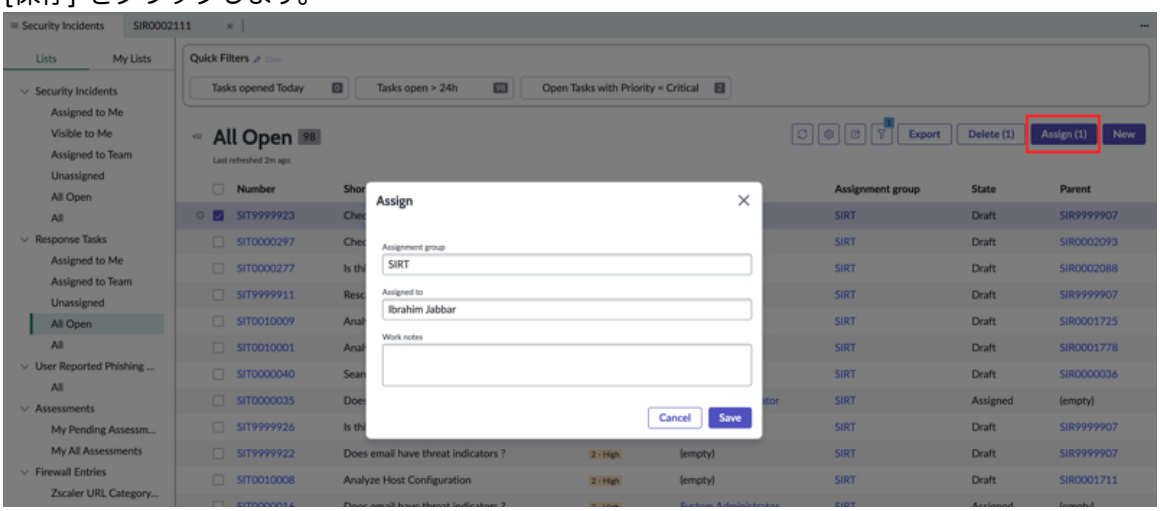
セキュリティ上の問題に応答タスクをアサインします。

始める前に

必要なロール：sn_si.basic

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. リスト ( ) アイコンをクリックします。
3. [リスト] をクリックします。
   たとえば、 対応タスク > オープンステータス.
4. 1 つ以上の応答タスクを選択します。
5. [アサイン] をクリックします。
6. 必要に応じて、[アサイン先グループ] や [アサイン先]、[作業メモを追加] などの詳細を入力します。
   その後、インシデントがユーザーにアサインされます。
7. [保存] をクリックします。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

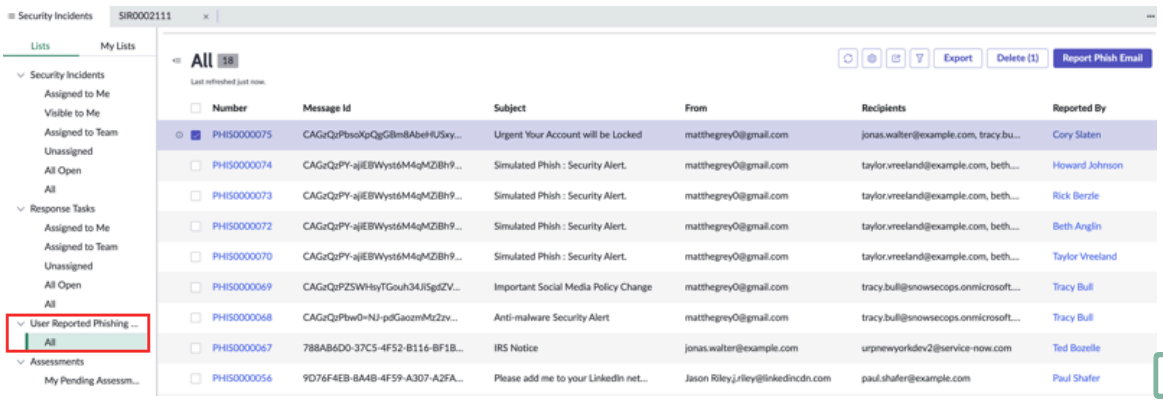
フィッシングメールを報告

リストビューからフィッシングメールを報告します。

始める前に
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. リスト ( ) アイコンをクリックします。
3. 検索項目 ユーザーから報告されたフィッシングメール > **All** (すべて).
   ユーザーから報告されたフィッシングメールのリストが表示されます。



4. [フィッシングメールを報告] ボタンをクリックします。
   フィッシングメールをアップロードして報告します。
5. [ファイルを追加] をクリックして添付ファイルを追加します。
6. [アップロード] をクリックします。

> **注:**
> 添付ファイルをアップロードしてフィッシングメールを報告します。報告できるフィッシングメールは一度に 1 つのみです。.eml 形式である必要があります。

7. [送信] をクリックします。
   セキュリティインシデントをログに記録するフィッシングメールが作成されます。

クイックフィルターの使用

クイックフィルターは、セキュリティインシデントおよび応答タスクのリストで利用可能な、簡単にアクセスできるフィルターです。

始める前に
必要なロール：sn_si.admin

SIR ワークスペース には、セキュリティインシデントまたは応答タスクのリストを簡単にフィルタリングできるクイックフィルター機能があります。

クイックフィルターを使用すると、新しいフィルターを設定したり、これらのリストに対して表示される既存のフィルターを変更したりすることができます。ベースシステムには、セキュリティインシデントごとに次のクイックフィルターが用意されています。

- 今日オープンされたインシデント
- **24** 時間を超えてオープン状態のインシデント **(Incidents open > 24hrs)**

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 優先度が [最重要] のオープンインシデント
- リスク **>= 80 (Risk >= 80)**
- オープンフィッシングインシデント **(Open Phishing Incidents)**

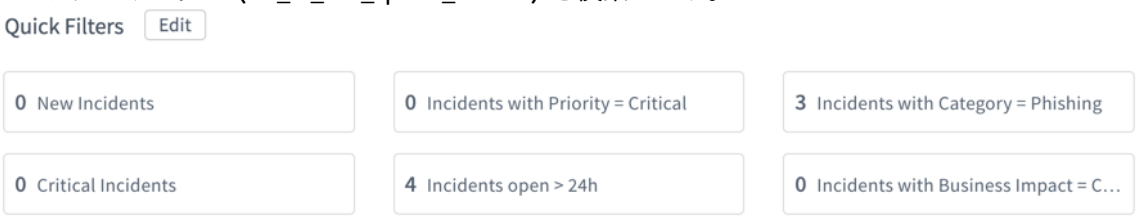
ベースシステムでは、応答タスクごとに次のクイックフィルターが用意されています。

- **24** 時間を超えてオープンになっているタスク **(Tasks open > 24h)**
- 優先度が [最重要] のオープンタスク **(Open Tasks with Priority = Critical)**

> **注:**
> アドミニストレーターは、組織のニーズに応じて必要なクイックフィルターのリストを設定できます。

手順

1. 次のように移動する。 システム定義 > テーブル.
2. クイックフィルター (sn_si_aw_quick_filters) を検索します。



3. 検索項目 関連リンク > リストを表示 節。
   [クイックフィルター] リストページが表示されます。以下は、アプリケーションに含まれているすぐに利用可能なクイックフィルターのリストです。

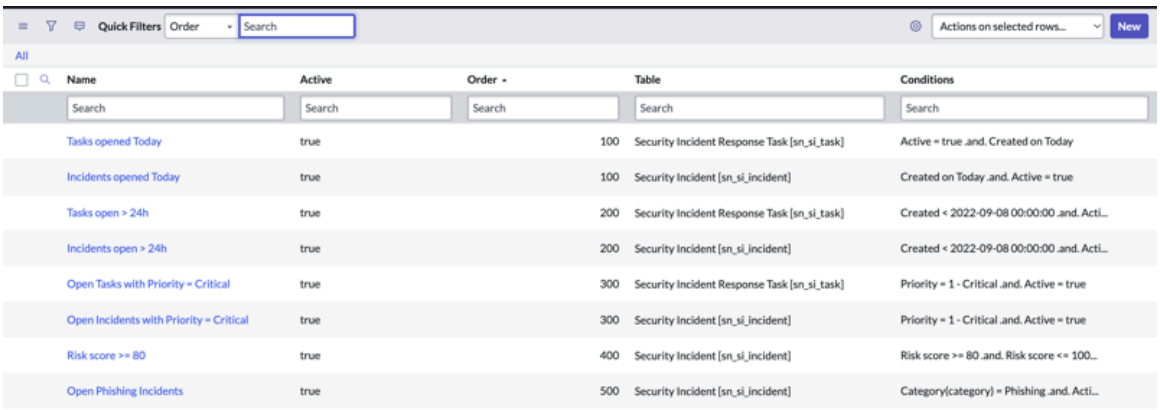
名前	テーブル	値
本日オープンされたタスク	セキュリティインシデントタスク [sn_si_task]	true
今日オープンされたインシデント	セキュリティインシデント [sn_si_incident]	true
24 時間を超えてオープンになっているタスク (Tasks open > 24h)	セキュリティインシデントレスポンスタスク [sn_si_task]	true
24 時間を超えてオープン状態のインシデント	セキュリティインシデント [sn_si_incident]	true
優先度が [最重要] のオープンタスク (Open Tasks with Priority = Critical)	セキュリティインシデントレスポンスタスク [sn_si_incident]	true
優先度が [最重要] のオープンインシデント	セキュリティインシデント [sn_si_incident]	true
リスクスコア >= 80 (Risk score >= 80)	セキュリティインシデント [sn_si_incident]	true
オープンフィッシングインシデント (Open Phishing Incidents)	セキュリティインシデント [sn_si_incident]	true

自動翻訳

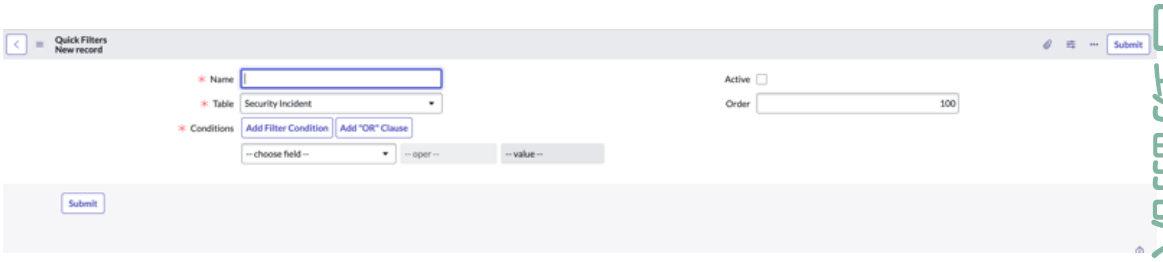
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
続いてセキュリティアドミンはこれらのクイックフィルターを設定することもできます。アドミニストレーターは、ビジネスニーズに応じて既存の値を false に変更し、新しいクイックフィルターを作成できます。

クイックフィルター



4. [新規] をクリックして新しいフィルターを作成します。
5. フィルターの名前を入力し、[テーブル] を選択してフィルター条件を指定します。
6. [送信] をクリックして、前のリストページに戻ります。
   新しく追加したフィルターがページのリストに表示されます。



注:

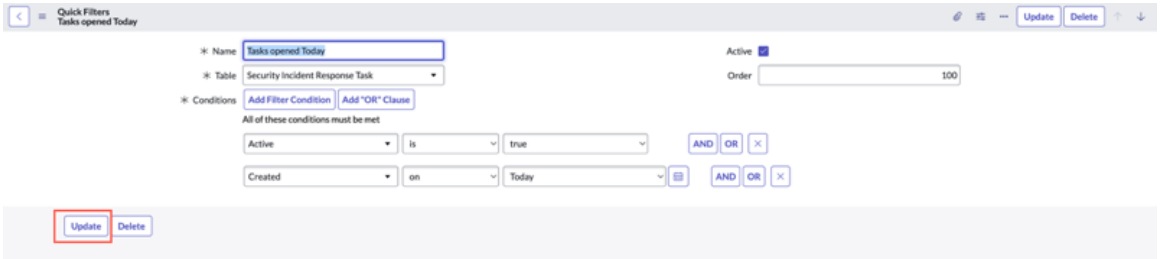
- クイックフィルターは、[アクティブ] チェックボックスがオンになっている場合にのみ適用されます。
- ログインユーザーは、アプリケーションで利用可能なアクティブなクイックフィルターをワークスペース内でカスタマイズできます。ユーザーは、新しく作成されたクイックフィルターを非表示にしたり再表示したりすることができます。この機能はユーザー設定に基づいています。
- ユーザーがクイックフィルターの環境設定を変更した後に新しいクイックフィルターが作成された場合、クイックフィルターがアクティブに設定されていると、ユーザーの環境設定には適用されません。ユーザーはカスタマイズされたビューで環境設定を手動で変更する必要があります。

7. 既存のクイックフィルターを変更するには、既存のフィルターレコードを選択します。
8. 名前とフィルター条件を変更します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

9. [更新] をクリックします。

クイックフィルター



クイックフィルターの追加または変更

リストビュー内のセキュリティインシデントまたは応答タスクのクイックフィルターを追加または変更します。

始める前に

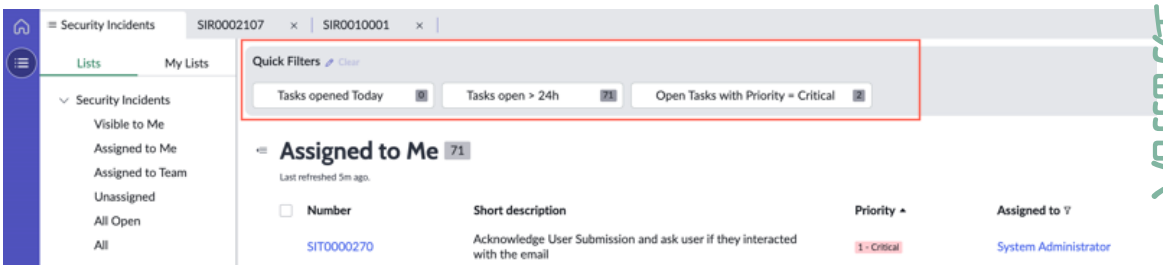
必要なロール：sn_si.basic

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.

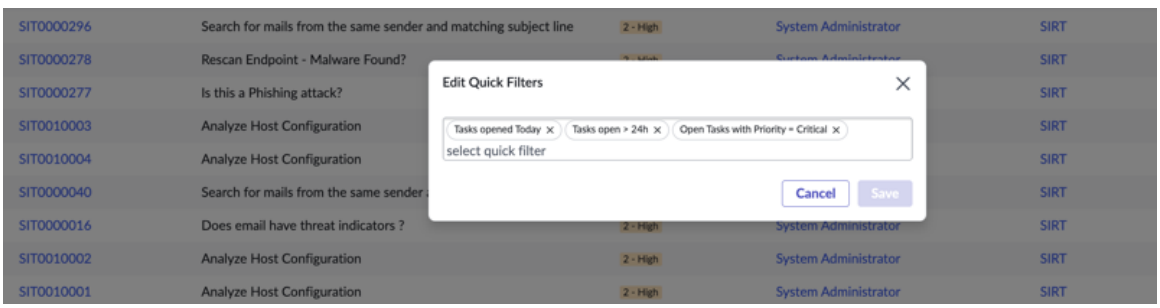
2. リスト ( ) アイコンをクリックします。

3. たとえば、 **Lists** (リスト) > セキュリティインシデント > クイックフィルター 節。



4. [編集] アイコンをクリックして変更します。

> **注:**
> 行った変更は保持され、ユーザーが次回このページに戻ったときに、保持された環境設定が表示されます。



5. [保存] をクリックします。

セキュリティインシデントまたは応答タスクのエクスポート

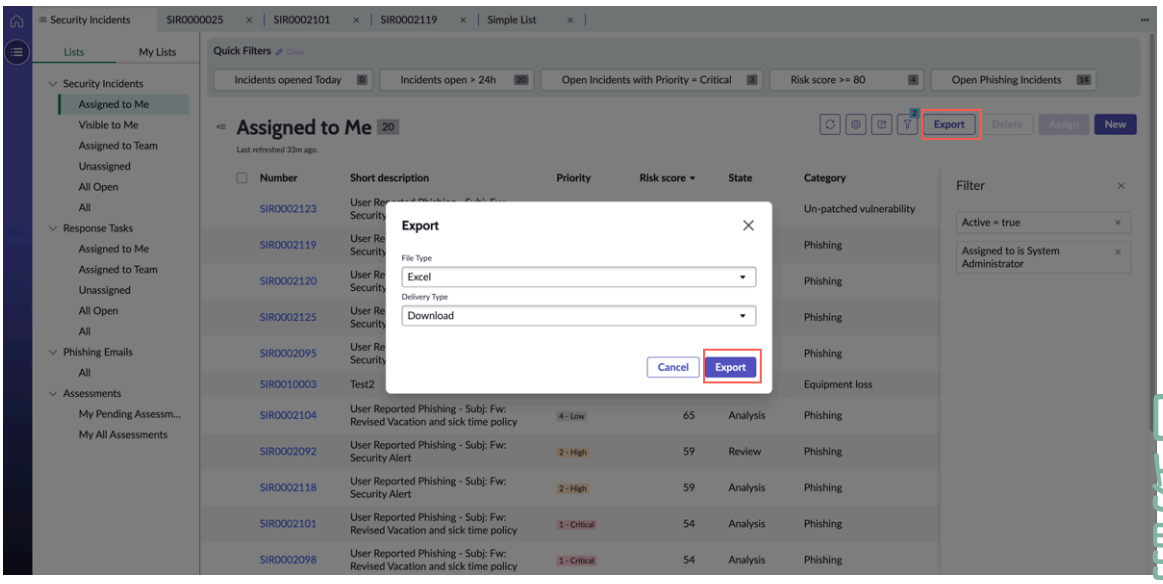
セキュリティインシデントまたは応答タスクをリストビューからエクスポートします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. リスト のアイコンをクリックします。
3. [リスト] をクリックします。
4. 検索項目 セキュリティインシデントまたは応答タスク > オープンステータス.
5. リストを表示し、[エクスポート] をクリックします。



6. [ファイルタイプ] と [デリバリタイプ] を選択します。
   たとえば、**[Excel]** でリストを [ダウンロード] するか [メール] で送信します。
7. [エクスポート] をクリックします。
   選択したオプションに応じて、ファイルがダウンロードまたはメールで送信されます。

シフト引き継ぎレコードの管理

シフト引き継ぎレコードのリストビューを使用して、シフト引き継ぎレコードを作成、編集、コピー、または削除します。各シフト引き継ぎレコードは、シフト引き継ぎレポートテンプレートに関連付けられています。

始める前に
必要なロール：

- sn_escm_sh.shift_analyst：シフト引き継ぎレコードにアクセスするための最小要件。
- sn_escm_sh.shift_owner：シフトオーナーが属するユーザーグループの引き継ぎログレコードを作成、編集、削除します。このロールは sn_escm_sh.shift_analyst ロールを継承します。
- sn_escm_sh.shift_analyst：すべてのシフト引き継ぎログレコードを表示しますが、シフトアナリストのグループにアサインされた進行中のシフト引き継ぎレコードにのみ寄与できます。
- sn_si.analyst - sn_escm_sh.shift_analyst ロールを継承します。
- sn_si.admin - sn_escm_sh.shift_admin ロールを継承します。
- sn_escm_sh.shift_admin - sn_escm_sh.shift_owner ロールを継承します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重要:
管理者としてシフト引き継ぎテンプレートを構成する方法については、「シフト引き継ぎテンプレートを構成する」を参照してください。

このタスクについて

シフトオーナーとそれぞれのチームまたはユーザーグループが、シフト引き継ぎログレコードを作成します。シフトオーナーは、シフト引き継ぎレポートで作業するシフト引き継ぎテンプレートとユーザーグループを選択する必要があります。シフト引き継ぎレポートが完了すると、次にアクティブなシフトオーナーおよびチームと共有されます。

シフト引き継ぎテンプレートの重要なポイント：

- アクティブなシフトチームの他のアナリストが自分より先にレポートを更新しており、変更が処理されている場合は、保留中のコンテンツ更新があることを示すエラーメッセージが表示されることがあります。30 秒待ってから、もう一度 [ステータスを「レビュー」に変更 **(Change to "Review" state)]** を選択する必要があります。右側のペインの統合レポートが、他のアナリストの更新内容で更新されているのを確認できます。
- シフトオーナーが [レビュー] ステータスのセクションのコンテンツを変更した場合、レコードが [進行中] ステータスに戻ると、同じコンテンツがアナリストに反映されます。
- シフトオーナーは、[レビュー] ステータスのコンテンツを編集したり、2 つの行の結合、2 つのセクションの結合、セクションの削除などのアクションを実行したりすると、他のアナリストのシフト引き継ぎレポートに影響するため注意する必要があります。
- シフト引き継ぎレポートを公開した後、シフトオーナーはコンテンツを変更できますが、レコードのステータスを変更することはできません。
- 誰かがコンテンツを変更しているときに、その間にレコードのステータスが [進行中] から [レビュー] に変更されると、未保存のコンテンツの変更は破棄されます。
- シフト管理者は、ユーザーグループに関係なく、すべてのシフト引き継ぎログレコードへの書き込みアクセス権を持ちます。

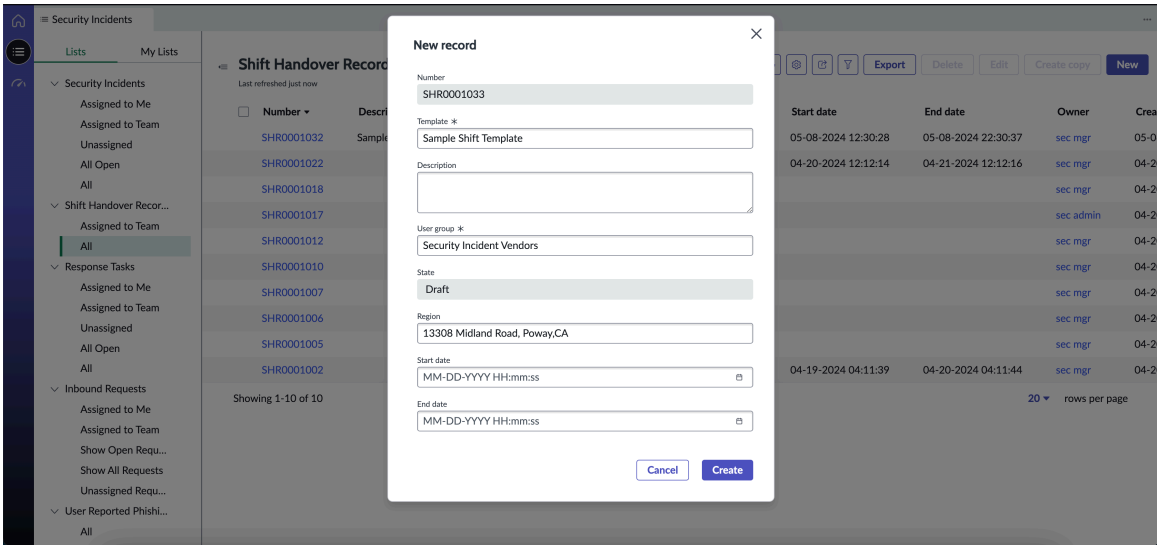
手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. セキュリティインシデントリスト アイコンを選択します。
3. [リスト] タブで、[シフト引き継ぎレコード **(Shift Handover Records)]** を選択します。
4. [すべてのレコード] を選択して、すべてのシフト引き継ぎレコードのリストを表示します。
5. [チームにアサイン済み **(Assigned to Team)]** を選択して、アナリストが属するすべてのチーム/ユーザーグループにアサインされているシフト引き継ぎレコードのリストを表示します。
6. 新しいシフト引き継ぎレコードを作成するには、[新規] を選択します。
7. フォームの各フィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

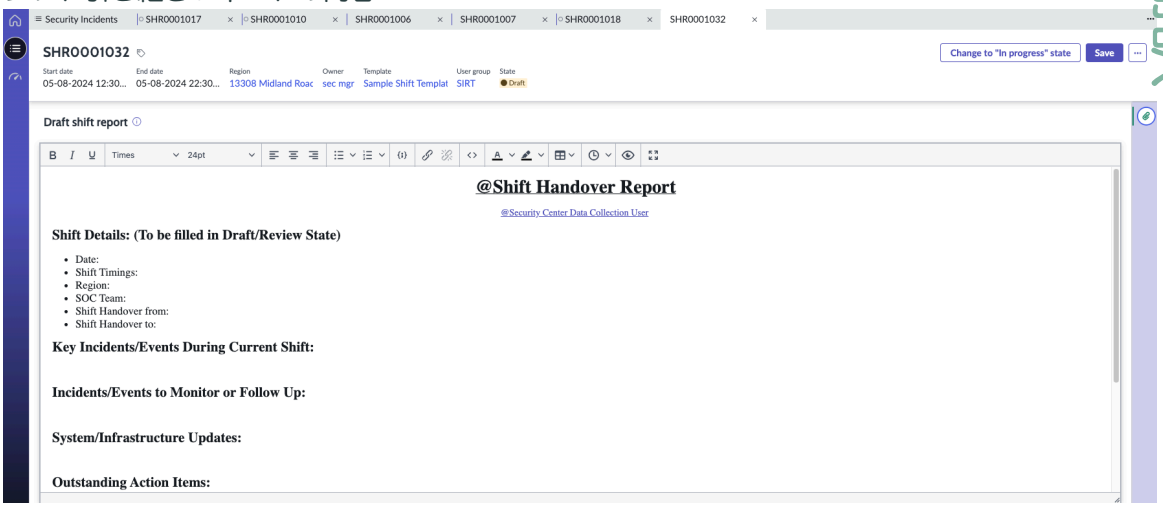
シフト引き継ぎレコードの作成



8. [作成] を選択します。
   新しいシフト引き継ぎレコードは、選択してリストビューに追加したテンプレートに基づいて作成されます。
9. 新しいシフト引き継ぎレコードを開いて、シフト引き継ぎレポートのセキュリティインシデントのステータスと詳細を更新します。
   デフォルトでは、シフト引き継ぎレコードは [ドラフト] ステータスです。

   注:
   コンテンツを変更できるのはシフトオーナーのみです。

シフト引き継ぎレポートの内容



10. ドラフトシフトレポートエディターで、[シフト引き継ぎレポートテンプレート (Shift Handover report template)] セクションを使用して、セキュリティインシデントとユーザーの詳細を更新します。

    エディターのすべてのオプション (フォント、色、箇条書き、リンク、添付ファイルなど) を使用してレポートを書式設定できます。

    注:
    シフトオーナーとシフトアナリストはどちらもコンテンツを変更できます。

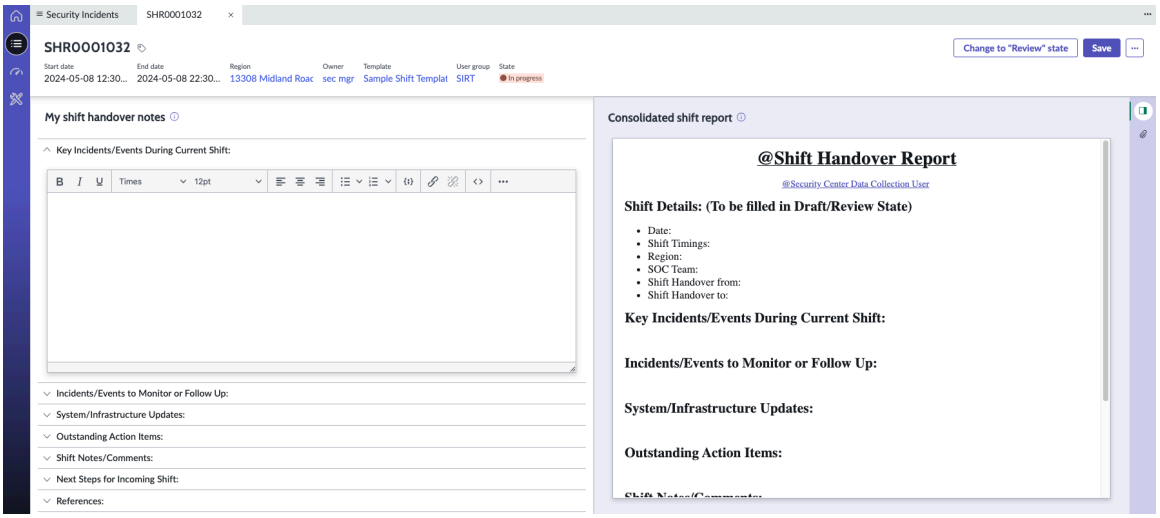
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. シフト引き継ぎレポートに必要な変更を加えた後、[保存] を選択します。

b. [ステータスを「進行中」に変更 **(Change to "In-progress" state)]** アクションを選択して、シフト引き継ぎレコードを [進行中] ステータスに移行します。

シフト引き継ぎが進行中

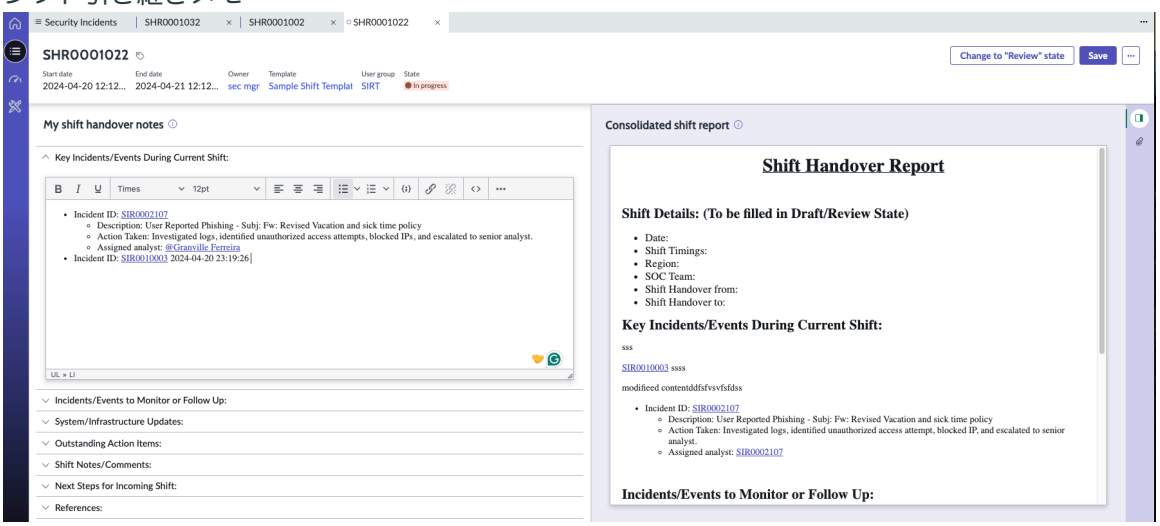


11. 自分のシフト引き継ぎメモエディターで、セキュリティインシデントやユーザーの詳細など、すべてのセクションに必要な詳細を更新します。

> **注:**
> シフトオーナーとシフトアナリストはどちらもコンテンツを変更できます。

a. エディターで特定のレコードを指定するには、**/** を使用して [レコードを選択 **(Select a record)]** を選択し、ポップアップ表示されるテーブルのリストからレコードを選択します。
たとえば、[セキュリティインシデント] レコードを選択すると、セキュリティインシデントのリストが表示されます。リストからセキュリティインシデント (**SIR0010025**) を選択し、必要なシフト引き継ぎの詳細を更新します。セキュリティインシデント番号の後に **/** を使用して、簡単な説明やウォッチリストなどのセキュリティインシデントに関連付けられたフィールドを指定することもできます。

シフト引き継ぎメモ



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

b. エディターで特定のユーザーをメンションするには、**/** を使用して [ユーザーを選択 **(Select a user)]** を選択し、ポップアップ表示されるリストからユーザーを選択します。

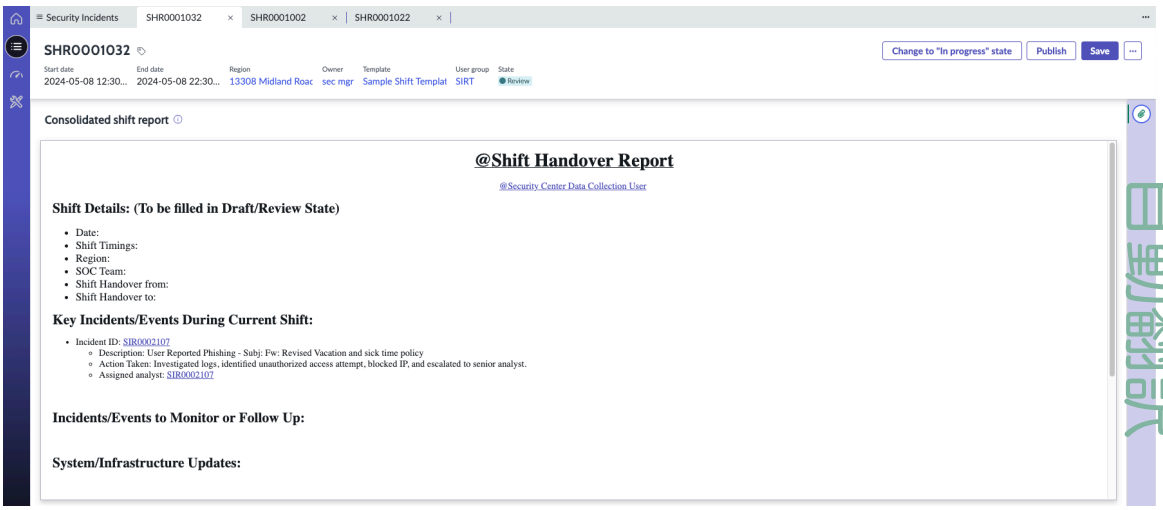
c. エディターのすべてのオプション (フォント、色、箇条書き、リンク、添付ファイルなど) を使用してレポートを書式設定できます。

d. シフト引き継ぎメモに必要な変更を加えた後、[保存] を選択します。

e. シフト引き継ぎレコードを [レビュー] ステータスに移行するには、[ステータスを「レビュー」に変更 **(Change to "Review" state)]** アクションを選択します。

> **注:**
> アクティブなシフトチームの他のアナリストが自分より先にレポートを更新していて、変更が処理されている場合は、エラーメッセージが表示されることがあります。数秒待ってから、もう一度 [ステータスを「レビュー」に変更 **(Change to "Review" state)]** を選択する必要があります。

シフト引き継ぎのレビュー



12. 統合シフトレポートで、シフト引き継ぎレポートを確認し、必要な変更を加えます。

> **注:**
> コンテンツを変更できるのはシフトオーナーのみです。

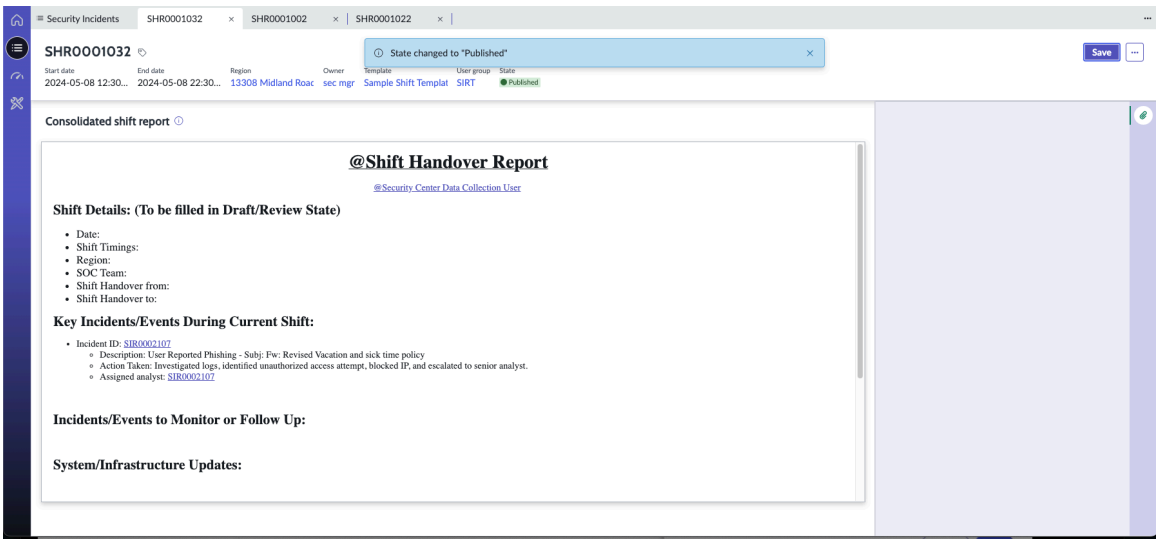
a. シフト引き継ぎメモに必要な変更を加えた後、[保存] を選択します。

b. シフト引き継ぎレポートでアナリストによる更新がさらに必要な場合は、[ステータスを「進行中」に変更 **(Change to "In-progress" state)]** を選択できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

c. [公開] アクションを選択して、シフト引き継ぎレポートを公開します。

シフト引き継ぎ公開



13. [保存] を選択して、シフト引き継ぎレポートを保存します。
保存すると、最新の更新を含むシフト引き継ぎレポートのプレビューが [プレビュー] ペインに表示されます。

> **注:**
> シフト引き継ぎレポートで行った更新はすぐにプレビューできますが、他のアナリストが変更を確認するまでに数秒かかる場合があります。

14. シフトオーナーは、[シフト引き継ぎ] リストビューで次のアクションを実行することもできます。

a. 既存のシフト引き継ぎレコードを編集するには、レコードを選択して [編集] アクションを選択します。
変更できるのは、[開始時間]、[終了時間]、[説明]、および [地域] のみです。

b. シフト引き継ぎレコードのコピーを作成するには、レコードを選択し、[コピーを作成] アクションを選択します。

c. 既存のシフト引き継ぎレコードを削除するには、レコードを選択して [削除] アクションを選択します。

SIR ワークスペースの構成

このセクションでは、セキュリティインシデントレスポンスワークスペース を操作するために必要な設定について説明します。

SIR レコードのビューの設定

このセクションでは、簡単に操作できるように、関連リストが SIR の [関連レコード] タブでどのようにグループ化されて表示されるかについて説明します。

ワークスペースユーザーは、関連リストを名前でも簡単に検索することができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SI 設計時調査の設定

このセクションを使用して、セキュリティインシデント設計時の調査ページを設定し、セキュリティインシデントレスポンスワークスペース 内に複数のエントリーポイントとその関連レコードを追加します。

必要なロール：sn_si.admin

セキュリティインシデントレスポンスワークスペース の調査ページを設定する手順の詳細を次に示します。

- 関連情報テーブルのビューの作成
- エントリーポイントリストの追加
- 関連情報ビューのエントリーポイントリストへのマッピング
- ビューから各関連リストを設定してランタイムデータのレンダリングを処理する

関連情報

調査キャンバスの詳細

関連情報テーブルのビューの作成

調査画面では、セキュリティインシデントに対して作成された関連リストビューを活用して、関連リストを構成します。

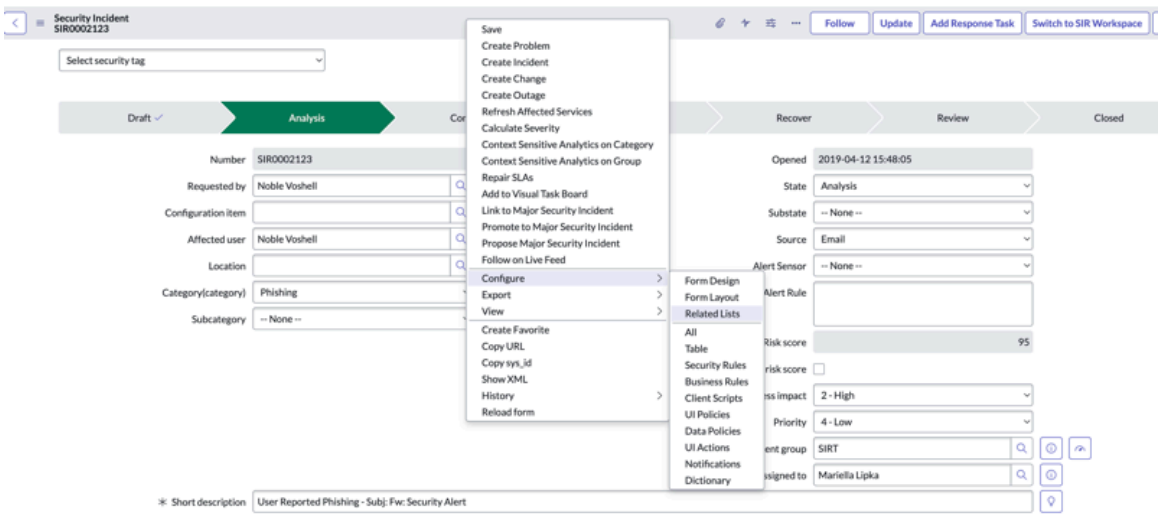
始める前に

必要なロール：sn_si.admin

ビューを作成し、それに関連リストを追加する手順は次のとおりです。

手順

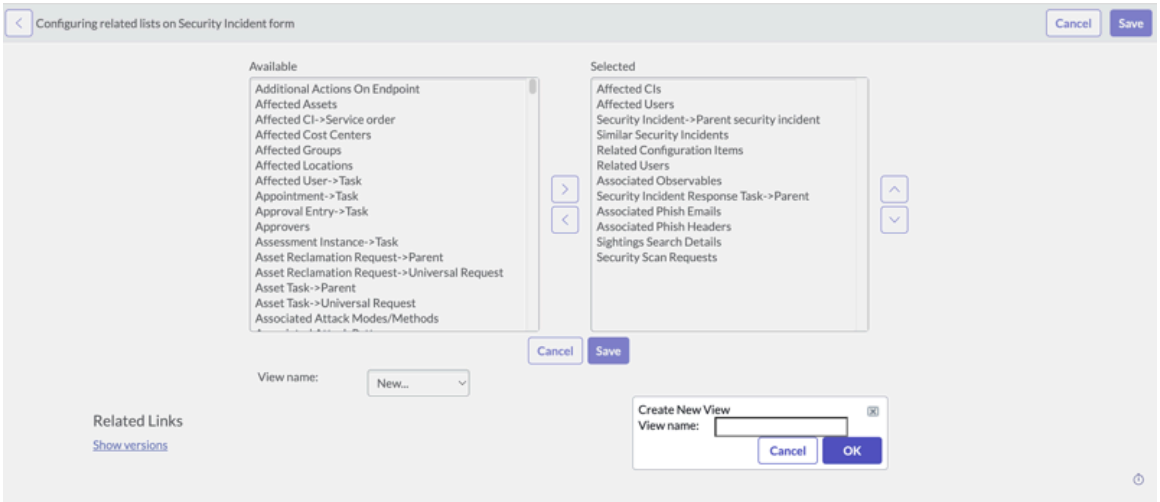
1. [セキュリティインシデント] リストに移動します。
2. クラシック UI でセキュリティインシデントを開きます。
3. フォームコンテキストメニューから、 構成 > 関連リスト.
   スラッシュバケットウィンドウが表示されます。



4. [ビュー名] ドロップダウンリストに移動し、[新規] をクリックして新しいビューを作成します。
   ビューに名前を追加する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. 新しく作成されたビューの下の右側のバケットに目的の関連リストを追加し、ビューを保存します。
   このビューは、[調査] タブに関連情報を表示するために使用されます。

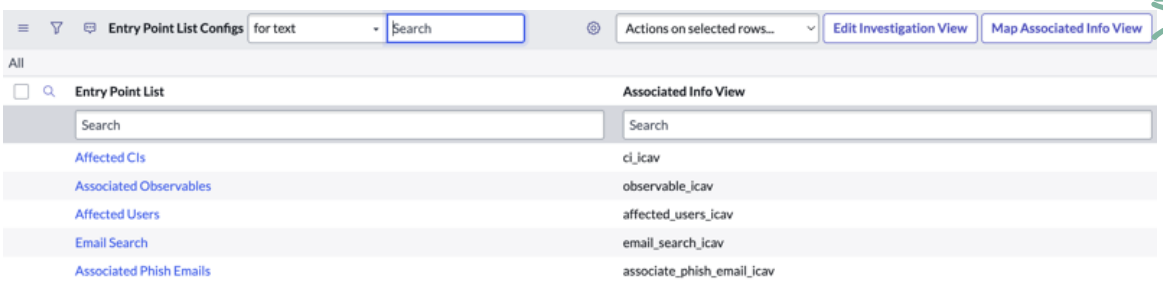
エントリーポイントリストの追加

新しいエントリーポイントリストを構成して、調査ページに追加します。

始める前に
必要なロール：admin

手順

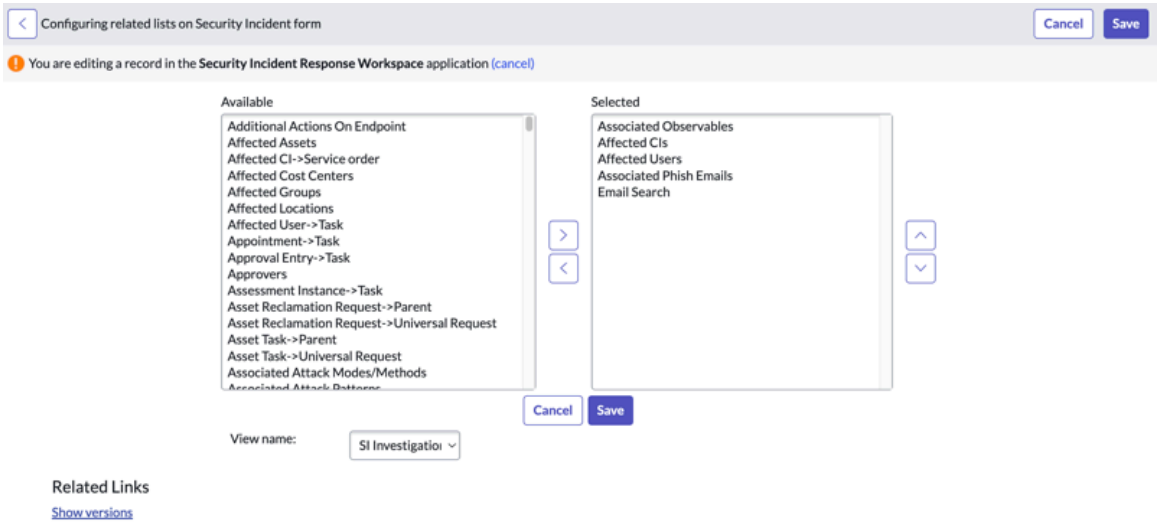
1. 次のように移動する。 **sn_si_aw_entry_point_config.list**.
   [エントリーポイントリスト構成 **(Entry Point Lists Configs)]** ページが表示されます。



2. [調査ビューを編集] ボタンをクリックして、エントリーポイントリストを調査画面に追加します。
   [セキュリティインシデントフォームでの関連リストの構成 **(Configuring related lists on Security Incident form)]** が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. スラッシュバケットビューでエントリーポイントリストを追加または削除します。
4. [保存] をクリックします。

> **注:**
> エントリーポイントリストを保持する [調査] 画面に対応するビューは **[SI** 調査ビュー] と呼ばれ、[調査ビューを編集] ページに移動するとデフォルトで選択されます。
>
> エントリーポイントリストが調査キャンバスに表示される順序は、スラッシュバケットの選択済みビューでの順序によって決まります。

関連情報ビューのエントリーポイントリストへのマッピング

[関連情報ビューをマップ] アクションを使用して、関連情報ビューを新しく追加されたエントリーポイントリストにマッピングします。

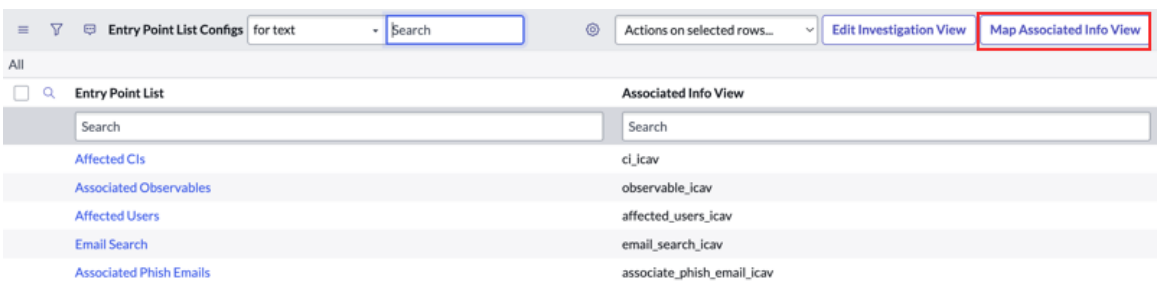
始める前に

> **注:**
> この手順は、エントリーポイントリストを [調査] ページに表示するために必要です。関連情報リストをエントリーポイントの下に表示しない場合でも、ダミービューを作成してマッピングする必要があります。

必要なロール：admin

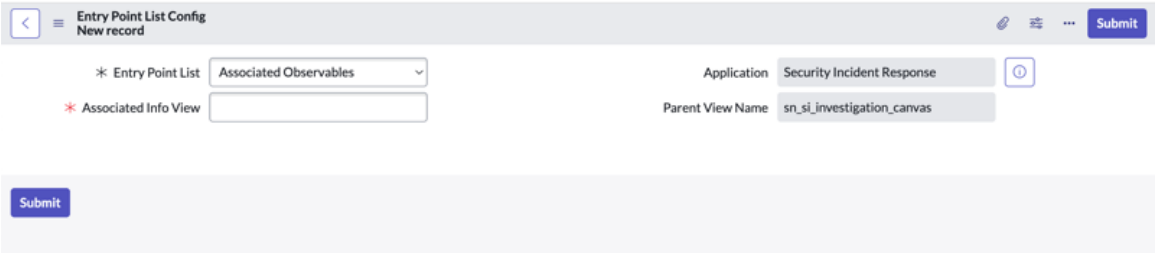
手順

1. [エントリーポイント構成 **(Entry Point Configs)]** ページの [関連情報ビューをマップ] ボタンをクリックします。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. [エントリーポイントリスト] ドロップダウンリストから、新しく追加されたエントリーポイントリストを選択します。
3. 関連情報の関連リストを含むビュー名を [関連情報ビュー] フィールドに入力します。
   関連情報の関連リストのビューを作成する方法については、「関連情報テーブルのビューの作成」を参照してください。



4. [保存] をクリックしてフォームを保存します。
5. さらに、必要に応じて [関連情報ビューを編集] を使用して、関連するリストを追加または削除できます。
   [エントリーポイントリストレイアウトを編集] アクションを使用して、エントリーポイントリストのレイアウトを設定することもできます。必要に応じてスラッシュバケットの列を追加または削除し、フォームを保存します。

ビューから各関連リストを設定してランタイムデータのレンダリングを処理する

ランタイムデータのレンダリングを処理するには、ビューから関連する各リストを設定します。

始める前に

> **注:**
> この手順は、関連情報ビューで構成された関連リストごとに必須です。これを行わない場合、関連リストを調査ページで使用できません。

(関連情報ビューをエントリーポイントリストにマッピングするときに) 追加された各関連リスト 関連情報ビューのエントリーポイントリストへのマッピング (またはビューから直接) には、ランタイムレコードの選択とフィルターの選択に関してデータをフィルタリングする追加の設定が必要です。

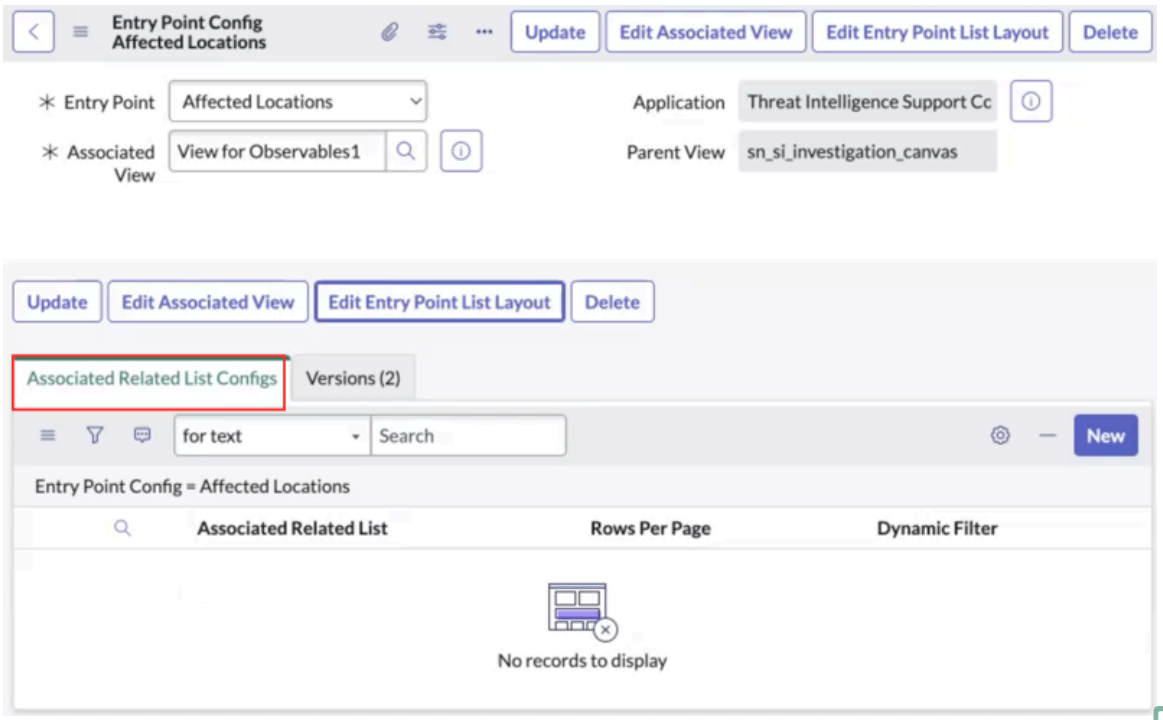
必要なロール：admin

自動翻訳

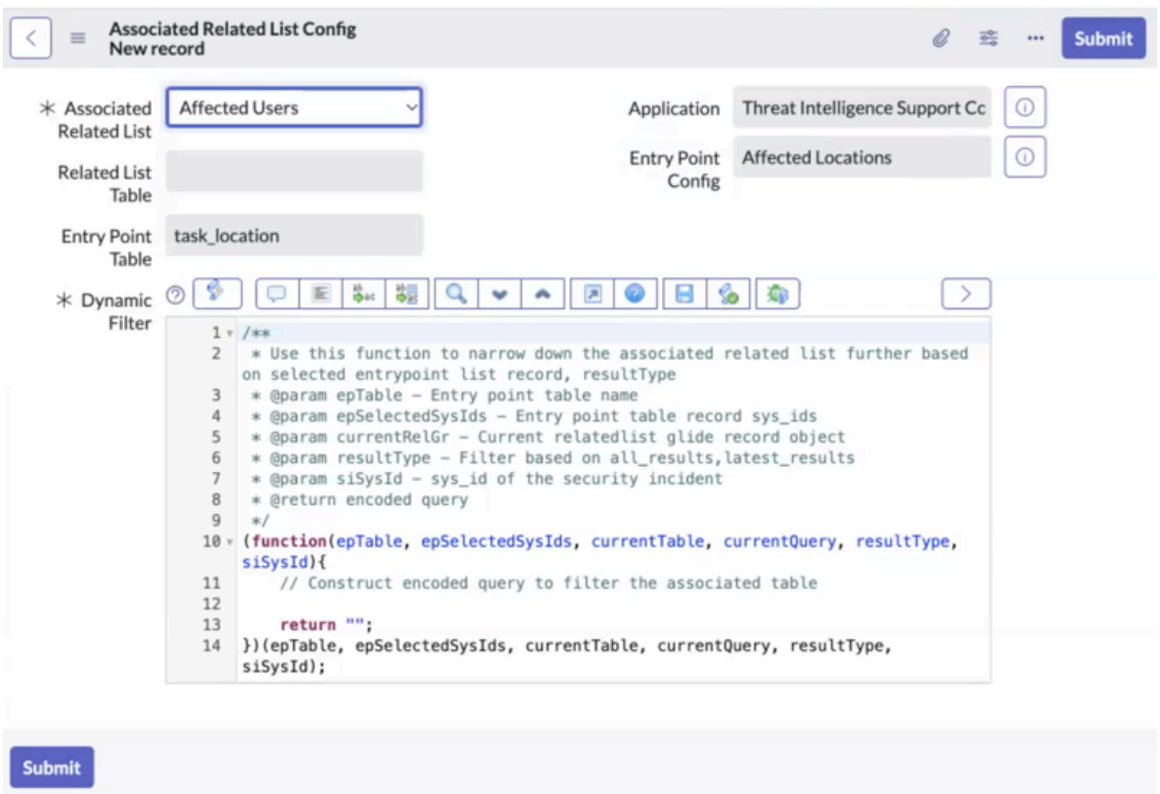
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. [関連リスト構成] から [新規] をクリックします。



2. [関連リスト] フィールド値を選択します。
3. [動的フィルター] 列を使用して、選択したエントリーポイントリストレコードと結果タイプ (各ベンダー実装からの最新の結果、すべての結果) に基づいて、関連するリストをさらにフィルタリングします。
   製品に含まれている既存の例を参照してください。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. また、[関連リストレイアウトを編集] アクションを使用して、関連リストレイアウトを設定することもできます。
   スラッシュバケットウィンドウで、必要に応じて列を追加または削除します。

SIR ワークスペース関連レコード

このセクションは、関連する観察事項や構成アイテムなどのセクションにグループ化された関連リストアイテムで構成されています。

次の関連リストは、ベースシステムの一部として利用可能なグループです。アプリケーションおよび各アクション内で、これらのグループを変更したりグループを作成したりすることができます。

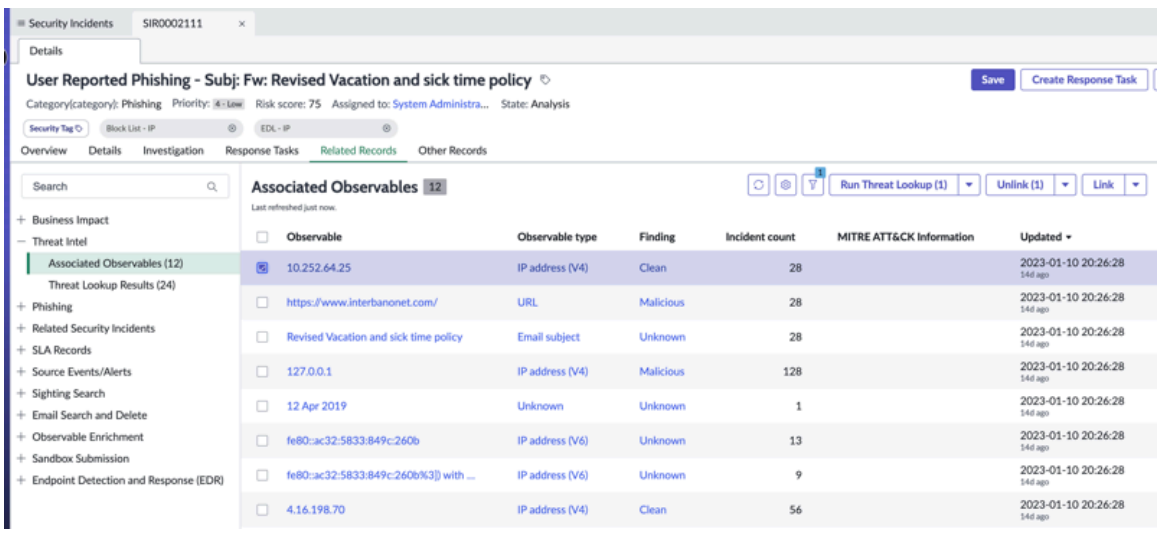
これらのグループを変更することも、新しいグループを作成することもできます。セキュリティインシデントと応答タスクの関連リストを設定してグループ化する方法の詳細については、「セキュリティインシデント関連リストの設定」を参照してください。SIR ワークスペース 内では各関連リストの全機能が使用できます。

関連リスト	グループ化されたアイテム
ビジネスインパクト	• 構成アイテム ID • 影響を受けるユーザー • 関連する構成アイテム • 関連ユーザー • 影響を受けるサービス
Threat Intel	• 関連する観測事象 • 脅威のルックアップの結果
フィッシング	• 関連フィッシングメール • 関連フィッシングヘッダー
関連するセキュリティインシデント	• 親セキュリティインシデント • 子セキュリティインシデント • 類似のセキュリティインシデント
SLA レコード	タスク SLA
ソースイベント/アラート	ソースイベントまたはアラートは、ソースメール、LogRhythm ドリルダウンログ、LogRhythm イベント、集計された IBM QRadar 違反などの SIEM 統合が有効な関連リストです。 **注:** このリストは、インスタンスの統合に完全に依存します。関連する SIEM 統合関連リストを表示するには、最新バージョンをインストールする必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連リスト	グループ化されたアイテム
サイティング検索	• サイティング検索結果 • サイティング検索の詳細 • サイティング
観測事象の拡張	• 観測事象のエンリッチメント結果 • 関連付けられた MISP イベント • MISP エンリッチメント結果
Endpoint Detection and Response (EDR)	• ホストの詳細 • 実行中のプロセス • 実行中のサービス • ログオンユーザー • ネットワーク統計 • ファイルを取得 • ホスト隔離エントリー • エンドポイントでの追加アクション • Microsoft Defender for Endpoint の関連マシンの詳細



注:
一般に、必要に応じて関連リストグループに対して、新しいレコードを作成したり、既存のレコードや新しいレコードをリンクまたはリンク解除したりすることができます。

関連情報

セキュリティインシデント関連リストの設定

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデント関連リストの設定

新しい関連リストまたは新しい関連リストグループを追加し、SIR ワークスペース に表示される既存のグループまたは関連リストを変更できます。

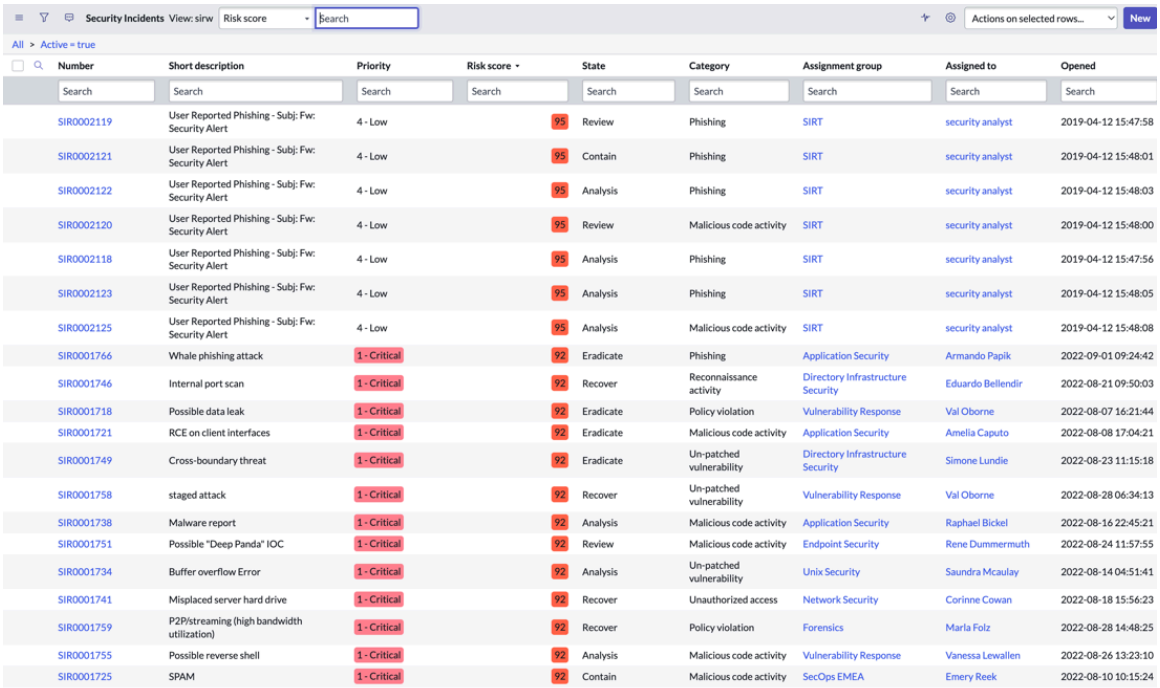
始める前に

セキュリティインシデント関連リストがグループ化され、ワークスペースの [関連レコード] タブにグループ関連リストアイテムとして表示されます。

必要なロール：sn_si.admin

手順

1. クラシック UI で、次に移動します: **All** (すべて) > セキュリティインシデント > オープンインシデントを表示.

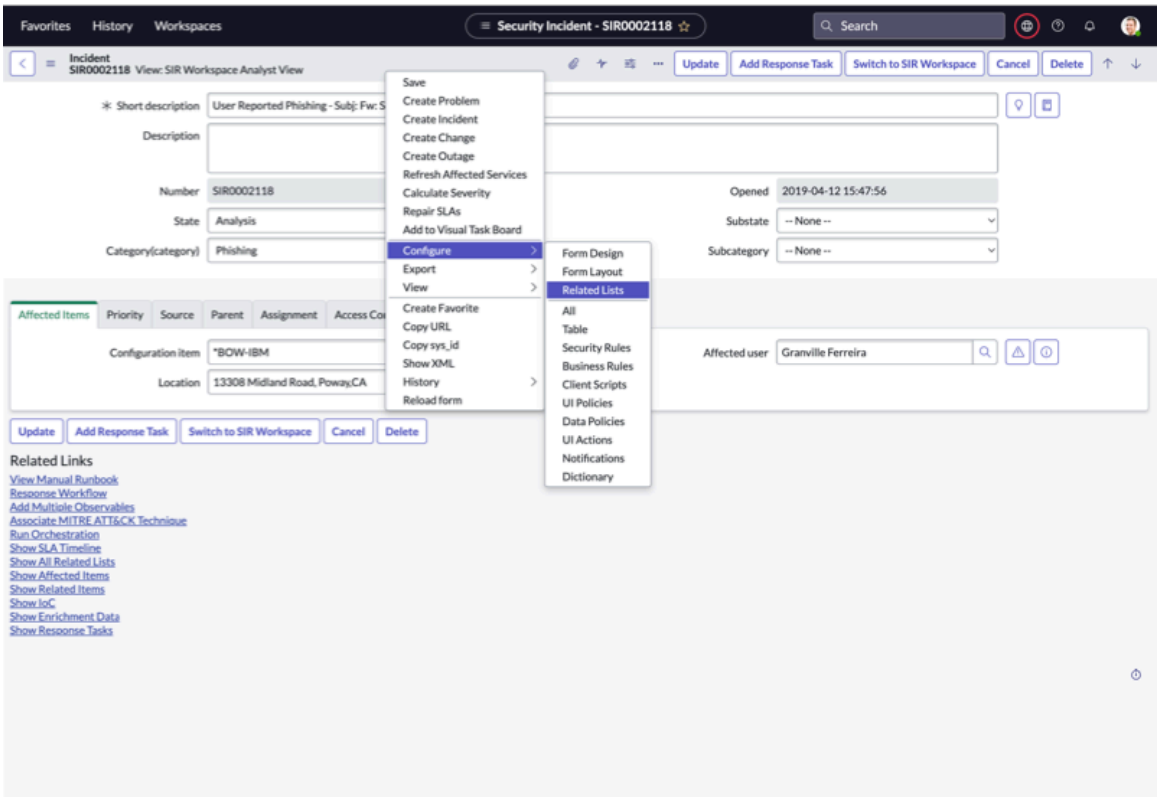


Number	Short description	Priority	Risk score	State	Category	Assignment group	Assigned to	Opened
SIR0002119	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Phishing	SIRT	security analyst	2019-04-12 15:47:58
SIR0002121	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Contain	Phishing	SIRT	security analyst	2019-04-12 15:48:01
SIR0002122	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:03
SIR0002120	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:00
SIR0002118	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:47:56
SIR0002123	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:05
SIR0002125	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:08
SIR0001766	Whale phishing attack	1 - Critical	92	Eradicate	Phishing	Application Security	Armando Papik	2022-09-01 09:24:42
SIR0001746	Internal port scan	1 - Critical	92	Recover	Reconnaissance activity	Directory Infrastructure Security	Eduardo Bellendir	2022-08-21 09:50:03
SIR0001718	Possible data leak	1 - Critical	92	Eradicate	Policy violation	Vulnerability Response	Val Oborne	2022-08-07 16:21:44
SIR0001721	RCE on client interfaces	1 - Critical	92	Eradicate	Malicious code activity	Application Security	Amelia Caputo	2022-08-08 17:04:21
SIR0001749	Cross-boundary threat	1 - Critical	92	Eradicate	Un-patched vulnerability	Directory Infrastructure Security	Simone Lundie	2022-08-23 11:15:18
SIR0001758	staged attack	1 - Critical	92	Recover	Un-patched vulnerability	Vulnerability Response	Val Oborne	2022-08-28 06:34:13
SIR0001738	Malware report	1 - Critical	92	Analysis	Malicious code activity	Application Security	Raphael Bickel	2022-08-16 22:45:21
SIR0001751	Possible "Deep Panda" IOC	1 - Critical	92	Review	Malicious code activity	Endpoint Security	Rene Dummermuth	2022-08-24 11:57:55
SIR0001734	Buffer overflow Error	1 - Critical	92	Analysis	Un-patched vulnerability	Unix Security	Saundra Mcaulay	2022-08-14 04:51:41
SIR0001741	Misplaced server hard drive	1 - Critical	92	Recover	Unauthorized access	Network Security	Corinne Cowan	2022-08-18 15:56:23
SIR0001759	P2P/streaming (high bandwidth utilization)	1 - Critical	92	Recover	Policy violation	Forensics	Marla Folz	2022-08-28 14:48:25
SIR0001755	Possible reverse shell	1 - Critical	92	Analysis	Malicious code activity	Vulnerability Response	Vanessa Lewallen	2022-08-26 13:23:10
SIR0001725	SPAM	1 - Critical	92	Contain	Malicious code activity	SecOps EMEA	Emery Reek	2022-08-10 10:15:24

2. 任意のインシデントレコードを選択します。
3. インシデントコンテキストメニューを右クリックします。
4. 検索項目 構成 > 関連リスト.

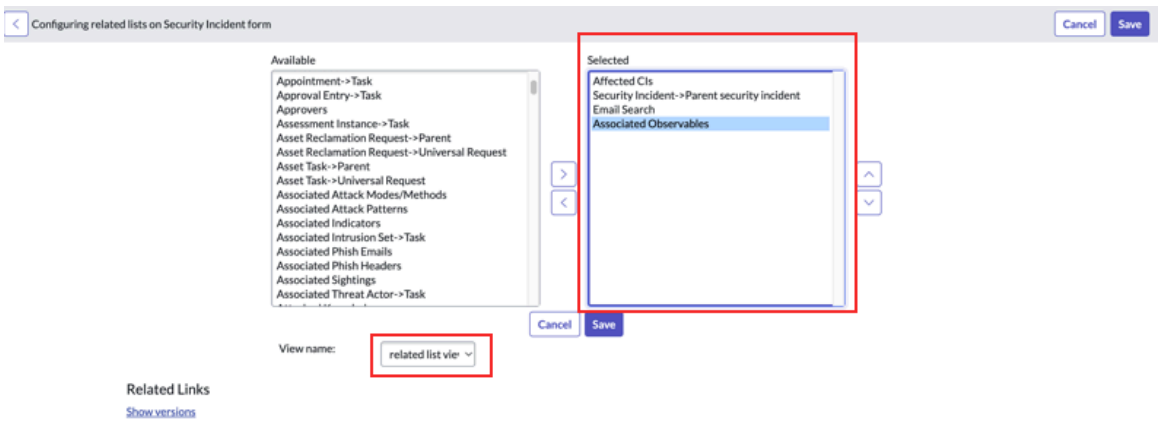
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[セキュリティインシデントフォームでの関連リストの構成 **(Configuring related lists on Security Incident form)]** が表示されます。

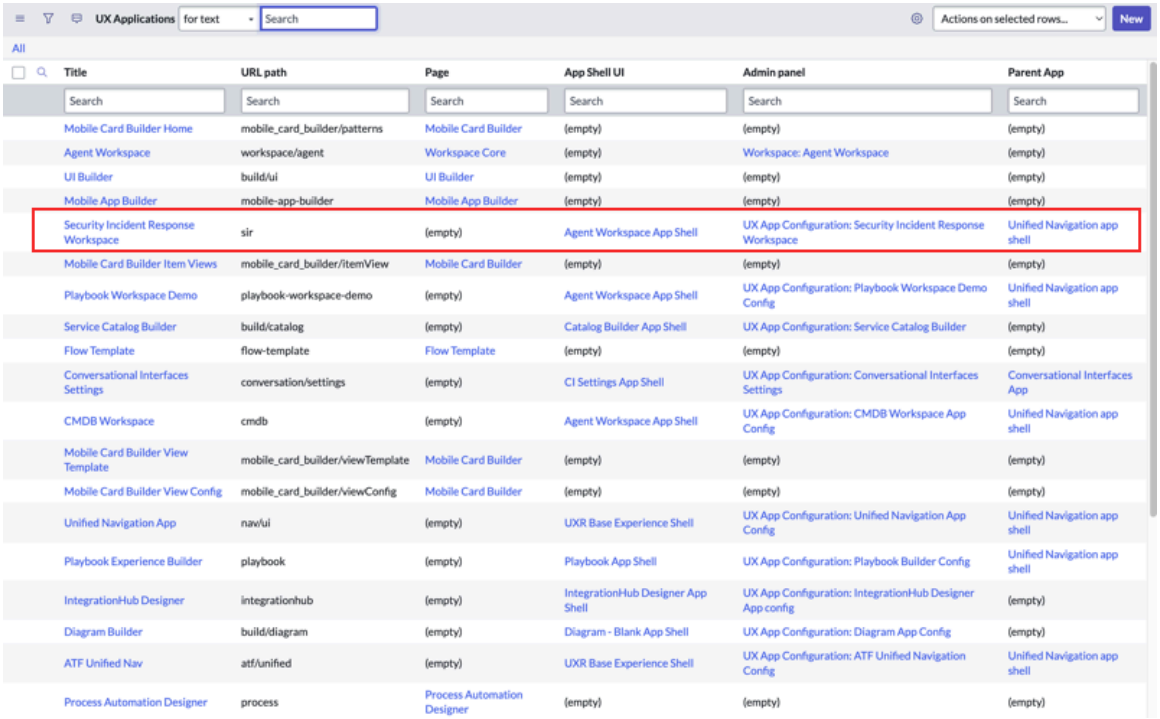
5. [ビュー名] に移動し、[新規] を選択します。
6. ビュー名を入力します。
7. 新しく作成したビューを選択します。
   ビューを選択したら、スラッシュバケットから必要な関連リストフィールドを選択します。



> **注:**
> 変更する場合は、ビューを選択してアイテムを削除または追加します。

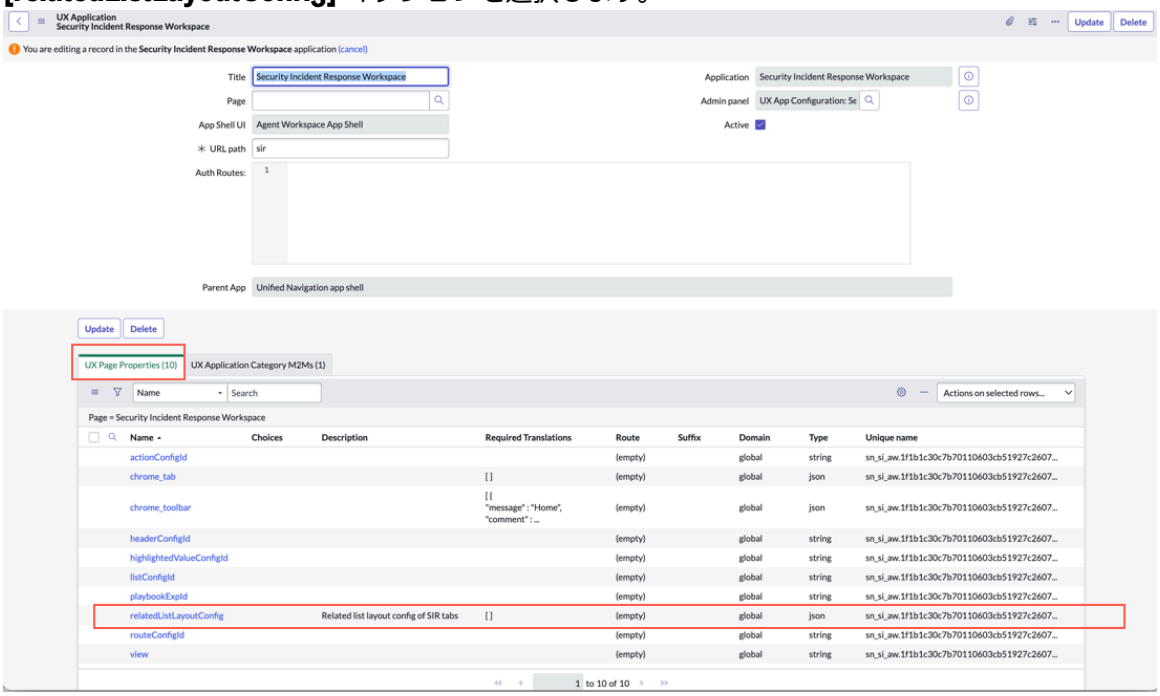
8. **[Save** (保存)] をクリックします。
9. 左側のナビゲーションで、 **All** (すべて) > **Now Experience** フレームワーク > エクスペリエンス.
10. [セキュリティインシデントレスポンスワークスペース] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

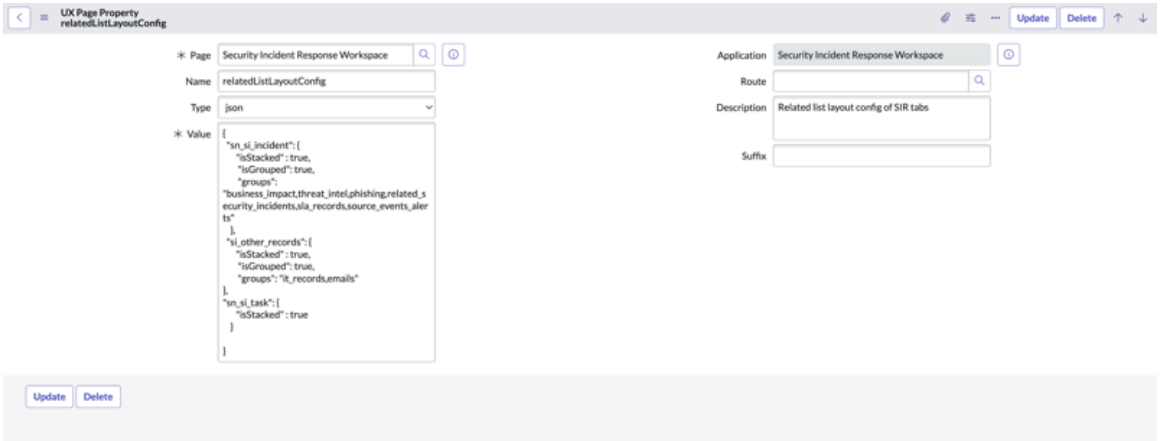


[UX アプリケーションセキュリティインシデントレスポンスワークスペース] ページが表示されます。

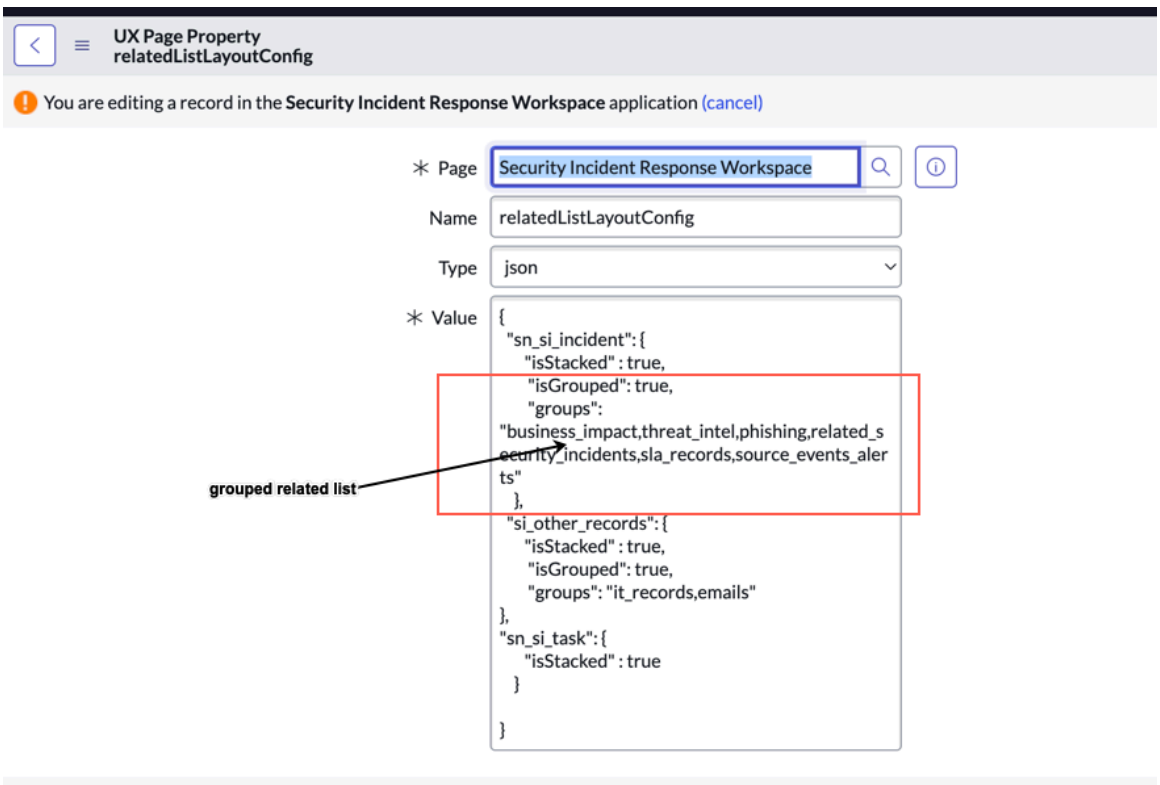
11. [ユーザーエクスペリエンスページプロパティ] タブに移動し、リストビューで **[relatedListLayoutConfig]** オプションを選択します。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



12. **[sn_si_incident.viewsUsedForGrouping]** フィールドの下にある [値] テキストボックスの既存の値のリストに、新しく作成されたビュー名をカンマで区切って追加します。
たとえば、新しいビュー名を「ビジネスインパクト」として作成した場合、[値] テキストボックスで、それを [sn_si_incident:groups] フィールドの下の **[business_impact]** (ビュー名内ではアンダースコアで区切り、既存の値の後はカンマで区切る) として指定する必要があります。



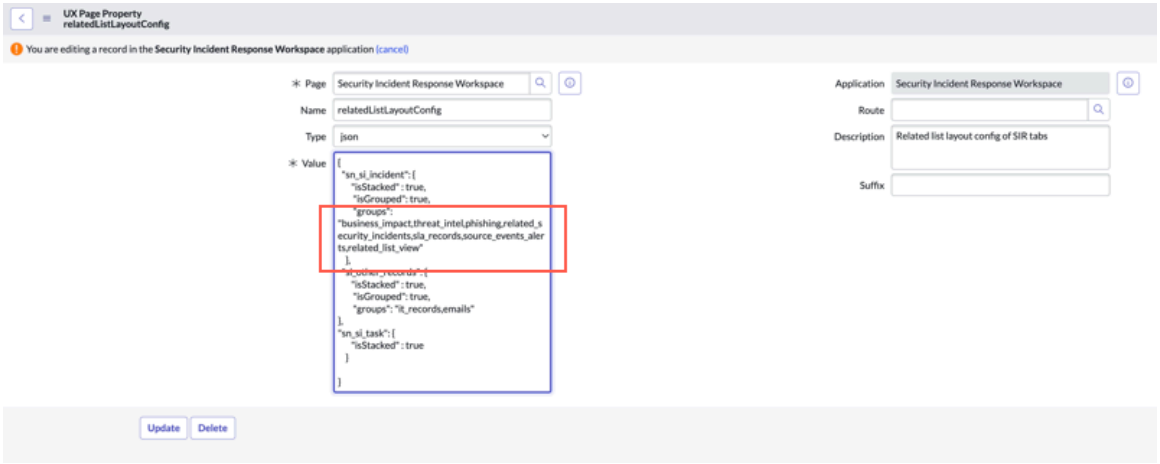
自動翻訳

注:
[sn_si_incident.viewsUsedForGrouping] フィールドに新しいビュー名を追加すると、ワークスペースの [関連レコード] タブにエントリが作成されます。

[si_other_records.viewsUsedForGrouping] のビュー名エントリを更新すると、関連リストグループがワークスペースの [その他のレコード] タブに追加されます。

新しく作成されたビューが追加されたビューの例を以下に示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
[requiredRolesForGrouping] には、カンマ区切りの sys_user_role レコード名が含まれています。グループ化された関連リストを使用するには、SIR ワークスペースユーザーがこれらのロールの少なくとも 1 つを持っている必要があります。ユーザーがこれらのロールを持っていない場合、表示ルール構成を使用して現在のユーザーロールに構成された関連リストビューは、グループ化されずに垂直に表示されます。**[isGrouped]** プロパティが false に設定されている場合、このプロパティは無視されます。このプロパティが空の場合、すべてのユーザーがグループ化された関連リストにアクセスできます。

13. **[Save** (保存)] をクリックします。
14. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
15. 特定のセキュリティインシデントを選択します。
16. ワークスペースの [関連レコード] タブに移動します。
    グループ化された関連リストが表示されます。

応答タスク関連リストの設定

このセクションを使用して、セキュリティインシデントレスポンスアプリケーションに表示される応答タスクの新しい関連リストを設定します。

始める前に
必要なロール：sn_si.admin

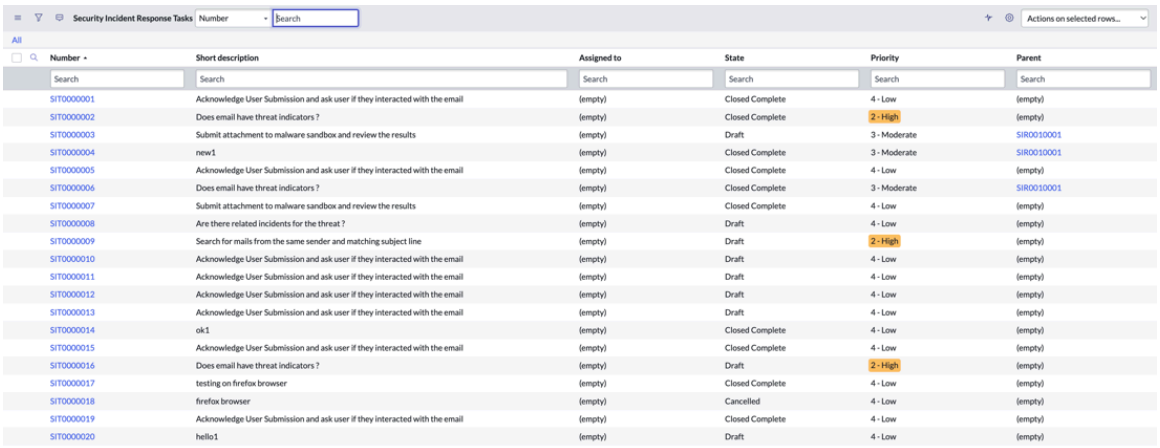
このタスクについて
デフォルトのリストが少ないため、応答タスク関連リストはグループ化されませんが、個々の関連リストアイテムとして表示されます。ワークスペースのセキュリティインシデントレコードの [応答タスク] タブから応答タスク関連アイテムを表示します。

自動翻訳

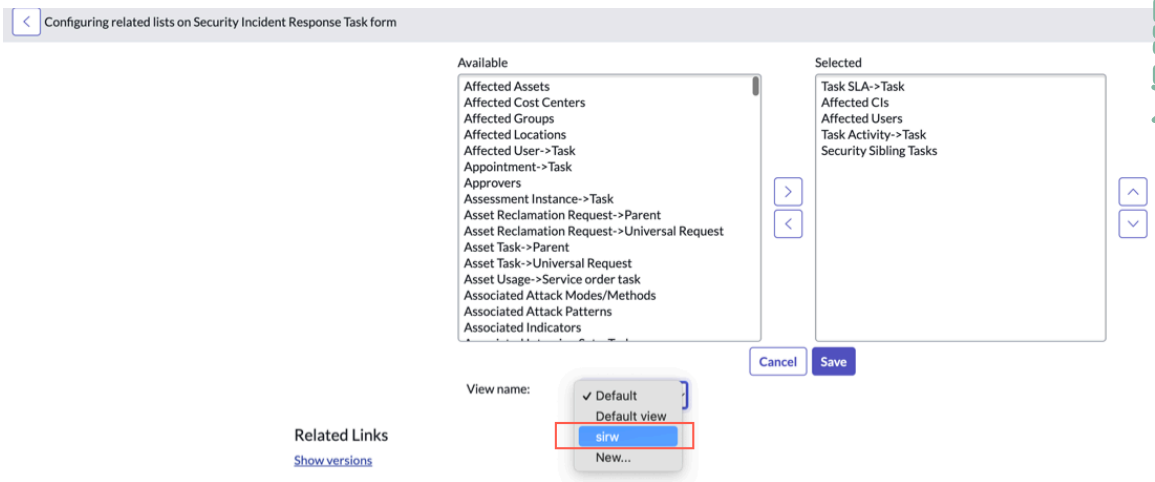
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > 対応タスク > すべてのタスクを表示.



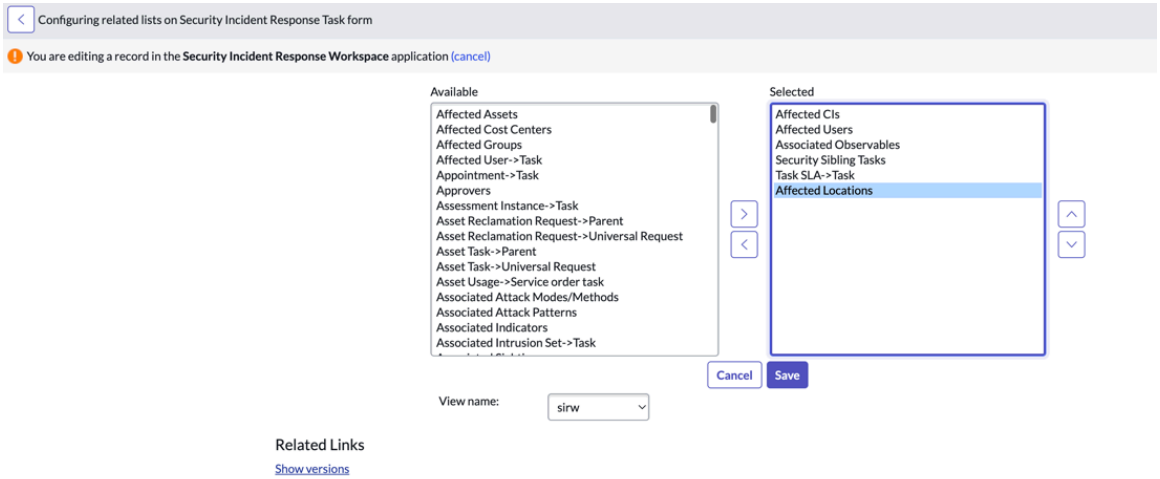
2. 任意の応答タスクレコードを選択します。
3. [セキュリティインシデントレスポンスタスク] コンテキストメニューを右クリックします。
4. 次のように移動する。 構成 > 関連リスト.
   [セキュリティ応答タスクフォームでの関連リストの構成 **(Configuring related lists on Security Response Task form)]** が表示されます。
5. [ビュー名] に移動し、**[sirw]** を選択します。



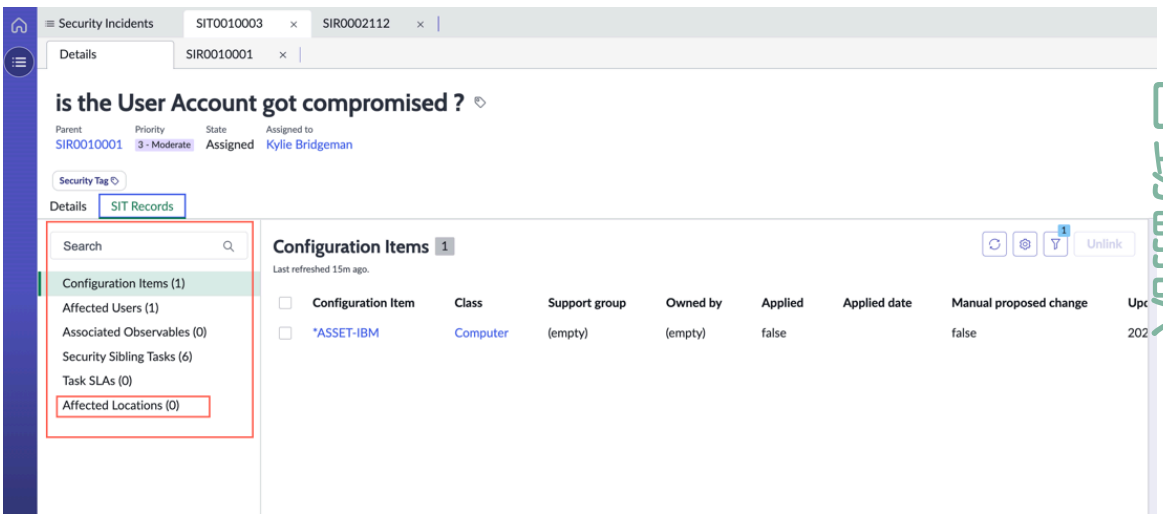
6. スラッシュバケットから目的の関連リストフィールドを選択します。
   たとえば、[影響を受ける場所] です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



7. **[Save** (保存)] をクリックします。
8. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > 対応タスク > **SIT** レコード.
   構成された関連リスト (選択された [影響を受ける場所] など) が SIT レコードリスト内に表示されます。



新しいリスクスコア算出ルールの定義

新しいリスクスコア算出を使用して、ユーザー定義の基準に基づいてセキュリティインシデントのリスクスコアを定義および計算します。これにより、セキュリティインシデントの透過的なインテリジェンススコアリングが提供されます。セキュリティインシデントレコードのリスクスコアが自動的に計算されます。

始める前に

必要なロール：sn_si.admin

sn_si_aw.activate_new_risk_score_calculator システムプロパティを True に設定して、新しいリスクスコア算出をアクティブ化します。

このタスクについて

ユーザー定義のパラメーターに基づいて生成されるセキュリティインシデントレコードのリスクスコアを定義します。ベースシステムには 1 つのリスクスコアルールがプロビジョニングされており、それに応じてカスタマイズして有効にすることができます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

- デフォルトでは、新しいリスクスコア算出ルールは非アクティブです。セキュリティインシデントのリスクスコアを表示するには、ルールを有効にする必要があります。
- ベースシステムで利用可能なもの以外の追加の関連テーブルのリスクスコアを計算するには、「追加の関連テーブルのリスクスコア算出」を参照してください。

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > アドミニストレーション.
2. 次のように移動する。 ルールエンジン > リスクスコア算出ルール.
   [リスクスコア算出ルール (Risk Score Calculator Rule)] ページが表示されます。

   注:

   - ベースシステムの一部として、リスクスコアを表示、編集、または変更するための事前定義されたリスクスコアルールのテンプレートが 1 つあります。ただし、事前定義されたリスクスコアルールのテンプレートを作成または削除することはできません。
   - 変更内容は、新しいセキュリティインシデントや既存のセキュリティインシデントの更新に適用されます。履歴スコアを再表示するには、[スコアを再計算 **(Recalculate Score)]** アクションを使用します。

3. [リスクスコア算出] ルールを選択します。
4. フォームの各フィールドに入力します。

フィールド	説明
名前	リスクスコア値の名前。例：リスクスコア算出。
全体的な重み付け（基準ビルダーに適用）	リスクルール内でのこのフィールドの重み付け。このフィールドは編集できません。有効な基準に対応する重み付けに基づいて計算された全体的な重み付けが表示されます。全体の重み付けは常に 100% にする必要があります。
説明	リスクスコアレコードの説明。たとえば、事前定義された基準スコアの重み付け合計に基づいてリスクスコアを計算します。
採点基準	セキュリティインシデントの採点基準を示します。 次のオプションを使用して、リスク採点基準を定義できます。 ○ 基準ビルダー： このオプションを使用して、リスクスコアの計算に寄与する基準を追加、編集、削除、有効化および無効化して、重み付けの合計集計が 100% であることを確認します。 ○ スクリプトを使用 (詳細) **(Use Script (Advanced))**：スクリプティング機能

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	は、0～100 の範囲のリスクスコアを返すカスタムスクリプトを構築するための高度な機能です。

5. 基準ビルダーを使用して採点基準を定義するには、次の手順を実行します。

> **注:**
> 既存の基準を編集または変更したり、新規の基準を追加したりすることができます。

a. 新しい条件を追加するには、**[+** 新しい条件] アクションを選択します。

b. 基準を設定するテーブルを選択します。

> **注:**
> - 選択したテーブルがセキュリティインシデントの場合、リスクスコアが計算されるセキュリティインシデントレコードに条件が適用されます。選択したテーブルがセキュリティインシデントでない場合、リスクスコアが計算されるセキュリティインシデントにレコードが関連している場合にのみ条件が適用されます。
> - セキュリティインシデントに関連付けられた関係の数に基づいてスコアを定義するために、追加の集計タイプが追加されます。

c. 選択したテーブルの [タイプ] 基準を選択します。
[タイプ] の値は、選択したテーブルに基づいて [フィールド] または [アグリゲート] のいずれかになります。

d. 選択したテーブルの [フィールド] 基準を選択します。
[タイプ] の値を [フィールド] として選択した場合、[フィールド] 基準にはテーブルに関連するフィールド値が表示されます。[タイプ] の値を [アグリゲート] として選択した場合、[フィールド] 基準にはテーブルに関連する集計値が表示されます。

> **注:**
> アグリゲートタイプはカウント値のみをサポートします。

たとえば、[テーブル] 基準で [セキュリティインシデント] を選択すると、[タイプ] 基準には [フィールド] オプションのみが表示されます。[フィールド] 基準には、テーブルに関連するすべてのフィールド値 (重大度、アクティブなど) が表示されます。同様に、[テーブル] 基準で [影響を受けるユーザー **(Affected Users)]** を選択した場合、[タイプ] 基準には [フィールド] と [アグリゲート] の両方のオプションが表示されます。[タイプ] で [アグリゲート] を選択した場合、[フィールド] 基準には、テーブルに関連する集計値 (カウント) が表示されます。

e. 基準の重み付けを 0～100 の範囲で入力します。
すべての基準の全体的な重み付けが 100% になるようにする必要があります。

f. 基準の名前と簡単な説明を入力します。

g. [採点基準を有効にする **(Enable scoring criteria)]** チェックボックスをオンにして、採点基準を有効にします。

h. 条件を定義し、条件のスコアを設定します。

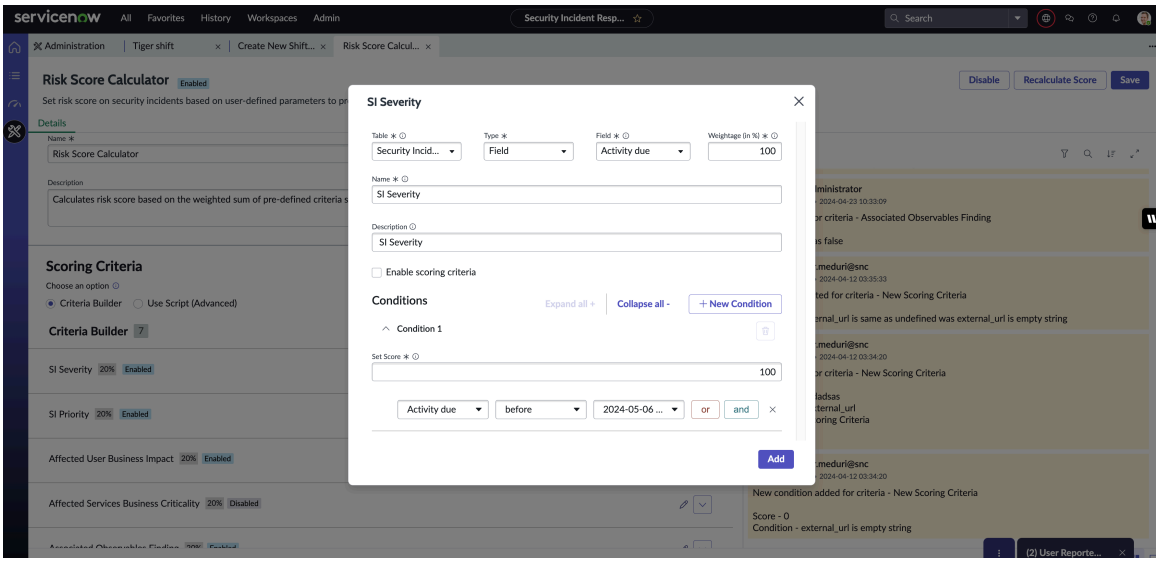
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

i. [新規条件] オプションを使用して新しい条件を追加したり、[基準を削除] アイコンを使用して既存の条件を削除したりすることもできます。

j. [追加] を選択して、構成した基準を追加します。

基準ビルダーを使用した採点基準



6. [スコアを再計算 **(Recalculate Score)]** オプションを選択して、リスクスコアを再計算します。

   たとえば、リスクスコアルールが変更された場合などです。その場合は、過去に計算済みのリスクスコアを持つセキュリティインシデントに採点ルールを再適用する必要があります。[スコアを再計算 **(Recalculate Score)]** アクションを使用して、再計算ジョブをトリガーします。

7. [確認] を選択します。

   注:
   このアクションをトリガーすると、プロセスがバックグラウンドで実行され、完了するまでに数分かかります。完了するまで、変更を加えることはできません。

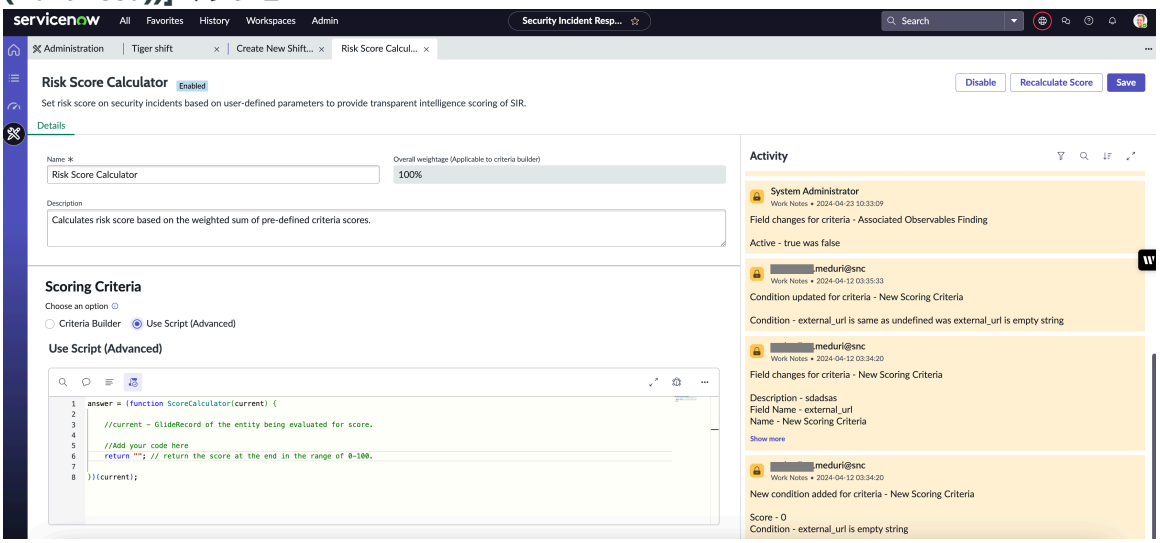
8. [スクリプトを使用 (詳細) **(Use Script (Advanced))]** オプションを使用して採点基準を定義するには、次の手順を実行します。

   a. この事前定義されたスクリプトを使用して、0～100 の範囲のリスクスコアを返すカスタムスクリプトを作成します。
   詳細スクリプトフィールドには、パラメーター **current** を取る関数が自動的に入力され、この関数は 0～100 の範囲のリスクスコアを返す必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[スクリプトを使用した採点基準 (詳細) **(Scoring Criteria using Script (Advanced))]** オプション



ここで、現在のパラメーターは、リスクスコアが計算されるエンティティ (セキュリティインシデント) の GlideRecord オブジェクトです。セキュリティインシデントの場合は、sn_si_incident テーブルの GlideRecord に相当します。

9. リスクスコア算出を無効にするには、[無効化] を選択します。
10. [保存] を選択します。

追加の関連テーブルのリスクスコア算出

リスクスコア算出には、ユーザー定義の基準に基づいてセキュリティインシデントのリスクスコアを計算するためのベースシステムの一部として、1 つのリスクスコアリングルールがプロビジョニングされます。ただし、リスクスコアを計算するために、追加の関連テーブルをカスタマイズして含めることができます。

始める前に

必要なロール：sn_si.admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデント > すべてのインシデントを表示.
2. 任意のセキュリティインシデントレコードを選択します。
3. セキュリティインシデント番号の横にある [他のアクション] オプションを選択します。
4. 検索項目 構成 > 関連リスト.
5. [ビュー名] に移動し、[リスクスコア算出] を選択します。
   ビューを選択したら、スラッシュバケットから必要な関連リストフィールドを選択します。たとえば、関連するサイティングなどです。
6. [保存] を選択します。
   リスクスコアを計算する新しい関連リストまたはテーブルが正常に追加されました。

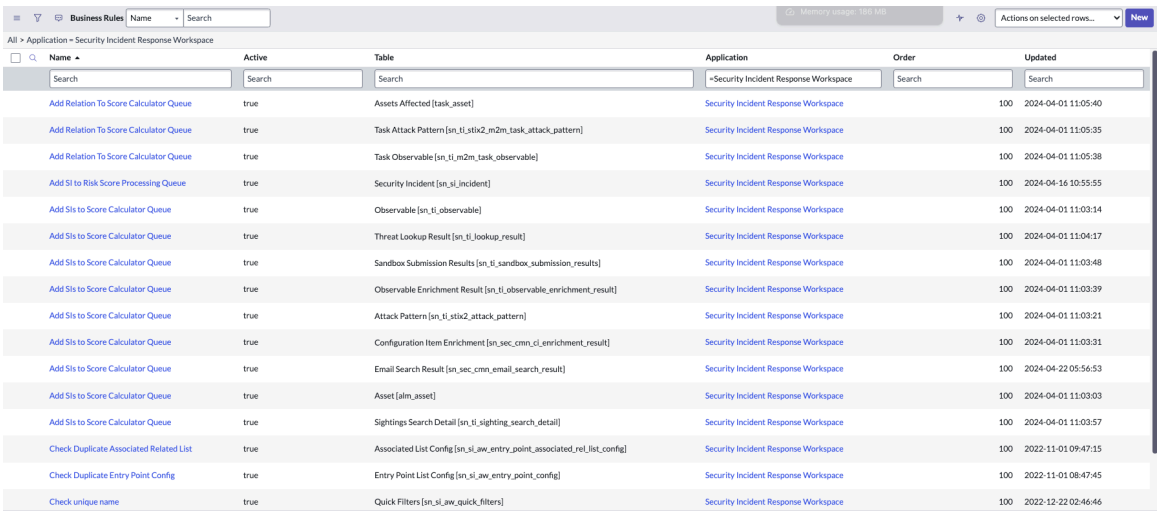
> **重要:**
> 新しく作成された関連リストを使用して、新しい基準を持つセキュリティインシデントのリスクスコアを計算するには、関連リストのベーステーブルでビジネスルールを定義する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. 次のように移動する。 **All** (すべて) > システム定義 > ビジネスルール.
   次の 2 つのビジネスルールを参照して、独自のビジネスルールを作成できます。
   - スコア算出キューへのセキュリティインシデント (SI) の追加
   - スコア算出キューに関係を追加 (これは m2m テーブルに適用されます)

ビジネスルール



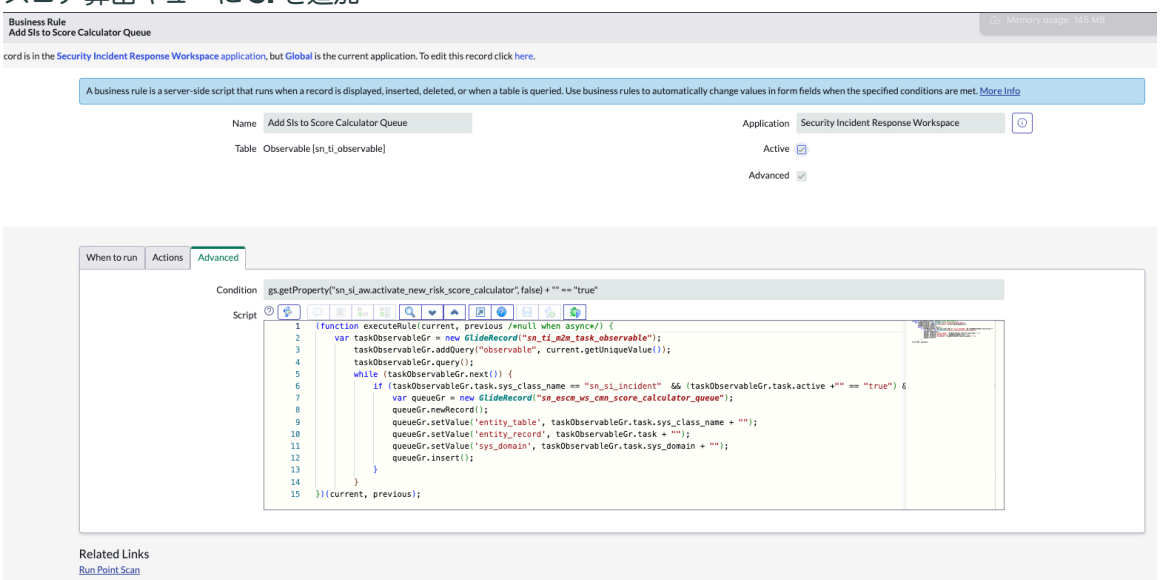
Name	Active	Table	Application	Order	Updated
Add Relation To Score Calculator Queue	true	Assets Affected [task_asset]	Security Incident Response Workspace	100	2024-04-01 11:05:40
Add Relation To Score Calculator Queue	true	Task Attack Pattern [sn_ti_stix2_m2m_task_attack_pattern]	Security Incident Response Workspace	100	2024-04-01 11:05:35
Add Relation To Score Calculator Queue	true	Task Observable [sn_ti_m2m_task_observable]	Security Incident Response Workspace	100	2024-04-01 11:05:38
Add SI to Risk Score Processing Queue	true	Security Incident [sn_si_incident]	Security Incident Response Workspace	100	2024-04-16 10:55:55
Add SIs to Score Calculator Queue	true	Observable [sn_ti_observable]	Security Incident Response Workspace	100	2024-04-01 11:03:14
Add SIs to Score Calculator Queue	true	Threat Lookup Result [sn_ti_lookup_result]	Security Incident Response Workspace	100	2024-04-01 11:04:17
Add SIs to Score Calculator Queue	true	Sandbox Submission Results [sn_ti_sandbox_submission_results]	Security Incident Response Workspace	100	2024-04-01 11:03:48
Add SIs to Score Calculator Queue	true	Observable Enrichment Result [sn_ti_observable_enrichment_result]	Security Incident Response Workspace	100	2024-04-01 11:03:39
Add SIs to Score Calculator Queue	true	Attack Pattern [sn_ti_stix2_attack_pattern]	Security Incident Response Workspace	100	2024-04-01 11:03:21
Add SIs to Score Calculator Queue	true	Configuration Item Enrichment [sn_sec_cmn_ci_enrichment_result]	Security Incident Response Workspace	100	2024-04-01 11:03:31
Add SIs to Score Calculator Queue	true	Email Search Result [sn_sec_cmn_email_search_result]	Security Incident Response Workspace	100	2024-04-22 05:56:53
Add SIs to Score Calculator Queue	true	Asset [alm_asset]	Security Incident Response Workspace	100	2024-04-01 11:03:03
Add SIs to Score Calculator Queue	true	Sightings Search Detail [sn_ti_sighting_search_detail]	Security Incident Response Workspace	100	2024-04-01 11:03:57
Check Duplicate Associated Related List	true	Associated List Config [sn_si_aw_entry_point_associated_rel_list_config]	Security Incident Response Workspace	100	2022-11-01 09:47:15
Check Duplicate Entry Point Config	true	Entry Point List Config [sn_si_aw_entry_point_config]	Security Incident Response Workspace	100	2022-11-01 08:47:45
Check unique name	true	Quick Filters [sn_si_aw_quick_filters]	Security Incident Response Workspace	100	2022-12-22 02:46:46

8. たとえば、関連する観測事象の基準を機能させるために、2 つのビジネスルールを定義しました。

   1 つ目は、「スコア算出キューに **SI** を追加」ビジネスルールです。

   たとえば、新しいセキュリティインシデントが作成され、観測事象 (Observables[sn_ti_observable]) テーブルに関連付けられます。脅威のルックアップの後、観測事象が悪意のある事象であることが判明しました。次に、この悪意のある観測事象に関連付けられているすべてのセキュリティインシデントをキューに追加して、セキュリティインシデントのリスクスコアを再計算する必要があります。

スコア算出キューに **SI** を追加



   2 つ目は、「**Add Relation To Score Calculator Queue**」ビジネスルールです。

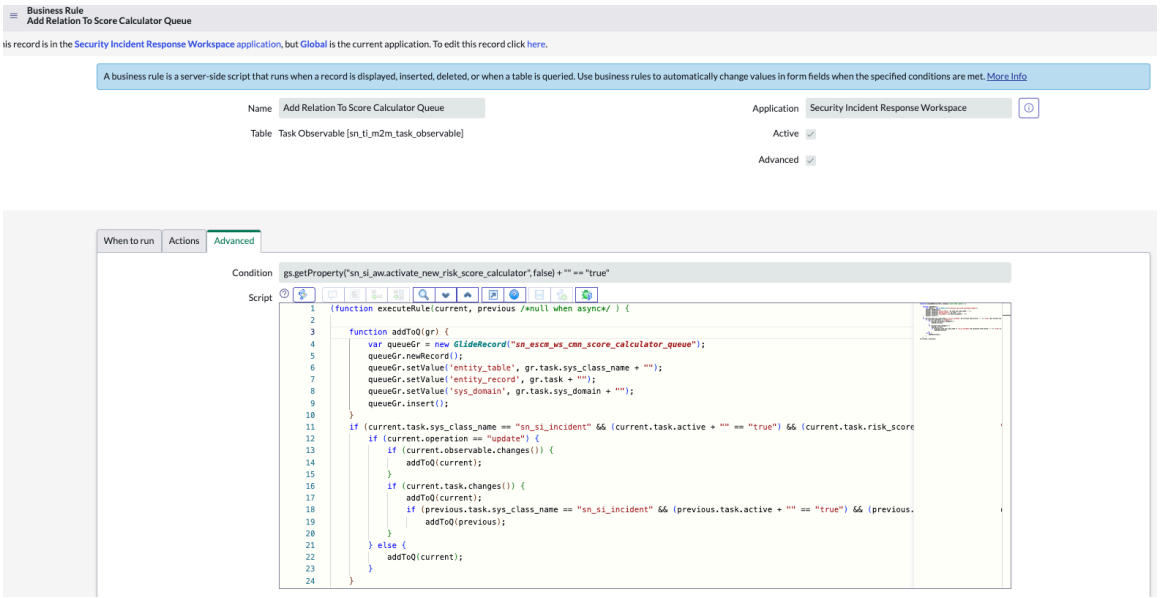
   たとえば、新しいセキュリティインシデントが作成または削除され、観測事象 (タスク観測事象 [sn_ti_m2m_task_observable]) テーブルに関連付けられます。セキュリティインシデントの関連

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

付けが変更されました。その後、そのセキュリティインシデントをキューに追加して、セキュリティインシデントのリスクスコアを再計算する必要があります。

スコア算出キューへの関係を追加



シフト引き継ぎテンプレートを構成する

管理者は、シフトオーナーがシフト引き継ぎレコードを作成して、次のシフトチームに渡すためのさまざまなシフト引き継ぎテンプレートを定義および構成できます。

始める前に

必要なロール：

- sn_escm_sh.shift_admin
- sn_si.admin は sn_escm_sh.shift_admin ロールを継承する

このタスクについて

シフト引き継ぎテンプレートを構成するには、管理者が新しいシフト引き継ぎテンプレートを作成するか、「サンプルシフトテンプレート」という名前の既存のテンプレートをベースシステムで開き、要件に応じて詳細とセクションを変更します。

シフトオーナーは、構成されたテンプレートを使用してシフト引き継ぎログレコードを作成し、シフト引き継ぎレポートを次のアクティブなシフトオーナーおよびチームと共有できます。

注:
アクティブなシフト引き継ぎテンプレートのみが表示され、シフトオーナーは引き継ぎログレコードを作成できます。

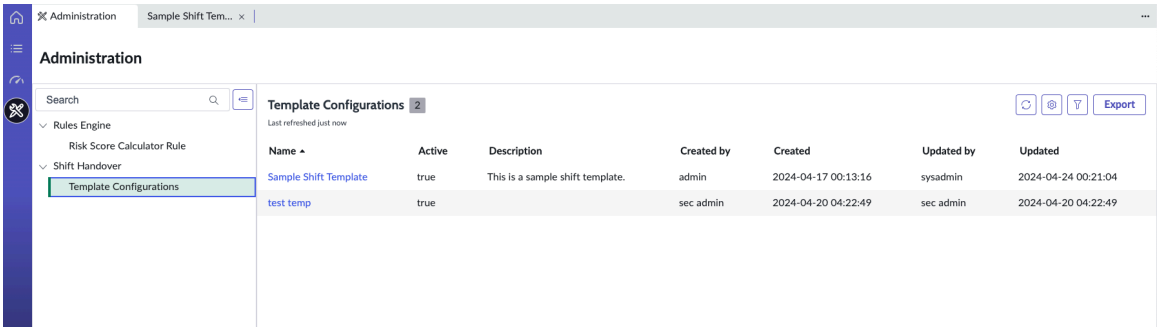
手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > アドミニストレーション.
2. 次のように移動する。 シフトの引き継ぎ > テンプレート構成.
   [テンプレート構成] ページが表示されます。

注:
ベースシステムの一部として、シフト引き継ぎテンプレートを表示、編集、または変更するための事前定義されたシフト引き継ぎテンプレート構成が 1 つ提供されます。ただし、事前定義されたシフト引き継ぎテンプレート構成を作成または削除することはできません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

シフト引き継ぎテンプレート構成



3. 新しいシフト引き継ぎテンプレートを作成するには、[新規] を選択します。

4. [詳細] フォームで、フィールドに入力します。

新しいシフト引き継ぎテンプレートを作成する

フィールド	説明
名前	シフト引き継ぎテンプレートの名前。例：SIR テンプレート。
アプリケーション	シフト引き継ぎテンプレートを作成するアプリケーションの名前。例：セキュリティインシデントレスポンスワークスペース
アクティブ	シフト引き継ぎテンプレートがアクティブかどうかを示すオプション。シフト引き継ぎテンプレートをアクティブ化するには、このオプションを有効にします。
説明	シフト引き継ぎテンプレートの説明。
レコードメンション構成	このフィールドを使用して、リッチテキストエディター (RTE) のレコードメンションの詳細を構成します。入力は、次のフィールドを持つ JSON オブジェクトのアレイです。 ○ *sourceTable*：ソーステーブルの名前。 ○ *label*：表示するラベルの名前。 ○ *filterCondition*：フィルタリング用のエンコードされたクエリ。 ○ *fields*：パターンをクエリするフィールドを選択する。 [レコードメンション構成] フィールドにコピー & ペーストができるサンプル構成。 `[ { "sourceTable": "incident", "label": "Incidents", "filterCondition": "active=true", "fields": [ "number" ]`

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	<pre> }]</pre> サンプル構成をコピーするには、[コンテキスト支援] ペインの [クリップボードにコピー] アクションを使用します。その後、要件に基づいて追加の変更を加えることができます。

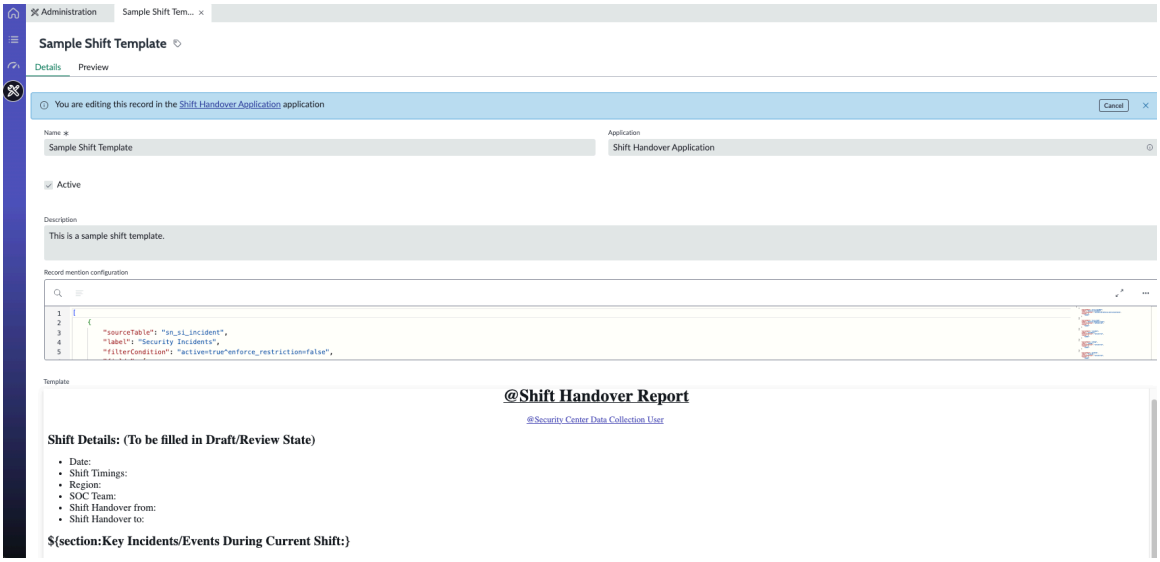
テンプレート	セクションを使用してシフト引き継ぎテンプレートを作成します。アナリストがテンプレートに基づいてシフト引き継ぎログレコードに貢献できるように、少なくとも 1 つのセクションがあることを確認してください。
	
	テンプレートでは、適切なセクションに静的テキストや画像などを含めることができます。画像をコピーして [テンプレート] フィールドに直接貼り付けることができます。次のコードを使用して、テンプレートにセクションを作成できます。
	<pre>${section:Section Label}</pre>
	例：
	<pre>${section:Key Incidents/Events During Current Shift}
	${section:Incidents/Events to Monitor or Follow Up}
	${section:System/Infrastructure Updates}
	${section:Next Steps for Incoming Shift}
	${section:References}</pre>
	注:
	詳細については、右ペインの「コンテキスト支援」を参照してください。

5. 既存のシフト引き継ぎテンプレートを使用および変更するには、[サンプルシフトテンプレート **(Sample Shift Template)]** を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

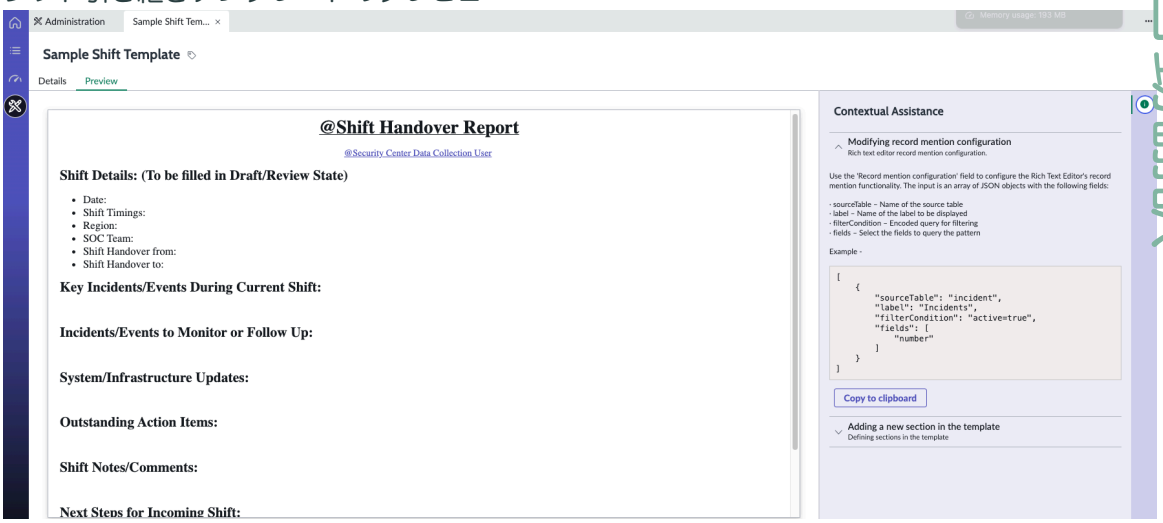
シフト引き継ぎテンプレート



6. 要件に応じてシフト引き継ぎテンプレートを更新します。
7. [プレビュー] を選択して、シフト引き継ぎテンプレートのランタイムプレビューを表示します。

   レポートは、シフト引き継ぎテンプレート構成に基づいてプレビューを生成します。

シフト引き継ぎテンプレートのプレビュー



8. [保存] を選択して、シフト引き継ぎテンプレートを保存します。

次のタスク
リストビューでシフト引き継ぎレコードを管理する方法、およびシフト引き継ぎレコードの作成、編集、コピー、削除などのアクションを実行する方法については、「シフト引き継ぎレコードの管理」を参照してください。

セキュリティインシデントレスポンス 電話会議

セキュリティインシデントレスポンス カンファレンスコール統合を使用すると、アナリスト、マネージャー、および影響を受けるユーザーのカンファレンスコールとチャットを管理および開始できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

カンファレンス機能を使用すると セキュリティインシデントレスポンス 顧客やピアエージェントと協力して、電話でセキュリティインシデントを解決できます。グループチャットを使用してコラボレーションすることもできます。

Microsoft Teams、Cisco Webex、Zoom 会議などのサードパーティの通信チャネルを使用して、カンファレンスコールを開始できます。チャットを使用してコラボレーションするには、SIR アプリケーションのサイドバーチャットを使用します。

主要な機能

セキュリティインシデントレスポンスコールコラボレーションの主な機能は次のとおりです。

- SIR マネージャー/アナリストは、セキュリティインシデントから直接 Microsoft Teams、Cisco Webex、または Zoom のカンファレンスコールを開始できます。
- SIR マネージャー/アナリストは、SIR アプリケーションから直接チャットを開始できます。
- 追加の参加者をコールまたはチャットに招待します。
- コール記録とチャットの詳細を表示します。
- メールと Microsoft Teams チャットを介して参加者に招待状を送信します。

カンファレンスコールのユーザーとグループの管理

アドミニストレーターは、カンファレンス設定を構成して、コールに追加するユーザーとグループの事前定義済みリストを表示できます。

始める前に
必要なロール：sn_si.admin

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > アドミニストレーション.
2. [カンファレンス]、**[**通話の構成] の順に選択します。
3. [通話の構成] ページで、[カンファレンスの構成] を選択します。
   ユーザーとグループの事前定義リストを構成するための設定ページが表示されます。
4. [詳細] フォームで、フィールドに入力します。

フィールド	説明
名前	カンファレンスコール構成の名前。
ユーザーの自動入力	カンファレンスの構成済みユーザーを自動入力するオプション。このオプションを選択すると、構成されたユーザーとグループがカンファレンスに追加されます。 **注:** 通話を開始するときにも、ユーザー/グループを追加または削除できます。
影響を受けるユーザーを表示	コールに追加する際に影響を受けるユーザーを表示するオプション。
アサイン先グループユーザーを表示	コールに追加するアサイン先グループユーザーを表示するオプション。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
デフォルトグループ	コールに追加するデフォルトグループを追加するオプション。
デフォルトユーザー	通話に追加するデフォルトユーザーを追加するオプション。

5. [保存] を選択して、カンファレンスコールの構成を保存します。

SIR とサードパーティコミュニケーションチャネルの統合

Microsoft Teams、Zoom、Cisco Webex などのサードパーティのコミュニケーションチャネルとの SIR カンファレンスコールの統合により、セキュリティインシデントから直接コールを管理および開始できます。

主要な機能

- 任意のセキュリティインシデントから直接カンファレンスコールを開始および終了します。
- カンファレンスコールの参加者を追加または削除します。
- さらに分析するために、会議の期間や出席者などの会議の詳細を追跡して報告します。

前提条件

ServiceNow インスタンスに次の Integration Hub プラグインがインストールされていることを確認します。

- 通知プラグイン (com.snc.notify)。詳細については、「Configuring Notify」を参照してください。
- 構成可能なワークスペースの通知 UI コンポーネント
- Microsoft Teams をコミュニケーションチャネルとして統合する場合:
  - Microsoft Teams Communications スポークプラグイン (sn_msteams_com_spk)。
  - Azure Active Directory ユーザーマッピングプラグイン (sn_now_azure)
- Zoom をコミュニケーションチャネルとして統合する場合:
  - Zoom スポーク (sn_zoom_spoke)
  - Zoom に通知 (sn_notify_zoom)
- Cisco Webex をコミュニケーションチャネルとして統合する場合:
  - Cisco Webex Connector (sn_notify_webex) に通知
  - Cisco Webex Teams スポーク (sn_cisco_teams_spk)

詳細については、「Request Integration Hub」を参照してください。

構成

使用するコミュニケーションチャネルについて、次の構成を実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 通知通信チャネルを使用してカンファレンスコール Cisco Webex インテグレーションを設定するには、「 Configure Notify Cisco Webex Connector 」を参照してください。

- 通知コミュニケーションチャネルを使用してカンファレンスコール Zoom 統合を設定するには、「 Configure Notify Zoom connector in Notify 」を参照してください。

- 事前設定されたアプリを使用してカンファレンスMicrosoft Teams統合を構成するには、「 Integrate Notify connector pre-published app with Microsoft Teams 」を参照してください。

- 自己設定アプリを使用してカンファレンスMicrosoft Teams統合を構成するには、「 Integrating Notify connector self-configured app with Microsoft Teams 」を参照してください。

でのレポートテンプレートの構成 セキュリティインシデントレスポンス

レポートテンプレートを作成して、インシデントサマリーまたはエグゼクティブサマリーを生成し、分析と共有することができます。

セキュリティインシデントレスポンスレポートテンプレート機能を使用してレポートテンプレートを作成し、インシデントのアナリストレベルまたはエグゼクティブレベルのサマリーを提供するレポートを生成します。さまざまなインシデントフィールドを使用して、要件に基づいてレポートを書式設定および構成できます。

次のテーブルで、ベースシステム内でプロビジョニングされるレポートテンプレートについて説明します。

セキュリティインシデントレスポンスのレポートテンプレート

名前	説明
アナリストステータスレポート	アナリストにセキュリティインシデントの完全な情報を提供します。
エグゼクティブサマリー	管理向けのセキュリティインシデントのステータスの概要を提供します。

注:
デフォルトでは、これらのレポートはドラフトステータスであり、読み取り専用モードです。レポートテンプレートを作成して公開するには、これらのデフォルトテンプレートを再利用する必要があります。

でのレポートテンプレートの作成 セキュリティインシデントレスポンス

アナリストサマリー用の新しいレポートテンプレートまたはインシデントのエグゼクティブサマリーを作成します。

始める前に
必要なロール：sn_si.admin

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > アドミニストレーション.
2. [レポート]、[レポートテンプレート] の順に選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[レポートテンプレート] ページに、ベースシステムで利用可能なすべてのテンプレートが表示されます。

3. **[New** (新規)] を選択します。
テンプレートの [詳細] ページを表示します。
4. テンプレートの名前と説明を入力します。
5. **[Save** (保存)] を選択します。
6. [コンテンツ] タブを選択します。
テンプレートのコンテンツページを空白のレポートとともに表示します。
7. [展開] を選択し、目的のフィールドをテンプレート本文に挿入します。
   - 共通 **SIR** フィールド:インシデントで最もよく使用されるフィールドのリスト。
   - すべての **SIR** フィールド:インシデントに関連するすべてのフィールド。たとえば、インシデントレポートを生成していて、[簡単な説明] というフィールドを追加する場合は、[すべての SIR フィールド] からそのフィールドを選択できます。[簡単な説明] フィールドは、レポートテンプレートに変数として追加されます。アナリスト向けのレポートを生成するときに、レポートにインシデントが表示される場合の簡単な説明。
   - 関連レコード:特定のインシデントの関連レコード。たとえば、関連する観測事象をレポートに追加する場合は、レポートテンプレートに追加できます。これらの関連レコードは、テーブル形式で表示されます
   - スクリプト:レポートの日時を追加するには、現在の日時スクリプトをレポートテンプレートに追加します。これにより、レポートの作成日時がレポートに追加されます。
   -
8. [コンテンツの保存] を選択して、レポートテンプレートの内容を保存します。
9. [プレビュー] を選択して、レポート形式をプレビューします。

   レポートテンプレートにすべての必須フィールドを追加したら、レポートテンプレートを公開する必要があります。

10. [公開] を選択してテンプレートを公開します。

    レポートテンプレートを公開するかどうかを確認するメッセージが表示されます。

11. オプション: その他のアクション アイコンを選択し、削除 を選択してレポート テンプレートを削除します。

レポートのシステムプロパティ

セキュリティインシデントレスポンスレポートのシステムプロパティについて、以下で説明します。

レポートのシステムプロパティ

プロパティ	説明	値
sn_si.sn_si_incident.load_all_records	このテンプレートから作成されたレポートにリストのすべてのレコードをロードします。true：すべてのレコードをロードします。false：sn_si.sn_si_incident.reporting_list_records_count プロパティで定義された特定の数のレコードをロードします。	誤り

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

レポートのシステムプロパティ (続く)

プロパティ	説明	値
sn_si.sn_si_incident.max_list_columns_allowed	Limit PDF でリストをレンダリングするときに追加できる列の数を制限します。これにより、最初からビューから許容される制限までの列が使用されます。	5
sn_si.sn_si_incident.report_default_style_object	CUI プロパティを使用して、フリーフォームフィールド、左パネル、レポートリストの css を制御します。	(JSON オブジェクト)
sn_si.sn_si_incident.reporting_list_records_count	指定の数のレコードをレポートエディターにロードします。	200
sn_si_reporting_email_template_sn_si_incident	共有ページで使用される SIR (sn_si_incident) テーブルのメールクライアントテンプレートの Sys ID。	9ce97ae643461210416896ed3ab8f258
sn_si.sn_si_incident.ctx_menu_field_header	フィールドヘッダー	sn_si_incident_report_field_header、sn_si_inc
sn_si.sn_si_incident.defang_record_list_urls	URL をデフラグするかどうかを制御します。	誤り
sn_si.sn_si_incident.reporting_dot_walk_tables	ドットウォークで結合に使用できるテーブルのリスト。	(JSON オブジェクト)

でのレポートテンプレートの複製 セキュリティインシデントレスポンス

レポートテンプレートを複製して編集するか、既存のテンプレートを再利用して新しいテンプレートを作成します。

始める前に

> **注:**
> エグゼクティブサマリーテンプレートとアナリストステータスレポートテンプレートを再利用するには、そのコピーを作成する必要があります。

エグゼクティブサマリーとアナリストステータスレポートを再利用するには、これらのコピーを作成してから、

必要なロール：sn_si.admin

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > アドミニストレーション.
2. [レポート]、[レポートテンプレート] の順に選択します。
   [レポートテンプレート] ページに、ベースシステムで利用可能なすべてのテンプレートが表示されます。
3. テンプレートを選択します。
4. [複製] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスクの結果
選択したテンプレートのコンテンツが複製され、選択したテンプレートのコピーがテンプレートのリストに表示されます。複製されたテンプレートは [ドラフト] ステータスです。コンテンツをカスタマイズし、必要に応じてテンプレートの名前を変更できます。

次のタスク
でのレポートテンプレートの編集 セキュリティインシデントレスポンス

でのレポートテンプレートの編集 セキュリティインシデントレスポンス

レポートテンプレートを編集して既存のテンプレートを再利用し、新しいテンプレートを作成します。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > アドミニストレーション.
2. [レポート]、[レポートテンプレート] の順に選択します。
   [レポートテンプレート] ページに、ベースシステムで利用可能なすべてのテンプレートが表示されます。
3. テンプレートを選択します。
   編集モードでテンプレートの [詳細] タブを表示します。
4. テンプレートの名前と説明を更新します。
5. **[Save** (保存)] を選択します。
6. [コンテンツ] タブを選択します。
   テンプレートのコンテンツページを空白のレポートとともに表示します。
7. [展開] を選択し、目的のフィールドを挿入/削除します。
   - 共通 **SIR** フィールド:インシデントで最もよく使用されるフィールドのリスト。
   - すべての **SIR** フィールド:インシデントに関連するすべてのフィールド。たとえば、インシデントレポートを生成していて、[簡単な説明] というフィールドを追加する場合は、[すべての SIR フィールド] からそのフィールドを選択できます。[簡単な説明] フィールドは、レポートテンプレートに変数として追加されます。アナリスト向けのレポートを生成するときに、レポートにインシデントが表示される場合の簡単な説明。
   - 関連レコード:特定のインシデントの関連レコード。たとえば、関連する観測事象をレポートに追加する場合は、レポートテンプレートに追加できます。これらの関連レコードは、テーブル形式で表示されます
   - スクリプト:レポートの日時を追加するには、現在の日時スクリプトをレポートテンプレートに追加します。これにより、レポートの作成日時がレポートに追加されます。
8. [コンテンツの保存] を選択して、レポートテンプレートの内容を保存します。
9. [プレビュー] を選択して、レポート形式をプレビューします。

   レポートテンプレートにすべての必須フィールドを追加したら、レポートテンプレートを公開する必要があります。

10. [公開] を選択してテンプレートを公開します。

    レポートテンプレートを公開するかどうかを確認するメッセージが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SIR ワークスペースの使用

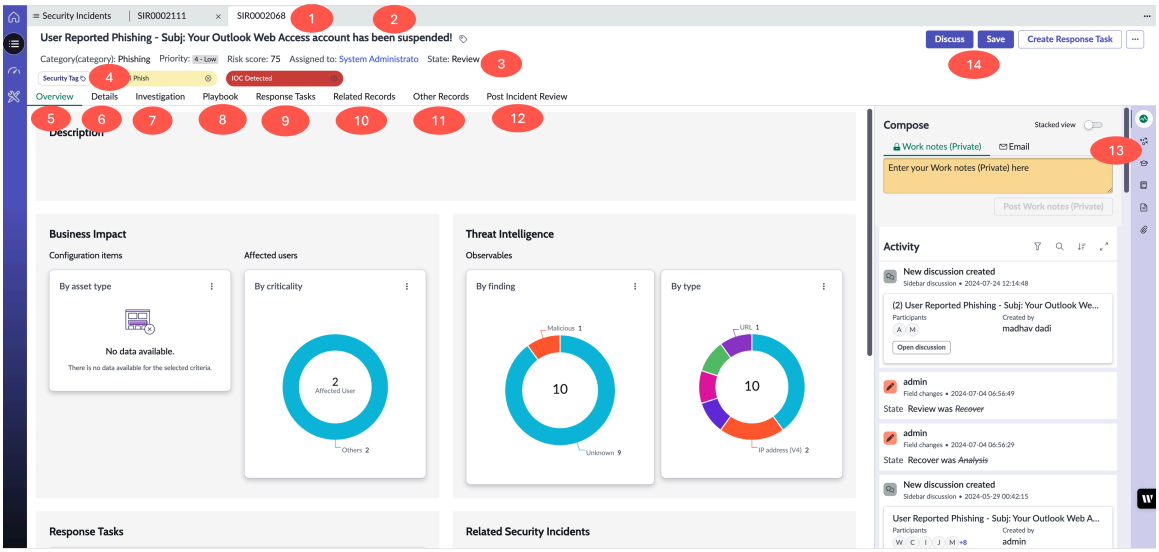
セキュリティアナリストとマネージャーは、ユーザーエクスペリエンスが改善された SIR ワークスペースを使用して、日常業務、全インシデント調査を行い、概要を把握します。

セキュリティインシデントレコードの使用

セキュリティインシデントレコードは以下で構成されます。

セキュリティインシデントレコードで利用可能な主要コンポーネント：

セキュリティインシデントの主要コンポーネント



番号	名前	説明
1	セキュリティインシデント番号	セキュリティインシデント番号はタブ名に対して使用できます。
2	簡単な説明	フォームバナーの上に表示されるセキュリティインシデントの簡単な説明。
3	フォームバナー	読み取り専用のセクション。[カテゴリ]、[優先度]、[リスクスコア]、[ステータス]、および [インシデントのアサイン] の詳細などのキーフィールドが含まれています。 **注:** ここでは通常のプラットフォームタグも適用できます。
4	セキュリティタグ	セキュリティインシデントに関連付けられたセキュリティタグを表示します。
5	概要	[説明]、タイプ別の資産の詳細で構成される [ビジネスインパクト]、重要度別の [影響を受けるユーザー]、結果別およびタイプ別の観測事象で構成される [脅威インテリジェンス] アイテム、[応答タスク]、子セキュリティインシデントおよび類似のセキュリティインシデントで構成される [関連するセキュリティインシデント] など、セキュリティインシデントのスナップショットの概要が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

番号	名前	説明
6	詳細	[詳細] タブにセキュリティインシデントフォームが表示されます。
7	調査	[調査] タブには、インシデント調査エクスペリエンスが表示されます。
8	プレイブック	Playbook は プロセスオートメーションデザイナー (PAD) によってトリガーされます。プロセスが作成され、トリガー条件がセキュリティインシデントのプレイブックをトリガーするように設定されている場合、プレイブックが表示されます。
9	対応タスク	応答タスクは、セキュリティインシデントに関連するすべての応答タスクをキャプチャします。
10	関連レコード	[関連レコード] タブは、このセクションのクラシック UI のすべての関連リストで構成されています。関連リストは、簡単に操作できるよう、[ビジネスインパクト]、[Threat Intel] などのさまざまなセクションの下にグループ化されています。
11	その他のレコード	[その他のレコード] タブは、このセクションにグループ化されて表示される変更要求、インシデント、メールなどの IT レコードで構成されます。
12	インシデントの事後レビュータブ	セキュリティインシデントが [レビュー] ステータスに進むと、[インシデントの事後レビュー] タブが表示されます。タブ内にはインシデントの事後アセスメントとレポートも表示されます。
13	コンテキストメニュー	クイックアクションに簡単にアクセスでき、アナリストが必要なときにいつでもすべてのタブからアクセスできるようにします。 コンテキストメニューを使用すると、次のような複数のリソースに簡単に移動できます。 **1.** アクティビティストリーム **2.** プレイブック **3.** アナリスト支援 **4.** Runbook **5.** テンプレート **6.** 添付ファイル
14	フォームの UI アクション	インシデントフォームの右上に、さまざまなセキュリティインシデントフォームの UI アクションが表示されます。使用可能なフォーム UI アクションは次のとおりです。 • ディスカッション • 保存 • 対応タスクを作成 • メールの作成 • プレイブックを追加

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

番号	名前	説明
		• 関連ワークフローを開く • インシデントを作成 • 問題を作成 • 変更要求の作成 • 機能停止の作成 • 重大度の計算 • 重大セキュリティインシデントへのリンク • 重大セキュリティインシデントとしての提案 • 重大セキュリティインシデントに昇格 • エンドポイントで他のアクションを実行 • 関連 MITRE ATT&CK テクニック • 以前の UI に切り替え • セキュリティケースに追加 • 削除 詳細については、「フォーム UI アクションの操作」を参照してください。

セキュリティインシデントの概要セクション

ワークスペースの [概要] セクションには、セキュリティインシデントに関連付けられた重要な情報が表示されます。

ドーナツグラフはドリルダウンすることができます。アナリストがいずれかのチャートアイテムを選択すると、その対応するタブ内にあるアイテムのフィルター済みリストビューの各レコードに移動します。たとえば、[悪意のある観測事象] を選択すると、[関連レコード] タブに悪意のある観測事象のフィルター済みリストビューの観測事象が表示されます。

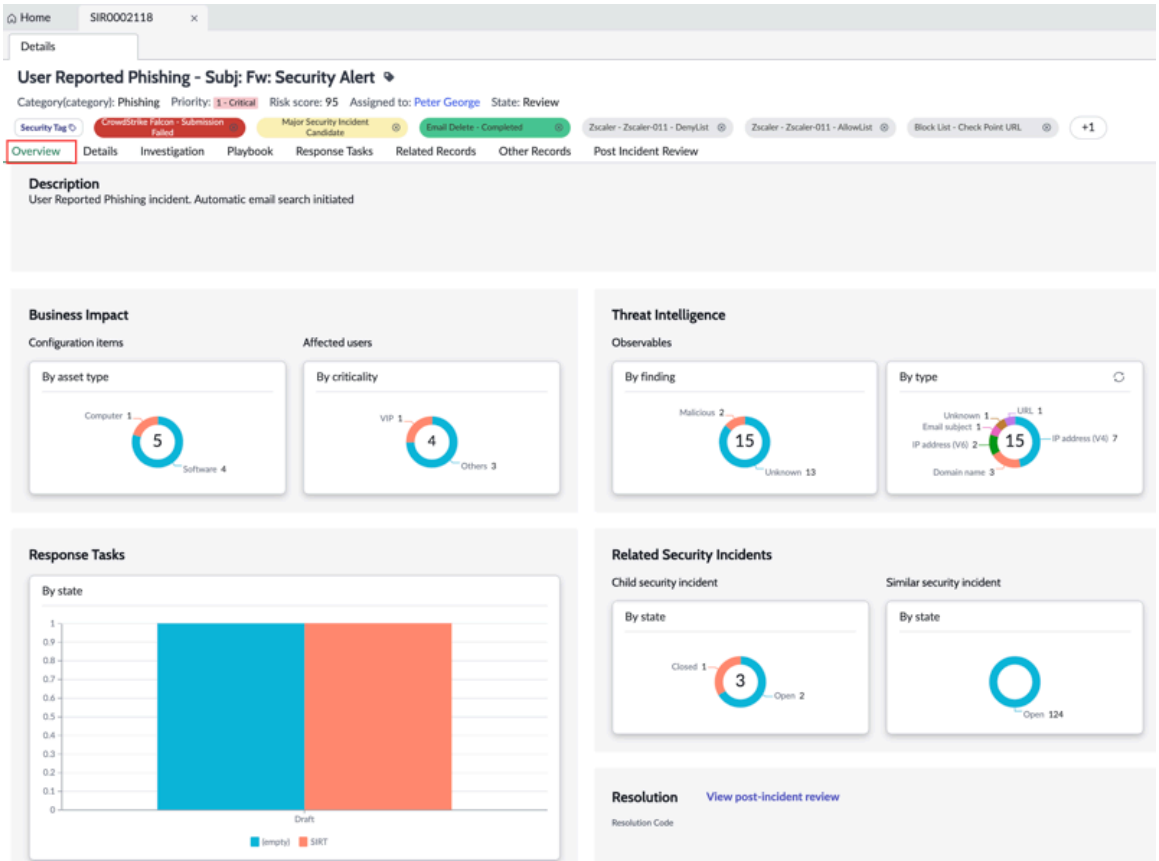
[概要] ページには次のセクションが表示されます。

- セキュリティインシデントの説明
- 資産タイプ別の構成アイテムや重要度別の影響を受けるユーザー (VIP ユーザーか他のユーザーか) など、ビジネスインパクトの詳細
- 結果別 (観測事象、悪意がある、不明) やタイプ別の観測事象などの脅威情報アイテム
- ステータスおよびアサイン先グループ別の応答タスク
- ステータス別 (オープンまたはクローズ) の子セキュリティインシデントと、ステータス別 (オープンまたはクローズ) の類似のセキュリティインシデントで構成される関連セキュリティインシデント
- インシデントが [レビュー] ステータスに移行すると [解決] セクションが表示され、インシデントの事後レビューを表示できる [概要] セクション内に [解決] セクションが表示されます。
- 解決 - インシデントの事後レビューを表示：リンクを選択して、[インシデントの事後レビュー] ページに移動します。
- インシデントがクローズされると、[解決] セクションに [解決コード]、 [解決メモ]、インシデントの事後レビューの詳細とともに [解決者] (ユーザー) が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[概要] セクション



セキュリティインシデント詳細セクション

このセクションには、セキュリティインシデントのクラシック UI からレンダリングされるセキュリティインシデントフォームのフィールドが表示されます。

クラシック UI には、作成された **[SIRW]** ビューと呼ばれるビューがあります。このビューは、新しいワークスペースの [詳細] タブにマッピングされます。必要なカスタマイズはすべてこのビューに実装する必要があります。

フォームフィールドは次のセクションにグループ化され、[詳細] タブのフォームビューに表示されます。いずれかのセクションをクリックするか、フォーム内のそれぞれのセクションに移動します。

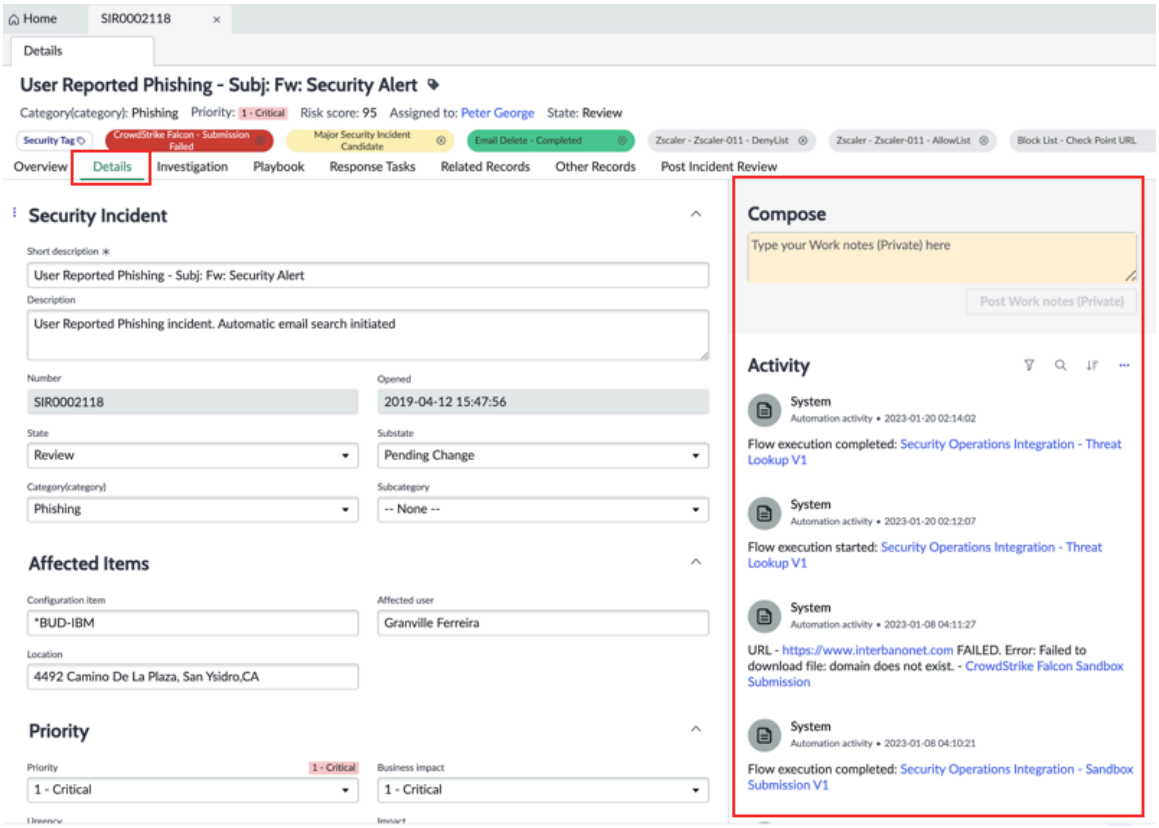
- セキュリティインシデント
- 優先度
- ソース
- 親
- アサイン
- アクセスコントロール
- 影響を受けるアイテム
- 解決

[詳細] タブには、セキュリティアナリストが素早くアクセスしてコメントを追加し投稿できるように、詳細フォーム内に [アクティビティ] ストリームセクションが含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

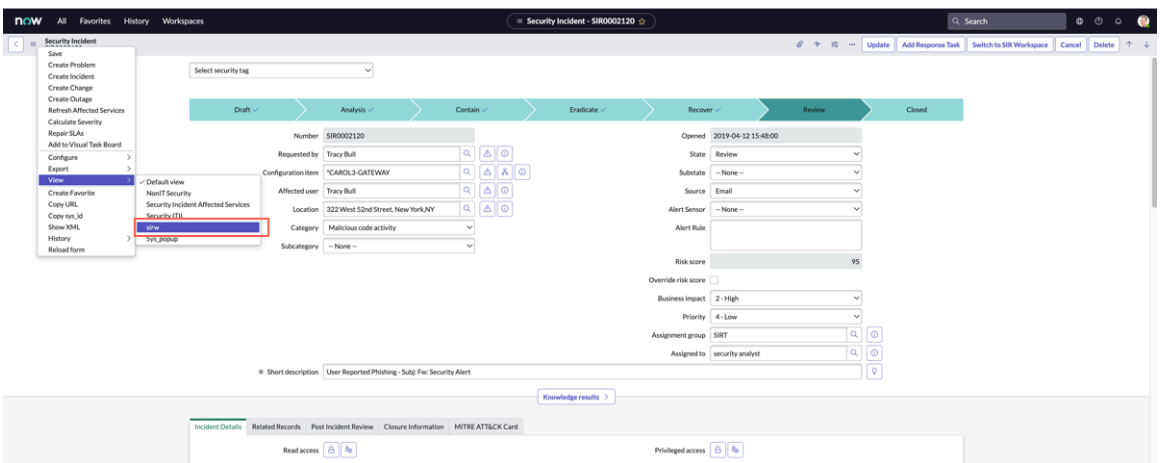
[詳細] タブとアクティビティストリーム



SIR アナリストワークスペースビューを表示するには：

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > オープンインシデントを表示.
2. 任意のセキュリティインシデントレコードを選択します。
3. コンテキストメニューをクリックし、 ビュー > **sirw**.

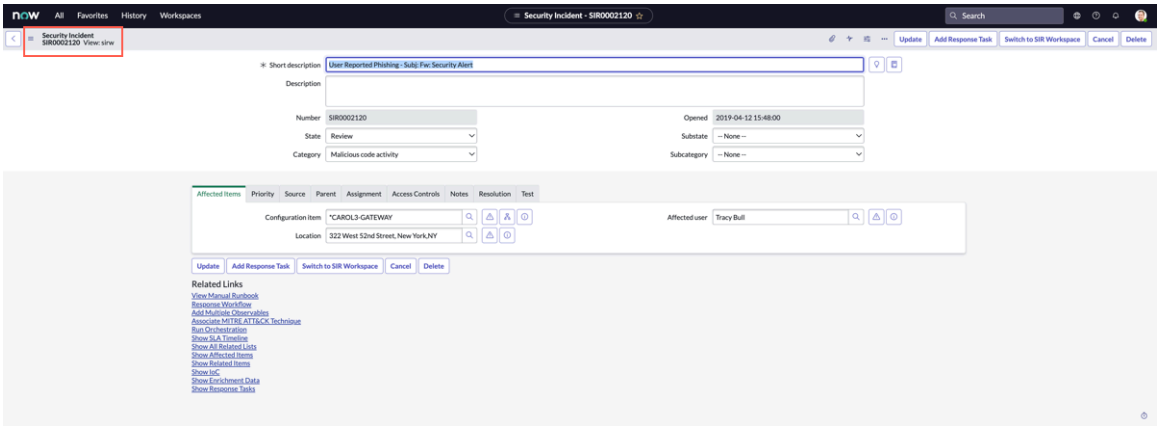
> 注:
> クラシック UI フォームの **[sirw]** ワークスペースビューを使用してカスタマイズできます。



4. セキュリティインシデントワークスペースビューは、次のように表示されます。

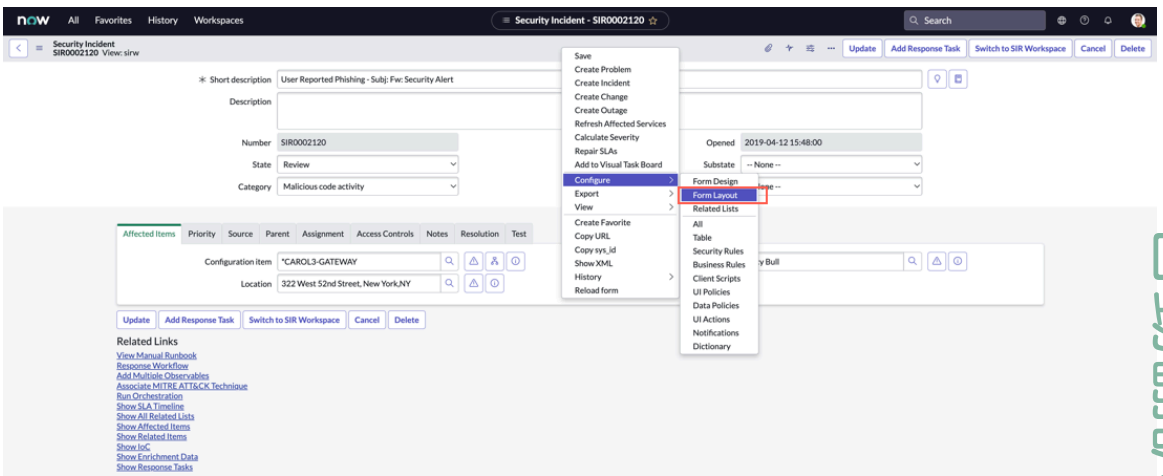
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SIR ワークスペースビュー



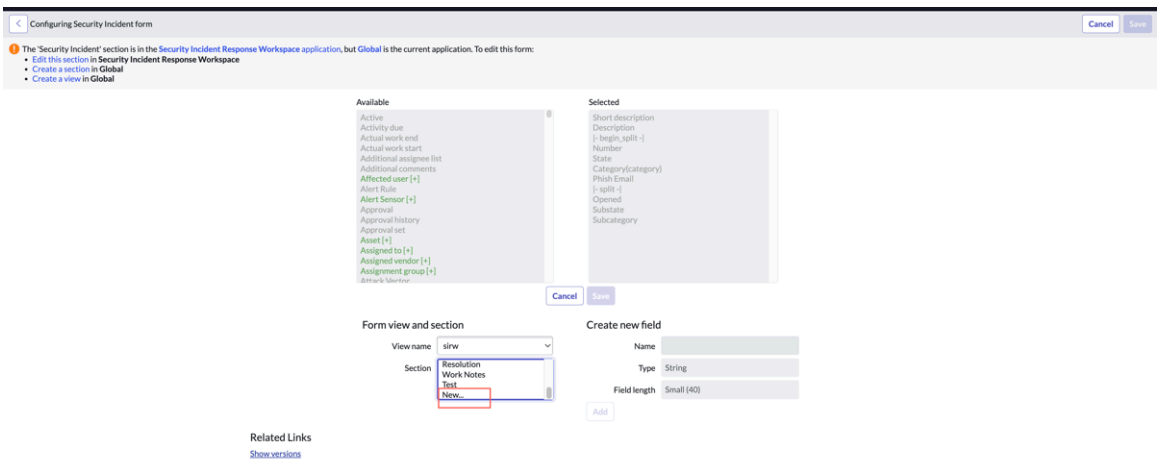
5. [Security Incident] レコードを右クリックして、 構成 > フォームレイアウト.

フォームレイアウト



6. [フォームビューとセクション] にドリルダウンし、[セクション] から [新規] を選択して新しいセクションを作成します。

フォームレイアウト - セクションビュー



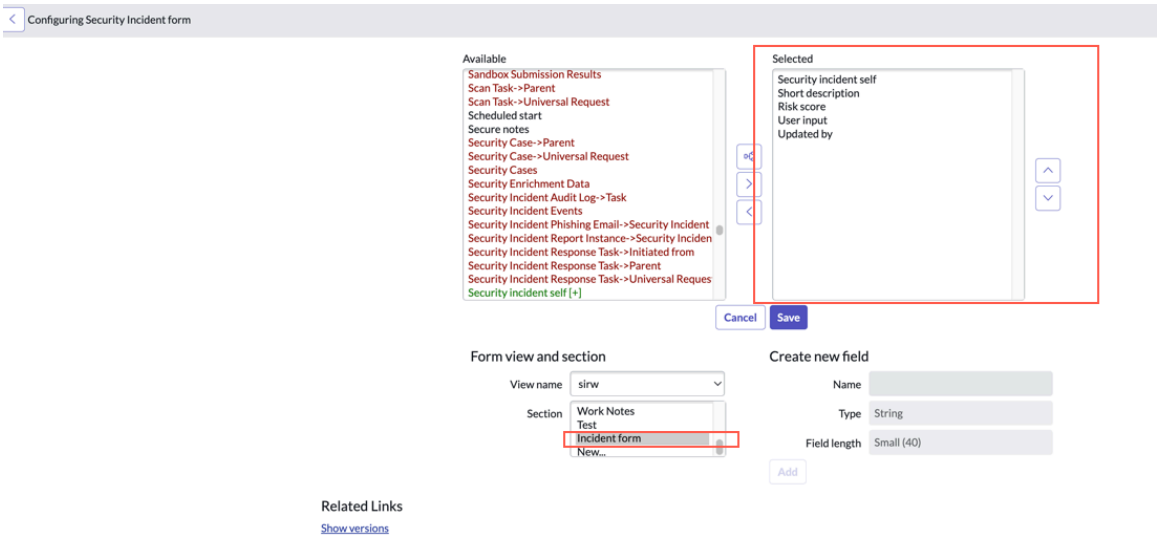
7. 新しいセクション名を入力し、**[OK]** をクリックします。

たとえば、[インシデント] フォームなどです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

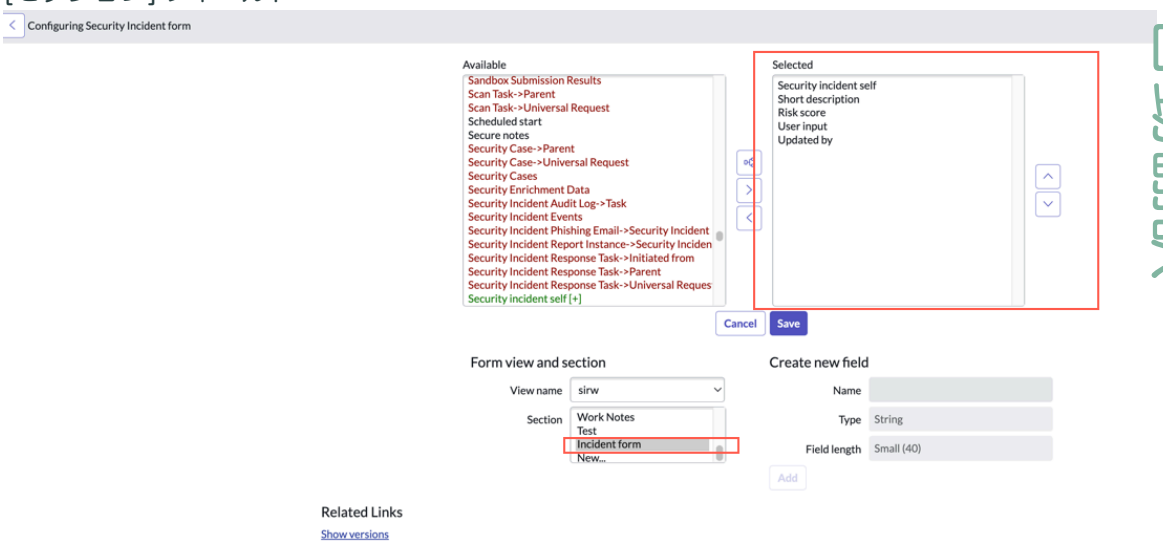
自動翻訳

8. 新しいセクションが作成され、[セクション] に追加されます。



9. 新しいセクションを選択し、必要なセクションフィールドをスラッシュバケットに追加して、[保存] をクリックします。

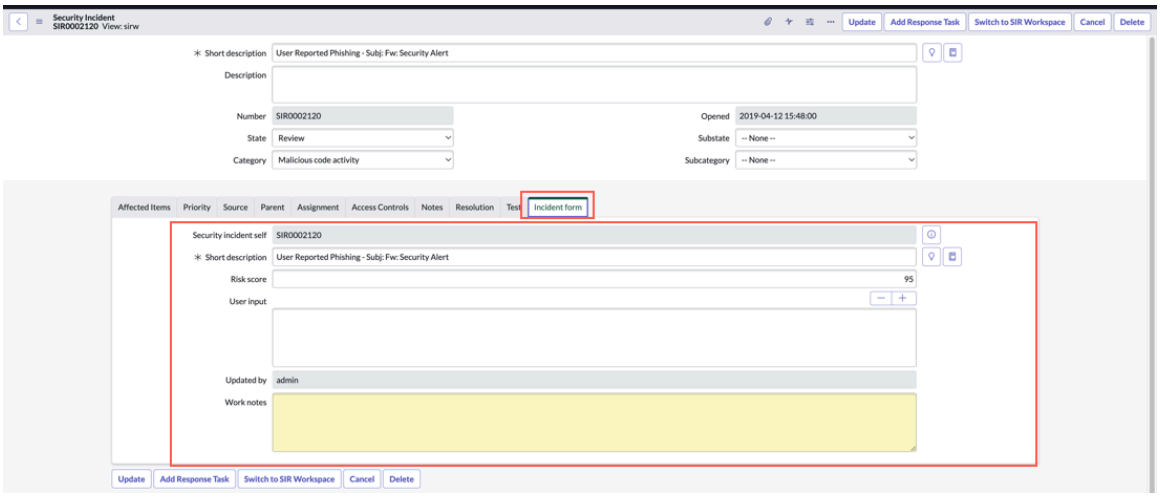
[セクション] フィールド



10. 新しく追加されたセクションは、セキュリティインシデントフォーム内の既存のセクションレイアウトとともに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



11. ここで、**[SIR** ワークスペースに切り替え] をクリックして、セキュリティインシデントフォームと、ワークスペースの [詳細] タブ内のカスタマイズされたセクションに移動します。

SIR ワークスペース オーケストレーション

セキュリティインシデントレスポンスワークスペース オーケストレーションアクティビティは、セキュリティアナリストが調査キャンバスを表示し、適用可能なさまざまなアクションを実行するのに役立ちます。

SIR ワークスペース 調査キャンバス

セキュリティインシデントレスポンスワークスペース により、セキュリティアナリストは、インシデントの修復プロセス中にセキュリティインシデントに関連する重要な情報を表示できます。重要な情報には、[観測事象]、[脅威のルックアップの結果]、[サイティング検索]、[観測事象の拡張] などの関連リストも含まれます。

クラシック UI では、すぐに利用可能な統合に関連付けられたほとんどのオーケストレーションアクションを関連リストに対して使用できます。たとえば、[脅威のルックアップを実行]、[観測事象の拡張を実行] などが [関連する観測事象] 関連リストに存在します。同様に、[ホストの詳細を取得] や [ネットワーク統計情報を取得] などは、[構成アイテム] 関連リストに対して使用できます。

セキュリティアナリストがこれらのアクションを実行すると、別の関連リストに結果が入力されます。たとえば、ユーザーが [脅威のルックアップを実行] を行うと、結果が [脅威のルックアップの結果] テーブルで利用可能になります。場合によっては、結果は複数の異なるテーブルで利用できます。このプロセスでは、セキュリティアナリストが複数の場所からの情報を相互に関連付けると、まとまりのないユーザーエクスペリエンスになります。

再ビルドされた新しい SIR ワークスペース では、[調査] キャンバス (タブ) に、アナリストが調査を実行できるように論理的にグループ化されたすべての必要情報が表示されます。

調査キャンバスの詳細

調査キャンバスの主な目的は、必要なセキュリティインシデントデータを 1 つの共通の場所に表示することです。

SIR ワークスペース 内では、セキュリティインシデントの調査は主にいくつかの重要なエントリーポイントを中心に展開されます。

ベースシステム内でセキュリティアナリスト向けにプロビジョニングされる主要なエントリーポイントは次のとおりです。

- 関連する観測事象
- 構成アイテム ID

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 影響を受けるユーザー
- 関連フィッシングメール
- メールの検索

必要に応じてエントリーポイントを追加、変更、または削除することで、上記のエントリーポイントを設定することもできます。詳細については、「SI 設計時調査の設定」を参照してください。

[調査] タブでは、エントリーポイントテーブルが親テーブルとして機能します。親テーブルで実行されたオーケストレーションアクションの結果を保持するすべてのテーブルは、エントリーポイント内の子テーブルとして表示されます。

たとえば、[関連する観測事象] エントリーポイントの場合、[関連する観測事象] テーブルが親テーブルで、[脅威のルックアップの結果]、[サンドボックスの送信結果] などの他のテーブルが子テーブルです。

セキュリティアナリストは、[関連する観測事象] テーブルですべてのオーケストレーションアクションを実行でき、複数の場所を移動しなくても同じページ内ですべての関連情報を表示できます。

注:
ユーザーが [概要] ページで悪意のある観測事象などのインタラクティブなチャートをクリックすると、調査キャンバス内の悪意のある観測事象のフィルター済みビューに移動します。または、すべてのデータがある調査キャンバスに移動して、調査を直接開始することもできます。

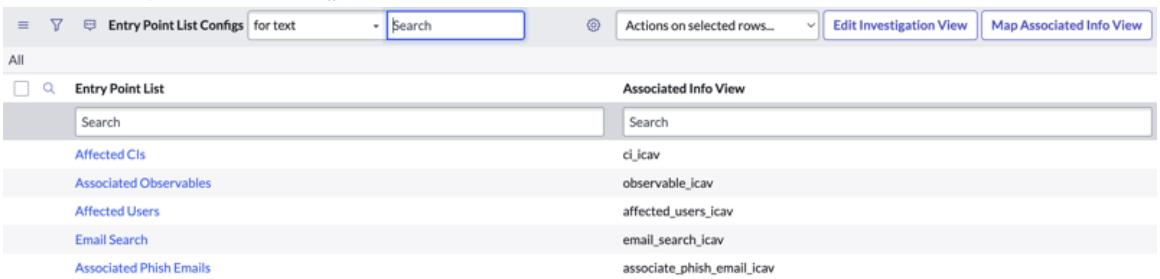
エントリーポイントの子テーブルのリストも構成可能です。詳細については、「SI 設計時調査の設定」を参照してください。

ベースシステム内で構成およびプロビジョニングされたエントリーポイント (関連する観測事象) の詳細な例を次に示します。

1. ドロップダウンリストから [関連する観測事象] エントリーポイントを選択します。

   ここでは、親テーブルも [関連する観測事象] です。

   エントリーポイントリスト構成



2. 親テーブルから 1 つ以上の観測事象を選択します。
3. 目的の機能を実行します。

   たとえば、[脅威のルックアップを実行] を選択して、選択した観測事象の脅威のルックアップの結果をフェッチします。

   注:
   対応する観測事象アクションが実行されると、プロセスがバックエンドで実行され、結果が [観測事象] リストの下に表示されます。

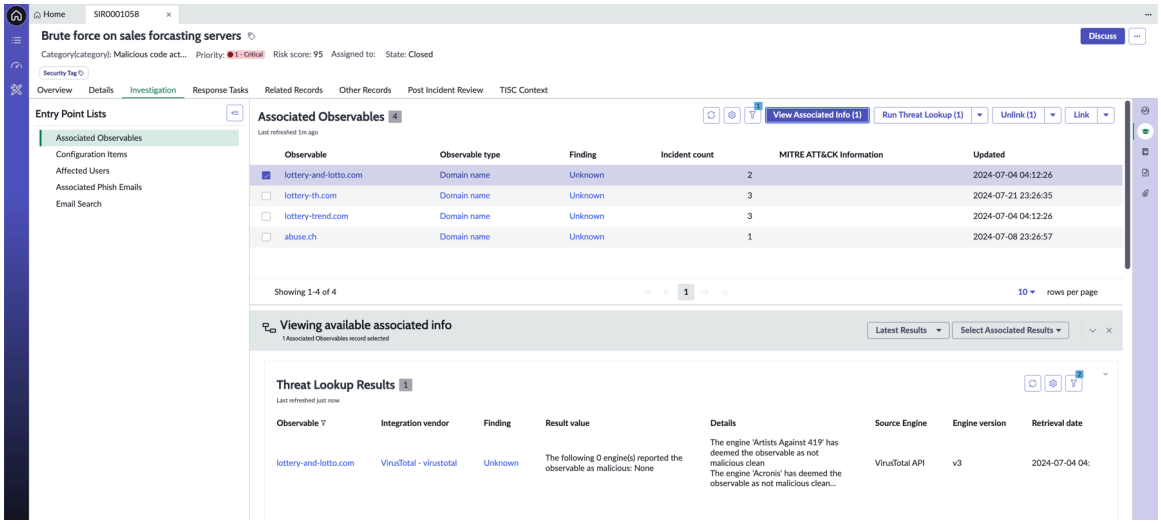
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

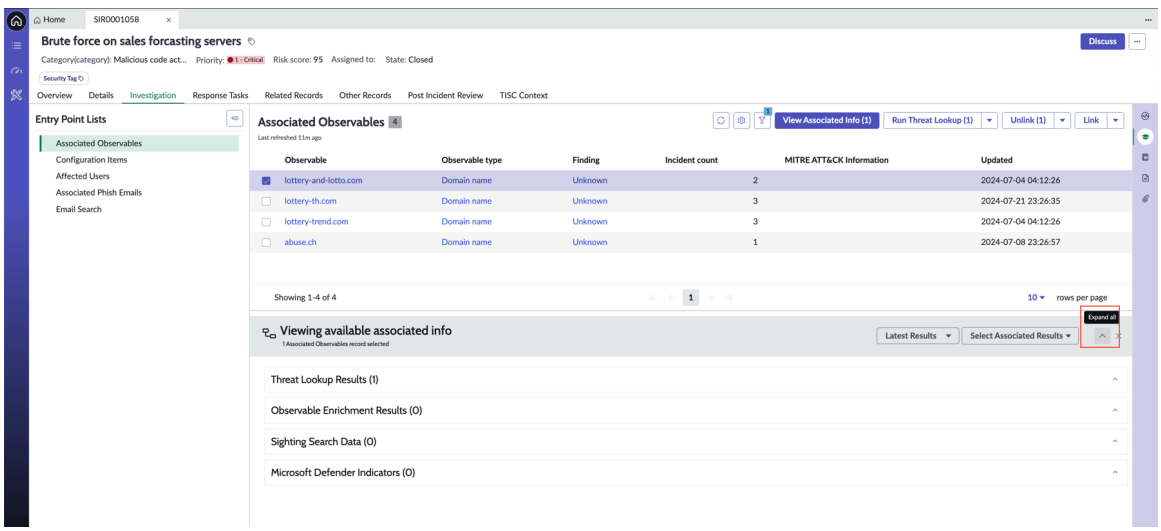
4. [関連情報を表示] をクリックして、観測事象の結果を表示します。結果は同じページに表示されます。

   注:
   結果別のフィルターを使用して結果を表示するには、[すべての結果] または [最新の結果] のいずれか適切なビューを選択します。デフォルトでは、最新の結果が表示されます。(統合の) 実装が複数ある場合は、実装ごとの最新の結果が表示されます。

   さらに、子テーブルの結果である [関連する関連リスト別 **(by associated related lists)]** で結果をフィルタリングできます。デフォルトでは、構成されたすべての子テーブル関連リストが表示されます。詳細については、「SI 設計時調査の設定」を参照してください。ただし、必要な子テーブルのみを選択することもできます。



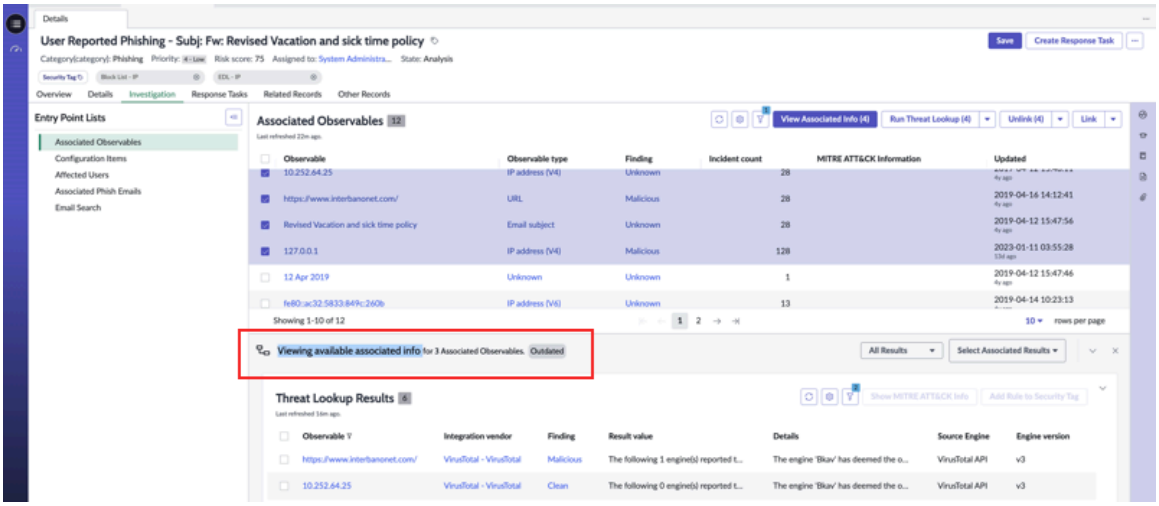
5. [関連情報を表示] をクリックすると、関連するすべての子テーブルデータを 1 つの場所で表示でき、[ビューを閉じる] ボタンを選択することで関連リストビューを閉じることができます。ビューを閉じると、前と同じように観測事象の親テーブルのみが表示されます。
6. [利用可能な関連情報を表示しています] 結果テーブル内の [すべて展開] 上方向アイコンをクリックして、すべての関連リストの子テーブルデータを展開します。



7. 下向き矢印の [すべて折りたたむ] アイコンをクリックすると、関連リストの子テーブルデータがすべて折りたたまれます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
すべての子テーブルデータを含む関連情報セクションの上部にあるバナーには、ユーザーに表示されている観測可能な関連情報の数が表示されます。たとえば、最初に 2 つの観測事象を選択して [関連情報を表示] をクリックすると、バナーに **[2** つの関連する観測事象について利用可能な関連情報を表示中 **(Viewing available associated info for 2 Associated Observables)]** と表示されます。たとえば、別の観測事象を選択すると、その情報が期限切れであることを示すバナーが表示されます (以下のスクリーンショットを参照)。最新のデータを取得するには、[関連情報を表示] を再度クリックする必要があります。



観測事象関連情報の上記の包括的なビューに加えて、親テーブルのレコードに関する詳細情報を表示するには、観測事象をクリックして、親テーブルレコードフォームを別のタブで開き、選択したレコードのより詳細なビューを表示します。選択した特定のレコードの関連するすべての子テーブルデータも [関連情報] セクションに表示されます。

ただし、[関連情報] セクションには、調査キャンバスに表示される子テーブルの最新の結果のみが読み取り専用モードで表示されます。このビューではアクションは実行できません。子テーブルのフォームページを新しいタブで開くと、任意のアクションの全機能を使用できるページが表示されます (ある場合)。

ドロップダウンリストを使用して、さまざまなテーブルを切り替えることができます。[関連情報] セクションで各フォームを展開したり折りたたんだりすることもできます。

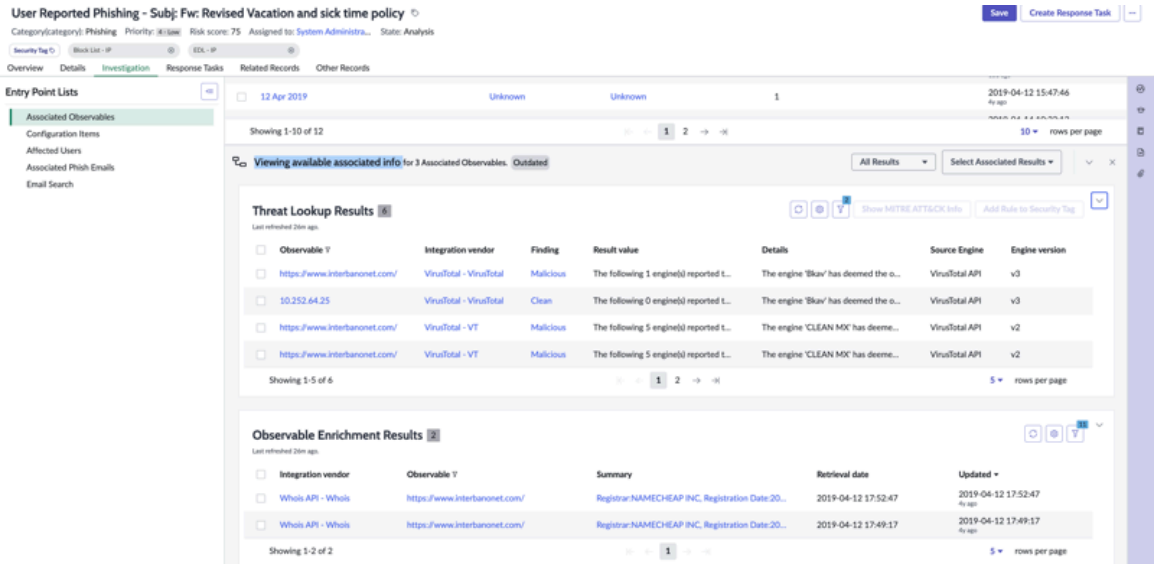
[観測事象] フォームページ (親テーブルレコードフォームページ) 内で、利用可能な特定のアクションを実行できます。アクションを実行するたびに、関連情報バナーをクリックしてデータを更新できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

8. [すべて展開] をクリックして、すべての関連リストの子テーブルを展開します。デフォルトでは、すべての子が展開されます。

観測事象を展開したビュー



関連情報

SI 設計時調査の設定

機能フレームワークを利用した統合のための統一されたエクスペリエンスフレームワーク

クラシック UI では、脅威の検索の実行、サイティング検索の実行などのオーケストレーションアクティビティを実行すると、まとまりがなくなります。実行時のエクスペリエンスは各機能に特有のものです。新しいワークスペースでは、すべての機能が統一されています。

統一されたエクスペリエンスは、機能フレームワークに含まれる統合およびオーケストレーションアクティビティにのみ適用されます。Microsoft Defender でのインジケーターの作成など、統合に固有のアクションが存在する可能性があります。これらのアクションには、ユースケースに必要な独自のエクスペリエンスがあります。

新しいフレームワークは、以下で説明する 3 つのステップを含むモーダル画面で構成されています。

1. 実装：最初のステップでは、選択した機能に対して存在する 1 つ以上の実装を選択します。

   たとえば、アナリストが [脅威のルックアップを実行] をクリックすると、[脅威のルックアップを実行] 機能に存在する 1 つ以上の実装を選択できます。

   各実装には統合ソースの詳細が含まれます。以下のテーブルを参照してください。各実装に対する補足情報も表示されます。

   補足情報には、フィルター、サポートされている観測事象のタイプなどの情報を含めることができます。補足情報は必要に応じて設定できます。詳細については、UX フレームワークを技術的に構成する手順を参照してください。

統一実装フレームワークモーダル

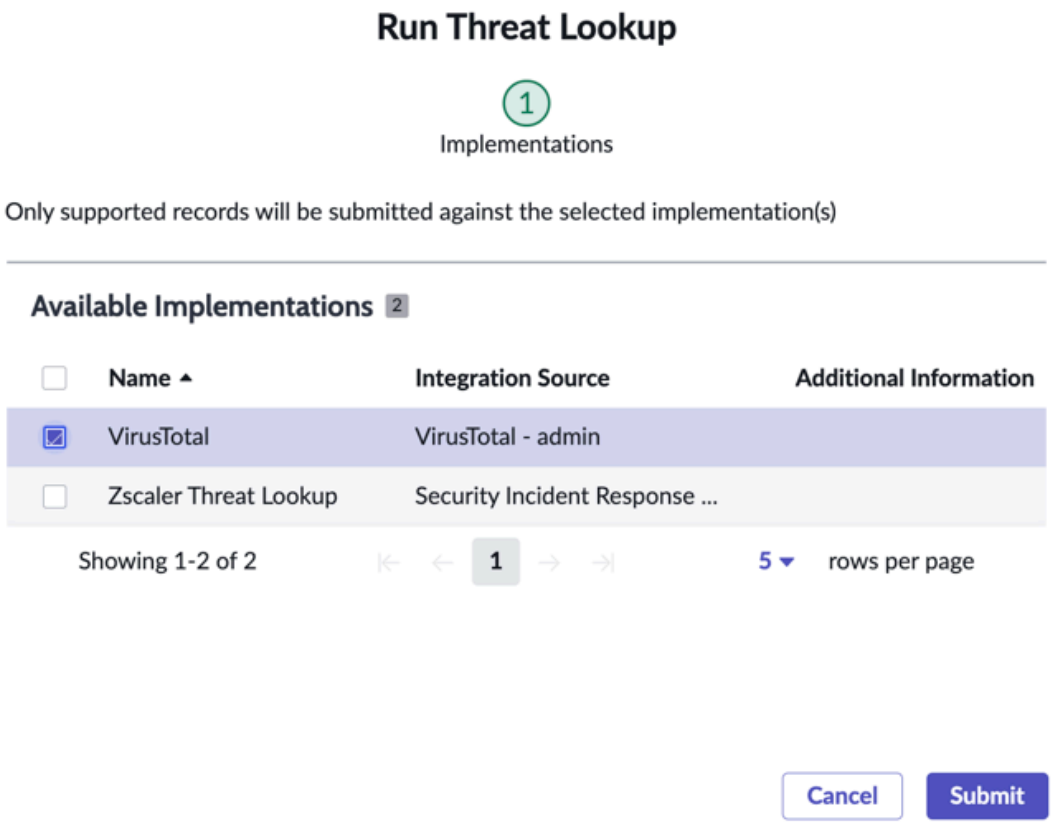
実装	説明
名前	実装の名前。
統合ソース	使用されている構成などの実装のソース。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

実装	説明
追加情報	この列は、アクションを続行するために、選択した実装に対してセキュリティアナリストにコンテキストを提供する静的情報をキャプチャします。たとえば、サポート性やフィルタリングされた情報などです。また、実装が [ドメイン] や [URL] などの特定のタイプの観測事象のみをサポートしている場合は、この列に補足情報を追加して、ユーザーにコンテキストを提供できます。 **注:** UI フレームワークでは、基本的に、あらゆるタイプの実装とあらゆるタイプの観測事象を選択できます。送信中、同梱される既存のベースシステム統合がバックエンドでフィルタリングを処理し、サポートされているタイプの観測事象のみを送信します。サポート性と一致しない残りのレコードは無視されます。このため、機能を選択すると、[選択した実装に対してサポートされているレコードのみが送信されます] という UI 情報メッセージが表示されます。

画面 1：実装

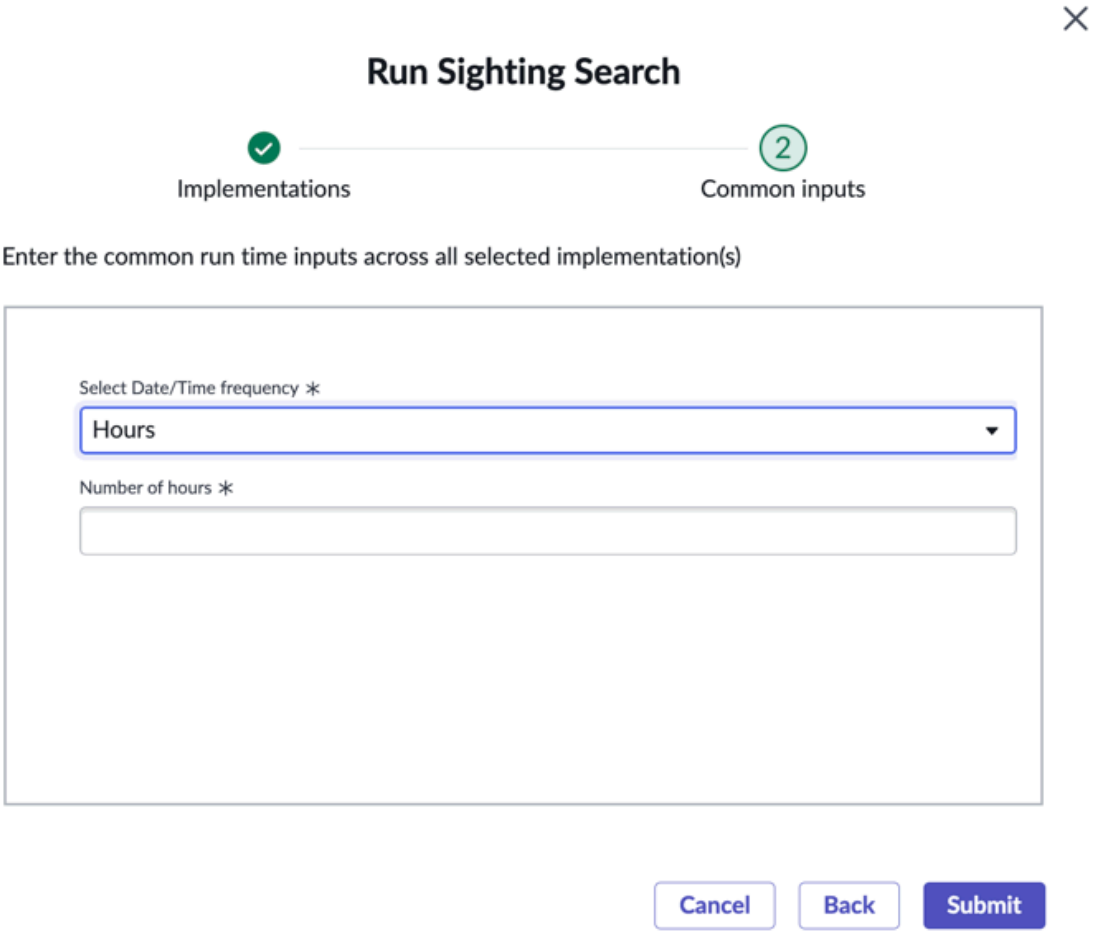


自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. 共通入力 **(Common inputs)**：選択した実装または選択したすべての適用可能な実装に共通する入力を追加します。これは実装の画面 2 です。たとえば、現在、共通入力画面があるのは [サイティング検索] のみです。この実装は、画面 1 (実装) と画面 2 (共通入力) の組み合わせです。

画面 **1** + 画面 **2**

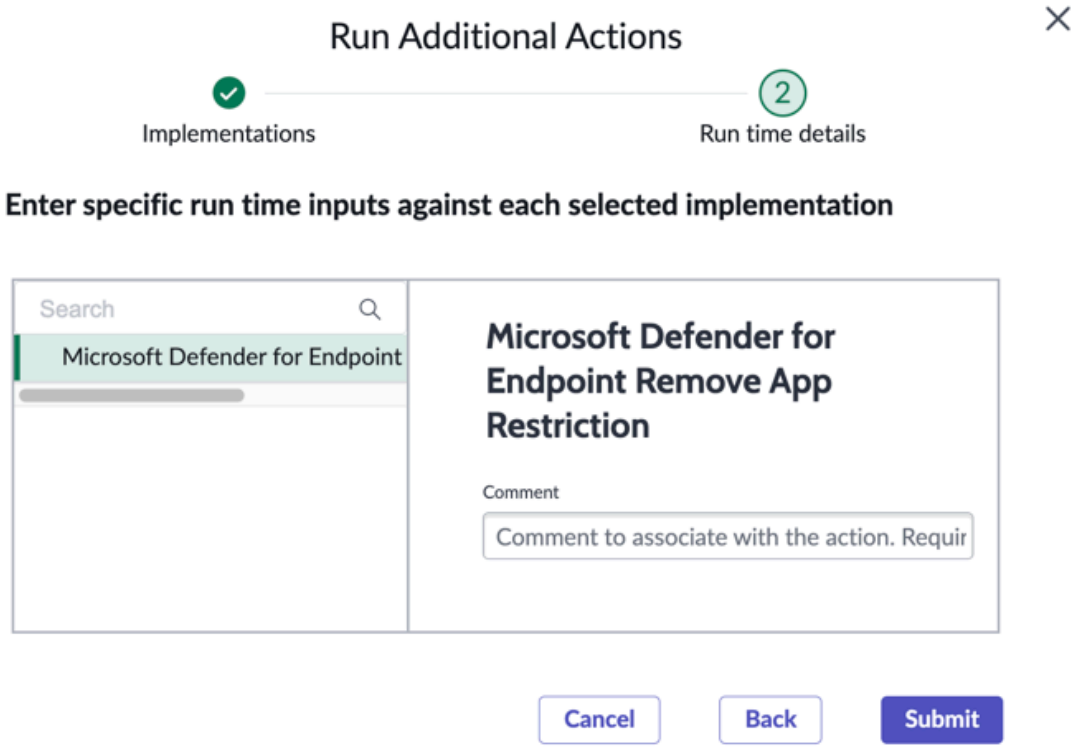


自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 実行時間の詳細 **(Run time details)**：選択した実装に対して、他の実装とは異なる特定の実行時間入力を追加します。これは実装の画面 3 です。この実装は、画面 1 (実装) と画面 3 (特定の実行時間入力) の組み合わせです。

特定の入力



注:
必ずしも 3 つのステップすべてが必要なわけではありません。機能と必要な入力のタイプに応じて、実行時間の詳細ステップと共通入力ステップが表示されます。

統一されたエクスペリエンス機能とモーダル画面

次の表で、機能と適用される画面について説明します。

機能	適用される **UX** フレームワーク画面	サポートされる統合
脅威のルックアップを実行	画面 1 の [実装を選択 (Select Implementations)] のみが適用されます。 [脅威のルックアップの実行] に適用される共通入力または実装固有の入力はありません。 したがって、1 つ以上の実装を選択する画面 1 のみがセキュリティアナリストに表示されます。実装を選択すると、セキュリティアナリストはアクションを送信できるようになります。	• ウイルス合計 • ハイブリッド分析 • セキュリティインシデントレスポンスと zScaler の統合 • PhishTank • MetaDefender • ThreatCrowd • Have I Been Pawned? • Crowd Strike Falcon Intelligence

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

機能	適用される **UX** フレームワーク画面	サポートされる統合
観測事象の拡張を実行	画面 1 の [実装を選択 (Select Implementations)] のみが適用されます。 [観測事象の拡張を実行] に適用される共通入力または実装固有の入力はありません。 したがって、1 つ以上の実装を選択する画面 1 のみがセキュリティアナリストに表示されます。実装を選択すると、セキュリティアナリストはアクションを送信できるようになります。	• MISP • Microsoft Defender for Endpoint • Shodan • RiskIQ • WHOIS • Reverse WHOIS
サイティング検索を実行/Web サイティング検索を実行 (Run Web Sighting Search)/メールサイティング検索を実行 (Run Email Sighting Search)	画面 1 の [実装を選択 **(Select Implementations)]** および画面 2 の [共通入力 **(Common Inputs)]** が適用されます。 サイティング検索では、Splunk およびその他の統合の複数の実装に共通する入力として日付と時刻の頻度が使用されます。 この画面は、日時の頻度を取得するセキュリティアナリストに表示されます。 FireEye HX など、これらの入力を必要としない統合の場合は無視されます。実装を 1 つ以上選択し、共通入力を指定すると、セキュリティアナリストはアクションを送信できるようになります。	• Splunk - Incident Enrichment • Carbon Black • Elasticsearch • FireEye HX • McAfee ESM • Microsoft Defender for Endpoint • Splunk Sighting • QRadar Sightings Search • MISP
サンドボックスに送信	画面 1 の [実装を選択 (Select Implementations)] および画面 3 の [実装固有の入力 (Implementation specific inputs)] が適用されます。 [サンドボックスに送信] は、実装ごとに異なる入力を受け取ります。現在、この機能に共通の入力はありません。 たとえば、アナリストが CrowdStrike Falcon X Quick Scan、CrowdStrike Falcon X Windows 64、 CrowdStrike Falcon X Linux、および Zscaler を選択した場合、入力	• CrowdStrike Falcon X Sandbox 統合 • セキュリティインシデントレスポンスと zScaler の統合

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

機能	適用される UX フレームワーク画面	サポートされる統合
	は変化します。CrowdStrike Falcon X Quick Scan および Zscaler には、それ以上の実行時間入力は必要ありません。CrowdStrike Falcon X Windows 64 は、CrowdStrike Falcon X Linux とは異なるオプションの実行時間入力を受け取ります。したがって、これらは個別に選択された実装に対して必要に応じて画面 3 で指定できます。	
ウォッチリストに公開	画面 1 の [実装を選択 (Select Implementations)] のみが適用されます。 [ウォッチリストに公開] に適用される共通入力または実装固有の入力はありません。 したがって、1 つ以上の実装を選択する画面 1 のみがセキュリティアナリストに表示されます。実装を選択すると、セキュリティアナリストはアクションを送信できるようになります。	CrowdStrike Falcon ホスト
要求を許可またはブロック	画面 1 の [実装を選択 (Select Implementations)] のみが適用されます。 [要求を許可またはブロック] に適用される共通入力または実装固有の入力はありません。 したがって、1 つ以上の実装を選択する画面 1 のみがセキュリティアナリストに表示されます。実装を選択すると、セキュリティアナリストはアクションを送信できるようになります。	• Palo Alto Network NGFW • Check Point NGFW • セキュリティインシデントレスポンスと zScaler の統合
ホストの詳細を取得	画面 1 の [実装を選択 (Select Implementations)] のみが適用されます。 [ホストの詳細を取得] に適用される共通入力または実装固有の入力はありません。 したがって、1 つ以上の実装を選択する画面 1 のみがセキュリティアナリストに表示されま	• FireEye HX • Microsoft Defender for Endpoint

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

機能	適用される **UX** フレームワーク画面	サポートされる統合
	す。実装を選択すると、セキュリティアナリストはアクションを送信できるようになります。	
ファイルを取得	画面 1 の [実装を選択 (Select Implementations)] および画面 2 の [共通入力 (Common Inputs)] が適用されます。 [ファイルを取得] はファイル名、パスを共通入力として受け取ります。実装を 1 つ以上選択し、共通入力を指定すると、セキュリティアナリストはアクションを送信できるようになります。	FireEye HX
ネットワーク統計情報を取得	画面 1 の [実装を選択 (Select Implementations)] のみが適用されます。 [ネットワーク統計情報を取得] に適用される共通入力または実装固有の入力はありません。したがって、1 つ以上の実装を選択する画面 1 のみがセキュリティアナリストに表示されます。実装を選択すると、セキュリティアナリストはアクションを送信できるようになります。	• FireEye HX • NetStat
実行中プロセスを取得	画面 1 の [実装を選択 (Select Implementations)] のみが適用されます。 [実行中のプロセスを取得] に適用される共通入力または実装固有の入力はありません。 したがって、1 つ以上の実装を選択する画面 1 のみがセキュリティアナリストに表示されます。実装を選択すると、セキュリティアナリストはアクションを送信できるようになります。	• FireEye HX • Carbon Black • システムコマンド
実行中のサービスを取得	画面 1 の [実装を選択 (Select Implementations)] のみが適用されます。 [実行中のサービスを取得] に適用される共通入力または実装固有の入力はありません。	FireEye HX

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

機能	適用される UX フレームワーク画面	サポートされる統合
	したがって、1 つ以上の実装を選択する画面 1 のみがアナリストに表示されます。実装を選択すると、アナリストはアクションを送信できるようになります。	
ホストを隔離/ホストの隔離を解除	画面 1 の [実装を選択 (Select Implementations)] および画面 3 の [実装固有の入力 (Implementation specific inputs)] が適用されます。 [ホストを隔離]/[ホストの隔離を解除] は、実装ごとに異なる入力を受け取ります。 現在、この機能に共通の入力はありません。たとえば、アナリストがエンドポイントに FireEye HX と Microsoft Defender を選択した場合、入力は変化します。 FireEye HX には実行時間入力は必要ありません。一方、Microsoft Defender は [隔離タイプ] や [コメント] などの入力を受け取ります。 したがって、これらは個別に選択された実装に対して必要に応じて画面 3 で指定できます。	• FireEye HX • Microsoft Defender for Endpoint • Carbon Black
他のアクションを実行	画面 1 の [実装を選択 (Select Implementations)] および画面 3 の [実装固有の入力 (Implementation specific inputs)] が適用されます。 [追加のアクションを実行するホスト (Run Additional Actions Host)] は、実装ごとに異なる入力を受け取ります。現在、この機能に共通の入力はありません。 たとえば、アナリストが FireEye HX Standard Investigative Details Script、FireEye HX Triage Acquisition、および CrowdStrike Falcon Insight	• FireEye HX • Microsoft Defender for Endpoint • CrowdStrike Falcon Insight

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

機能	適用される **UX** フレームワーク画面	サポートされる統合
	reg unload を選択すると、入力は変化します。 FireEye HX Standard Investigative Details Script と FireEye HX Triage Acquisition は、両方で異なる可能性がある入力として [コメント] を受け取ります。CrowdStrike Falcon Insight reg unload は [サブキー (Subkey)] を入力として受け取ります。 したがって、これらは個別に選択された実装に対して必要に応じて画面 3 で指定できます。 **注:** 現在、選択できる実装は 1 つのみです。将来のリリースでは、実装の複数選択がサポートされる予定です。	

統一されたエクスペリエンスの例

この例は、統一されたエクスペリエンスフレームワークの機能を示しています。

例 1：実装を選択 **(Select** implementations)：脅威のルックアップ

以下の例は、実装を示しています。

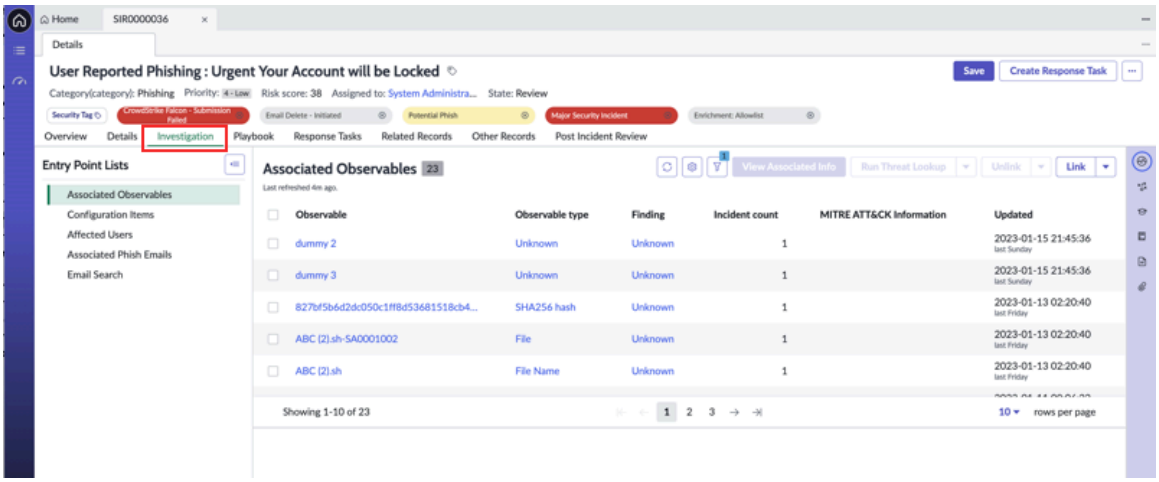
例 1：画面 **1** のみ：脅威のルックアップ

SIR ワークスペース の [調査] タブを使用して、[脅威のルックアップを実行] 関連の統合機能アクションを実行できます。

1. [調査] タブで、ページの左側に表示される [エントリーポイントリスト **(Entry Points Lists)]** セクションに移動します。
2. 任意のエントリーポイントを選択し、統合機能アクションを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
ワークスペースの [関連レコード] タブに移動して、統合機能アクションを実行することもできます。

[脅威のルックアップ] は、統合の実行方法を詳細に説明する例の 1 つです。

実装の選択

必要に応じて実装を 1 つ以上選択します。

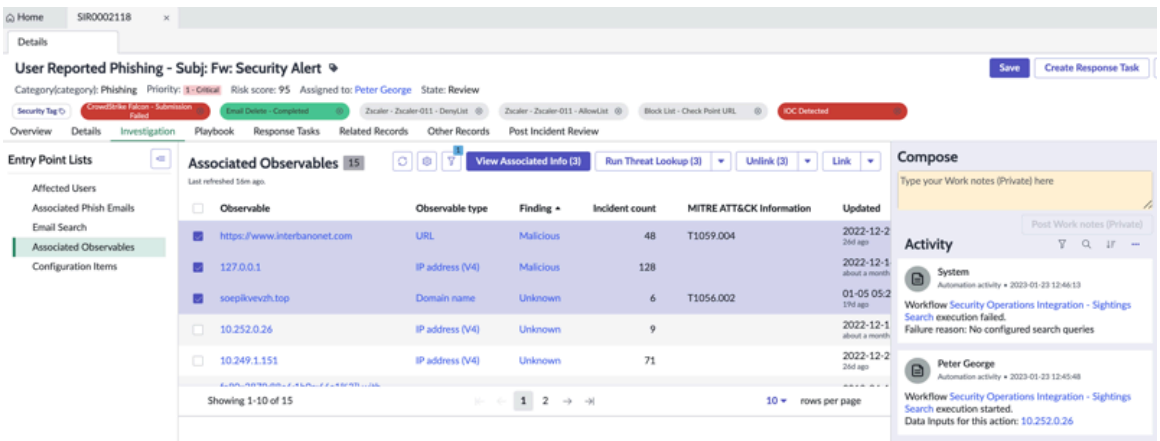
始める前に

必要なロール：sn_si.analyst

利用可能な実装が一覧表示されます。実装を選択します。選択すると、選択した各実装に対してサポートされているレコードのみが送信されます。

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. 任意のセキュリティインシデントを開きます。
3. ワークスペースの [調査] タブに移動します。
   エントリーポイントリストを含む [調査] タブが表示されます。



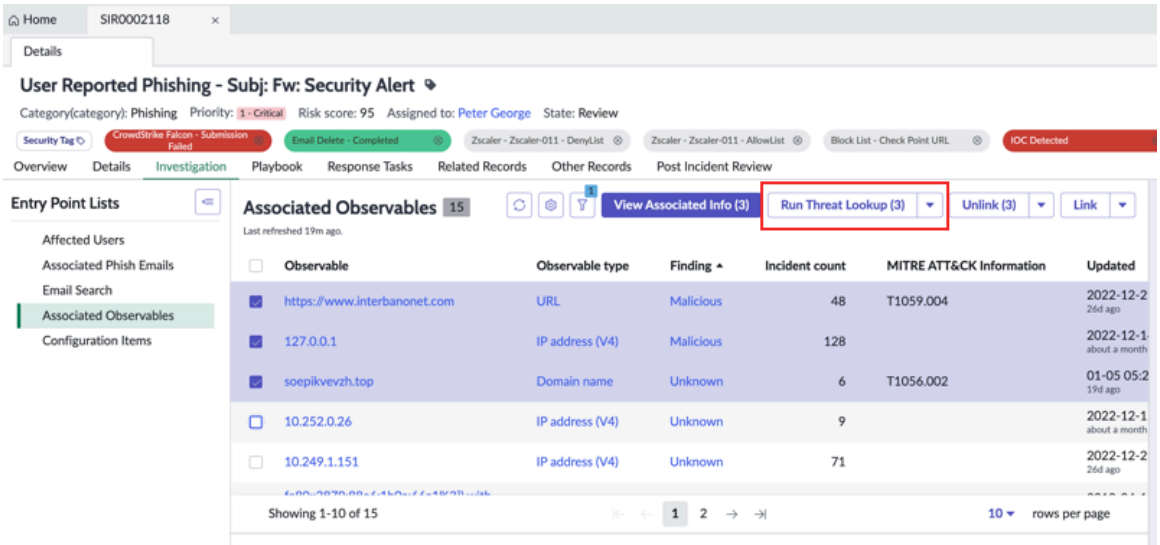
4. エントリーポイントリストから関連する観測事象を選択します。
   たとえば、 関連する観測項目 関連付けられます対応する観測事象レコードが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:
選択した観測事象に対してルックアップを実行する実装を選択するか、すべての実装を選択してルックアップを実行できます。

脅威のルックアップを実行

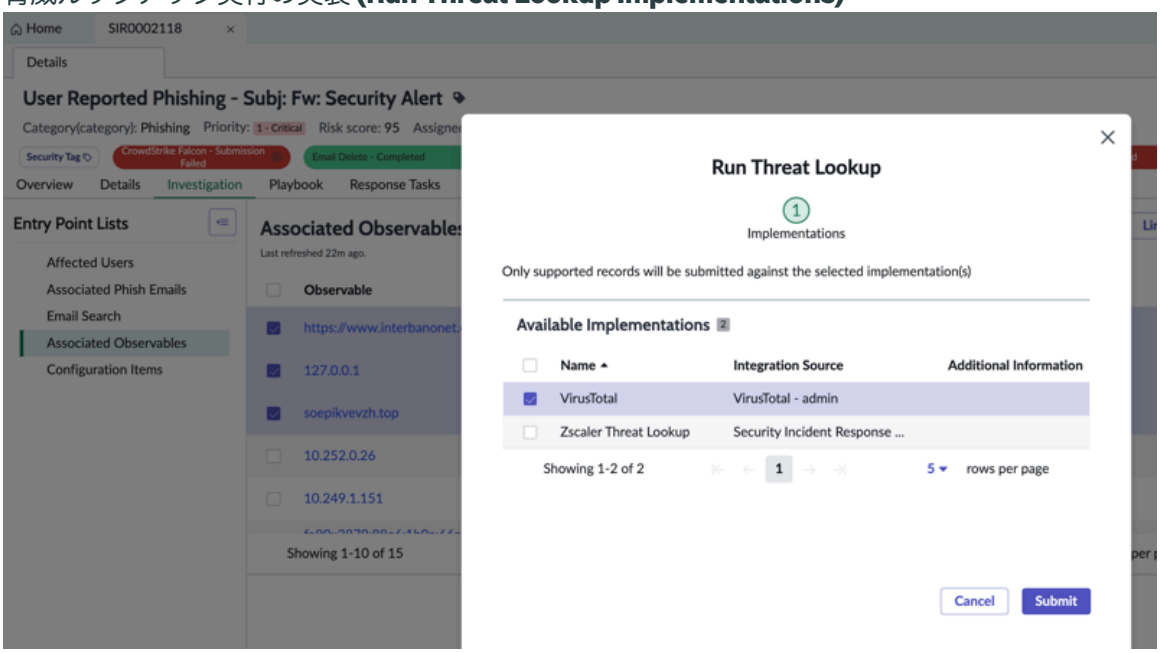


5. 脅威のルックアップを実行する観測事象のチェックボックスをオンにします。
6. 関連リストページの上部に表示される関連リストアクションドロップダウンに移動します。
7. [脅威のルックアップを実行] を選択して、脅威インテリジェンス関連の統合機能アクションを実行します。

注:
[脅威のルックアップを実行] 機能では、脅威インテリジェンスのルックアップを実行し、1 つ以上の観測事象が既知のセキュリティ上の脅威に関連するかどうかを判断します。

[脅威ルックアップ実行の実装 **(Run Threat Lookup Implementations)**] モーダル画面が表示されます。

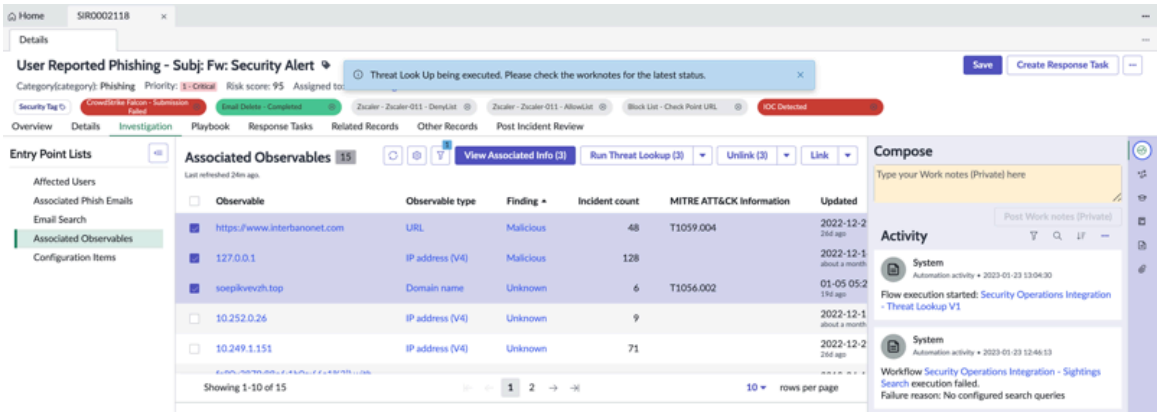
脅威ルックアップ実行の実装 **(Run Threat Lookup Implementations)**



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

8. リストから実装を 1 つ以上選択します。
9. [送信] をクリックします。
   選択したレコードが送信されると、ルックアップが実行されていることを示すメッセージが表示されます。実装がバックエンドで処理されると、結果が [脅威のルックアップの結果] 関連リストセクションに表示されます。また、それぞれの実装アクティビティが [アクティビティ] セクションに表示されます。2 つのアクティビティ (1 つは実装が実行開始されたとき、もう 1 つは実行が完了したとき) が表示されます。



> **注:**
> 関連する観測事象関連リストなどの **[Threat Intel]** 関連リストが [脅威のルックアップの結果] セクションに表示され、[サイティング検索] 関連リストが関連レコードの下の [発生検索結果] セクションに表示されます。

例 2：共通入力 (Common Inputs)：サイティング検索

以下の例は、共通入力機能アクションを示しています。

SIR ワークスペース の [調査] タブを使用して、[サイティング検索を実行] 関連の統合機能アクションを実行できます。

1. [調査] タブで、ページの左側に表示される [エントリーポイントリスト **(Entry Points Lists)**] セクションに移動します。
2. 各エントリーポイントを選択し、統合機能アクションを実行します。

> **注:**
> ワークスペースの [関連レコード] タブに移動して、統合機能アクションを実行することもできます。

実装への共通入力の追加

必要に応じて、選択したすべての実装に適用される共通の実行時間入力を追加します。

始める前に

必要なロール：sn_si.analyst

利用可能な実装が一覧表示されます。実装を選択します。選択すると、選択した各実装に対してサポートされているレコードのみが送信されます。

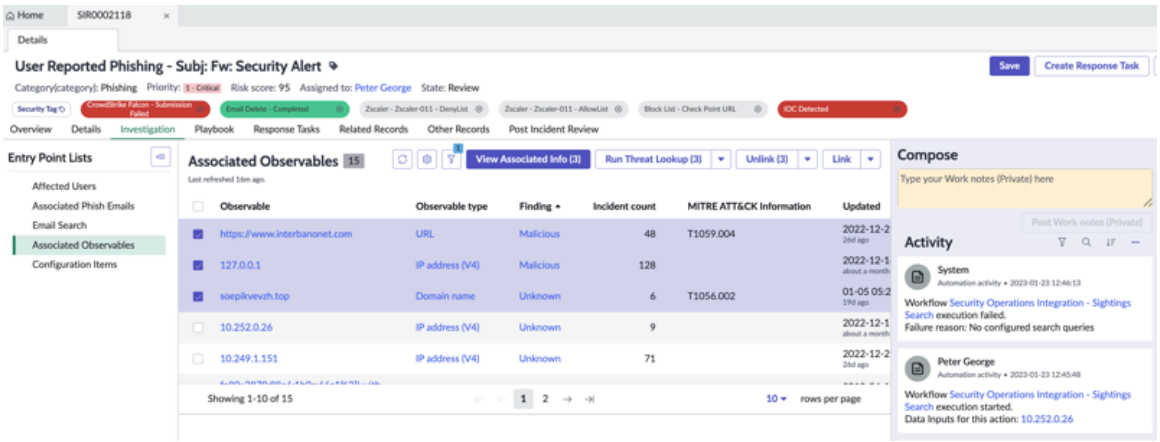
手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. 任意のセキュリティインシデントを開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

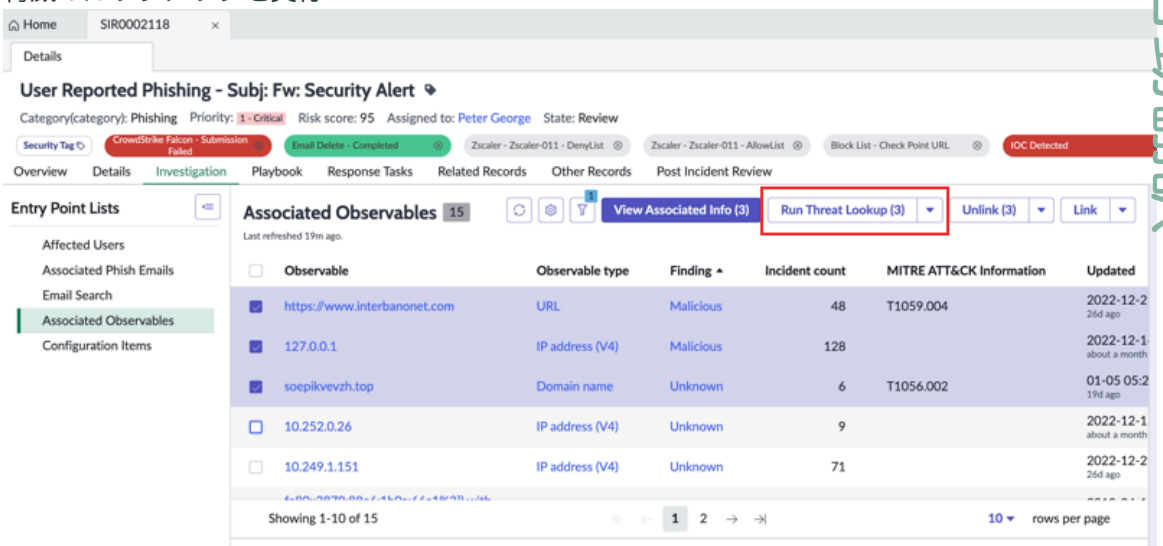
3. ワークスペースの [調査] タブに移動します。
   エントリーポイントリストを含む [調査] タブが表示されます。



4. エントリーポイントリストから関連する観測事象を選択します。
   たとえば、 関連する観測項目 関連付けられます対応する観測事象レコードが表示されます。

   注:
   実装を 1 つまたは複数選択し、選択した観測事象に対してサイティング検索を実行できます。

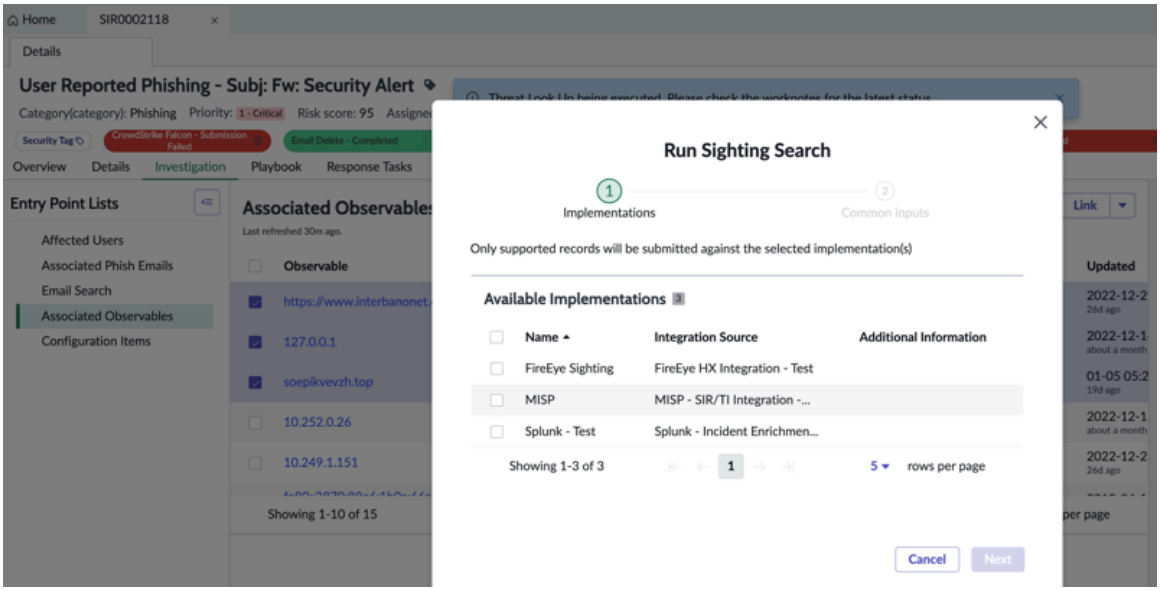
   脅威のルックアップを実行



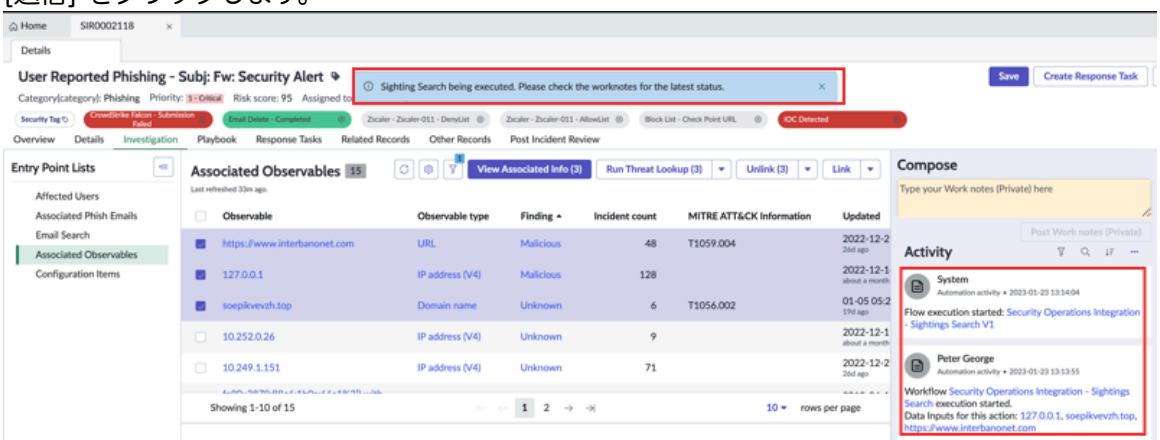
5. 脅威のルックアップを実行する観測事象のチェックボックスをオンにします。
6. [サイティング検索を実行] を選択してメール検索を実行します。
   [サイティング検索を実行] の [実装] モーダルダイアログボックスが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サイティング検索機能を選択して共通の実行時間入力を追加する方法を示す例



7. リストから実装を 1 つ以上選択します。
8. [次へ] をクリックします。
   選択したレコードが送信されると、サイティング検索が要求されていることを示すメッセージが表示されます。実装がバックエンドで処理されると、結果が [サイティング検索] 関連リストセクションに表示されます。また、それぞれの実装アクティビティが [アクティビティ] セクションに表示されます。2 つのアクティビティ (1 つは実装が実行開始されたとき、もう 1 つは実行が完了したとき) が表示されます。
9. 共通の実行時間入力値を選択します。
10. [送信] をクリックします。



選択したレコードが送信されると、サイティング検索が要求されていることを示すメッセージが表示されます。実装がバックエンドで処理されると、結果が [発生検索結果] 関連リストセクションに表示されます。また、それぞれの実装アクティビティの処理ステータスが [アクティビティ] セクションに表示されます。

例 3：特定の実行時間の詳細の入力を実装 [他のアクションを実行] に追加する

特定の実行時間の詳細の入力を実装 [他のアクションを実行] に追加します。

SIR ワークスペース の [調査] タブを使用して、[他のアクションを実行] 関連の統合機能アクションを実行できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

1. [調査] タブで、ページの左側に表示される [エントリーポイントリスト **(Entry Points Lists)]** セクションに移動します。
2. 各エントリーポイントを選択し、統合機能アクションを実行します。

   注:
   ワークスペースの [関連レコード] タブに移動して、統合機能アクションを実行することもできます。

実装への特定の入力の追加

必要に応じて、選択した各実装に特定の実行時間入力を追加します。

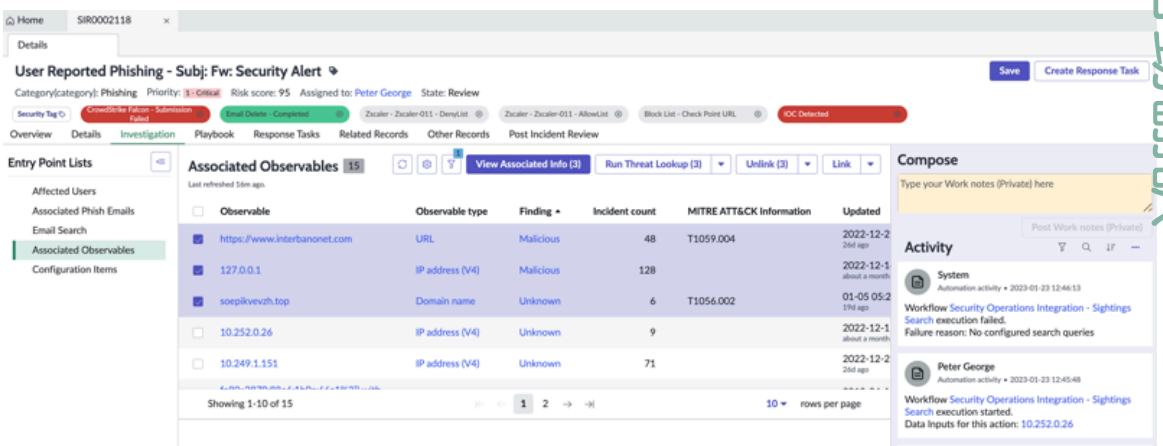
始める前に

必要なロール：sn_si.analyst

利用可能な実装が一覧表示されます。実装を選択します。選択すると、選択した各実装に対してサポートされているレコードのみが送信されます。

手順

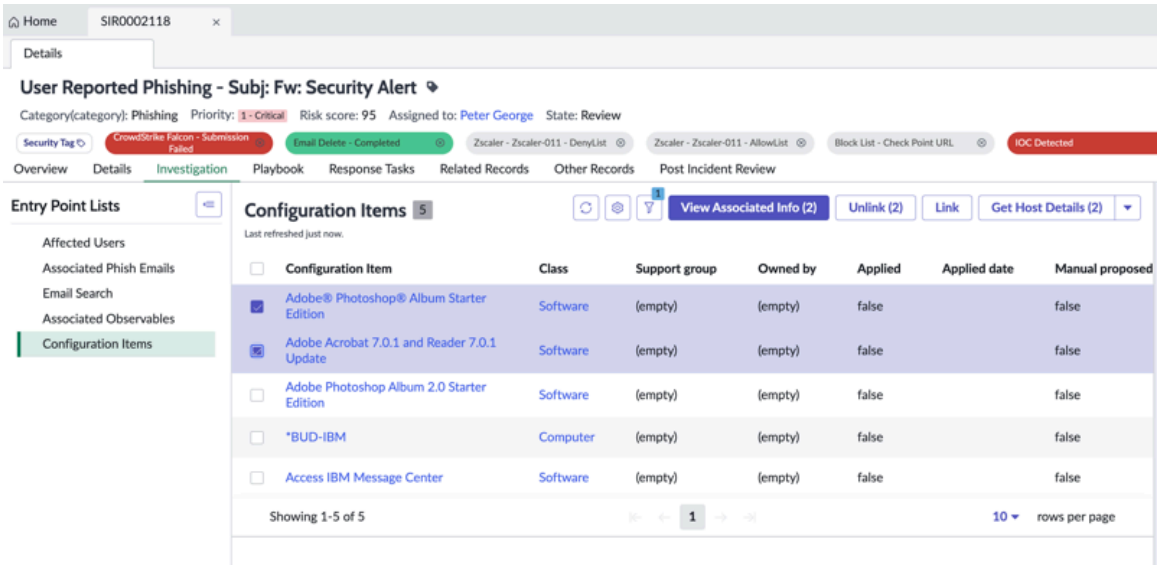
1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. 任意のセキュリティインシデントを開きます。
3. ワークスペースの [調査] タブに移動します。
   エントリーポイントリストを含む [調査] タブが表示されます。



4. エントリーポイントリストから構成アイテムを選択します。
   たとえば、[構成アイテム] エントリーポイントリストを選択します。対応する構成アイテムレコードが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

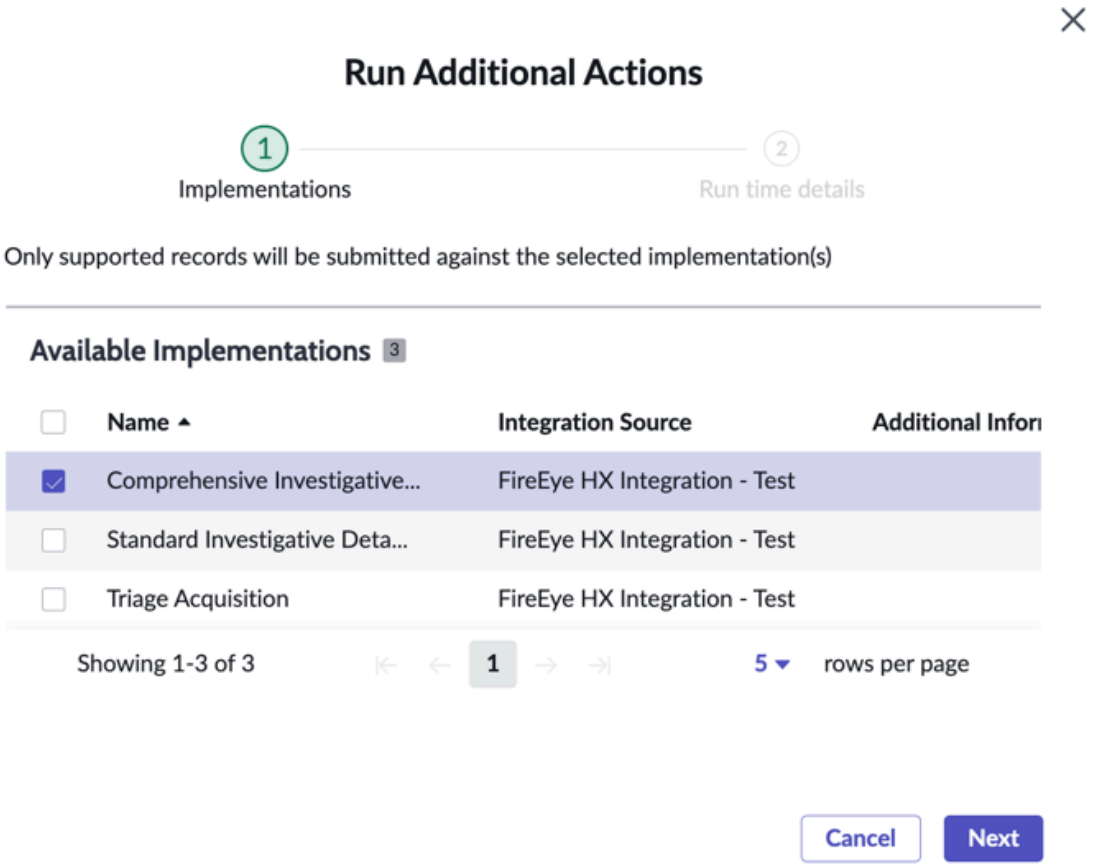
構成アイテムの選択



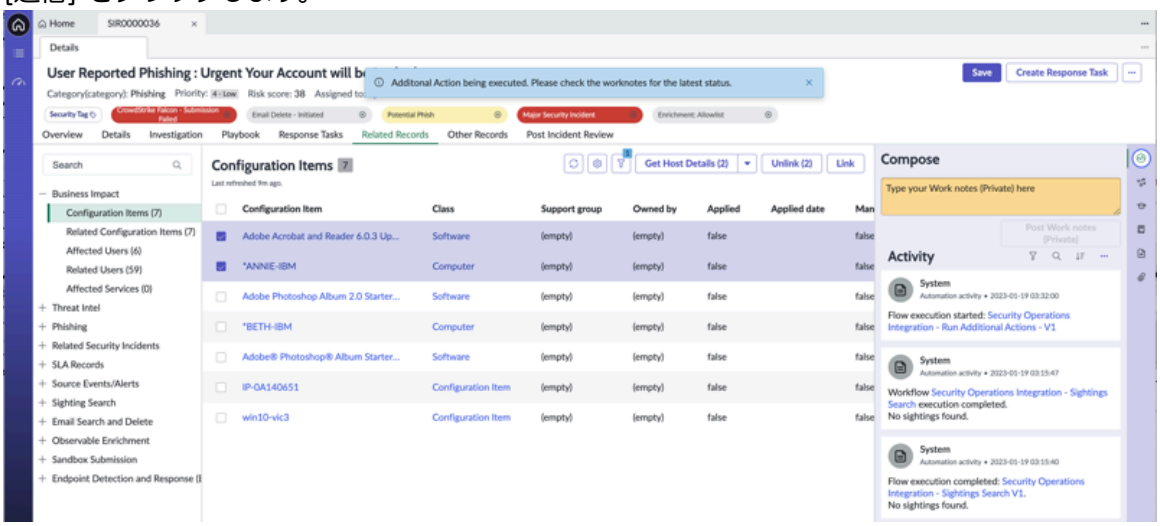
5. 任意の構成アイテムを選択します。
6. ページの上部に表示される関連リストドロップダウンに移動します。
   セキュリティインシデント構成アイテム (CI) の場合、ドロップダウンリストには次の機能アクションのリストが含まれています。リストされている CI アクションは結果を収集し、セキュリティインシデントの拡張データとして保存します。
   - ファイルを取得：この機能は、特定のハッシュ値またはファイル名を持つファイルを取得するアクションを実行します。
   - ホストを隔離：この機能は、他のデバイスへのシステム接続を制限します。
   - ホストの詳細を取得：この機能は、ホストの詳細、ログインしているユーザーの詳細、およびその他の拡張機能を取得します。
   - 他のアクションを実行：この機能は、標準アクション以外のアクションを追加で実行します。
   - ネットワーク統計情報を取得：この機能は、影響を受けるリソースのネットワーク統計情報を取得します。
   - 実行中のプロセスを取得：この機能は、ホストから構成アイテム (CI) で実行中のプロセスのリストを取得します。
   - ログオンユーザーを取得：ログオンユーザーのデータを収集し、セキュリティインシデントに関連付けます。
7. [他のアクションを実行] を選択して、脅威インテリジェンス関連の統合機能アクションを実行します。
   [他のアクションを実行] の [実装] モーダルダイアログボックスが表示されます。
8. リストから実装を 1 つ以上選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



9. **[Next]** をクリックします。
   次のステップに移動して、実行時間の詳細を追加します。
10. アクションに関連付けるコメントを入力します。
11. [送信] をクリックします。



選択したレコードが送信されると、[他のアクション] 要求が実行されていることを示すメッセージが表示されます。また、それぞれの実装アクションの進行状況が [アクティビティ] セクションに表示されます。

12. [EDR] 関連リストセクションの結果を表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

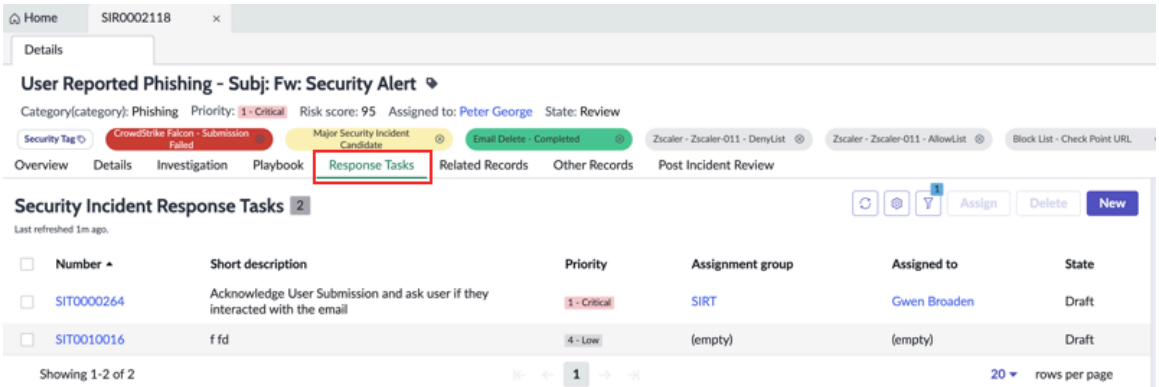
セキュリティインシデントレスポンスタスク

[応答タスク] セクションには、セキュリティインシデントに関連するすべての応答タスクが表示されます。

アナリストは次のことができます。

- 新しい応答タスクの作成
- 自身または他のユーザーへの応答タスクのアサイン
- 応答タスクの削除

ワークスペースの応答タスク



注:
応答タスクをすばやく編集するには、応答タスクを選択すると、応答タスクのリストが表示されるので、レコードを選択して変更を加え、応答タスクを保存します。

応答タスクの作成

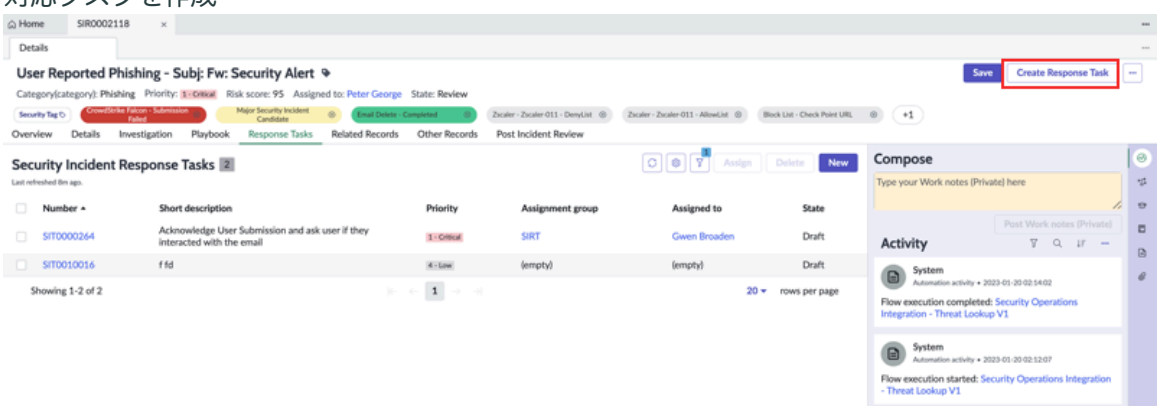
応答タスクを作成して、セキュリティ問題に対応するために実行する個別のアクションを追跡します。

始める前に
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. UI アクションから [対応タスクを作成] をクリックします。

対応タスクを作成



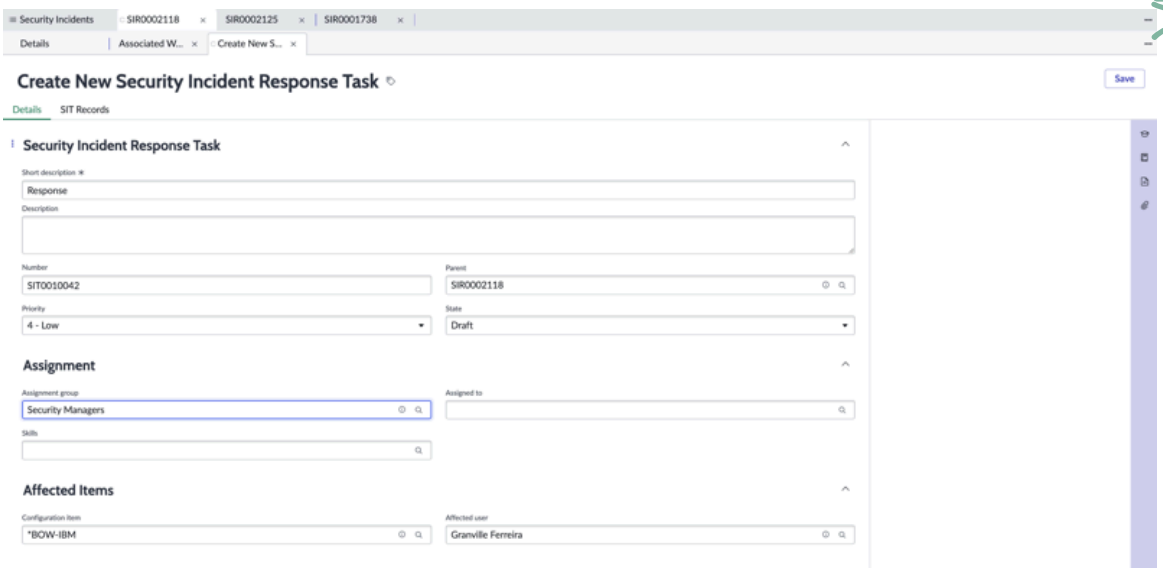
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 必要に応じて、フォームのフィールドに入力します。

セキュリティインシデント

フィールド	説明
簡単な説明	セキュリティインシデントレスポンス タスクの説明。
説明	選択したタスクの説明。
数値	セキュリティインシデントに対して自動的に生成される一意の番号。
親	関連するセキュリティインシデントの番号。
優先度	このタスクをいつ実行するかを決定するために使用される優先度。
状況	セキュリティ応答タスクの現在のステータス。デフォルトでは、初期ステータスは [ドラフト] です。
アサイン先グループ	アサインされるワーカーが選択されるアサイン先グループ。
アサイン先	タスクを実行するようアサインされる個人。
スキル	このタスクを実行するために必要なスキル。ルックアップから検索し、必要なスキルを選択します。
影響を受けるアイテム	セキュリティ上の問題によって影響を受けるアイテム。
構成アイテム	セキュリティ上の問題によって影響を受ける構成アイテム。
影響を受けるユーザー	セキュリティ上の問題によって影響を受けるユーザー。



4. [保存] をクリックします。
新しい応答タスク (SIT) が作成されます。

セキュリティインシデントレスポンスのその他のレコード

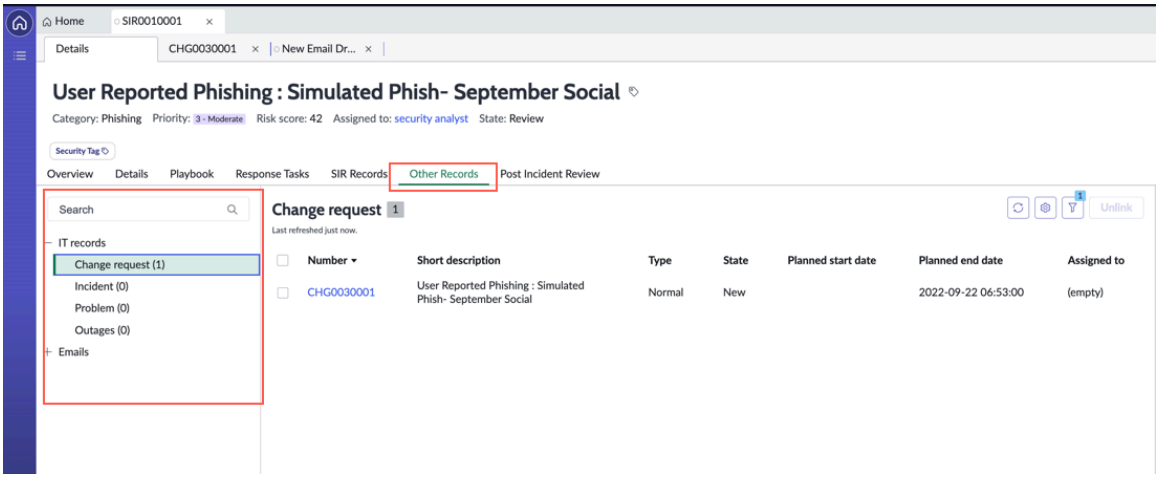
このセクションには、IT 関連レコードやメールレコードなどの他のレコードが表示されます。[IT] レコードの下に、[インシデント]、[変更要求]、[問題]、および [機能停止] が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[メール] の下に、 [ドラフト]、 [送信メール]、および [受信済みメール] が表示されます。

その他のレコード



インシデントの作成

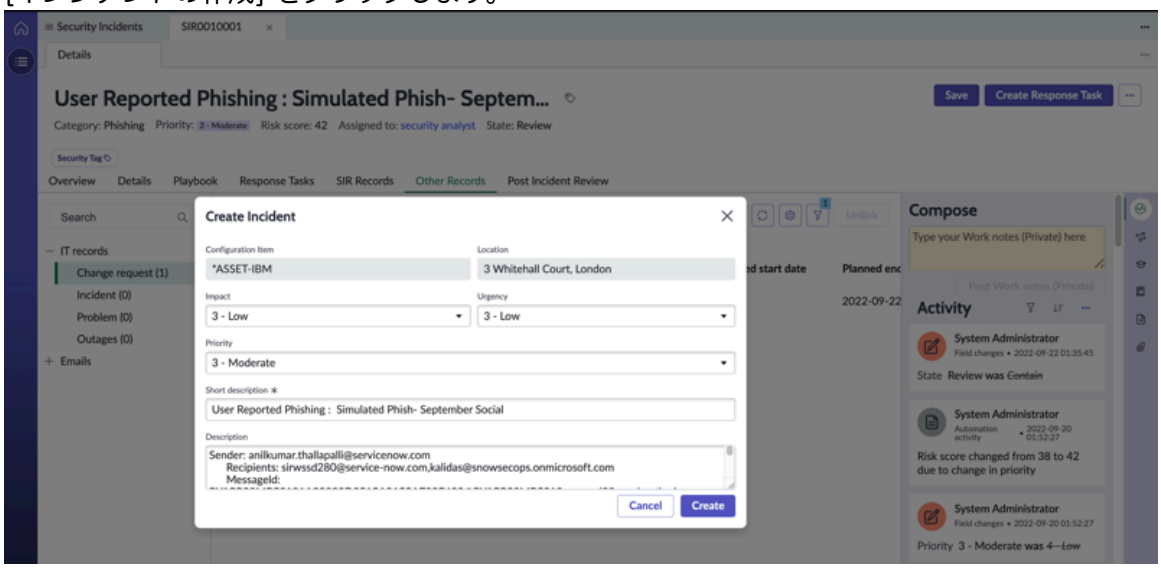
セキュリティインシデント内にインシデントを作成します。

始める前に

必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. インシデントレコードを開きます。
3. [インシデントの作成] をクリックします。

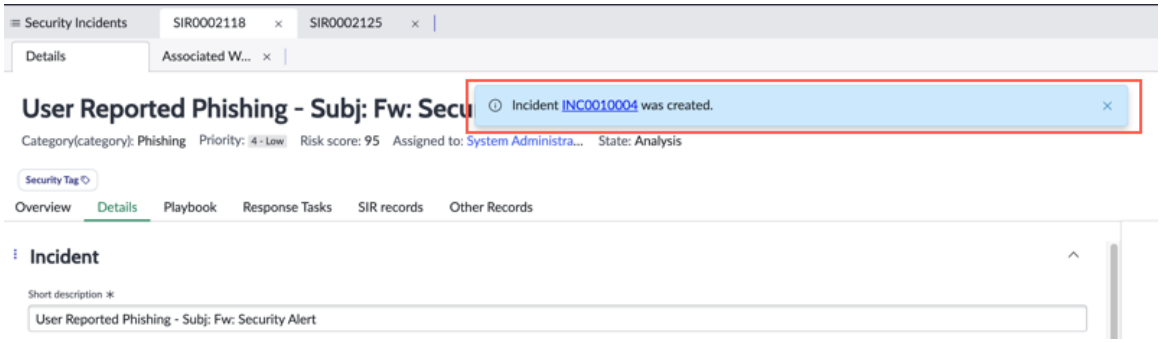


4. [構成アイテム]、[影響度]、[緊急度]、[場所]、[優先度]、[簡単な説明] などの詳細を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. [作成] をクリックしま



す。

6. インシデントが作成されます。

問題タスクの作成

問題タスクを作成します。

始める前に

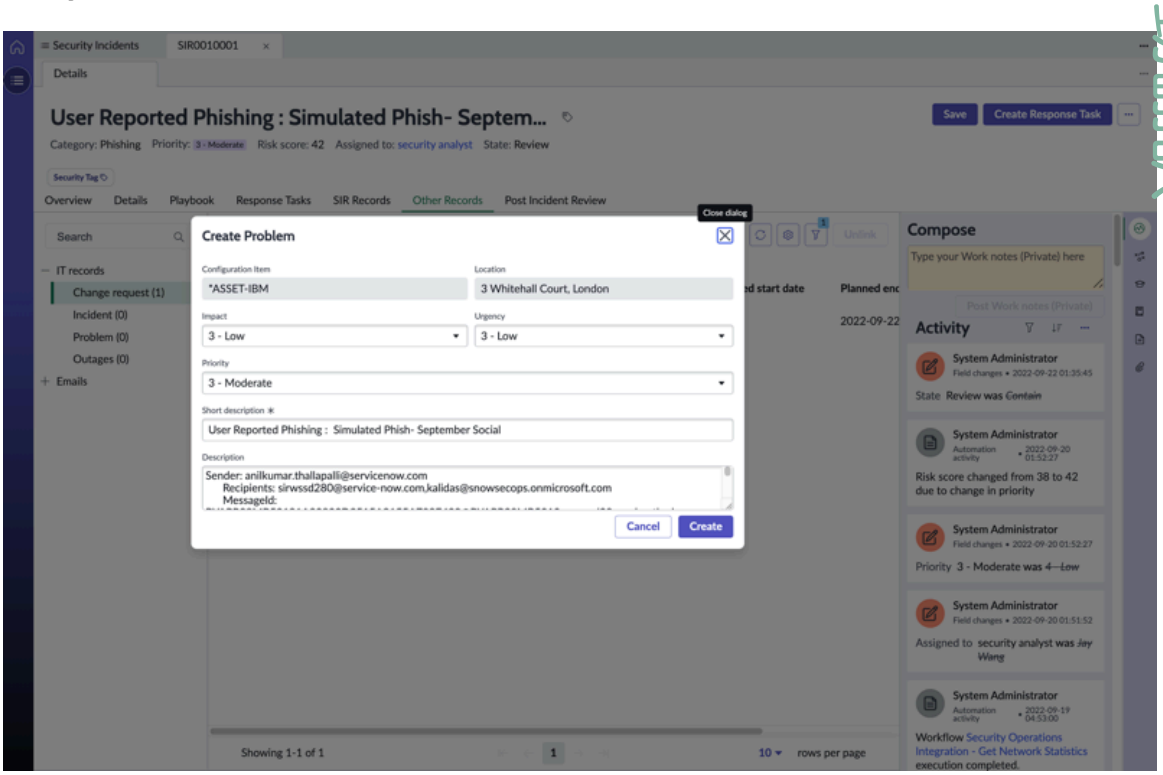
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.

2. インシデントレコードを開きます。

3. [問題を作成] をクリックします。

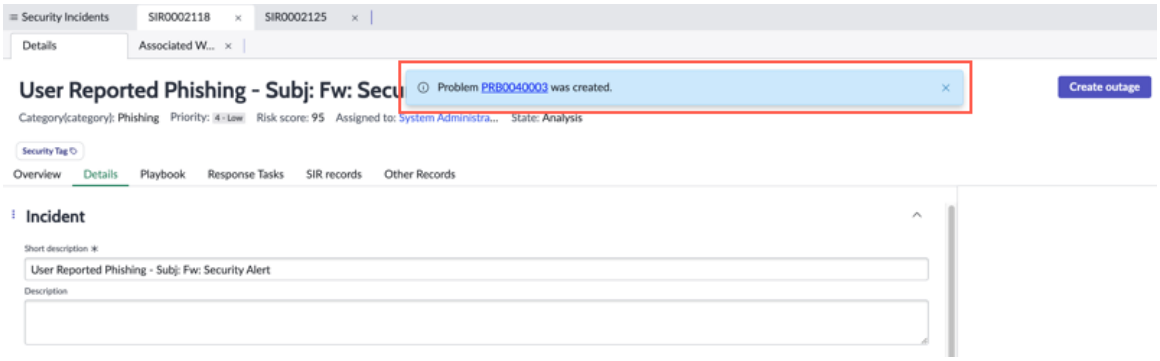


4. [構成アイテム]、[場所]、[影響度]、[緊急度]、[優先度]、[簡単な説明] などの詳細を入力します。

5. [作成] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

問題タスクを作成



6. 問題タスクが作成されます。

変更要求の作成

変更要求を作成します。

始める前に

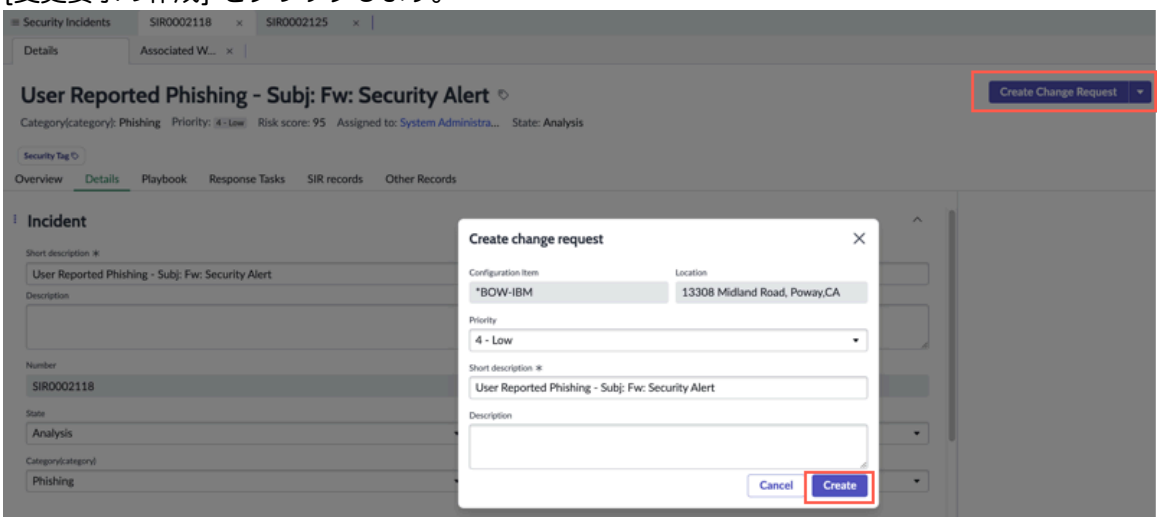
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.

2. インシデントレコードを開きます。

3. [変更要求の作成] をクリックします。

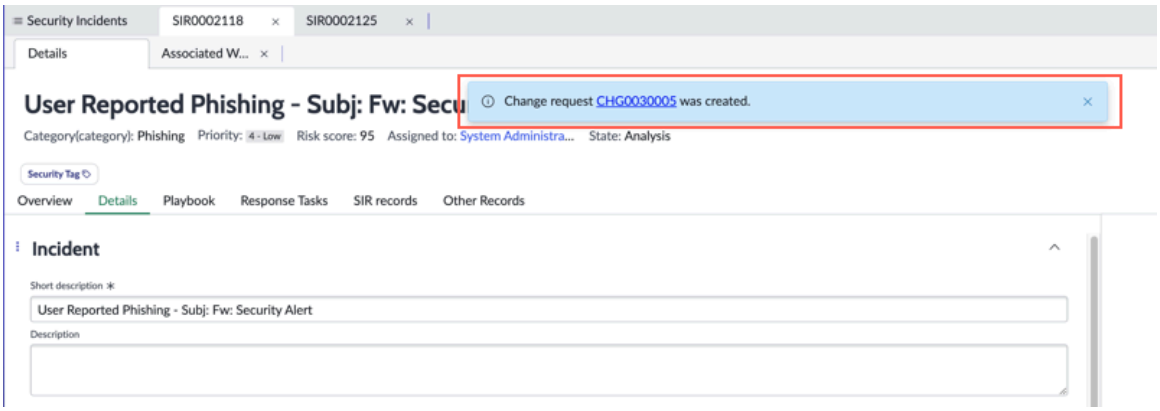


4. [構成アイテム]、[場所]、[優先度]、[簡単な説明] などの詳細を入力します。

5. [作成] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



6. 変更要求が作成されます。

機能停止の作成

インシデントから機能停止を作成して、構成アイテムのダウンタイムを追跡します。

始める前に

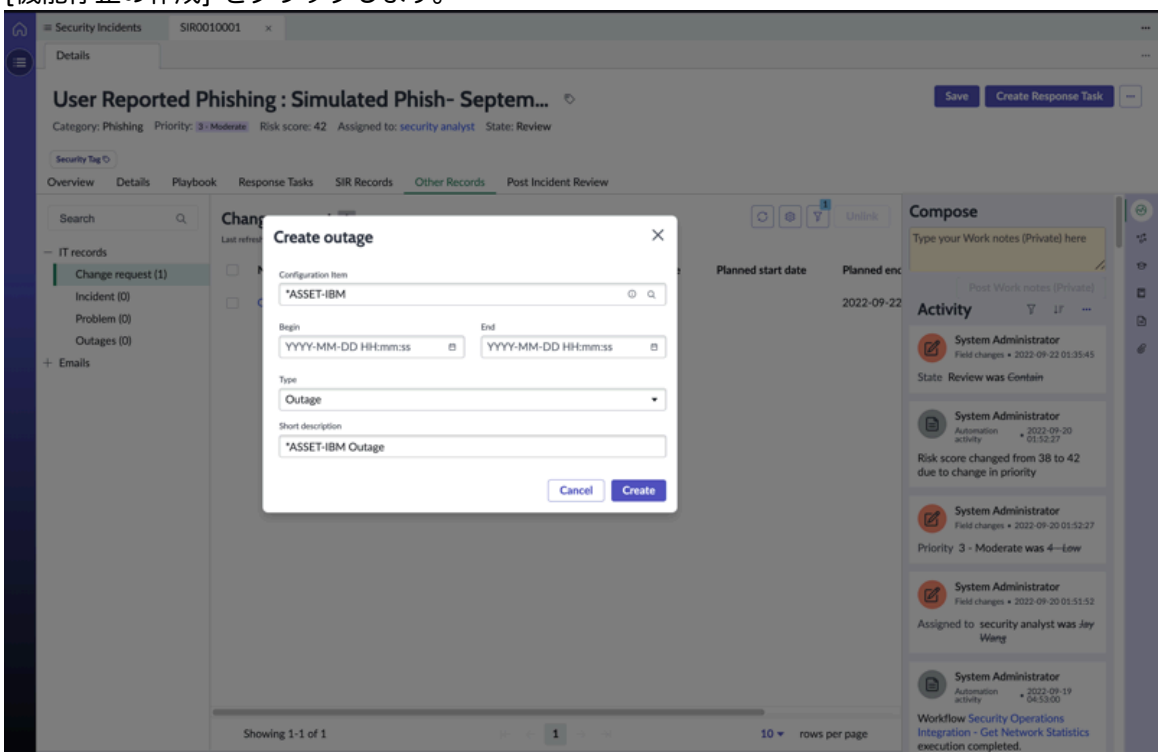
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.

2. インシデントレコードを開きます。

3. [機能停止の作成] をクリックします。

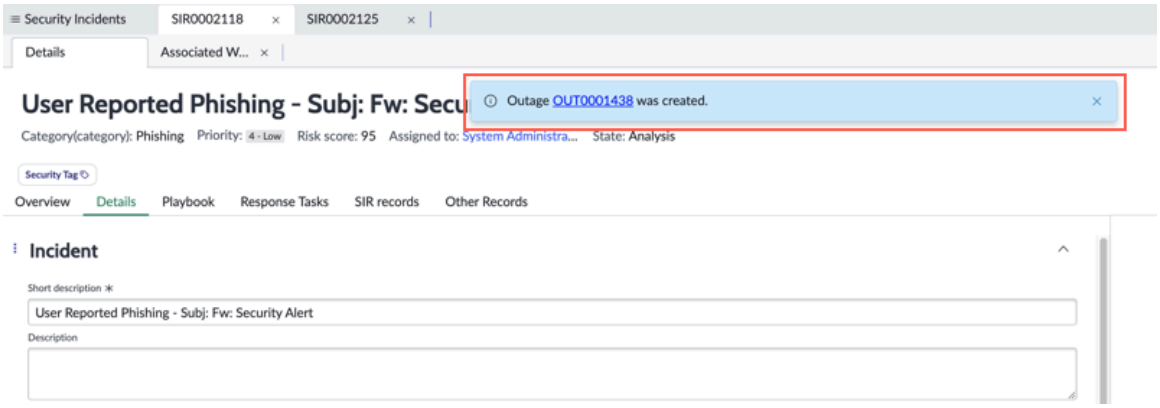


4. [構成アイテム]、[開始日]、[終了日]、[タイプ]、[簡単な説明] などの詳細を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. [作成] をクリックします。



メールの作成

アナリストは、セキュリティインシデントから直接メールを作成できます。

始める前に

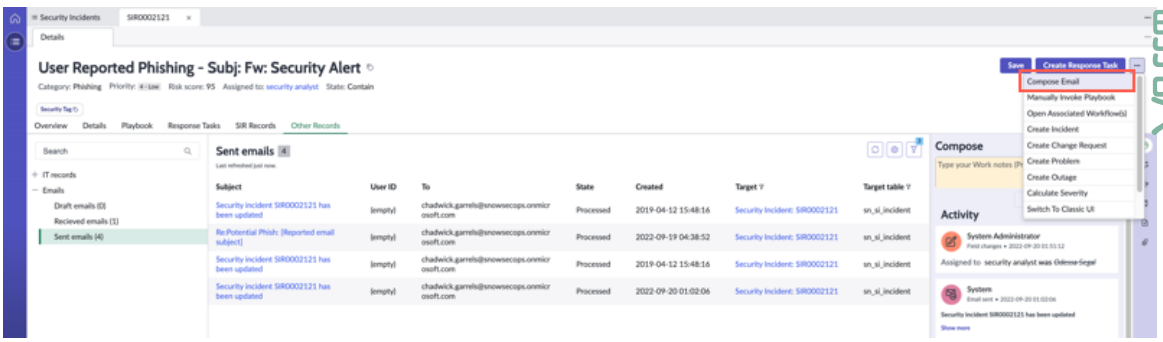
必要なロール：sn_si.analyst

手順

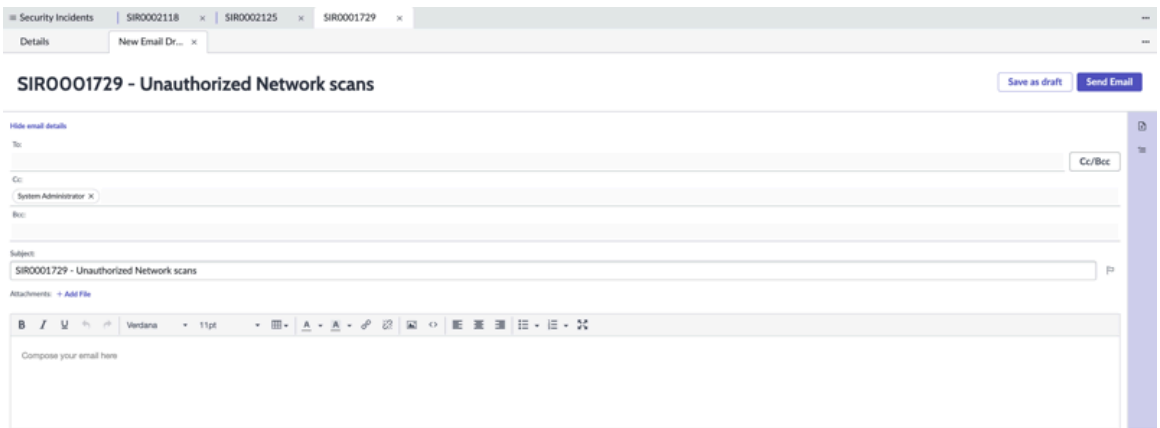
1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.

2. メールを作成するインシデントを選択して開きます。

3. オーバーフローをクリックし、[メールの作成]を選択します。

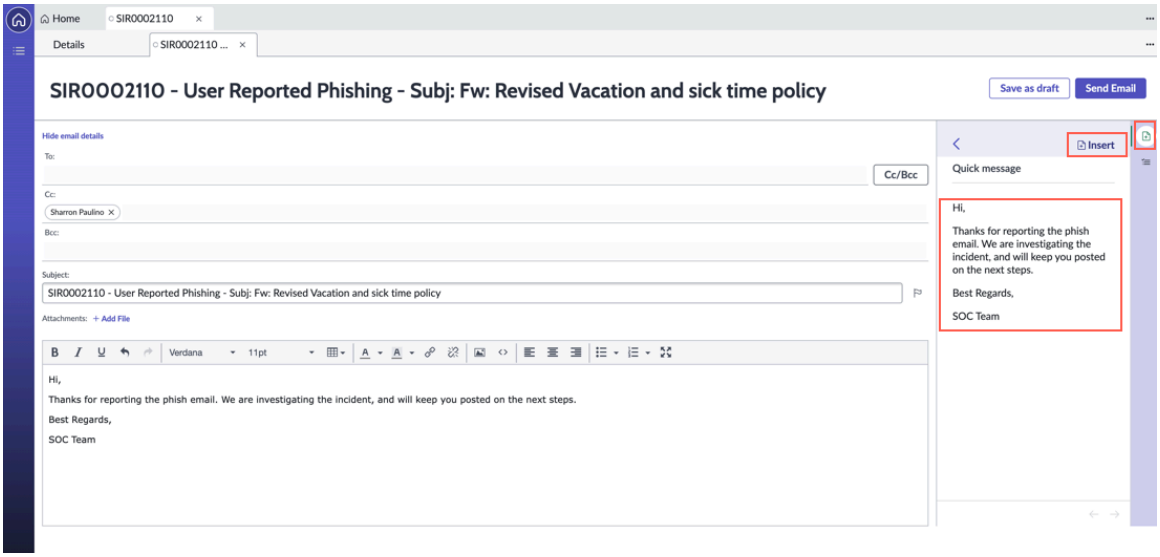


4. [宛先] および **[CC]** フィールドに入力します。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. 必要に応じて添付ファイルを [追加] します。
6. [メール] フォーム内で [クイックメッセージ] をクリックすると、[メールの作成 **(Compose Emails)]** セクションの右側に表示されるクイックメッセージを確認できます。
   利用可能なクイックメッセージが表示されます。メッセージを選択し、[挿入] をクリックします。
   メッセージはメールの本文に挿入されます。



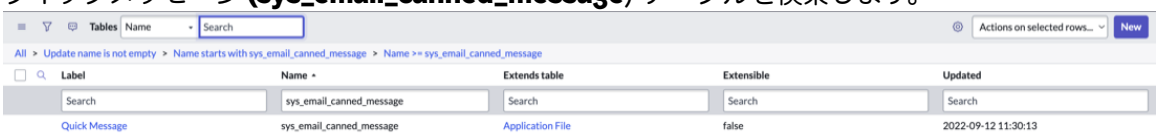
7. メールを作成し、[メールを送信] をクリックします。

> **注:**
> メールをドラフトとして保存できます。これらのドラフトメールは、[その他のレコード] タブで使用できます。

クイックメッセージの設定方法：

a. 次のように移動する。 システム定義 > テーブル.

b. クイックメッセージ **(sys_email_canned_message)** テーブルを検索します。



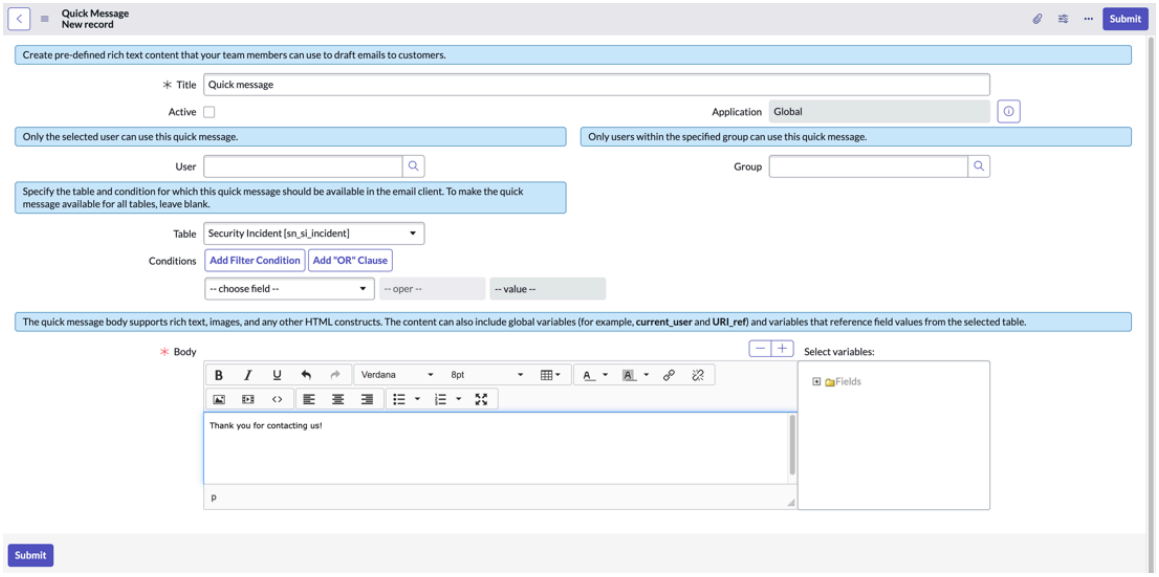
c. 検索項目 関連リンク > リストを表示.

d. [新規] に作成します。

e. [タイトル **(Title)]**、[メッセージの本文] を入力し、[テーブル：セキュリティインシデント **(sn_si_incident) (Table: Security Incident (sn_si_incident))]** および **[Active]** チェックボックスをオンにします。

自動翻訳

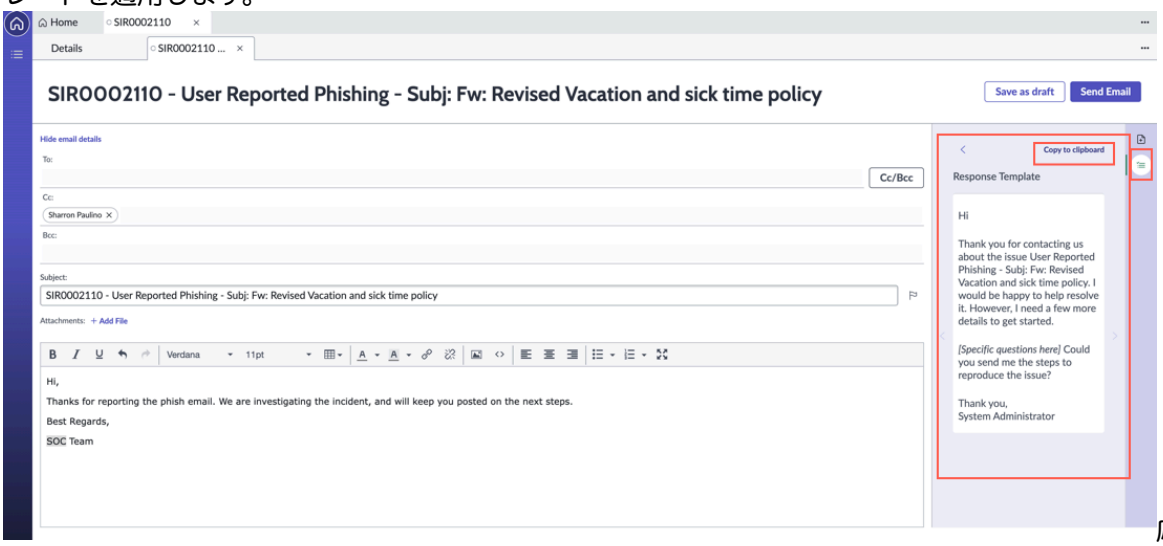
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



f. [送信] をクリックします。
テーブル内に新しいエントリが作成されると、コンテキストメニューにクイックメッセージが表示されます。

8. 必要に応じて [テンプレート] をクリックしてテンプレートを追加します。

9. [応答テンプレート] を選択し、[クリップボードにコピー] をクリックして、必要に応じてテンプレートを適用します。



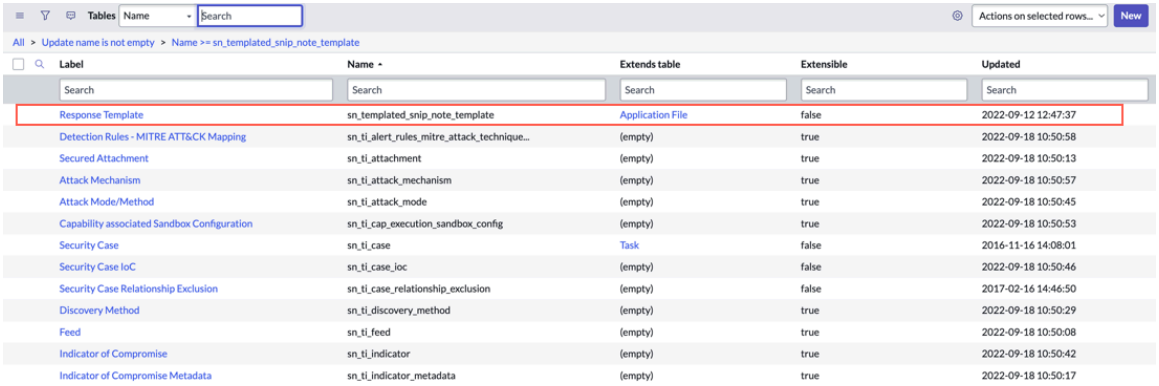
応答テンプレートの設定方法：

a. 次のように移動する。 システム定義 > テーブル.

b. 応答テンプレート **[sn_templated_snip_note_template]** テーブルを検索します。

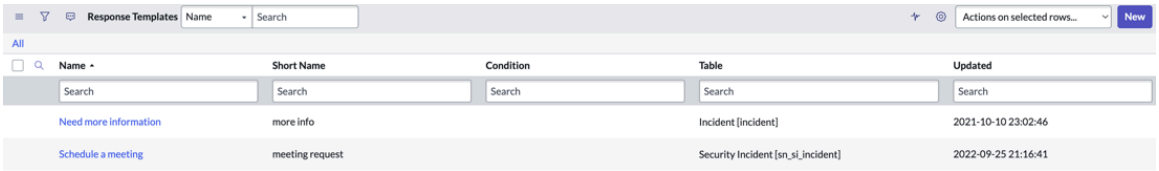
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

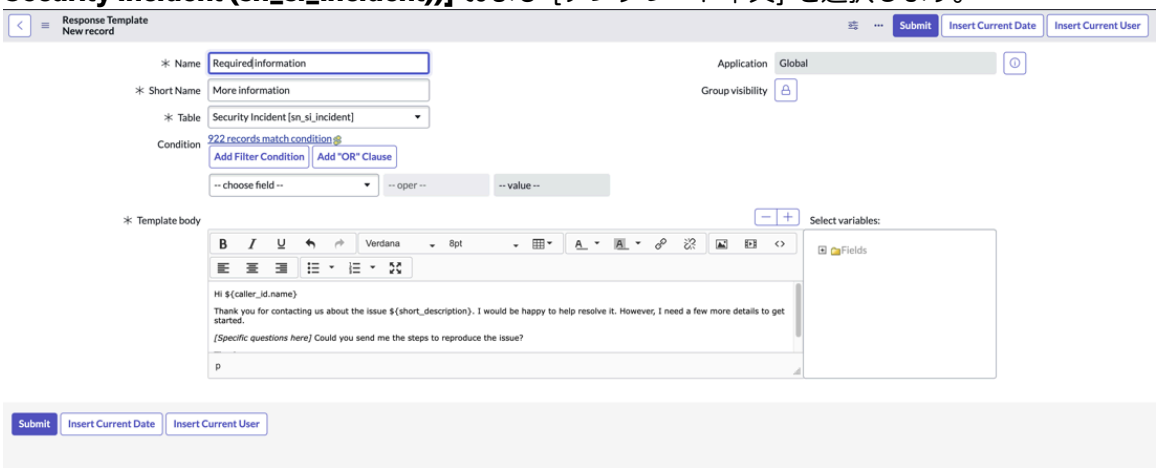


c. 検索項目 関連リンク > リストを表示.

d. [新規] に作成します。



e. [名前]、[短い名前] を入力し、[テーブル：セキュリティインシデント **(sn_si_incident) (Table: Security Incident (sn_si_incident))]** および [テンプレート本文] を選択します。



f. [送信] をクリックします。
テーブル内に新しいエントリが作成されると、コンテキストメニューに新しいテンプレートが表示されます。

セキュリティインシデントレスポンスのインシデント事後レビュー

インシデントの事後レビューは、インシデントが [レビュー] ステータスに移行すると表示されます。

インシデントの事後アクティビティの実行の詳細については、「インシデントの事後レビューレポート」を参照してください。

インシデントの事後レビューは、次のセクションで構成されています。

1. アセスメント
2. レポート

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

セキュリティインシデントレスポンスワークスペースから、これらの新しい 2 つの UI アクションを使用してアセスメントを要求して実施することができます。

名前	説明
アセスメント	[アセスメント] には、セキュリティインシデントのその他のアセスメントに関連付けられているすべてのアセスメントが表示されます。アナリストはアセスメントを実施したり、アセスメントを要求したりすることができます。 • アセスメントを実施：[アセスメントを実施] をクリックしてアセスメントを行い (該当する場合)、アセスメントを完了します。アセスメントを完了する前は、セキュリティインシデントのステータスは [取得可能] で、インシデントの期日は赤で表示されます。 • アセスメントを要求：追加のアセスメントの [アセスメントを要求] をクリックすると、要求する新しいユーザーを追加できます。 注: 既に要求したユーザーはこのセクションに表示されません。 このインシデントのアセスメントは、[インシデントの事後レビュー] で設定された条件に基づいて構成され、必須またはオプションのいずれかとなります。
レポート	ランタイム構成を変更し、レポートを生成します。 [レポートインスタンス] を選択し、フィルターを変更してレポートを保存します。アナリストは、PIR レポートをプレビューしてダウンロードできます。

SIR ワークスペースでの TISC 統合

次のセクションには、SIR ワークスペースコンテキスト内からの脅威インテリジェンスセキュリティセンター統合に関する情報が含まれています。

SIR ワークスペースから TISC へのデータの送信

次のセクションで説明する手順に従って、脅威インテリジェンスセキュリティセンター (TISC) と セキュリティインシデントレスポンス (SIR) のワークスペース間でデータがどのように連携および共有されるかについて学習します。

データ送信のシステムプロパティ

SIRW と組み合わせる TISC 統合のシステムプロパティを確認します。これらのプロパティを構成することで、双方のアプリケーションでの統合管理を制御できるようになります。

主な考慮事項

TISC 統合のシステムプロパティでは、アプリケーションでの観測事象や拡張の処理方法に対して高度な構成オプションが利用できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

1. SIRW 内で TISC 統合のシステムプロパティを設定するには、脅威インテリジェンスの [システムプロパティ] に移動して、[sys_properties] テーブルにアクセスします。
2. システムプロパティでは、個々のデータプッシュの実行動作を制御および処理します。
3. このプロパティが有効な場合、SIR ワークスペースで観測事象や拡張データが生成されると、データが自動的にプッシュされます。
4. このプロパティが無効な場合、データプッシュは手動となり、ユーザーが SIR ワークスペースの UI アクションでデータをプッシュできるようになります。

「TISC - SIR」統合のシステムプロパティは、次のリストのとおりです。

- SIR から観測事象データを自動または手動でプッシュ：「sn_ti.allow_observable_and_enrichment_records_push」プロパティを有効化して、データを自動または手動でプッシュします。このプロパティを無効化すると、SIR からのすべてのデータプッシュに対する自動モードも手動モードも無効になります。
- 脅威のルックアップの結果をプッシュ：「sn_ti.automatic_push_threat_lookup_results」のシステムプロパティを有効化して、脅威のルックアップデータを TISC に自動的にプッシュします。無効化しても、セキュリティアナリストが脅威のルックアップデータを手動でプッシュすることができます。
- サイティング検索結果を TISC にプッシュ：「sn_ti.automatic_push_sighting_results_to_tisc」のシステムプロパティを有効化して、サイティング検索データを TISC に自動的にプッシュします。無効化しても、セキュリティアナリストがサイティング検索データを手動でプッシュすることができます。
- 観測事象をプッシュ：「sn_ti.automatic_push_observable_to_tisc」のシステムプロパティを有効化して、観測事象データを TISC に自動的にプッシュします。無効化しても、セキュリティアナリストが観測事象データを手動でプッシュすることができます。
- エンリッチメント結果をプッシュ：「sn_ti.automatic_push_enichment_results」のシステムプロパティを有効化して、エンリッチメント結果データを TISC に自動的にプッシュします。無効化しても、セキュリティアナリストがエンリッチメント結果データを手動でプッシュすることができます。

自動翻訳

TISC ケースにセキュリティインシデントを追加する

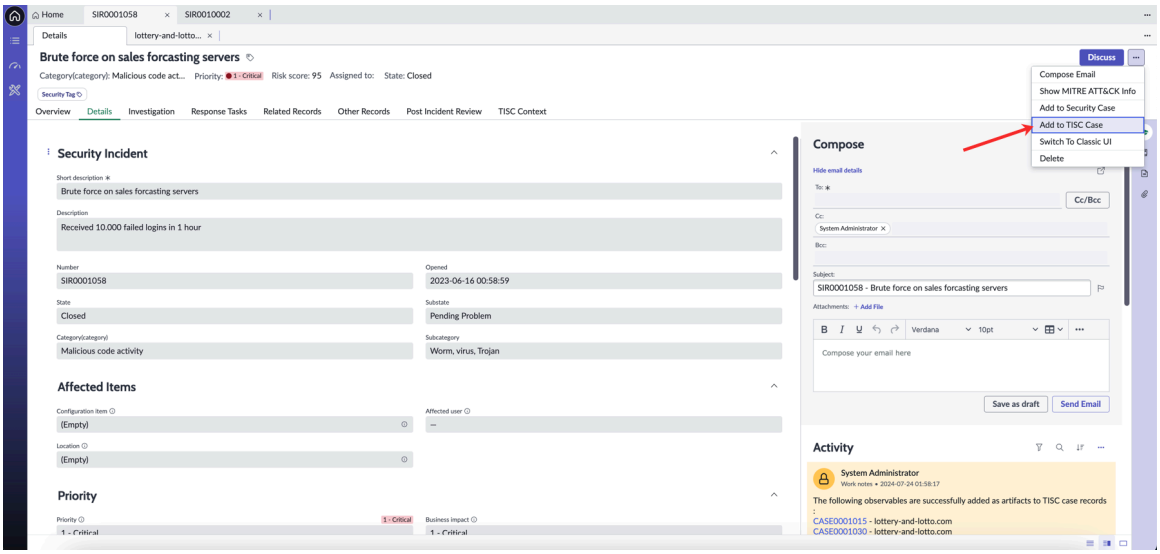
TISC ケースレコードにセキュリティインシデントを追加します。

始める前に
必要なロール：sn_si.analyst、sn_sec_tisc.case_write

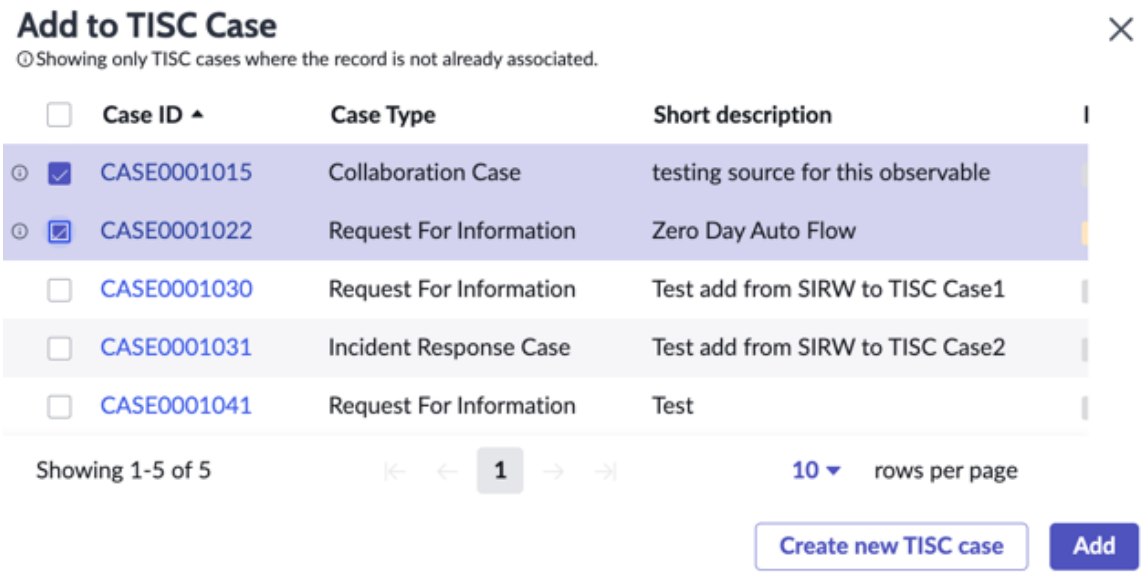
手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > セキュリティインシデント > **All** (すべて).
2. 調査している特定のセキュリティインシデントを見つけて開きます。
   これは、インシデント ID を検索するか、[クイックフィルター] セクションから参照するか、インシデントステータスでフィルタリングすることによっても実行できます。
3. その他のアクションアイコンをクリックします。
4. **[TISC** ケースに追加 **(Add to TISC Case)]** アクションをクリックします。
   [TISC ケースに追加 (Add to TISC Case)] ダイアログボックスが表示され、インシデントがまだ関連付けられていない TISC ケースのみが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



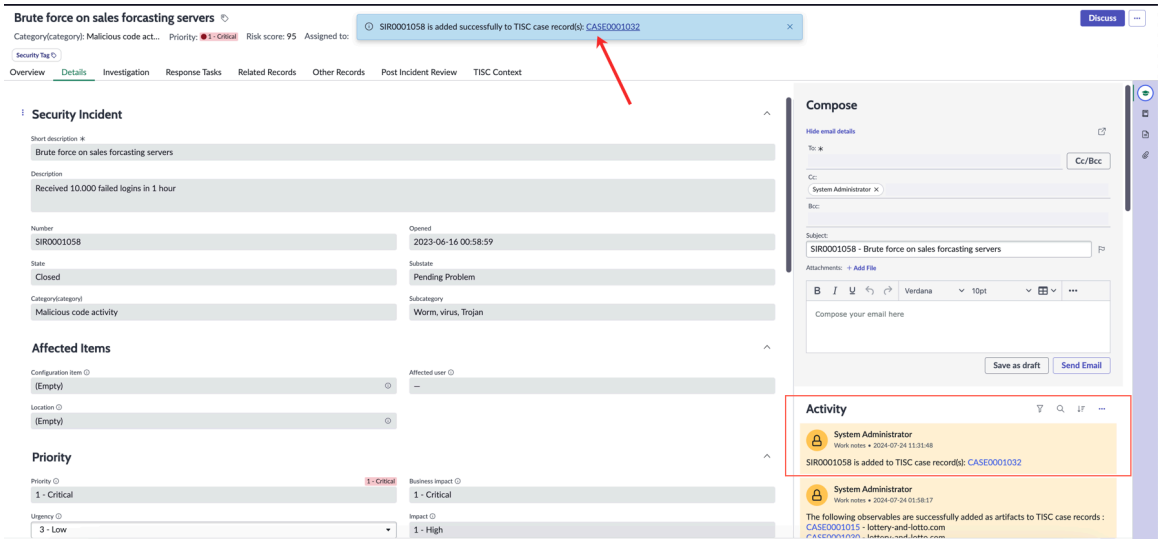
5. [ケースに追加 **(Add to Case)]** ダイアログボックスでケースを選択します。



注:
ケースレコードがない場合は、新しい TISC ケースを作成します。ケースの作成方法の詳細については、「脅威アナリストワークベンチを使用したケースを作成する」を参照してください。

6. [追加] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



7. ケースレコードをクリックすると、表示された情報メッセージまたは [アクティビティ] ストリームから TISC にケースが表示されます。

> **注:**
> リンクされたセキュリティインシデントを表示するには、セキュリティインシデントの [アクティビティ] ストリームから特定のケースレコードをクリックします。これをクリックすると、TISC ワークスペースのケースレコードに移動し、ケース管理モジュールの [アーティファクト **(Artifacts)]** タブにセキュリティインシデントが追加されます。

観測事象を **TISC** ケースに追加

TISC ケースレコードに観測事象を追加します。

始める前に

必要なロール：sn_si.analyst、sn_sec_tisc.case_write

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > セキュリティインシデント > **All** (すべて).
2. 調査している特定のセキュリティインシデントを見つけて開きます。
   これは、インシデント ID を検索するか、[クイックフィルター] セクションから参照するか、インシデントステータスでフィルタリングすることによっても実行できます。
3. [関連レコード] タブをクリックします。
   [セキュリティインシデントレスポンスワークスペース] のさまざまなタブを使用して、TISC ケースに観測事象を追加するアクションを実行できます。

> **注:**
> 以下に移動できます
>
> - [関連レコード] タブの [観測事象] 詳細ページ。
> - [調査] タブから、ページの左側に表示される [エントリーポイントリスト] セクションに移動し、[関連する観測事象] を選択して、TISC ケースに観測事象を追加します。

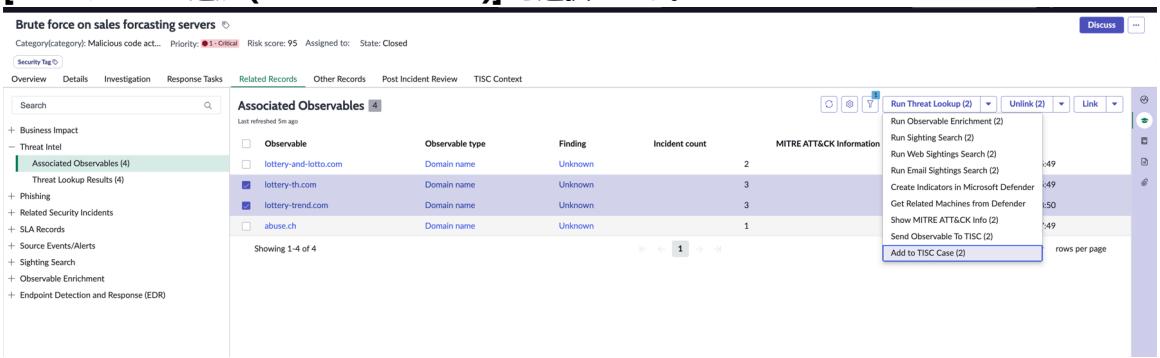
4. たとえば、 **Threat Intel** > 関連する観測項目.
5. 1 つまたは複数の観測事象を選択して、選択した観測事象をケースレコードに追加します。

自動翻訳

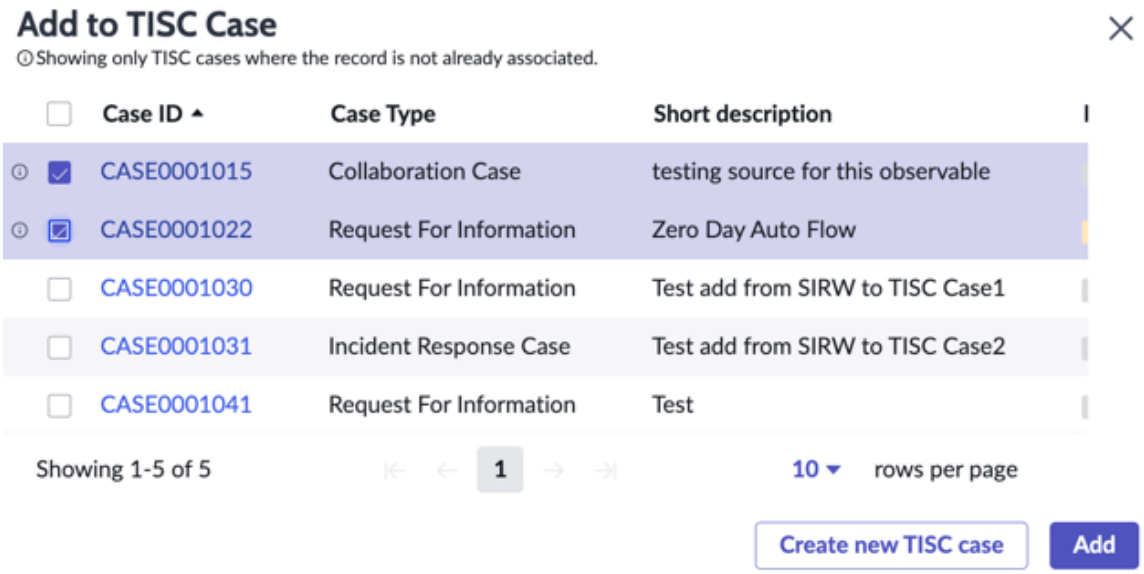
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> いずれかの観測事象レコードをクリックすると、別のタブで観測事象の詳細ページが開き、[TISC ケースに追加 (Add to TISC Case)] をクリックして、ここからケースレコードを追加することもできます。

6. [機能アクション] 分割ボタンをクリックします。
7. **[TISC** ケースに追加 **(Add to TISC Case)]** を選択します。



8. [ケースに追加 **(Add to Case)]** ダイアログボックスでケースを選択します。



> **注:**
> ケースレコードがない場合は、新しい TISC ケースを作成します。ケースの作成方法の詳細については、「脅威アナリストワークベンチを使用したケースを作成する」を参照してください。

9. [追加] をクリックします。
10. ケースレコードをクリックすると、表示された情報メッセージまたは [アクティビティ] ストリームから TISC にケースが表示されます。

> **注:**
> 観測事象に対応する TISC 観測事象がない場合、SIR ワークスペースで選択した観測事象が自動的に TISC に送信され、その後、選択した TISC ケースレコードに追加されます。リンクされた観測事象を表示するには、 [アクティビティ] ストリームから特定のケースレコードをクリックします。これをクリックすると、TISC ワークスペースのケースレコードに移動し、ケース管理モジュールの [アーティファクト] タブに観察事項が追加されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

タスクの結果
観測事象データを脅威インテリジェンスセキュリティセンターケースマネジメントに正常に送信できました。

観測事象を **TISC** に送信

この機能を利用すると、セキュリティアナリストが観測事象データを SIR から TISC にプッシュできるようになります。TISC コンテキストを利用すると、観測事象が TISC に存在するかどうかを確認できます。存在しない場合は、セキュリティアナリストが必要に応じてデータをプッシュできます。

始める前に
必要なロール：sn_si.analyst

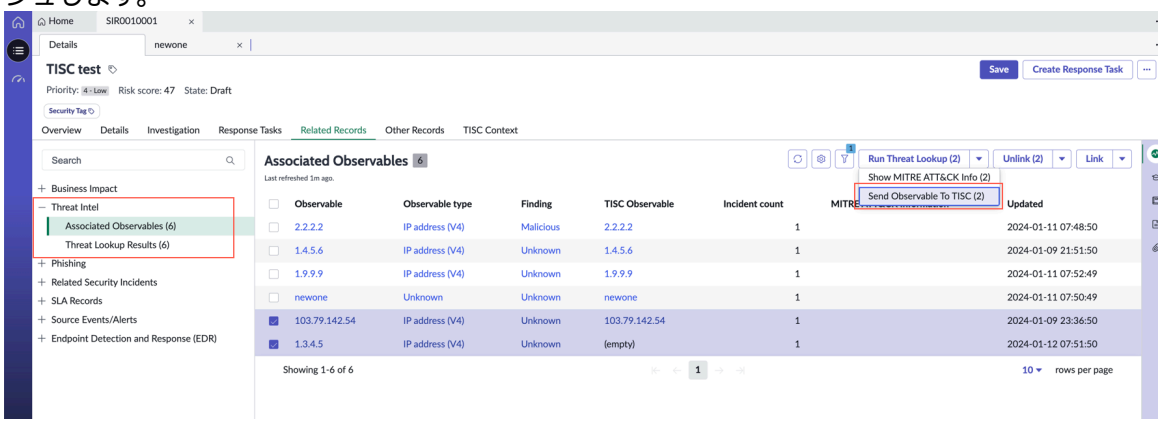
手順

1. SIR ワークスペースの [関連レコード] タブに移動して、TISC 統合機能アクションを実行します。

   注:

   - [調査] タブに移動し、ページの左側に表示される [エントリーポイントリスト] セクションに移動し、[関連する観測事象] を選択してプッシュ操作を実行することもできます。
   - [調査] タブで [関連情報を表示] をクリックして、選択した観測事象に関連する脅威のルックアップ、サイティング検索、拡張データをすべて表示します。詳細については、「調査キャンバスの詳細」を参照してください。

2. たとえば、 **Threat Intel** > 関連する観測項目 でプッシュ操作を実行し、手動でデータを TISC にプッシュします。
3. 観測事象レコードを 1 つ以上選択し、「観測事象を **TISC** に送信」の操作を実行してデータをプッシュします。



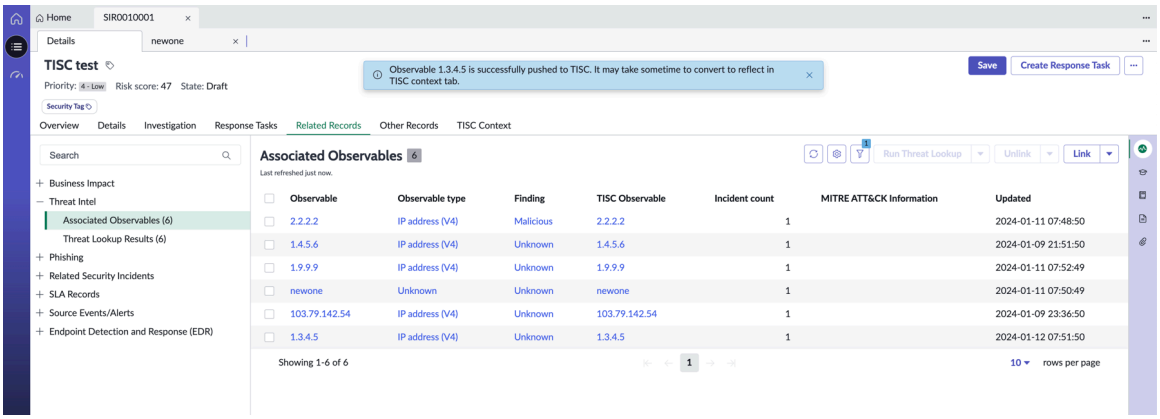
4. [観測事象を **TISC** に送信] をクリックします。

   注:

   - 選択した観測事象が TISC に存在しない場合、最初に観測事象が観測事象ソースとして作成されます。その後、ソース観測事象により TISC 観測事象レコードが作成されると、観測事象レコードが、新たに作成された観測事象に自動的に関連付けられます。
   - 観測事象のプッシュ操作が実行されると、「観測事象 0.0.0.0 が TISC に正常にプッシュされました。TISC コンテキストタブに反映されるように変換されるまでに時間がかかる場合があります。」という情報メッセージが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



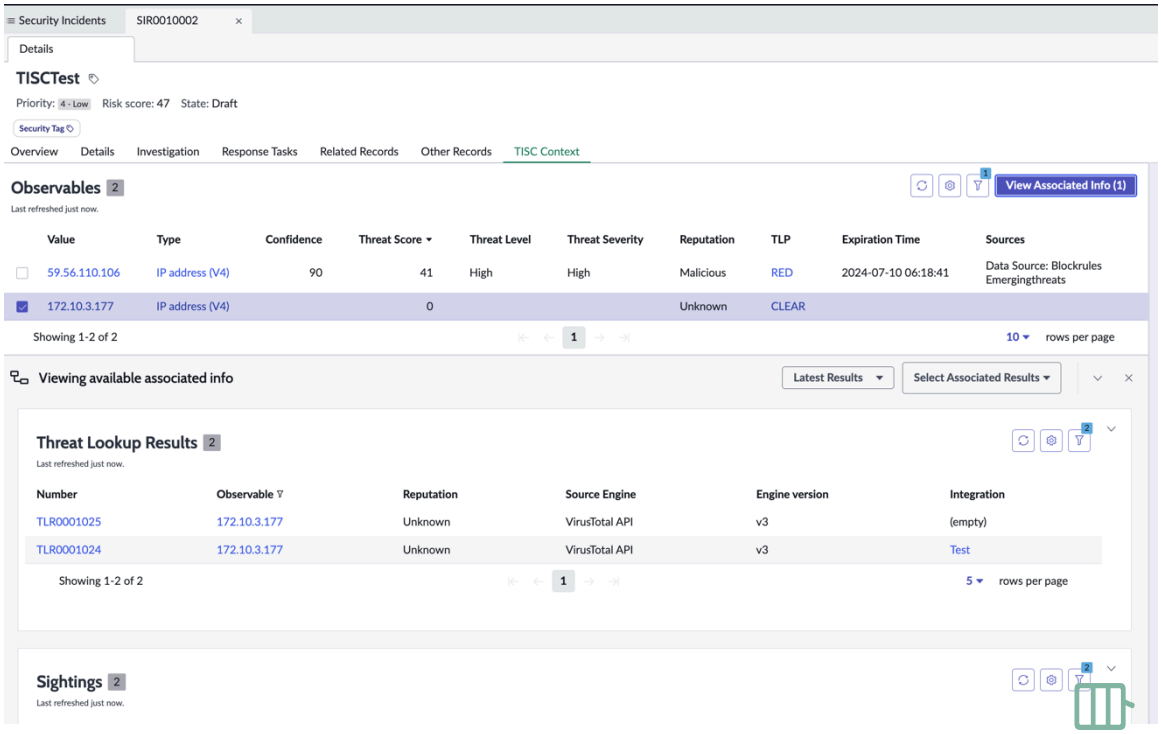
5. [TISC コンテキスト] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
:

- SIR アプリケーションから TISC にプッシュされた観測事象が表示されます。



- 手動でのプッシュ操作の場合：観測事象データは、セキュリティインシデントにリンクされている場合にのみプッシュできます。観測事象が SIR からプッシュされた場合、ソースは観測事象にリンクされているセキュリティインシデントのリファレンスを有することになり、これによりデータを識別できるようになります。
- 自動でのプッシュ操作の場合：観測事象や拡張データは、セキュリティインシデントに関連付けられたときに自動的にプッシュされます。
- **TISC** コンテキスト には、SIR に関連する観測事象がすべて表示されます。これらは、TISC にも存在するものとなります。
- TISC コンテキストを使用すると、SIR アナリストが、脅威のルックアップ、サイティング検索、観測事象のエンリッチメント結果など、すべての TISC 拡張データを確認できるようになります。
- [関連情報を表示] には、選択した観測事象における関連の観測事象拡張データがすべて表示されます。

6. 結果を表示します。

脅威のルックアップを **TISC** に送信

セキュリティアナリストは、この機能を使用して、脅威のルックアップデータを SIR から TISC にプッシュできます。TISC コンテキストを使用すると、脅威のルックアップの結果が TISC に存在するかどうかを確認できます。存在しない場合は、セキュリティアナリストは必要なときにいつでもデータをプッシュできます。

始める前に
必要なロール：sn_si.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

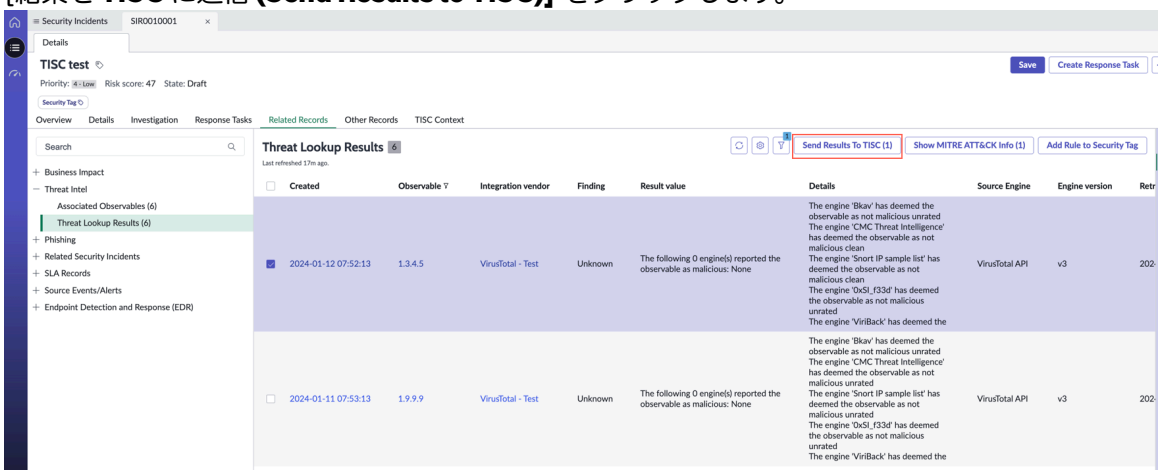
手順

1. SIR ワークスペースの [関連レコード] タブに移動して、TISC 統合機能アクションを実行します。

   注:

   - [調査] タブに移動し、ページの左側に表示される [エントリーポイントリスト] セクションに移動し、[関連する観測事象] を選択してプッシュ操作を実行することもできます。
   - [調査] タブで [関連情報を表示] をクリックして、選択した観測事象に関連するすべての脅威のルックアップ、サイティング検索、および拡張データを表示します。詳細については、「調査キャンバスの詳細」を参照してください。

2. 選択 **Threat Intel** > 脅威情報ルックアップの結果 でプッシュ操作を実行し、手動でデータを TISC にプッシュします。
3. 1 つ以上の [脅威のルックアップの結果] レコードを選択します。
4. [結果を **TISC** に送信 **(Send Results to TISC)]** をクリックします。



   注:

   - 選択した脅威のルックアップの観測事象が TISC に存在しない場合、手動モードでは、最初に観測事象が観測事象ソースとして作成されます。その後、ソース観測事象が TISC 観測事象レコードを作成すると、観測事象レコードが新しく作成された観測事象に自動的に関連付けられます。また、選択した脅威のルックアップも、手動モードで新しく作成された脅威のルックアップの観測事象にプッシュされます。
   - 自動モードでは、観測事象が存在する場合、観測事象はプッシュされず、脅威のルックアップが自動的にプッシュされます。観測事象が存在しない場合、脅威のルックアップはプッシュされません。

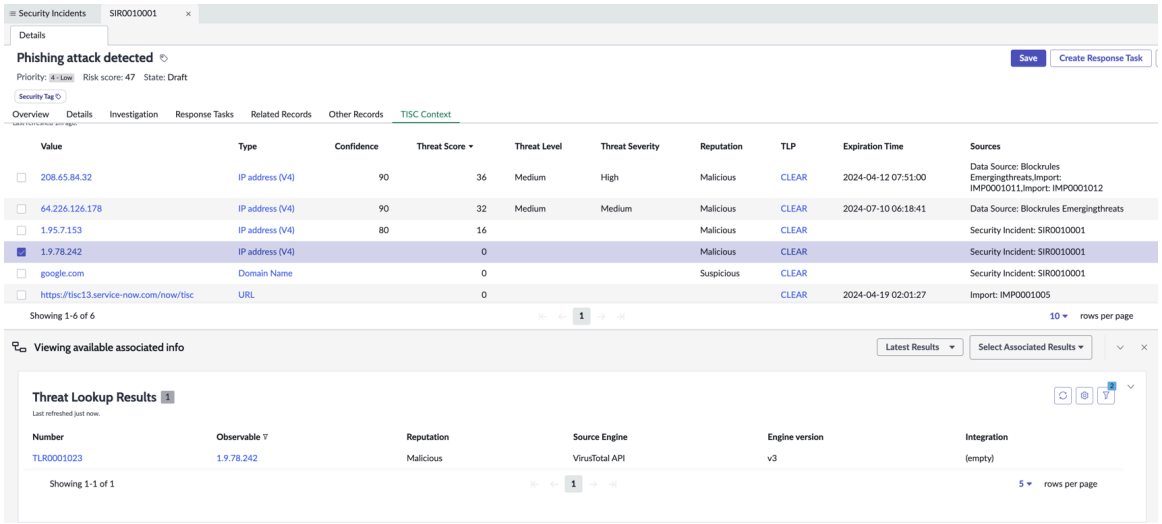
5. [選択した脅威のルックアップレコードの観測事象 (1.9.78.242) が TISC に存在しません。観測事象が作成され、TISC で観測事象の脅威のルックアップレコードが自動的に関連付けられるまでには、しばらく時間がかかります。(The observable (1.9.78.242) for the selected threat lookup record does not exist in TISC. It will take sometime to create observable and to automatically associate the observable threat lookup record in TISC.)] という確認メッセージが表示されます。これが処理されてプッシュされると、結果を確認できます。
6. **[TISC** コンテキスト] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
:

- SIR アプリケーションから TISC にプッシュされた観測事象が表示されます。



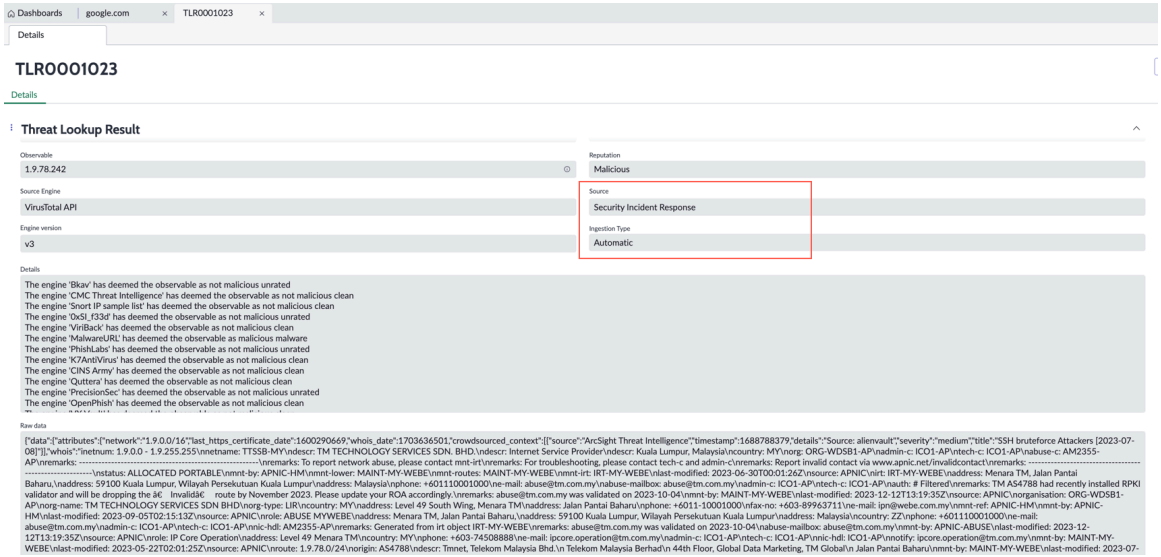
- 手動でのプッシュ操作の場合：観測事象データは、セキュリティインシデントにリンクされている場合にのみプッシュできます。観測事象が SIR からプッシュされた場合、ソースは観測事象にリンクされているセキュリティインシデントのリファレンスを有することになり、これによりデータを識別できるようになります。
- 自動でのプッシュ操作の場合：観測事象や拡張データは、セキュリティインシデントに関連付けられたときに自動的にプッシュされます。
- **TISC** コンテキストには、SIR に関連する観測事象がすべて表示されます。これらは、TISC にも存在するものとなります。
- TISC コンテキストを使用すると、SIR アナリストが、脅威のルックアップ、サイティング検索、観測事象のエンリッチメント結果など、すべての TISC 拡張データを確認できるようになります。
- [関連情報を表示] には、選択した観測事象における関連の観測事象拡張データがすべて表示されます。

7. リストビューにはすべての脅威のルックアップの結果が表示されますが、任意のレコードを選択して [関連情報を表示] ボタンをクリックします。
8. 脅威のルックアップの結果を表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

9. 任意の脅威のルックアップの結果レコードをクリックして、フォームビューにレコードを表示します。このビューには、プッシュまたは [取り込みタイプ] ([自動] または [手動]) も表示され、[ソース] はセキュリティインシデントレスポンスになります。



サイティング検索を **TISC** に送信

セキュリティアナリストはこの機能を使用して、サイティング検索データを SIR から TISC にプッシュできます。アナリストは、TISC コンテキストを使用して、サイティング検索データが TISC に存在するかどうかを確認できます。存在しない場合は、必要に応じてデータをプッシュできます。

始める前に
必要なロール：sn_si.analyst

手順

1. SIR ワークスペースの [関連レコード] タブに移動して、TISC 統合機能アクションを実行します。

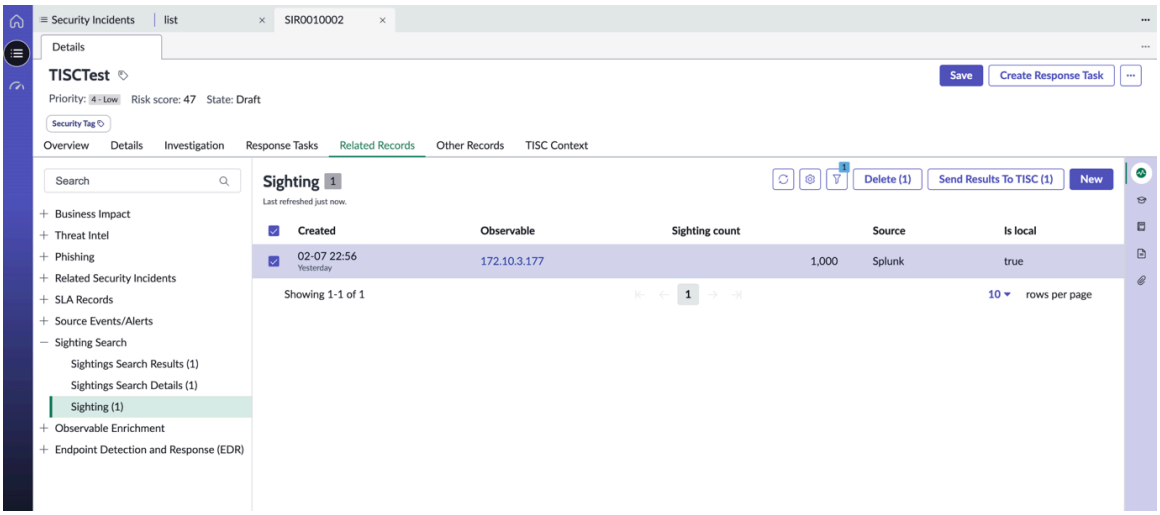
   注:

   - [調査] タブに移動し、ページの左側に表示される [エントリーポイントリスト] セクションに移動し、[関連する観測事象] を選択してプッシュ操作を実行することもできます。
   - [調査] タブで [関連情報を表示] をクリックして、選択した観測事象に関連するすべての脅威のルックアップ、サイティング検索、および拡張データを表示します。詳細については、「調査キャンバスの詳細」を参照してください。

2. 選択 サイティング検索 > サイティング検索結果 でプッシュ操作を実行し、手動でデータを TISC にプッシュします。
3. 1 つ以上のサイティング検索結果レコードを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

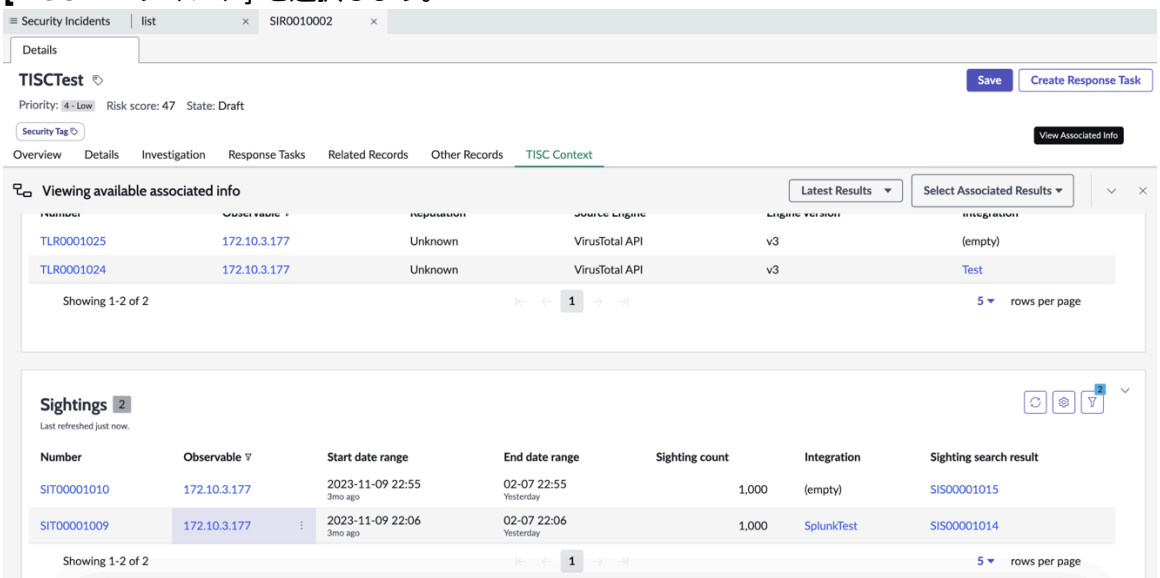


4. [結果を **TISC** に送信 **(Send Results to TISC)]** をクリックします。

注:

- 選択したサイティング検索の観測事象が TISC に存在しない場合、手動モードでは、最初に観測事象が観測事象ソースとして作成されます。その後、ソース観測事象が TISC 観測事象レコードを作成すると、観測事象レコードが新しく作成された観測事象に自動的に関連付けられます。また、選択したサイティング検索も、手動モードで新しく作成された脅威のルックアップの観測事象にプッシュされます。
- 自動モードでは、観測事象が存在する場合、観測事象はプッシュされず、脅威のルックアップが自動的にプッシュされます。観測事象が存在しない場合、脅威のルックアップはプッシュされません。

5. **[TISC** コンテキスト] を選択します。



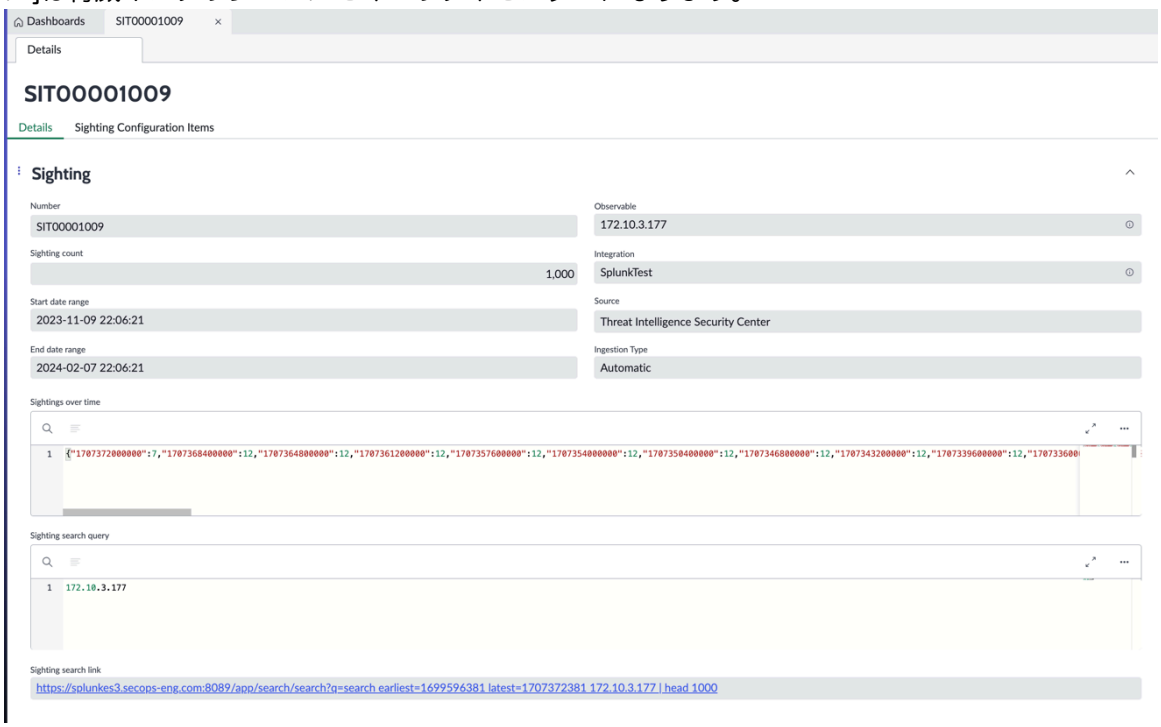
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
:

- SIR アプリケーションから TISC にプッシュされた観測事象が表示されます。
- 手動でのプッシュ操作の場合：観測事象データは、セキュリティインシデントにリンクされている場合にのみプッシュできます。観測事象が SIR からプッシュされた場合、ソースは観測事象にリンクされているセキュリティインシデントのリファレンスを有することになり、これによりデータを識別できるようになります。
- 自動でのプッシュ操作の場合：観測事象や拡張データは、セキュリティインシデントに関連付けられたときに自動的にプッシュされます。
- **TISC** コンテキスト には、SIR に関連する観測事象がすべて表示されます。これらは、TISC にも存在するものとなります。
- TISC コンテキストを使用すると、SIR アナリストが、脅威のルックアップ、サイティング検索、観測事象のエンリッチメント結果など、すべての TISC 拡張データを確認できるようになります。
- [関連情報を表示] には、選択した観測事象における関連の観測事象拡張データがすべて表示されます。

6. レコードが処理されたら、レコードを選択して [関連情報を表示] をクリックします。
7. 結果を表示します。
8. 任意のサイティング検索結果レコードをクリックして、フォームビューにレコードを表示します。このビューには、プッシュまたは [取り込みタイプ] ([自動] または [手動]) も表示され、[ソース]は脅威インテリジェンスセキュリティセンターになります。



観測事象の拡張を **TISC** に送信

セキュリティアナリストはこの機能を使用して、サイティング検索データを SIR から TISC にプッシュできます。アナリストは、TISC コンテキストを使用して、サイティング検索データが TISC に存在するかどうかを確認できます。存在しない場合は、必要に応じてデータをプッシュできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：sn_si.analyst

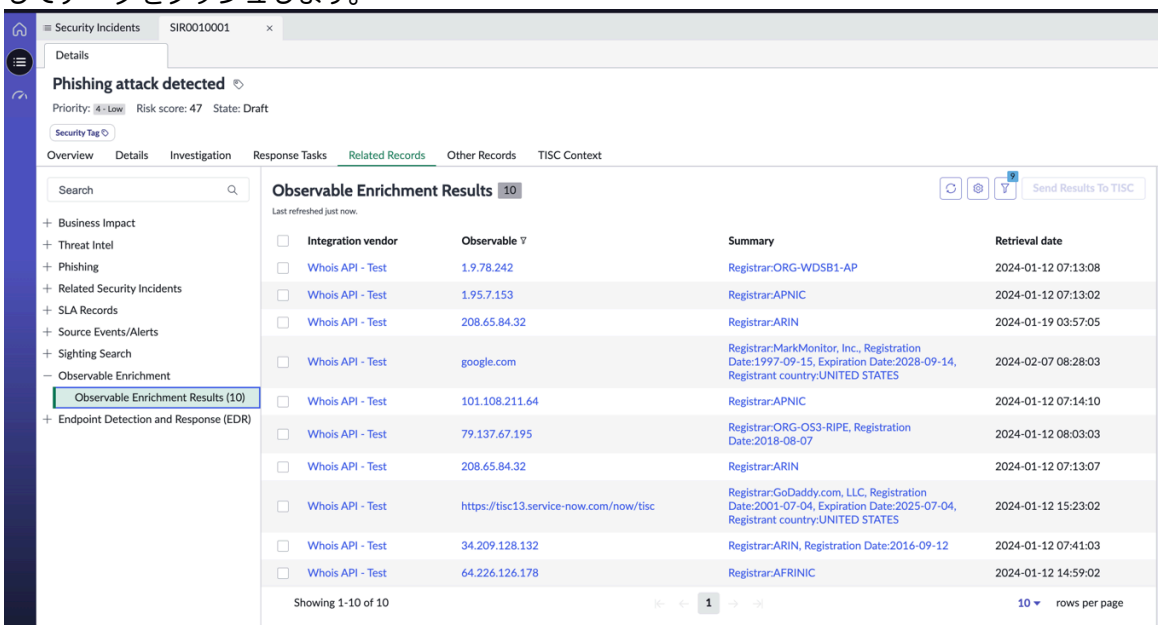
手順

1. SIR ワークスペースの [関連レコード] タブに移動して、TISC 統合機能アクションを実行します。

   注:

   - [調査] タブに移動し、ページの左側に表示される [エントリーポイントリスト] セクションに移動し、[関連する観測事象] を選択してプッシュ操作を実行することもできます。
   - [調査] タブで [関連情報を表示] をクリックして、選択した観測事象に関連するすべての脅威のルックアップ、サイティング検索、および拡張データを表示します。詳細については、「調査キャンバスの詳細」を参照してください。

2. 選択 観察事項の拡張 > 観測事象のエンリッチメント結果 でプッシュ操作を実行し、手動でデータを TISC にプッシュします。
3. 1 つ以上の観測事象レコードを選択し、[結果を **TISC** に送信 **(Send Results to TISC)]** 操作を実行してデータをプッシュします。



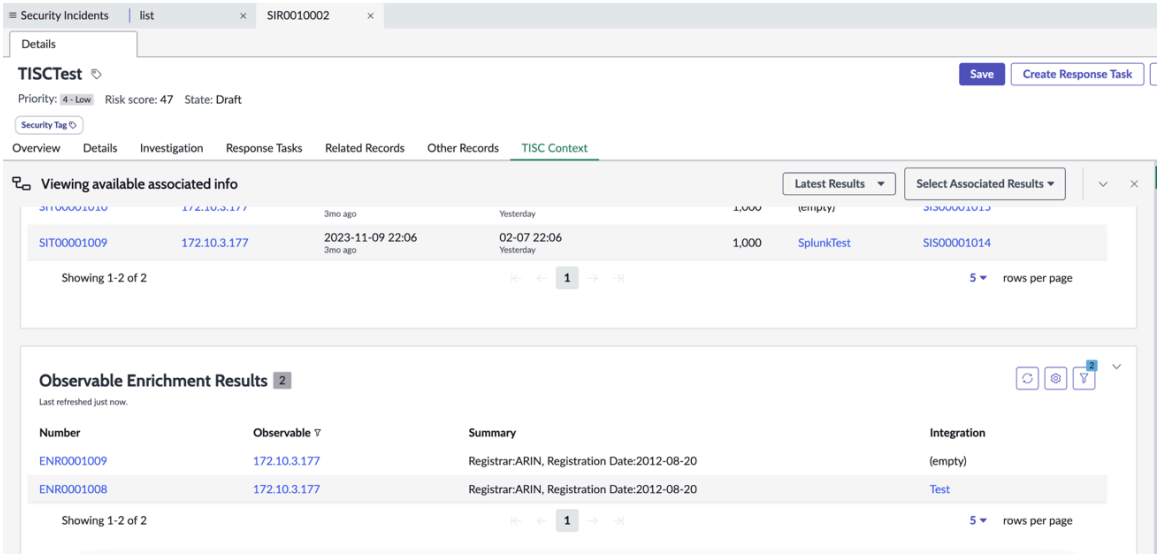
4. [結果を **TISC** に送信 **(Send Results to TISC)]** をクリックします。

   注:

   - 選択した観測事象が TISC に存在しない場合、最初に観測事象が観測事象ソースとして作成されます。その後、ソース観測事象により TISC 観測事象レコードが作成されると、観測事象レコードが、新たに作成された観測事象に自動的に関連付けられます。
   - 観測事象のプッシュ操作が実行されると、「観測事象 0.0.0.0 が TISC に正常にプッシュされました。TISC コンテキストタブに反映されるように変換されるまでに時間がかかる場合があります。」という情報メッセージが表示されます。

5. **[TISC** コンテキスト] を選択します。

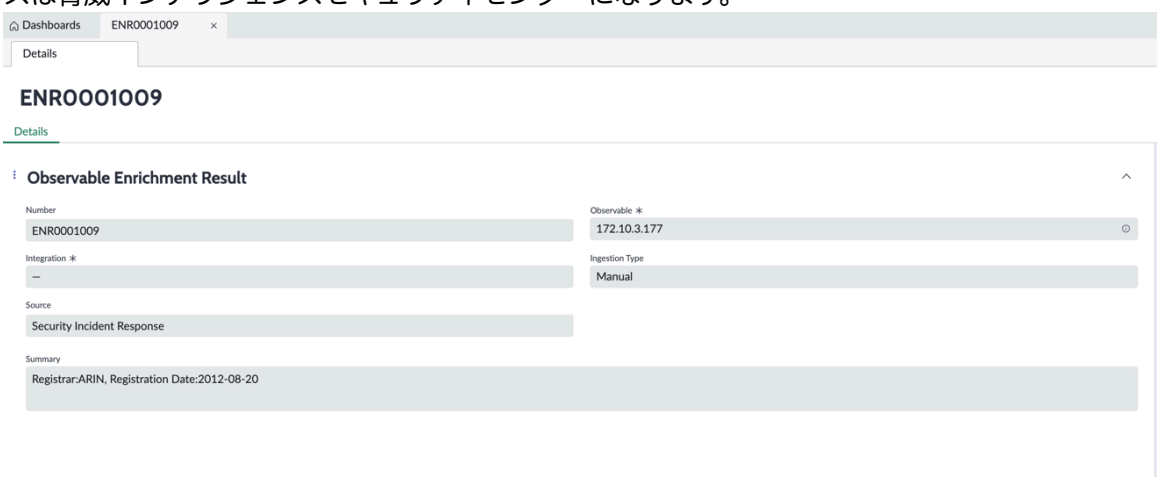
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
:

- SIR アプリケーションから TISC にプッシュされた観測事象が表示されます。
- 手動でのプッシュ操作の場合：観測事象データは、セキュリティインシデントにリンクされている場合にのみプッシュできます。観測事象が SIR からプッシュされた場合、ソースは観測事象にリンクされているセキュリティインシデントのリファレンスを有することになり、これによりデータを識別できるようになります。
- 自動でのプッシュ操作の場合：観測事象や拡張データは、セキュリティインシデントに関連付けられたときに自動的にプッシュされます。
- **TISC** コンテキスト には、SIR に関連する観測事象がすべて表示されます。これらは、TISC にも存在するものとなります。
- TISC コンテキストを使用すると、SIR アナリストが、脅威のルックアップ、サイティング検索、観測事象のエンリッチメント結果など、すべての TISC 拡張データを確認できるようになります。
- [関連情報を表示] には、選択した観測事象における関連の観測事象拡張データがすべて表示されます。

6. 結果を表示します。
7. 任意の観測事象のエンリッチメント結果レコードをクリックして、フォームビューにレコードを表示します。このビューには、プッシュまたは取り込みタイプ (自動または手動) も表示され、ソースは脅威インテリジェンスセキュリティセンターになります。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

TISC コンテキストの使用

TISC コンテキストを使用すると、セキュリティインシデントレスポンスワークスペースで観測事象などの脅威インテリジェンスデータの確認がスムーズになります。

これにより、セキュリティアナリストは、ワークスペースでセキュリティインシデントをより効果的に検出、調査、対応できるようになります。

セキュリティインシデントレスポンスワークスペースで TISC コンテキストを使用すると、セキュリティアナリストは、セキュリティインシデントや観測事象をワークスペースから直接 TISC ケースに追加できるだけでなく、拡張結果を表示したり、関連する攻撃者、攻撃パターン、キャンペーンなどの観測事象の関連情報を表示したりすることもできるようになります。

このセクションを使用すると、次のことができます。

1. 観測事象を TISC ケースに関連付ける。
2. 関連する観測事象情報を表示する。
3. 観測事象のエンリッチメント結果を表示する。

詳細や手順については、次のセクションを参照してください。TISC ワークスペースと SIR ワークスペース間の統合の仕組みに関するの詳細は、脅威インテリジェンスセキュリティセンター の「SIR ワークスペースとの TISC 統合」を参照してください。

観測事象を TISC ケースに追加

このセクションを使用して、セキュリティインシデントや観測事象を TISC ケースに追加します。

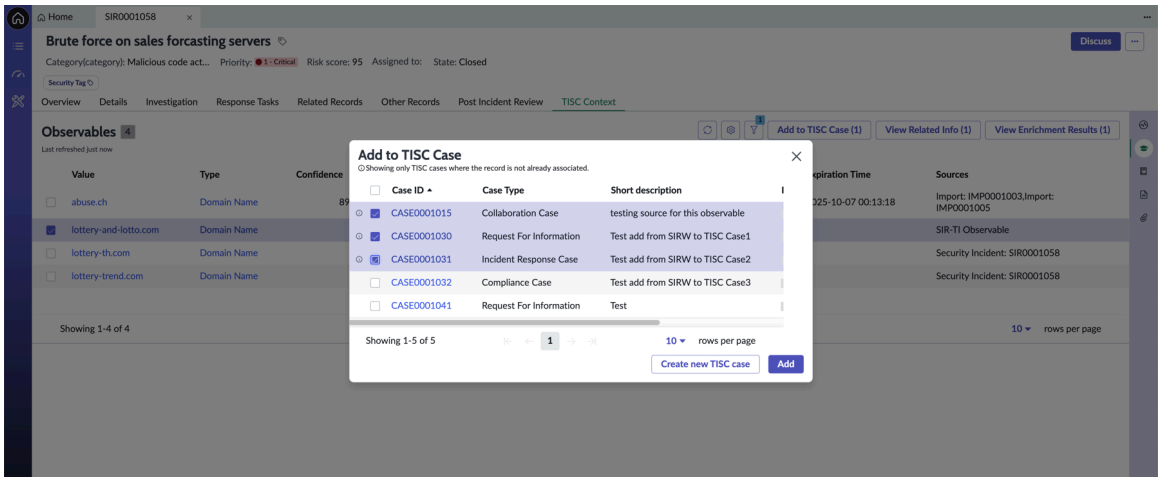
始める前に
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > セキュリティインシデント > **All** (すべて).
2. 調査している特定のセキュリティインシデントを見つけて開きます。
   これは、インシデント ID を検索するか、[クイックフィルター] セクションでフィルタリングする、またはインシデントステータスで参照することでも実行できます。
3. **[TISC** コンテキスト] タブを選択します。
4. **[TISC** ケースに追加] ボタンをクリックします。
   [TISC ケースに追加] ダイアログボックスが表示され、レコードがまだ関連付けられていない TISC ケースのみが表示されます。
5. 観測事象を選択します。
6. ケースを選択して [追加] をクリックし、ケースを観測事象に追加してセキュリティインシデントに関連付けます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
既存のケースがない場合は、[新しい **TISC** ケースを作成] をクリックして新しいケースを作成することもできます。

次の確認メッセージが表示されます。

- 次の観測事象がアーティファクトとして正常に追加されました。
- 次の観測事象が TISC に送信され、選択した TISC ケースレコードに正常に追加されます。

注:
観測事象アクティビティの処理や関連付けは、関連付けの完了時にアクティビティストリームにポストされます。

7. 脅威インテリジェンスセキュリティセンターのワークスペースにログインして、関連するケースレコードを表示し、手順を進めます。
詳細については、「SIR ワークスペースとの TISC 統合」を参照してください。

注:

セキュリティインシデントレスポンスワークスペースで、[調査] タブや [関連レコード] タブから観測事象をケースレコードに関連付けることもできます。

注:
[調査] から観測事象を関連付けるには、以下の手順に従い、「関連レコード」の 観測事象を TISC ケースに追加 から関連付けます。また、[調査] タブに移動し、ページの左側に表示される [エントリーポイントリスト] セクションに移動し、[関連する観測事象] を選択して、TISC ケースに観測事象を追加することもできます。

TISC からの関連情報を表示

このセクションを使用して、SIR ワークスペースで、関連する攻撃者、攻撃パターン、キャンペーン、ケースなどの TISC からの関連情報を表示します。

始める前に
必要なロール：sn_si.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

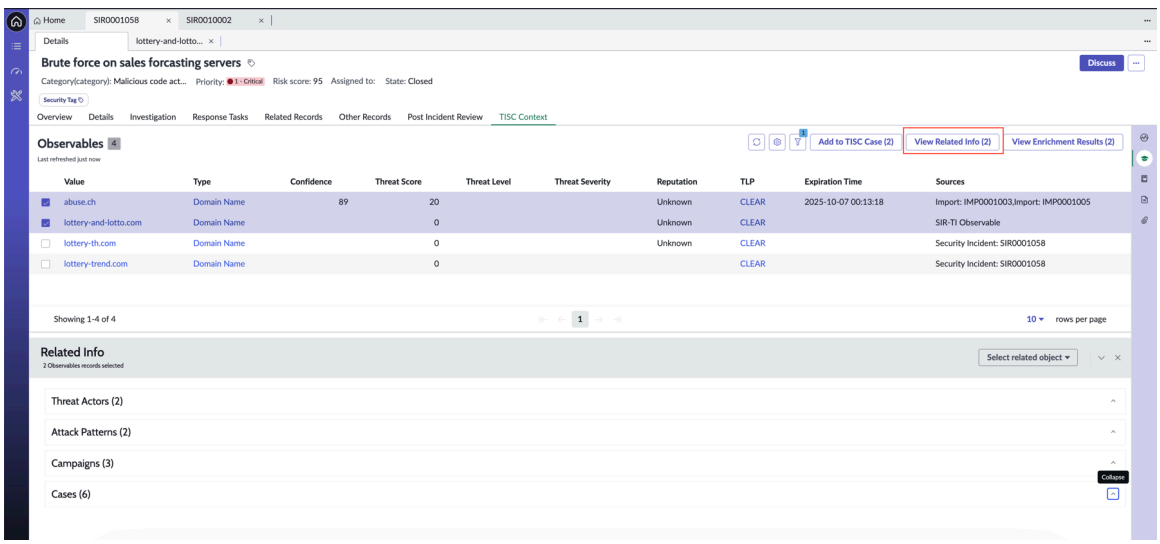
1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > セキュリティインシデント > **All** (すべて).
2. 調査している特定のセキュリティインシデントを見つけて開きます。
   これは、インシデント ID を検索するか、[クイックフィルター] セクションから参照するか、インシデントステータスでフィルタリングすることによっても実行できます。
3. インシデントが開いたら、**[TISC** コンテキスト] タブに移動します。
   [関連情報を表示] の表示：

   インシデントの詳細では、複数のセクションで関連情報を確認することができます。

   a. 観測事象を 1 つ以上選択します。

   b. [関連情報を表示] ボタンをクリックします。
   このセクションには、選択した観測事象に関する関連情報が表示されます。

名前	説明
攻撃者	選択した観測事象に関連する攻撃者に関する TISC からの情報を表示します。
攻撃パターン	選択した観測事象に関連する攻撃パターンに関する TISC からの情報を表示します。
キャンペーン	選択した観測事象に関連するキャンペーンに関する TISC からの情報を表示します。
ケース	選択した観測事象に関連する TISC ケースに関する TISC からの情報を表示します。



エンリッチメント結果を表示

このセクションを使用して、SIR ワークスペースで TISC からの [脅威のルックアップの結果]、[サイティング]、[観測事象のエンリッチメント結果] などの観測事象のエンリッチメント結果を表示します。

始める前に

必要なロール：sn_si.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

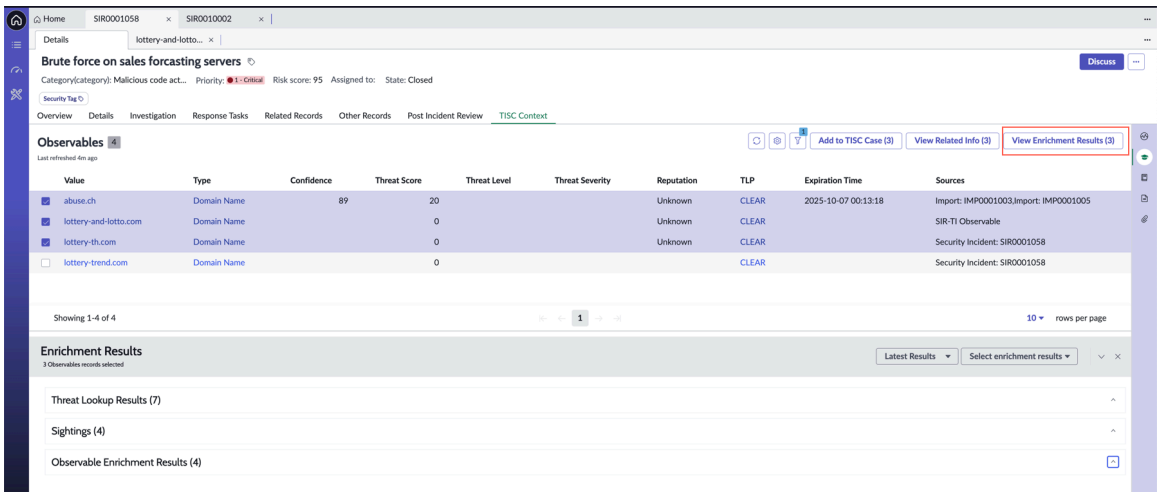
1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > セキュリティインシデント > **All** (すべて).
2. 調査している特定のセキュリティインシデントを見つけて開きます。
   これは、インシデント ID を検索するか、[クイックフィルター] セクションから参照するか、インシデントステータスでフィルタリングすることによっても実行できます。
3. インシデントが開いたら、**[TISC** コンテキスト] タブに移動します。
   エンリッチメント結果を表示：

   インシデントの詳細では、複数のセクションで関連情報を確認することができます。

   a. 観測事象を 1 つ以上選択します。

   b. [エンリッチメント結果を表示] ボタンをクリックします。
   このセクションでは、選択した観測事象に関連する詳細情報が表示されます。

名前	説明
脅威のルックアップの結果	選択した TISC 観測事象に関連する脅威のルックアップ結果をすべて一覧表示します。
サイティング	選択した TISC 観測事象に関連するサイティングをすべて一覧表示します。
観測事象のエンリッチメント結果	選択した TISC 観測事象に関連する観測事象のエンリッチメント結果をすべて一覧表示します。



セキュリティインシデントレスポンス のレポート

セキュリティインシデントに関連付けられたすべてのレポートは、[レポート] セクション内で分析および共有に使用できます。

アナリストは次のことができます。

- レポートの作成
- レポートの編集
- レポートの削除

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

レポートの作成

アナリストは、インシデントのステータスを含むレポートを セキュリティインシデントレスポンス で作成し、メールで共有できます。

始める前に
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. 任意のセキュリティインシデントを開きます。
3. [レポート] を選択します。

   [レポート] ページには、選択したインシデントに対して作成されたすべてのレポートのリストが表示されます。

4. **[New** (新規)] を選択します。
   [テンプレートを選択] ページに、公開されたすべてのテンプレートのリストが表示されます。テンプレートのリストは、アドミンがレポートテンプレートを公開している場合にのみ使用できます。詳細については、「でのレポートテンプレートの作成 セキュリティインシデントレスポンス」を参照してください。
5. レポートテンプレートを選択します。
   レポートが編集モードで開き、テンプレートで構成されたインシデントデータが表示されます。
6. [展開] を選択し、目的のフィールドを挿入/削除します。
   - 共通 **SIR** フィールド:インシデントで最もよく使用されるフィールドのリスト。
   - すべての **SIR** フィールド:インシデントに関連するすべてのフィールド。たとえば、インシデントレポートを生成していて、[簡単な説明] というフィールドを追加する場合は、[すべての **SIR** フィールド] からそのフィールドを選択できます。フィールドを追加するときに、インシデントがレポートに表示される場合の簡単な説明。
   - 関連レコード:特定のインシデントの関連レコード。たとえば、関連する観測事象をレポートに追加する場合は、レポートに追加できます。これらの関連レコードは、テーブル形式で表示されます
   - スクリプト:レポートの日付と時刻を追加するには、現在の日時スクリプトをレポートに追加します。これにより、レポートの作成日時がレポートに追加されます。
7. [プレビュー] を選択して、レポートのプレビューを表示します。
8. [コンテンツの保存] を選択して変更を保存します。
9. オプション: [レポートの詳細を編集] アイコンを選択して、レポート名と説明を更新します。
10. [公開] を選択してレポートを公開します。
11. [レポートをメールで共有] アイコンを選択します。
    a. [宛先] フィールドと **[CC/BCC**] フィールドに受信者のメールを入力します。
    b. メール の件名と本文を更新します。
    c. [送信] を選択して、レポートをメールで共有します。

レポートの編集

アナリストは、未公開のレポートを セキュリティインシデントレスポンス で変更し、メールで共有できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. 任意のセキュリティインシデントを開きます。
3. [レポート] を選択します。

   [レポート] ページには、選択したインシデントに対して作成されたすべてのレポートのリストが表示されます。

4. 更新するレポートを開きます。
   レポートが編集モードで開き、テンプレートで構成されたインシデントデータが表示されます。
5. 必要に応じてレポートを編集します。
6. [プレビュー] を選択して、レポートのプレビューを表示します。
7. [コンテンツの保存] を選択して変更を保存します。
8. オプション: [レポートの詳細を編集] アイコンを選択して、レポート名と説明を更新します。
9. [公開] を選択してレポートを公開します。
10. レポートをメールで共有アイコン を選択します。
    a. [宛先] フィールドと **[CC/BCC**] フィールドに受信者のメールを入力します。
    b. メール の件名と本文を更新します。
    c. [送信] を選択して、レポートをメールで共有します。

レポートの削除

公開済みまたはドラフトステータスの セキュリティインシデントレスポンス レポートを削除できます。

始める前に
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. 任意のセキュリティインシデントを開きます。
3. [レポート] を選択します。

   [レポート] ページには、選択したインシデントに対して作成されたすべてのレポートのリストが表示されます。

4. 削除するレポートを開きます。
5. [削除] を選択します。
   確認メッセージが表示されます。
6. [削除] を選択してレポートを削除します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

でカンファレンスコールまたはチャットを使用したコラボレーション セキュリティインシデントレスポンス

アナリストや影響を受けるユーザーとコラボレーションして、 セキュリティインシデントレスポンス アプリケーションでインシデントについて解決したり、話し合ったりすることができます。

関連情報

セキュリティインシデントレスポンスでカンファレンスコールを開始する

セキュリティインシデントレスポンスでのサイドバーチャットの開始

セキュリティインシデントレスポンスでカンファレンスコールを開始する

セキュリティアナリストは、カンファレンスコールを使用して、他のアナリストや影響を受けるユーザーとリアルタイムでコラボレーションできます。これらのコールにより、インシデントの解決に役立つ情報交換が容易になります。

始める前に

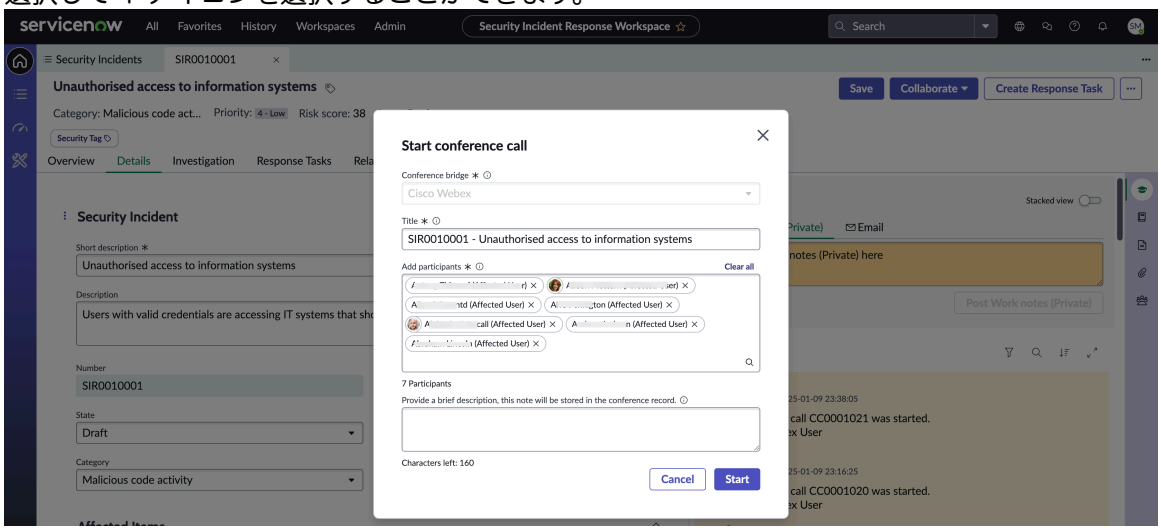
次のアプリとプラグインのインストールとアクティブ化が完了していることを確認します。

- 通知プラグイン (com.snc.notify)。
- 構成可能ワークスペースアプリの通知 UI コンポーネント。
- ビジュアルタスクボードプラグイン (com.devsnc.snb_vtb)

必要なロール:sn_si.analyst または sn_si.manager

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. カンファレンスコールを開始するセキュリティインシデントを開きます。
3. コラボレーション を選択し、通話の開始 を選択するか、カンファレンスコールアイコン) を選択して + アイコンを選択することができます。



[カンファレンスコールを開始] ポップアップが表示されます。

4. [会議ブリッジ] フィールドで会議ブリッジを選択します。
5. [タイトル] にカンファレンスのタイトルを入力します。

> **注:**
> デフォルトでは、インシデントのタイトルがコールのタイトルとして入力されます。デフォルトのタイトルを変更できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

6. [参加者の追加] で通話参加者を追加または削除します。

   注:
   カンファレンス設定の構成に基づいて、事前に入力された参加者リストが [参加者を追加] に追加されるか、参加者の [推奨事項] リストを使用できます。詳細については、「カンファレンスコールのユーザーとグループの管理」を参照してください。

7. カンファレンスコールを開始するための簡単な説明を入力します。
8. [開始] を選択します。

   選択した会議ブリッジでカンファレンスコールが開始されます。すべての参加者は、メールと会議ブリッジを通じて通知を受信します。参加者は、リンクまたは通知を使用してコールに参加できます。

9. セキュリティインシデントレスポンスアプリケーションで関連するインシデントを開いて、カンファレンスコールの詳細を表示します。
10. オプション: [招待をコピー] を選択して、アクティブな通話に参加者を追加します。
11. [コールを終了] を選択します。
    最後の参加者がカンファレンスコールを退出すると、コールは終了します
12. オプション: カンファレンスコールを再開するには、[完了] セクションに移動し、必要なカンファレンスコールの [再開始] オプションを選択します。

アクティブなカンファレンスコールに参加者を追加する

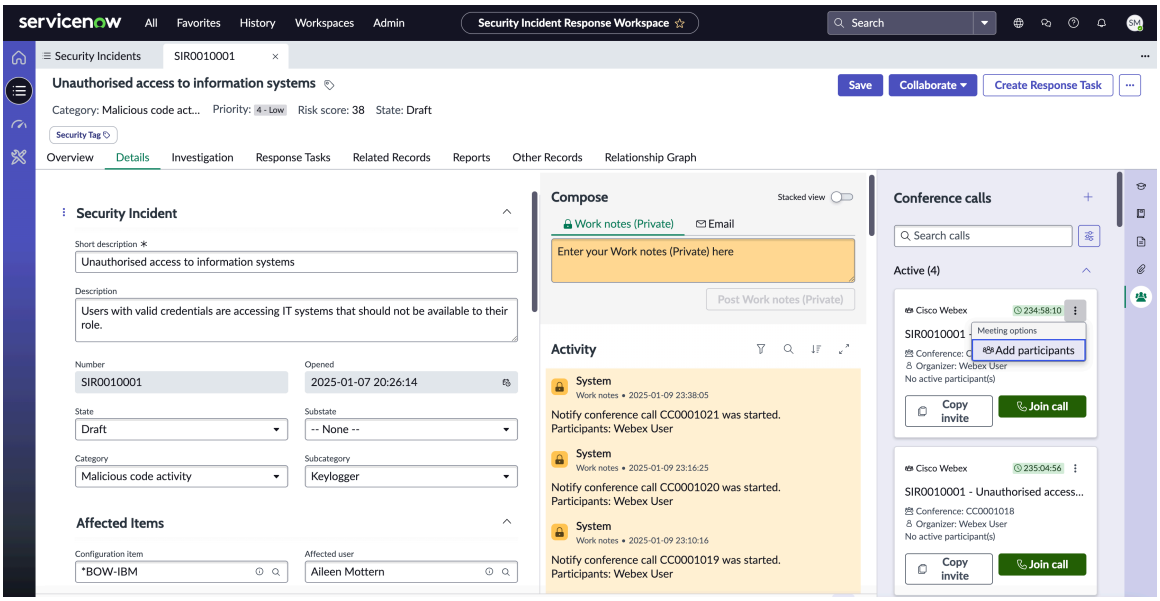
カンファレンスコールを開始する前に参加者を追加していない場合は、アクティブなカンファレンスコールに追加できます。

始める前に
必要なロール:sn_si.analyst、sn_si.manager

手順
1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. カンファレンスコールを開始するセキュリティインシデントを開きます。
3. カンファレンスコールの詳細を表示するには、カンファレンスコールアイコンを選択します。
4. アクティブなカンファレンスへの参加者の追加:

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



- 会議オプションアイコンを選択します ⋮ をクリックして、 参加者の追加を選択します。
- [カンファレンスコール] セクションで [招待をコピー] を選択し、必要な参加者と招待を共有します。

セキュリティインシデントレスポンスでのサイドバーチャットの開始

サイドバーを使用すると、セキュリティアナリストはワークスペースタスクベースまたはインタラクションベースのレコードに基づいて、他のユーザーとリアルタイムでコラボレーションできます。サイドバーディスカッションは、情報や知識の交換を促進して、より迅速な問題解決や質の高い成果の実現を支援します。

始める前に

必要なロール：sn_si.read

Omni-Experience Standard Feature Set プラグインが有効になっていることを確認します。詳細については、「Installing Sidebar」を参照してください。

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. リストビュー アイコンを選択します。
3. サイドバーディスカッションを開始するセキュリティインシデントを開きます。
4. コラボレーション を選択し、チャットの開始 を選択します。
   [サイドバーディスカッションを開始] ダイアログが表示されます。

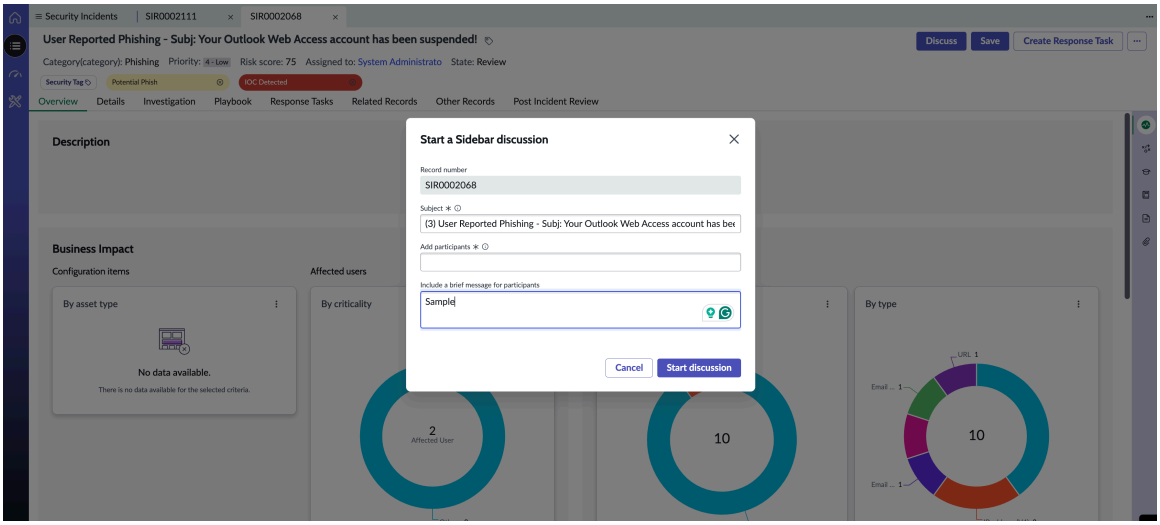
   注:
   サイドバーと Microsoft Teams の統合により、サイドバーユーザーと Microsoft Teams ユーザーはそれぞれのプラットフォームから相互に通信できます。詳細については、「Sidebar and Microsoft Teams」を参照してください。

5. [サイドバーディスカッションを開始] ダイアログボックスで、フィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンスでのサイドバーチャットの開始



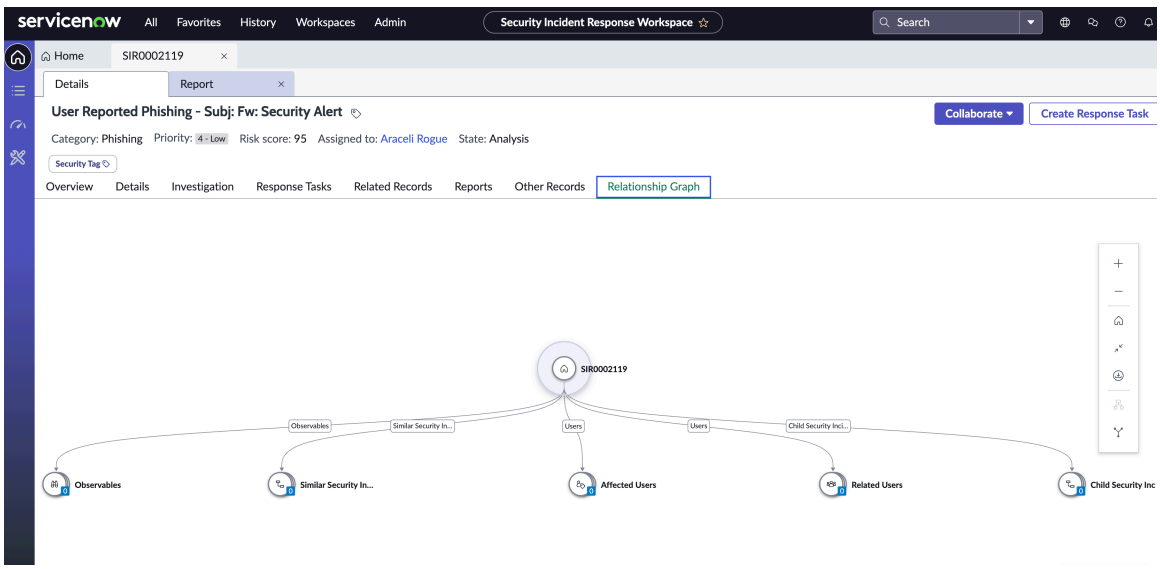
6. [ディスカッションを開始] を選択します。
7. クイックアクションなどの追加構成を実行できます。
   アクションの使用を制限するには、クイックアクションページの [グループに適用 **(Apply to group)**] フィールドを使用します。詳細については、「Creating a quick action」を参照してください。

インシデントの詳細の表示 **a relationship graph**

関係グラフは、インシデントの相互接続されたエンティティを視覚的に表現し、セキュリティインシデントの分析と理解を深めます。これにより、ユーザーは既存のセキュリティインシデントを関連する観測事象、構成アイテム、類似のオープン SIR、およびその他のエンティティと相互リンクできます。

注:
この機能は、 セキュリティインシデントレスポンス ワークスペースでのみ使用できます。

次の関係グラフは、インシデントの詳細を表示します。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インシデントのカテゴリノード

次のカテゴリノードを関係グラフに追加できます。

注:
関係グラフはステートレスであり、デフォルトのグラフに更新を保存することはできません。

- 観察事項
- 影響を受けるユーザー
- 類似のセキュリティインシデント
- 子セキュリティインシデント
- 関連ユーザー
- 構成アイテム
- 関連構成アイテム
- 対応タスク
- 関連フィッシングメール
- 関連フィッシングヘッダー
- サイティング検索の詳細
- 脅威情報ルックアップの結果

インシデントの関係グラフを開くと、デフォルトで次のカテゴリノードが追加されます。

- 観察事項
- 影響を受けるユーザー
- 類似のセキュリティインシデント
- 子セキュリティインシデント
- 関連ユーザー

次の操作を実行できます。

- 任意のオブジェクトを拡大し、画面に収まり、ノードをドラッグします。
- 利用可能な場合は各ノードにサブサイドを追加し、サブノードの詳細を表示します。
- グラフからノードまたはサブノードを非表示にします。
- サブノードの詳細を表示します。

インシデントの関係グラフの作成

セキュリティインシデントレスポンス でノード関係グラフを作成して、既存のインシデントを悪意のある観測事象や関連する構成アイテムなどと関連付けることで、既存のインシデントの理解を深めることができます。

始める前に

注:
関係グラフはステートレスであり、デフォルトのグラフに更新を保存することはできません。

必要なロール：sn_si.analyst

自動翻訳

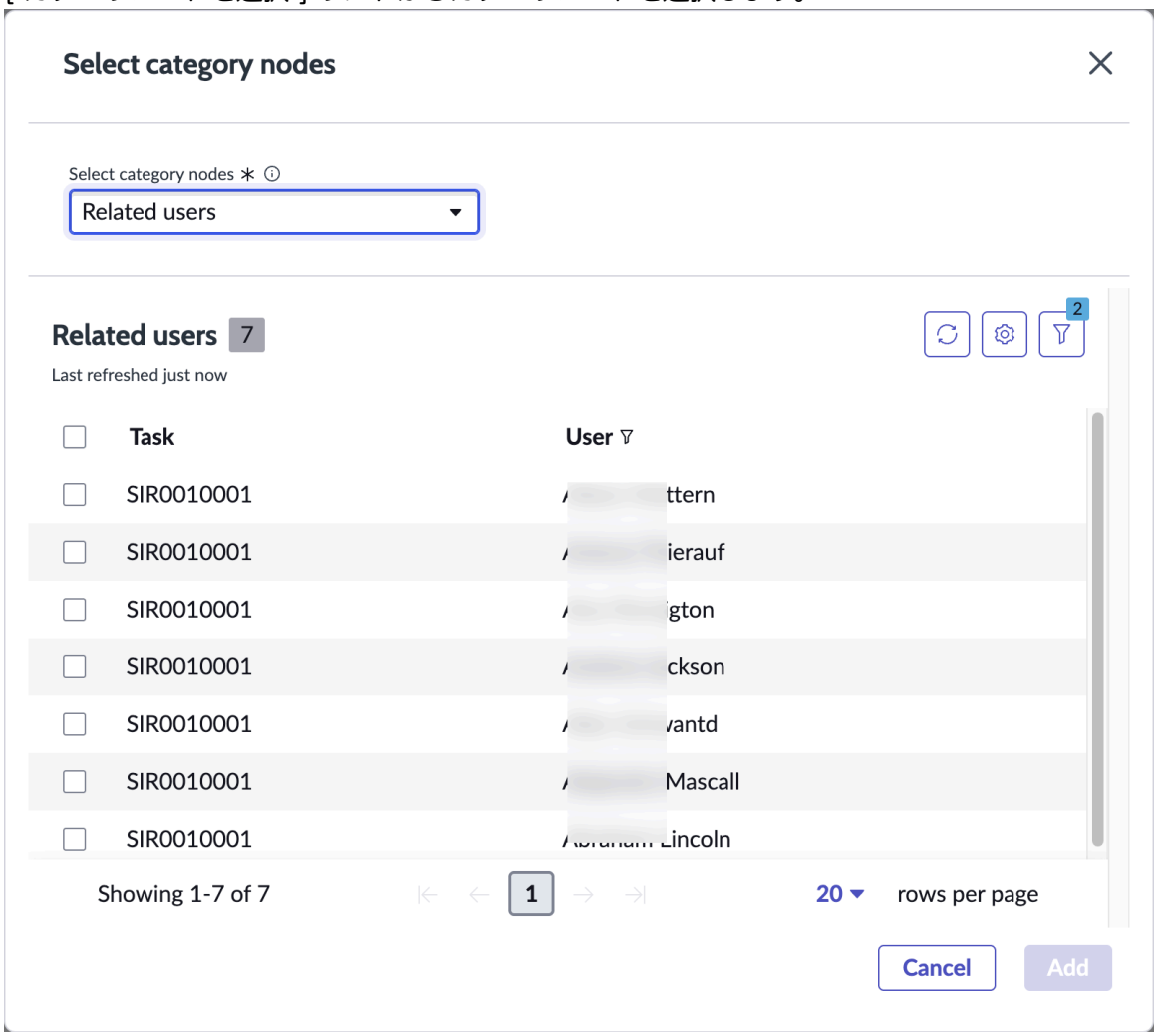
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. 任意のセキュリティインシデントを開きます。
3. 関係グラフを選択します。

   選択したインシデントの関係グラフが開き、親ノードとデフォルトのカテゴリノードが表示されます。

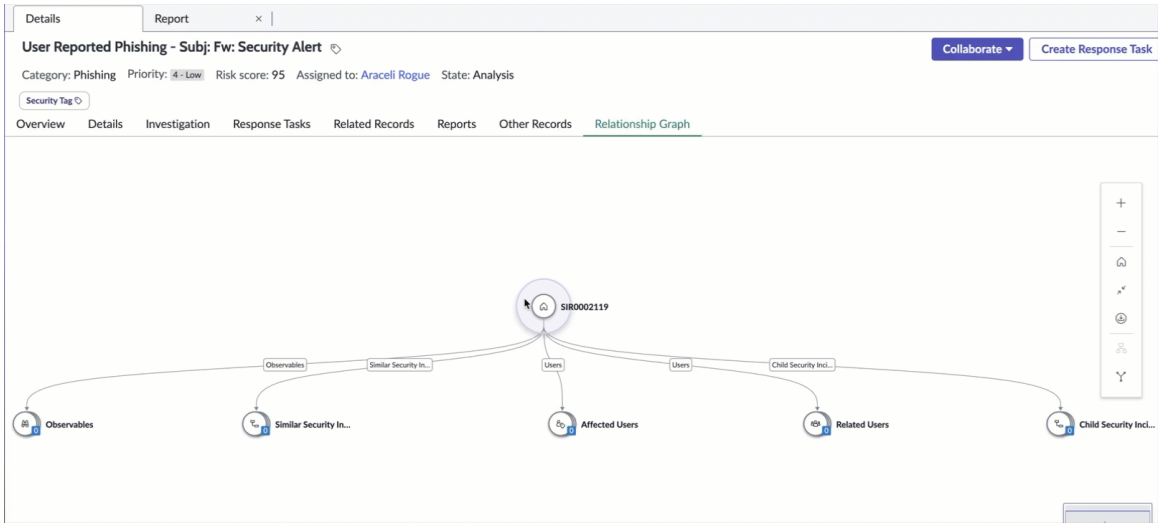
4. 親ノードを選択して長押し (または右クリック) します。
5. [リンクノード] を選択します。
   [カテゴリノードを選択] ページが表示されます。
6. [カテゴリノードを選択] リストからカテゴリノードを選択します。



   選択したカテゴリのすべての関連レコードのリストが表示されます。たとえば、ノードカテゴリから [影響を受けるユーザー] を選択すると、このインシデントの影響を受けるすべてのユーザーのリストが表示されます。

7. リストからレコードを選択します。
8. [**Add**] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



カテゴリがノードとして追加され、その関連レコードがサブノードとしてマップに追加されます。

9. [マップをエクスポート] アイコンを選択します。 [ ] を選択して、マップをシステムにダウンロードします。

> **注:**
> 画面に表示されるマップの部分は、PDF ファイルで利用できます。PDF で完全なマップを取得するには、マップをエクスポートする前に [画面に合わせる] を選択します。

10. サブノードを選択し、[詳細の表示] を選択してサブノードの詳細を表示します。

セキュリティインシデントプレイブック

セキュリティインシデントのプレイブックフローを自動または手動で呼び出します。

Playbook は、少なくとも 1 つのプレイブックがセキュリティインシデントに関連付けられている場合にのみ表示されます。プレイブックコンポーネントは、プロセスオートメーションデザイナー (PAD) でビルドされたプロセスでのみ機能し、フローデザイナーでビルドされたフローでは機能しません。既存のフローデザイナーが有効になっている場合は引き続き機能し、アクティビティは応答タスクとして引き続きレンダリングされます。

プレイブックをセキュリティインシデントに関連付けるには、次の 2 つの方法があります。

- プレイブックを自動的に呼び出す
- プレイブックを手動で追加する

プレイブックを自動的に呼び出す

プレイブックを自動的に呼び出すには、[プロセスオートメーションデザイナー **(PAD)]** を使用してプロセスを定義する必要があります。トリガー条件が満たされると、Playbook のタブが自動的にレンダリングされ、プレイブックアクティビティが表示されます。

プレイブックを手動で追加する

プレイブックを手動で呼び出すには、 フォーム UI アクションのドロップダウンに移動し、[プレイブックを追加] を選択します。詳細については、「プレイブックを追加」を参照してください。

> **注:**
> 利用可能なプレイブックが既に存在する場合、追加された新しい Playbook は既存のプレイブックと並行して実行されます。

自動翻訳

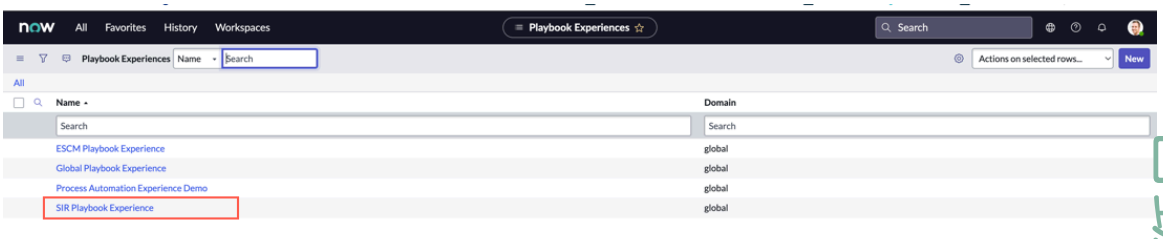
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- プレイブック内では、アナリストはステータス別にプレイブックカードをフィルタリングできます。
- アナリストは、省略記号アイコンからプレイブックを選択してキャンセルできます。
- 各アクティビティ内では、アナリストは [スキップ]、[完了としてマーク]、[キャンセル] などのアクティビティカード内で定義されたアクション、または [サンドボックスに送信]、[メールの検索 (Search Emails)] などのオーケストレーションアクションを実行できます。
- これらの各アクションはアクティビティ定義内で定義され、表示される全カードはアクティビティ定義自体のビルド時にカスタマイズできます。

注:
今後のアクティビティ定義と実行する次の手順はすべてロックアイコン付きで表示され、ユーザーに対しては読み取り専用モードとなります。Playbook 表示モードは、以下で説明する構成によって制御されます。

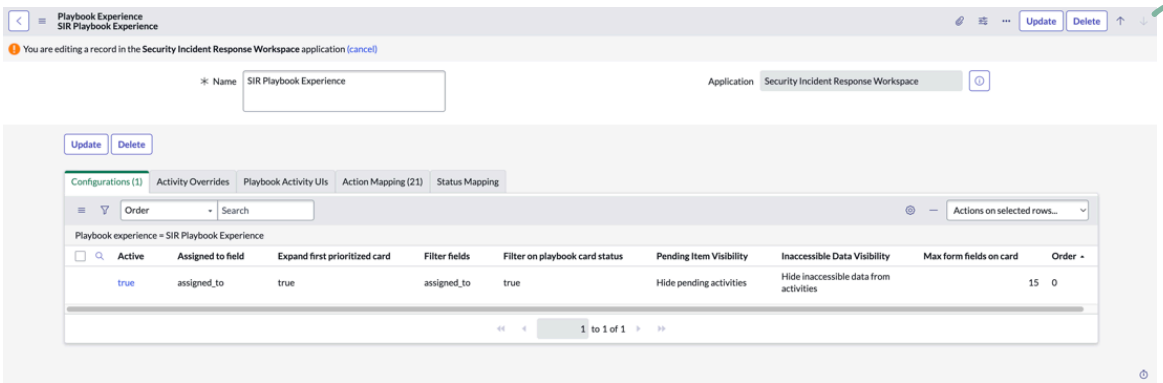
1. 次のように移動する。 **All** (すべて) > プレイブックエクスペリエンス.
2. [プレイブックエクスペリエンス] ページで、**[SIR** プレイブックエクスペリエンス] を選択します。

プレイブックエクスペリエンス



[プレイブックエクスペリエンス **SIR** プレイブックエクスペリエンス] ページが表示されます。

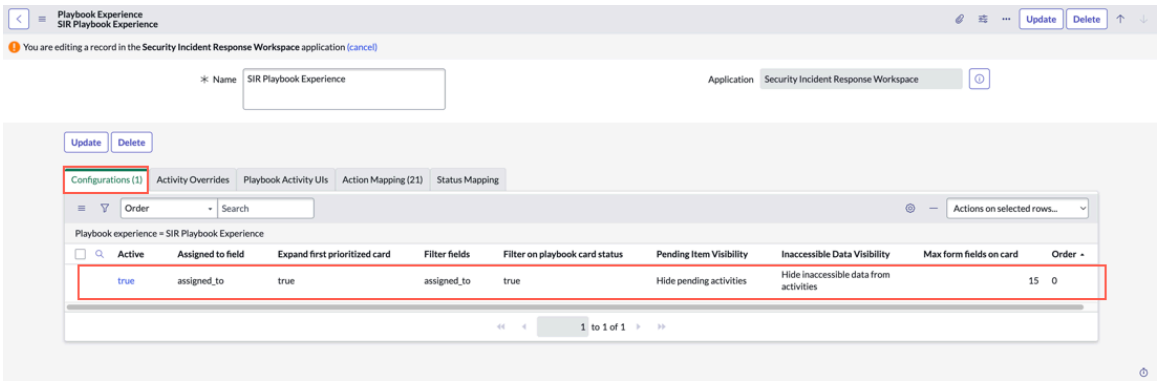
プレイブックエクスペリエンスレコード



3. [設定] レコードをクリックします。

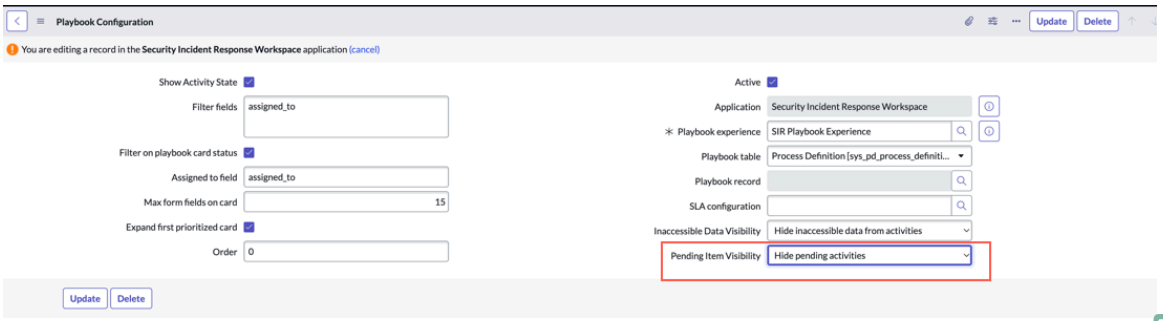
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [構成] タブで、[SIR プレイブックエクスペリエンス構成] をクリックします。

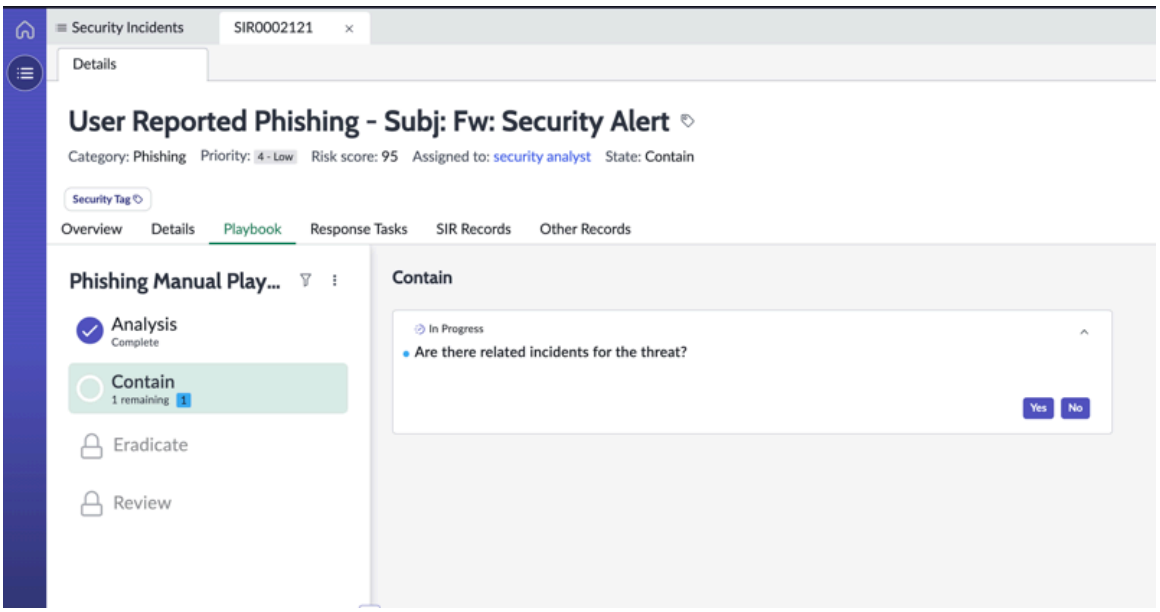
プレイブック構成



5. [保留中のアイテムのヴィジビリティ] フィールドのドロップダウンリストに移動し、目的のオプションを選択してレコードを保存します。次のオプションから選択します。

- 処理待ちのアクティビティを非表示にします：ワークスペースの [Playbook] セクションで表示させる処理待ちのアクティビティを非表示にするには、このオプションを選択します。

ユーザーから報告されたフィッシングの例

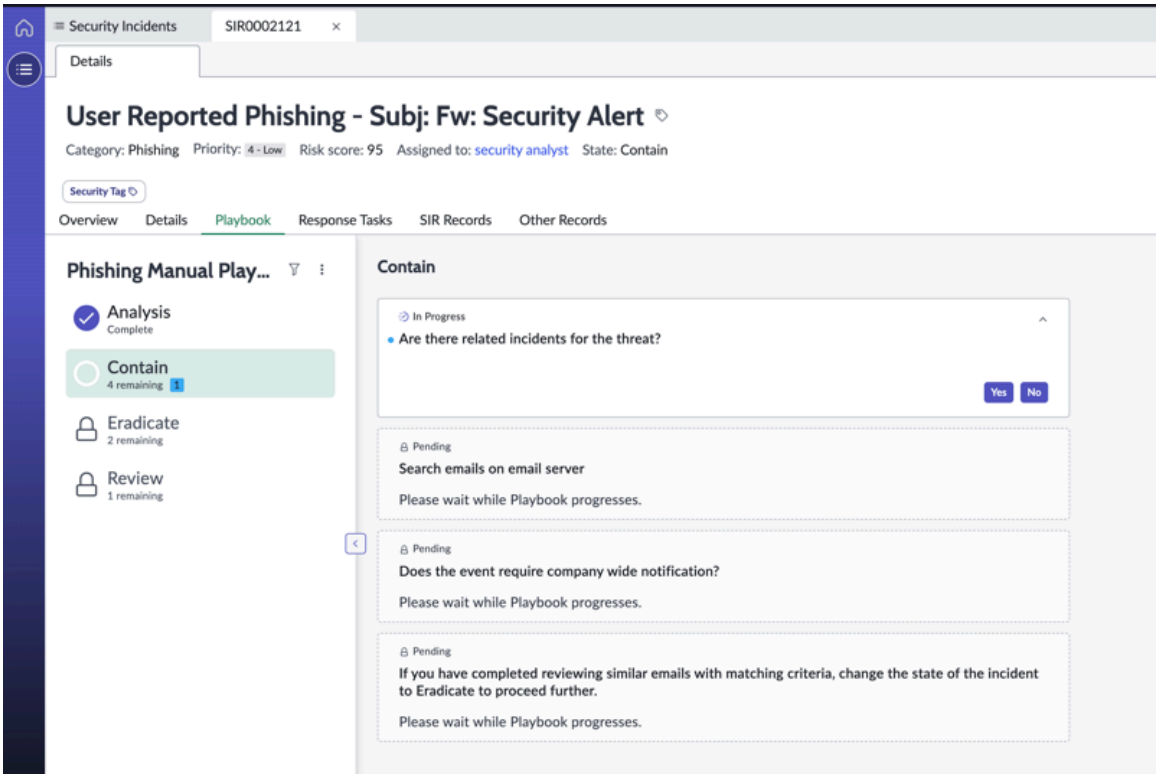


- 処理待ちのステージとアクティビティを表示します：ワークスペースの [Playbook] セクションで表示させる処理待ちのステージおよびアクティビティを表示するには、このオプションを選択します。

自動翻訳

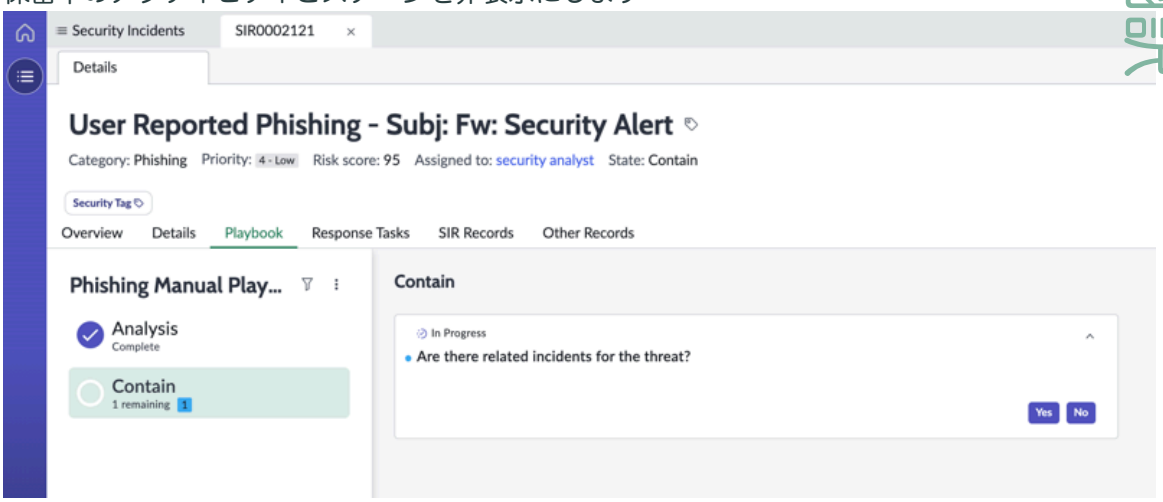
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

保留中のステージとアクティビティを表示します



- 処理待ちのアクティビティとステージを非表示にします：ワークスペースの [Playbook] セクションで表示させる処理待ちのステージおよびアクティビティを非表示にするには、このオプションを選択します。

保留中のアクティビティとステージを非表示にします

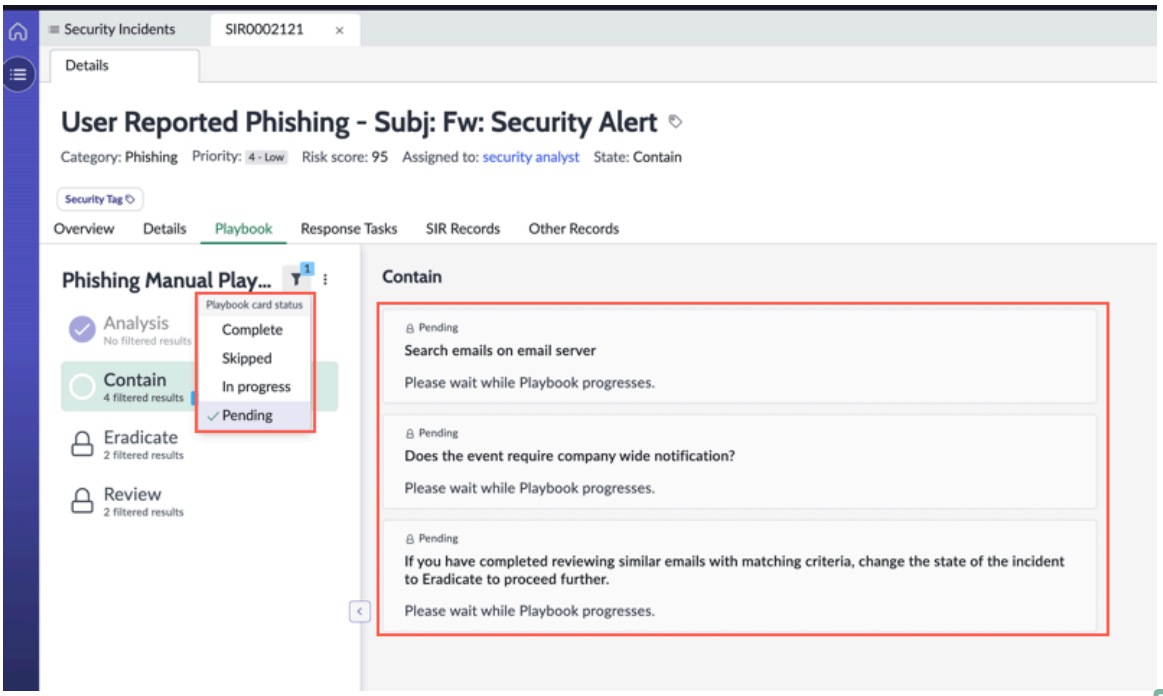


自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [プレイブック] セクションで、フィルターオプションを使用して、プレイブックカードステータス (アクティビティ定義) でアクティビティをフィルタリングします。

プレイブックカードステータス



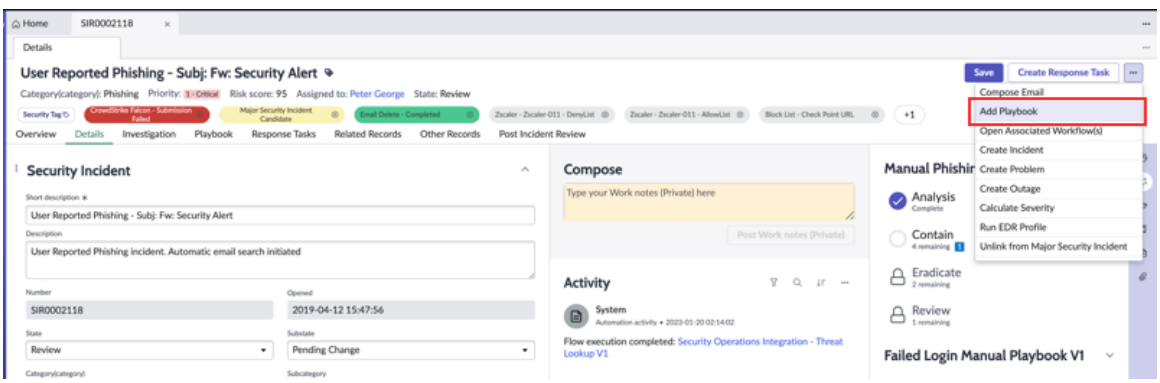
プレイブックを追加

このセクションを使用して、プレイブックを手動で追加します。

始める前に
必要なロール：sn_si.analyst

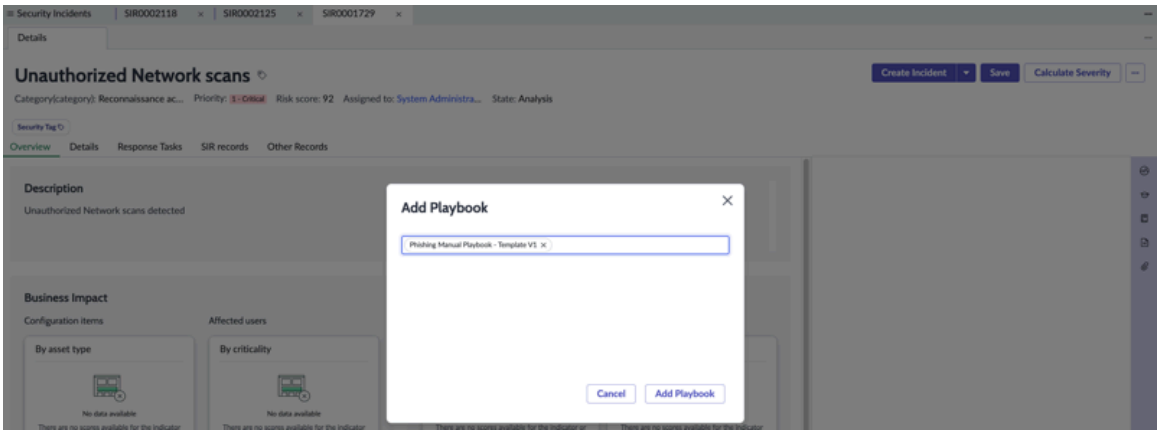
手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > セキュリティアナリストワークスペース.
2. インシデントレコードを開きます。
3. [プレイブックを追加] をクリックします。

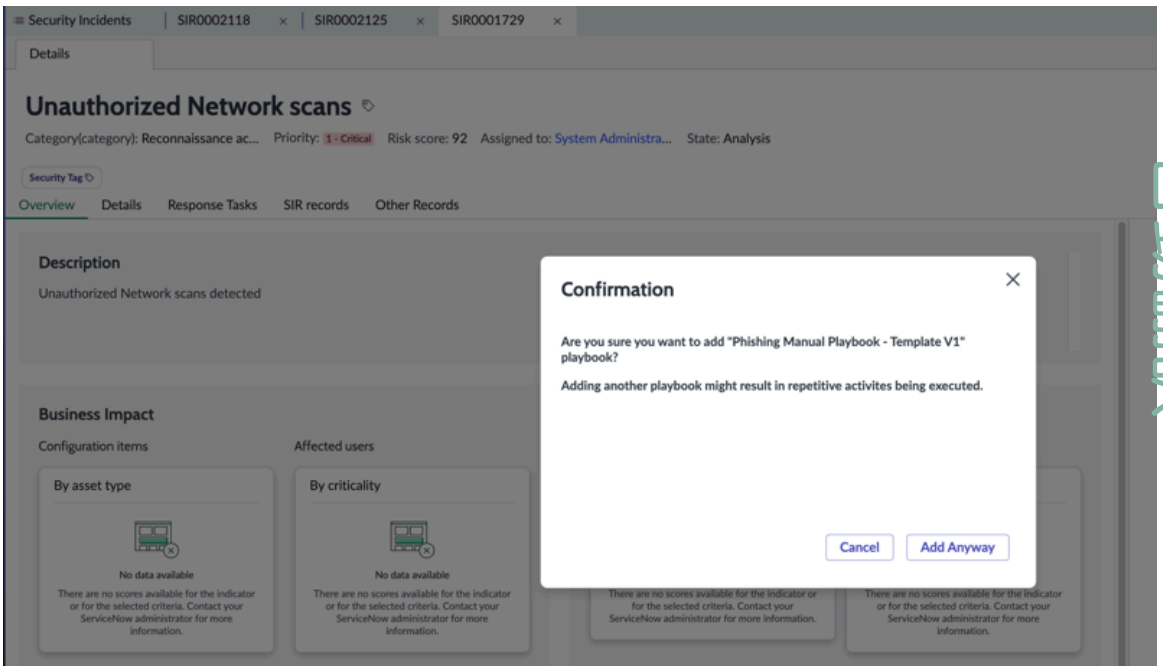


[プレイブックを追加] ダイアログボックスが表示されます。

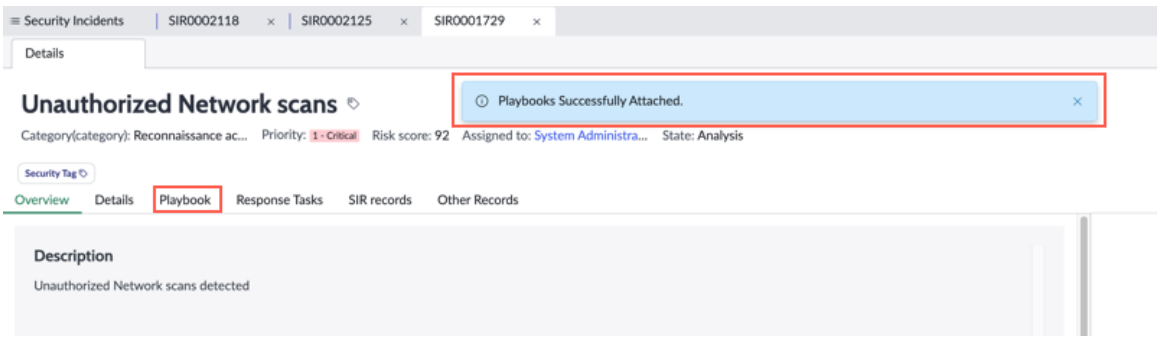
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. プレイブックのテンプレートを選択します。
5. [プレイブックを追加] をクリックします。
   確認のための確認メッセージダイアログボックスが表示されます。
6. [このまま追加] をクリックします。

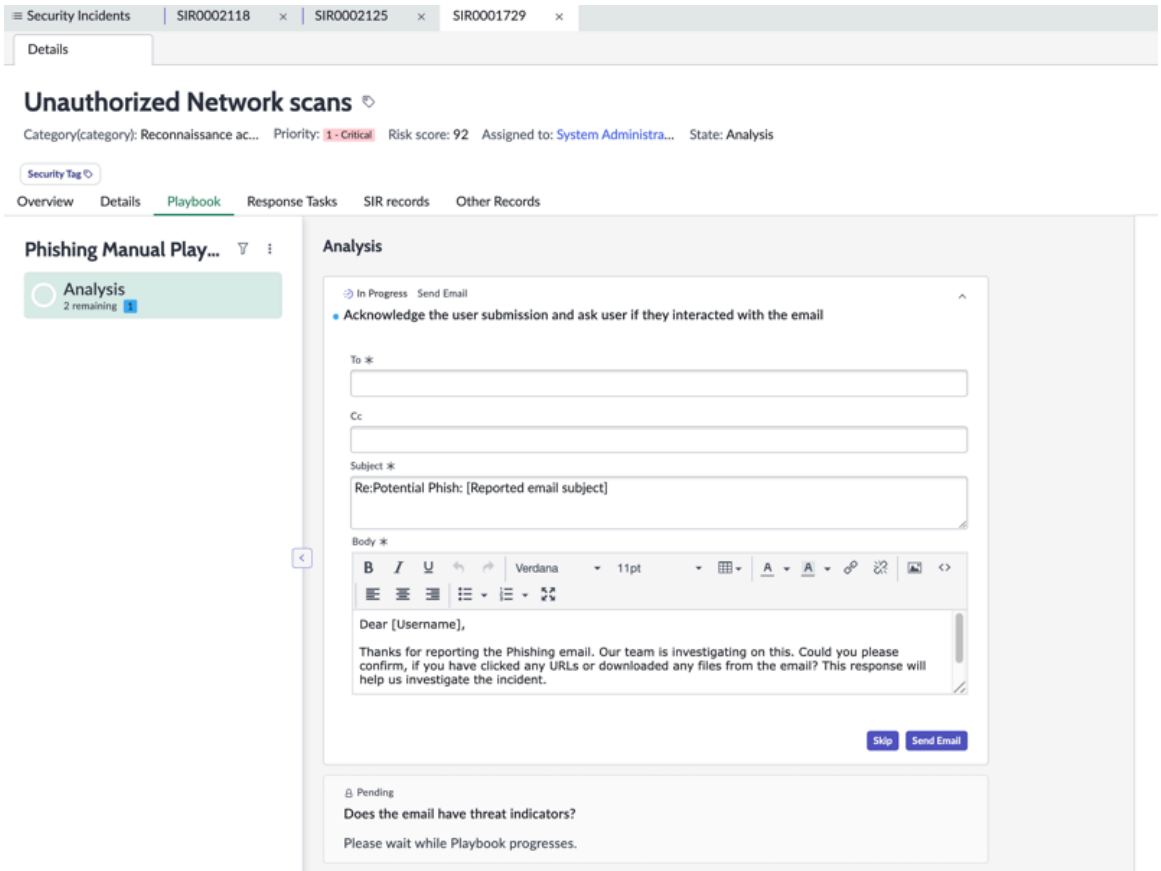


7. [プレイブック] が [詳細] タブの横に追加されます。



8. **[Playbook]** タブをクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



9. 次のレベルに移動するには、リストされている一連のアクティビティを実行します。

> **注:**
> セキュリティインシデントがプレイブックに関連付けられている場合、関連付けられたプレイブックがクローズされるかキャンセルされるまで、ユーザーは同じセキュリティインシデントに同じプレイブックを再度関連付けることはできません。

プレイブックの前提条件

プレイブックをビルドするには、次のロールとプラグインが必要です。

必要なロール：admin

- プロセスオートメーションデザイナー (PAD) [com.glide.pad.license] プラグインを有効にします。
- プレイブックエクスペリエンスの次のプラグインを有効にします。
  - com.playbook_experience
  - now_playbook_exp
  - com.glide.playbook_experience.config
- Security Operations スポークを有効にしてフロー [com.snc.secops.spoke] にアクセスします。
- エンタープライズセキュリティケース管理 PAD 共通

このガイドを読み始める前に、プレイブックエクスペリエンスおよび プロセスオートメーションデザイナー のプラットフォームドキュメントをお読みください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ワークフロースタジオでの既存プレイブックの再構築

ワークフロースタジオで既存のフローをプレイブックに直接変換することはできません。アナリストをガイドする応答タスクを作成する各フローデザイナーのステップは、個別のアクションまたはサブフローに分解する必要があります。

ワークフロースタジオで既存のフローをプレイブックに直接変換することは許可されていません。アナリストをガイドする応答タスクを作成する各フローデザイナーのステップは、個別のアクションまたはサブフローに分解する必要があります。これらの詳細なサブフローまたはアクションを使用して、アクティビティ定義を作成する必要があります。これらのアクティビティ定義をビルドすると、プロセス定義のステージ内にアクティビティとして追加されます。複数のプレイブックでアクティビティ定義を再利用できます。

各アクティビティをカスタマイズして、アクティビティ定義をビルドするときに必要なアクションとカードの外観をレンダリングできます。アクティビティでは、メールクライアント、テーブル、アクション、KB 記事、URL などを表示できます。アクティビティ定義と基になるアクションまたはサブフローの作成方法を定義できます。

詳細については、以下のセクションを参照してください。

- アクティビティ定義
- プロセスオートメーションデザイナー

アクティビティ定義

Now Platform では、ベースシステム内のいくつかのアクティビティ定義を利用できます。さらに、SIR ワークスペースのベースシステムであるプレイブックには、エンタープライズセキュリティケース管理 PAD 共通アプリケーションのベースシステムで定義されたいくつかのアクティビティ定義があります。

必要なロール：sn_si.admin

ベースシステムの一部であるアクティビティ定義のリストは次のとおりです。

アクティビティ定義	テーブル	説明	アプリケーション
エクスペリエンスなしの条件待ち (Wait For Condition with No Experience)	グローバル [global]	エクスペリエンスなしの条件待ち (Wait For Condition with No Experience)	エンタープライズセキュリティケース管理 PAD 共通
CSF X サンドボックスに送信	セキュリティインシデント [sn_si_incident]	サンドボックスに送信	エンタープライズセキュリティケース管理 PAD 共通
メール送信	セキュリティインシデント [sn_si_incident]	SIR プレイブックのメールアクティビティを送信します。	エンタープライズセキュリティケース管理 PAD 共通
メールを検索	セキュリティインシデント [sn_si_incident]	メールサーバーでメールを検索します。	エンタープライズセキュリティケース管理 PAD 共通
タスクステータスを更新	セキュリティインシデント [sn_si_incident]	タスクステータスを更新します。	Enterprise Security ケース管理 PAD Commons
メールを削除	セキュリティインシデント [sn_si_incident]	メールを削除します。	エンタープライズセキュリティケース管理 PAD 共通

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクティビティ定義	テーブル	説明	アプリケーション
はい/いいえでの結果 (Yes No Outcome)	タスク [task]	期待される成果	エンタープライズセキュリティケース管理 PAD 共通

アクティビティ定義の例：メールを送信

[メールを送信] アクティビティ定義の例を次に示します。

基本

基本的な詳細は、名前 (ラベル)、アプリケーション、説明、テーブル、およびアクセス可能なすべてのアプリケーションをキャプチャします。

自動化プランとアクティビティエクスペリエンスを追加して送信します。送信後、ドキュメントを編集して各タブに詳細を追加します。

自動化プラン

自動化プランは、フローデザイナーを使用してビルドされたバックエンドアクションまたはサブフローを関連付けます。この例では、[メールを送信 **- ESCM** アクティビティ **(Send Email - ESCM Activity)]** サブフローを使用します。

このサブフローはメールを送信できるようにします。メールを送信するコアロジックが含まれており、すべての入力フィールドと出力フィールドが定義されています。

入力フィールドはすべて自動化プランセクション内に表示されます。各入力フィールドは、アドミニストレーターに対してのみ、標準のモーダル、標準のモーダルおよび構成パネルで表示できます。

- アドミン表示のみ **(Admin visibility only)**：アドミニストレーターに設定すると、アドミンのみが表示できます。
- 標準のモーダルに含める **(Include in standard model)**：標準のモーダルで表示するように設定すると、プロパティモーダルにのみ表示されます。
- 標準のモーダルと構成パネルに含める **(Include in standard model and configuration panel)**：標準のモーダルと構成パネルで表示するように設定すると、PAD 構成パネルとプロパティモーダルに表示されます。詳細については、「アクティビティ定義の作成」を参照してください。

構成時にこれらの値を変更する必要がない場合は、アクティビティ定義の時点で入力フィールドを定義できます。これにより、ビジネスプロセスオーナーはプロセス内でアクティビティを構成する時間を節約できます。

アクティビティエクスペリエンス

[アクティビティエクスペリエンス] タブは、実行時のアクティビティカードの表示方法を定義します。ベースシステムには、以下のコンテンツタイプがあります。

- 承認
- カタログアイテム
- レコードを作成
- 説明
- ナレッジ
- リスト

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 通知
- レコード

選択したエクスペリエンスのタイプに基づいて、追加のフィールドが入力されます。詳細については、Now Platform のドキュメントを参照してください。

この例では [レコード] タイプが選択されています。

> **注:**
> たとえば、テーブルをレンダリングする場合は、エクスペリエンスタイプとしてリストを選択できます。

関連レコード

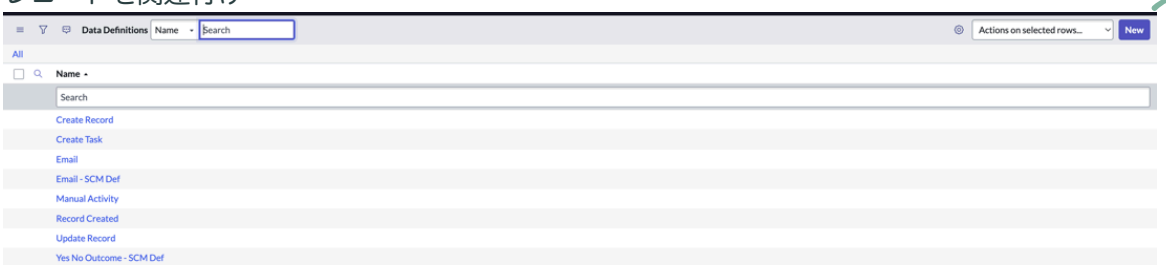
このレコードを使用して、現在のアクティビティに関連するデータを保存します。これにより、ランタイムデータとエクスペリエンスのステータスがキャプチャされます。

- 関連テーブル：フローデータ
- 関連レコード：VL
- エクスペリエンスステータステーブル：フローデータ
- エクスペリエンスステータスレコード：VL

この例では、フローデータテーブルを使用してランタイムデータをキャプチャします。ランタイムデータはユースケースに応じて変わります。この例でのランタイムデータは [宛先]、[CC]、[件名]、[本文] などのフィールドです。ユースケースごとにフローデータ定義を作成し、ランタイムデータのタイプを定義する必要があります。

1. 左ペインに移動し、「**sys_flow_data_definition.list**」と入力します。フローデータテーブル用に作成された定義のリストが表示されます。

レコードを関連付け

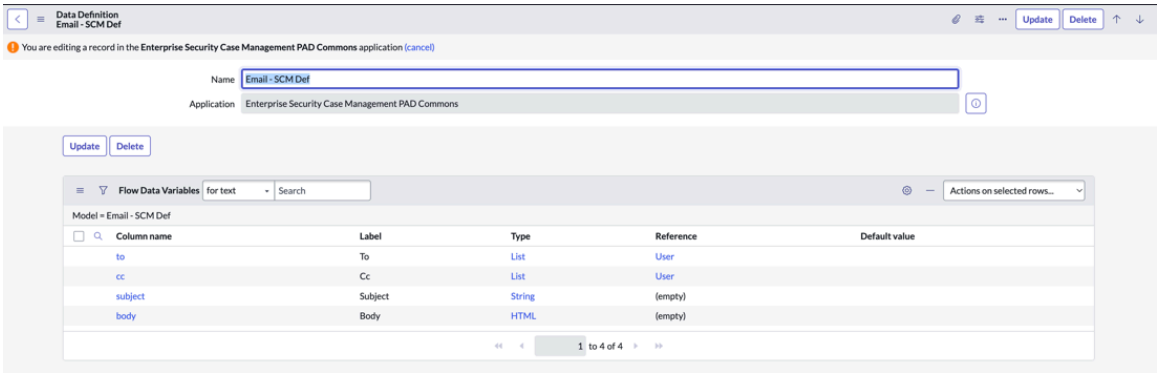


2. [メール **- SCM** 定義 **(Email - SCM Def)]** を開いて、この例に関連する定義を表示します。

自動翻訳

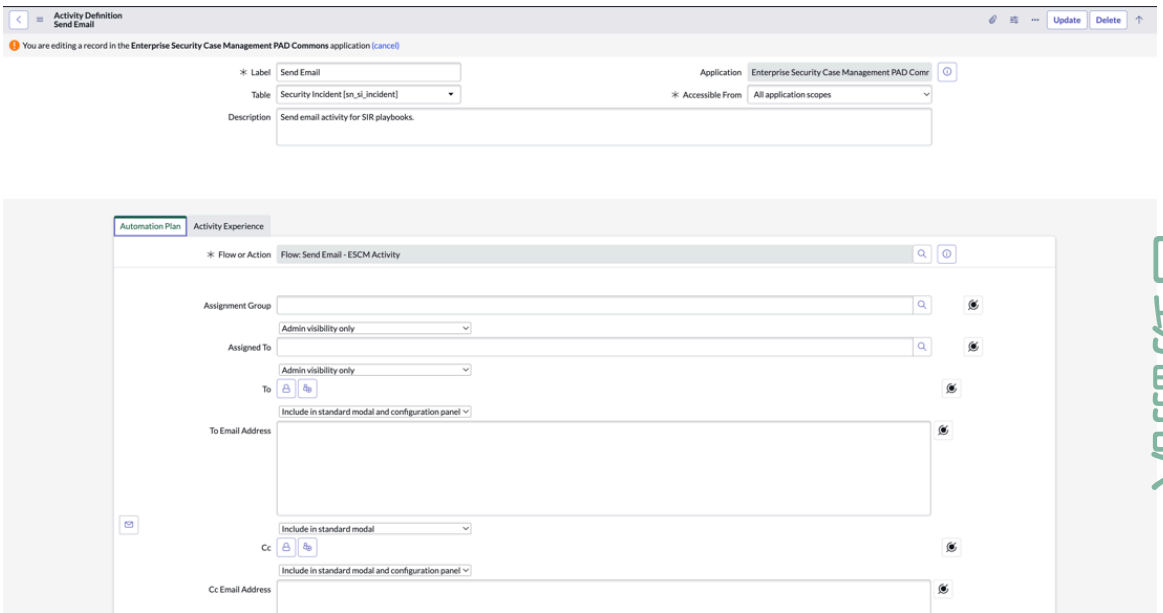
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

メール - **SCM** 定義 **(Email - SCM Def)**



このフローデータの定義は、ランタイムデータをキャプチャするために、このアクティビティ定義 (自動化プランを参照してください) に関連付けられているサブフローまたはアクションで使用する必要があります。

アクティビティ定義



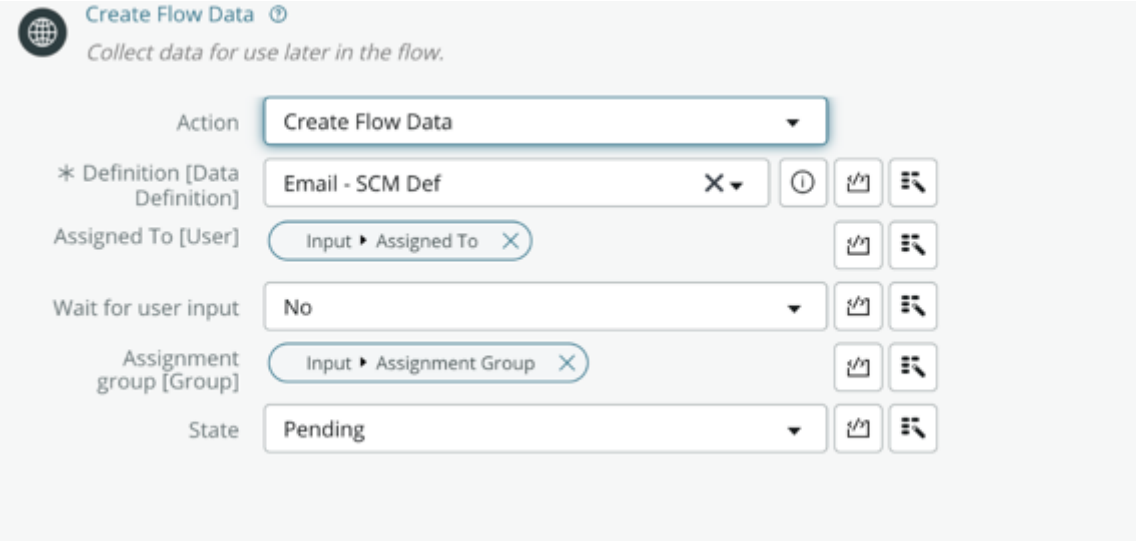
3. この例では、[メール送信 **- ESCM** アクティビティ **(Send Email - ESCM Activity)]** サブフローを使用します。[フローデータを作成] ステップで、作成したフローデータ定義が [定義] フィールドに対してマッピングされます。このフローデータレコードは、サブフロー全体で使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

この例では、アクティビティカードのステータス (エクスペリエンスステータス) がフローデータテーブルにキャプチャされます。

メール送信 **- ESCM** アクティビティ **(Send Email - ESCM Activity)**



注:
フローデータテーブル以外の別のテーブルレコードでランタイムデータをキャプチャする場合 (応答タスクなど)、関連テーブルを応答タスクテーブルとして選択できます。関連レコードは、サブフローによって作成された応答タスクレコードに設定する必要があります。

同様に、エクスペリエンスステータステーブルはアクティビティカードのステータスをキャプチャします。ベースシステムでは、フローデータテーブルのステータスフィールドがアクティビティカードのステータスにマッピングされます。そのため、フローデータテーブルを使用してエクスペリエンスステータスをキャプチャすると、アクティビティカードのステータスが自動的に更新されます。フローデータテーブル以外の別のテーブルを使用して、エクスペリエンスステータスをキャプチャすることもできます。

たとえば、応答タスクのステータスをアクティビティカードのステータスにマッピングすることが可能です。これを行うには：

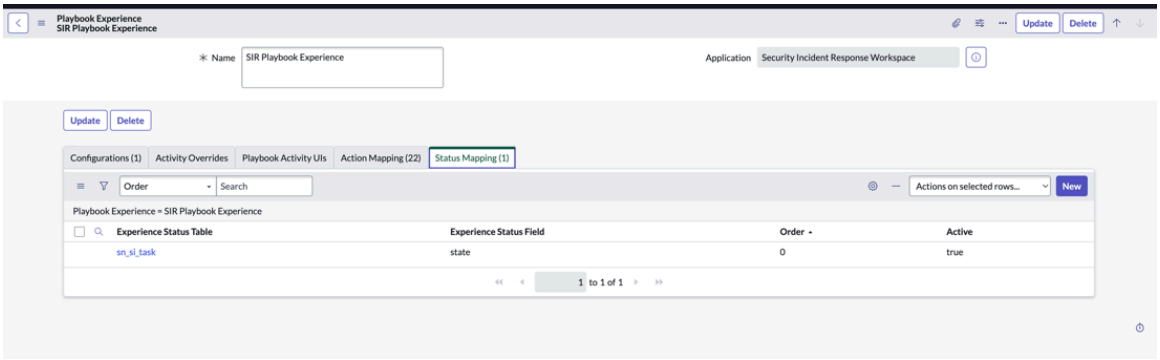
1. 次のように移動する。 **All** (すべて) > プレイブックエクスペリエンス.

Playbook Experience (プレイブックエクスペリエンス)

2. **[SIR** プレイブックエクスペリエンス] を開きます。
3. [ステータスマッピング] 関連リストを開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プレイブックエクスペリエンス

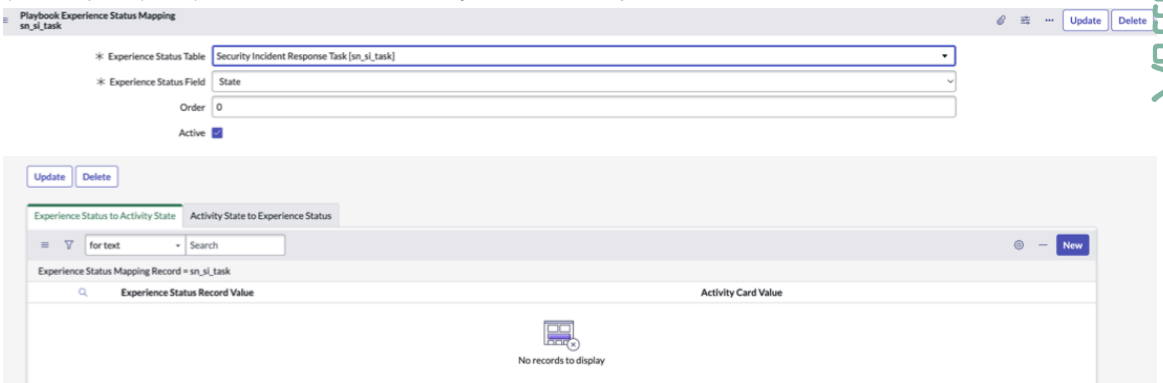


4. [エクスペリエンスステータステーブル] フィールドに [応答タスク] を入力します。
5. [エクスペリエンスステータステーブル] フィールドに [ステータス] を入力します。

エクスペリエンスステータス

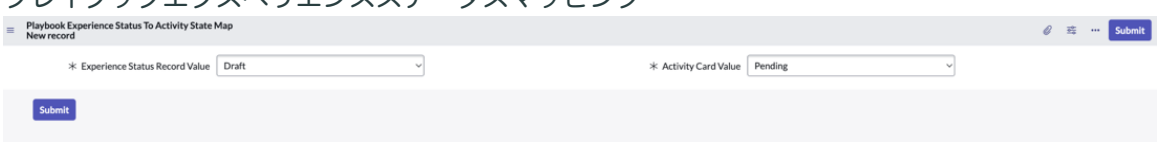
6. [送信] をクリックします。レコードが作成されます。

プレイブックエクスペリエンスステータスマッピング



7. [エクスペリエンスステータスからアクティビティステータスへ] で、応答タスクの状況をアクティビティカードの状況にマッピングします。
8. 左側には応答タスクの状況が表示され、右側にはアクティビティカードのステータスが表示されます。

プレイブックエクスペリエンスステータスマッピング



9. マッピングは双方向に行うことができます。[アクティビティステータスからエクスペリエンス (Activity State to Experience)] 関連リストでも同様に、ステータスを正しくマッピングします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このステップは、前のステップとは逆になっています。左側にはアクティビティカードのステータスが表示され、右側には応答タスクのステータスが表示されます。

プレイブックエクスペリエンスステータスマッピング

詳細

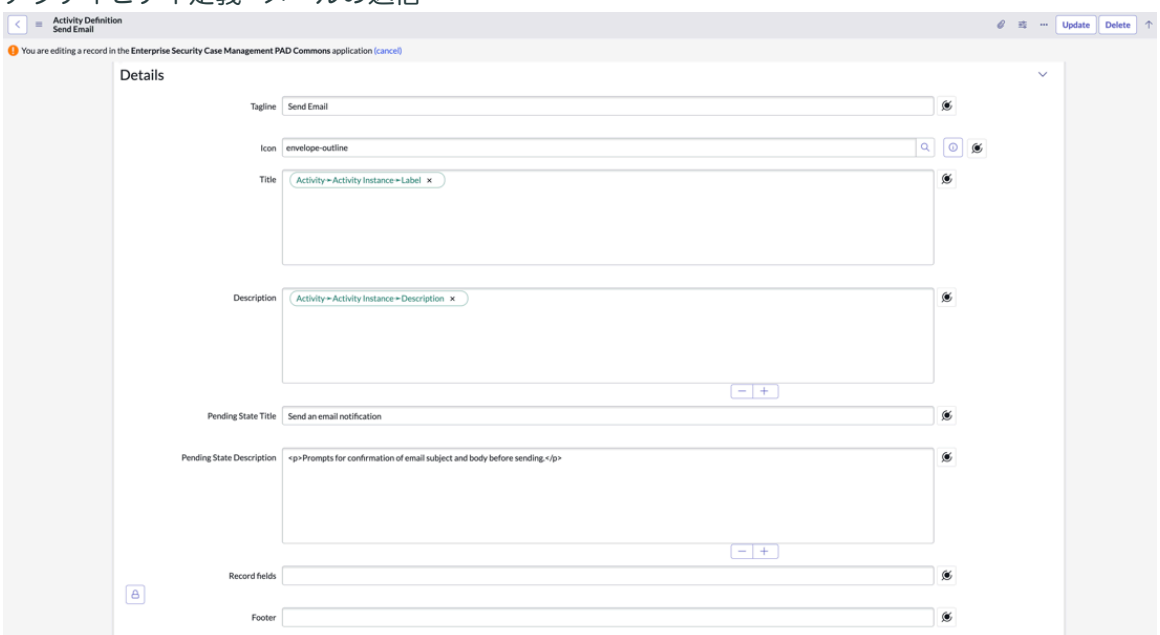
- キャッチコピー：メールを送信
- アイコン：封筒の形 (ユーザーインターフェイスには表示されません)
- タイトル： アクティビティ > アクティビティインスタンス > ラベル. ここではアクティビティインスタンスのラベルを選択しました。このドット連結は、実行時にタイトルとしてラベル値を動的に置き換えます。
- Description (説明)： アクティビティ > アクティビティインスタンス > 説明. ここではアクティビティインスタンスの説明を選択しました。このドット連結は、実行時にタイトルとしてラベル値を動的に置き換えます。
- 処理待ちステータスのタイトル：メール通知を送信します。これは、アクティビティが [処理待ち] ステータスの場合のタイトルです。
- 処理待ちステータスの説明：送信前にメールの件名と本文を確認するよう求めるプロンプト。ステータスが [処理待ち] の場合のアクティビティカードの説明。レコードフィールド：この例ではレコードフィールドが選択されています。

  [レコードフィールド] は、名前/値ペアのリスト内の関連レコードに表示されるフィールド名のカンマ区切りリスト。データはサーバーでプリフェッチされます。ドット連結がサポートされており、各フィールドで **[canRead()]** 権限が評価されます。

- フッター：この例ではフッターは定義されていません。

  フッターは、カードフッターの灰色の領域のテキストです。重要な情報を追加して表示できます。

アクティビティ定義 - メールの送信



自動翻訳

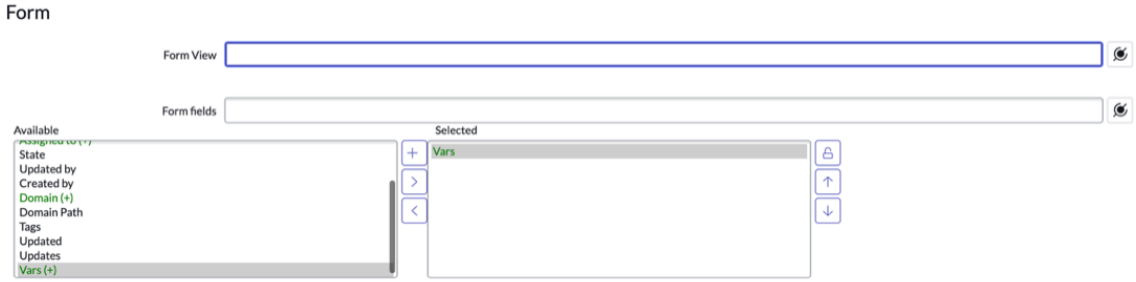
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フォーム

- フォームビュー：collect_data
- フォームフィールド：

この例では、collect_data ビューを使用して、ユーザーが入力する必要があるフィールドを表示します。collect_data ビューは、フローデータテーブルに対応するプラットフォーム提供のビューです。または、[フォームビュー] を空のままにして、[フォームフィールド] で使用可能な値のリストから [変数] を選択することもできます (ロックアイコンをクリックすると、使用可能な値のリストが開きます)。

フォームビュー



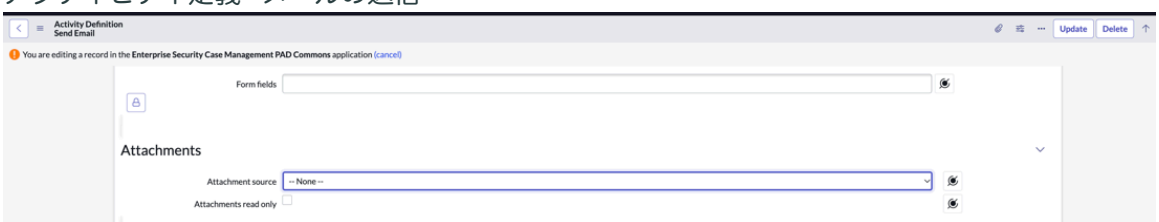
添付ファイル

この例では：

- [添付ファイルソース] が空です。
- [添付ファイルは読み取り専用] が選択されていません。

1. 添付ファイルソース：ドロップダウン。親レコードまたは関連レコードに添付するファイル、あるいは何も添付しないことをカードに表示します。
2. 添付ファイルは読み取り専用：True または False で指定します。ユーザーが既存の添付ファイルの名前を変更したり削除したりできないようにします。

アクティビティ定義 - メールの送信



特徴

この例では、次のようになります。

- SLA の表示 - クリア
- チェックリストの表示 - クリア
- 自動化 - クリア

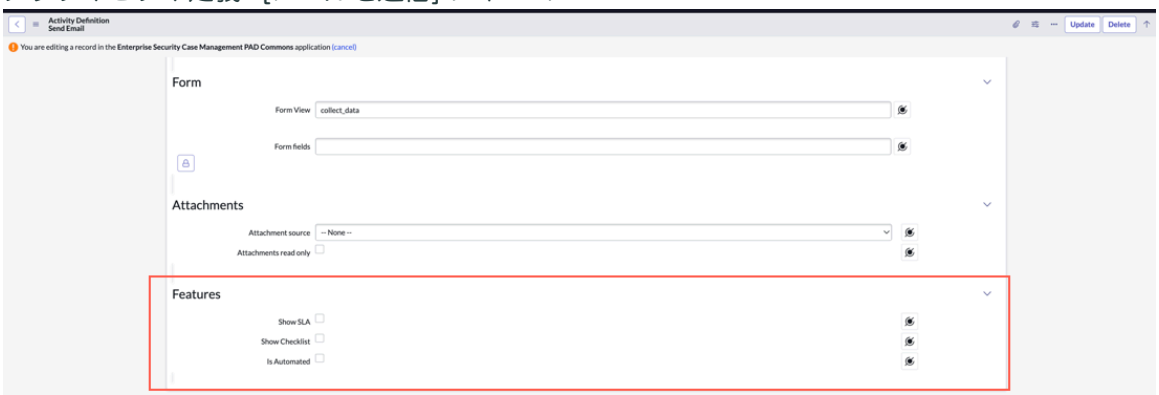
SLA の表示：True/False で指定します。関連レコードのカードのヘッダーに SLA タイマーを表示します。SLA は、プレイブック構成で指定された SLA 設定レコードに従って選択されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. チェックリストの表示：True または False で指定します。関連レコードに添付されているチェックリストを表示します。チェックリストは編集可能であり、変更は [宣言アクション] を必要とせずに保存されます。
2. 自動化：True または False で指定します。True の場合、**[tagline]** と [アイコン] は、「自動タスク」というテキストと自動アイコンで上書きされます。

アクティビティ定義 - [メールを送信] フォーム

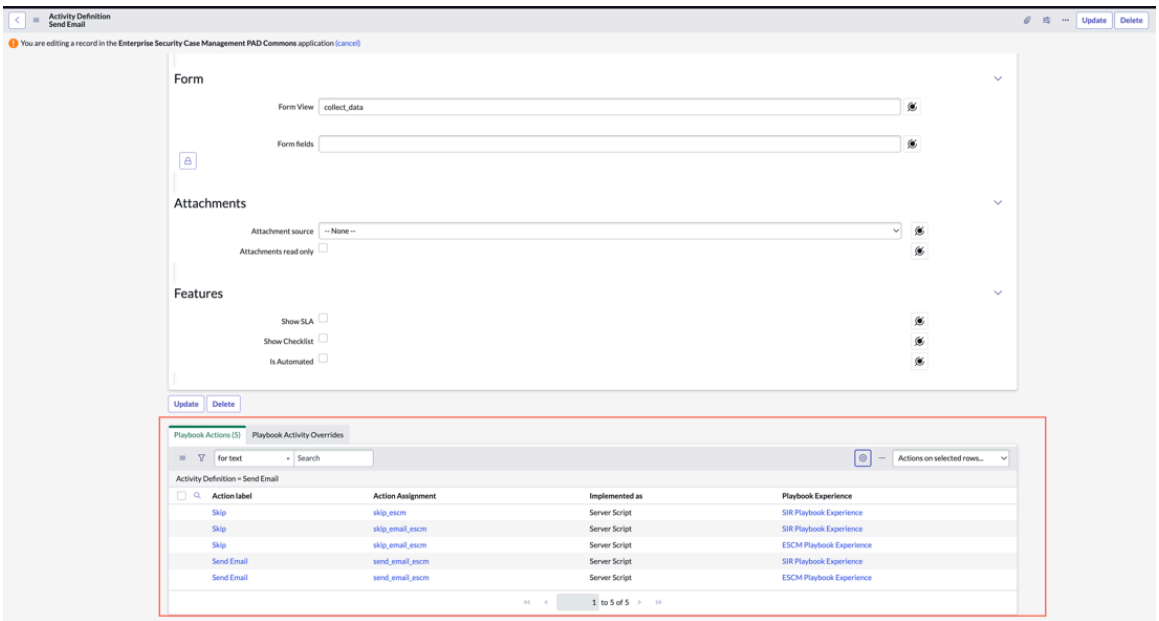


アクティビティ定義の プレイブックアクション

このセクションには、アクティビティカードに表示されるアクションがあります。この例では、アクションとして [スキップ]、[メールを送信] があります。

アクティビティカードに新しいアクションを追加するには、ページの下部にある [プレイブックアクション] 関連リストにレコードを作成する必要があります。

プレイブックアクション



1. [新規] をクリックします。
2. [アクションのアサイン] フィールドに対する既存のアクティビティアクションを選択します。
3. [プレイブックエクスペリエンス] フィールドに対して **[SIR** プレイブックエクスペリエンス] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

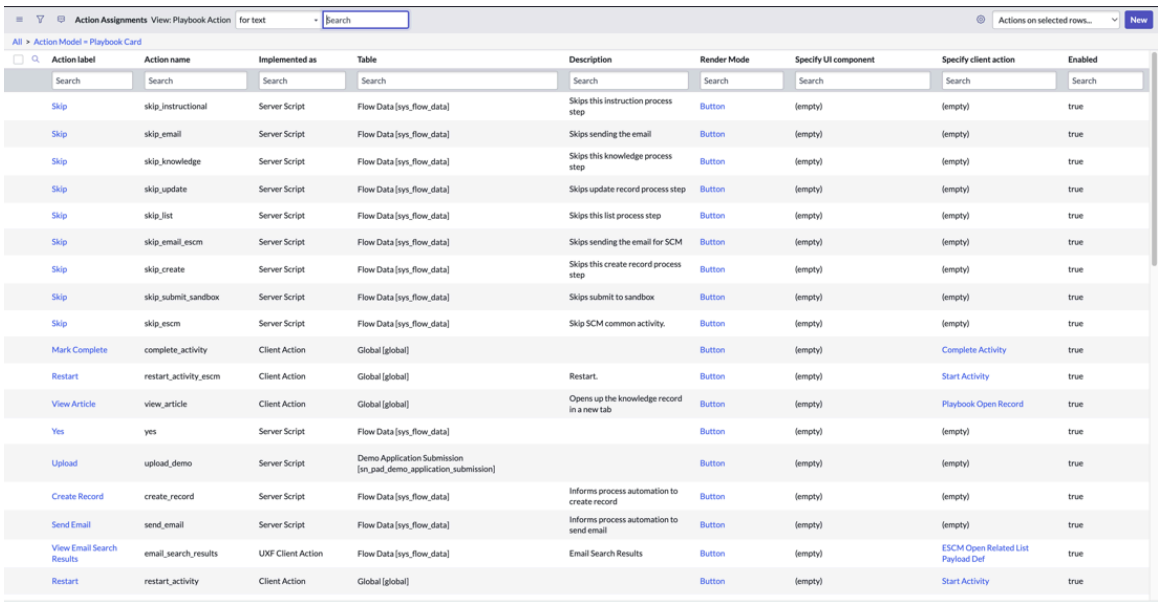
アクティビティアクションの作成

アクティビティアクションを作成する手順は次のとおりです。

始める前に
必要なロール：sn_si.admin

手順

1. 次のように移動する。 **All** (すべて) > プレイブックエクスペリエンス > **Actions** (アクション) > アクティビティアクション.



Action label	Action name	Implemented as	Table	Description	Render Mode	Specify UI component	Specify client action	Enabled
Skip	skip_instructional	Server Script	Flow Data [sys_flow_data]	Skips this instruction process step	Button	(empty)	(empty)	true
Skip	skip_email	Server Script	Flow Data [sys_flow_data]	Skips sending the email	Button	(empty)	(empty)	true
Skip	skip_knowledge	Server Script	Flow Data [sys_flow_data]	Skips this knowledge process step	Button	(empty)	(empty)	true
Skip	skip_update	Server Script	Flow Data [sys_flow_data]	Skips update record process step	Button	(empty)	(empty)	true
Skip	skip_list	Server Script	Flow Data [sys_flow_data]	Skips this list process step	Button	(empty)	(empty)	true
Skip	skip_email_escm	Server Script	Flow Data [sys_flow_data]	Skips sending the email for SCM	Button	(empty)	(empty)	true
Skip	skip_create	Server Script	Flow Data [sys_flow_data]	Skips this create record process step	Button	(empty)	(empty)	true
Skip	skip_submit_sandbox	Server Script	Flow Data [sys_flow_data]	Skips submit to sandbox	Button	(empty)	(empty)	true
Skip	skip_escm	Server Script	Flow Data [sys_flow_data]	Skip SCM common activity.	Button	(empty)	(empty)	true
Mark Complete	complete_activity	Client Action	Global [global]		Button	(empty)	Complete Activity	true
Restart	restart_activity_escm	Client Action	Global [global]	Restart.	Button	(empty)	Start Activity	true
View Article	view_article	Client Action	Global [global]	Opens up the knowledge record in a new tab	Button	(empty)	Playbook Open Record	true
Yes	yes	Server Script	Flow Data [sys_flow_data]		Button	(empty)	(empty)	true
Upload	upload_demo	Server Script	Demo Application Submission [sn_pad_demo_application_submission]		Button	(empty)	(empty)	true
Create Record	create_record	Server Script	Flow Data [sys_flow_data]	Informs process automation to create record	Button	(empty)	(empty)	true
Send Email	send_email	Server Script	Flow Data [sys_flow_data]	Informs process automation to send email	Button	(empty)	(empty)	true
View Email Search Results	email_search_results	UXF Client Action	Flow Data [sys_flow_data]	Email Search Results	Button	(empty)	ESCM Open Related List Payload Def	true
Restart	restart_activity	Client Action	Global [global]		Button	(empty)	Start Activity	true

2. [新規] をクリックします。

   これらのアクションの作成方法については、Now Platform のドキュメントを参照してください。この例では、[スキップ] はサーバースクリプトとして実装されています。

3. **Playbook** の上書き：**(Playbook override:)**

   既存のアクティビティエクスペリエンスタイプは上書きすることができます。詳細については、Now Platform のドキュメントを参照してください。この例ではプレイブックは上書きしません。

CSF X サンドボックスに送信

CSF X サンドボックスへの送信は、アクティビティ定義プロセスの一例です。

基本

基本的な詳細では、名前 (ラベル)、アプリケーション、説明、テーブル、およびアクセス可能なすべてのアプリケーションをキャプチャします。

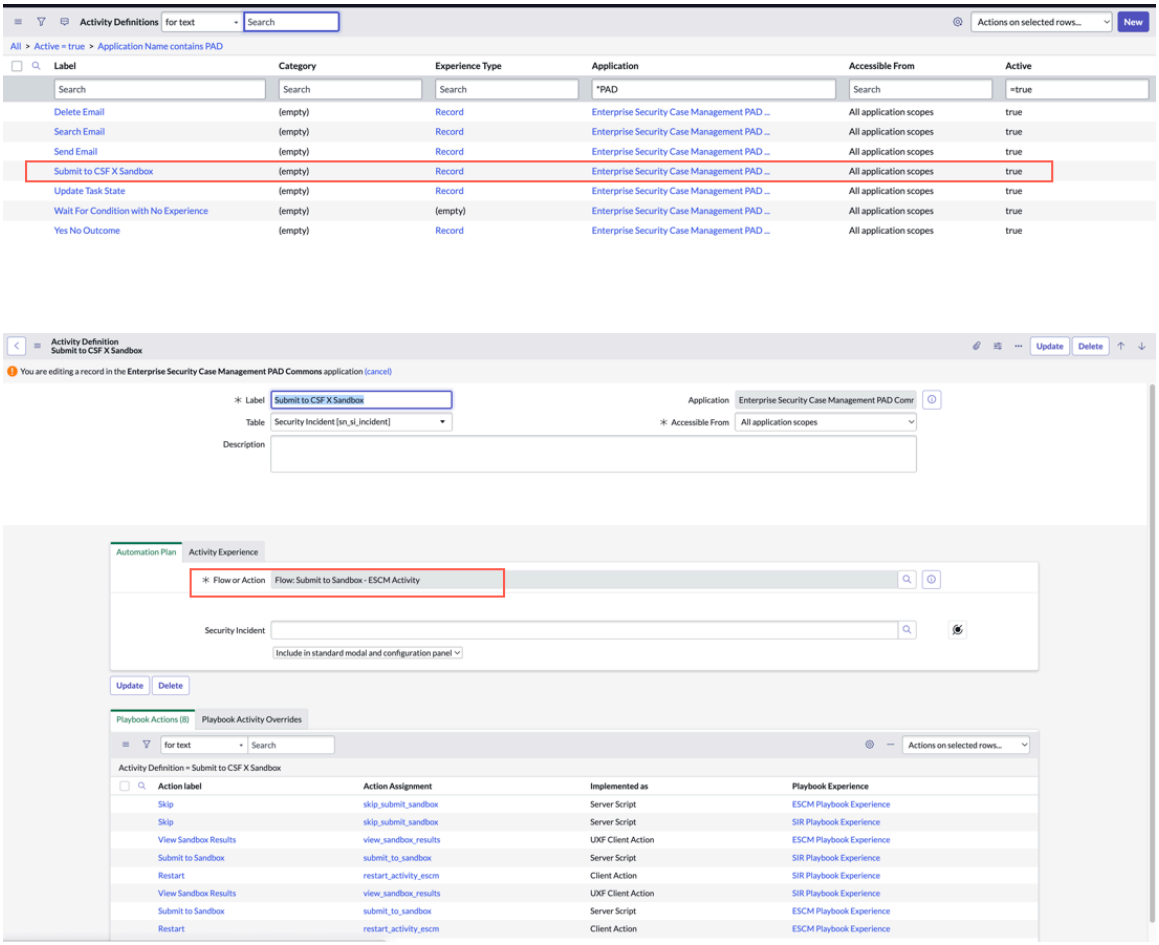
自動化プランとアクティビティエクスペリエンスを追加して送信します。送信後、ドキュメントを編集して各タブに詳細を追加します。

自動化プラン

自動化プランは、フローデザイナーを使用してビルドされたバックエンドアクションまたはサブフローを関連付けます。この例では、[サンドボックスに送信 **- ESCM** アクティビティ **(Submit to Sandbox - ESCM Activity)]** サブフローを使用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



このサブフローにより、悪意のある観測事象をサンドボックスに送信できます。すべての入力フィールドと出力フィールドが定義されています。

セキュリティインシデントは入力フィールドです。

アクティビティエクスペリエンス

この例では [レコード] タイプが選択されています。

関連レコード

関連レコードを使用して、現在のアクティビティに関連するデータを保存します。これにより、ランタイムデータとエクスペリエンスのステータスがキャプチャされます。

- 関連テーブル：フローデータ
- 関連レコード：VL
- エクスペリエンスステータステーブル：フローデータ
- エクスペリエンスステータスレコード：VL

詳細

- キャッチコピー：メールを送信
- アイコン：封筒の形
- タイトル： アクティビティ > アクティビティインスタンス > ラベル. ここではアクティビティインスタンスのラベルを選択しました。このドット連結は、実行時にタイトルとしてラベル値を動的に置き換えます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 説明：VL (サブフロー出力がマッピングされています)
- 処理待ちステータスのタイトル：空
- 処理待ちステータスの説明：空
- レコードフィールド
- フッター

フォーム

- フォームビュー：空
- フォームフィールド：空

添付ファイル

この例では：

- 添付ファイルソース - なし
- 添付ファイルは読み取り専用 - オフ

1. 添付ファイルソース：ドロップダウン。親レコードまたは関連レコードに添付するファイル、あるいは何も添付しないことをカードに表示します。
2. 添付ファイルは読み取り専用：True または False で指定します。ユーザーが既存の添付ファイルの名前を変更したり削除したりできないようにします。

特徴

この例では、次のようになります。

- SLA の表示 - オフ
- チェックリストの表示 - オフ
- 自動化 - オフ

アクティビティ定義の プレイブックアクション

このセクションには、アクティビティカードに表示されるアクションがあります。

この例には、[スキップ]、[サンドボックスの結果を表示 (View Sandbox Results)]、[サンドボックスに送信]、および [やり直し] の各アクションがあります。

アクティビティカードに新しいアクションを追加するには、ページの下部にある [プレイブックアクション] 関連リストに新しいレコードを作成する必要があります。

プレイブックの上書き

この例ではプレイブックは上書きしません。

SIR ワークスペースのサンプルプレイブック

複雑なコードを記述することなく、SIR ワークスペースのプレイブックを迅速かつ簡単に作成または構成できます。これらのプレイブックを使用して、ステップバイステップ方式でセキュリティ脅威を解決できます。セキュリティインシデントのプレイブックフローを自動または手動で呼び出すことができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンスは、ベースシステムで次のプレイブックを提供します。

- 手動フィッシング用プレイブック
- 自動フィッシングプレイブック
- 手動マルウェアプレイブック
- 自動マルウェアプレイブック
- ログイン失敗手動プレイブック

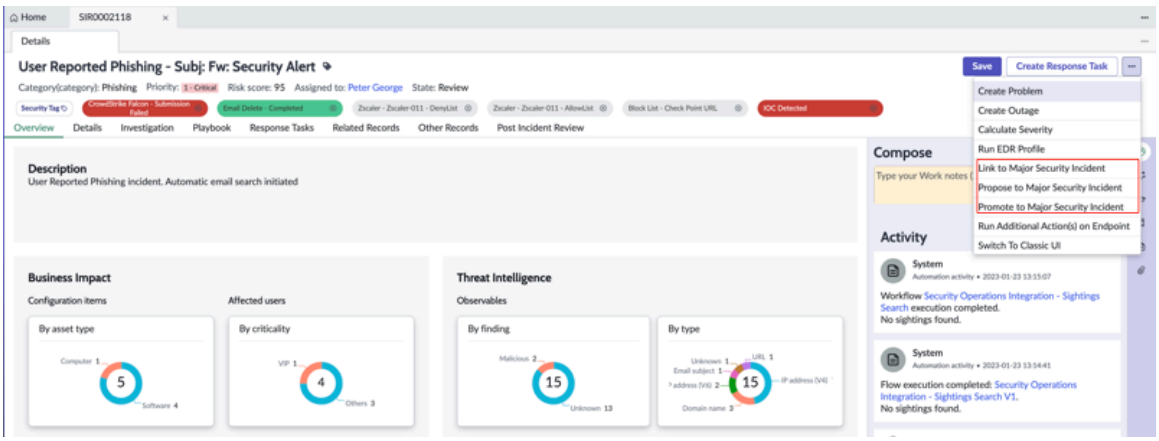
MSI レコードの使用

セキュリティインシデントレスポンスワークスペースを使用すると、インシデントが組織に対する重大な脅威として識別された場合に、セキュリティインシデントを重大なセキュリティインシデントとして提案、昇格、またはリンクすることができます。

重大セキュリティインシデント管理 (MSIM) を Now Platform インスタンスにインストールすると、セキュリティインシデントから重大なインシデントへの移行を処理できます。

重大セキュリティインシデント管理 (MSIM) UI アクションは、SIR ワークスペースのセキュリティインシデントフォームバナーの右上に表示されます。必要に応じて UI アクションを選択します。

注:
一部のアクションはコンテキストに依存します。たとえば、[リンクを解除] アクションは、セキュリティインシデントが既に提案または昇格されている場合、または重大なセキュリティインシデントにリンクされている場合にのみ使用できます。



重大なセキュリティインシデントとして提案

重大なセキュリティインシデント (MSI) としてセキュリティインシデントを提案します。

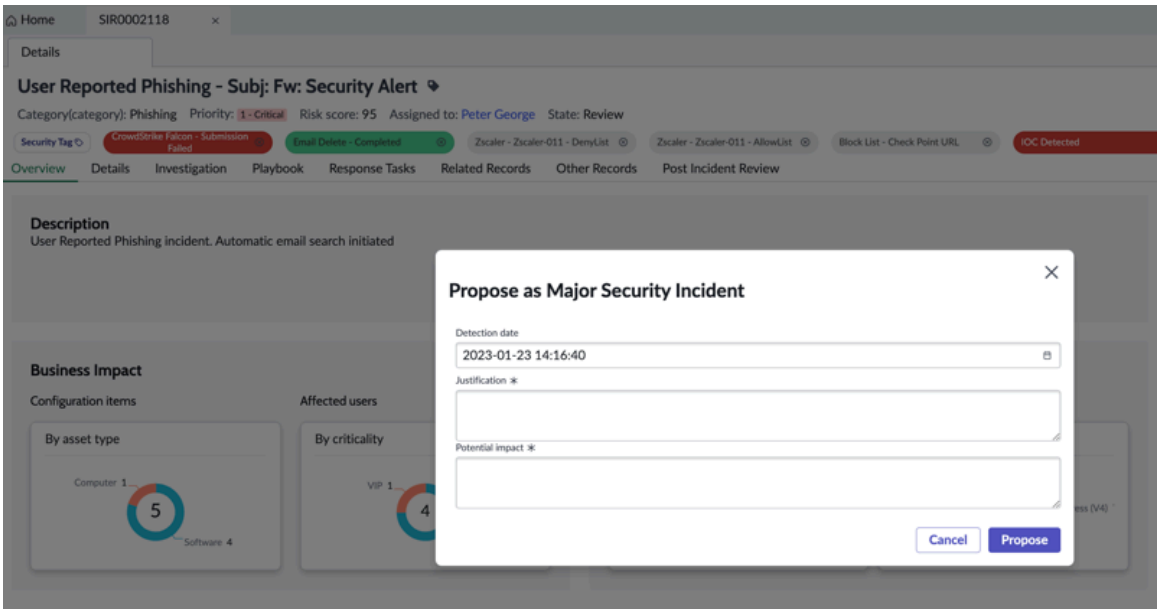
始める前に

必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. 任意のセキュリティインシデントを開きます。
3. [重大なセキュリティインシデントに提案 **(Propose to Major Security Incident)**] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. フォームで、[検出日]、[正当性]、[潜在的な影響] などのフィールドに入力します。
5. [提案] をクリックします。
   インシデントレコードが重大なセキュリティインシデント候補として提案されます。
   インシデントレコードが重大なセキュリティインシデント候補として提案されると、[重大なセキュリティインシデント候補 **(Major Security Incident Candidate)]** タグが適用され、セキュリティインシデントフォームのバナーに表示されます。

   注:
   インシデントを提案しない場合、または重大な影響がない場合は、[重大なセキュリティインシデントからリンク解除] をクリックします。インシデントはリンク解除され、是正のためセキュリティアナリストに表示されます。

重大なセキュリティインシデントに昇格

セキュリティインシデントを重大なセキュリティインシデントに昇格します。

始める前に

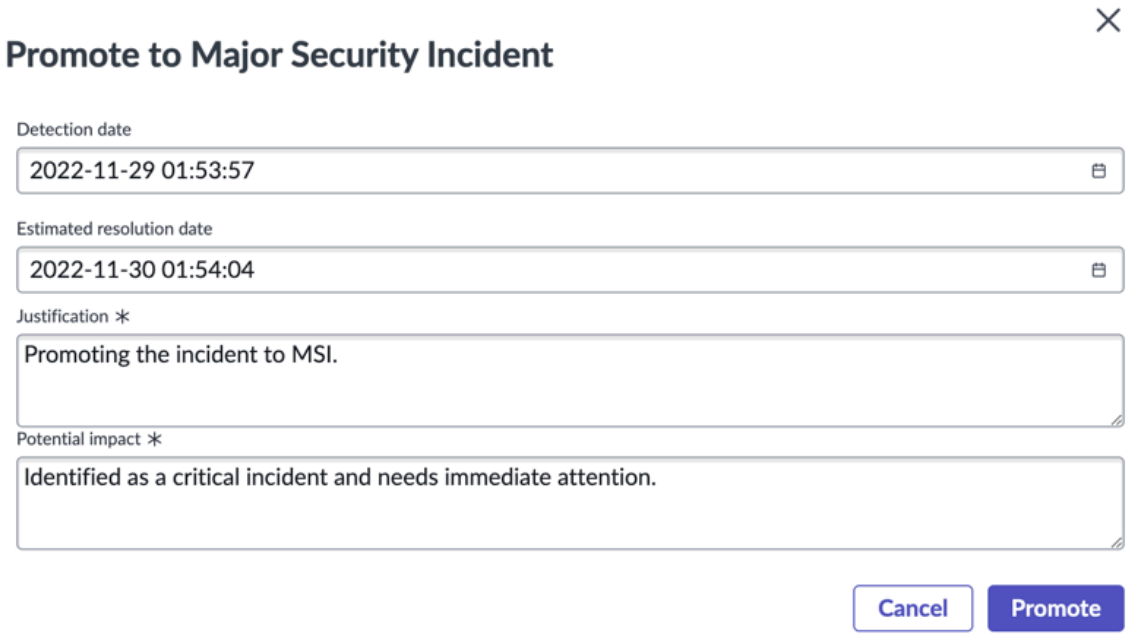
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. 任意のセキュリティインシデントを開きます。
3. [重大なセキュリティインシデントに昇格] をクリックします。
4. フォームで、[検出日]、[推定解決日]、[正当性]、[潜在的な影響] などのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. [昇格] をクリックします。
   インシデントレコードが重大なセキュリティインシデントとして昇格されます。
   インシデントレコードが重大なセキュリティインシデントとして提案されると、[重大なセキュリティインシデント] タグが適用され、フォームのバナーに表示されます。

   注:
   そのインシデントが重大でない場合は、重大なインシデントのリンクを解除することもできます。その場合、インシデントはリンク解除され、セキュリティアナリストが是正するリストビューに表示されます。

自動翻訳

重大なセキュリティインシデントへのリンク

セキュリティインシデントを子セキュリティインシデントとして重大なセキュリティインシデントにリンクします。

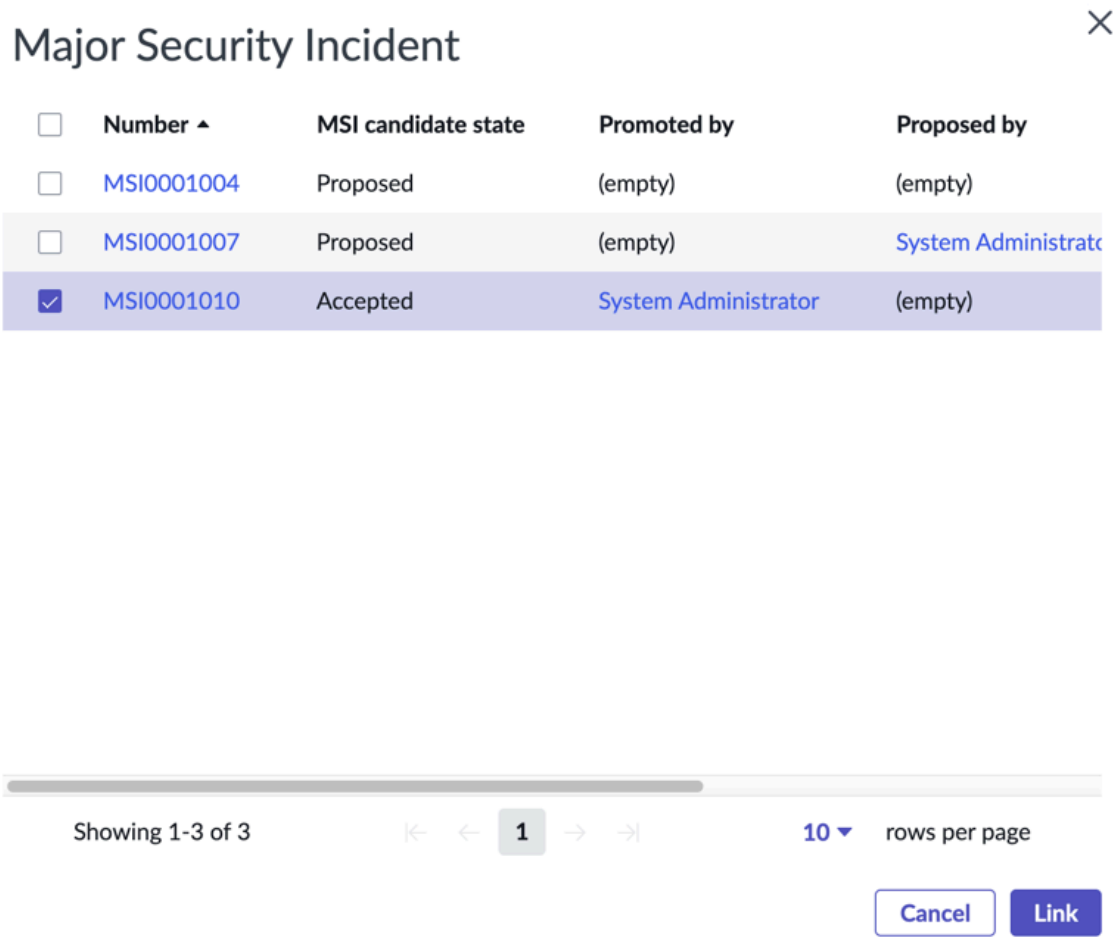
始める前に

必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. 任意のセキュリティインシデントを開きます。
3. [重大なセキュリティインシデントへのリンク] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. 重大なセキュリティインシデントにリンクするインシデントを選択します。
5. [リンク **(Link)]** をクリックします。
6. インシデントレコードが重大なセキュリティインシデントの子インシデントとしてリンクされます。
   インシデントが重大なセキュリティインシデントの子インシデントとしてリンクされると、[重大なセキュリティインシデント] タグが適用され、フォームのバナーに表示されます。

フォーム **UI** アクションの操作

セキュリティインシデントフォームに表示される UI アクションは次のとおりです。

フォーム UI アクションに移動するには：

1. 検索項目 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. リストビューから任意のセキュリティインシデントを選択します。
3. UI アクションはすべてセキュリティインシデントフォームの右上隅にあります。

ワークスペースフォーム **UI** アクション

フィールド名	説明
ディスカッション	セキュリティインシデントに関するサイドバーディスカッションを作成または開始します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド名	説明
保存	変更を加えた後、[セキュリティインシデントレスポンス] レコードを保存または更新します。
対応タスクを作成	セキュリティインシデントの応答タスクを作成します。
メールの作成	セキュリティインシデントのメールを作成します。
プレイブックを追加	セキュリティインシデントのプレイブックを手動で追加します。
インシデントを作成	セキュリティインシデント内にインシデントを作成します。
カスタマーサービスケースを作成	カスタマーサービス管理 (CSM) チームが追跡するセキュリティインシデントのカスタマーサービスケースを作成します。 **注:** このオプションは、カスタマーサービス管理 (CSM) がインストールされている場合にのみ使用できます。
関連ワークフローを開く	セキュリティインシデントに関連付けられている任意のワークフローコンテキストを開きます。このオプションは、ワークフローがある場合にのみ表示されます。
変更要求の作成	セキュリティインシデント内に変更要求を作成します。
問題を作成	セキュリティインシデント内に問題を作成します。
機能停止の作成	セキュリティインシデント内に機能停止を作成します。
重大度の計算	事前定義された計算機を使用して、セキュリティインシデントの重大度を計算します。重大度は、計算機の事前定義されたルールに基づいて計算されます。インシデントの重大度は、[リスクスコア]、[ビジネスインパクト]、および [優先度] に基づいています。
EDR プロファイルを実行	必要な統合の EDR プロファイルを選択して実行します。 **注:** このオプションは、任意の統合がインストールされている場合にのみ使用できます。
重大なセキュリティインシデントへのリンク	セキュリティインシデントを重大なセキュリティインシデントにリンクさせます。
リスクイベントを報告	このセキュリティインシデントをリスクイベントとしてリスク管理チームに報告します。リスク管理チームはイベントを分析し、そのようなイベントと関連する損失が再発しないようにします。 **注:** このオプションは、リスク管理がインストールされている場合にのみ使用できます。
重大なセキュリティインシデントからリンク解除	重大なセキュリティインシデントからリンク解除します。
重大なセキュリティインシデントとして提案	重大なセキュリティインシデントとしてセキュリティインシデントを提案します。

自動翻訳

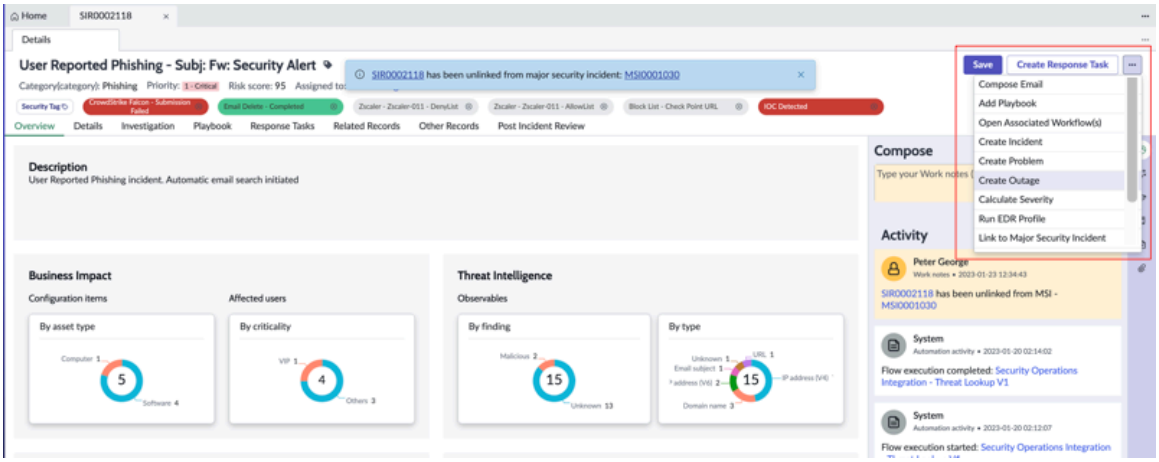
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド名	説明
重大なセキュリティインシデントに昇格	セキュリティインシデントを重大なセキュリティインシデントとして昇格させます。
エンドポイントで他のアクションを実行	エンドポイントで他のアクションを実行します。 **注:** このオプションは、エンドポイント統合がインストールされている場合にのみ使用できます。例：FireEye HX
MISP で新しいイベントを作成	MISP でイベントを自動または手動で作成および変更します。 **注:** このオプションは、MISP 統合がインストールされている場合にのみ使用できます。
関連 **MITRE ATT&CK** テクニック	MITRE ATT&CK テクニックをセキュリティインシデントに関連付けます。 **注:** このオプションは、ATT&CK がインストールされている場合にのみ使用できます。
MITRE ATT&CK 情報	セキュリティインシデントに関連付けられた MITRE ATT&CK 情報を表示します。 **注:** このオプションは、ATT&CK がインストールされている場合にのみ使用できます。
セキュリティケースに追加	既存または新規のセキュリティケースにセキュリティインシデントを追加します。 **注:** このオプションは、Threat Intel がインストールされている場合にのみ使用できます。
以前の **UI** に切り替え	アナリストが従来の UI と新しい UI を切り替えて、新しいワークスペースでまだ利用できない既存の機能を操作できるようにします。
キャンセル	セキュリティインシデントをキャンセルします。[キャンセル] を選択した後、応答タスクや子セキュリティインシデントなどの関連レコードもすべてキャンセルされます。
削除	セキュリティインシデントレコードを削除します。

4. セキュリティインシデントレコードを表示するには、セキュリティインシデント番号をクリックします。UI アクションはページの上部に表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



セキュリティインシデントのクローズワークフロー

インシデント状況を更新して、セキュリティインシデントをクローズします。

始める前に
必要なロール：sn_si.analyst

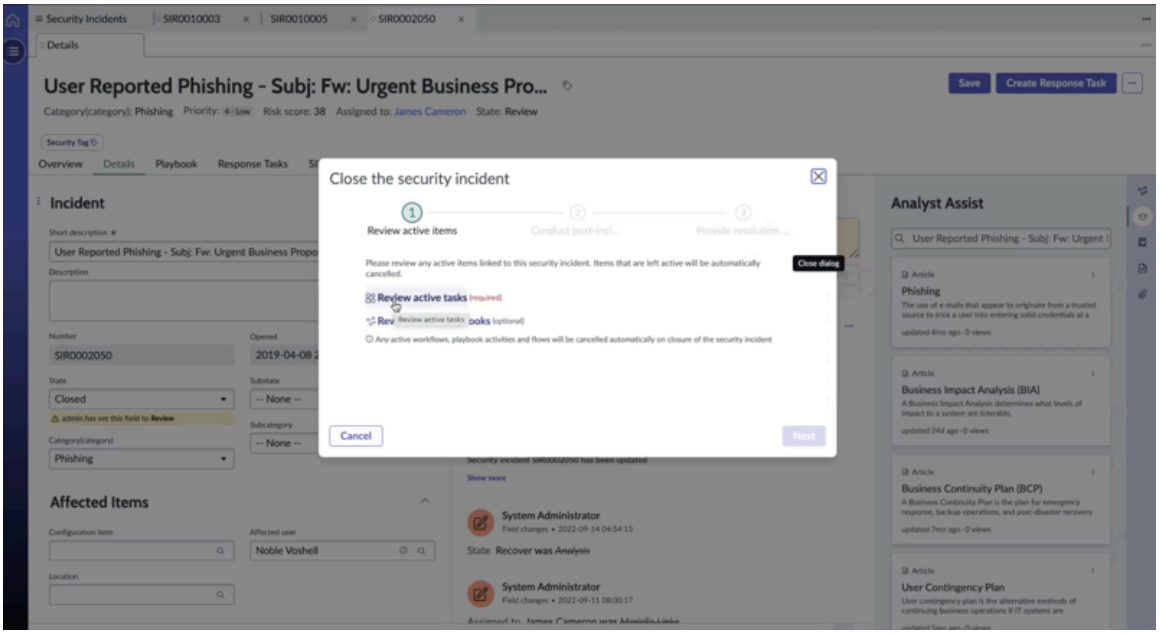
手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. たとえば、 **Lists** (リスト) > セキュリティインシデント > オープン中のインシデント.
3. クローズするインシデントを開きます。
4. [詳細] タブに移動します。
5. インシデント状況にドリルダウンし、[クローズ] を選択します。
6. クローズ処理を実行します。
   - これは、セキュリティインシデントをクローズする前にタスクをレビューする必須のステップです。応答タスクは、セキュリティインシデントとしてクローズする前に、アナリストがレビューし、クローズまたはキャンセルする必要があります。アナリストが [アクティブなタスクをレビュー] をクリックすると、[応答タスク] タブに移動します。セキュリティインシデントをクローズ中であることを示すセッションメッセージが表示されます。[続行] をクリックします。
   - [続行] をクリックします。最初のステップである、セキュリティインシデントのクローズにおけるアクティブなタスクのレビューが完了しました。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

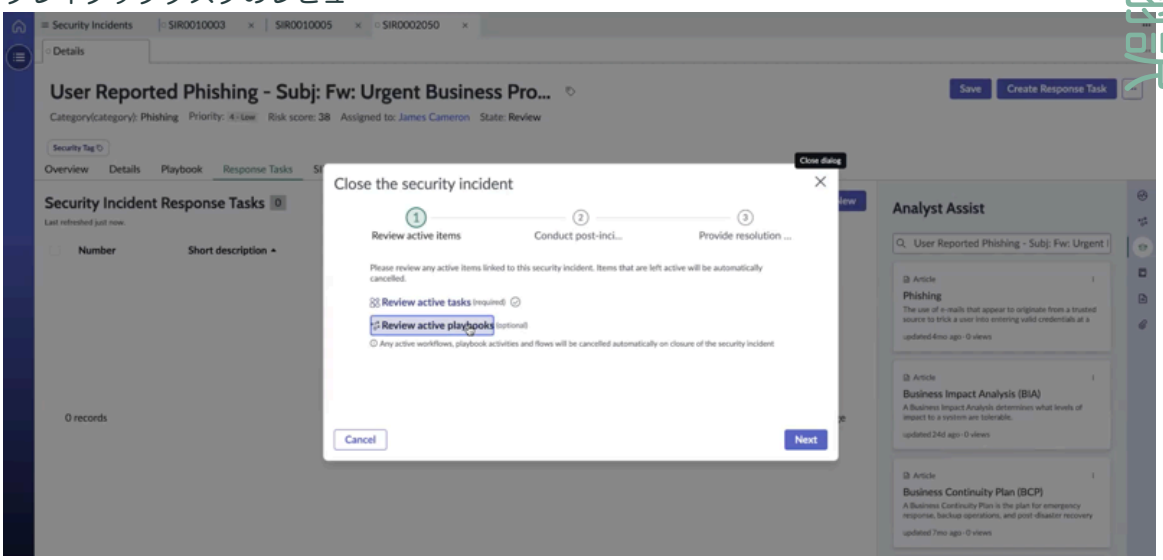
クローズタスクのレビュー



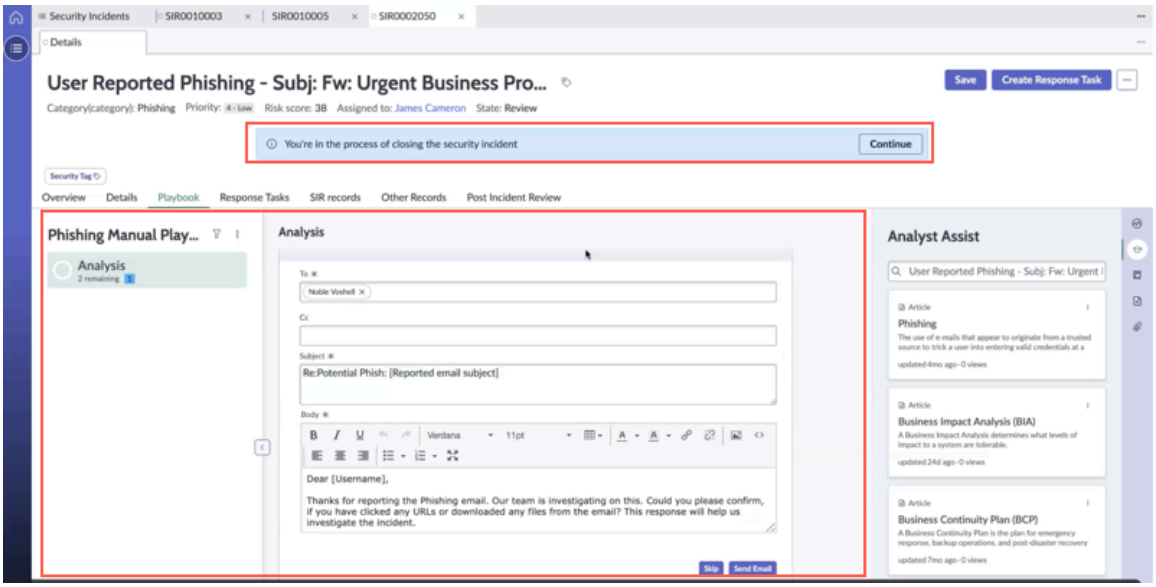
- 必要に応じて、次のステップでアナリストがレビューするアクティブなプレイブックを確認します。リンクをクリックすることで、アクティブなプレイブックタスクをレビューし、必要に応じてクローズできます。

  注:
  アクティブなワークフロー、プレイブックアクティビティ、およびフローは、セキュリティインシデントのクローズ時に自動的にキャンセルされます。

  プレイブックタスクのレビュー

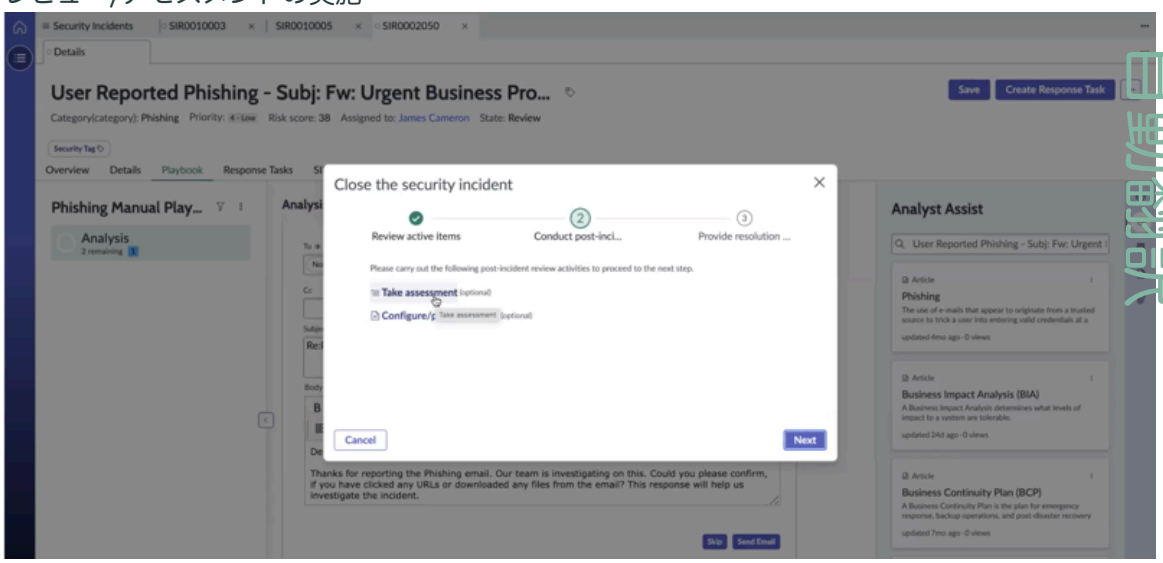


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

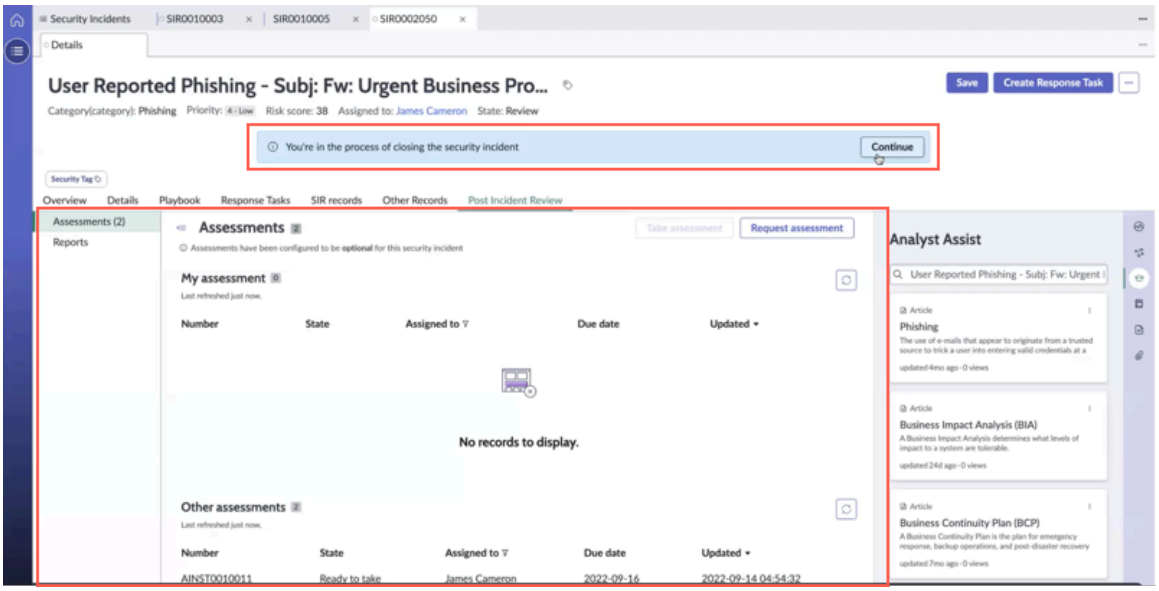


- インシデントの事後レビューレポート：続いてインシデントの事後アクティビティをレビューし、クローズを続行します。アセスメントがオプションの場合はステップをスキップし、アセスメントが必須の場合はアセスメントを実施して完了します。

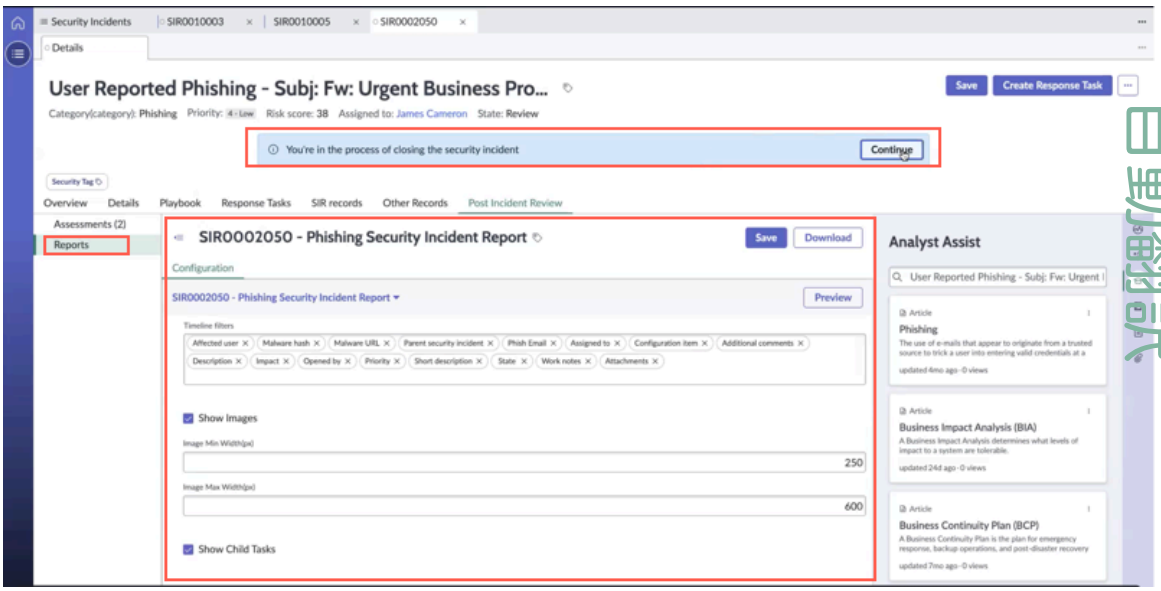
レビュー/アセスメントの実施



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



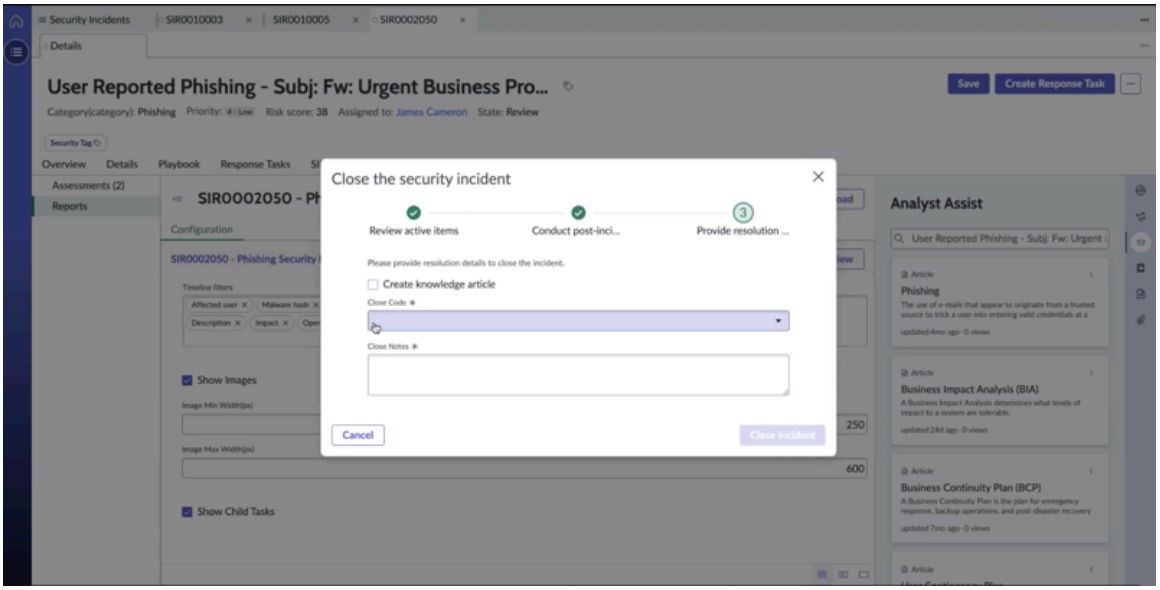
- レポートの設定/プレビュー：これもオプションのステップです。リンクをクリックしてレポートを確認し、[次へ] と進みます。



- 解決策の詳細を入力 (Provide Resolution details)：アナリストは、チェックボックスをオンにしてナレッジ記事を自動的に作成できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [クローズコード] と [クローズメモ] を入力し、[インシデントのクローズ] をクリックします。



注:
アナリストが [セキュリティインシデントをクローズ] ダイアログボックスをキャンセルした場合、アナリストは [詳細] タブに移動し、インシデント状況を [クローズ] に変更することができます。

SIR ワークスペースダッシュボードの表示

このセクションには、新しいセキュリティインシデントやオープンセキュリティインシデントの平均経過時間など、セキュリティインシデントレスポンス プロセスを分析する上で重要なメトリクスが表示されます。

クラシック UI では、ホームページで利用可能ないくつかの標準ダッシュボードと、パフォーマンスアナリティクス for セキュリティインシデントレスポンス プラグインがインストールされている場合に利用可能な パフォーマンスアナリティクス ダッシュボードがあります。これらはすべて、**[SIR ダッシュボード]** セクションの新しいワークスペースで利用できるようになりました。

ホームページの標準ダッシュボード：

- セキュリティインシデントレスポンス概要
  - アナリストの概要
  - マネージャーの概要 (今後のリリースでサポート)
  - CISO の概要 (今後のリリースでサポート)
- セキュリティインシデントレスポンス のプラットフォームアナリティクス
  - Security Incident Explorer
  - CISO ダッシュボード (今後リリース予定)
  - Major Security Incident
  - セキュリティインシデント管理プレミアム版 KPI
  - Security Operations 効率
  - コンテキスト依存アナリティクス - SI ダッシュボード

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
CISO ダッシュボードなどのセキュリティインシデントレスポンスダッシュボードには、標準およびプラットフォームアナリティクス間にダッシュボードの繰り返しが存在する可能性があります。プラグインがインストールされると、これらのダッシュボードにコンテンツが追加され、重複して使用できなくなります。

セキュリティインシデントレスポンスダッシュボードをワークスペースに表示させるには、ユーザーは [プラットフォームアナリティクス] の下にリストされているダッシュボードのプラグインをインストールする必要があります。これを行わない場合、標準のダッシュボードしか使用できません。

SIR ワークスペース の現在のバージョンでは、**[SIR** ダッシュボード] セクションで次のダッシュボードを利用できます。ここに記載していない他のダッシュボードは、今後のリリースで利用できるようになります。

セキュリティインシデントレスポンスダッシュボード

ダッシュボード	説明
標準ダッシュボード	
セキュリティアナリスト概要	セキュリティアナリストは、このダッシュボードを使用して、アナリストの重要な優先度の作業、優先度の高い作業、アナリストにアサインされたセキュリティインシデント、アナリストにアサインされたタスク、およびインシデント数に基づいて要約されたセキュリティインシデントを表示できます。
セキュリティインシデント対応のパフォーマンスアナリティクス (PA) ダッシュボード	
Security Incident Explorer	セキュリティマネージャーおよびアナリストは、このダッシュボードを使用して、カテゴリ、サブカテゴリ、場所、優先度、およびビジネスインパクト別に集計されグループ化されたセキュリティインシデントを表示できます。これらのビューにより、マネージャーおよびアナリストは、攻撃の発生頻度と影響を受けるビジネスサービスをすばやく把握できます。
重大セキュリティインシデント	セキュリティマネージャーは、このダッシュボードを使用して、初期分析/検出から封じ込め、除去、復旧までのセキュリティインシデントのボリューム、パフォーマンス、および進捗状況を簡単に追跡できます。
CISO ダッシュボード	将来のリリースでのサポートが提案されています。
Security Operations 効率	マネージャーおよびアナリストは、このダッシュボードを使用して全体的な効率メトリクスを表示し、SOC のパフォーマンスを測定できます。
セキュリティインシデント管理プレミアム KPI	セキュリティマネージャーは、このダッシュボードを使用して、初期分析/検出から封じ込め、除去、復旧までのセキュリティインシデントのボリューム、パフォーマンス、および進捗状況を追跡して表示できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンスダッシュボード (続く)

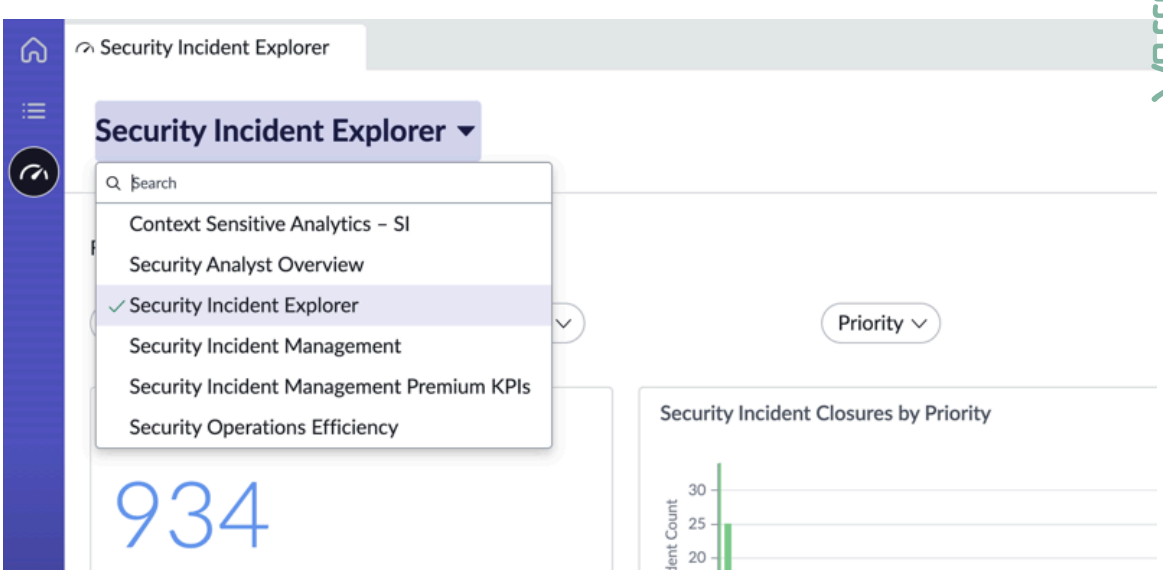
ダッシュボード	説明
コンテキスト依存アナリティクス - S	マネージャーとアナリストは、このダッシュボードを使用して、オープンセキュリティインシデント、オープンセキュリティインシデントの平均経過時間、セキュリティインシデントの平均クローズ所要時間、同じ日にオープンされてクローズされたセキュリティインシデントの割合、過去 5 日間および 30 日間更新されていないインシデントの割合を表示できます。

SIR および PA ダッシュボードへのアクセス

ワークスペースのホームページの左側に **[SIR** ダッシュボード] アイコンが表示されます。

> **注:**
> sn_si.manager または sn_si.admin のアクセス権を持つユーザーは、ダッシュボードを編集できます。ユーザーは、ユーザーが編集しようとしているダッシュボードと同じスコープ内に存在する必要があります。たとえば、[セキュリティアナリスト概要] ダッシュボードが SIR ワークスペースで利用可能な場合、ダッシュボードを編集するにはユーザーが同じ SIR ワークスペースのスコープ内にいる必要があります。

1. 次のように移動する。 ワークスペース > セキュリティインシデント管理ワークスペース.
2. **[SIR** ダッシュボード] アイコンをクリックします。
3. ドロップダウンリストから目的のダッシュボードを選択します。



ダッシュボードを編集したり、ダッシュボードに新しい要素を追加したり、独自のダッシュボードを作成したりすることができます。ダッシュボードの使用方法については、「レスポンシブダッシュボードの操作」を参照してください。

セキュリティアナリスト概要ダッシュボードの表示

セキュリティアナリストは、このダッシュボードを使用して、アナリストの重要な優先度の作業、優先度の高い作業、アナリストにアサインされたセキュリティインシデント、アナリストにアサインされたタスク、およびインシデント数に基づいて要約されたセキュリティインシデントを表示できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

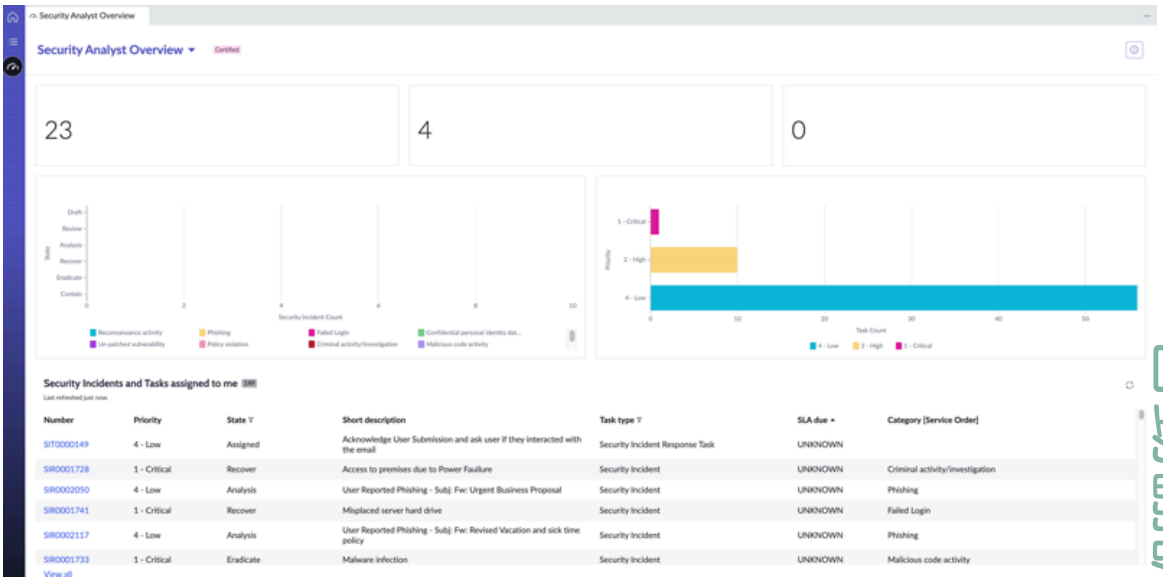
自動翻訳

始める前に
デフォルトでは、[セキュリティアナリスト概要] ダッシュボードは sn_si.analyst アクセス権を持つユーザーに対して表示されます。

必要なロール：sn_si.analyst (読み取り)、sn_si.manager または sn_si.admin (書き込み)

手順

1. 次のように移動する。 ワークスペース > **Security Incident Response** (セキュリティインシデントレスポンス).
2. ワークスペースのホームページの左側に表示された **[SIR** ダッシュボード] アイコンをクリックします。
3. ドロップダウンリストから [セキュリティアナリスト概要] を選択します。



さらに他の操作を行う場合は [セキュリティアナリスト概要] ダッシュボードを表示します。セキュリティアナリスト概要ダッシュボードの詳細については、「セキュリティインシデントレスポンス プラットフォームアナリティクスソリューション」を参照してください。

Security Incident Explorer ダッシュボードの表示

セキュリティマネージャーは、このダッシュボードを使用して、カテゴリ、サブカテゴリ、場所、優先度、およびビジネスインパクト別に集計されグループ化されたセキュリティインシデントを表示できます。

始める前に
デフォルトでは、[Security Incident Explorer] ダッシュボードは sn_si.manager アクセス権を持つユーザーに対して表示されます。

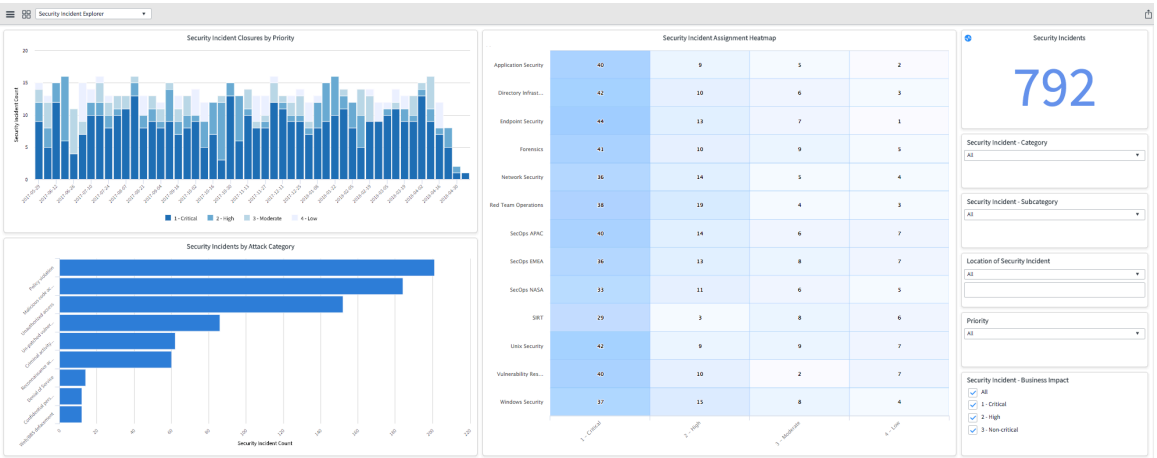
必要なロール：sn_si.analyst (読み取り)、sn_si.manager または sn_si.admin (書き込み)

手順

1. 次のように移動する。 ワークスペース > **Security Incident Response** (セキュリティインシデントレスポンス).
2. ワークスペースのホームページの左側に表示された **[SIR** ダッシュボード] アイコンをクリックします。
3. ドロップダウンリストから **[Security Incident Explorer]** を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



さらに他の操作を行う場合は [Security Incident Explorer] ダッシュボードを表示します。Security Incident Explorer ダッシュボードの詳細については、「Security Incident Explorer dashboard ダッシュボード」を参照してください。

現在のリリースでは、次のレポートのリストは [Security Incident Explorer] ダッシュボードでサポートされていません。

- セキュリティインシデントアサインヒートマップ (Security Incident Assignment HeatMap)：ヒートマップによるビジュアル化は利用できません。
- セキュリティインシデントマップ (Security Incident Map)：マップによるビジュアル化は利用できません。

Major Security Incident ダッシュボードの表示

セキュリティマネージャーは、このダッシュボードを使用して、初期分析/検出から封じ込め、除去、復旧までのセキュリティインシデントのボリューム、パフォーマンス、および進捗状況を簡単に追跡できます。

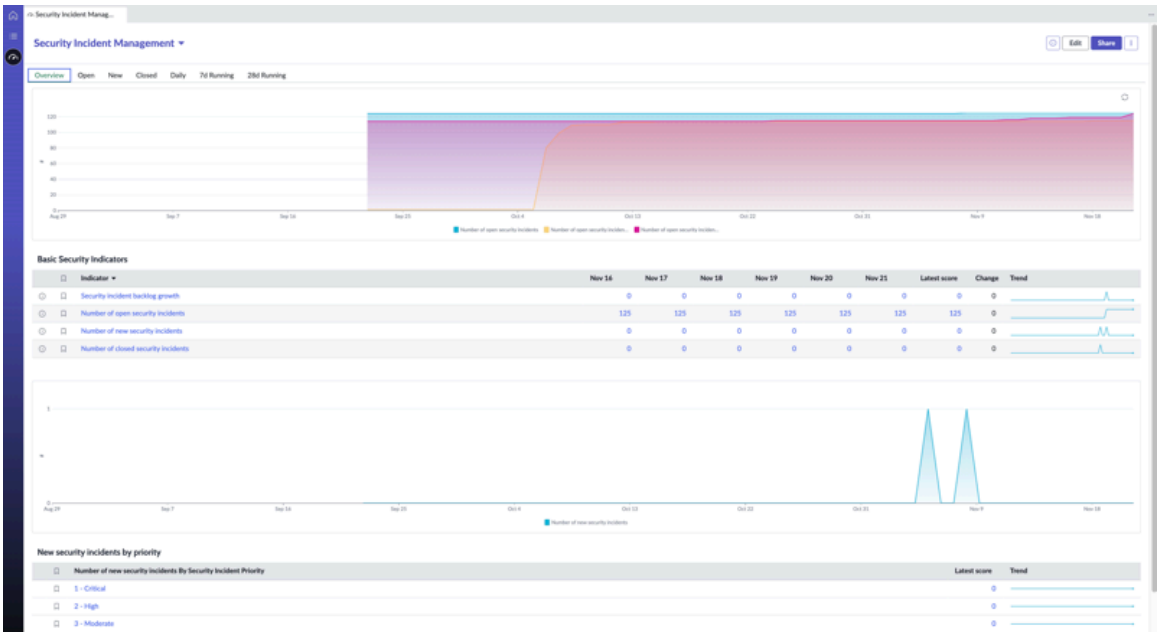
始める前に
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > **Security Incident Response** (セキュリティインシデントレスポンス).
2. ワークスペースのホームページの左側に表示された **[SIR** ダッシュボード] アイコンをクリックします。
3. ドロップダウンリストから [重大セキュリティインシデント] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



さらに他の操作を行う場合は [セキュリティインシデント管理] ダッシュボードを表示します。セキュリティインシデント管理 ッシュボードの詳細については、「セキュリティインシデント管理ダッシュボード」を参照してください。

Security Operations 効率ダッシュボードの表示

Security Operations Center (SOC) のマネージャーは、全体的な効率メトリクスを表示し、組織内の SOC チームメンバーの個々のパフォーマンスを測定できます。

始める前に

現在のリリースでは、次のレポートのリストは [Security Operations 効率] ダッシュボードでサポートされていません。

- セキュリティインシデントステージ分析：ワークベンチは利用できません。

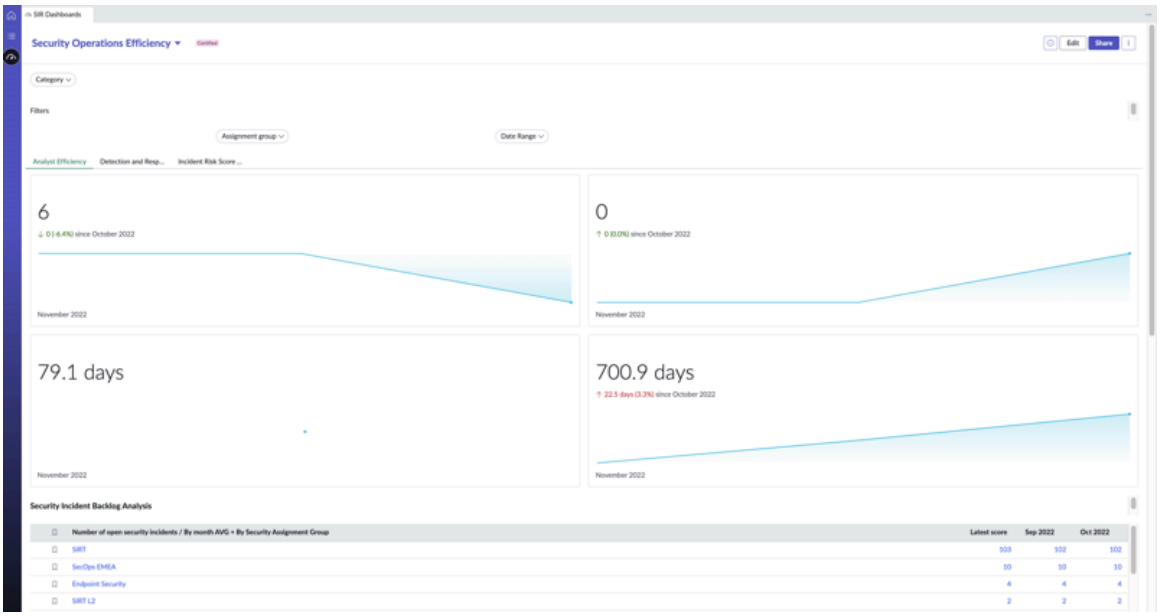
必要なロール：sn_si.analyst (読み取り)、sn_si.manager または sn_si.admin (書き込み)

手順

1. 次のように移動する。 ワークスペース > **Security Incident Response** (セキュリティインシデントレスポンス).
2. ワークスペースのホームページの左側に表示された **[SIR** ダッシュボード] アイコンをクリックします。
3. ドロップダウンリストから **[Security Operations** 効率] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



さらに他の操作を行う場合は [Security Operations 効率] ダッシュボードを表示します。[Security Operations 効率] ダッシュボードの詳細については、「Security Operations Efficiency dashboard (Security Operations 効率ダッシュボード)」を参照してください。

セキュリティインシデントレスポンスプレミアム **KPI** ダッシュボードの表示

セキュリティマネージャーは、このダッシュボードを使用して、初期分析/検出から封じ込め、除去、復旧までのセキュリティインシデントのボリューム、パフォーマンス、および進捗状況を追跡して表示できます。

始める前に

現在のリリースでは、次のレポートのリストは [セキュリティインシデントレスポンスプレミアム KPI] ダッシュボードでサポートされていません。

- プロセス - ステータス：ワークベンチは利用できません。
- プロセス - 経過時間：ワークベンチは利用できません。
- 30 日を超えてオープン中のセキュリティインシデント (アサイン先グループおよびステータス別) (Security Incidents Open for More Than 30 Days by Assignment Group and State)：ヒートマップによるビジュアル化は利用できません。
- 30 日を超えて更新されていないセキュリティインシデント (アサイン先グループおよびステータス別) (Security Incidents Not Updated for More Than 30 Days by Assignment Group and State)：ヒートマップによるビジュアル化は利用できません。
- アクティブでないアサイニーのセキュリティインシデント (Security Incidents With Assignee That is not Active)：ヒートマップによるビジュアル化は利用できません。

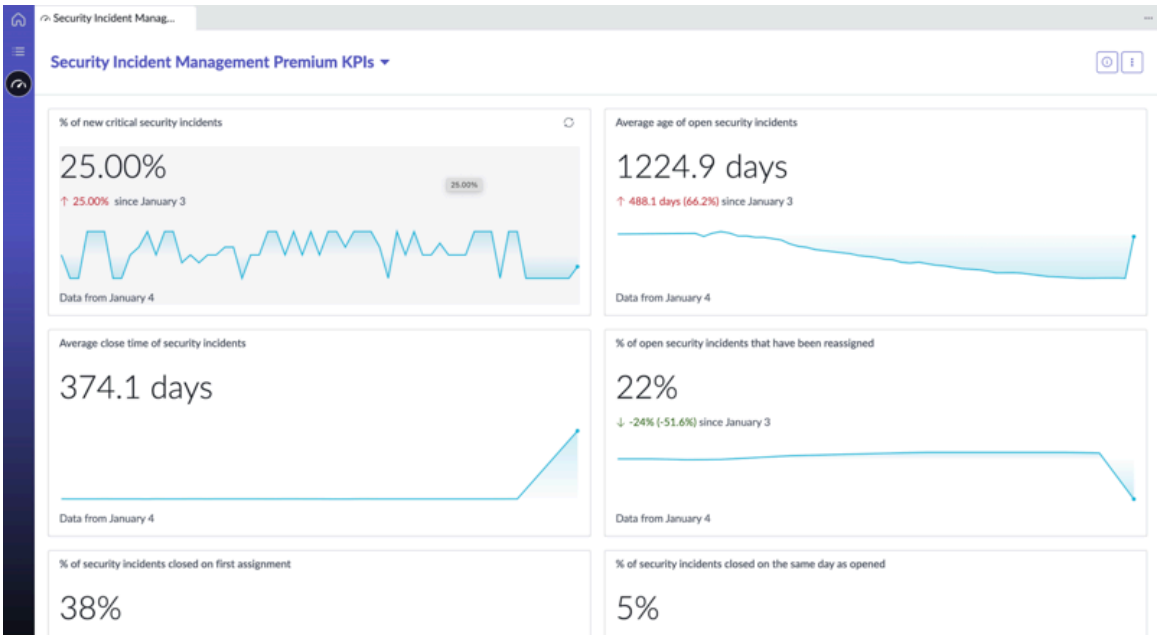
必要なロール：sn_si.analyst (読み取り)、sn_si.manager または sn_si.admin (書き込み)

手順

1. 次のように移動する。 **All** (すべて) > ワークスペース > **Security Incident Response** (セキュリティインシデントレスポンス).
2. ワークスペースのホームページの左側に表示された **[SIR** ダッシュボード] アイコンをクリックします。
3. ドロップダウンリストから [セキュリティインシデントレスポンス プレミアム **KPI]** を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. さらに他の操作を行う場合は [セキュリティインシデントレスポンス プレミアム KPI] ダッシュボードを表示します。
   セキュリティインシデントレスポンス プレミアム KPI ダッシュボードの詳細については、「セキュリティインシデント管理プレミアムダッシュボード」を参照してください。

コンテキスト依存アナリティクスの表示 - SI ダッシュボード

マネージャーとアナリストは、このダッシュボードを使用して、オープンセキュリティインシデント、オープンセキュリティインシデントの平均経過時間、セキュリティインシデントの平均クローズ所要時間、同じ日にオープンされてクローズされたセキュリティインシデントの割合、過去 5 日間および 30 日間更新されていないインシデントの割合を表示できます。

始める前に

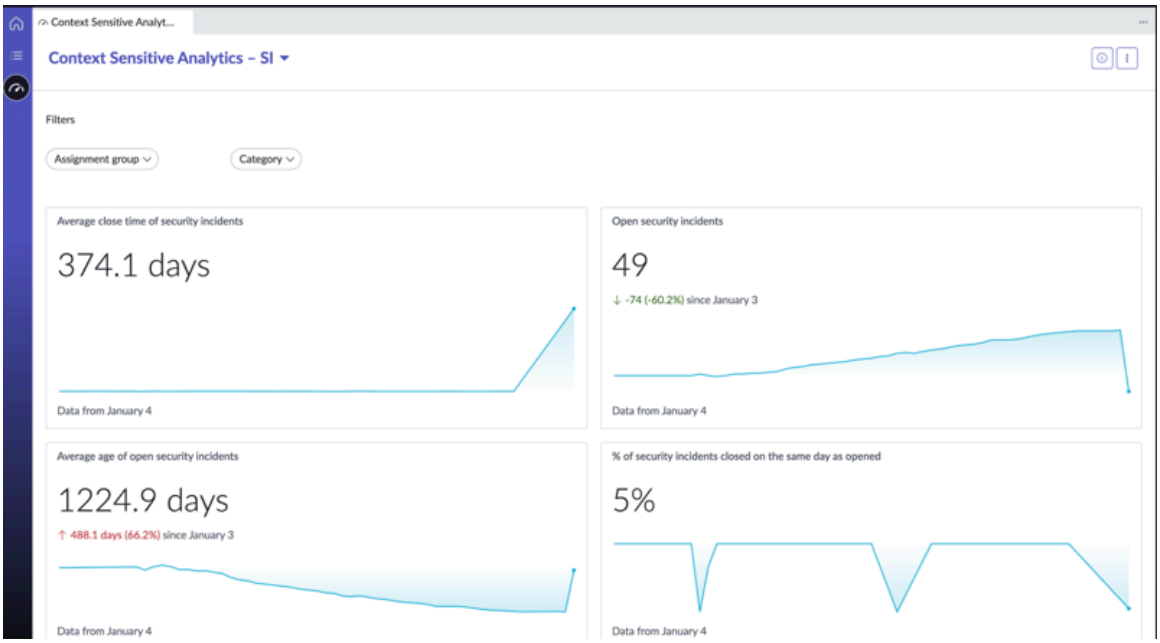
必要なロール：sn_si.analyst (読み取り)、sn_si.manager または sn_si.admin (書き込み)

手順

1. 次のように移動する。 **All** (すべて) > ワークスペース > **Security Incident Response** (セキュリティインシデントレスポンス).
2. ワークスペースのホームページの左側に表示された **[SIR** ダッシュボード] アイコンをクリックします。
3. ドロップダウンリストから [コンテキスト依存アナリティクス - **SI]** を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. さらに他の操作を行う場合は、[コンテキスト依存アナリティクス - SI] ダッシュボードを表示します。

CISO ダッシュボードの表示

このダッシュボードは、最高情報セキュリティ責任者 (CISO) を対象に、インスタンスのセキュリティインシデントとインシデントの傾向 (週次) の概要をグラフィカルなチャート形式で表示します。これらのチャートは、Security Operations Center (SOC) のパフォーマンスを効果的に表示および分析するのに役立ちます。

始める前に

- 必要なロール：sn_si.admin および sn_si.ciso - インシデントの編集および表示。
- セキュリティインシデント対応のパフォーマンスアナリティクスアプリがインストールされていることを確認します。

このタスクについて

注:
クラシック UI では、CISO ダッシュボードと CISO 概要ダッシュボードは異なる 2 つのダッシュボードでした。この 2 つのダッシュボードの機能が CISO ダッシュボードに統合されました。

CISO ダッシュボードには、セキュリティインシデントに関する重要なインサイトが週単位で表示されます。インジケーターを設定して、インジケータープロパティの条件に一致するインシデントのデータスナップショットを収集できます。収集されたデータは、ダッシュボードのウィジェットを使用してビジュアル化されます。

CISO ダッシュボードのウィジェットを使用して、週次の傾向を可視化できます。セキュリティインシデントの傾向に関するデータや統計情報は、組織で定義されている週次のインシデントのインジケータープロパティから収集されます。次のチャートから重要なインサイトを得ることができます。

- 平均識別時間 (週次)：このチャートは、セキュリティインシデントの識別に要した平均時間 (週次) を示します。
- 平均封じ込め時間 (週次)：このチャートは、セキュリティインシデントの封じ込めに要した平均時間 (週次) を示します。

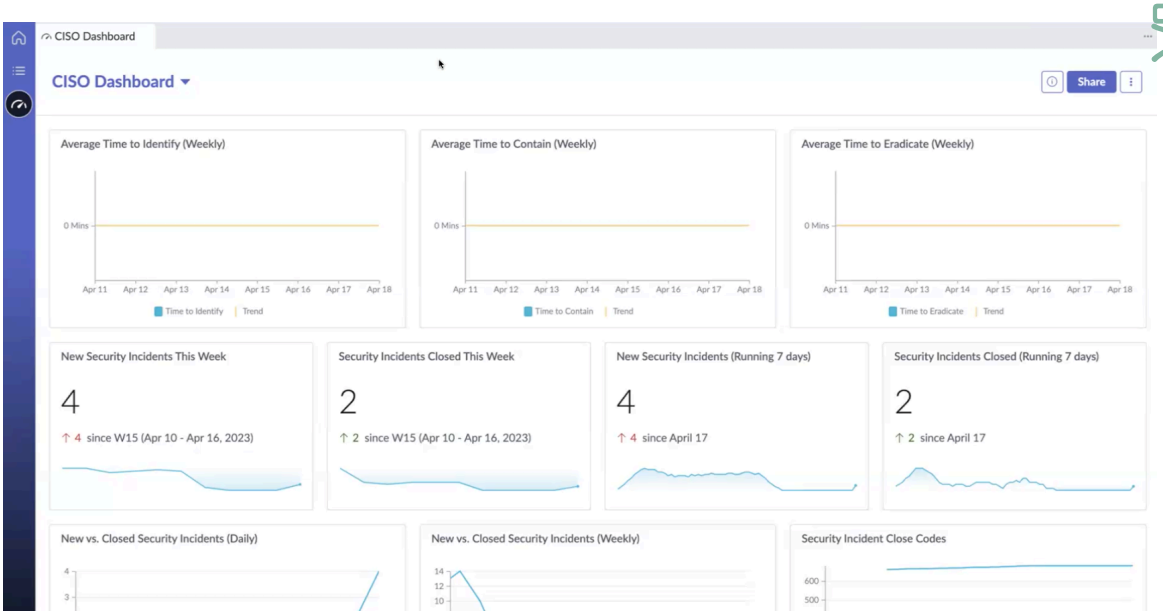
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 平均除去時間 (週次)：このチャートは、セキュリティインシデントの除去に要した平均時間 (週次) を示します。
- 今週の新規セキュリティインシデント：このチャートは、今週の新規セキュリティインシデントの数を示します。
- 今週クローズされたセキュリティインシデント：このチャートは、今週クローズされたセキュリティインシデントの数を示します。
- 新規セキュリティインシデント **(7** 日間移動合計)：このチャートは、今週の新規セキュリティインシデントの数 (移動合計) を示します。
- クローズされたセキュリティインシデント **(7** 日間移動合計)：このチャートは、今週のクローズされた新規セキュリティインシデントの数 (移動合計) を示します。
- 新規インシデント対クローズ済みインシデント (日次) **(New vs Closed incidents (Daily))**：このチャートは、日次新規セキュリティインシデントと日次クローズ済みセキュリティインシデントの比較を示します。
- 新規インシデント対クローズ済みインシデント (週次) **(New vs Closed incidents (Weekly))**：このチャートは、週次新規セキュリティインシデントと週次クローズ済みセキュリティインシデントの比較を示します。
- セキュリティインシデントのクローズコード **(Security Incident Closed Codes)**：このチャートは、セキュリティインシデントのクローズコードを示します。

手順

1. 次のように移動する。 **All** (すべて) > ワークスペース > **Security Incident Response** (セキュリティインシデントレスポンス).
2. ワークスペースのホームページの左側にある **[SIR** ダッシュボード] アイコンをクリックします。
3. ドロップダウンリストから **[CISO** ダッシュボード] を選択します。



4. CISO ダッシュボードでその他のアクションを確認します。

CISO レポート概要ダッシュボードの表示

このダッシュボードは、最高情報セキュリティ責任者 (CISO) を対象に、インスタンスのセキュリティインシデントとインシデントの傾向 (週次) のレポート概要をグラフィカルなチャート形式で表

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

示します。これらのチャートは、Security Operations Center (SOC) のパフォーマンスを効果的に表示および分析するのに役立ちます。

始める前に
必要なロール：sn_si.admin および sn_si.ciso - インシデントの編集および表示。

このタスクについて
CISO レポート概要ダッシュボードは、セキュリティインシデントに関する重要なインサイトを週単位で表示します。ウィジェットを使用して週次の傾向を視覚化できます。次のチャートから CISO レポートに関する重要なインサイトを得ることができます。

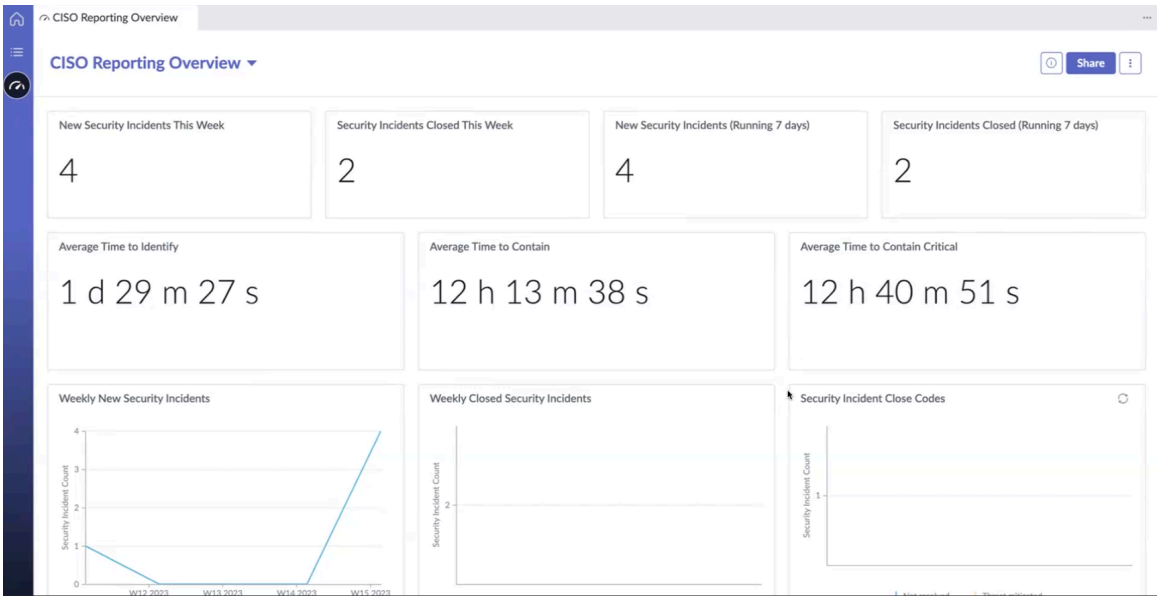
- 今週の新規セキュリティインシデント：このタイルには、今週の新規セキュリティインシデントの数のレポートが表示されます。
- 今週クローズされたセキュリティインシデント：このタイルには、今週クローズされたセキュリティインシデントの数のレポートが表示されます。
- 新規セキュリティインシデント **(7** 日間移動合計)：このタイルには、今週の新規セキュリティインシデントの数 (移動合計) のレポートが表示されます。
- クローズされたセキュリティインシデント **(7** 日間移動合計)：このタイルには、今週のクローズされたセキュリティインシデントの数 (移動合計) のレポートが表示されます。
- 平均識別時間：このタイルには、セキュリティインシデントの識別に要した平均時間 (週次) のレポートが表示されます。
- 平均封じ込め時間：このタイルには、セキュリティインシデントの封じ込めに要した平均時間 (週次) のレポートが表示されます。
- 平均封じ込め時間 (重大) **(Average Time to Contain Critical)**：このタイルには、重要なセキュリティインシデントの封じ込めに要した平均時間 (週次) のレポートが表示されます。
- 新規セキュリティインシデント (週次) **(Weekly New Security Incidents)**：このチャートは、週次の新規セキュリティインシデントのレポートを示します。
- クローズされたセキュリティインシデント (週次) **(Weekly Closed Security Incidents)**：このチャートは、週次のクローズされたセキュリティインシデントのレポートを示します。
- セキュリティインシデントのクローズコード **(Security Incident Closed Codes)**：このチャートは、セキュリティインシデントのクローズコードのレポートを示します。

手順

1. 次のように移動する。 **All** (すべて) > ワークスペース > **Security Incident Response** (セキュリティインシデントレスポンス).
2. ワークスペースのホームページの左側にある **[SIR** ダッシュボード] アイコンをクリックします。
3. ドロップダウンリストから **[CISO** レポート概要 **(CISO Reporting Overview)]** を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. CISO レポートダッシュボードでその他のアクションを確認します。

セキュリティインシデントマネージャー概要ダッシュボードの表示

このダッシュボードは、チームレベルでの優先度が重大または高のセキュリティインシデント、24 時間以内に期限切れになる SLA、およびインスタンスの週次のインシデント傾向の概要を、レポートとグラフィカルチャートの形式でマネージャーに対して表示します。

始める前に

必要なロール：

- sn_si.admin：ダッシュボードの編集および表示。
- sn_si.manager：ダッシュボードの表示。

このタスクについて

優先度が重大または高のセキュリティインシデント、または緊急の対応が必要な SLA を分析できます。セキュリティインシデントマネージャー概要ダッシュボードのウィジェットを使用して、週次の傾向を可視化できます。セキュリティインシデントの週次または月次の傾向のデータや統計情報は、組織で定義されているインシデントテーブルから収集されます。次のチャートから重要なインサイトを得ることができます。

- チームの重大なセキュリティインシデント **(Team Critical Security Incidents)**：このタイルには、今週発生したチームの重大なセキュリティインシデントの数が表示されます。
- チームの高セキュリティインシデント **(Team High Security Incidents)**：このタイルには、今週発生したチームの高セキュリティインシデントの数が表示されます。
- **24** 時間以内に期限切れになる **SLA (SLAs expiring within 24 hours)**：このタイルには、24 時間以内に期限切れになる SLA の数が表示されます。
- 平均識別時間：このタイルには、セキュリティインシデントの識別に要した時間の週次の平均時間が表示されます。
- 平均封じ込め時間：このタイルには、セキュリティインシデントの封じ込めに要した平均時間 (週次) が表示されます。
- 平均封じ込め時間 (重大) **(Average Time to Contain Critical)**：このタイルには、重要なセキュリティインシデントの封じ込めに要した平均時間 (週次) が表示されます。

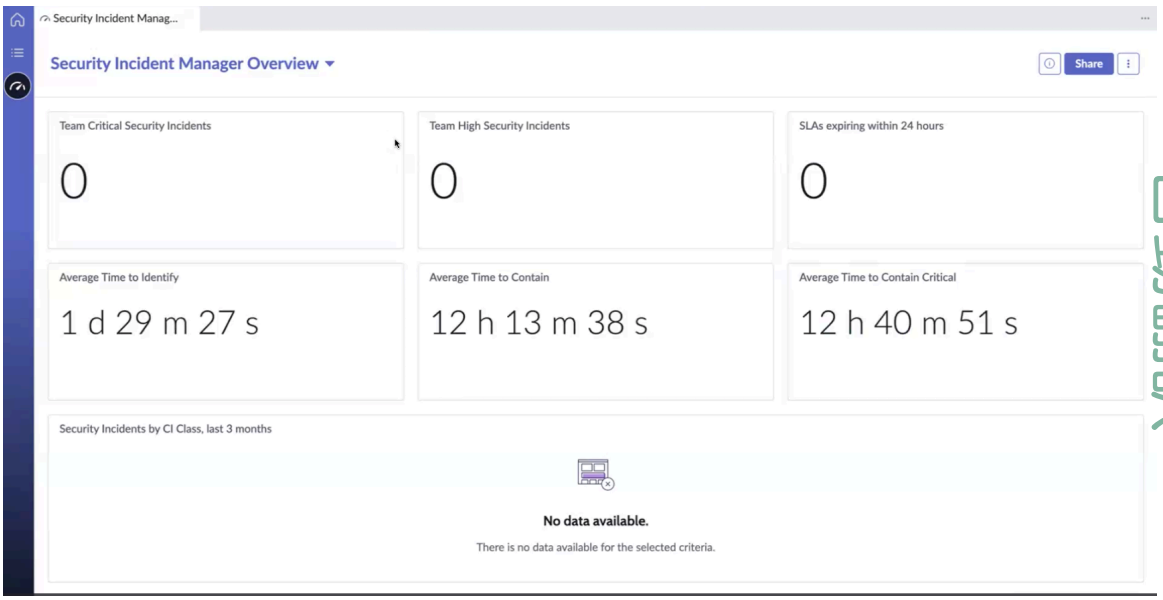
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- **CI** クラス別セキュリティインシデント **(3** か月) **(Security Incident by CI Class, last 3 months)**：このチャートは、CI クラスに基づく過去 3 か月間のすべてのセキュリティインシデントの傾向を示しています。
- すべてのセキュリティインシデントの傾向（カテゴリ別）**(Trend of All Security Incidents by Category)**：このチャートは、カテゴリに基づくすべてのセキュリティインシデントの傾向を示します。
- すべてのセキュリティインシデントの傾向（優先順位別）**(Trend of All Security Incidents by Priority)**：このチャートは、優先度に基づくすべてのセキュリティインシデントの傾向を示します。

手順

1. 次のように移動する。 **All** (すべて) > ワークスペース > **Security Incident Response** (セキュリティインシデントレスポンス).
2. ワークスペースのホームページの左側にある **[SIR** ダッシュボード] アイコンをクリックします。
3. ドロップダウンリストから [セキュリティインシデントマネージャー概要] を選択します。



4. さらに他の操作を行う場合はセキュリティインシデントマネージャー概要ダッシュボードを表示します。

セキュリティインシデントレスポンスヘルスダッシュボードの表示

セキュリティインシデントレスポンスヘルスダッシュボード機能により、セキュリティインシデントレスポンスプロセスの実装、発生した問題/エラー、パフォーマンスのメトリクスに関連する重要な側面が一元的に表示されます。組織におけるセキュリティインシデントセキュリティインシデントレスポンス機能の有効性を監視および最適化する重要なツールとして機能します。

始める前に

必要なロール：「sn_si.admin」「sn_si.analyst」「sn_si.analytics_read」のいずれか - ダッシュボードを確認してください。

このタスクについて

各アプリケーションのウィジェットや傾向チャートを使用して、セキュリティインシデントの健全性を監視することができます。これらの統計情報では、SIR アプリケーション内の構成ステータスや修復の有効性を詳述した包括的な健全性スコアを提供します。セキュリティインシデントレスポンスヘルスダッシュボードは、次の 4 つのタブをサポートしています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- プロセス：このタブには、週単位でグループ化されたさまざまなアラートセンサーからのすべてのインシデントに関するサマリーが表示されます。
- 実装：このタブには、顧客がインスタンスで実行するカスタマイズが表示されます。スクリプトインクルード、ビジネスルール、フロー、アップグレードが対象になります。
- 問題/エラー：このタブには、統合プロセスのエラー、インシデントの生データの取り込み時における不整合、SIR アプリケーションの送信 HTTP エラー、プレイブックの実行時に発生した問題を強調表示するウィジェットが表示されます。
- パフォーマンス：このタブには、パフォーマンスクエリ、ビジネスルール、スクリプトの速度低下など、SIR アプリケーションのパフォーマンスの問題が表示されます。

手順

1. 次のように移動する。 **All** (すべて) > ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. SIR ワークスペースのホームページにある **[SIR** ダッシュボード] アイコンをクリックします。
3. ドロップダウンリストから [セキュリティインシデントレスポンスヘルスダッシュボード] を選択します。
4. [プロセス] タブを選択すると、チャートの各アラートセンサーでトリガーされたセキュリティインシデントの数が週次ベースで表示されます。

[プロセス] タブ

次のタスクを実行できます。

a. チャートのアラートセンサーを選択すると、1 週間にアラートセンサーでトリガーされたセキュリティインシデント数に関する KPI 詳細が表示されます。

b. 特定の週の KPI 詳細を取得するには、[カレンダー] オプションを使用します。

c. アラートセンサーでトリガーされたセキュリティインシデントを比較するには、**[** 比較レコード] オプションを選択します。

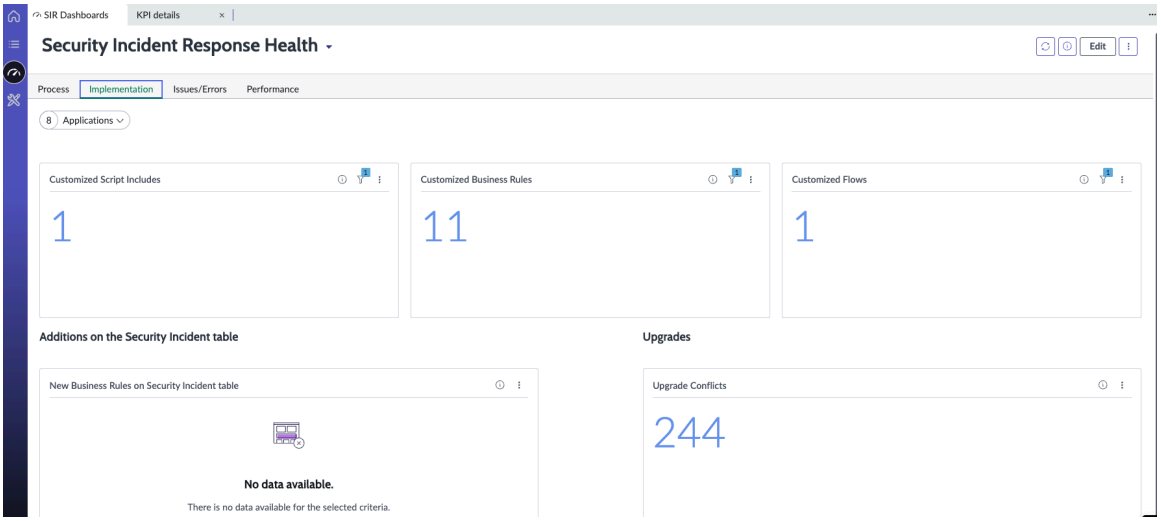
d. 「グラフのタイプ」「時系列」「分析」を使用するには、 [チャートオプション] を選択します。

5. [実装] タブを選択すると、セキュリティインシデントレスポンスアプリケーションに、セキュリティインシデントに対して作成されたカスタマイズの数が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[実装] タブ



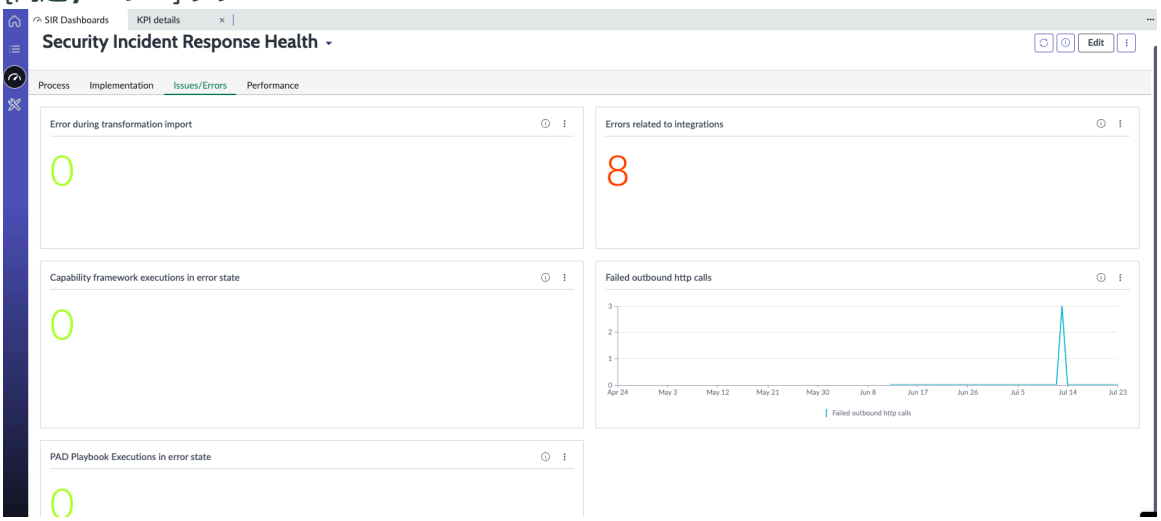
[実装] タブ：

各インシデントレスポンスアプリケーションに対して作成されたカスタマイズ数に関する集計ダッシュボードを表示できます。

- カスタムのスクリプトインクルード：このウィジェットには、SIR アプリケーションの要件に基づいて追加されたカスタムスクリプトの数が表示されます。
- カスタムのビジネスルール：このウィジェットには、SIR アプリケーションの要件に基づいて追加されたカスタムのビジネスルールの数が表示されます。
- カスタムのフロー：このウィジェットには、SIR アプリケーションの要件に基づいて追加されたカスタムのフローの数が表示されます。
- セキュリティインシデントテーブルの新しいビジネスルール：このウィジェットには、セキュリティインシデントテーブルで作成されたビジネスルールの数が表示されます。
- アップグレードの競合：このウィジェットには、SIR アプリケーションのアップグレード時にトリガーされた競合の数が表示されます。

6. [問題 / エラー] タブを選択すると、セキュリティインシデントレスポンスアプリケーションでトリガーされた問題やエラーの数が表示されます。

[問題 / エラー] タブ



[問題 / エラー] タブ：

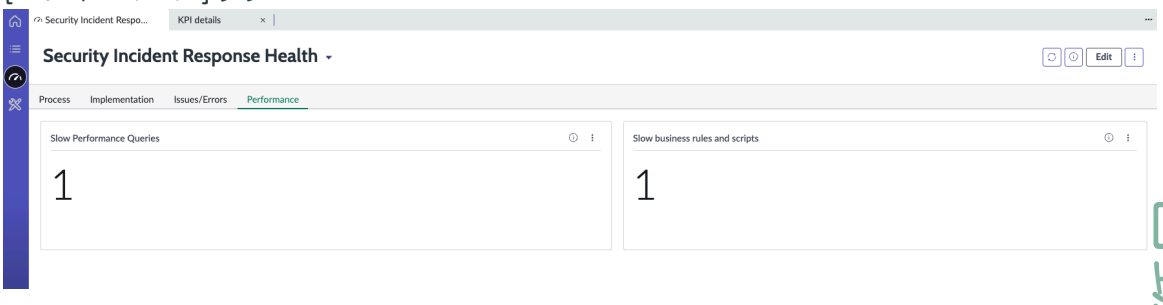
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンスアプリケーションの問題やエラーについては、集計ダッシュボードで確認することができます。

- 変換のインポート時のエラー：このウィジェットには、SIR アプリケーションでの変換のインポート時にトリガーされたエラーの数が表示されます。
- 統合関連のエラー：このウィジェットには、SIR 統合時にトリガーされたエラーの数が表示されます。
- エラーステータスになった機能フレームワークの実行：このウィジェットには、SIR アプリケーションでの機能フレームワークの実行時にトリガーされたエラーの数が表示されます。
- 失敗した送信 **HTTP** 呼び出し：このウィジェットには、SIR アプリケーションでトリガーされた、失敗した送信 HTTP 呼び出しの数が表示されます。
- エラーステータスになった **PAD** プレイブックの実行：このウィジェットには、SIR アプリケーションでトリガーされた PAD プレイブックの実行エラーの数が表示されます。

7. [パフォーマンス] タブを選択すると、セキュリティインシデントレスポンスアプリケーションでトリガーされたパフォーマンスの問題の数が表示されます。

[パフォーマンス] タブ



[パフォーマンス] タブ：

セキュリティインシデントレスポンスアプリケーションのパフォーマンスの問題については、集計ダッシュボードで確認することができます。

- 低速のパフォーマンスクエリ：このウィジェットには、SIR アプリケーションの平均実行時間が 10 ミリ秒以上、平均実行回数が 1000 回以上のときのパフォーマンスクエリの数が表示されます。
- 低速のビジネスルールおよびスクリプト：このウィジェットには、SIR アプリケーションの平均実行時間が 10 ミリ秒以上、平均実行回数が 1000 回以上のときのビジネスルールおよびスクリプトの数が表示されます。

8. [リフレッシュ] アイコンを使用すると、セキュリティインシデントレスポンスヘルスダッシュボードのデータをリフレッシュできます。
9. [ダッシュボードの詳細を表示] アイコンを使用すると、セキュリティインシデントレスポンスヘルスダッシュボードの詳細を表示できます。
10. [編集] オプションを使用すると、セキュリティインシデントレスポンスヘルスダッシュボードの詳細を変更できます。
11. [その他 **(More)**] オプションを使用すると、セキュリティインシデントレスポンスヘルスダッシュボードでその他のアクションを実行できます。

セキュリティインシデントの作成

セキュリティインシデントは、フォームから手動で作成することも、Splunk などの統合されたサードパーティのアラートモニタリングツールから受信したセキュリティイベントを介して自動的に作成することもできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重要:
セキュリティインシデントレスポンス の最新機能は、セキュリティインシデントレスポンス ワークスペース でのみ利用できます。シフト引き継ぎ、リスクスコア算出などの機能にアクセスして活用するには、最新の セキュリティインシデントレスポンス または セキュリティインシデントレスポンスワークスペース バージョンをインストールまたはアップグレードしてください。

セキュリティロールがある場合は、次のいずれかの方法を使用して、セキュリティインシデントを手動で作成できます。

セキュリティインシデントを手動で作成する方法

メソッド	説明
セキュリティインシデントリストから手動で作成する	セキュリティインシデントリストで、[新規] をクリックして、新しいセキュリティインシデントを作成します。
セキュリティインシデントカタログから手動で作成する	セキュリティインシデントカタログで定義されたセキュリティ脅威のカテゴリから選択して、セキュリティインシデントを作成できます。
インシデント管理	インシデント管理のインシデントフォームで、[セキュリティインシデントを作成] をクリックして、新しいセキュリティインシデントを作成します。
セキュリティ要求から手動で変換する	セキュリティの要求フォームで、[セキュリティインシデントへの変換] をクリックして、新しいセキュリティインシデントを作成します。
イベント管理アラートから手動で作成する	イベント管理アラートフォームで、[セキュリティインシデントを作成] をクリックして、アラートから新しいセキュリティインシデントを作成します。
アラートからの手動での作成	イベント管理アラートフォームで、[セキュリティインシデントを作成] をクリックして、新しいセキュリティインシデントを作成します。
脆弱性レコードから手動で変換する (脆弱性対応プラグインがアクティブ化されている場合)	[脆弱性一致アイテム] フォームで、[セキュリティインシデントを作成] をクリックして、新しいセキュリティインシデントを作成します。

セキュリティインシデントの自動作成

通常、セキュリティアドミニストレーターは、セキュリティインシデントを自動的に生成するためのアラートルールを設定する責任を負います。

セキュリティアドミニストレーターがセキュリティインシデントを作成する方法

メソッド	説明
アラートルールを使用して自動的に作成する	データセンターの イベント管理 アプリケーションで定義されたアラートルールに基づいて、セキュリティインシデントを作成できます。

セキュリティインシデントの手動作成

セキュリティインシデントは、セキュリティインシデントフォームやその他のフォームから作成できます。

次のフォームから、既存のレコードに基づいてセキュリティインシデントを作成できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 任意のセキュリティインシデントリスト
- インシデントフォーム
- イベント管理 アラートフォーム
- 脆弱性一致アイテムフォーム
- セキュリティの要求フォーム

セキュリティインシデントリストからのセキュリティインシデントの作成

セキュリティインシデントを自動的に作成する方法の他に、必要に応じて手動で作成することもできます。

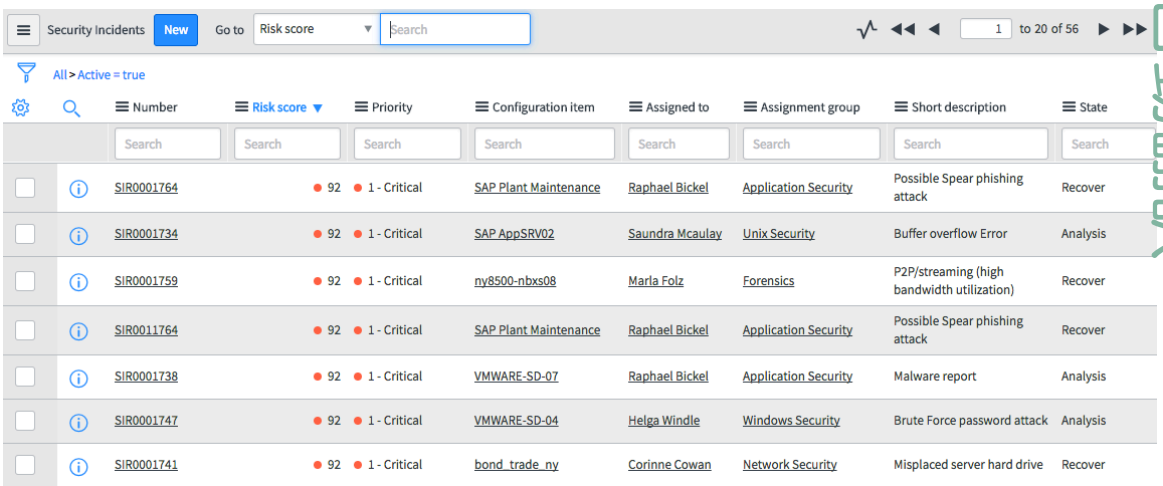
このビデオでは、[セキュリティインシデント] リストからセキュリティインシデントを作成する方法をご覧いただきながら総括的に紹介します。

セキュリティインシデントリストからのセキュリティインシデントの作成

始める前に
必要なロール：sn_si.basic

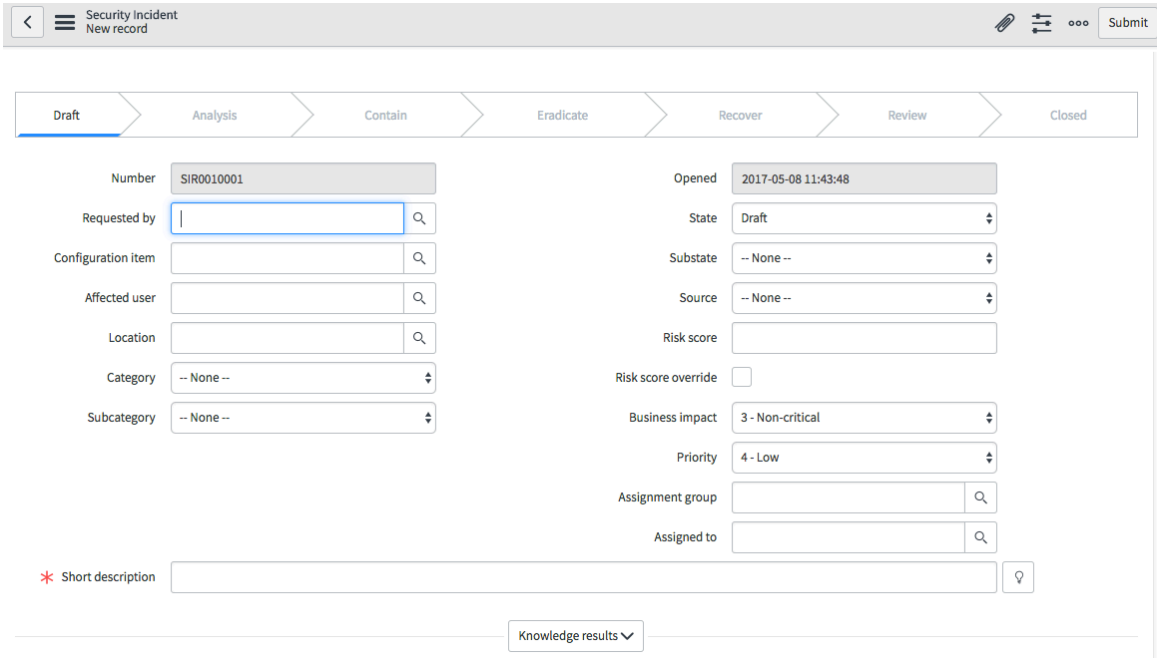
手順

1. 任意のセキュリティインシデントリスト (例: **All** (すべて) > セキュリティインシデント > インシデント > すべてのインシデントを表示) を開きます。



2. [新規] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. フォームのフィールドに入力します。

フィールド	説明
セキュリティタグを選択	必要に応じて、[セキュリティタグ] を選択してレコードにメタデータを追加するか、このセキュリティインシデントレコードにアクセスする必要があるユーザーを識別できるようにします。このフィールドは、セキュリティインシデントが保存された後にのみ表示されます。
数値	[読み取り専用] セキュリティインシデント番号
要求者	実行すべき作業を要求しているユーザー
構成アイテム	セキュリティ問題の影響を受けるサーバー、コンピューター、ルーター、その他の構成アイテム
影響を受けるユーザー	セキュリティ上の問題によって影響を受けるユーザー。
ロケーション	要求者またはリソースの場所[構成アイテム] が選択されていない場合、このフィールドには要求者の場所が事前に入力されます。
カテゴリ	セキュリティ問題のタイプを識別するカテゴリ。 カテゴリが選択されている場合、この問題を分析するためのワークフローがレコードの保存時に実行されます。たとえば、[サービス拒否] を選択すると、[セキュリティイ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	ンシデント - サービス拒否 - テンプレート (Security Incident - Denial of Service – Template)] ワークフローが実行されます。 詳細については、「セキュリティインシデントレスポンスのワークフローテンプレート」を参照してください。
サブカテゴリ	問題をさらに細かく定義するサブカテゴリ
オープン	[読み取り専用] インシデントが開かれた日時を表示します。
状況	セキュリティインシデントの現在のステータス。セキュリティインシデント作成時のこのフィールドのデフォルトは [ドラフト] です。
サブステート	セキュリティインシデントに処理待ちの問題または変更が含まれているかどうかを識別します。
ソース	メール、電話、ネットワーク監視などのセキュリティインシデントのソースを識別します。
アラートセンサー	CarbonBlack、CrowdStrike、McAfee などのアラートまたはイベントデータを取り込むためのセキュリティ統合
アラートルール	このセキュリティインシデントの作成をトリガーしたセキュリティ製品のルール
リスクスコア	このセキュリティインシデントに対して計算されたリスクスコアを表示します。この値は、セキュリティインシデントの優先度、セキュリティインシデントのタイプ (サービス拒否、スピアフィッシング、または悪意のあるコードアクティビティ)、およびインジケーター上の否定的な評価スコアの要因となったソース数に基づいています。リスクスコアは、アナリストのセキュリティインシデント作業の優先順位付けに役立ちます。 3 つのセキュリティインシデントプロパティを使用すると、より識別しやすいように、リストビューのリスクスコアの横に表示される色分けされたドットを指定できます。 [ビジネスインパクト] や [優先度] などのセキュリティインシデントの特定のフィールドに変更を加え、レコードを保存すると、[リスクスコア] が自動的に再計算されて表示されます。変更は、作業メモと [リスクスコアの監査] 関連リストにも反映されます。 **注:** 影響を受けるユーザーがセキュリティインシデント、影響を受けるサービス、または脆弱性一致アイテムに関連付けられた場合も、リスクスコアは再計算されます。 新しい [リスクスコア] を手動で入力することもできます。これは、特定のセキュリティインシデントを分析対象のセキュリティインシデントのリストの一番上に表示しておきたい場合に便利です。新しい [リスクスコア] を入力すると、[リスクスコアの上書き] チェックボックスが自動的にオンになります。セキュリティインシデントが変更されたか

自動翻訳

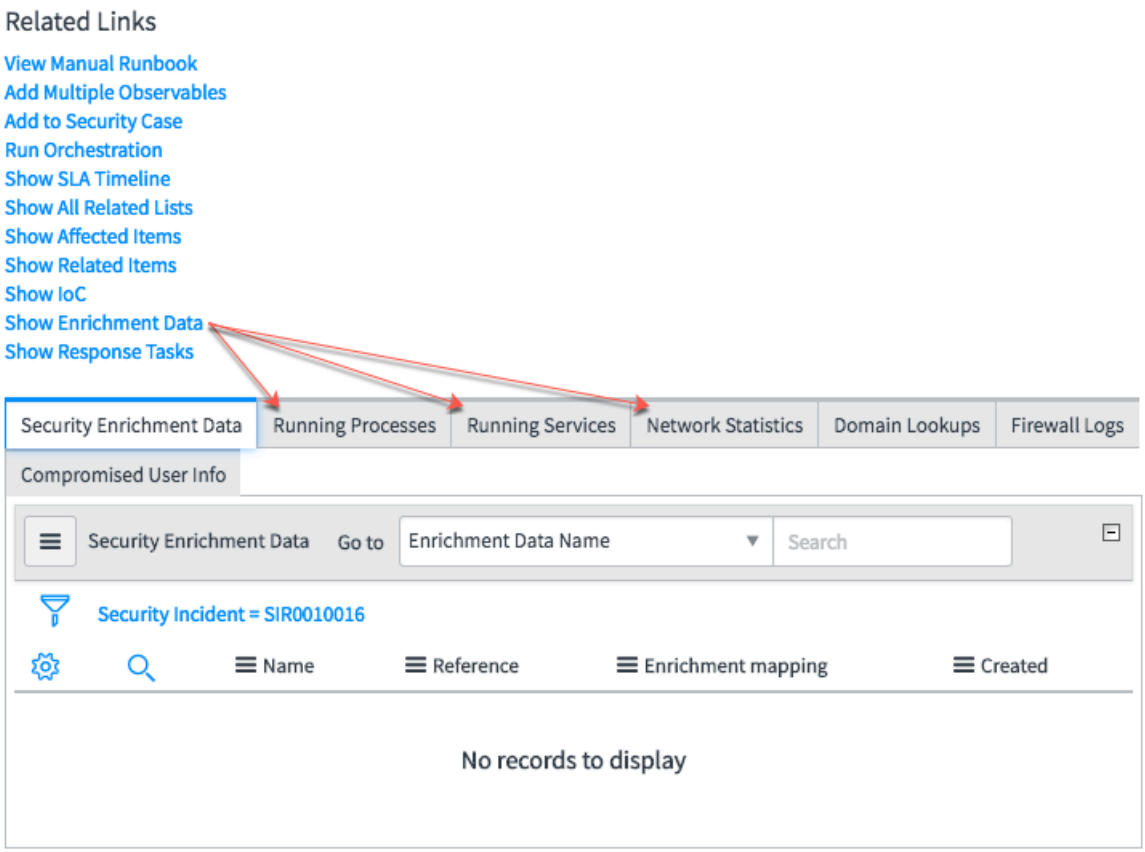
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	どうかに関係なく、手動で入力されたリスクスコアが自動的に再計算されることはありません。 **注:** 以前のリリースからインスタンスをアップグレードした場合、すべてのオープンセキュリティインシデントについてリスクスコアが計算されていました。詳細については、「セキュリティインシデント算出の理解」を参照してください。
リスクスコアの上書き	リスクスコアの自動更新を上書きするには、このチェックボックスをオンにします。上書きは作業メモに反映されます。
ビジネスインパクト	このセキュリティインシデントのビジネスに対する重要性を選択します。デフォルト値は [重大ではない] です。セキュリティインシデントレコードの保存後に、[優先度] や [リスク] フィールドの値を変更すると、[ビジネスインパクト] が再計算されます。
優先度	緊急度に基づいて、このセキュリティインシデントに対処する順序を選択します。レコードの保存後にこの値を変更すると、[ビジネスインパクト] の計算に影響する可能性があります。
アサイン先グループ	このセキュリティインシデントがアサインされているグループ
アサイン先	このセキュリティインシデントの分析がアサインされている個人。アサインは手動または自動で実行できます。詳細については、「セキュリティアナリストのアサイン」を参照してください。
簡単な説明	セキュリティインシデントの簡単な説明
ナレッジ結果	簡単な説明を入力するに伴い、ナレッジベースの関連記事へのリンクが表示されます。 情報をスキャンすると問題が解決する可能性があります。

4. レコードヘッダーを右クリックして、[保存] を選択します。
セキュリティインシデントに新しい CI を追加すると、次の統合ワークフローが自動的に実行されます。
   - Security Operations - 実行中のプロセスを取得フロー。このワークフローは、ホストまたはエンドポイントから構成アイテム (CI) で実行中のプロセスのリストを取得します。
   - セキュリティインシデントレスポンス - 実行中のサービスを取得ワークフロー。このワークフローは、Windows ベースの CI から実行中のサービスのリストを取得します。
   - [Security Operations Integrations - ネットワーク統計情報を取得] フロー。このワークフローは、ホストまたはエンドポイントから、アクティブなネットワーク接続のリストを取得します。
5. これらのワークフローによって取得された情報を表示するには、[拡張データを表示] 関連リンクをクリックし、表示されたタブのいずれかをクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
追加のワークフローは、アクティブ化したサードパーティ統合に基づいて次のように実行されます - Security Operations Carbon Black 統合 - 実行中のプロセスを取得フロー

関連情報

セキュリティインシデントレスポンス のセットアップ

セキュリティインシデントカタログからのセキュリティインシデントの作成

社内のユーザーは、セキュリティインシデントカタログを使用して、さまざまなタイプのセキュリティ関連の分析を要求できます。

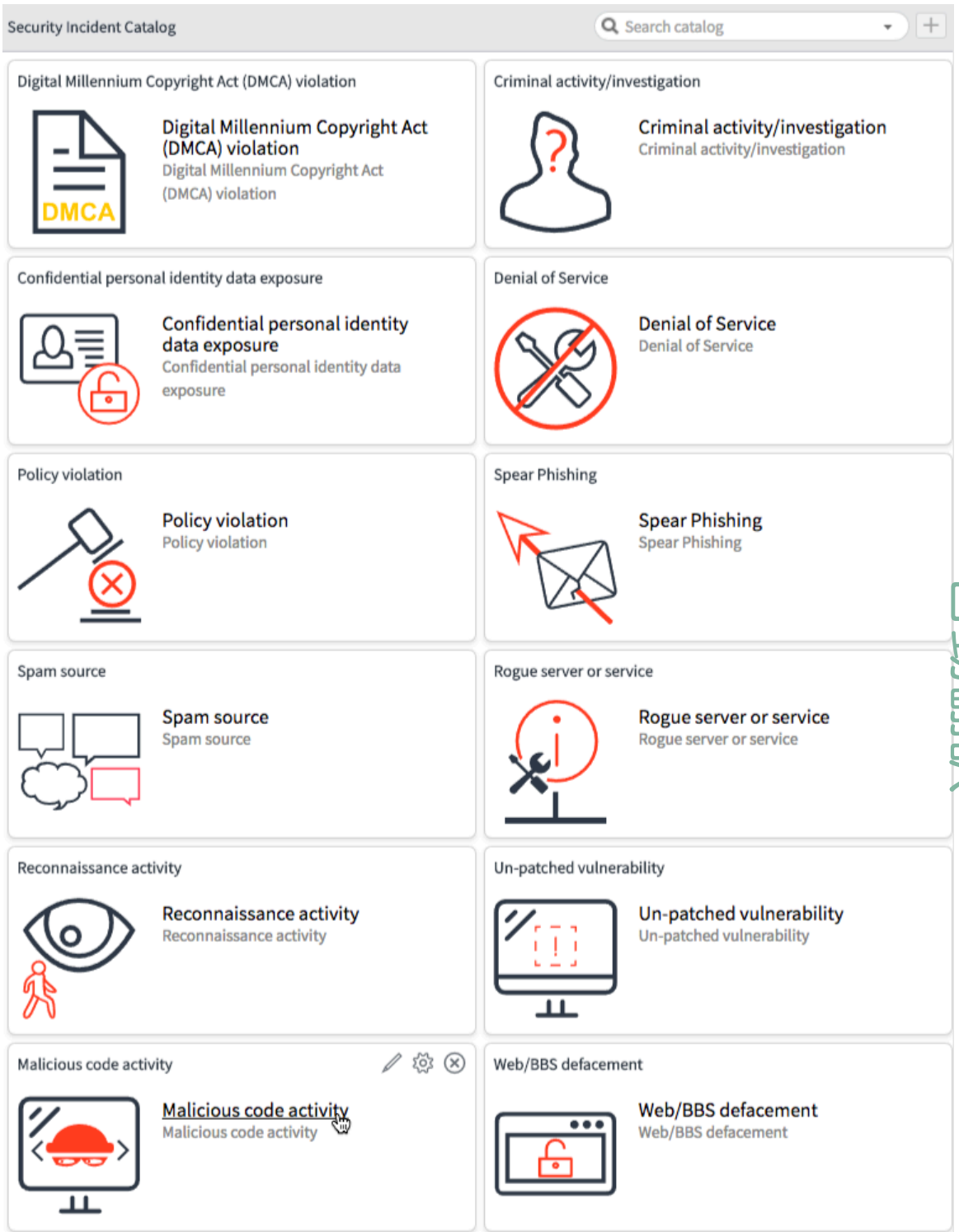
始める前に
必要なロール：なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

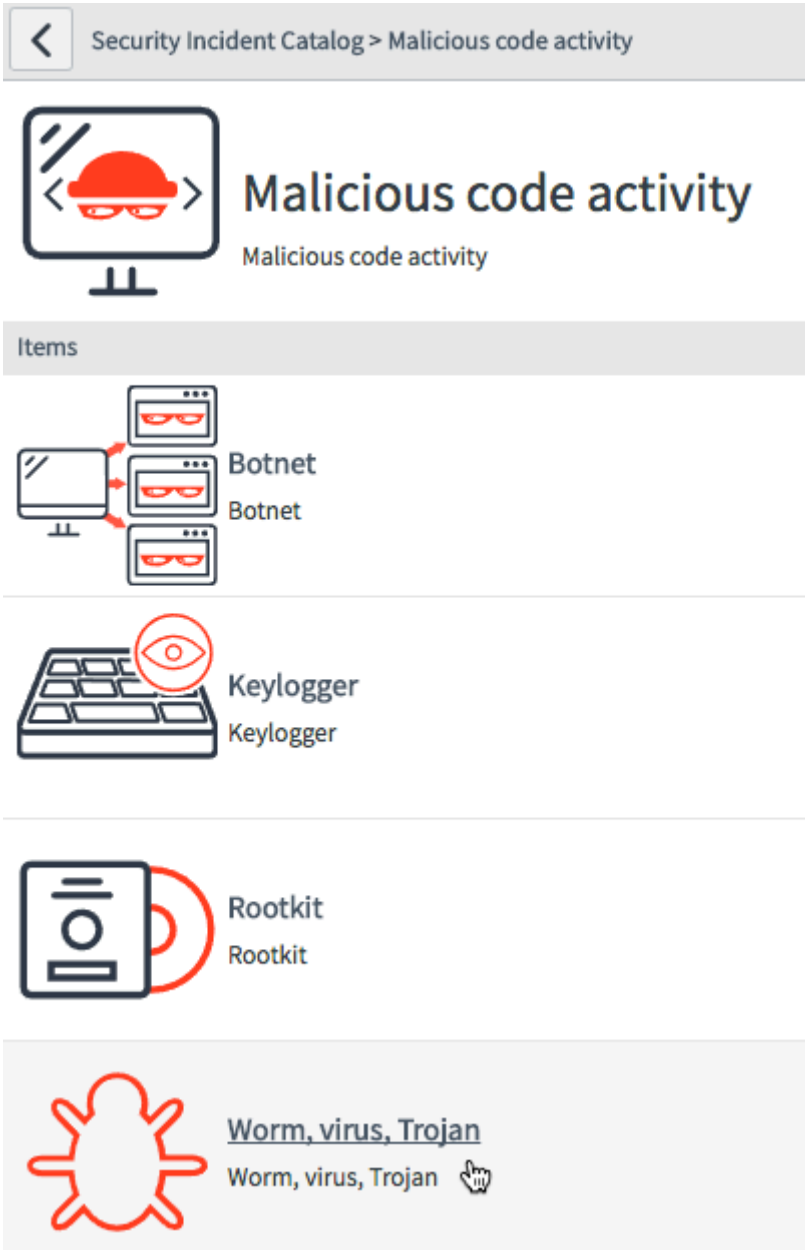
1. 次のように移動する。 **All** (すべて) > セルフサービス > セキュリティインシデントカタログ.



2. 要求を行うカタログアイテムをクリックします。
メインカタログから選択したアイテムにサブカテゴリが含まれている場合は、リストが表示されます。次の例では、[悪意のあるコードアクティビティ] が選択されています。

自動翻訳

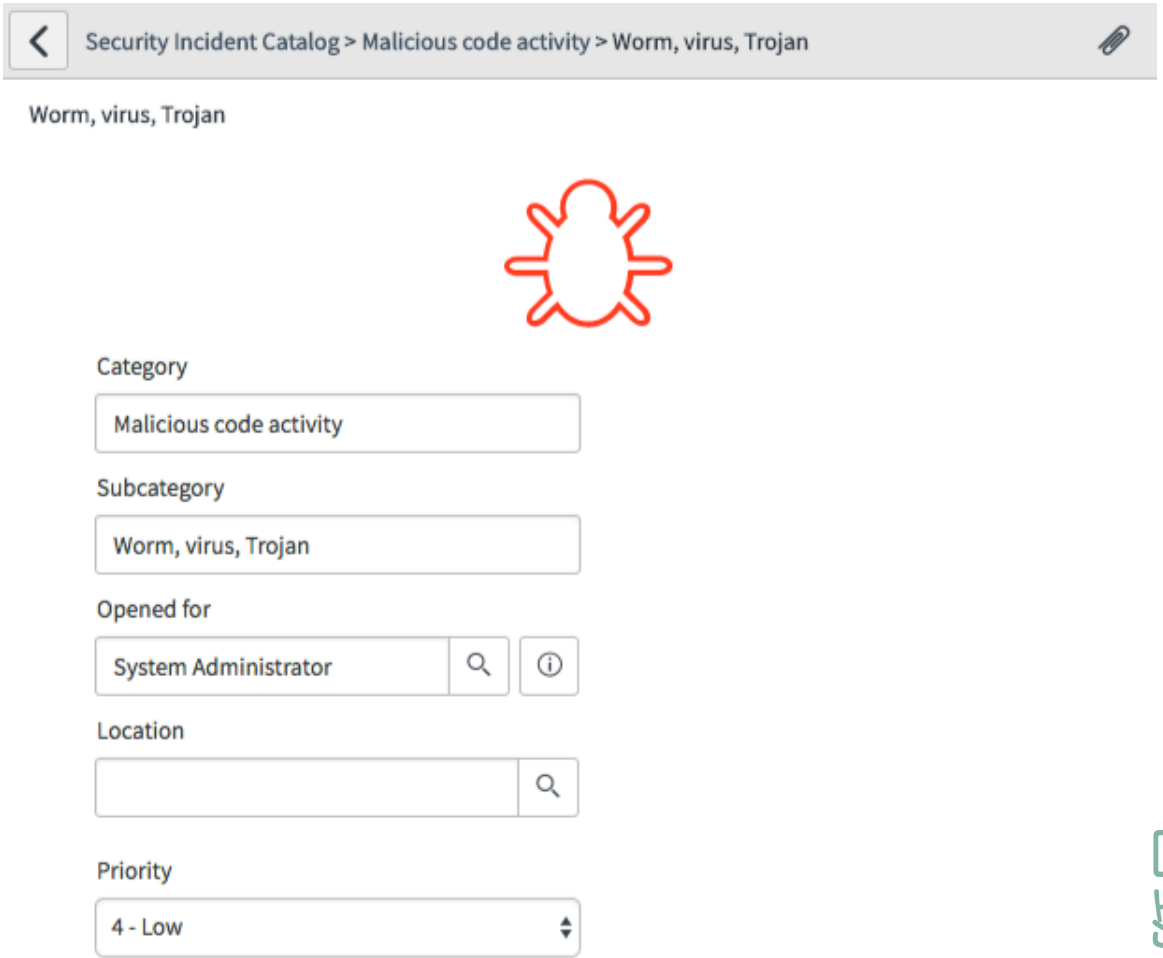
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. 行う要求のタイプに最適なサブカテゴリをクリックします。
この例では、[ワーム、ウィルス、トロイの木馬] サブカテゴリが選択されています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. 要求の情報を入力して、[送信] をクリックします。
   要求がセキュリティインシデント部門に送信されます。
5. 要求を送信した後、次の場所に移動して進捗状況を追跡できます セルフサービス > 自分の要求をクリックし、要求番号を入力します。

イベント管理 - アラートからのセキュリティインシデントの作成

イベント管理がアクティブになっていると、アラートフォームからセキュリティインシデントを手動で作成できます。

始める前に

イベント管理プラグインを利用するには、個別のサブスクリプションが必要であり、ServiceNow の担当者によるアクティブ化が必要です。このプラグインにはデモ データが含まれ、関連プラグインがまだアクティブ化されていない場合はアクティブ化します。イベント管理がアクティブになると、サービスアナリティクスが自動的にアクティブになります。
必要なロール：evt_mgmt_admin、evt_mgmt_operator、または evt_mgmt_user

手順

1. 次のように移動する。 **All** (すべて) > イベント管理 > すべてのアラート.
2. アラート番号をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [セキュリティインシデントを作成] をクリックします。
4. [更新] をクリックします。

セキュリティインシデントの自動作成

Splunk などのサードパーティのモニタリングツールからインポートされたセキュリティイベントでセキュリティインシデントが自動的に生成されるように、それらのツールと セキュリティインシデントレスポンス を統合できます。サードパーティツールからセキュリティアラートにデータをインポートすることもできます。

アラートモニタリングツールを セキュリティインシデントレスポンス に統合するには、REST API を使用してセキュリティインシデントインポート [sn_si_incident_import] テーブルに書き込む必要があります。次に、[セキュリティインシデントの変換 **(Security Incident Transform)]** 変換マップ を使用して、インポートセットのソーステーブルをターゲットセキュリティインシデント [sn_si.incident] テーブルのフィールドにマッピングします。

変換マップによって認識されない CI レコードをインポートしようとすると、変換マップスクリプトは次のレコードを (次の順序で) チェックして一致を確認します。

- sys_id
- CI 名
- 完全修飾ドメイン名
- IP アドレス

> **注:**
> 使用しているサードパーティのアラートモニタリングツールに対して [セキュリティインシデントの変換 **(Security Incident Transform)]** 変換マップが適切でない場合は、必要に応じて変換マップを複製して、新しいマップを作成し、フィールドを編集します。

イベントおよびアラートから作成されたセキュリティインシデント

イベントがアラートモニタリングツールからインポートされると、まず イベント管理 によって処理され、アラートにグループ化されます。これらのアラートを使用して、カスタマイズ可能なアラートルールに基づいてセキュリティインシデントを作成することも、手動で確認してセキュリティインシデントとして調査するアラートを選択することもできます。

イベント管理 アプリケーションの アラートルール モジュールに、「重大なアラートからセキュリティインシデントを作成する **(Create security incidents from critical alerts)**」というアラートルールのサンプルがあります。このアラートルールは、ServiceNow 内またはサードパーティのモニタリングアプリケーションから重大なセキュリティ関連イベントを受信したときに、セキュリティインシデントを自動的に作成します。セキュリティインシデントが作成されると、新しいイベントの受信時に更新されます。アラートルールのタスクテンプレートを変更して、このアラートルールによって作成されたセキュリティインシデントの初期値を変更できます。作成するさまざまなセキュリティインシデントを個別に処理するために、さまざまな条件で他のアラートルールを定義できます。

セキュリティアドミンロールを持つユーザーの場合は、不審なアラートから [セキュリティインシデントを作成] ボタンをクリックして、セキュリティインシデントを手動で作成できます。

外部ツールから受信したイベントに次の情報が含まれていることが重要です。

- 影響を受けるリソースになる CI の名前、IP アドレス、または sys_id に設定されたノード
- 他の IT イベントと区別するために [セキュリティ] に設定されたイベント分類
- セキュリティインシデントの説明が設定された、イベントの説明

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 追加情報には、カテゴリ、攻撃ベクトル、戻り先 URL、相関 ID など、前にリストしたフィールドや他のイベントフィールドに適合しない追加情報を含めることができます。形式は、次の JSON 形式を使用して、フィールド名とその値をリストした文字列です。

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

注:
フィールドと値のペアごとに、列名が fieldName と一致するセキュリティインシデントのフィールドが空の場合、fieldValue に設定されます。セキュリティインシデントのフィールドが空でない場合、フィールドは変更されません。いずれの場合も、追加情報でエンコードされたイベントとすべてのフィールドおよび値は、イベントを説明する作業メモエントリーに記録されます。セキュリティインシデントが変更されない場合、作業メモエントリーは作成されません。テーブルに追加するカスタムフィールドを含む、セキュリティインシデントのフィールドを設定できます。

セキュリティアラートにインポートされたデータ

JSON エンコードデータをさらに使用してイベントが作成されると、そのデータは JSON データ内のその値の fieldName と一致する名前を持つフィールドにインポートされます。

サードパーティのモニタリングソフトウェア (Splunk など) にベースシステムと共通していないデータがある場合は、アラートテーブルに新しいフィールドを追加してデータをインポートできます。アラートにデータをインポートするための JSON 形式は、イベントやアラートからセキュリティインシデントを作成するために使用される形式と同じです。

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

唯一の違いは、フィールドのデータが常に fieldValue で上書きされることです。

セキュリティイベントデータがインポートされると、一致するフィールド名がアラートテーブルのフィールドに入力されます。アラートが後でセキュリティインシデントになった場合、同じ追加情報データがセキュリティインシデントの一致するフィールドに入力されます。

ユーザーから報告されたフィッシングメールからのセキュリティインシデントの作成

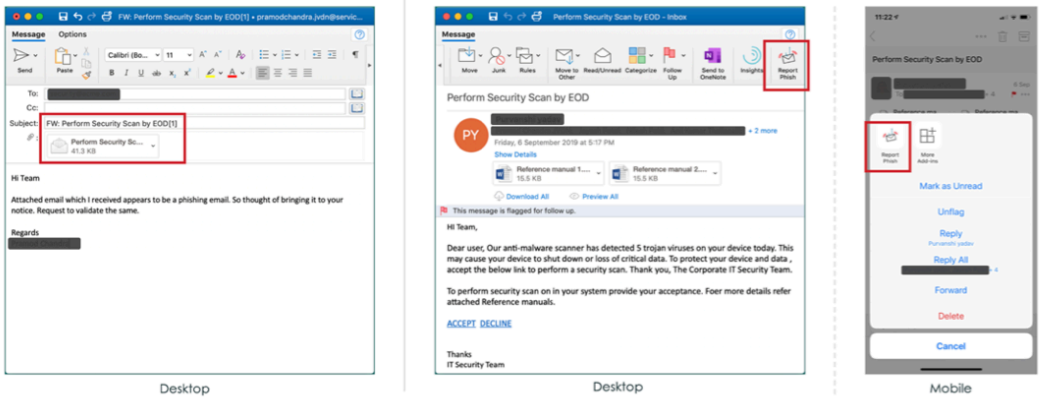
この機能を使用して、ユーザーから報告されたフィッシングメールからセキュリティインシデントを作成します。

拡張されたユーザーから報告されたフィッシング機能には、集計機能、メールヘッダー抽出、および構成が含まれます。

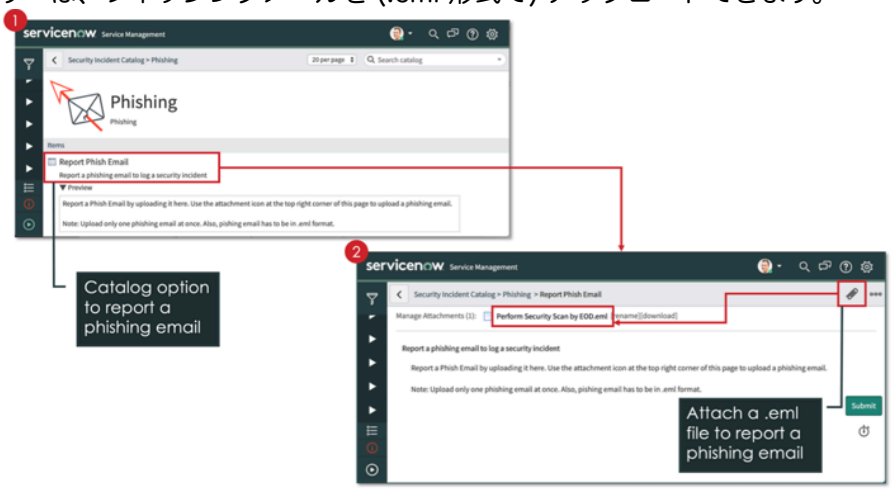
- ユーザーは複数の方法でフィッシングメールを報告できます。
  - メールは添付ファイルとして転送できます。
  - **PhishAlarm** プラグイン (旧 Wombat) が Microsoft Outlook クライアントに構成されている場合、ユーザーは、次の操作を実行できます。
    - [フィッシングを報告] ボタンをクリックする。
    - [フィッシングを報告] オプションを使用して、モバイルデバイスからフィッシングメールを転送する。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



- ユーザーは、フィッシングメールを (.eml 形式で) アップロードできます。



- ユーザーから報告されたフィッシングには、組織内のユーザーによって報告された重複したフィッシングメールを識別する集計ビジネスロジックが含まれています。ユーザーは、この機能を使用して次のことを実現できます。
  - 重複する、または類似のユーザーから報告されたフィッシングインシデント (会社が開始したフィッシングキャンペーン) を集計する。
  - 重複するユーザーから報告されたフィッシングインシデントをトリアージすることを回避し、インシデントの統合に伴う手動の労力を削減する。
  - セキュリティアナリストが単一のユーザーから報告されたフィッシングインシデントを処理できるようにする。
- ユーザーから報告されたフィッシングインシデント内のフィッシングメールヘッダーを提供します。
  - セキュリティアナリストは、インシデント内の重要なメールヘッダー情報をスキャンできます。
  - 他のソースから手動でヘッダー情報を収集する必要がなくなります。
- 送信された元のフィッシングメールは、新しいテーブルにフィッシングメールレコードとして保存されます。
- セキュリティアナリストは、フィッシングメールの内容、ヘッダー、送信元など、元のフィッシングメールの詳細を表示できます。
- セキュリティアドミニストレーターは、以下を含む特定の拡張機能を構成できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- メール本文からメールヘッダーを抽出するための構成 ([フィッシングを報告] による送信)。
- 選択したヘッダーをキャプチャするためのフィルター。
- 重複するフィッシングメールレコードが特定された場合に親と子のインシデントの関連付けを処理するための構成。
- 要件に基づいて集計ビジネスロジックを変更するためのフローデザイナーの構成。

ユーザーから報告されたフィッシングの取り込みルールのセットアップ

sn_si.admin ロールを持つユーザーは、メール一致ルールを定義して、特定の基準に基づいてユーザーから報告されたフィッシングメールをフィルタリングできます。たとえば、直接または [フィッシングを報告] ボタンを介して *security@acme.com* に送信されたすべてのメールを「ユーザーから報告されたフィッシングメール」として分類するルールを定義できます。詳細については、「ユーザーから報告されたフィッシングの取り込みルールのセットアップ」を参照してください。

ユーザーから報告されたフィッシングプロパティの定義

ユーザーから報告されたフィッシングメールから取得する必要があるヘッダー情報を定義します。詳細については、「ユーザーから報告されたフィッシングプロパティの定義」を参照してください。

ユーザーが報告したフィッシングメールから作成されたフィッシングメールレコード

ユーザーから報告されたフィッシングメールは、定義されたメール一致ルールに基づいてセキュリティインシデントに変換されます。詳細については、「ユーザーが報告したフィッシングメールから作成されたフィッシングメールレコード」を参照してください。

フィッシングメールをセキュリティインシデントに変換 **(Transform Phishing Email to Security Incident)**

フィッシングメールをセキュリティインシデントに変換フローでは、フィッシングメールレコードをセキュリティインシデントに変換します。詳細については、「ユーザーから報告されたフィッシングメールのセキュリティインシデントへの変換」を参照してください。

フィッシングメールレコードから作成されたセキュリティインシデントレコード

関連リスト、作業メモ、その他の重要な情報を含むセキュリティインシデントレコードの詳細を表示します。詳細については、「フィッシングメールレコードから作成されたセキュリティインシデントレコード」を参照してください。

必要なコンポーネントとプラグイン

このリリースで利用可能なユーザーから報告されたフィッシング機能は、London リリースで利用可能な既存のユーザーから報告されたフィッシング機能の拡張バージョンです。詳細については、London ドキュメントの「**Create rules to validate user-reported phishing attacks** (ユーザーから報告されたフィッシング攻撃を検証するためのルールの作成)」を参照してください。

重要なインストール手順

この機能拡張は、ユーザーから報告されたフィッシング機能の既存の設計を置き換えるものです。新しい設計には以下の更新が含まれます。

- 既存のユーザーから報告されたフィッシングメール受信アクション (タイプ = 転送、タイプ = 新規) は無効化されました。
- 新しいフィッシングメールの作成受信アクションが利用可能になりました。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ユーザーから報告されたフィッシングメールのセキュリティインシデントへの変換 は、新しい設計のセキュリティインシデントの作成および集計ビジネスロジックを含む新しいフローです。新しいデザインを有効にするには、このフローをアクティブ化する必要があります。
- 既存のユーザーから報告されたフィッシングルールは、アップグレード中も保持されます。

注:
ユーザーから報告されたフィッシング送信に対してカスタムメール受信アクションとカスタムワークフローを使用する場合は、競合または重複する機能について古い設計と新しい設計の両方を確認する必要があります。

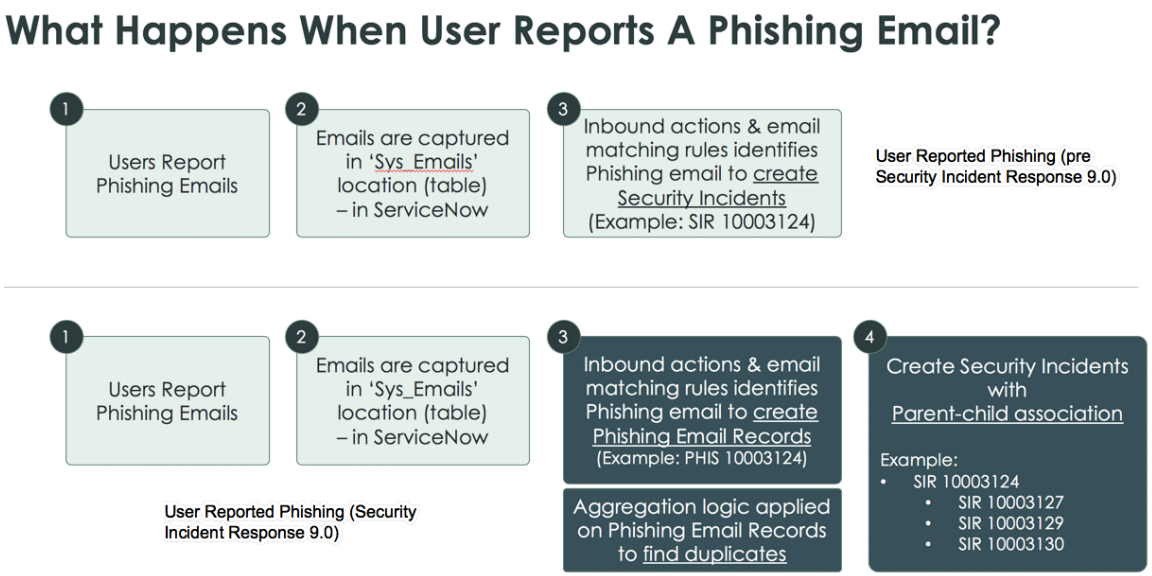
ユーザーから報告されたフィッシング機能拡張の詳細：機能拡張の詳細は次のとおりです。

- 複数の方法でのフィッシングメールのレポート：詳細については、「ユーザーから報告されたフィッシングメールからのセキュリティインシデントの作成」を参照してください。フィッシングメールは、次に *sn_si_phishing_email* テーブルに移動されます。
- フィッシングメールレコードの作成：メール一致ルールが満たされている場合 (「ユーザーから報告されたフィッシングの取り込みルールのセットアップ」を参照)、フィッシングメールの作成受信アクションによってフィッシングメールレコードが作成されます。解析されたメールヘッダーは、cm*sn_si_phishing_email_header* テーブルに保存され、関連リストとしてフィッシングメールに関連付けられます。
- 類似のフィッシングレコードを単一のセキュリティインシデントに集計：ユーザーから報告されたフィッシングメールのセキュリティインシデントへの変換フローでは、フィッシングメールレコードからセキュリティインシデントを作成し、類似のレコードを単一のインシデントに集計します。このフローでは、必要に応じて集計条件を変更できます。

注:

- セキュリティインシデントレスポンス 9.0 より前のリリースで利用可能なユーザーから報告されたフィッシング受信アクションは無効化されました。セキュリティインシデントは、無効化された受信アクションによって作成されなくなりました。
- 新しい設計を有効にするには、Security Operations スポークアプリケーションをインストールする必要があります。これには、デフォルトで非アクティブ状況で提供される ユーザーから報告されたフィッシングメールのセキュリティインシデントへの変換 フローが含まれます。フィッシングメールレコードからセキュリティインシデントを作成するには、このフローをアクティブ化します。

次の画像は、古い設計と新しい設計の違いを示しています。



自動翻訳

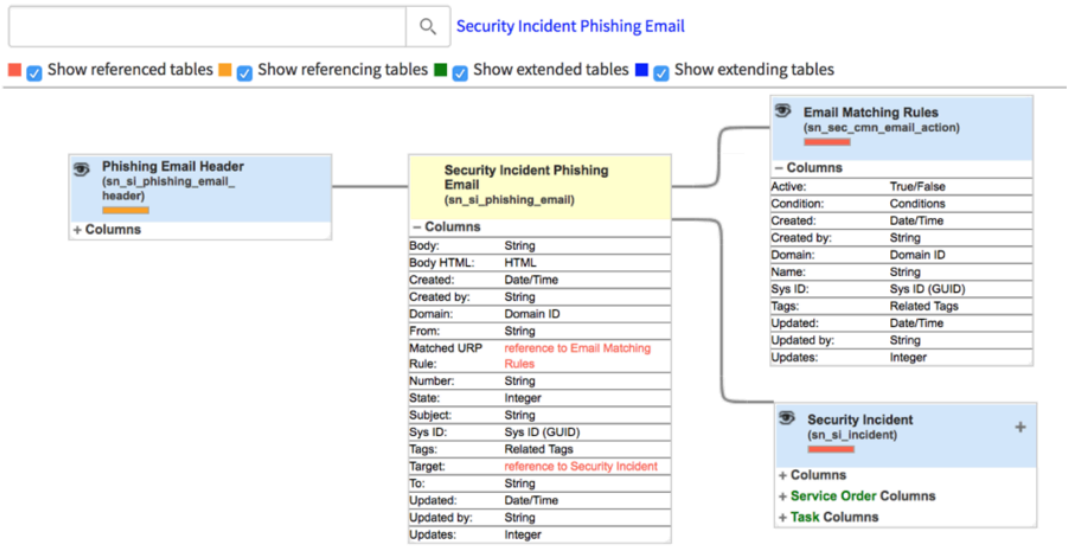
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

拡張されたユーザーから報告されたフィッシング機能を使用するには、次のプラグインとコンポーネントが必要です。

- Security Support Common (*sn_sec_cmn*)：含まれる内容：
  - 受信アクション
  - 新しい EmailUserReportedPhishing スクリプト
  - 取り込みルールテーブル
- セキュリティインシデントレスポンス (sn_si)：含まれる内容：
  - セキュリティインシデントテーブル (sn_si_incident)
  - セキュリティフィッシングメールテーブル (sn_si_phishing_email)
  - セキュリティフィッシングメールヘッダーテーブル (sn_si_phishing_email_header)
  - EML アップロードレコードプロデューサー
- Security Operations スポーク

  メールを集計し、フィッシングメールをセキュリティインシデントに変換するためのフローとサブフロー。

次の図は、新しいフィッシングメールテーブルと、対応する URP ルールとターゲットセキュリティインシデントレコード (sn_si_incident) への参照を示しています。



ユーザーから報告されたフィッシングの取り込みルールのセットアップ

sn_si.admin ロールを持つユーザーは、メール一致ルールを定義して、特定の基準に基づいてユーザーから報告されたフィッシングメールをフィルタリングできます。たとえば、直接または [フィッシングを報告] ボタンを介して *security@acme.com* に送信されたすべてのメールを「ユーザーから報告されたフィッシングメール」として分類するルールを定義できます。

始める前に

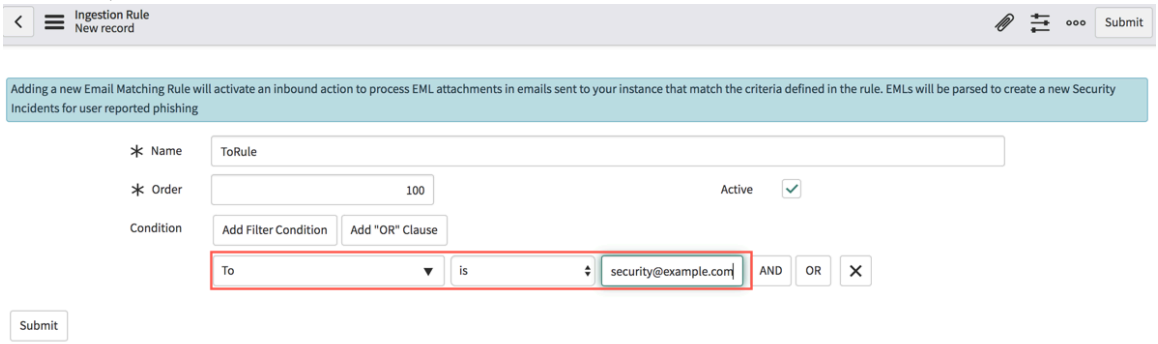
必要なロール：sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

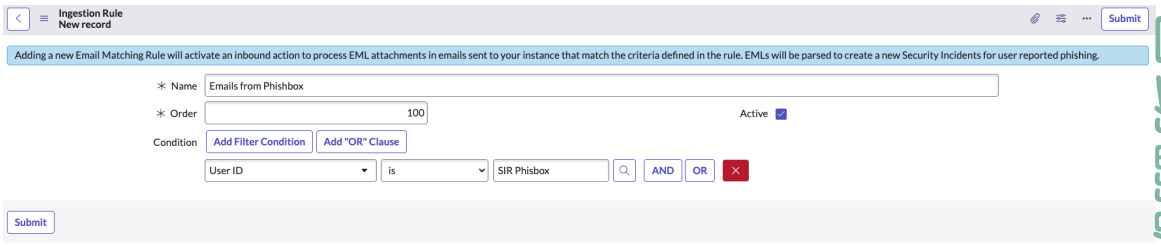
手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > メール処理 > 取り込みルール - ユーザーから報告されたフィッシング.
2. [新規] をクリックして、新しいメール一致ルールを作成します。
3. 名前を入力し、ルールの条件を 1 つ以上定義します。
4. [送信] をクリックしてルールを保存します。
   以下にいくつかのサンプルルールを示します。
   - **ToRule**：直接送信されたメール、または *security@example.com* メール ID に転送されたメールをフィルタリングしま



す。

   - ユーザー **ID** ルール：特定のメール ID から送信されたメールをフィルタリングしま



す。

自動翻訳

ユーザーから報告されたフィッシングプロパティの定義

ユーザーから報告されたフィッシングメールからキャプチャする必要があるヘッダー情報を定義します。

始める前に

必要なロール：sn_si.admin

このタスクについて

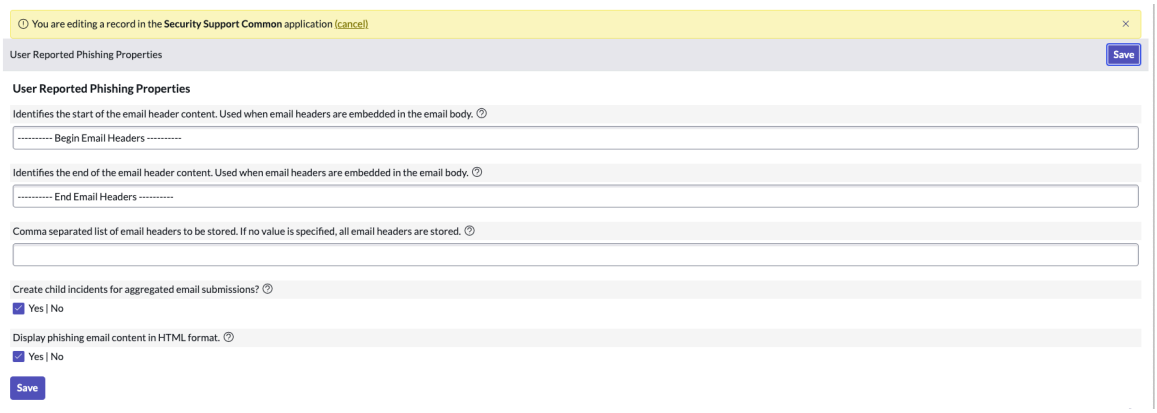
これらのオプションを使用して、次のようなユーザーから報告されたフィッシングの設定を構成します。

- メール本文からメールヘッダーを抽出するための構成 ([フィッシングを報告 **(Report Phish)**] による送信)
- ヘッダーを選択するフィルター
- 親子の関連付けの有効化または無効化

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > メール処理 > ユーザーから報告されたフィッシングプロパティ.



2. メール本文からメールヘッダーを抽出するための構成を指定します。
   - メールヘッダーの開始を識別する文字列を入力します。
   - メールヘッダーの終了を識別する文字列を入力します。

   > **注:**
   > これらの設定は、フィッシングメールのメール本文の一部としてキャプチャされたヘッダーにのみ適用されます。たとえば、**PhishAlarm** プラグイン (旧 Wombat) が Microsoft Outlook クライアントに構成されている場合、ユーザーが [フィッシングを報告 **(Report Phish)**] ボタンをクリックすると、ここで定義された構成に従ってメールヘッダーがキャプチャされます。フィッシングメールが添付ファイルとして転送された場合、ヘッダー情報はキャプチャされません。

3. セキュリティインシデントの調査に不要なヘッダーを除去するためのフィルターを指定します。

   ユーザーから報告されたフィッシングメールからキャプチャする必要があるメールヘッダーのリストをカンマ区切りで入力します。ここで何も値を指定しない場合、すべてのヘッダー情報がキャプチャされます。

4. 親子の関連付けの有効化または無効化
   デフォルトでは [はい] オプションが有効になっています。ユーザーから報告されたフィッシングメールを集計するときに子セキュリティインシデントを作成する必要があることを示す場合は、[はい] を選択します。[いいえ] を選択すると、子セキュリティインシデントは作成されませんが、ユーザーから報告されたフィッシングメールはセキュリティインシデントに関連付けられ、セキュリティインシデントレコードが更新されます。子セキュリティインシデントの作成方法の詳細については、「ユーザーから報告されたフィッシングメールのセキュリティインシデントへの変換」を参照してください。

5. フィッシングメールのコンテンツを HTML 形式で表示するオプションを有効または無効にします。
   デフォルトでは [はい] オプションが有効になっています。フィッシングメールのコンテンツを HTML 形式で表示するには、[はい] を選択します。[いいえ] を選択すると、HTML 形式のメールコンテンツはフィッシングレコード内に表示されません。

ユーザーが報告したフィッシングメールから作成されたフィッシングメールレコード

ユーザーが報告したフィッシングメールは、定義されているメール一致ルールに基づいて、セキュリティインシデントに変換されます。

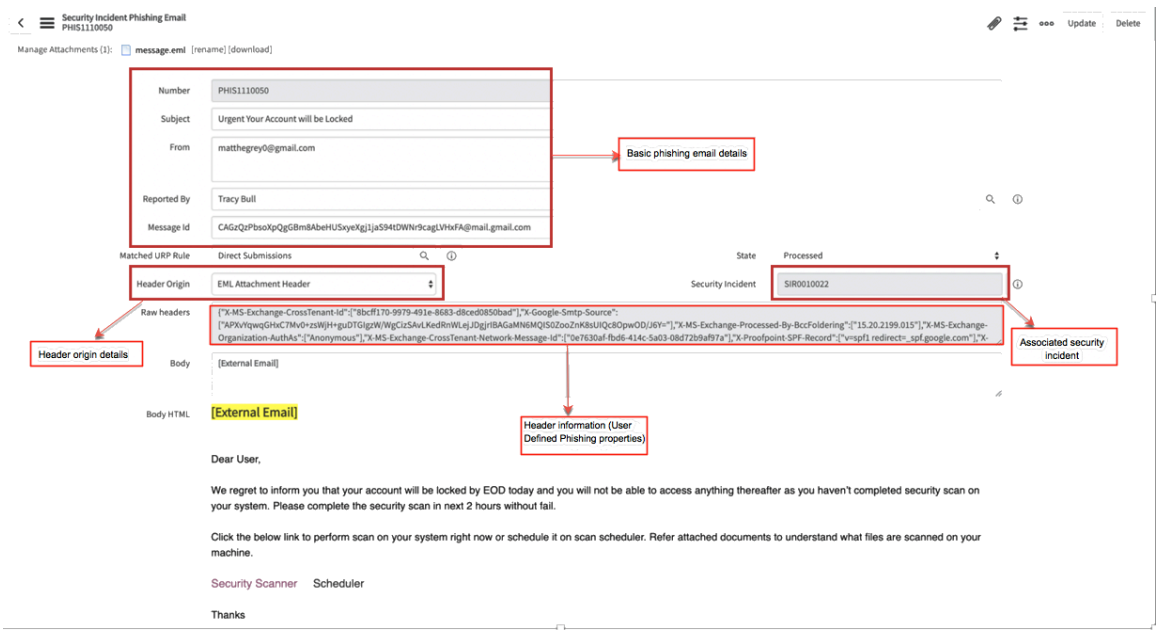
新しいフィッシングメールが報告されると、次のアクションが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- *sys_email* テーブルにメールレコードが作成されます。
- [フィッシングメールの作成] 受信アクションはメールレコードで実行され、メール一致ルール (「ユーザーから報告されたフィッシングの取り込みルールのセットアップ」を参照) を使用してフィッシングメールかどうかを判定します。
- フィッシングメールとして識別されると、sn_si_phishing_email テーブルにフィッシングメールレコードが作成されます。
- 最後に、「ユーザーから報告されたフィッシングメールのセキュリティインシデントへの変換」のフローが適用され、フィッシングメールレコードがセキュリティインシデントに変換されます。

メールの詳細を表示するには、次に移動します: セキュリティインシデント > すべてのフィッシングメールを表示. フィッシングメールレコードのリストが表示されます。[作成日時] 列の日付リンクをクリックして、メールレコードを表示します。

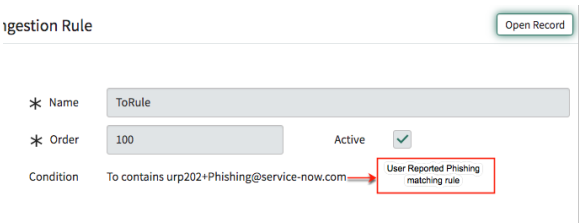


セキュリティインシデントフィッシングメールの詳細

フィールド名	説明
数値	ユーザーが報告したフィッシングメールにアサインされた番号。
件名	メールの件名。件名ルールは、シミュレートされたフィッシングキャンペーンやテストに役立ちます。この場合、フィッシングや同様のメール攻撃への対応をテストするために、組織は偽のメールを自社のスタッフに送信します。 シミュレートされたフィッシングメールテストで、**PhishAlarm** プラグイン (旧称「Wombat」) を備えた Microsoft Outlook メールクライアントが使用されている場合、ユーザーは [フィッシングを報告 **(Report Phish)]** ボタンをクリックしてフィッシングメールを報告できます。メールは、件名に「**Simulated Phishing**」が追加された状態で Security Operations チームに送信されます。これは、メールがシミュレートされたフィッシングメールであることを識別するために使用されます。
送信元	このフィッシングメールの送信元のメールアドレス。この情報は、フィッシングメールが .EML ファイルの添付ファイルとして転送された

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

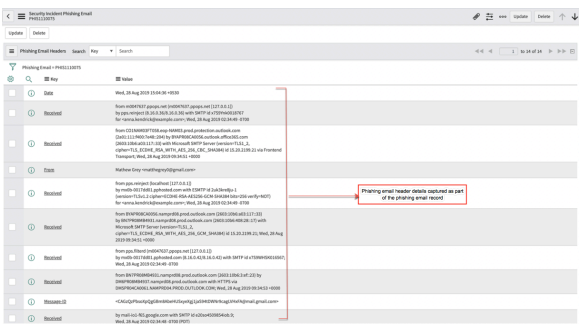
セキュリティインシデントフィッシングメールの詳細 (続く)

フィールド名	説明
	場合、または元のヘッダーがメールに埋め込まれている場合に利用できます。 ユーザーがフィッシングメールを直接転送した場合、送信元アドレスを使用できない可能性があります。
報告者	このフィッシングメールを報告したユーザーのメール ID。[情報] アイコンをクリックすると、追加の詳細が表示されます。
メッセージ ID	メッセージにアサインされた ID。
一致する URP ルール (Matched URP rule)	このメールに適用される、「ユーザーから報告されたフィッシング」ルール。[情報] アイコンをクリックすると、追加の詳細が表示されます。
 ご覧のように、この例では、このメールに ToRule が適用され、セキュリティインシデントが作成されていることが [条件] フィールドに示されています。メール一致ルールの定義の詳細については、「ユーザーから報告されたフィッシングの取り込みルールのセットアップ」を参照してください。	
ステータス	sn_si_phishing_email テーブルに新しいフィッシングメールレコードが作成されると、[ステータス (State)] フィールドが [新規] に設定されます。このメールレコードがセキュリティインシデントに変換されると (「ユーザーから報告されたフィッシングメールのセキュリティインシデントへの変換」を参照)、 [ステータス (State)] フィールドは [処理済み] に更新されます。
ヘッダーの作成元	このフィールドは、メールヘッダーがどのように生成されたか、またはユーザーがフィッシングメールをどのように報告したかを示します。 • メールヘッダー：ユーザーがセキュリティオペレーションチームにフィッシングメールを転送しました。 • メールテキスト本文： ○ ユーザーが [フィッシングを報告 **(Report Phish)]** オプションをクリックしました (**PhishAlarm** プラグイン (旧称「Wombat」) がメールクライアントで構成されている場合)。 ○ 定義済みの「ユーザーから報告されたフィッシング」ルールに基づいて、フィッシングメールが Security Operations チームに転送されます。 • **EML** 添付ファイルヘッダー：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントフィッシングメールの詳細 (続く)

フィールド名	説明
	○ 添付ファイル：ユーザーがメールを添付ファイル (.EML ファイル) として転送しました。 ○ サービスカタログの送信：ユーザーがメールを .EML ファイルとしてデスクトップにダウンロードし、指定した場所にアップロードしました。その後、セキュリティインシデントがメールから作成されます。 • **EML** 添付ファイル本文： ○ ユーザーが [フィッシングを報告 **(Report Phish)**] オプションをクリックしました (**PhishAlarm** プラグイン (旧称「Wombat」) がメールクライアントで構成されている場合)。 ○ 定義済みの「ユーザーから報告されたフィッシング」ルールに基づいて、フィッシングメールが添付ファイルとして Security Operations チームに転送されます。
セキュリティインシデント	ユーザーから報告されたフィッシングメールの最初の報告時には、このフィールドは空白です。「ユーザーから報告されたフィッシングメールのセキュリティインシデントへの変換」フローが実行されると、このメールはセキュリティインシデントレコードに変換され、そのレコードの番号がここに表示されます。
生のヘッダー	このフィールドには、「ユーザーから報告されたフィッシングプロパティの定義」ページで定義されているメールから抽出された完全なヘッダー情報が表示されます。ヘッダーはキーと値のペアに解析され、フィッシングメールヘッダーリストに表示されます。
	
本文	これは、ユーザーから報告されたフィッシングメールの本文です。

ユーザーから報告されたフィッシングメールのセキュリティインシデントへの変換

[フィッシングメールをセキュリティインシデントに変換 **(Transform Phishing Email to Security Incident)**] フローは、フィッシングメールレコードをセキュリティインシデントに変換する新しいフローです。

始める前に

注:
ユーザーから報告されたフィッシング機能を有効にするには、フローのコピーを作成してアクティブにする必要があります。ユーザーから報告されたフィッシング送信を処理するためのカスタムインバウンドアクションとカスタムフローを作成している場合は、ここで説明するフローの変更は必要ありません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

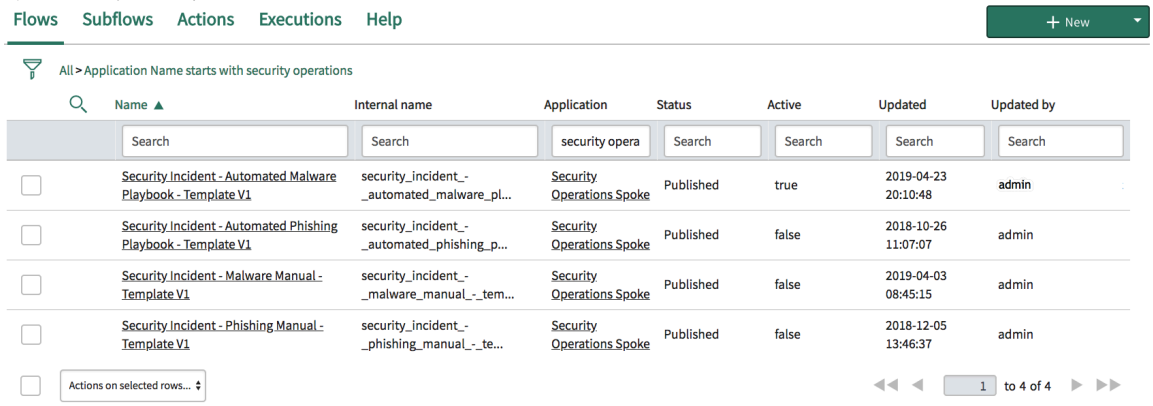
- 必要なロール：sn_si.admin
- フローデザイナースポークをインストールする必要があります。

このタスクについて
このフローは、ステータスが [新規] に設定されている、ユーザーから報告されたフィッシングメールレコードが作成されたときに自動的に起動します。このフローには、以下を実行するロジックが含まれています。

- セキュリティインシデントの集計
- 関連するメモによるセキュリティインシデントの更新
- ヘッダーデータの追加
- 必要に応じた子インシデントの作成

手順

- 次のように移動する。 **Flow Designer** > デザイナー をクリックして、Security Operations スポークで利用可能なフローを表示します。

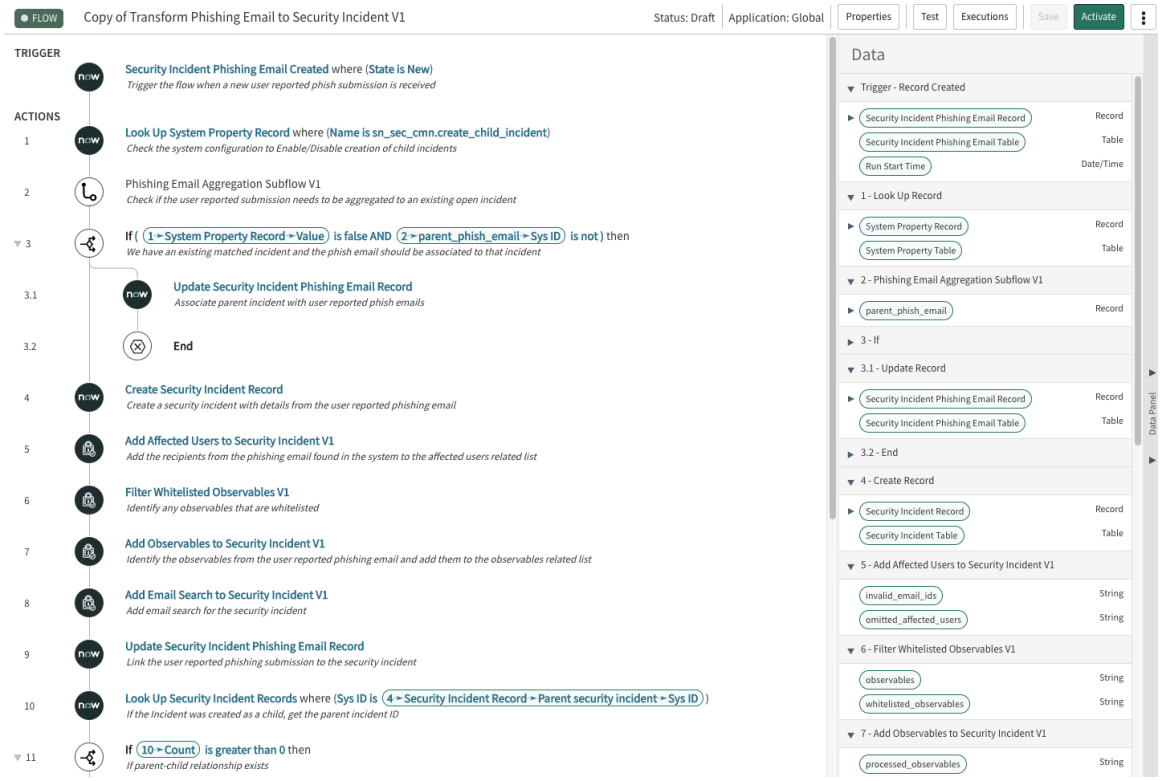


- [フィッシングメールをセキュリティインシデントに変換 **(Transform Phishing Email to Security Incidents)]** リンクをクリックしてフローを表示します。
- このフローはベースシステムで提供されますが、[読み取り専用] モードであるため使用できません。
  詳細アイコン をクリックしてフローのコピーを作成し、それを開いて使用します。これで、トリガー条件やアクションの変更、アクションの追加や削除など、フローを変更できるようになりました。必要な変更を行った後、フローをアクティブ化して、実行できるように

自動翻訳

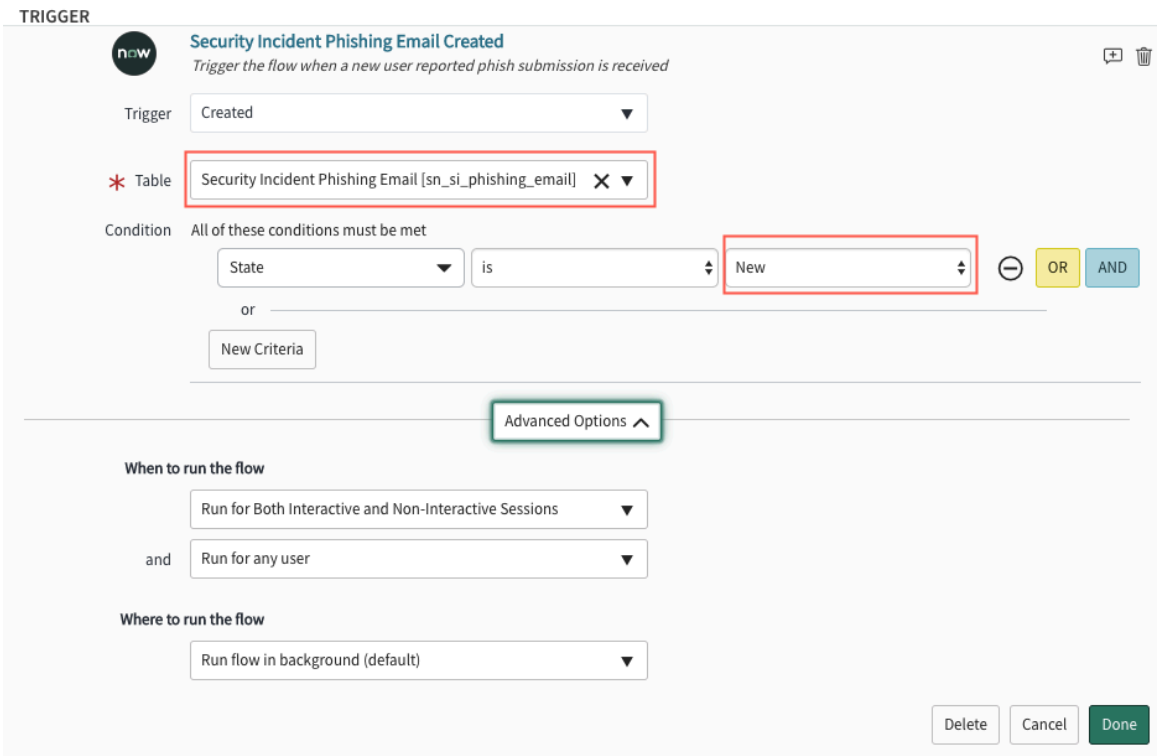
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

する必要があります (「セキュリティインシデントレスポンス フローのアクティブ化」を参照)。



この図は、トリガーおよびフローで実行されるステップを示しています。右側のパネルにはデータフローが表示されています。アイコンをクリックすると、ステップが展開され、詳細が表示されます。

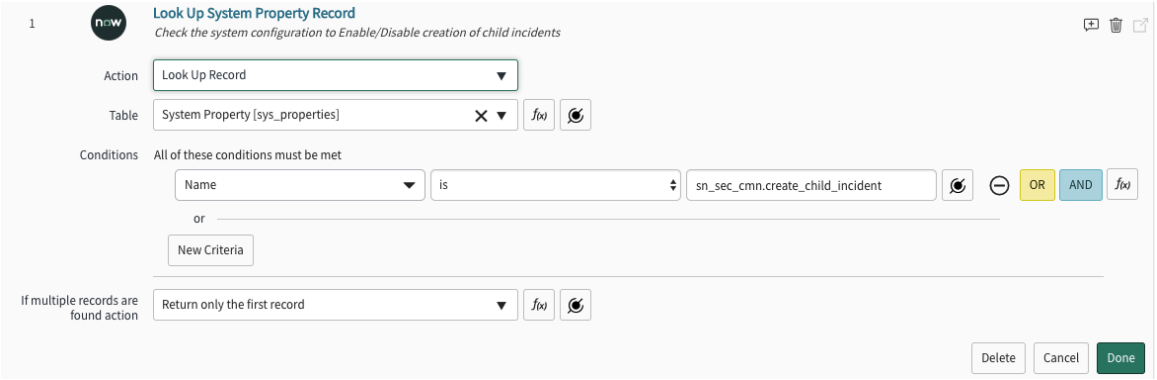
- [トリガー] アイコンをクリックします。
最初のステップでは、フローのトリガーを定義または設定します。条件が満たされたときに実行されるトリガーとタスクの条件を指定します。このフローは、[新規] レコードが sn_si_phishing_email テーブルにアップロードされると開始されます。



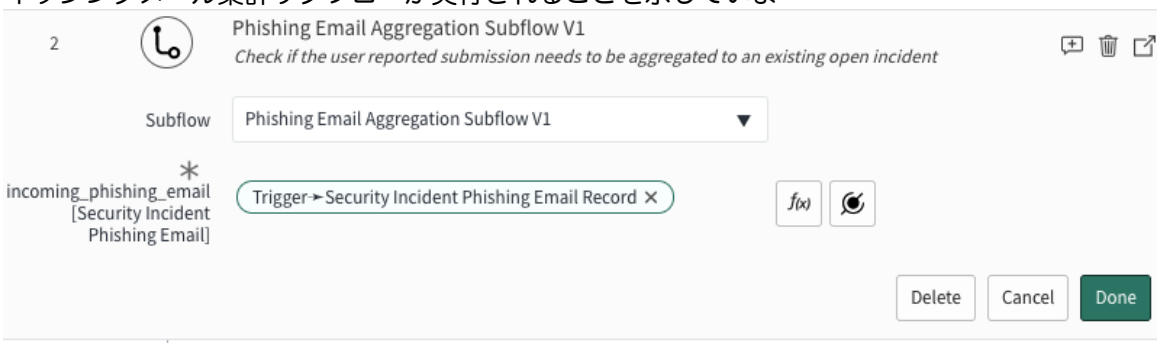
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ステップ 1 では、フローは「ユーザーから報告されたフィッシングメールのセキュリティインシデントへの変換」ページの [集計されたメール送信の子インシデントを作成しますか？] フラグが有効か無効かを確認します。

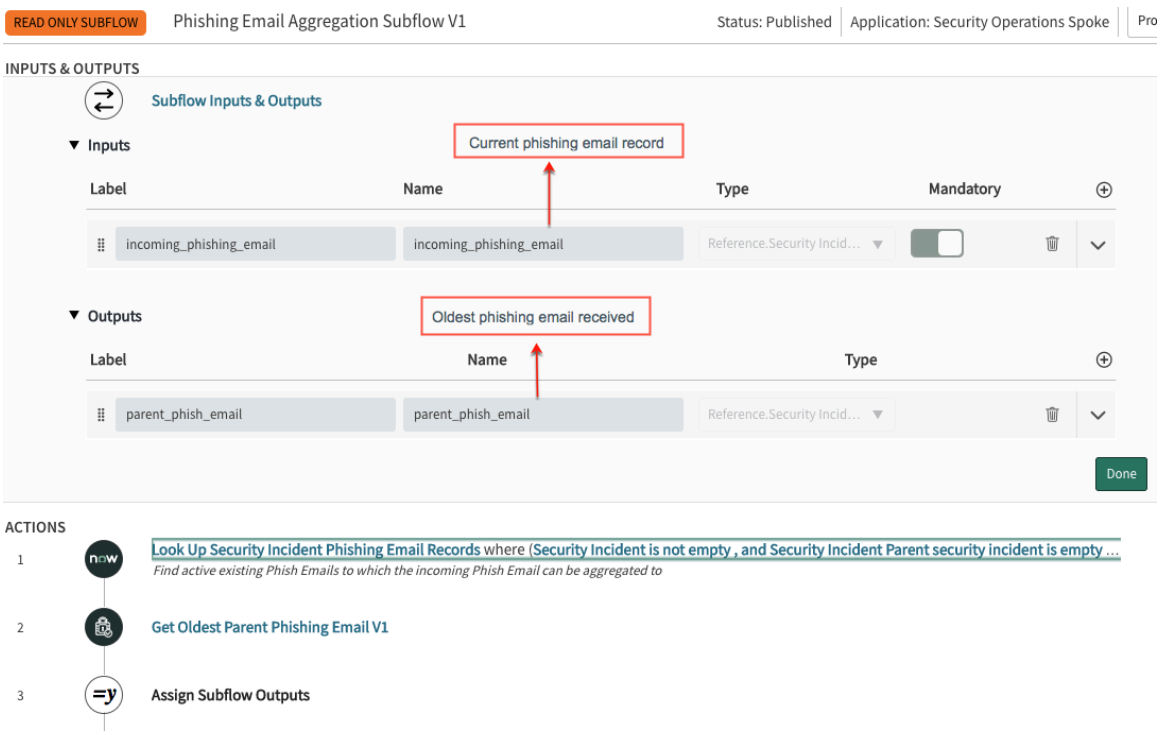


- ステップ 2 では、最も古い親セキュリティインシデントを特定します。ステップ 2 のアイコンに注目してください。このステップの一部としてフィッシングメール集計サブフローが実行されることを示していま



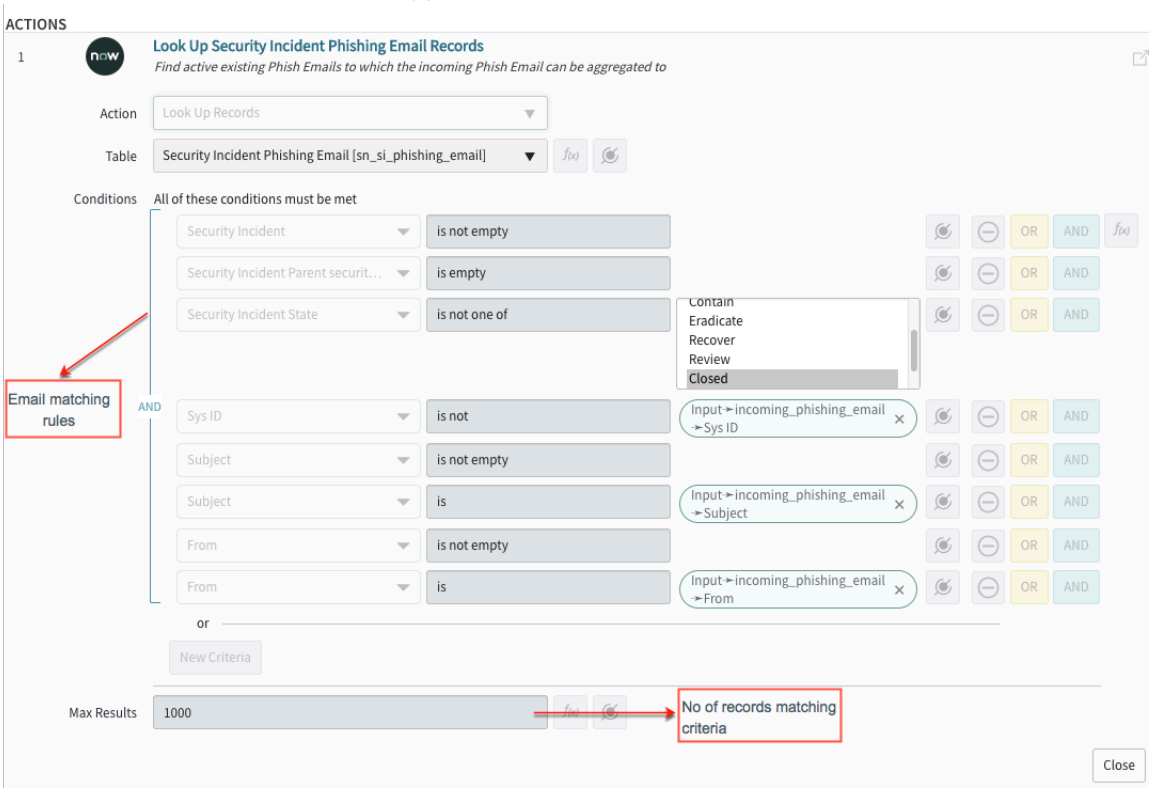
す。

アクションデザイナーアイコンをクリックして、アクションの詳細ビューを確認します。このサブフローはフィッシングメールをチェックし、指定された基準に基づいて既存のセキュリティインシデントと照合します。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このサブフローが実行されると、これら 2 つのアクションが実行されます。最初のアクションのリンクをクリックすると、追加の詳細が表示されます。

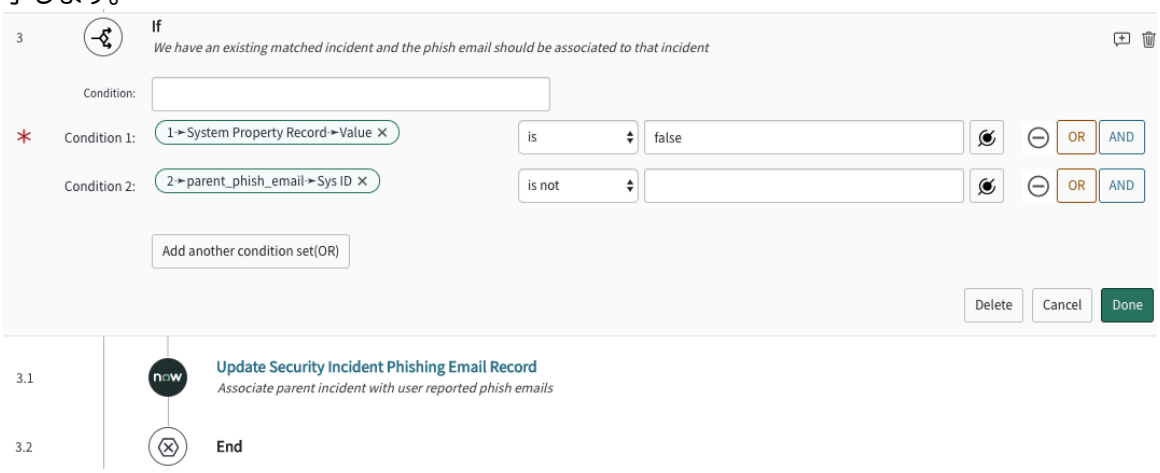


このアクションは、次のような条件に基づいて、新しい受信メールの基準に一致するメールをチェックします。

- セキュリティインシデントのステータスが [クローズ済み] ではない。
- [件名] または [差出人] の値が、定義されたメール一致ルール条件と一致している (「ユーザーから報告されたフィッシングの取り込みルールのセットアップ」を参照)。

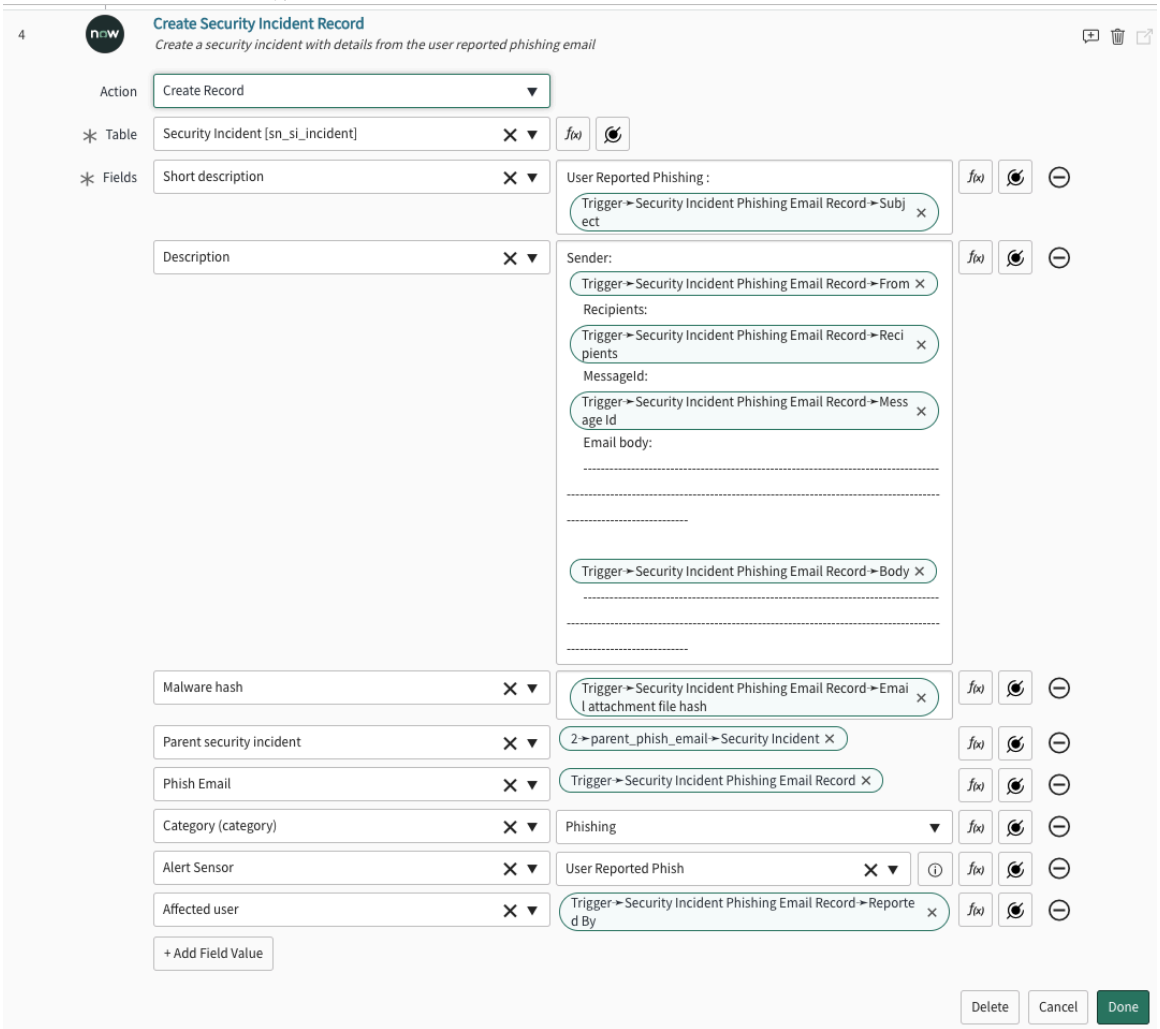
これらの条件が満たされると、基準に一致するレコードの数が [結果の最大数] フィールドに表示されます。リスト内の最も古いレコードまたは最初のレコードが、セキュリティインシデントが集計される親レコードとして指定されます。

- ステップ 3 は、「ユーザーから報告されたフィッシングメールのセキュリティインシデントへの変換」ページの [集計されたメール送信の子インシデントを作成しますか？] フラグが [いいえ] に設定されている場合のみ適用されます。
この場合、フィッシングメールがセキュリティインシデントレコードに関連付けられ、フローは終了します。

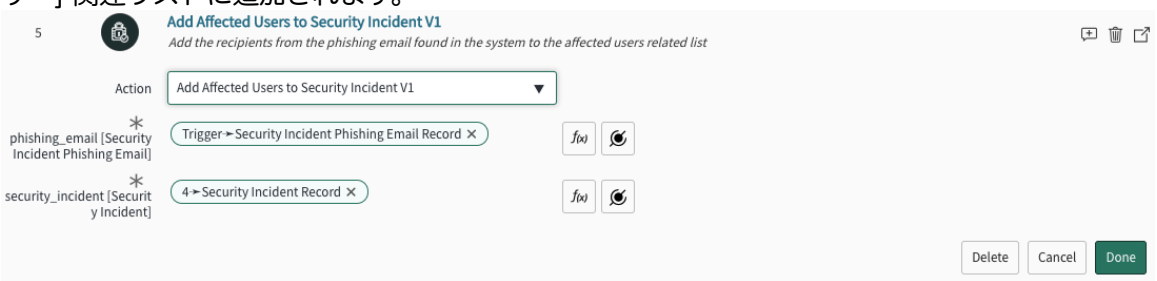


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [集計されたメール送信の子インシデントを作成しますか？] フラグが [はい] に設定されている場合、フローは実行を続行し、ユーザーから報告されたフィッシングメールに基づいて新しいセキュリティインシデントが作成されます。

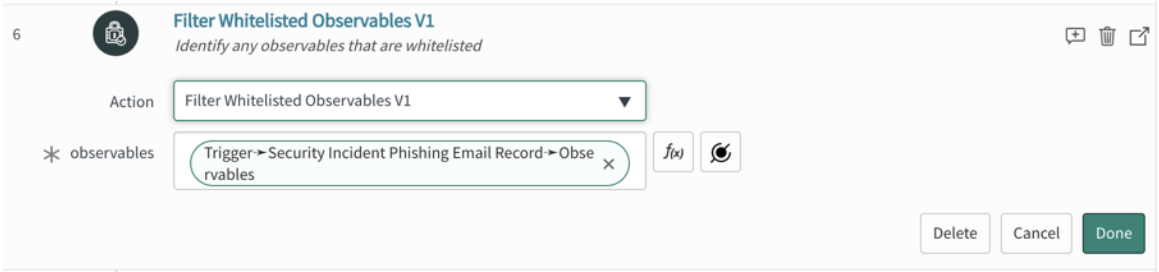


- ステップ 5 で、フィッシングメールを受信したユーザー (フィッシングメールの [宛先] および [CC] リストに含まれる従業員) が、セキュリティインシデントレコードの [影響を受けるユーザー] 関連リストに追加されます。

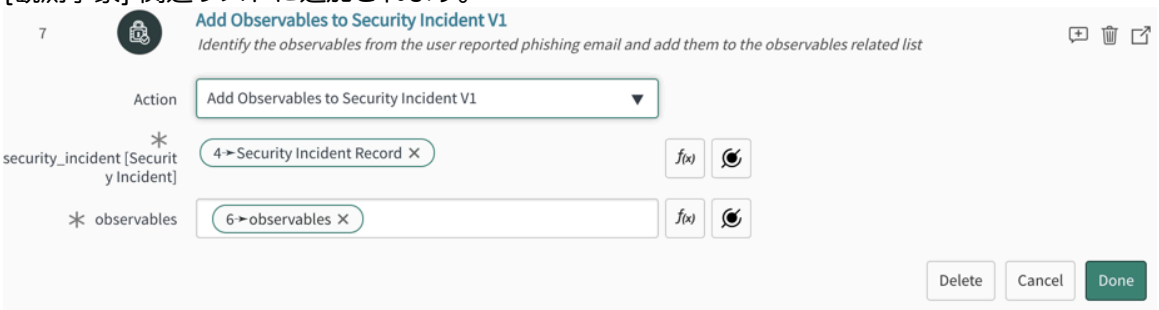


- ステップ 6 では、セキュリティインシデントの観測事象のリストから、許可リストに含まれる観測事象がフィルタリングされます。
これらの許可リストの観測事象は、セキュリティインシデントに追加されません。

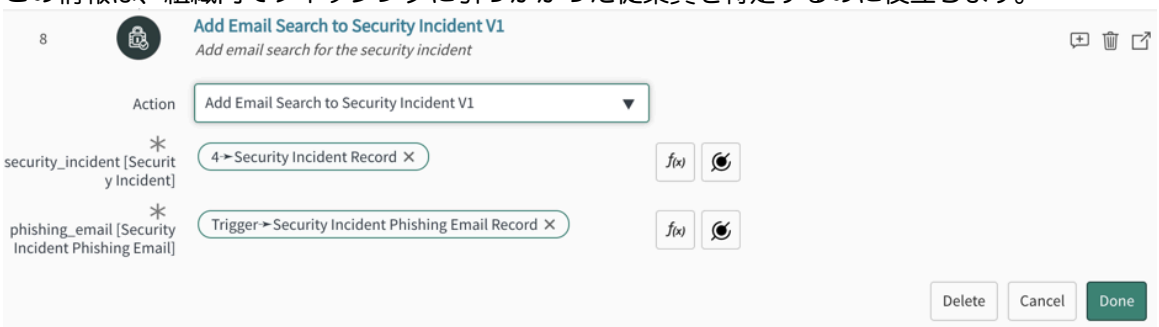
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



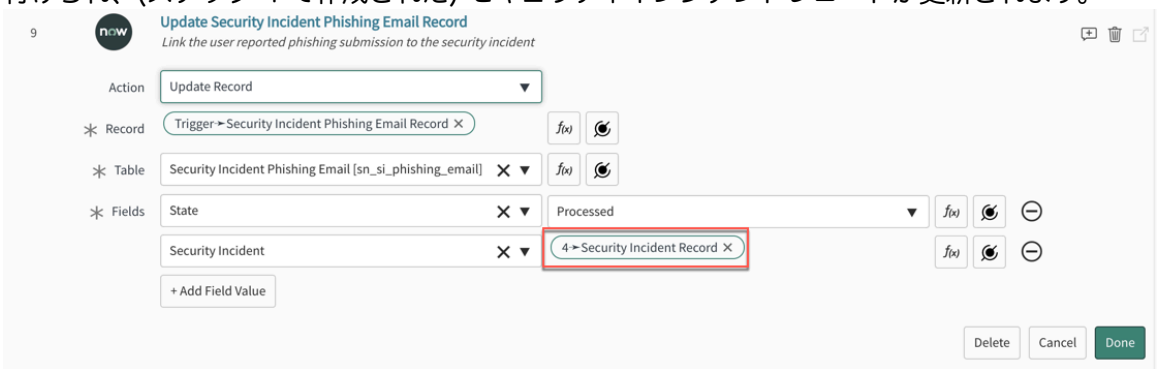
- ステップ 7 では、ユーザーから報告されたフィッシングメールから不明な観測事象が識別され、[観測事象] 関連リストに追加されます。



- ステップ 8 では、メールの件名と送信元アドレスを組み合わせたメール検索クエリが生成されます。
この情報は、組織内でフィッシングに引っかかった従業員を特定するのに役立ちます。



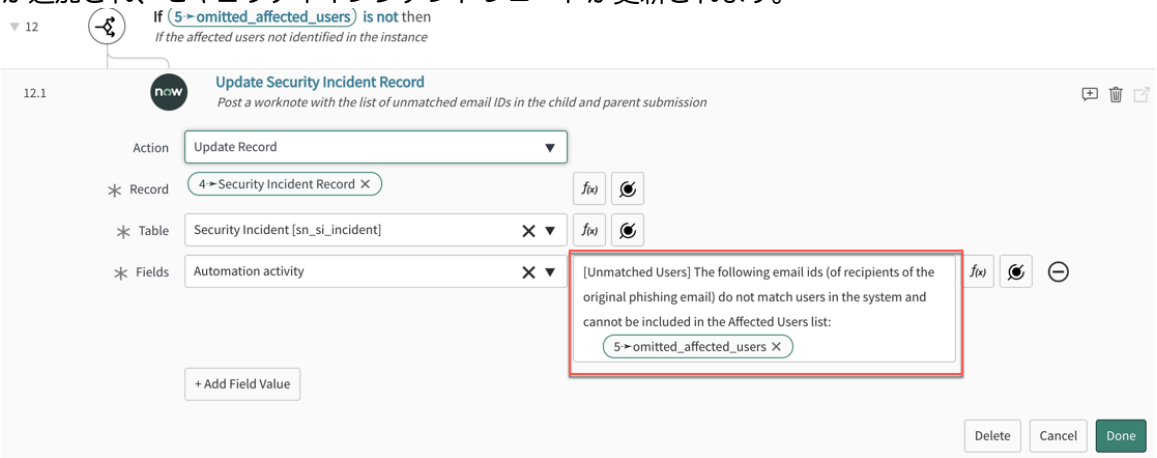
- ステップ 9 では、ユーザーから報告されたフィッシングメールがセキュリティインシデントに関連付けられ、(ステップ 4 で作成された) セキュリティインシデントレコードが更新されます。



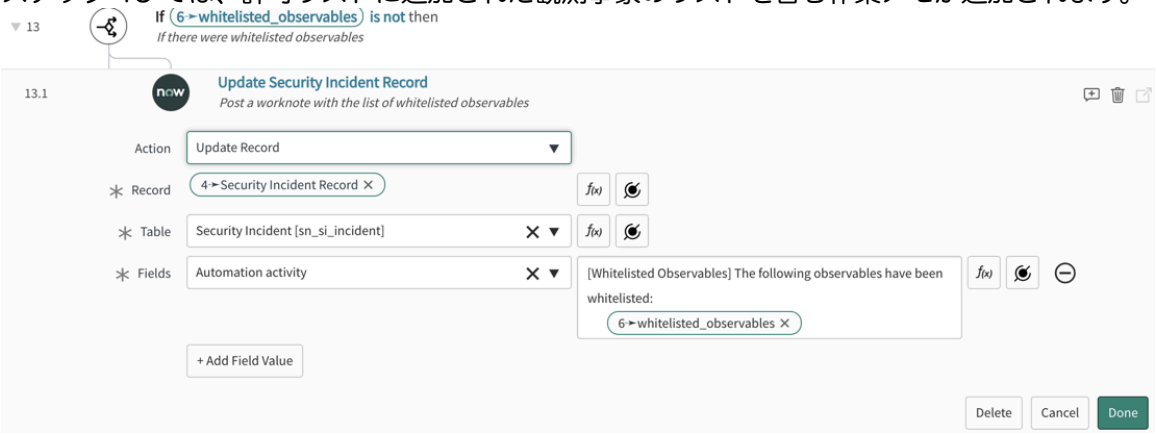
- ステップ 10 では、親セキュリティインシデントが特定され、オープンセキュリティインシデントレコードであるかどうかが確認されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 親セキュリティがアクティブな場合、子と親のセキュリティインシデントレコードに、それらが互いにどのように関連付けられているかを示すメモが追加されます。
- ステップ 12 では、影響を受けるユーザーが見つからない場合 (ステップ 5 のフロー)、作業メモが追加され、セキュリティインシデントレコードが更新されます。



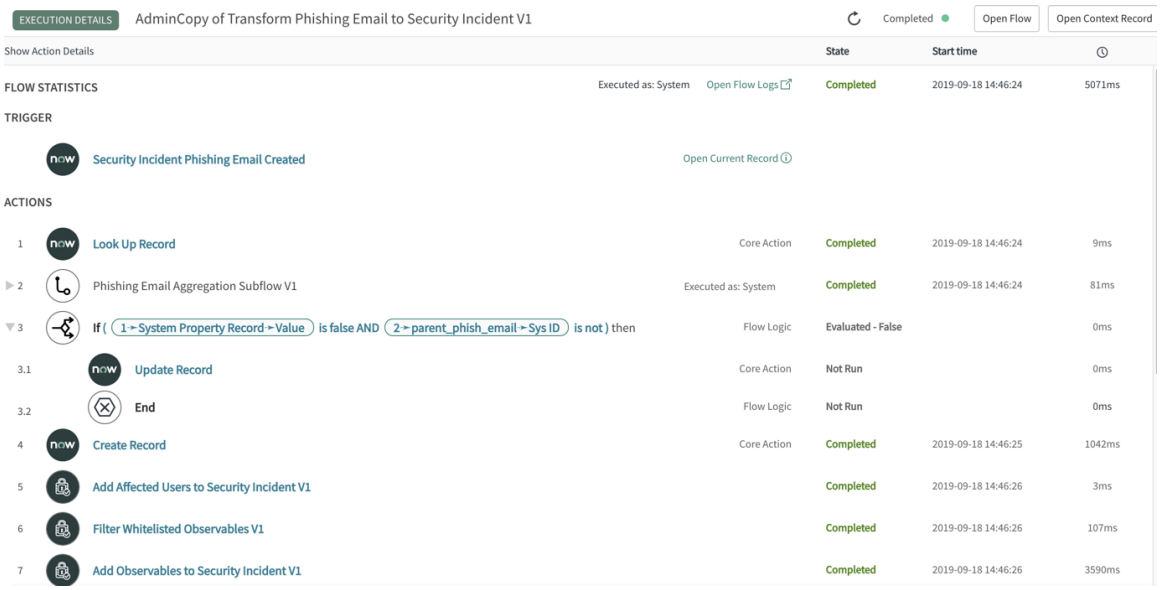
- ステップ 13 では、許可リストに追加された観測事象のリストを含む作業メモが追加されます。



次のタスク
[テスト] をクリックすると、公開される前にフロー内のアクションをシミュレートできます。フローをテストした後、[アクティブ化] をクリックしてフローをアクティブ化して、実行できるようにします。

[実行] をクリックして、フローの実行の詳細を表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

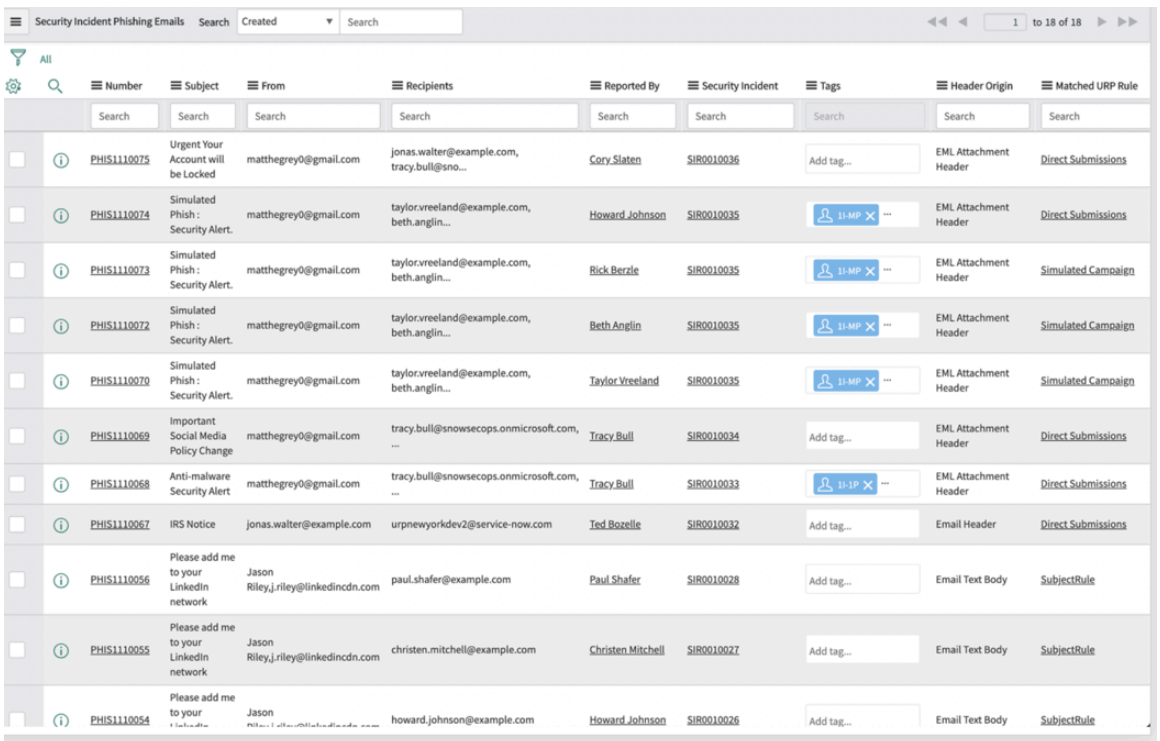


フローが実行されると、フィッシングメールレコードはセキュリティインシデントに変換されます。「フィッシングメールレコードから作成されたセキュリティインシデントレコード」を参照してください。

フィッシングメールレコードから作成されたセキュリティインシデントレコード

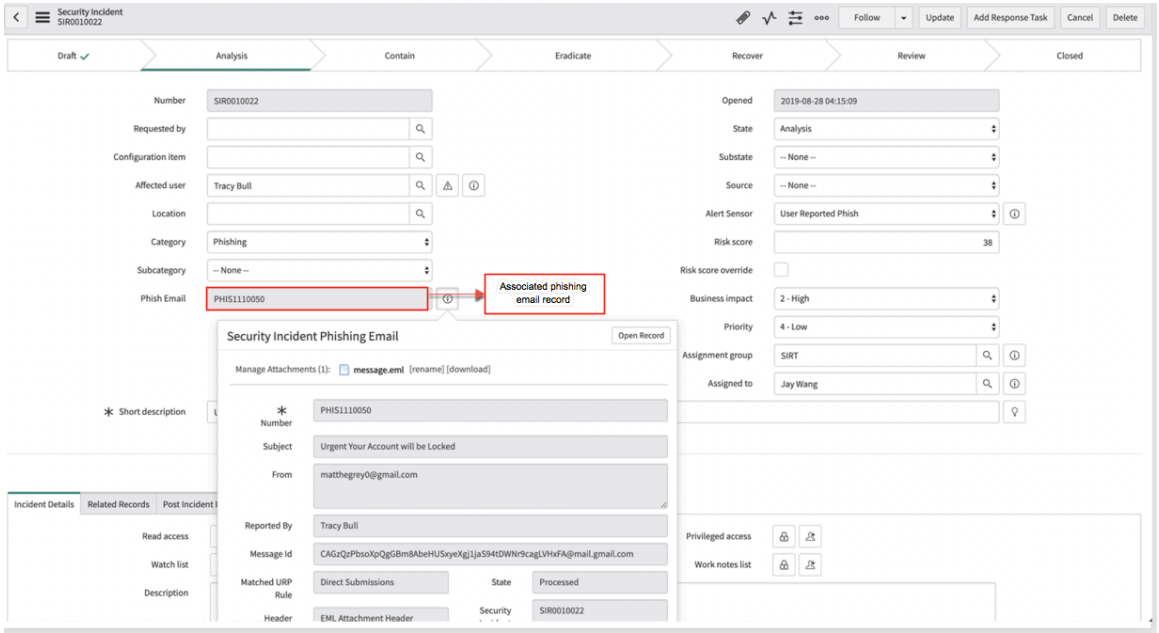
sn_si_Phishing_email テーブルに格納されているフィッシングメールレコードは、セキュリティインシデントレコードに変換されます。

フィッシングメールレコードに関連付けられたセキュリティインシデントを表示するには、次をクリックします セキュリティインシデント > フィッシングメール > すべてのフィッシングメールを表示.



フィッシングメールレコードに関連付けられた [セキュリティインシデント] 列のリンクをクリックします。セキュリティインシデントの詳細が表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



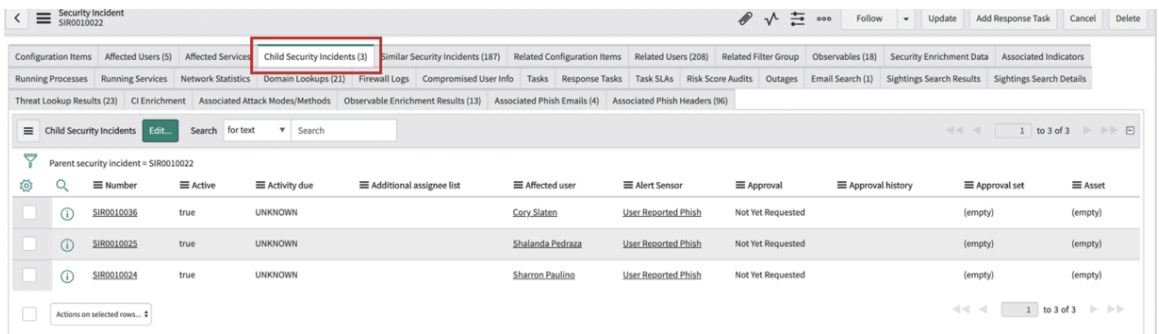
関連リスト

下へスクロールしてセキュリティインシデントの [関連リンク] セクションに移動し、[すべての関連リストを表示] をクリックします。子セキュリティインシデント、影響を受けるユーザー、関連付けられたフィッシングメールなどの詳細を表示します。

子セキュリティインシデント

[子セキュリティインシデント] タブをクリックします。適用された集計ロジックに基づいて、親セキュリティインシデントに関連付けられた子セキュリティインシデントのリストを表示できます。追加されたすべての子レコードに対して、自動化システムアクティビティが親レコードに追加されます ([作業メモ] セクション)。これにより、集計された子レコードについてセキュリティアナリストに通知されます。

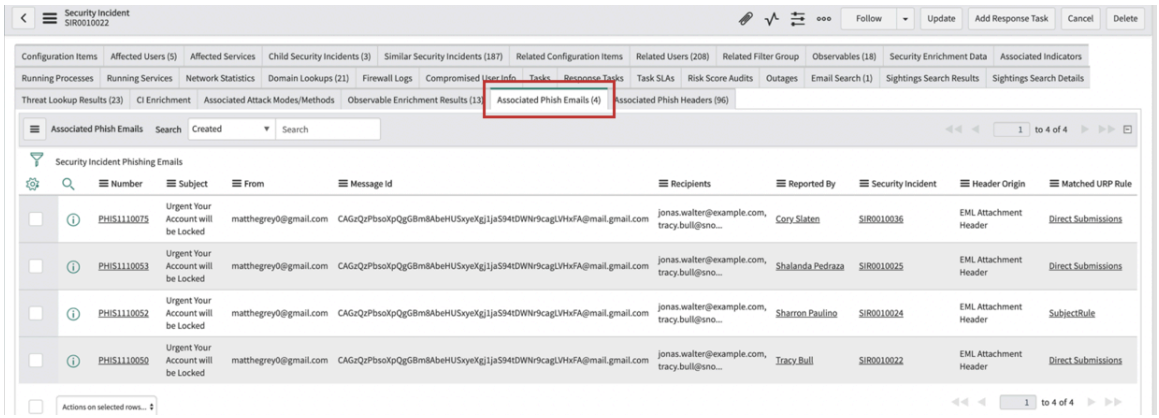
注:
ここで子セキュリティインシデントを表示できるのは、[ユーザーから報告されたフィッシングプロパティ] ページで [集計されたメール送信の子インシデントを作成しますか？] フラグが [はい] に設定されている場合のみです。詳細については、「ユーザーから報告されたフィッシングプロパティの定義」を参照してください。



関連フィッシングメール

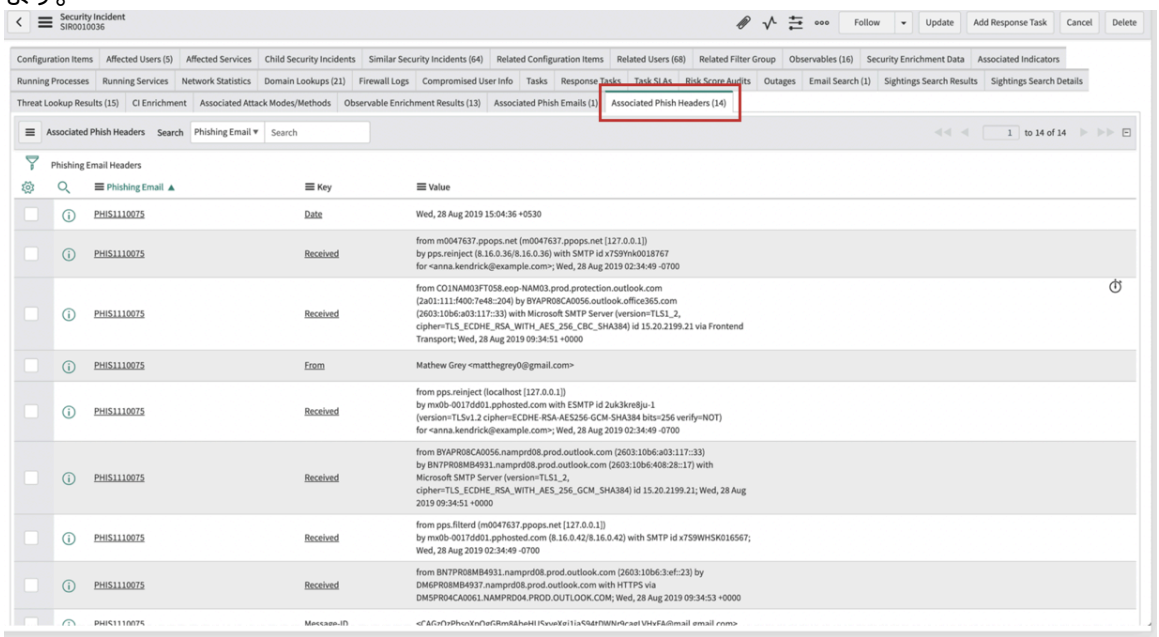
[関連フィッシングメール] タブをクリックします。親フィッシングメールレコードに関連付けられたフィッシングメールレコード (重複レコード) のリストが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



関連フィッシングメールヘッダー

[関連フィッシングメール] タブをクリックします。セキュリティインシデントの一部としてキャプチャされたフィッシングメールヘッダーの詳細が表示されます。親セキュリティインシデントに集計されたすべての子レコードのロールアップされたヘッダーとフィッシングメールレコードを表示できます。



許可リスト観測事象

ユーザーから報告されたフィッシングメールのセキュリティインシデントへの変換フローの実行時、セキュリティインシデントのステータスを監視できます。特定の観測事象が許可リスト観測事象としてマークされている場合、その観測事象は [観測事象] 関連リストに追加されません。観測事象を許可リストにマークすることで、重要な詳細のみが表示されるようにすることができます。たとえば、www.google.com が許可リストとしてタグ付けされた URL の 1 つである場合、次のシステムメッセージが表示されます。許可リスト観測事象により、重要な観測事象のみが監視されるようになります。

不一致ユーザーのキャプチャ

フィッシングメールの宛先および CC リスト内の一部のメール ID が組織内のユーザーに属していない場合があります。これらのメール ID は、不一致ユーザーとして分類され、[影響を受けるユーザー] 関連リストに含まれません。これらが不一致ユーザーであることを示す作業メモが表示されます。

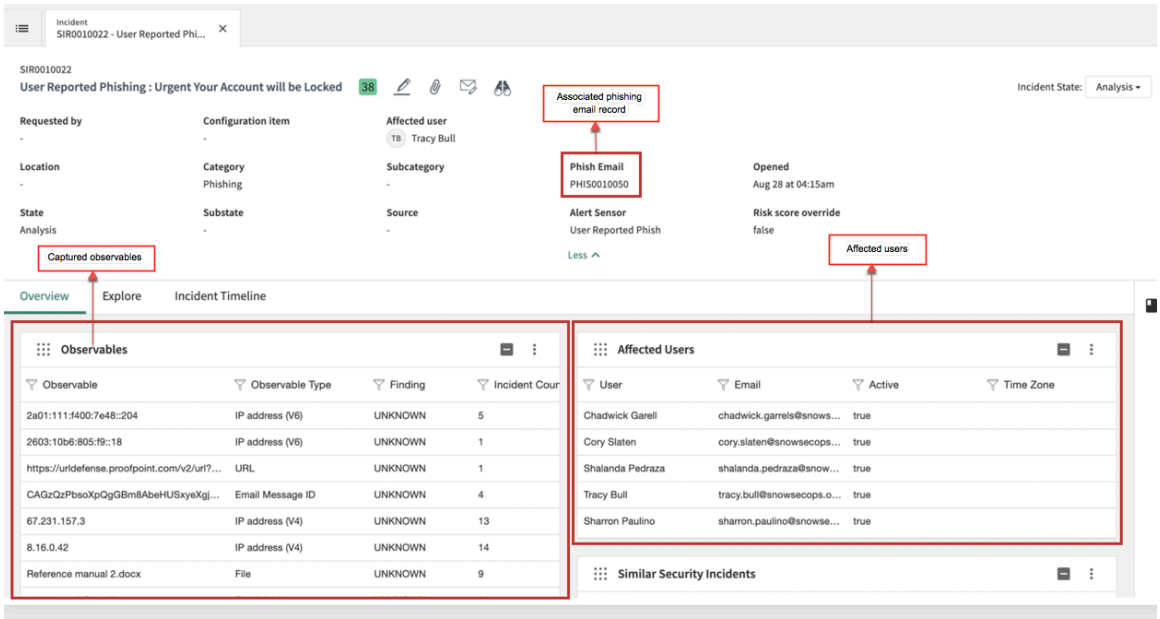
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

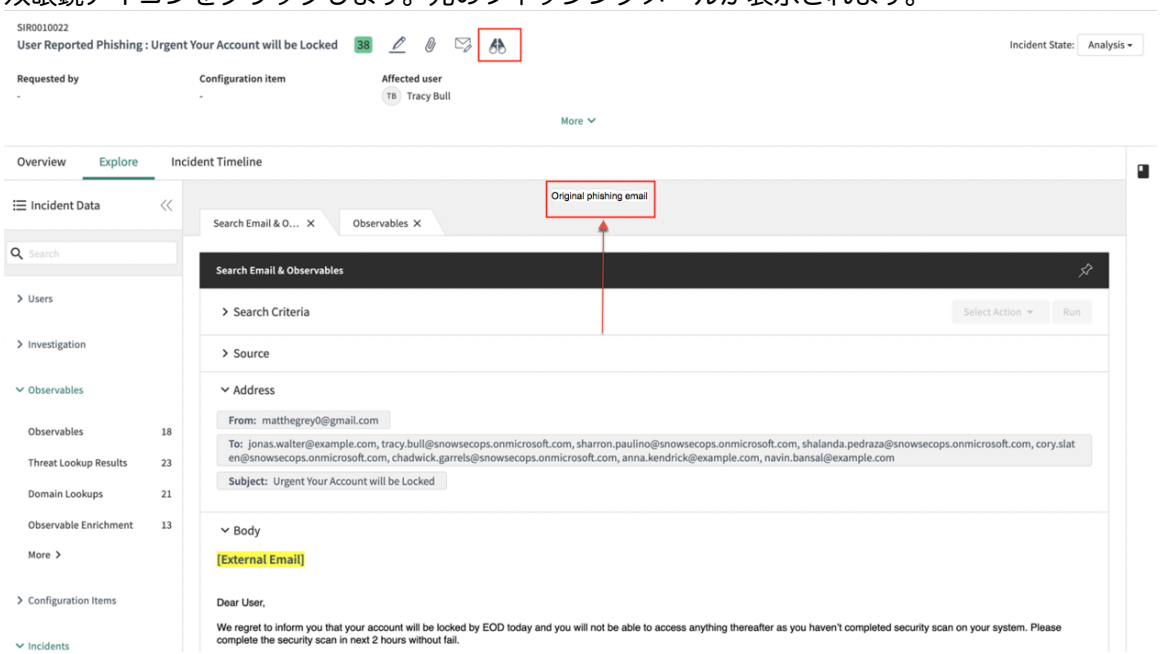
セキュリティアナリストワークスペースでのユーザーから報告されたフィッシング

フィッシングメールレコードに関連付けられたセキュリティインシデントはセキュリティアナリストワークスペースに表示できます。

次のように移動する。 セキュリティインシデント > 新しい **UI**. ワークスペースが別のブラウザータブで開きます。フィッシングメールレコードに関連付けられたセキュリティインシデントをクリックすると、セキュリティインシデントが表示されます。



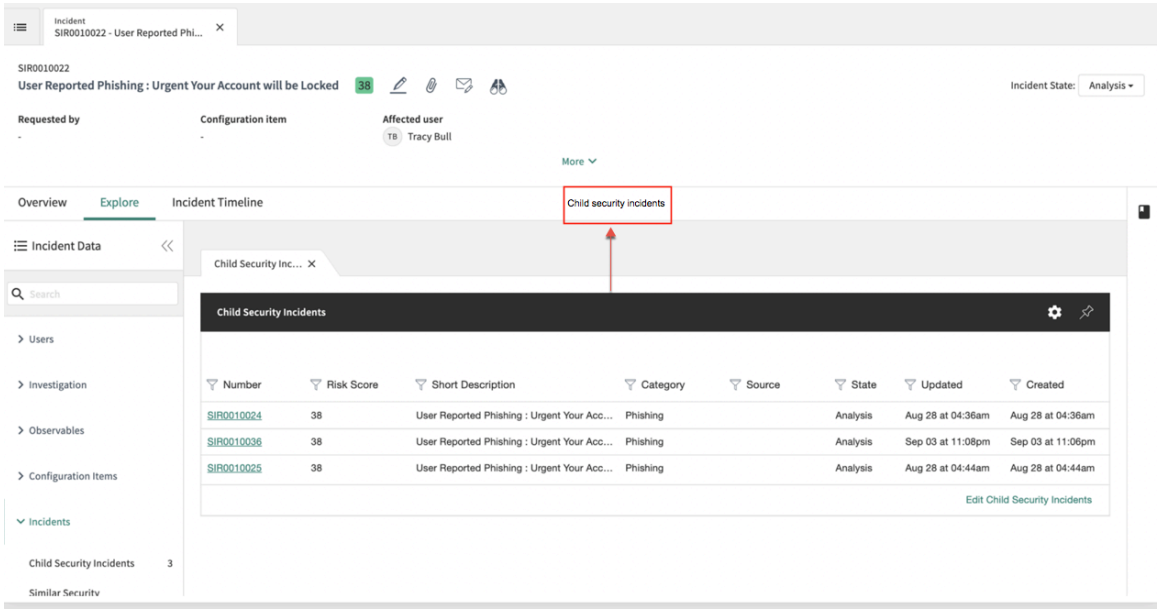
双眼鏡アイコンをクリックします。元のフィッシングメールが表示されます。



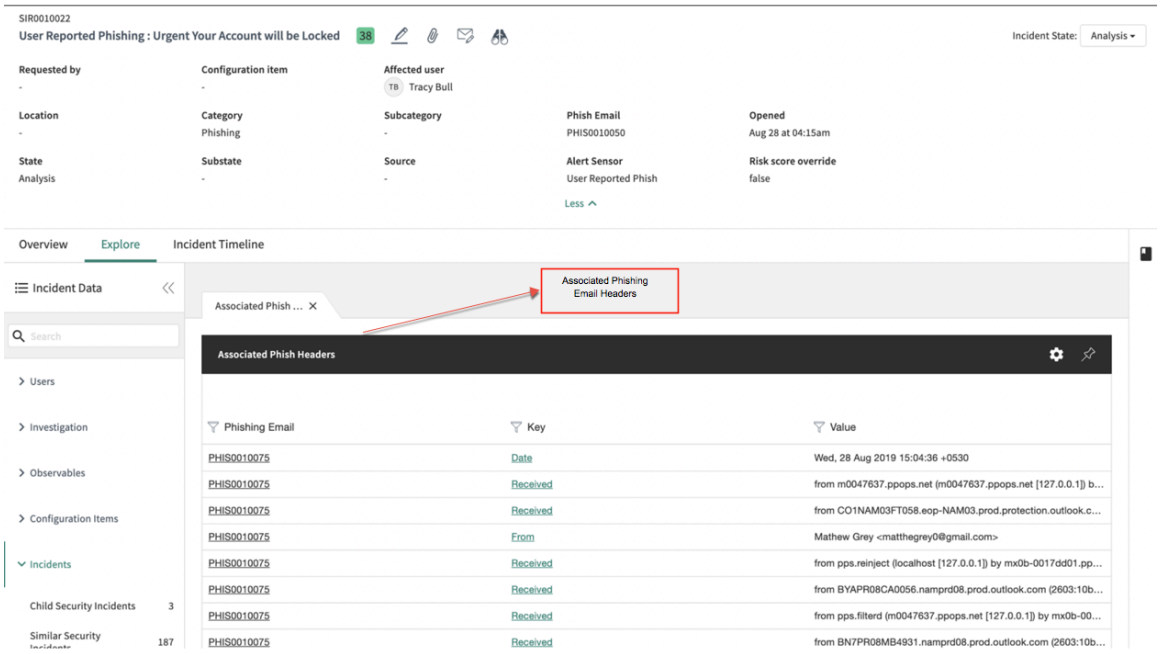
[探索] タブで、 インシデント > 子セキュリティインシデント.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



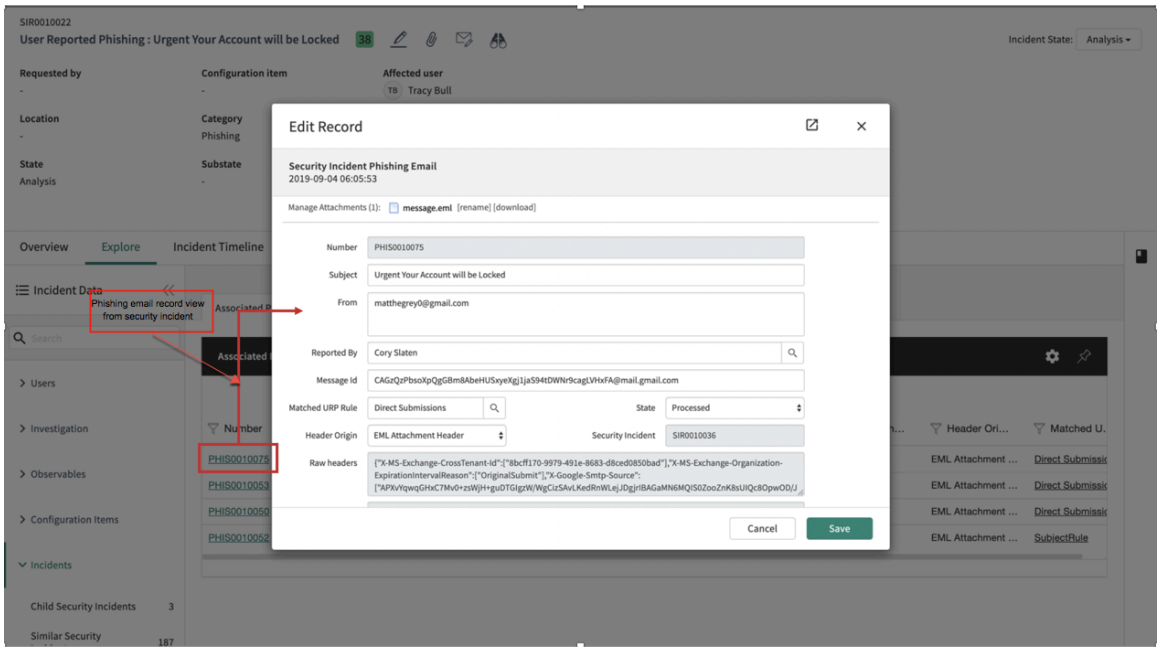
クリックします インシデント > 関連フィッシングヘッダー > . 親セキュリティインシデントに集計されたすべての子レコードのロールアップされたヘッダーとフィッシングメールレコードを表示できます。



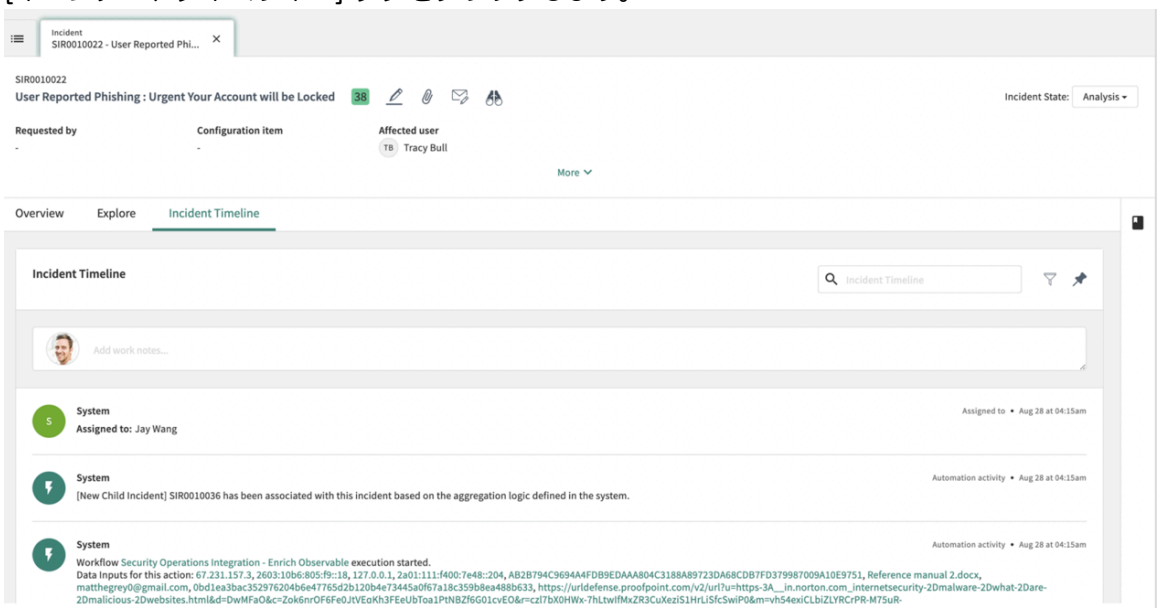
フィッシングメールリンクをクリックすると、セキュリティインシデントに関連付けられたフィッシングメールレコードが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[インシデントタイムライン] タブをクリックします。



以下を示すシステム更新が表示されます。

- 特定された重複する子レコード。
- 許可リスト観測事象。
- フィッシングメールを受信した一方で [影響を受けるユーザー] リストに属していない不一致ユーザー。

よく寄せられる質問

このセクションでは、拡張されたユーザーから報告されたフィッシング機能に関してよく寄せられる質問について説明します。

1. 新しいセキュリティインシデントレスポンススポークをインストールしましたが、ユーザーから報告されたフィッシングインシデントが表示されません。

   デフォルトでは、ユーザーから報告されたフィッシング機能は無効になっています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

この機能を有効にするには、読み取り専用の ユーザーから報告されたフィッシングメールのセキュリティインシデントへの変換 フローのコピーを作成し、使用する前にアクティブ化する必要があります。

2. フィッシングメールを取り込んでセキュリティインシデントに変換する際に、フィッシングメール内の悪意のあるリンクや添付ファイルを処理するためにどのような予防措置が使用されますか？

   ServiceNow アンチアンチウイルススキャナーにより、このような悪意のある添付ファイルやリンクがスキャンされます。ただし、セキュリティアナリストがインシデントを正確に調査できるように、セキュリティインシデントレスポンス アプリケーションによってフィッシングメールの一部であるすべてのアーティファクトがキャプチャされます。その一方で、フィッシングメール内の悪意のあるリンクは、セキュリティアナリストが誤ってこれらのリンクをクリックしないように、ユーザーから報告されたフィッシング機能によってミュートされます。悪意のある添付ファイルに関しては、セキュリティアナリストは、それらのダウンロードについて注意する必要があります。

3. セキュリティインシデント拡張のためにフィッシングメールの一部である悪意のあるファイルはすべてキャプチャされますか？

   はい。フィッシングメールに含まれるファイルはすべてキャプチャされます。これらの詳細は、セキュリティインシデント観測事象の一部としてファイルハッシュの形式で表示できます。

4. フィッシングメール内の悪意のあるファイルとリンクは調査のためにサンドボックスインスタンスに送信されますか？

   現在、悪意のあるファイルやリンクを調査するためのすぐに使用可能なサンドボックス統合はサポートされていません。

5. 重複する受信フィッシングメールレコードが親セキュリティインシデントに関連付けられている期間を定義する期間枠またはトリガーはありますか？

   重複するフィッシングメールレコードは、アクティブな親セキュリティインシデントにのみ集計されます。親インシデントがクローズまたはキャンセルされた場合、受信した新しい重複フィッシングメールは新しいセキュリティインシデントとして作成されます。ただし、このシナリオでは、新しいセキュリティインシデント内で、[類似のセキュリティインシデント] 関連リストでクローズまたはキャンセルされた親セキュリティインシデントを表示できます。

   注:
   この動作は、フローデザイナーを使用して構成できます。

6. ユーザーから報告されたフィッシング機能でメールヘッダーの詳細をキャプチャするために使用がサポートされているのは Microsoft Outlook **PhishAlarm** プラグイン (旧 Wombat) のみですか？

   ユーザーから報告されたフィッシング機能は、メールヘッダーを解析するためにビルドされ、RFC822 標準に準拠しています。したがって、**PhishAlarm** プラグイン (旧 Wombat)と同様に、RFC822 標準に基づいてメールヘッダーをキャプチャする他のすべての Microsoft Outlook プラグインがサポートされています。

セキュリティインシデントからのレコードの作成

セキュリティインシデントを作成して保存した後、そこから変更要求 (CHG)、インシデント (INC)、または問題 (PRB) レコードを作成できます。任意のセキュリティインシデントからカスタマーサービスケースを作成することもできます。

セキュリティインシデントからの変更、インシデント、または問題の作成

セキュリティインシデントを作成して保存した後、そこから変更要求 (CHG)、インシデント (INC)、または問題 (PRB) レコードを作成できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：sn_si.basic 以上

手順

1. 次のいずれかの方法を使用して、セキュリティインシデントを開きます。
   - に移動すると、既存のセキュリティインシデントを開きます。 セキュリティインシデント > アサイン解除済み > インシデントをクリックし、セキュリティインシデントをクリックします。
   - に移動してセキュリティインシデントを作成 セキュリティインシデント > アサイン解除済み > インシデントをクリックし、[新規] をクリックしてフォームに入力し、レコードを保存します。
2. セキュリティインシデントヘッダーバーを右クリックし、次のいずれかをクリックします。
   - 変更要求を作成
   - インシデントを作成
   - 問題を作成

   注:
   この選択は、ポップアッププロパティ (sn_vul.popup) が有効になっている場合のみ適用されます。これらのボタンのいずれかをクリックすると、プレビューウィンドウが開き、変更、インシデント、または問題の作成に使用されたセキュリティインシデントの情報が表示されます。つまり、構成アイテム、その場所、優先度、簡単な説明と詳細な説明です。変更要求を作成する場合は、[優先度]、[簡単な説明]、[説明] フィールドを編集できます。インシデントを作成する場合は、[優先度]、[緊急度]、[簡単な説明]、[説明] フィールドを編集できます。関連するセキュリティインシデント画面のフィールドは影響を受けません。
3. [送信] をクリックして、変更、インシデント、または問題を作成します。

セキュリティインシデントからのカスタマーサービスケースの作成

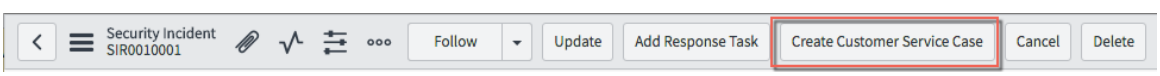
セキュリティインシデントレスポンス には、セキュリティインシデントを カスタマーサービス (CS) ケースにマッピングするデフォルトのフィールドマッピングが付属しています。任意のセキュリティインシデントから CS ケースを作成し、[優先度] を編集し、[オプションのメモ] を追加することもできます。

始める前に
必要なロール：sn_si.basic および sn_customerservice_agent

注:
このタスクを実行するには、カスタマーサービス プラグインをアクティブ化する必要があります。

手順

1. [セキュリティインシデント] に移動します。
2. CS ケースを追加するセキュリティインシデントを開きます。
3. 上部のヘッダーで **[Customer Service** ケースを作成] をクリックします。



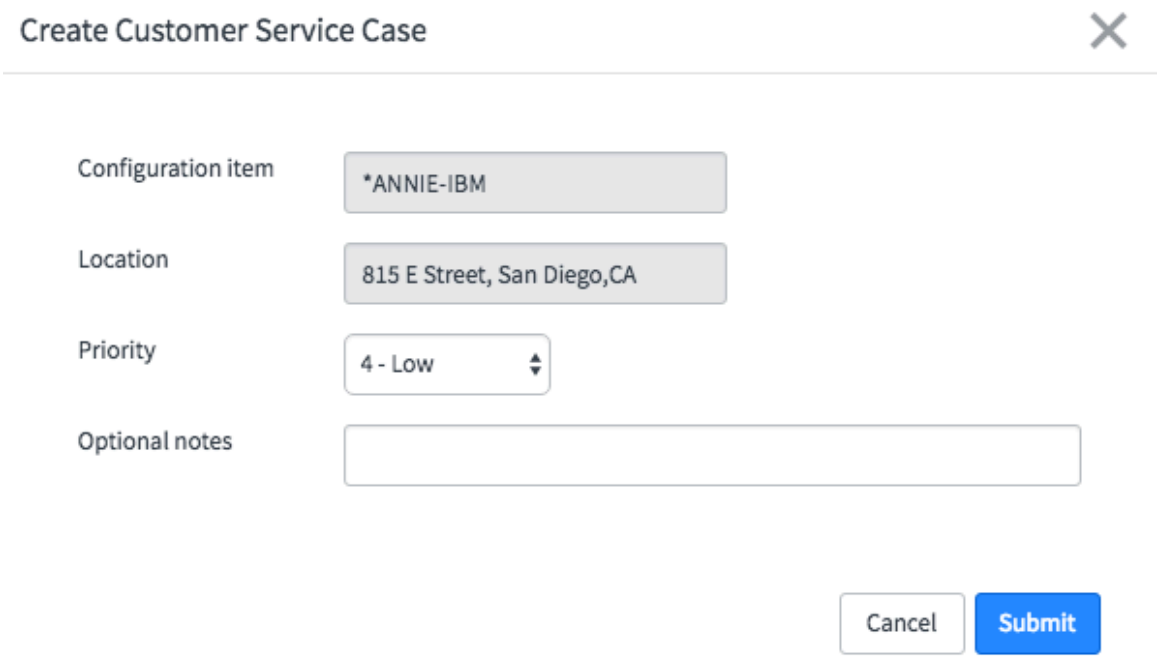
ポップアップウィンドウには、フィールドマッピングに基づいてセキュリティインシデントからの情報が事前入力されます。

4. 新しい [優先度] を選択し、[オプションのメモ] を追加できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[優先度] フィールドは、デフォルト設定を上書きします。[オプションのメモ] がインシデントに追加されます。



5. [送信] をクリックします。
   CS ケースが作成され、セキュリティインシデントの [カスタマーサービスケース] 関連リストに表示されます。
6. CS ケースのリンクをクリックして、ケースをフォローアップできます。

関連情報

カスタマーサービスケース管理

セキュリティケースへのセキュリティインシデントの追加

セキュリティインシデントにさらに高レベルの分析が必要であると判断した場合は、そのインシデントを新規または既存のケースに追加します。

始める前に

セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

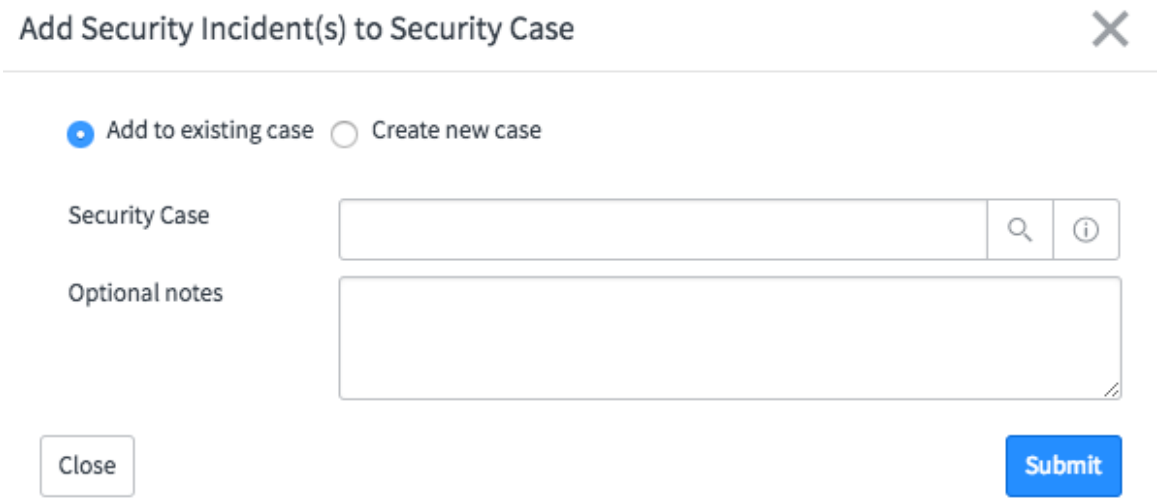
必要なロール：sn_si.admin、sn_ti.case_user_write

手順

1. をクリックして、エスカレーションが必要なセキュリティインシデントに移動します。 セキュリティインシデント > インシデント > 自分にアサイン済みをクリックし、セキュリティインシデントを開きます。
2. [セキュリティケースに追加] 関連リンクをクリックします。
   [セキュリティケースへのセキュリティインシデントの追加 **(Add Security Incident(s) to Security Case)]** ダイアログボックスが開きます。

自動翻訳

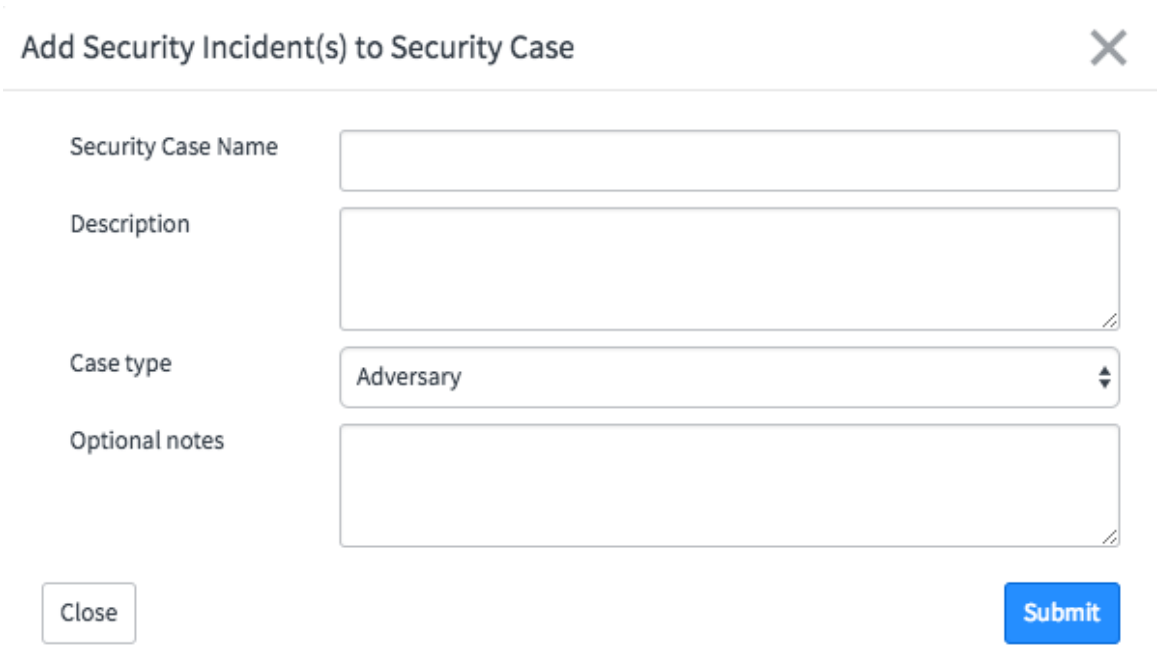
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. このセキュリティインシデントの追加先ケースが自分にアサインされている場合は、必要に応じてフィールドに入力し、[送信] をクリックします。

フィールド	説明
セキュリティケース	セキュリティケースを選択します。
オプションのメモ	必要に応じて、ケースアナリストにとって有益な追加のメモを入力します。

4. 1 つ以上のケースが自分にアサインされている場合に、新しいケースを作成してそれにセキュリティインシデントをアサインするには、[新規ケースを作成] をクリックして追加のフィールドを表示します。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
自分にアサインされたケースがない場合は、まず上の画面が開きます。

5. 必要に応じてフィールドを入力します。

フィールド	説明
セキュリティケース名 (Security Case Name)	新しいセキュリティケースの名前を入力します。
説明	ケースの説明を入力します。
ケースのタイプ	調査対象のケースタイプを選択します。
オプションのメモ	必要に応じて、ケースアナリストにとって有益な追加のメモを入力します。

6. [Submit] をクリックします。
セキュリティインシデントの上部に、新しいケースへのリンクとともにメッセージが表示されます。

関連情報

Security Case Management

応答タスクの作成

セキュリティインシデントが作成された後、応答タスクを作成して、セキュリティ問題に対応するために実行される個別のアクションを追跡できます。

始める前に
必要なロール：sn_si.basic

手順

1. 適切な場所に移動して、タスクを作成するセキュリティインシデントを開きます。
例：

- アサインされたセキュリティインシデントに基づいて応答タスクを作成するには、次を選択します セキュリティインシデント > インシデント > 自分にアサイン済み.
- チームにアサインされたセキュリティインシデントに基づいて応答タスクを作成するには、次を選択します セキュリティインシデント > インシデント > チームにアサイン済み > インシデント.
- 未アサインのセキュリティインシデントに基づいて応答タスクを作成するには、次を選択します セキュリティインシデント > インシデント > 未アサインのインシデント.

2. 応答タスクを追加するセキュリティインシデントを開きます。

3. フォームヘッダーにある [対応タスクの追加] ボタンをクリックします。

注:
その他のタスクを作成するには、インシデント関連リストの [タスク] タブをクリックします。

4. 必要に応じて、フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデント

フィールド	説明
セキュリティタグを選択	セキュリティタグをセットアップしてアクティブ化した場合、1 つ以上のタグを選択してレコードにメタデータを追加したり、応答タスクの機密性の度合いを指定したりすることができます。 セキュリティタグを設定またはアクティブ化していない場合、このドロップダウンリストは表示されません。
数値	[読み取り専用] 自動的に生成される セキュリティインシデントレスポンス 番号。
親	[読み取り専用] 関連するセキュリティインシデントの番号。
構成アイテム	セキュリティ上の問題によって影響を受ける構成アイテム (リソース)。
影響を受けるユーザー	セキュリティ上の問題によって影響を受けるユーザー。
優先度	このタスクをいつ実行するかを決定するために使用される優先度。
状況	セキュリティ応答タスクの現在のステータス。タスク作成時のこのフィールドのデフォルトは [ドラフト] です。
スキル	このタスクを実行するために必要なスキル。ロックアイコンをクリックして、必要なスキルを選択します。選択が完了したら、ロックアイコンを再びクリックします。
アサイン先グループ	アサインされるワーカーが選択されるアサイン先グループ。
アサイン先	タスクを実行するようアサインされる個人。
簡単な説明	セキュリティインシデントレスポンス タスクの説明。
説明	選択したタスクの説明。
保護されたメモ	暗号化され、顧客には表示されない作業メモ。
作業メモ	顧客には表示されない作業メモ。
追加コメント	顧客に表示するコメント。

5. 入力が完了したら、[送信] をクリックします。

注:
セキュリティインシデントレスポンス タスクを作成した後、[応答タスク] モジュールで次のいずれかのアプリケーションを使用してタスクを表示できます。

- 自分にアサイン済み
- チームにアサイン済み
- オープンタスクを表示

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- すべてのタスクを表示
- 未アサインタスク

ユーザーからのフィッシング報告予測インテリジェンスの管理

Predictive Intelligence for User Reported Phishing 機能は、ユーザーから報告されたフィッシングメールのトリアージと優先順位付けを行うための重要なソリューションです。

このセクションでは、以下について説明します。

- ユーザーからのフィッシング報告予測インテリジェンス
- 必要なコンポーネントとプラグイン
- ユーザーから報告されたフィッシングに関する最終判定の生成
- ユーザーからのフィッシング報告予測インテリジェンスのトラブルシューティング

ユーザーからのフィッシング報告予測インテリジェンス

この機能は、ユーザーから報告されたフィッシングメールのトリアージと優先順位付けを行うセキュリティアナリストを支援します。

予測インテリジェンスフレームワークは、データの結果を予測、推奨、および整理するようにシステムをトレーニングするためのソリューションを提供します。予測インテリジェンスの詳細については、「Predictive Intelligence」を参照してください。このフレームワークを使用すると、ユーザーから報告されたフィッシングメールが疑わしいか正当であるかを自動的に予測するモデルをビルドできます。

セキュリティアナリストは、過去のユーザーから報告されたフィッシングセキュリティインシデントデータ (メールヘッダー、メール本文、およびセキュリティインシデントクローズコードによって取得されたトリアージ結果) を使用してシステムをトレーニングして、ユーザーから受信したフィッシングの報告を、さらにトリアージする必要があるもの (疑わしいもの) と正当な報告であるものとに分類できます。

受信メールを自動的にトリアージすることで、セキュリティアナリストは、インシデントキューを簡単に優先順位付けし、何よりもまず組織にとってリスクとなる可能性のあるインシデントに焦点を当て、誤検出の可能性が高いメールに費やす労力を減らすことができます。 予測結果は、詳細な優先順位付けを可能にする分類の信頼スコアも提供します。

必要なコンポーネントとプラグイン

ユーザーからのフィッシング報告予測インテリジェンスを使用するには、次のアプリケーションをインストールする必要があります。

プラグイン名	最低バージョン
セキュリティインシデントレスポンス	9.0.1 または 10.0.2
予測インテリジェンス	Orlando バージョン
ユーザーからのフィッシング報告予測インテリジェンス	10.0.2

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
セキュリティインシデントレスポンス 10.4 では、次の新しい機能拡張を使用できます。

- モデルトレーニング用のカスタムフィールドからクローズコードを選択する機能。
- モデルのビルド後に予測を明示的にアクティブ化する機能。
- ディシジョンテーブルを使用して、ユーザーから報告されたフィッシングに関する最終判定を生成する機能。(Security Operations Spoke 10.3.0 が必要)

新しい拡張機能を使用するには、次のアプリケーションをアップグレードする必要があります。

プラグイン名	アップグレード先
セキュリティインシデントレスポンス	10.0.4
ユーザーからのフィッシング報告予測インテリジェンス	10.3.1

新規および更新されたテーブル

- sn_sir_ml_urp_config (新規)：URP ML アプリケーションの構成が含まれます。
- sn_sir_ml_urp_feature (新規)：sn_si_phishing メールテーブルから抽出されたレコード。
- sn_sir_ml_urp_feature_import (新規)：過去のフィッシングメールデータをアップロードするために使用されます。
- sn_si_incident (更新)：次の新しいフィールドが追加されました。
  - 受け入れられた予測
  - 予測結果
  - 信頼スコア
- スクリプトインクルード
  - URPMLUtil：構成を取得し、予測ジョブを実行し、予測プロセスを追跡します。
  - URPMLProcessor：sn_si_phishing_email テーブルからデータを抽出して処理します。
  - URPMLAction：フローを実行して予測結果を受け入れます。

ユーザーから報告されたフィッシングに関する最終判定の生成

セキュリティインシデントレスポンスチームは、予測インテリジェンスおよび脅威エンリッチメント統合の結果に基づいて、ユーザーから報告されたフィッシングレコードに関する最終的な判定を下せるようになりました。

この最終判定の生成は、ディシジョンテーブル構成を介して有効化され、フロー内で活用されます。

必須条件

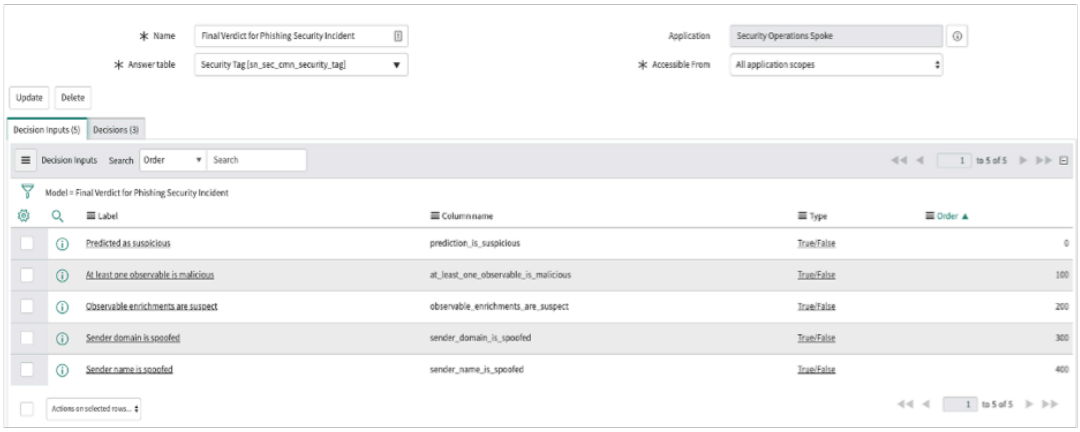
「必要なコンポーネントとプラグイン」にリストされているすべてのプラグインがインストールされていることを確認します。

次のように移動する。 フィッシング用予測インテリジェンス > 最終判断 > フィッシングセキュリティインシデントの最終判定.

[意思決定の入力] タブには、最終判定に到達するために評価されたさまざまな条件が表示されます。

自動翻訳

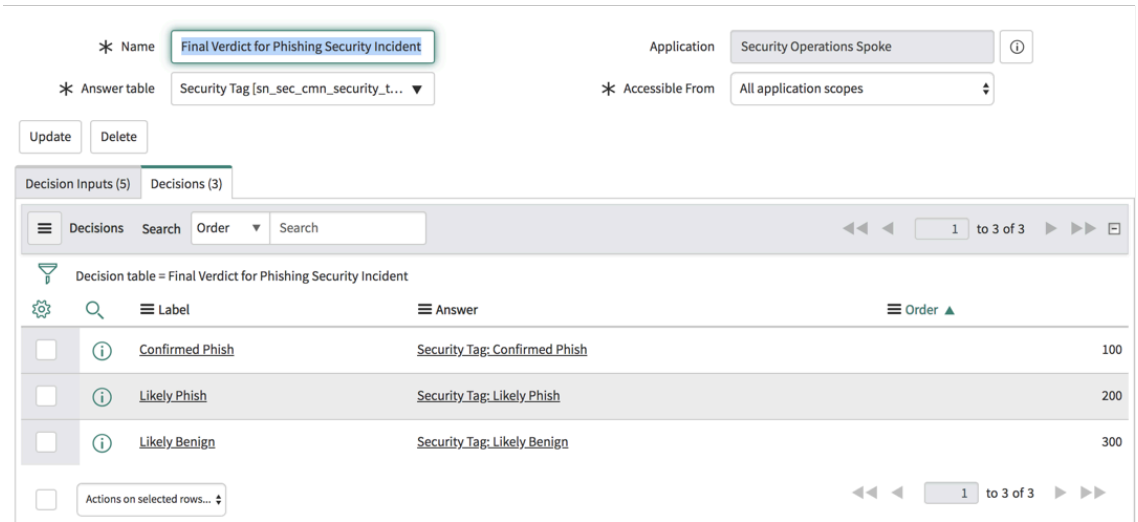
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



ベースシステムでは、次の条件を使用できます。

- 不審として予測：予測インテリジェンスによって、ユーザーから報告されたフィッシングメールが [不審] であると分類された場合。
- 少なくとも 1 つの観測事象に悪意がある：脅威インテリジェンスソースによって、セキュリティインシデントに関連する観測事象 (URL、ドメイン、IP、ハッシュなど) が [悪意がある] として分類された場合。
- 観測事象の拡張が疑わしい：観測事象の拡張 (たとえば、フィッシングドメイン登録の最新性、フィッシングドメイン登録の国) が疑わしい場合。
- 送信者ドメインが偽装されている：フィッシング攻撃者のメールドメインが信頼できるドメインになりすましている可能性がある場合。
- 送信者名が偽装されている：フィッシング攻撃者のメールアドレスが組織の信頼できる従業員になりすましている可能性がある場合。

[決定] タブには、特定のセキュリティインシデントに対して到達できる最終判定オプションが表示されます。

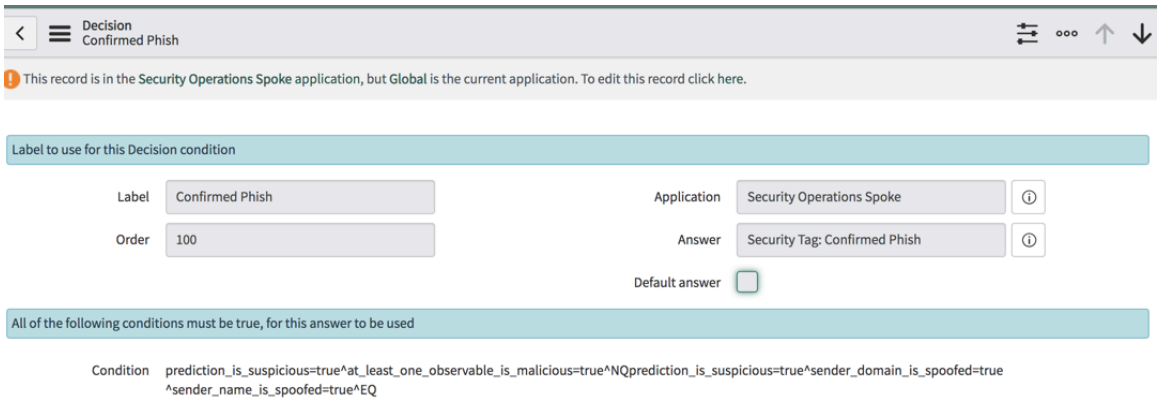


ベースシステムでは、次の決定を使用できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [確認済みのフィッシング (Confirmed Phish)]：条件により、確認済みのフィッシングメールであると最終判定された場合。
- [フィッシングの可能性あり (Likely Phish)]：条件により、潜在的なフィッシング試行であると最終判定された場合。
- [安全な可能性が高い]：条件により、無害であると最終判定された場合。

最終判定オプションごとに、評価された条件を確認できます。[ラベル] リンクをクリックして条件を表示します。



ベースシステムで提供されるディシジョンテーブルをカスタマイズすることも、独自のディシジョンテーブルを作成することもできます。このディシジョンテーブルは、セキュリティインシデントレスポンスプレイブックで利用できます。ベースシステムでは、フィッシングセキュリティインシデントの最終判定を生成サブフローを使用できます。このサブフローは、フィッシングセキュリティインシデントの最終判定を自動的に生成し、その決定に基づいてセキュリティタグを適用します。このサブフローは、自動フィッシングプレイブックの一部として含めることができます。

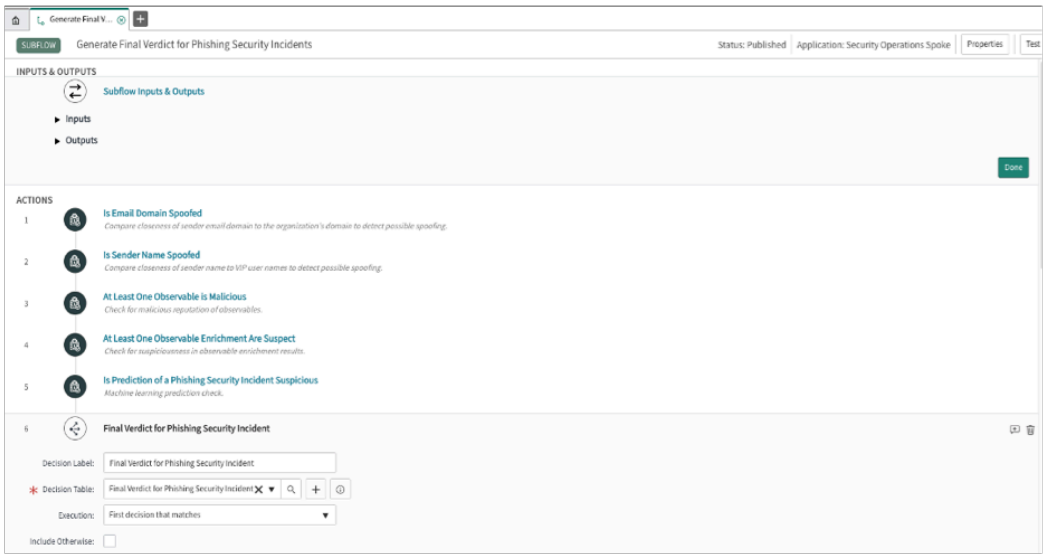
このサブフローの入力は次のとおりです。

- incident_id：フィッシングセキュリティインシデントの Sys ID。
- c_level_names：フィッシング攻撃で偽装されている可能性がある名前のカンマ区切りリスト (組織内の役員の名前など)。
- trusted_domains：信頼できるメールドメインのカンマ区切りリスト。
- enrichment_keywords：エンリッチメント結果から観測事象に悪意があることを示すキーワードのカンマ区切りリスト。
- sender_email (オプション)：フィッシングメールの送信者のメールアドレス。

このフローの出力は、[確認済みのフィッシング **(Confirmed Phish)]**、[フィッシングの可能性あり **(Likely Phish)]**、または [安全な可能性が高い] になります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



ユーザーからのフィッシング報告予測インテリジェンスのトラブルシューティング

このセクションでは、いくつかの一般的な問題のシナリオについて説明します。

- 問題：予測インテリジェンス構成を変更できない。

  ソリューション：操作に必要な権限があるかどうかを確認します。しきい値を変更するには、ml_admin ロールを持つユーザーとしてログインする必要があります。シナリオによっては、さらに高い権限が必要になる場合があります。たとえば、トレーニングデータ制限を変更する必要がある場合など。このようなシナリオでは、カスタマーサポートに連絡してサポートを受ける必要があります。

- 問題：モデルトレーニングに失敗した。

  ソリューション：ML スケジューラーの URL が設定されているかどうかを確認します。次のように移動する。 システムプロパティ > すべてのプロパティ をクリックし、*glide.shared_service_scheduler.url* プロパティが構成されているかどうかを確認します。

- 問題：セキュリティインシデントで予測結果を利用できない。

  ソリューション：

  - 予測 URL が *glide.prediction_service.url* システムプロパティに設定されているかどうかを確認し、データセンターが URL と一致していることを確認します。
  - 「ユーザーから報告されたフィッシングメールを予測 (Predict User Reported Phishing Email)」スケジュール済みジョブがアクティブかどうかを確認します。

ユーザーからのフィッシング報告予測インテリジェンスの構成

ユーザーから報告されたフィッシングメールを識別するためのモデルを構成して準備します。

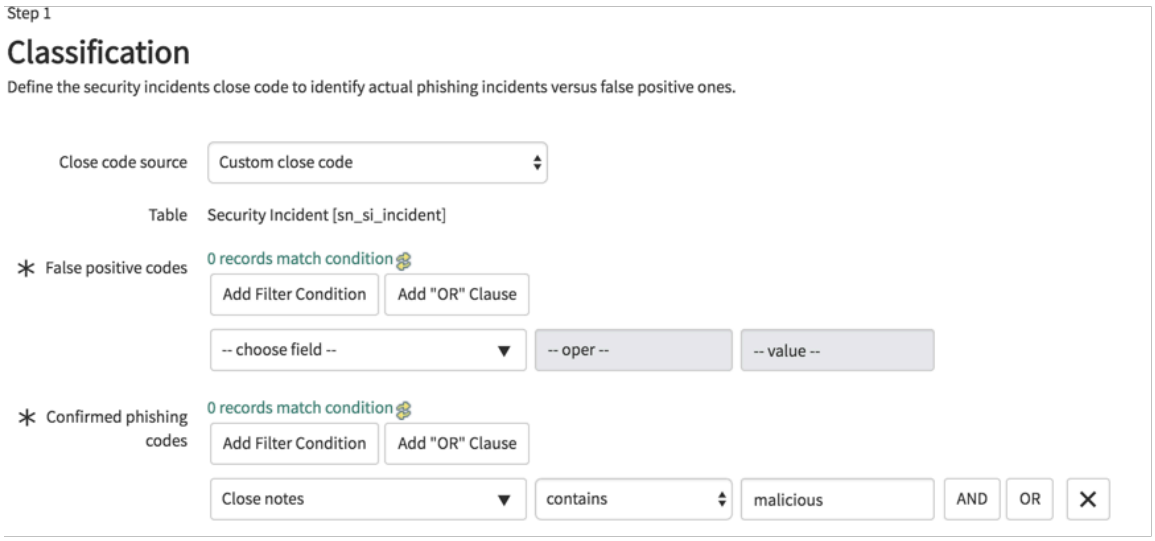
始める前に
必要なロール：ml_admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > フィッシング用予測インテリジェンス > 構成.
2. 構成のステップ 1 で、[終了コードソース] リストから次のいずれかのオプションを選択します。
   - デフォルトクローズコード：悪意のあるメールと正当なメールを識別するためにトレーニングモデルで使用する必要があるデフォルトのセキュリティインシデントクローズコードを指定するには、このオプションを選択します。ロックアイコンをクリックし、1 つ以上の誤検出コードまたは確認済みフィッシングコードを選択します。
   - カスタムクローズコード：既存のインシデント応答手順の一部として使用できるカスタムフィールドからクローズコードを定義する場合は、[カスタムクローズコード] オプションを選択します。クローズコードを定義するには、セキュリティインシデントテーブルからフィールドを選択し、1 つ以上のフィルター条件を指定します。



3. ステップ 2 で、モデルのトレーニングに使用できる履歴データをインポートします。
   履歴データをインポートするデータソースを選択します。次のいずれかを選択できます。
   - ユーザーから報告されたフィッシングメールテーブル：履歴データとしてインポートできるレコードの数を確認できます。このオプションを選択し、[インポート] をクリックします。
   - カスタムデータソース：履歴データレコードを含む単一のフォーマットされた CSV ファイルを添付できます。ファイルを選択し、[インポート] をクリックします。

   注:
   インポートする CSV ファイルには、次のヘッダーが含まれている必要があります。
   - ラベル
   - ヘッダー
   - 本文

   CSV ファイルの [ラベル] 列では、各レコードに [悪意がある] タグまたは [正当] タグが含まれている必要があります。

   データのインポートを停止するには、[インポートをキャンセル] をクリックします。インポートプロセスがキャンセルされ、それまでにインポートされたすべてのレコードが削除されます。
4. 履歴データをインポートした後、リンクをクリックしてページを更新します。
   さらにトレーニングデータをインポートすることも、そのまま次のステップに進むこともできます。

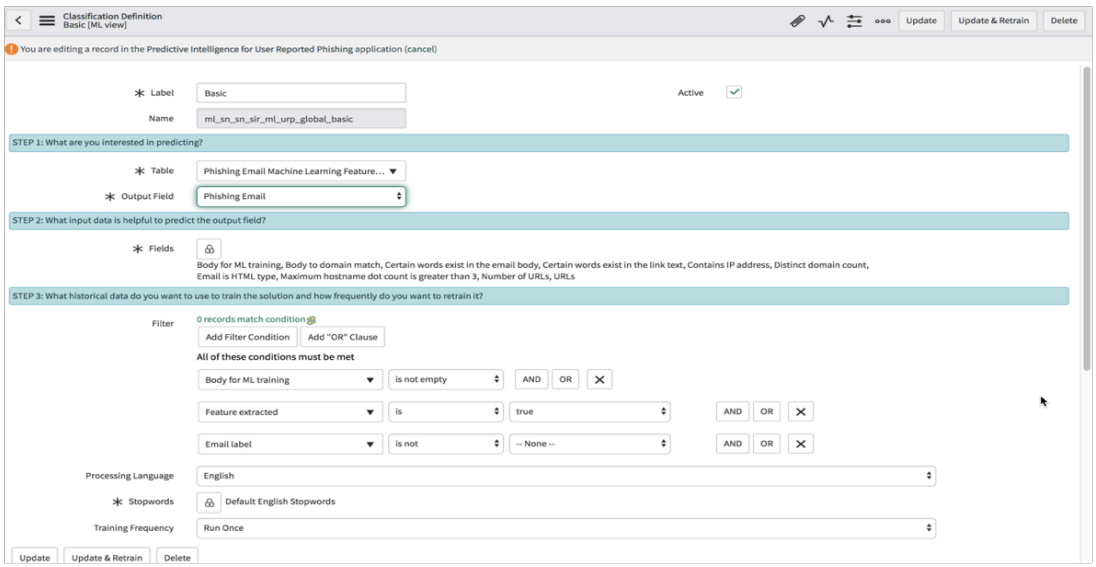
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. ステップ 3 で、トレーニングに利用可能なレコードの数が最小しきい値の要件を満たしているかどうかを確認します。

   注:
   トレーニングレコードの最大数と最小数のデフォルト値が表示されます。これらのしきい値は、プラットフォーム機械学習のプロパティページで変更できます。サポートが必要な場合は、カスタマーサポートにお問い合わせください。

6. トレーニングデータで十分な場合は、[モデルをトレーニング] をクリックします。
   下の画面でトレーニングの入力を更新できます。



7. 変更できる予測入力は次のとおりです。
   - 何の予測に興味がありますか？
   - 出力フィールドを予測するために役に立つ入力データは何ですか？
   - ソリューションをトレーニングするにはどのような履歴データを使用し、どのくらいの頻度で再トレーニングしますか？

   これらの入力のデフォルト値が表示されます。それらを変更して、次のいずれかをクリックします。
   - 更新：トレーニングモデルの定義を更新します。
   - 更新 **&** 再トレーニング：トレーニングモデルの定義を更新し、モデルを再トレーニングします ([モデルをトレーニング] 機能をトリガーします)。

8. 最後に、モデルのトレーニングが完了したら、[予測のアクティブ化] チェックボックスをクリックします。
   そのモデルを使用して、ユーザーから報告されたフィッシングレコードごとに予測が提供されるようになりました。ユーザーから報告されたフィッシングレコードに対する予測の提供を停止する場合は、[予測のアクティブ化] チェックボックスをオフにして、[非アクティブ化] をクリックします。

セキュリティアナリストのアサイン

[SIR 管理構成 (SIR Administration Configuration)] 画面の設定に応じて、セキュリティアナリストをセキュリティインシデントに手動でアサインするか、ワークフローを使用して自動的にアサインするか、または自動アサインを使用して自動的にアサインすることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アナリストの手動アサイン

他のユーザーまたは SIR アプリケーションがセキュリティインシデントを作成するかセキュリティ応答タスクを生成するたびにセキュリティアナリストの手動アサインを必要とするように セキュリティインシデントレスポンス の管理構成画面で設定できます。

セキュリティインシデントまたは応答タスクを自動アサインできない場合は、セキュリティアナリストの手動アサインを必要とするように SIR の管理構成画面で設定できます。これは、要求を完了するためのセキュリティアナリストの数が限られている場合、または単にセキュリティアナリストを自動アサインしたくない場合に適しています。

ワークフローベースのセキュリティアナリストのアサイン

他のユーザーまたは SIR アプリケーションがセキュリティインシデントまたはセキュリティ応答タスクを作成するたびに選択したワークフローを使用してセキュリティアナリストをアサインするようにセキュリティインシデントレスポンス の管理構成画面で設定できます。

セキュリティインシデントレスポンスの管理構成画面では、ワークフローを使用して各セキュリティインシデントまたはセキュリティ応答タスクにアナリストをアサインすることができます。このオプションは、セキュリティ問題を解決するためにカスタムプロセスを使用する組織や、自動化できるプロセスを持つ組織に適しています。

セキュリティアナリストの自動アサイン

他のユーザーまたは SIR アプリケーションがセキュリティインシデントまたはセキュリティ応答タスクを作成するたびにセキュリティアナリストを自動アサインするように セキュリティインシデントレスポンス の管理構成画面を設定できます。自動アサインを使用すると、組織のニーズに基づいて、アナリストをセキュリティインシデントに自動的にアサインする基準を定義できます。

エージェントの評価に基づいたエージェントの自動アサイン

自動アサインが有効になっており、セキュリティインシデントまたは応答タスクが作成されると、次のアクションが実行されます。

- 構成で定義された基準に基づいて、対応可能なセキュリティアナリストが評価されます。
- 適切なセキュリティアナリストがタスクに自動的にアサインされます。
- タスクが [アサイン済み] ステータスに移行します。

スキル、場所、タイムゾーン、グループのカバー範囲などの複数の条件のセットを考慮するように構成が設定されている場合は、重み付けプロパティの設定と他の基準に基づいてセキュリティアナリストが評価されます。これらの構成設定は、オプションのプロパティに基づいてエージェントを自動アサインするのに役立ちます。計算された評価は、セキュリティインシデントまたは応答タスクに最適なエージェントを決定するために使用されます。アプリケーションの構成画面で、評価ベースの方法の任意の組み合わせを有効にすることができます。

タスクが作成されると、使用可能なエージェントごとに有効な選択基準の各タイプの評価が計算されます。合計評価が最も高いエージェントが自動アサインで考慮されます。

自動アサインの重み付けプロパティの設定については、以下を参照してください。 セキュリティインシデント > アドミニストレーション > プロパティは、評価の計算に含まれます。

これらの値を使用して、組織にとって重要度の高い自動アサインの選択基準に優先度を付けることができます。1 (あまり重要ではない) から 10 (重要) までの優先度の値を設定します。

重み付けプロパティがエージェントの評価に与える影響の例については、「複数の選択基準を使用したエージェントの自動アサイン」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オンコールスケジューリング

オンコールスケジューリング アプリケーションは、発生した問題を解決するために専任のサポートチームメンバーを利用できるように支援します。オンコールスケジュール、勤務表ローテーション、エスカレーションポリシーを設定し、グループへの通知をエスカレーションし、エスカレーションの現在の連絡先を決定できます。アプリケーションは、たとえばインシデントをアサインするときなどに、サポートグループにアサインされたメンバーと対応可能なメンバーを識別します。詳細については、「On-Call Scheduling」を参照してください。セキュリティインシデントレスポンスのオンコールスケジューリングも同様に機能します。

場所を使用したエージェントの自動アサイン

エージェントは、ユーザーレコードのホームの場所とタスクの場所に基づいて自動的にアサインできます。

[エージェントの自動選択では、エージェントの場所が考慮されます] オプションが有効になっている場合、場所による自動アサインが実行されます。

タスク (セキュリティインシデントまたは応答タスク) が作成されると、タスクの場所に最も近いエージェントがタスクで考慮されます。場所のみを考慮するようにアプリケーションが構成されている場合、最も近いエージェントにタスクが自動アサインされます。

タスクが作成されると、エージェントの場所が次の範囲と比較され、各エージェントの場所の評価が決定されます。

場所の評価の計算

エージェントからタスクまでの距離 (マイル)	評価
0 ～ 0.1	1
0.11 ～ 0.5	0.9
0.51 ～ 5	0.7
5.1 ～ 10	0.5
10.1 ～ 20	0.4
20.1 ～ 30	0.3
30.1 ～ 40	0.2
40.1 ～ 100	0.1
100 を超える	0

スキル、タイムゾーン、スケジュールなどの他の選択基準を使用するようにアプリケーションが構成されている場合、すべての選択基準の評価が重み付けされ、合計されます。総合評価が最も高いエージェントがタスクに自動的にアサインされます。詳細については、「複数の選択基準を使用したエージェントの自動アサイン」を参照してください。

スキルを使用したエージェントの自動アサイン

エージェントは、エージェントのスキルと、タスクを実行するために必要なスキルに基づいて自動的にアサインできます。を使用したユーザーレコードへのスキルのアサイン スキル > ユーザー.

[タスクに対するエージェント自動選択がスキルの所持を要求] 構成オプションが [すべて] または [一部] に設定されている場合、スキルによる自動アサインを実行できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スキルを含むタスクが自動アサインされると、エージェントのスキルは、タスクの実行に必要なスキルと比較されます。評価は、スキル構成オプションに基づいて計算されます。このオプションが [一部] に設定されている場合、スキルに最も近いエージェントにタスクが自動的にアサインされます。このオプションが [すべて] に設定されている場合は、必要なスキルをすべて持っているエージェントだけが考慮されます。タスクを実行するために必要なすべてのスキルを持つエージェントがない場合は、自動的にアサインされません。

スキル評価は次のように計算されます。

Skills_agent/Skills_task

各項目の意味は次のとおりです。

- Skills_agent は、タスクに必要なスキルと一致する、エージェントが所有するスキルの数です。
- Skills_task は、タスクに必要なスキルの合計数です。

たとえば、タスクが 4 つのスキルを必要とし、エージェント A がそれらのうちの 3 つを所有し、エージェント B がそれらのうちの 2 つを所有する場合、次のようになります。

- エージェント A のスキル評価 = 3/4 または 0.75
- エージェント B のスキル評価 = 2/4 または 0.5

場所やタイムゾーンなどの他の選択基準を使用するようにアプリケーションが構成されている場合、すべての選択基準の評価が重み付けされ、合計されます。総合評価が最も高いエージェントがタスクで選択されます。詳細については、「複数の選択基準を使用したエージェントの自動アサイン」を参照してください。

タイムゾーンを使用したエージェントの自動アサイン

エージェントは、ユーザーレコードで定義されたタイムゾーンとタスクのタイムゾーンに基づいて自動的にアサインできます。

[エージェントの自動選択では、タスクのタイムゾーンが考慮されます] 構成オプションが有効になっている場合、タイムゾーンによる自動アサインを実行できます。

タスクが作成されると、タスクのタイムゾーンに最も近いタイムゾーンのエージェントがタスクで考慮されます。タイムゾーンのみを考慮するようにアプリケーションが構成されている場合、同じタイムゾーンのエージェントのみにタスクが自動アサインされます。

注:
エージェントとタスクのタイムゾーンが正しく設定されていることが重要です。

タスクが作成されると、エージェントは次の式を使用して、タスクとエージェントのタイムゾーンに基づいて評価されます。

1 - [abs(Task_tz - Agent_tz) ÷12]

各項目の意味は次のとおりです。

- abs は、絶対値を計算するための数学関数です。
- Task_tz は、タスクのタイムゾーンと GMT の間のオフセットです。
- Agent_tz は、エージェントのタイムゾーンと GMT の間のオフセットです。

たとえば、ニューヨーク市 (GMT-4) でタスクが作成され、ロサンゼルス (GMT-7) とフランスのパリ (GMT+1) の 2 つのエージェントがタスクを実行できます。

ロサンゼルスのエージェントの評価は、次のように計算されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1 - abs((-4) - (-7)) ÷ 12 または 0.75

パリのエージェントの評価は、次のように計算されます。

1 - abs((-4) - (+1)) ÷ 12 または 0.58

したがって、タスクの自動アサインがタイムゾーンのみに基づいている場合は、ロサンゼルスのエージェントにアサインされます。

スキルや場所などの他の選択基準を使用するようにアプリケーションが構成されている場合、すべての選択基準の評価が重み付けされ、合計されます。総合評価が最も高いエージェントがタスクで選択されます。詳細については、「複数の選択基準を使用したエージェントの自動アサイン」を参照してください。

グループのカバー範囲を使用したエージェントの自動アサイン

エージェントは、ユーザーレコードで定義されたグループのカバー範囲に基づいて自動アサインできます。

複数の選択基準を使用したエージェントの自動アサイン

タスクが作成されると、エージェントの評価が計算されます。詳細については、以下を参照してください。

- 場所を使用したエージェントの自動アサイン
- スキルを使用したエージェントの自動アサイン
- タイムゾーンを使用したエージェントの自動アサイン

自動アサインは、次の計算に基づいています。

(Criteria_1 評価 x Criteria_1 重み) + (Criteria_2 評価 x Criteria_2 重み) + (Criteria_3 評価 x Criteria_3 重み) / 使用される基準タイプの数

使用される基準タイプの数は、使用された場所、スキル、およびタイムゾーンの設定に応じて 1、2、または 3 となります。

この例では、場所とスキルに基づいてエージェントの自動アサインを計算します。この例は、以下の前提に基づいています。

- [エージェントの自動選択では、エージェントの場所が考慮されます] 構成オプションがアプリケーションに対して有効になっています。
- **[Auto-selection of agents requires them to have some of the required skills for the task]** (エージェントの自動選択では、タスクに必要なスキルの一部を持っていることが必要です) 構成オプションがアプリケーションに対して有効になっています。
- [スキルの重み] がアプリケーションに対して 10 に設定されています。
- [場所の重み] がアプリケーションに対して 5 に設定されています。
- エージェント A および B はタスクを実行するために利用可能であり、タスクには 4 つの特定のスキルが必要です。
- エージェント A の場所はタスクのサイトから 5 マイル離れており、必要な 4 つのスキルのうち 3 つを所有しています。
- エージェント B の場所はサイトから 4 分の 1 マイルで、必要なスキルのうち 2 つを所有しています。

エージェントの自動アサインに使用する計算：[(場所の評価 x 場所の重み) + (スキルの評価 x スキルの重み)]/ 2

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- エージェント A の自動アサインの計算：[(0.7 x 0.5) + (0.75 x 1)]/ 2 = 0.55
- エージェント B の自動アサインの計算：[(0.9 x 0.5) + (0.5 x 1)]/ 2 = 0.475

この例では、エージェント A にタスクが自動アサインされます。

セキュリティインシデントと受信要求の管理

セキュリティインシデントが作成された後、解決に向けて問題の分析が進むにつれて、さまざまなタイプの情報を追加したり表示したりできます。

重要:
セキュリティインシデントレスポンス の最新機能は、セキュリティインシデントレスポンス ワークスペース でのみ利用できます。シフト引き継ぎ、リスクスコア算出などの機能にアクセスして活用するには、最新の セキュリティインシデントレスポンス または セキュリティインシデントレスポンスワークスペース バージョンをインストールまたはアップグレードしてください。

このセクションでは、以下について説明します。

- インバウンド要求の作成
- 観測事象の管理
- ルックアップとスキャンの管理
- オンデマンドオーケストレーションの管理
- セキュリティインシデントの重大度の計算
- インシデントの事後アクティビティの管理
- セキュリティインシデントのクローズ

インバウンド要求の作成

セキュリティインシデントとは異なり、インバウンド要求は一般的に優先度が低くなります。ルックアップ、スキャン、新しいバッジの要求などが、インバウンド要求の例です。

始める前に
必要なロール：sn_si.basic ロール以上

手順

1. 要求フォームのいずれかに移動します。
   たとえば **All** (すべて) > セキュリティインシデント > 受け付けた要求 > 自分にアサイン済み.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

セキュリティの要求

フィールド	説明
数値	[読み取り専用] 自動的に生成されるセキュリティ要求番号
会社	要求者の会社
ロケーション	CI の場所 (該当する場合)。このフィールドは、CI が選択されている場合に事前に入力されます。
構成アイテム	要求の影響を受ける構成アイテム

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
優先度	要求の優先度
オープン	[読み取り専用] 要求が開かれた日時
状況	セキュリティ要求の現在のステータス。セキュリティ要求作成時のこのフィールドのデフォルトは [ドラフト] です。
アサイン先グループ	アサインされるワーカーが選択されるアサイン先グループ。
アサイン先	作業を実行するようアサインされる個人
簡単な説明	セキュリティ要求の簡単な説明。要求者に表示されます。
説明	要求の完全な説明。要求者に表示されます。
作業メモ	作業メモ。要求者に表示されます。

4. 入力が完了したら、[送信] をクリックします。
5. 要求をセキュリティインシデントにエスカレートする必要がある場合は、[セキュリティインシデントへの変換] をクリックします。

観測事象の管理

観測事象は、ネットワークまたはオペレーティングシステムで検出された、侵入を示す可能性のあるアーティファクトです。一般的な観測事象は、IP アドレス、マルウェアファイルまたは URL の MD5 ハッシュ、またはドメイン名です。脅威インテリジェンス 観測事象テーブルデータは、セキュリティインシデント内から確認できます。

観測事象情報には、値、タイプ、コンテキスト、およびタイムスタンプが含まれます。

観測事象は、手動で作成または削除することも、ルックアップ要求によって自動的に作成または削除することもできます。

新しい [結果] 列が [脅威のルックアップの結果] タブに追加されました。可能な値は、[悪意がある] および [不明] です。

IoC ルックアップ要求でセキュリティインシデント観測事象が見つからない場合は、[不明] とラベル付けされます。

IoC ルックアップ要求でセキュリティインシデント観測事象が見つかった場合は、[悪意がある] とラベル付けされます。

アップグレード中、既存のアイテムの [結果] 列は [悪意がある] に設定されます。

注:
脅威インテリジェンス 観測事象テーブルデータはセキュリティインシデントの一部ですが、脅威インテリジェンス モジュールとの他のインタラクションは含まれません。脅威の完全な機能については、脅威インテリジェンス プラグインをサブスクリプションで利用できます。

関連情報

セキュリティインシデント観測事象の作成

セキュリティインシデントの **IoC** 情報の表示

セキュリティインシデントに関連付けられた観測事象やサイティング検索結果などの IoC 情報を表示できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_si.basic

手順

1. IoC 関連情報を表示するセキュリティインシデントがまだ開いていない場合は、これを開きます。
2. **[IoC** を表示] 関連リンクをクリックします。
3. いずれかの関連リストをクリックし、セキュリティインシデントの情報を表示または追加します。

タブ	説明
観測事象	セキュリティインシデントに関連付けられた観測事象を表示するか、手動で追加または編集します。詳細については、「観測事象の管理」を参照してください。
関連するインジケーター	脅威インテリジェンス がアクティブになっている場合、同じ脅威レコードに関連付けられた他のインジケーターを表示できます。
サイティング検索結果	サイティング検索結果が含まれます。
サイティング検索の詳細	サイティング検索レコードの詳細が含まれます。
脅威のルックアップ	マルウェア検出システムからの拡張データを保存します。このタブは、脅威インテリジェンス プラグインをインストールした場合にのみ表示されます。
関連する攻撃モード/方法	脅威インテリジェンス がアクティブになっている場合、同じ脅威レコードに関連付けられた他の攻撃タイプを表示できます。
セキュリティスキャンの要求	脅威インテリジェンス がアクティブになっている場合、セキュリティインシデントに添付されたスキャン要求とルックアップ要求を表示できます。
類似の IoC のあるリソース	脅威インテリジェンス がアクティブになっている場合、類似のインジケーターを持つ他のリソースを表示できます。
類似の IoC のあるユーザー	脅威インテリジェンス がアクティブになっている場合、類似のインジケーターを持つ他のユーザーを表示できます。

4. さらにセキュリティインシデントを更新するには、以下の関連リンクのいずれかをクリックします。
   - 影響を受けるアイテムを表示
   - 関連アイテムを表示
   - 拡張データを表示
   - 対応タスクを表示
5. 入力が完了したら、[送信] をクリックします。

セキュリティインシデント観測事象の作成

セキュリティインシデント内で観測事象を作成および表示し、適切なアクションを実行できます。セキュリティインシデントで観測事象を利用できるようにすると拡張性が高まり、応答時間が短縮されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：

- sn_ti_observable.write (書き込み)
- sn_ti_observable.read (読み取り)
- sn_ti_observable.admin (削除)

手順

1. [セキュリティインシデント] に移動します。
2. インシデントを選択します。
3. [セキュリティインシデント観測事象 **(Security Incident Observables)]** 関連リストタブをクリックします。
4. [新規] をクリックします。
5. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
分類タグを選択	レコードにメタデータを追加するためにセキュリティタグを設定しアクティブ化した場合、1 つ以上のタグを選択して、観測事象の感度を指定できます。 セキュリティタグを設定またはアクティブ化していない場合、このドロップダウンリストは表示されません。
値	観測事象に関連付けられている値 (IP アドレスやハッシュなど)。 **注:** IP アドレスまたはハッシュに対する脅威スキャン がマルウェアまたはその他のエラーを返した場合、IP アドレスまたはハッシュの値が観測事象 [sn_ti_observable] テーブルに自動的に追加されます。そのため、[観測事象] フォームから検索できます。
観測可能タイプ	IP アドレスやファイルハッシュなどの観測事象の分類を選択します。これらの観測事象タイプは、[観測事象タイプ] モジュールで定義されます。
インシデント数	観測事象値が検出された回数。
構成である	このフィールドは、観測事象レコードが保存された後にのみ表示されます。 [観測事象タイプ] が [観測事象構成] 以外に設定されていて、この新しい観測事象が構成である場合は、このチェックボックスをオンにします。 [観測事象タイプ] が既に [観測事象構成] に設定されている場合、このチェックボックスはオンになっていて、読み取り専用になります。 観測事象構成は、子観測事象を含む観測事象です。
結果	次のいずれかを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ [悪意がある]：観測事象が組織に有害であることを示します。 ○ [不審]：観測事象が組織に有害であるおそれがあることを示します。 ○ [クリーン]：観測事象が組織に有害でないことを示します。 ○ [不明]：観測事象の結果がまだ確定していないことを示します。 ○ デフォルト値：[不明]。詳細については、「脅威のルックアップ検索計算ツール」を参照してください。 **注:** アップグレード後、既存の観測事象は [悪意がある] としてマークされます。
演算子	このフィールドは、[構成である] チェックボックスがオンの場合にのみ表示されます。このフィールドの設定に応じて、関連するインジケーターが存在するかどうかを決定するときに観測事象とその子が考慮されます。 関連するインジケーターが存在すると判断されるためにすべての子観測事象が存在する必要がある場合は、このフィールドを **[AND]** に設定します。 関連するインジケーターが存在すると判断されるためにいずれかの子観測事象が存在する必要がある場合は、このフィールドを **[OR]** に設定します。
存在できない	このフィールドは、観測事象レコードが保存された後にのみ表示されます。 このフィールドを選択した場合、観測事象が存在しないことが潜在的な問題 (レジストリーキーの欠落など) であることを示します。
ロケーション	2 つのプロパティの設定と 1 つのスクリプトインクルード定義を使用して、このフィールドに IoC データをさらにロードする をロードできます。
メモ	観測事象に関する追加のメモを入力します。

6. フォームヘッダーを右クリックし、[保存] をクリックします。
次の関連リストのいずれかをクリックして、追加情報を表示できるようになりました。

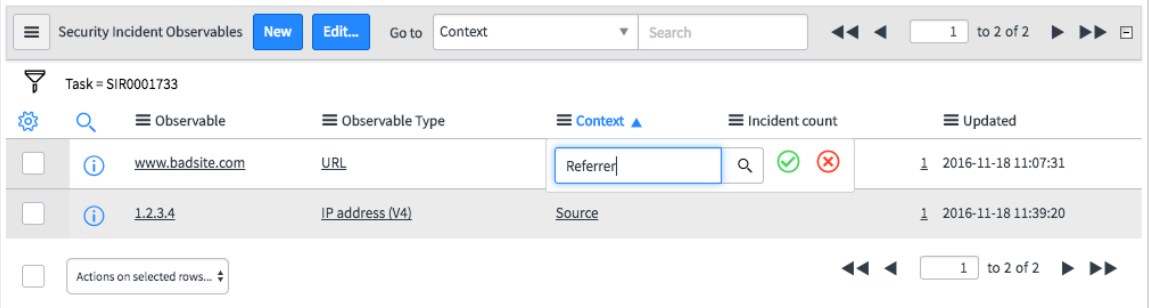
関連リスト	説明
関連するインジケーター	脅威のソースによって識別された、インジケーターを一覧表示します。
関連タスク	観測事象に関連する変更を一覧表示します。
子観測事象	脅威のソースによって識別された、関連する観測事象を一覧表示します。
IP の一致リソース	観測事象が IP アドレスの場合、このリストには、一致する IP アドレスを持つすべてのリソース (構成アイテム) が表示されます。
観測事象ソース	この観測事象のタイプを、ソースの信頼性レベルと共に一覧表示します。
セキュリティ注釈	この観測事象に追加されたセキュリティ注釈を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. セキュリティインシデントに戻ると、次の情報が利用可能です。

> **注:**
> セキュリティインシデントに観測事象を追加すると、システムによって他の構成アイテムや関連付けられているユーザーがチェックされます。それに応じて、[関連する構成アイテム] および [関連ユーザー] 関連リストのタブが更新されます。



列	定義
観測事象	観測事象に関連付けられている値 (IP アドレスやハッシュなど)。
観測事象タイプ	観測事象の特定のタイプ。
コンテキスト	ユーザーが選択します。選択肢は次のとおりです。 ○ IP - [ソース] または [宛先] **注:** 脅威インテリジェンス および Palo Alto Networks - Firewall がアクティブになっている場合、このフィールドの値を変更または追加すると、ログデータ取得フロー [Security Operations Palo Alto Networks - ログデータの取得 (Security Operations Palo Alto Networks - Get Log Data)] ワークフローが実行されます。ワークフローは、拡張された脅威ログデータをファイアウォールから取得し、セキュリティインシデントに添付します。この情報は解析され、[拡張データ] タブの [ファイアウォールログ] セクションにも表示されます。 ○ URL - [リファラー] **注:** ユーザーがフィッシングメールのリンクをクリックしたときに、マルウェアの URL にアクセスする直前の移動元の URL がリファラーです。
インシデン	この観測事象が表示されるインシデントの数。この値は、観測事象が手動またはワークフローによって別のインシデントに追加されると自動的に更新されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

列	定義
ト数	
更新日時	リストが最後に更新された日時。

注:
脅威インテリジェンス プラグインがインストールされている場合は、**[IoC** リポジトリ] の [観測事象] リストでも観測事象を表示できます。

関連情報

セキュリティインシデント観測事象リストの編集

複数のセキュリティインシデント観測事象の追加

ファイル観測事象の管理

ファイル観測事象の管理は、不審なファイルを保存するための厳格なセキュリティ対策を提供し、サンドボックス統合のためのファイルタイプ観測事象を有効にします。

始める前に

必要なロール：sn_ti_malicious_attachment_access (アップロード)

ファイルタイプ観測事象をアップロードします。

- 自動：フィッシングメールのセキュリティインシデントが作成されると、フィッシングメールの添付ファイルがファイルタイプ観測事象として作成されます。
- 手動：セキュリティアナリストは、不審なファイルをアップロードして、ファイルタイプ観測事象を作成することもできます。

このタスクについて

セキュリティインシデントのファイルタイプ観測事象を作成および表示できます。観測事象の一部である不審なファイルは特定の場所に保存され、セキュリティアナリストはそれらのファイルにアクセスして、特定のロールでのみダウンロードできます。

手順

1. セキュリティインシデントに移動します。
2. [すべての関連リストを表示] タブから [観測事象] を選択します。

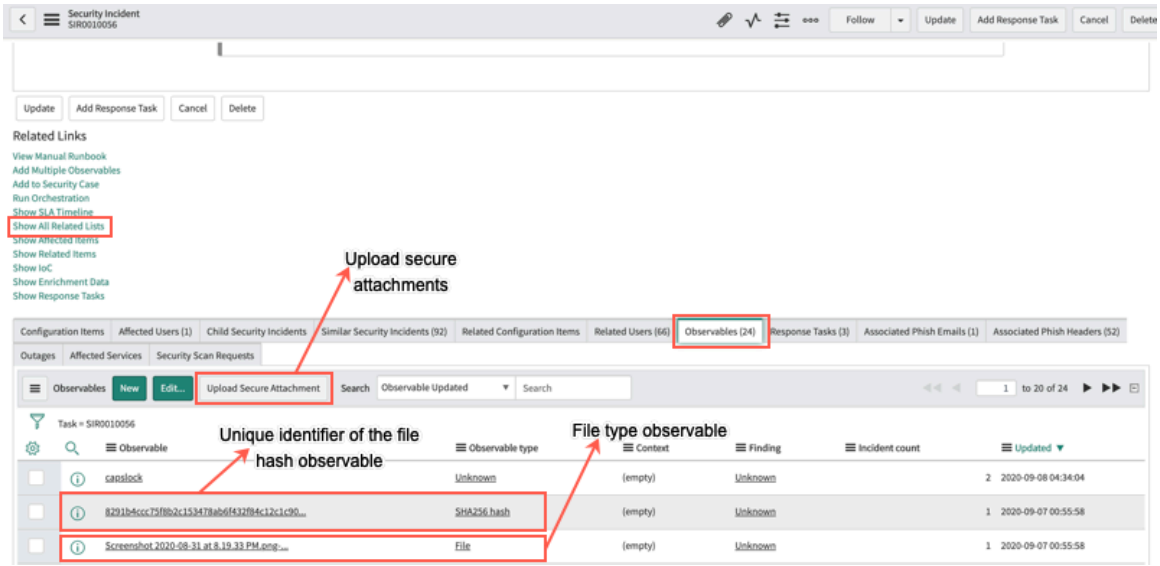
   フィッシングメールに添付ファイルがある場合、デフォルトでは、それらの添付ファイルは対応するセキュリティインシデントにファイルタイプ観測事象として作成されます。各添付ファイルは、2 つの観測事象 (ファイルタイプ観測事象およびファイルハッシュ観測事象) として作成されます。

3. 安全な添付ファイルを手動でアップロードするには：
   - [安全な添付ファイルをアップロード] をクリックします。
   - [安全な添付ファイルをアップロード] で、[ファイルを選択] をクリックして 1 つ以上のファイルをアップロードします。各ファイルは単一の観測事象レコードと見なされます。
   - [ファイル観測事象を作成] をクリックして、ファイルタイプ観測事象を作成します。1 つはファイルタイプ観測事象で、もう 1 つは一意の識別子であるファイルハッシュ観測事象です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ファイルタイプ観測事象



サンドボックス、脅威のルックアップなどの統合を進めるために処理するファイルタイプ観測事象を選択します。さらに、ファイルタイプ観測事象から添付ファイルをダウンロードすることもできます。

注:

脅威のルックアップ (VirusTotal) は、新しいファイルタイプ観測事象に対して保護された添付ファイルからファイルを取得します。以下のシステムプロパティは、新しいファイルタイプ観測事象には適用されません。

- sn_ti.scan.delete_attachment_after_hash
- sn_ti.scan.use_file_hash

すばやく参照できるように、ファイルタイプ観測事象はハッシュ観測事象の子としてマッピングされ、ハッシュ観測事象はファイル観測事象の子としてマッピングされます。

フィッシングメールの添付ファイルが定義されたサイズを超えている場合、観測事象は作成されません。サイズの大きいファイルをサポートするには、システムのプロパティを変更する必要があります。

ファイルサイズのシステムプロパティ

システム プロパティ	説明
glide.email.inbound.max_total_attachment_size_bytes	フィッシングメールを直接転送する場合は、このシステムプロパティ値を使用して、ファイルサイズを 18 MB から目的のファイルサイズに増やします。
com.glide.attachment.max_get_size	フィッシングメールを添付ファイルとして転送する場合は、このシステムプロパティ値を使用して、グローバルスコープでその下のシステムプロパティを作成し、ファイルサイズを 5 MB から目的のサイズに増やします。

次のようにして、新しいファイルタイプ観測事象を作成することもできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. [新規] をクリックします。

b. [観測事象タイプカテゴリ：ファイル **(Observable type Category: File)]** を選択します。

c. [アップロード] をクリックしてファイルを添付します。

セキュリティインシデント観測事象リストの編集

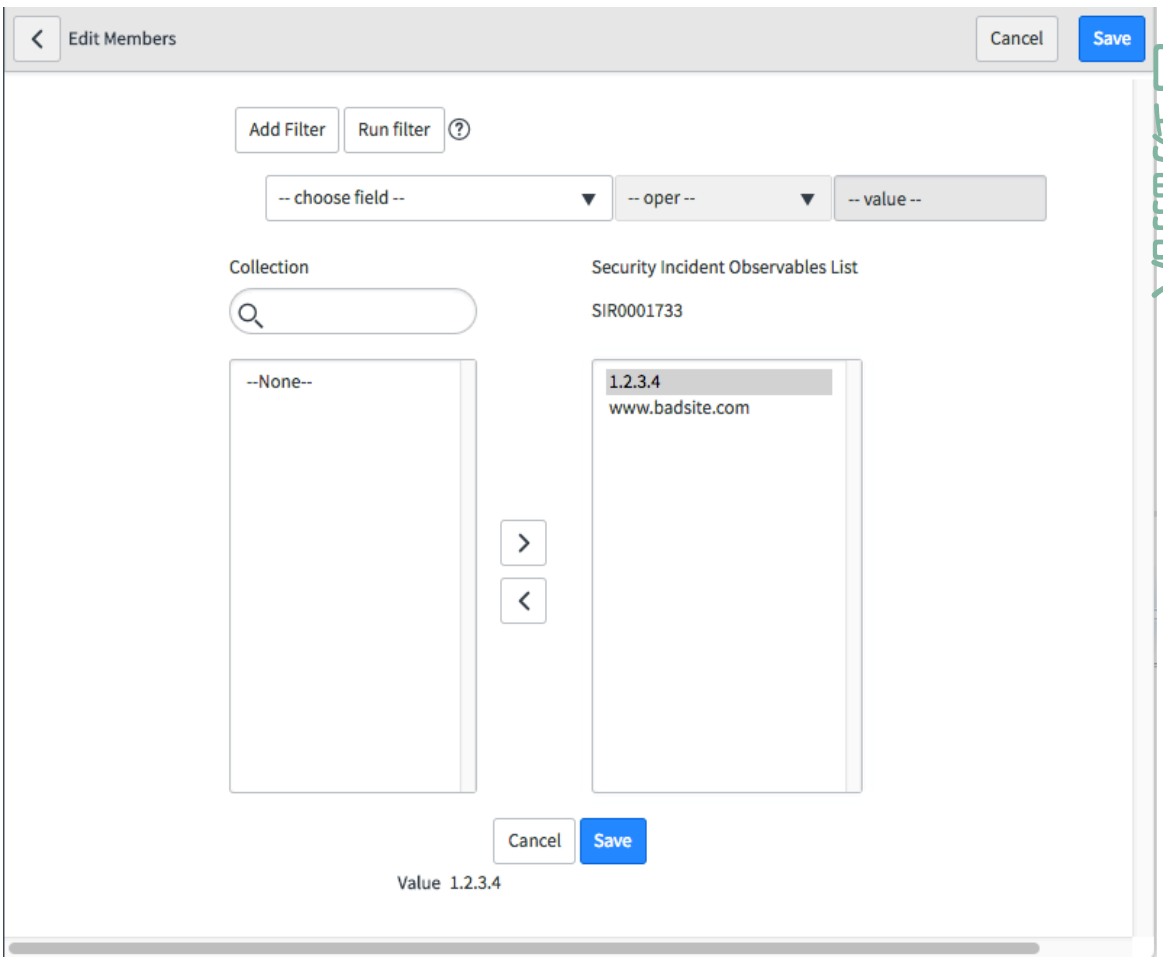
セキュリティインシデントに関連付けられたリスト内のどの観測事象を表示するかを編集できます。

始める前に

必要なロール：sn_si.basic

手順

1. [セキュリティインシデント] に移動します。
2. インシデントを選択します。
3. [セキュリティインシデント観測事象 **(Security Incident Observables)]** 関連リストタブをクリックします。
4. [編集] をクリックします。
5. リストから観測事象を追加または削除します。
   長いリストのフィルターを作成します。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [保存] をクリックします。

> **注:**
> セキュリティインシデントに観測事象を追加すると、システムによって他の構成アイテムや関連付けられているユーザーがチェックされます。それに応じて、[関連する構成アイテム] および [関連ユーザー] 関連リストのタブが更新されます。また、脅威インテリジェンス プラグインがアクティブになっており、少なくとも 1 つの セキュリティインシデントレスポンスの統合 統合実装がアクティブになっている場合、[Security Operations Integration - 脅威のルックアップ] 機能 によって 1 つ以上のワークフローが実行され、追加した観測事象に対して脅威のセキュリティルックアップが実行されます。[脅威のルックアップの結果] タブに結果が表示されます。

関連情報

複数のセキュリティインシデント観測事象の追加

セキュリティインシデント観測事象の作成

複数のセキュリティインシデント観測事象の追加

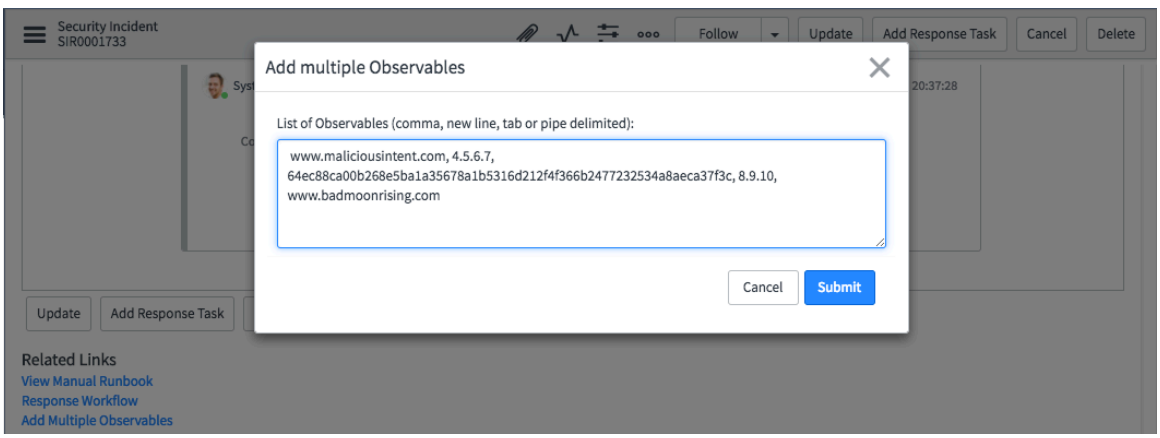
時間を節約するために、複数のセキュリティインシデント観測事象をセキュリティインシデント観測事象リストに追加できます。

始める前に
必要なロール：sn_ti_write

> **注:**
> 複数のセキュリティインシデント観測事象を追加すると、重複は処理中に無視されます。

手順

1. [セキュリティインシデント] に移動します。
2. インシデントを選択します。
3. [複数の観測事象を追加] 関連リンクをクリックします。
4. 複数の観測事象を入力または貼り付けます。
   任意のタイプの観測事象を入力できます。許容される形式は、カンマ、新しい行、タブ、またはパイプ区切り文字形式です。



> **注:**
> セキュリティインシデントに観測事象を追加すると、システムによって他の構成アイテムや関連付けられているユーザーがチェックされます。それに応じて、[関連する構成アイテム] および [関連ユーザー] 関連リストのタブが更新されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注意：自動検出されない観測事象の値は、[不明] タイプにアサインされます。

5. [送信] をクリックします。

自動セキュリティインシデント観測事象ログデータの拡張

脅威インテリジェンス と Palo Alto Networks - Firewall 統合を含む特定のアプリケーションと統合が設定されている場合、その観測事象のソース IP が変更されるたびに、セキュリティインシデント内の観測事象情報を自動的に拡張できます。

変更が発生すると、ビジネスルールによって、ファイアウォール上の脅威ログからデータを取得し、セキュリティインシデントの観測事象情報を拡張するワークフローが開始されます。

観測事象を拡張するには、事前に次のステップを実行する必要があります。

- 脅威インテリジェンスをアクティブ化する必要があります。
- Palo Alto Networks ファイアウォール統合をアクティブ化し、構成する必要があります。これには MID サーバーへの SSH 認証情報の設定 も含まれます。

このセットアップが完了した後、セキュリティインシデントに関連付けられた観測事象のソース IP が変更されると、ビジネスルールによって **Security Operations Palo Alto Networks -** ログデータの取得ワークフローが実行されます。ワークフローアクティビティは、ファイアウォール上の検索クエリをキューに入れ、ファイアウォールから脅威ログデータを取得してセキュリティインシデントに XML ファイルとして添付するために使用されるジョブ ID を返します。

関連情報

AutoFocus セッション情報拡張フローを取得

Security Operations Integration Palo Alto Networks ファイアウォールランチャーワークフロー

[Security Operations Palo Alto Networks - 値のチェックとブロック (Security Operations Palo Alto Networks - Check and Block Value)] ワークフロー

ログデータ取得フロー

WildFire データ拡張フローを取得

サードパーティのウォッチリストへの観測事象の公開

1 つ以上の観測事象または関連するインジケーターをサードパーティのウォッチリストに公開できます。現在、この機能をサポートする実装は CrowdStrike Falcon Host のみです。

始める前に

必要なロール：sn_si.analyst

このタスクについて

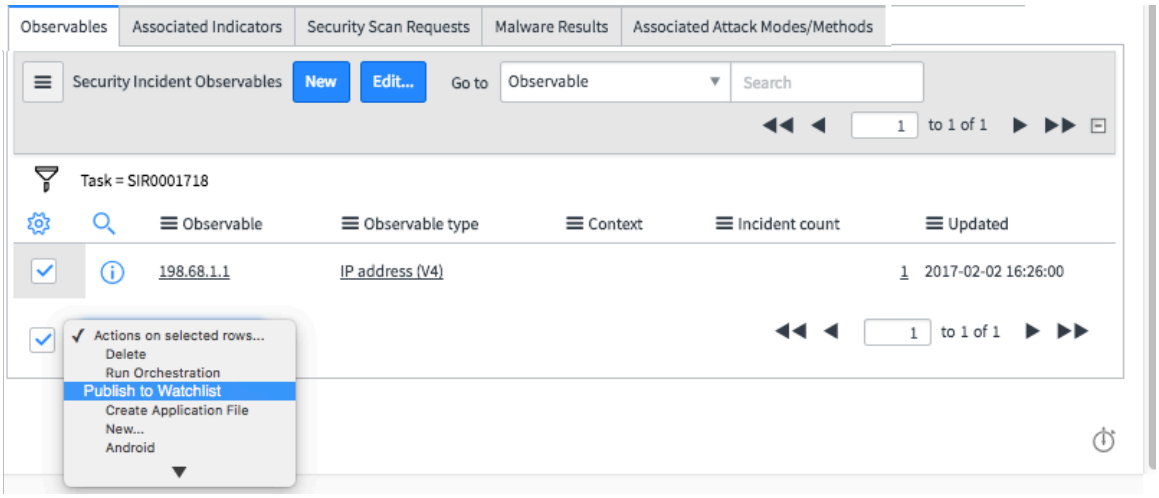
注:
利用可能な実装がない場合、機能アクションは製品メニューに表示されません。

手順

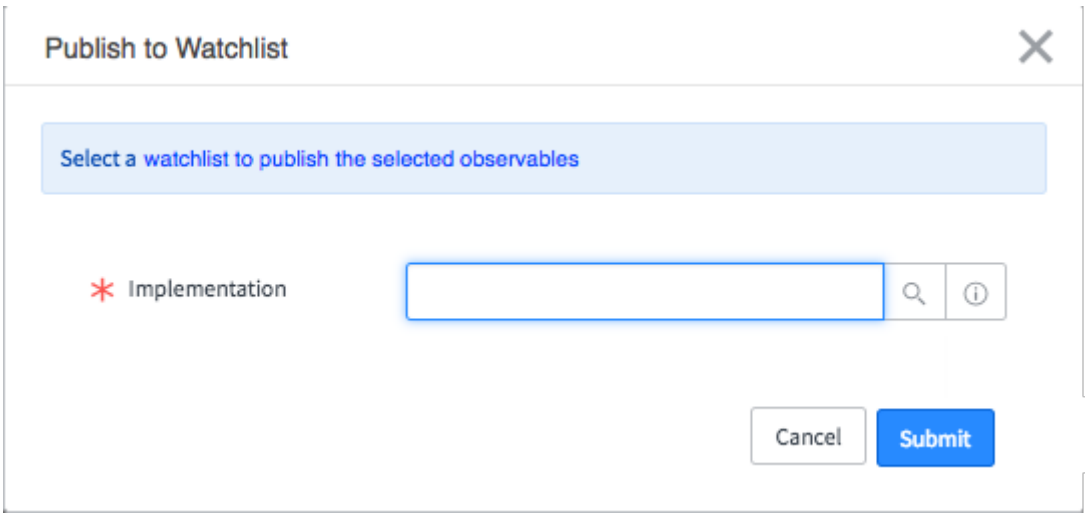
1. セキュリティインシデントに移動します。
2. [関連リスト] タブから [観測事象] を選択します。
3. [選択した行のアクション...] ドロップダウンメニューで [ウォッチリストに公開] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳



ダイアログボックスが表示されます。



4. [実装] を入力または選択します。

> **注:**
> CrowdStrike Falcon Host 実装を選択すると、Security Operations Integration - [ウォッチリストに公開] 機能 によってワークフローがトリガーされます。

5. [Submit] をクリックします。

ルックアップとスキャンの管理

セキュリティインシデントおよびセキュリティインシデントカタログからルックアップと脆弱性スキャンを実行して、潜在的な脅威と脆弱性を特定できます。

セキュリティインシデントから **IoC** ルックアップ要求を送信する

セキュリティインシデントに観測事象が追加されるたびに、IoC ルックアップが自動的に実行されます。また、セキュリティインシデントに添付ファイルがある場合は、ボタンを押すだけで簡単に見つけることができます。

始める前に
自動 IoC ルックアップの場合、脅威インテリジェンス プラグインをアクティブにする必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

必要なロール：sn_si.basic

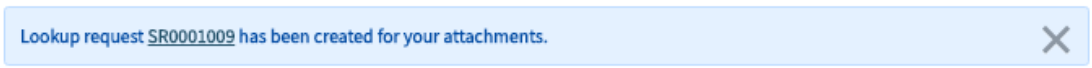
> **注:**
> デフォルトでは、[ファイル] の [ルックアップタイプ] は非アクティブです。

手順

1. 新しいセキュリティインシデントを作成するか、新しいファイルを添付したい場合は既存のセキュリティインシデントを開きます。
2. フォームヘッダーのペーパークリップアイコンをクリックし、1 つ以上のファイルを添付します。
3. フォームのエントリーへの入力が完了したら、フォームヘッダーを右クリックし、[保存] をクリックします。
   レコードが保存されると、[添付ファイルをルックアップ] ボタンが表示されます。
4. [添付ファイルをルックアップ] をクリックします。

   > **注:**
   > [インシデントの詳細] の下にある作業メモは、ルックアッププロセスの進捗状況を報告します。

5. メッセージの最後にあるルックアップ番号をクリックすると、ルックアップレコードを表示できます。
   [ルックアップ] 参照リンクをクリックすると、詳細な結果を表示できます。



セキュリティインシデントカタログから IoC ルックアップ要求を送信する

セキュリティインシデントレスポンス プラグインがアクティブ化されている場合、セキュリティインシデントカタログからファイル、ハッシュ値、URL、および IP アドレスの脅威のルックアップを送信できます。要求が送信され、[自分の要求] モジュールで結果を表示できます。

始める前に
必要なロール：なし

このタスクについて
ルックアップは、ルックアップレコードに一覧表示されている各ルックアップソースについて、デフォルトのルックアップタイプで自動的に実行されます。ルックアップ要求の結果は、[自分の要求] モジュールで使用できます。

手順

1. 次のように移動する。 **All** (すべて) > セルフサービス > セキュリティインシデントカタログ.
2. **[IoC** ルックアップ] をクリックします。
3. [ルックアップファイル、ハッシュ値、URL、または **IP** アドレス] をクリックします。
4. 次のうち 1 つ以上を入力します。

IoC ルックアップ要求

ルックアップアイテム	説明
ファイル	ペーパークリップアイコンをクリックし、ルックアップするファイルを見つけて添付します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ルックアップアイテム	説明
	注: デフォルトでは、[ファイル] の [ルックアップタイプ] は非アクティブです。ファイルは変換され、ハッシュ値として送信されます。
URL	**[URL]** フィールドに、ルックアップする URL をカンマで区切って入力します。 例：www.abc.com、www.xyz.net.
IP アドレス	**[IP** アドレス] フィールドに、ルックアップする IP アドレスをカンマで区切って入力します。
ハッシュ値	[ハッシュ値] フィールドに、ルックアップするハッシュ値をカンマで区切って入力します。 注: [ファイル] の [ルックアップタイプ] が非アクティブの場合、この値は [ファイル]と [ハッシュ値] の両方のデフォルトアクションです。

5. 選択が完了したら、[送信] をクリックします。
6. ルックアップのステータスや結果を表示するには、次に移動します: セルフサービス > 自分の要求.
7. 要求の SR 番号をクリックします。
[アクティビティ] の作業メモには、ファイル、ハッシュ値、URL、または IP アドレスごとの個別のルックアップの作成やルックアップ結果など、ルックアップ時に実行されたタスクが一覧表示されます。

セキュリティインシデントからの脆弱性スキャン要求の送信

セキュリティインシデントに 1 つ以上の構成アイテム (サーバー、コンピューターなど) がある場合は、セキュリティインシデントレスポンス フォームから脆弱性をスキャンできます。

始める前に
脆弱性対応 プラグインをアクティブにする必要があります。

必要なロール：sn_si.write

手順

1. セキュリティインシデントを作成し、少なくとも 1 つのリソースを含めます。
構成アイテムを含む既存のインシデントを開くこともできます。
2. フォームのエントリーへの入力が完了したら、フォームヘッダーを右クリックし、[保存] をクリックします。
レコードが保存されると、[脆弱性のスキャン **(Scan for Vulnerabilities)]** 関連リンクが表示されます。

   注:
   [脆弱性のスキャン] 関連リストが表示されない場合は、次に移動する必要があります 脆弱性 > スキャナーで、少なくとも 1 つのスキャナーをセットアップし、そのデフォルトを **true** に設定します。

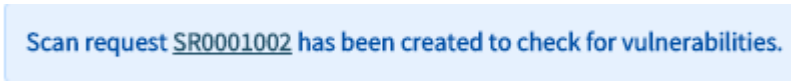
3. [脆弱性のスキャン **(Scan for Vulnerabilities)]** をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:

セキュリティインシデントフォームの上部に、スキャンレコードへのリンクとともにメッセージが表示されます。



4. スキャン要求番号をクリックすると、スキャンレコードを表示できます。
インシデントの詳細には、[セキュリティスキャン要求] レコードのスキャン結果が表示されます。

セキュリティインシデントレスポンスカタログからの脆弱性スキャン要求の送信

セキュリティインシデントレスポンス カタログから CI と IP アドレスの脆弱性スキャンを送信できます。要求が送信され、[自分の要求] モジュールで結果を表示できます。

始める前に
必要なロール：なし

手順

1. 次のように移動する。 **All** (すべて) > セルフサービス > セキュリティインシデントカタログ.
2. [脆弱性スキャン] をクリックします。
3. [構成アイテムと **IP** アドレスをスキャン] をクリックします。
4. スキャンする項目を以下から 1 つ以上入力します。

脆弱性スキャナー

スキャンするアイテム	説明
構成アイテム	[スキャンする構成アイテム] フィールドで、スキャンする CI を選択します。
IP アドレス	[スキャンする **IP** アドレス **(IP addresses to scan)]** フィールドに IP アドレスをカンマで区切って入力します。

5. 選択が完了したら、[送信] をクリックします。
観測事象が見つかった場合は、STXX 標準に従ってインジケーターが作成されます。
6. スキャンのステータスや結果を表示するには、 セルフサービス > 自分の要求.
7. 要求の SR 番号をクリックします。
[アクティビティ] の作業メモには、各 CI または IP アドレスの個別のスキャンの作成やスキャンの結果など、スキャン時に実行されたタスクが一覧表示されます。

オンデマンドオーケストレーションの管理

セキュリティインシデントレスポンス 分析中、セキュリティインシデントワークフローによって駆動されるタスクをセキュリティアナリストが実行する必要がある場合があります。たとえば、特定の CI でプロセスダンプを実行します。これは、オンデマンドオーケストレーションで実現できます。

登録された各 SecOps アプリケーションには、ベースシステムにいくつかのオンデマンドオーケストレーションが含まれています。必要に応じて、カスタムオンデマンドオーケストレーションを定義できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オンデマンドオーケストレーションは、セキュリティインシデントレスポンス 内の次のリストおよびフォームの下部にある選択リストから呼び出すことができます。

- セキュリティインシデントフォーム
- セキュリティインシデントリスト
- セキュリティインシデント観測事象関連リスト
- 構成アイテム関連リスト

注:

- Security Support Common の **sn_sec_cmn.use_on_demand_tbl_as_allowed** プロパティは、オンデマンド実行に使用できるワークフローを定義します。
- このプロパティが **true** に設定されている場合、オンデマンドオーケストレーション [sn_sec_cmn_on_demand_orchestration] テーブルに指定されているワークフローのみを使用できます。
- このプロパティが **false** (デフォルト) に設定されている場合、SecOps アプリケーションレジストリに構成されているアプリケーションのすべてのワークフローを使用できます。
- プロパティの設定に応じて、使用可能なワークフローのリストが、分析される情報のタイプに合わせて調整されます。

セキュリティインシデントフォームからのオンデマンドオーケストレーションの実行

オンデマンドオーケストレーションは、セキュリティインシデントフォームの下部にある選択リストから呼び出すことができます。

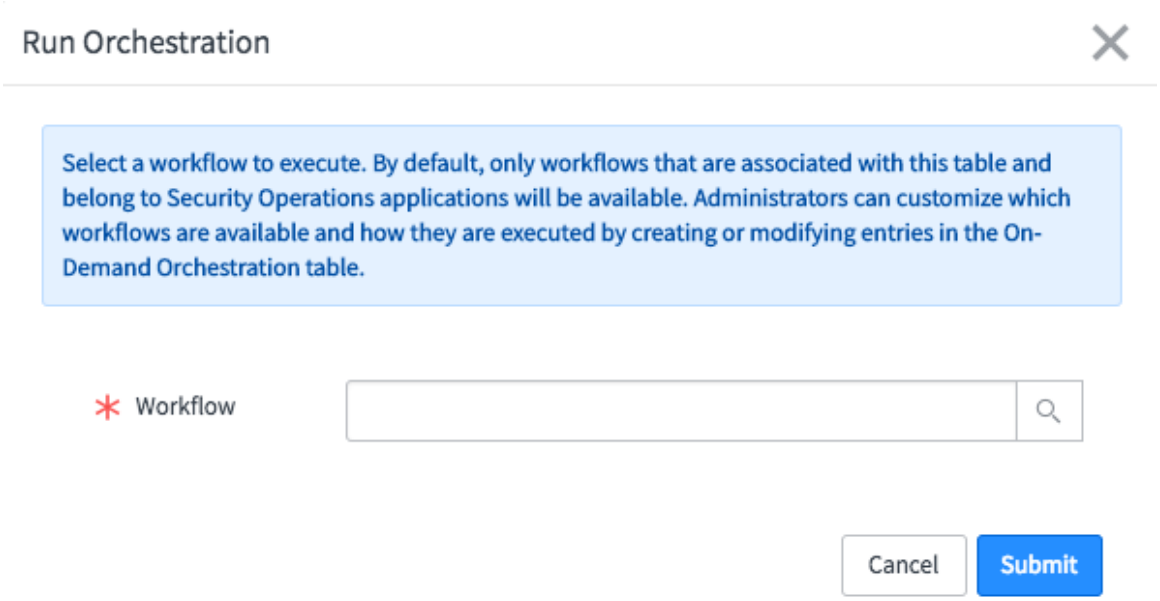
始める前に
必要なロール：sn_si.write

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデント > オープンインシデントを表示.
2. ワークフローを実行するレコード (セキュリティインシデント、観測事象、または CI) を選択します。
3. [オーケストレーションを実行] 関連リンクをクリックします。
   [オーケストレーションを実行] ダイアログボックスが開きます。ダイアログボックスの外観は、Security Support Common の sn_sec_cmn.use_on_demand_tbl_as_whitelist プロパティの設定によって異なります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. ルックアップアイコンをクリックし、実行するワークフローを選択します。
   選択したワークフローが実行されます。詳細については、「セキュリティインシデントレスポンス オーケストレーション のワークフローおよびアクティビティ」を参照してください。

セキュリティインシデントリストからのオンデマンドオーケストレーションの実行

オンデマンドオーケストレーションは、セキュリティインシデントリストからだけでなく、セキュリティインシデントレスポンス の関連リストからも呼び出すことができます。

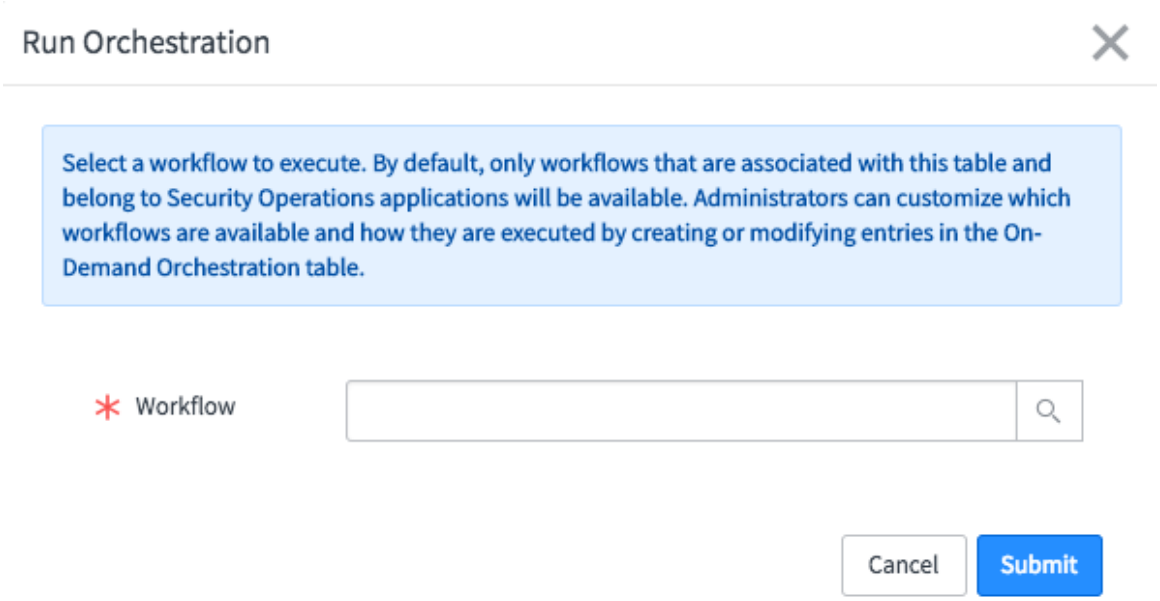
始める前に
必要なロール：sn_si.write

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデント > オープンインシデントを表示.
2. ワークフローを実行するセキュリティインシデントの横にあるチェックボックスをオンにします。
3. 画面の下部にある [選択した行のアクション] 選択リストをクリックし、[オーケストレーションを実行] をクリックします。
   [オーケストレーションを実行] ダイアログボックスが開きます。ダイアログボックスの外観は、Security Support Common の sn_sec_cmn.use_on_demand_tbl_as_whitelist プロパティの設定によって異なります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. ルックアップアイコンをクリックし、実行するワークフローを選択します。
   選択したワークフローが実行されます。詳細については、「セキュリティインシデントレスポンス オーケストレーション のワークフローおよびアクティビティ」を参照してください。

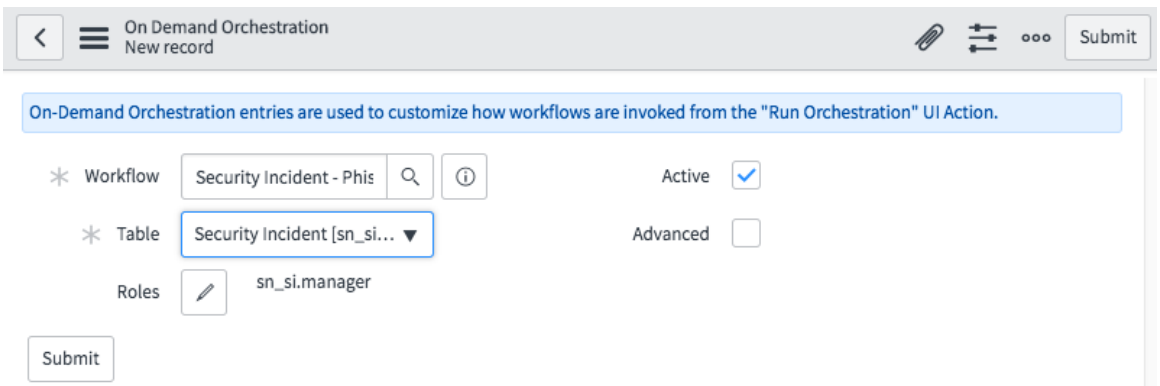
新しいオンデマンドオーケストレーションの定義

ベースシステムでは、事前定義されたワークフローを実行するオンデマンドオーケストレーションを選択できます。新しいオンデマンドオーケストレーションを定義して、[オーケストレーション を実行] 選択リストからワークフローを呼び出す方法をカスタマイズすることができます。

始める前に
必要なロール：sn_si.write

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > ユーティリティ > オンデマンドオーケストレーション
2. [**New**] をクリックします。



3. 必要に応じてフィールドに入力します。

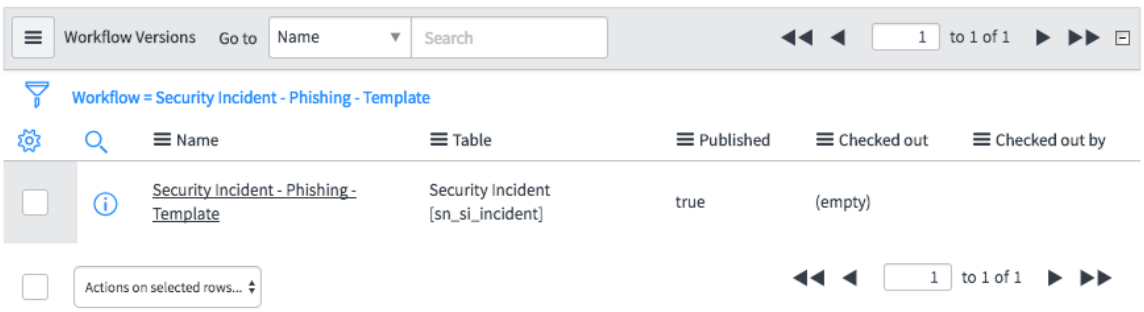
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オンデマンドオーケストレーション

フィールド	説明
ワークフロー	[オーケストレーションを実行] 選択リストに含めるワークフローを選択します。
テーブル	選択したワークフローが実行されるテーブルを選択します。テーブルが、選択したワークフローに設定したテーブルと一致しない場合、[詳細] チェックボックスをオンにし、実行時に正しいレコードをワークフローに渡すように [実行スクリプト] を変更する必要があります。
ロール	必要に応じて、[オーケストレーションを実行] 選択リストでこのワークフローを表示できるユーザーを制限する追加のロールを選択します。
有効	このオンデマンドオーケストレーションレコードをアクティブにするには、このチェックボックスをオンにします。
詳細	このワークフロー用に選択されたテーブルに正しいレコードを渡すように実行スクリプトを変更するには、このチェックボックスをオンにします。
実行スクリプト	このワークフロー用に選択されたテーブルに正しいレコードを渡すように実行スクリプトを変更します。 このフィールドは、[詳細] チェックボックスがオンになっている場合にのみ表示されます。

自動翻訳

4. レコードヘッダーを右クリックして、[保存] を選択します。
[ワークフローバージョン] 関連リストが表示されます。



5. ワークフローに追加の変更を加える必要がある場合は、チェックアウトする必要があります。

関連情報

ワークフローバージョンの操作

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オンデマンドオーケストレーション用の新しい **SecOps** アプリケーションの登録

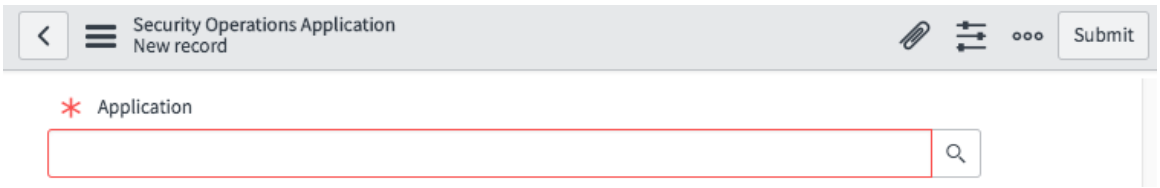
ベースシステムでは、SecOps アプリケーションは、アクティブになると自動的に登録されます。登録すると、アプリケーションに関連付けられたワークフローをオンデマンドオーケストレーション要求で使用できるようになります。必要に応じて新しいアプリケーションを定義し、オンデマンドオーケストレーション用にワークフローをそれらのアプリケーションに関連付けることができます。

始める前に

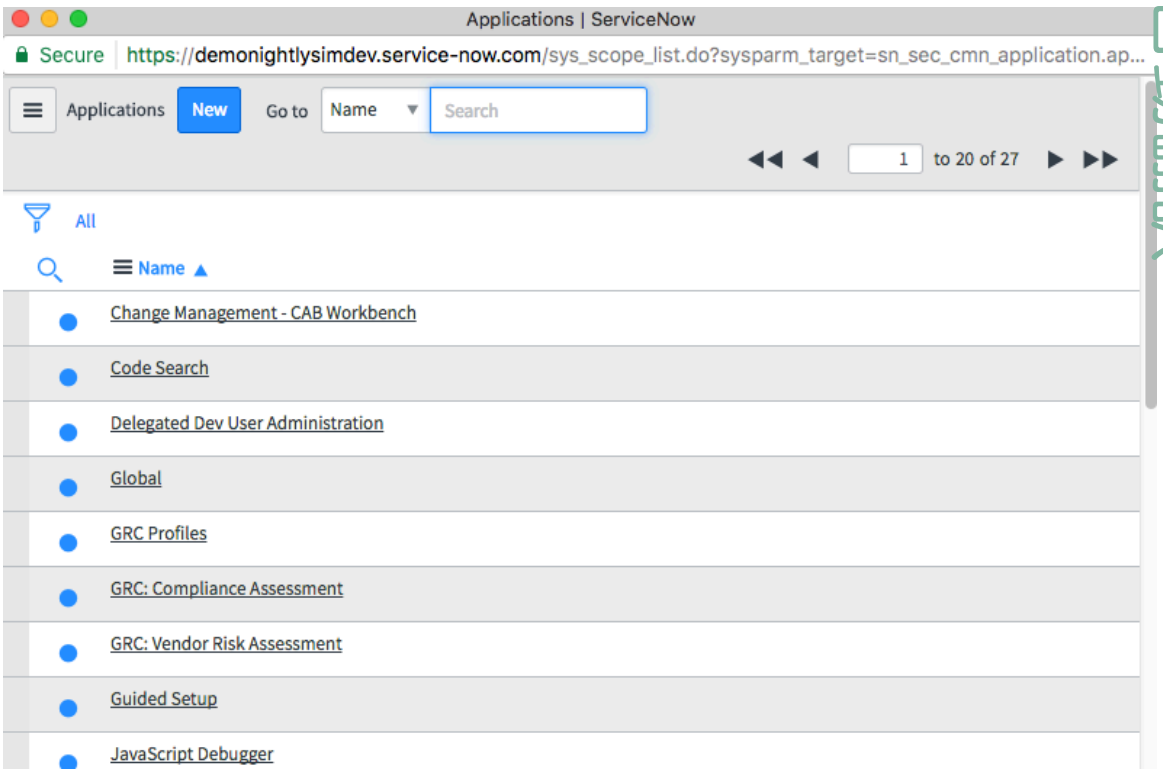
必要なロール：sn_si.write

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > ユーティリティ > **SecOps** 登録アプリケーションをクリックし、[アプリケーションの登録] をクリックします。
   [SecOps アプリケーション] 画面が表示されます。



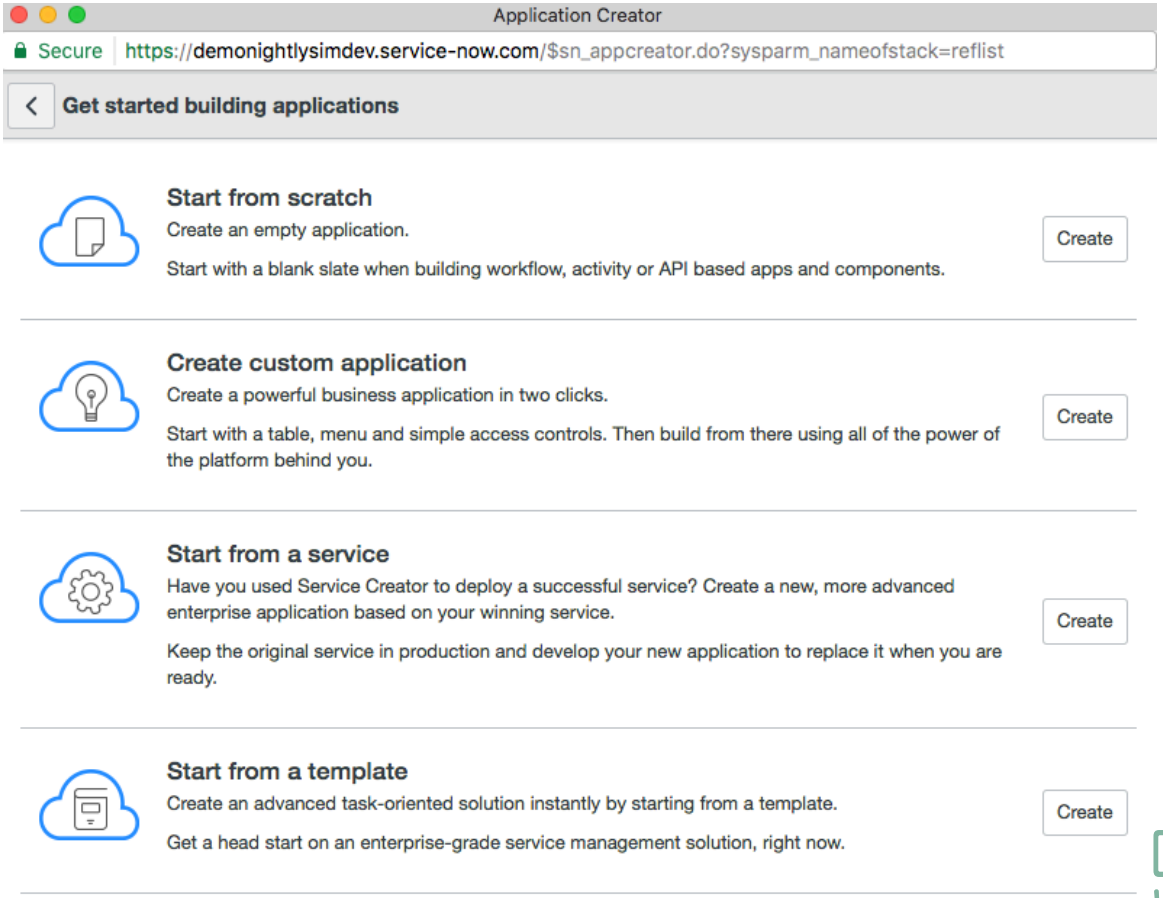
2. [アプリケーション] フィールドで、ルックアップ (虫眼鏡) アイコンをクリックします。
   [アプリケーション] 画面が表示されます。



3. [新規] をクリックします。
   [Application Creator] 画面が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
表示されるオプションは、アクティブ化したアプリケーションによって異なります。新しいアプリケーションの作成の詳細については、次を参照してください。 Building applications 。

4. アプリケーションが生成されたら、オンデマンドオーケストレーションを設定するためのスクリプトを作成できます。

注:
新しいアプリケーションのオンデマンドオーケストレーションを設定するには、スクリプト (ビジネスルール、UI アクション、ワークフローなど) のトリガーのスクリプティングおよび作成に関する高度な技術的知識が必要です。詳細については、ServiceNow Professional サービスにお問い合わせください。

セキュリティインシデントへの情報の追加

セキュリティインシデントが作成されたら、分析に役立つ詳細 (アクセスロールや各種のメモなど) をさらに追加できます。

始める前に
必要なロール：sn_si.basic

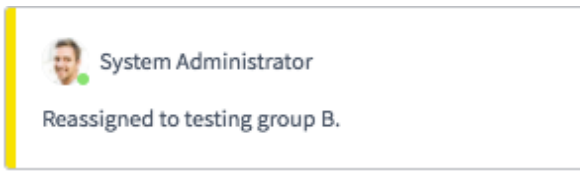
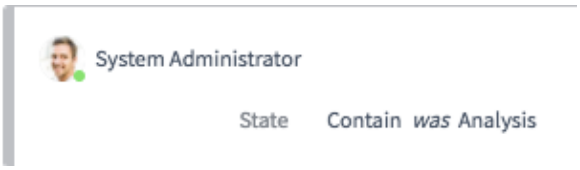
手順
1. 更新するセキュリティインシデントがまだ開いていない場合は、これを開きます。
2. [インシデントの詳細] タブをクリックします。
3. 必要に応じて、フィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
読み取りアクセス	[特別なアクセス **(special access)**] ロールを持つユーザーに、セキュリティインシデントへの読み取りアクセス権を付与します。このユーザーは作業メモの読み取りと書き込みができます。 **注:** ◦ ユーザーが [読み取りアクセス] リストと [特権アクセス] リストの両方に追加されている場合は、[特権アクセス] 権限のみが保持されます。 ◦ sn_si.admin ロールを持つユーザーのみが、読み取りアクセスと特権アクセスの両方を変更できます。
ウォッチリスト	ロックアイコンをクリックして、セキュリティインシデントが変更されたときに通知を受け取るユーザーを追加します。フィールドのロックを解除すると、複数のユーザーを追加または削除するオプションや、ユーザーのメールアドレスを入力するオプションが利用可能になります。入力が完了したら、ロックアイコンをクリックしてフィールドをロックします。
特権アクセス	[特別なアクセス **(special access)**] ロールを持つユーザーに、セキュリティインシデントの ([アサイン先] を除く) すべてのフィールドへの読み取りおよび書き込みアクセス権を付与します。特別なアクセスロールを持つユーザーは、自身にアサインされたすべてのセキュリティインシデントを含む独自のモジュールを持ちます。それ以外のモジュールは使用できません。他のユーザーは [閲覧可能なインシデント] モジュールを表示できません。 **注:** アサインされたユーザーまたはセキュリティロール (sn_si_analyst や sn_si.admin など) を持つユーザーのみが、[アサイン先] フィールドを変更できます。 ユーザーが [読み取りアクセス] リストと [特権アクセス] リストの両方に追加されている場合は、[特権アクセス] 権限のみが保持されます。
作業メモリスト	 ロックアイコン ( ) をクリックして、新しい作業メモが追加されたときに通知を受け取るユーザーを追加します。フィールドのロックを解除すると、複数のユーザーを追加または削除するオプションや、ユーザーの

自動翻訳

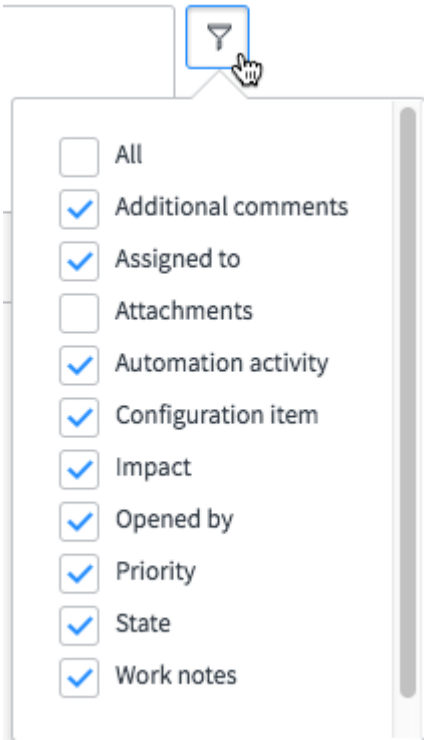
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	メールアドレスを入力するオプションが利用可能になります。入力が完了したら、ロックアイコンをクリックしてフィールドをロックします。
説明	セキュリティインシデントの詳細な説明と、問題の原因の特定または問題の解決に役立つ情報を入力します。
保護されたメモ	sn_si.admin および sn_si.analyst を持つユーザーロールのみが、保護されたメモを表示または編集できます。
作業メモ	顧客には表示されない作業メモを入力します。作業メモは [アクティビティ] エリアに表示されます。
アクティビティ	[作業メモ] に手動で入力された情報、およびこのセキュリティインシデントの関連レコードに関する動的に更新されるすべてのタスクアクティビティ (アクション、コメント、作業メモなど) を表示します。 作業メモは黄色のカラーバンドで表示されます。  自動的に生成されたメモは、グレーのカラーバンドで表示されます。 

4. [アクティビティ] フィールドに表示される情報のタイプを制限するには、フィルター ( ) アイコンをクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
[自動化アクティビティ] チェックボックスを使用すると、ワークフローアクティビティ、リスクスコアの更新など、このセキュリティインシデントによって実行される拡張を含めることができます。

5. セキュリティインシデントをさらに更新するには、次のいずれかのタブをクリックします。
- 関連レコード
- インシデントの事後レビュー
- クローズ情報

6. 入力が完了したら、[送信] をクリックします。

セキュリティインシデントへの関連する問題、変更、およびインシデントの追加

問題、変更、インシデントなどの関連レコードを既存のセキュリティインシデントに追加できます。

始める前に
必要なロール：sn_si.basic

手順

1. 更新するセキュリティインシデントがまだ開いていない場合は、これを開きます。

2. [関連レコード] タブをクリックします。

3. 必要に応じて、フィールドに入力します。

フィールド	説明
問題	このセキュリティインシデントを作成する原因となった根底にある問題を解決する問題 (PRB) レコードを選択します。このインシデントの PRB を作成するには、通常、

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	セキュリティインシデントフォームヘッダーを右クリックし、[問題を作成] を選択します。
親	このセキュリティインシデントを作成する原因となった根底にある問題に関連するタスクレコードを選択します。
親セキュリティインシデント	このセキュリティインシデントを作成する原因となった根底にある問題に関連するセキュリティインシデントレコードを選択します。「親と子のセキュリティインシデントの関係」を参照してください。
インシデント	このセキュリティインシデントを作成する原因となった根底にある問題を解決するインシデント (INC) レコードを選択します。 このインシデントを作成するには、通常、セキュリティインシデントフォームヘッダーを右クリックし、[インシデントを作成] を選択します。
変更要求	このセキュリティインシデントを作成する原因となった根底にある問題を解決する変更要求 (CHG) レコードを選択します。この変更要求を作成するには、通常、セキュリティインシデントフォームヘッダーを右クリックし、[変更を作成] を選択します。

4. セキュリティインシデントをさらに更新するには、次のいずれかのタブをクリックします。
   - インシデントの詳細
   - インシデントの事後レビュー
   - クローズ情報
5. 入力が完了したら、[送信] をクリックします。

Windows の拡張プロセスのプロセスダンプの呼び出し

セキュリティアナリストは、特定のプロセスでプロセスダンプを実行し、それをファイルにダンプして、内部ネットワーク上の共有サイトに投稿できます。アナリストは、セキュリティインシデントで赤くハイライト表示された、拒否リストに載っているプロセスを表示して、追加の分析を実行できます。

始める前に

次のものが必要です。

- Windows Vista 以降を実行しているクライアント、または Windows Server 2008 以降を実行しているサーバー。
- インストールされた ProcDump コマンドラインユーティリティと、procdump 実行可能ファイルのパスを指すシステム環境変数。変数の名前は必ず PROCDUMP にします。この名前は PowerShell スクリプトで使用されます。

必要なロール：sn_si.analyst

手順

1. をクリックして、procdump を呼び出す拡張プロセスを含むセキュリティインシデントに移動します **All** (すべて) > セキュリティインシデント > オープンインシデントを表示をクリックし、セキュリティインシデントを開きます。
2. [拡張データ] タブをクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [実行中のプロセスを取得 **(Retrieve Running Processes)]** 拡張レコードをクリックします。
4. procdump を実行する実行中のプロセスのチェックボックスをオンにし、リストの下部にある [選択した行のアクション] ドロップダウンリストをクリックして、**[Procdump** を実行] をクリックします。
   [選択したプロセスの開始済みプロダンプワークフロー **(Initiated prodump workflow for selected process**)] メッセージがリストの上部に表示され、[セキュリティインシデントレスポンス **- procdump** を実行] ワークフローが実行されます。

セキュリティインシデントの情報の表示

関連リンクを使用して、既存のセキュリティインシデントに対してその他のいくつかのアクションを実行できます。

始める前に
必要なロール：sn_si.basic

手順

1. 更新するセキュリティインシデントがまだ開いていない場合は、これを開きます。
2. [関連リンク] 内で、次のタスクを実行できます。

オプション	説明
手動 Runbook を表示	このセキュリティインシデントで利用可能な Runbook のリストを表示します。
ワークフロー	このインシデントに関連付けられたワークフローを表示します。
複数の観測事象を追加	カンマ、改行、タブ、またはパイプ区切り形式で観測事象のリストを追加します。
セキュリティケースに追加	セキュリティインシデントを 1 つ以上のセキュリティケースに追加します。新しいセキュリティケースを作成し、このセキュリティインシデントをそのケースに追加することもできます。
QRadar IP サマリーを取得	QRadar 統合が利用可能で、有効な CI、ソース、および宛先 IP アドレスが含まれている場合、QRadar ワークフローをトリガーして、作業メモに結果を表示します。
オーケストレーションを実行	Security Operations ワークフローを選択して実行します。
View SLA timeline	タスク SLA レコードまたは SLA 定義から、SLA タイムラインを表示できます。
すべての関連リストを表示	すべての標準関連リストと手動で追加されたリストを表示します。 **注:** 手動で追加されたアイテムは、このビューでのみ使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
影響を受けるアイテムを表示	このインシデントによって直接影響を受ける CI、ユーザー、およびサービスのリストを表示します。
関連アイテムを表示	このインシデントの影響を受ける関連インシデント、CI、ユーザー、およびグループのリストを表示します。
IoC を表示	このインシデントに関連付けられた観測事象、インジケーター、マルウェア、モードとメソッド、およびセキュリティスキャン要求のリストを表示します。
拡張データを表示	このインシデントに関連付けられた拡張データ、プロセス、サービス、統計、ルックアップ、ファイアウォールログ、および侵害されたユーザー情報のリストを表示します。
対応タスクを表示	このインシデントに関連付けられたタスク、SLA、リスクスコア監査、機能停止、および Exchange 検索のリストを表示します。
詳細を外部システムで表示	このセキュリティインシデントが外部アプリケーションから、直接またはイベントによって生成されており、元のデータへのリンクが提供されている場合は、[詳細を外部システムで表示] アクションによって URL が開きます。このインシデントを生成したログ全体を表示および検索できます。
脆弱性のスキャン (Scan for Vulnerabilities)	脆弱性対応 がアクティブになっており、影響を受けるセキュリティインシデントの CI を少なくとも 1 つ選択している場合は、CI に存在する脆弱性を特定するためにスキャン要求を送信できます。

自動翻訳

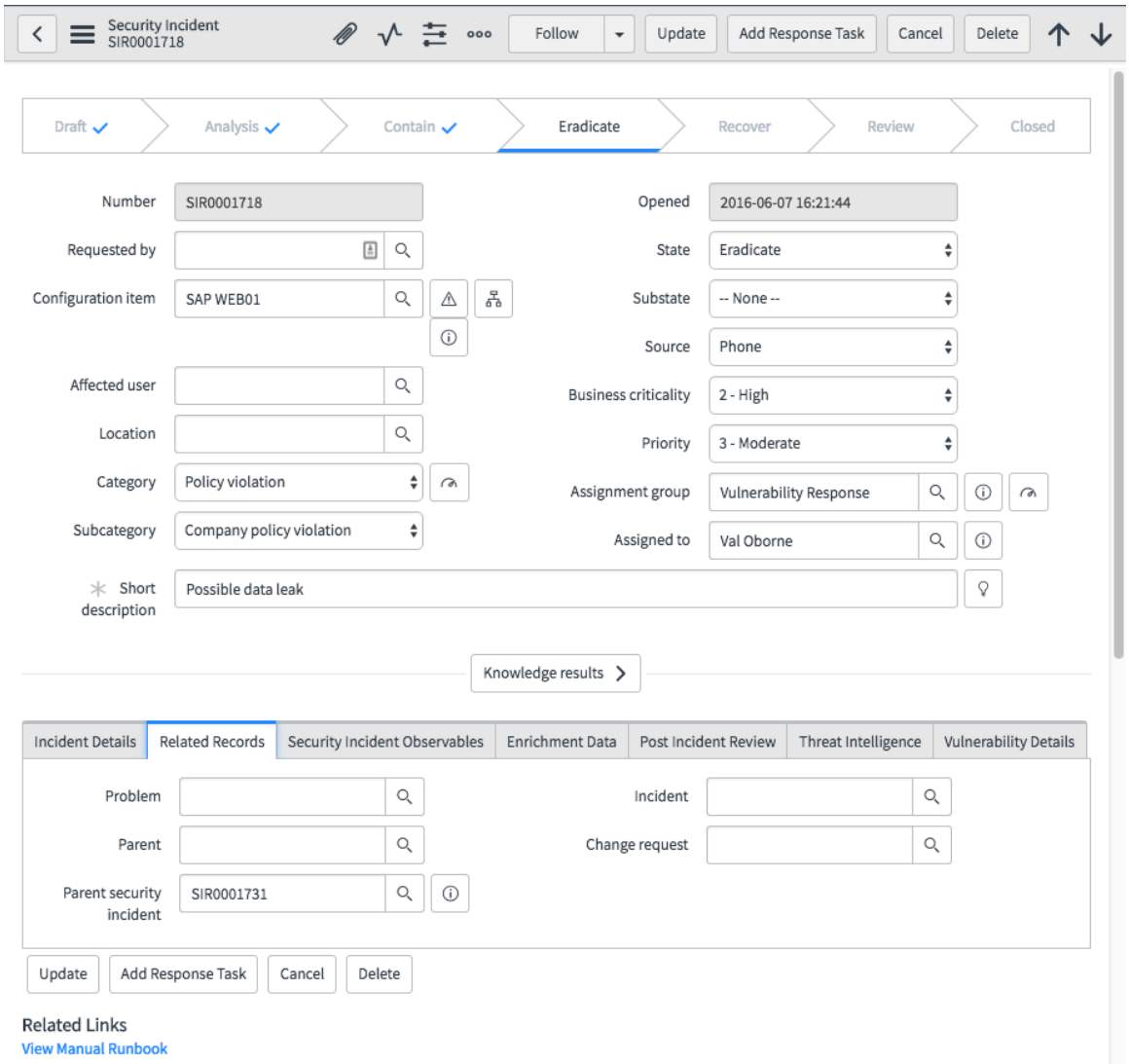
親と子のセキュリティインシデントの関係

セキュリティインシデントレスポンス の親と子のセキュリティインシデント関係を使用して、特定の問題の影響を関連付けて追跡できます。

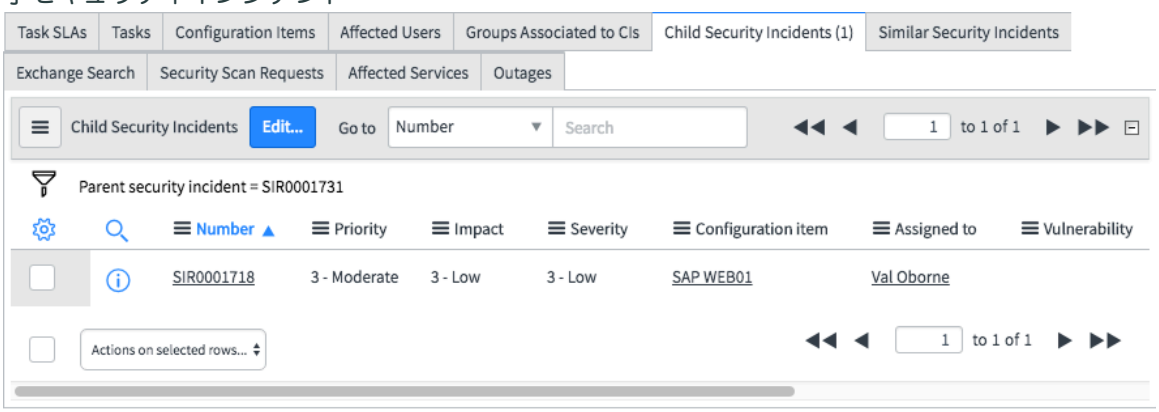
[関連レコード] タブを使用すると、[親セキュリティインシデント] の問題を任意の セキュリティインシデントレスポンス フォームに追加できます。この機能により、インシデントは自動的に親問題の [関連リスト - 子セキュリティインシデント **(Related Lists - Child Security Incidents)]** タブに表示される子になります。

注:
両方のインシデントに同じ番号を使用して、既存の親セキュリティインシデントをその子にすることはできません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



子セキュリティインシデント

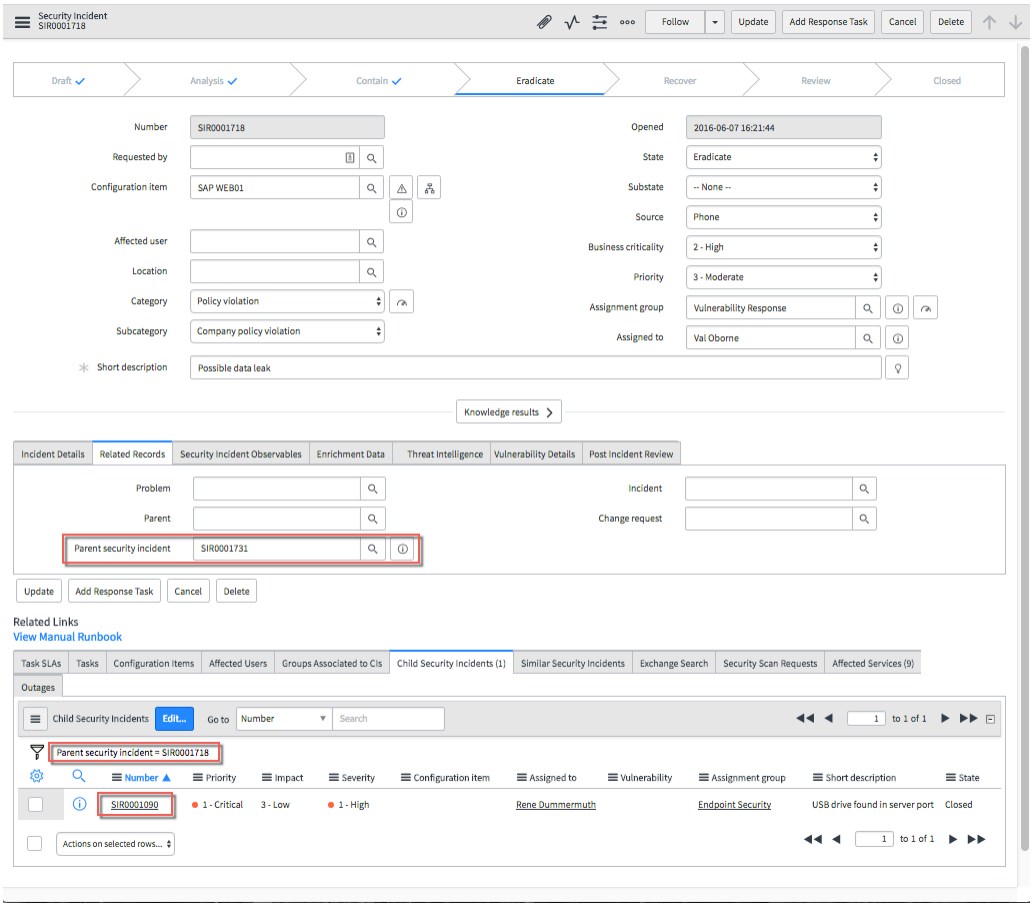


[子セキュリティインシデント] タブの [編集] ボタンを使用して、任意のセキュリティインシデントレコードに 1 つ以上の [子セキュリティインシデント] を追加することもできます。次の例では、3 つのレコードがすべて関連付けられています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

祖父母、親、および子のセキュリティインシデント



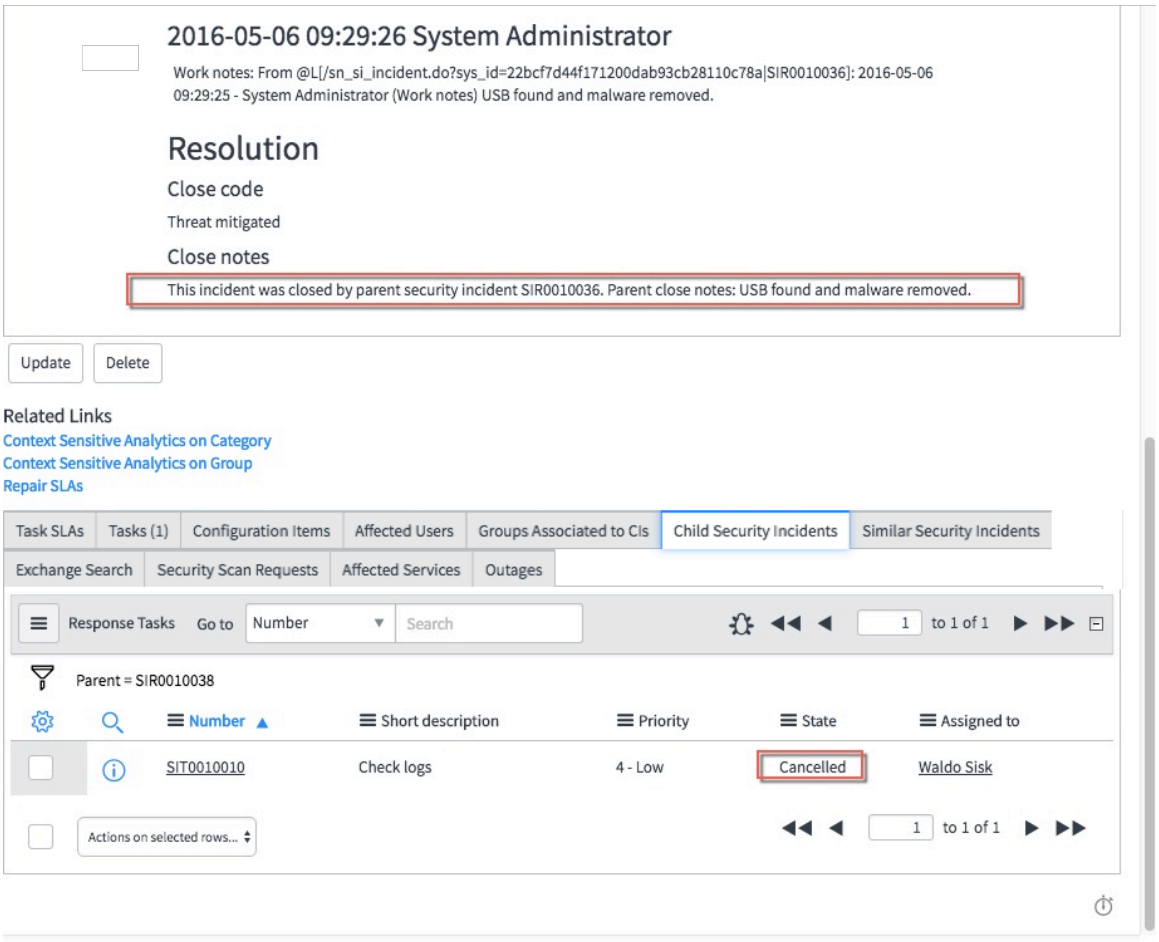
注意：親に記録されたすべての作業メモは、[インシデントの詳細] タブの [アクティビティ] のアクティブな子に伝播されます。

親がクローズまたはキャンセルされると、アクティブな子もクローズまたはキャンセルされます。子インシデントのアクティブな [応答タスク] はすべてキャンセルされます。他にオープンな [タスク] がない場合、子インシデントはクローズされます。クローズすると、[インシデントの事後レビュー] にクローズが記録され、[クローズ情報] タブで見つかった情報が親から子に伝播されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

子応答タスクのクローズ



セキュリティインシデントの影響を受けるアイテムの表示

セキュリティインシデントに関連付けられた CI、影響を受けるユーザー、影響を受けるサービスなどの、影響を受けるアイテムを表示できます。

始める前に

必要なロール：sn_si.basic

手順

1. 影響を受けるアイテムを表示するセキュリティインシデントがまだ開いていない場合は、これを開きます。
2. [影響を受けるアイテムを表示] 関連リンクをクリックします。
3. いずれかの関連リストをクリックし、セキュリティインシデントの情報を表示または追加します。

タブ	説明
構成アイテム	影響を受ける構成アイテム (CI)。影響を受ける CI が特定されたら、影響を受けるリソースをこの関連リストから手動で追加できます。
影響を受けるユーザー	影響を受けるユーザーが特定されたら、影響を受けるユーザーをこの関連リストから手動で追加できます。
影響を受ける	セキュリティインシデントに関連付けられたビジネスサービスを表示または追加します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タブ	説明
サービス	注: セキュリティインシデントがオープンされた後に影響を受ける CI が追加された場合は、フォームヘッダーを右クリックし、[影響を受けたサービスのリフレッシュ] を選択することをお勧めします。

注:
[Security Operations Integration：実行中のプロセスを取得] 統合機能がアクティブな場合に、CI をセキュリティインシデントに追加すると、[実行中のプロセスを取得] ワークフローが実行され、CI で実行中のプロセスのリストが取得されます。

[Security Operations Integration：ホストを隔離] 統合機能がアクティブな場合は、1 つ以上の CI を選択し、他のデバイスへのそれらのシステム接続を制限できます。これを行うには、CI のチェックボックスをオンにして、[選択した行のアクション] 選択リストから [ホストを隔離] をクリックします。

4. さらにセキュリティインシデントを更新するには、以下の関連リンクのいずれかをクリックします。
   - 関連アイテムを表示
   - IoC を表示
   - 拡張データを表示
   - 対応タスクを表示
5. 入力が完了したら、[送信] をクリックします。

セキュリティインシデントの関連アイテムの表示

セキュリティインシデントに関連付けられた類似のセキュリティインシデントと子セキュリティインシデント、関連するユーザー、脆弱性グループ、脆弱性一致アイテムなどの関連アイテムを表示できます。

始める前に
必要なロール：sn_si.basic

手順

1. 関連アイテムを表示するセキュリティインシデントがまだ開いていない場合は、これを開きます。
2. [関連アイテムを表示] 関連リンクをクリックします。
3. いずれかの関連リストをクリックし、セキュリティインシデントの情報を表示または追加します。

タブ	説明
子セキュリティインシデント	このセキュリティインシデントを作成する原因となった問題に関連するタスクレコードを選択します。
類似のセ	同じ観測事象レコードに関連付けられた他のセキュリティインシデントを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タブ	説明
キュリティインシデント	
関連する構成アイテム	このセキュリティインシデントと同じ観測事象を持つ構成アイテムを含むセキュリティインシデントのリストを表示します。このリストは、**[CI** 除外] フィルターグループを使用してフィルタリングできます。観測事象がセキュリティインシデントに追加されると、このリストが自動的に更新されます。デフォルトでは、コンテキストタイプが [宛先] の観測事象は除外されます。
関連ユーザー	このセキュリティインシデントと同じ観測事象を持つユーザーを含むセキュリティインシデントのリストを表示します。このリストは、[ユーザー除外 **(User exclusion)]** フィルターグループを使用してフィルタリングできます。観測事象がセキュリティインシデントに追加されると、このリストが自動的に更新されます。デフォルトでは、コンテキストタイプが [宛先] の観測事象は除外されます。
関連フィルターグループ	構成アイテムが識別されると、一致する CI またはフィルターグループが自動的に追加されます。
脆弱性グループ	脆弱性対応 がアクティブになっている場合、このセキュリティインシデントに関連付けられた脆弱性グループを表示できます。
脆弱性一致アイテム	脆弱性対応 がアクティブになっている場合、このセキュリティインシデントに関連付けられた脆弱性一致アイテムを表示できます。
リスク	いずれかのコアリスク管理プラグイン (ポリシーとコンプライアンス管理、Audit Management、またはリスク管理) がアクティブになっている場合、セキュリティインシデントに関連付けられたリスクを表示または追加できます。 この関連リストは、下のフォームヘッダーコンテキストメニューから追加できます 構成 > 関連リスト.
構成アイテムイベント	イベント管理 がアクティブになっている場合、イベントを表示できます。
構成アイテムアラート	イベント管理 がアクティブになっている場合、アラートを表示できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タブ	説明
カスタマーサービスケース	カスタマーサービス がアクティブになっている場合、カスタマーサービス ケース情報を表示できます。

4. さらにセキュリティインシデントを更新するには、以下の関連リンクのいずれかをクリックします。
   - 影響を受けるアイテムを表示
   - IoC を表示
   - 拡張データを表示
   - 対応タスクを表示
5. 入力が完了したら、[送信] をクリックします。

セキュリティインシデントの拡張データの表示

セキュリティインシデントに関連付けられた実行中のプロセス、実行中のサービス、ネットワーク統計などの拡張データを表示できます。

始める前に
必要なロール：sn_si.basic

手順
1. 拡張データを表示するセキュリティインシデントがまだ開いていない場合は、これを開きます。
2. [拡張データを表示] 関連リンクをクリックします。
3. いずれかの関連リストをクリックし、セキュリティインシデントの情報を表示または追加します。

> **注:**
> 生データの詳細は、拡張データレコードの添付ファイルに保存されます。詳細がフィールドの制限を超えた場合、表示される詳細は切り捨てられます。

タブ	説明
実行中のプロセス	セキュリティインシデントレスポンス [実行中のプロセスを取得] ワークフローによって作成されたレコードを保存します。
実行中のサービス	セキュリティインシデントレスポンス [実行中のサービスを取得] ワークフローによって作成されたレコードを保存します。
ネットワーク統計	セキュリティインシデントレスポンス [ネットワーク統計情報を取得] ワークフローによって作成されたレコードを保存します。
ドメインルックアップ	WhoisXML API Integration プラグインがアクティブになっている場合は、Whois ルックアップによって作成されたレコードを保存します。
ファイアウォールログ	Palo Alto Network ファイアウォールログなどのファイアウォールログからの拡張データを保存します。
侵害されたユーザー情報	[Have I Been Pwned?] ルックアップによって侵害されていると特定されたアカウントを保存します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注意：[セキュリティ拡張データ **(Security Enrichment Data)**] タブには、セキュリティインシデントレスポンス ワークフローからの生の拡張データ (ネットワーク統計情報や実行中のプロセスの取得など) が表示されます。このタブを表示するには、[すべての関連リストを表示] 関連リンクをクリックします。

4. さらにセキュリティインシデントを更新するには、以下の関連リンクのいずれかをクリックします。
   - 影響を受けるアイテムを表示
   - 関連アイテムを表示
   - IoC を表示
   - 対応タスクを表示
5. 入力が完了したら、[送信] をクリックします。

セキュリティインシデントの応答タスク情報の表示

セキュリティインシデントに関連付けられたタスク SLA、リスクスコア監査、機能停止などの応答タスク情報を表示できます。

始める前に
必要なロール：sn_si.basic

手順

1. 応答タスクを表示するセキュリティインシデントがまだ開いていない場合は、これを開きます。
2. [対応タスクを表示] 関連リンクをクリックします。
3. いずれかの関連リストをクリックし、セキュリティインシデントの情報を表示または追加します。

タブ	説明
タスク	セキュリティインシデントに対して既に定義されているタスクを表示します。応答タスクを手動で作成できます。
対応タスク	セキュリティインシデントに対応して実行するアクションを表示します。
SLA タスク	セキュリティインシデントに対して定義されたアクティブなタスク SLA を表示または追加します。
リスクスコアの監査	変更されるリスクスコアの各インスタンスの監査レコード。
機能停止	セキュリティインシデントに関連付けられた新しい機能停止レコードを表示するか、手動で追加します。
メールの検索	Microsoft® Exchange Server (インストールされている実装に基づく) などのメールサーバーでクエリを実行するための検索条件を保持し、受信した結果を格納するレコードのリスト **注:** 「Security Operations Integration - [メールの検索と削除] 機能」がアクティブでない場合、[メールの検索] 関連リンクは表示されません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. さらにセキュリティインシデントを更新するには、以下の関連リンクのいずれかをクリックします。
   - 影響を受けるアイテムを表示
   - 関連アイテムを表示
   - IoC を表示
   - 拡張データを表示
5. 入力が完了したら、[送信] をクリックします。

セキュリティインシデント内の関連イベントとアラートの表示

セキュリティインシデントの作業中に、イベントの詳細を表示できます。アラートの場合、これらのアラートを表示して確認し、必要に応じてそれらからインシデントまたはセキュリティインシデントを作成できます。

始める前に

セキュリティインシデントレスポンスイベント管理サポートプラグインをアクティブ化している必要があります。

必要なロール：si.sn_agent

手順

1. 任意のセキュリティインシデントリスト (例: **All** (すべて) > セキュリティインシデント > インシデント > 未アサインのインシデント) を開きます。
2. 表示しているセキュリティインシデントの影響を受けるリソースが過去 24 時間以内にアラートまたはイベントを受信している場合、次の関連リストの一方または両方が表示されます。
   - セキュリティインシデント CI アラート (Security Incident CI Alerts)
   - セキュリティインシデント CI イベント (Security Incident CI Events)
3. 表示したい関連リストをクリックします。

関連リスト	説明
セキュリティインシデント CI アラート (Security Incident CI Alerts)	過去 24 時間以内に受信したアラートの詳細を表示できます。[確認] をクリックすることで、自分がアラートに気付いており、現在処理中であることを示すことができます。アラートが重要でないことを示すには、[クローズ] を使用します。
セキュリティインシデント CI イベント (Security Incident CI Events)	過去 24 時間以内に受信したイベントの詳細を表示できます。

セキュリティインシデントからカスタマーサービスケースへのマッピングの表示

セキュリティインシデントレスポンス には、セキュリティインシデントを カスタマーサービス ケースにマッピングするデフォルトのフィールドマッピングが付属しています。セキュリティインシデントから CS ケースへのデフォルトマップを表示できます。

始める前に

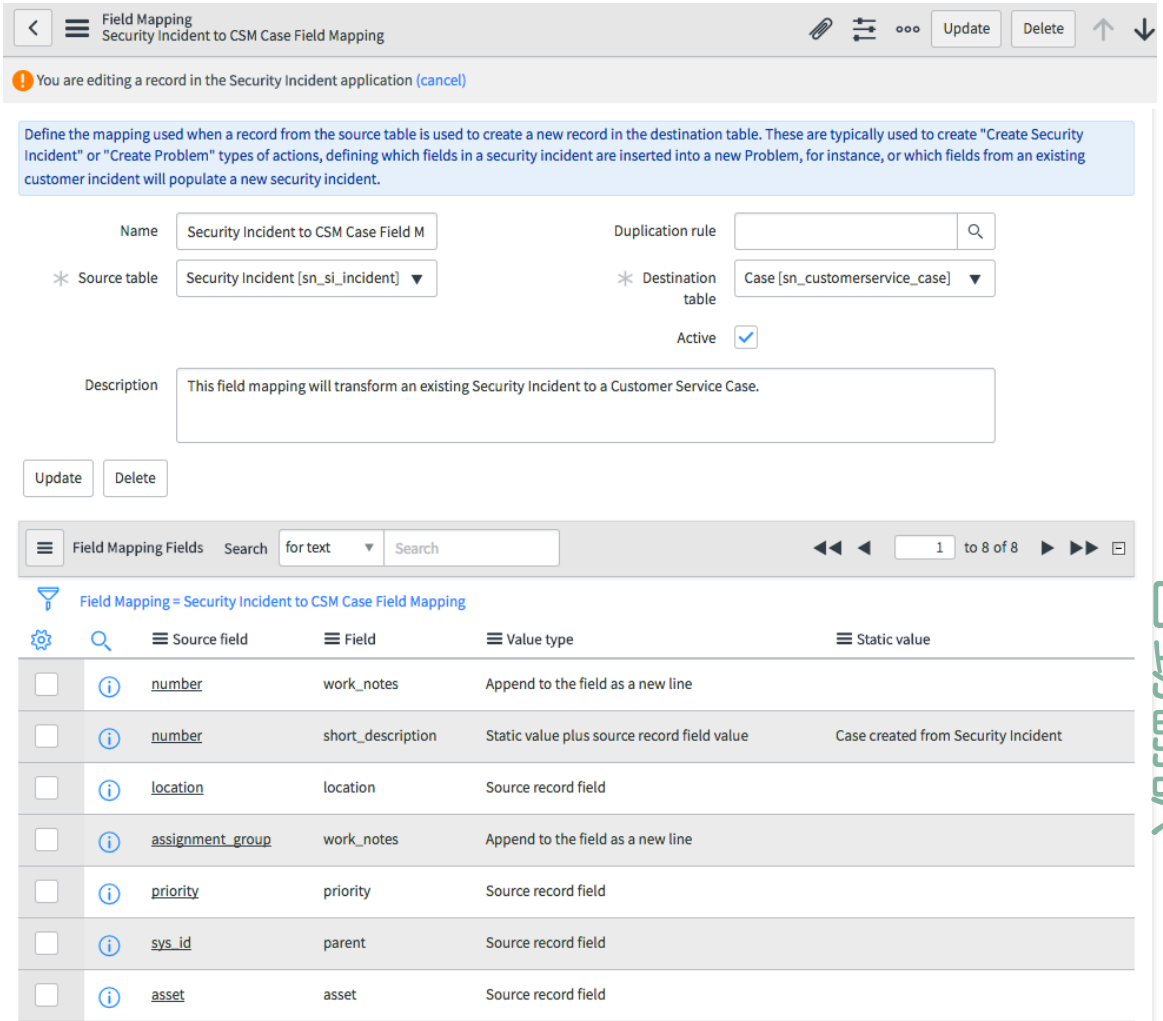
必要なロール：sec_cmn.read

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > ユーティリティ > フィールドマッピング.
2. [セキュリティインシデントから **CSM** ケースへのフィールドマッピング **(Security Incident to CSM Case Field Mapping)]** をクリックして、デフォルトマップを表示します。



3. 必要に応じてマッピングを編集できます。
4. 変更が完了したら、[更新] をクリックします。

セキュリティインシデントレスポンス **Runbook** の表示

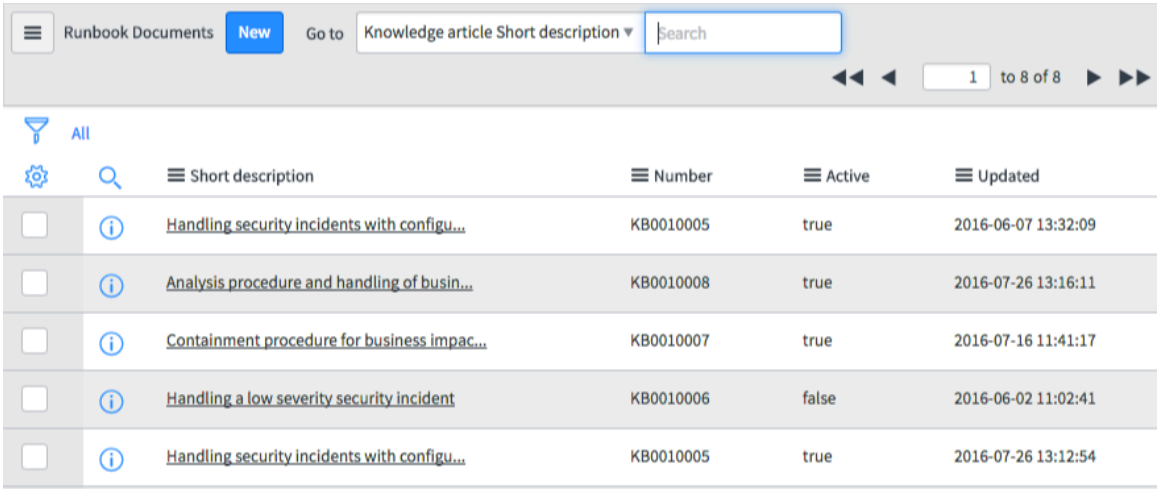
Runbook を使用すると、作業中のタスクに関連する手順にアクセスできます。

始める前に
必要なロール：sn.si.knowledge_admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > 手動 **Runbook** > **Runbook** ドキュメントを表示.
2. リストから Runbook を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. Runbook を作成するには、[新規] をクリックします。
   詳細については、「Create a runbook (Runbook の作成)」を参照してください。

セキュリティインシデントの影響を受けるすべての構成アイテムの特定

セキュリティインシデントの背後にあるリソース (サーバー、デスクトップ、またはその他の構成アイテム) がわかっていて、影響を受ける可能性のある関連リソースとビジネスサービスを特定したい場合は、ビジネスサービス管理 (BSM) マップを使用できます。

始める前に

必要なロール：admin、sn_si.admin

このタスクについて

BSM マップには、選択したルート CI の上流および下流の依存関係が表示されます。

CI の BSM マップを表示するために使用できる方法は 2 つあります。

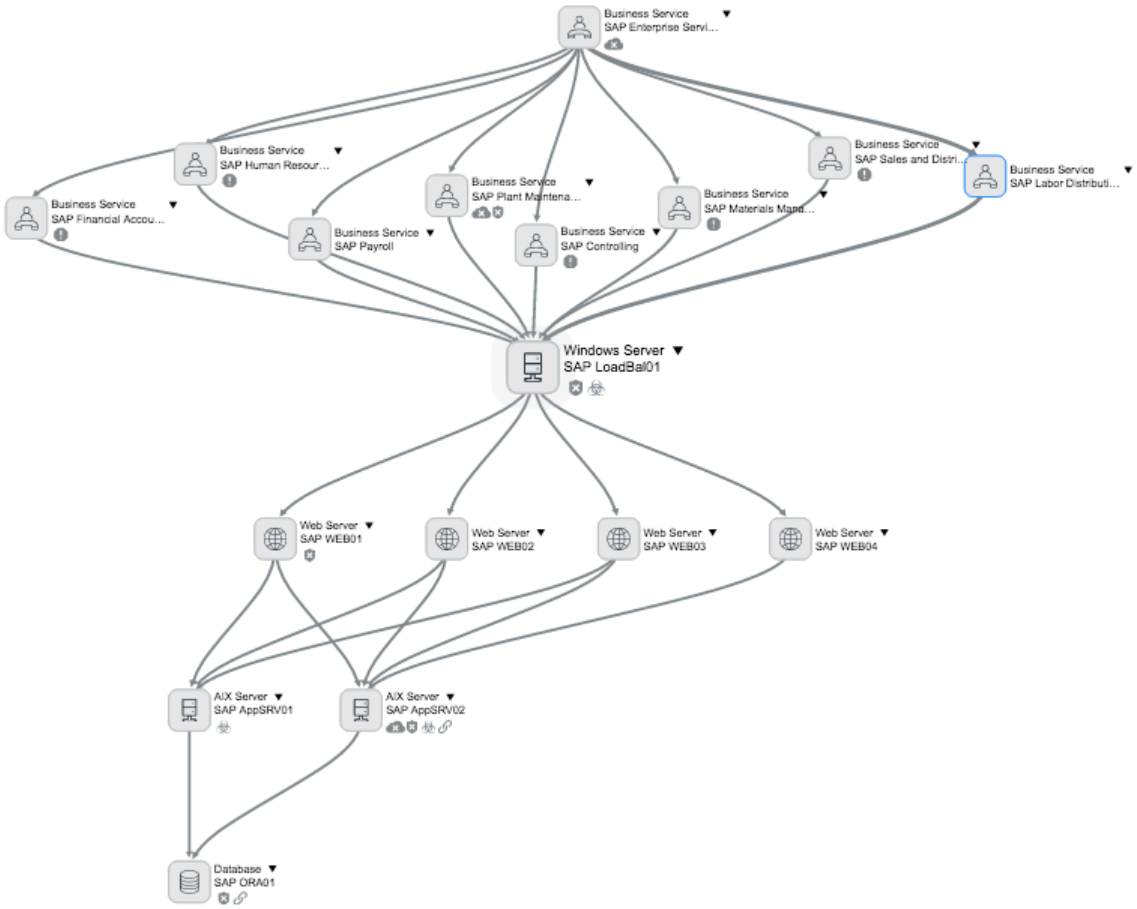
- タスクのコンテキストから CI を表示したい場合は、セキュリティインシデントフォームから表示します。
- タスクの視点から CI を表示したくない場合は、ナビゲーションバーから表示します。

手順

1. [セキュリティインシデント] フォームから、[構成アイテム] フィールドに入力し、BSM マップアイコン ( ) をクリックします。
   BSM マップ画面には、インシデント管理で最後にアクセスしたインシデントのマップ、またはセキュリティインシデント管理で最後にアクセスしたセキュリティインシデントのマップが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



2. 構成アイテムの横にあるアイコンをクリックすると、リソース (サーバー、デスクトップ、またはその他の CI) に関するさまざまな種類の詳細が表示されます。
   たとえば、(⚠) をクリックすると、CI に関連付けられているアラートが表示されます。

   注:
   利用可能なすべてのアイコンのリストを表示するには、BSM マップの上にある [フィルター] をクリックし、[フィルタータスクタイプ **(Filter Task Types)]** を展開します。

3. マップをさまざまな構成で並べ替えるには、マップの上にリストされている形式 ([垂直]、[水平]、[放射状]) のいずれかを選択するか、[フィルター] をクリックしてマップをフィルタリングして見やすくします。
4. セキュリティインシデントフォームから BSM マップを開いた場合は、CI を右クリックして [影響を受ける **CI** を追加] を選択すると、セキュリティインシデントに依存 CI を追加できます。
   一度に複数の CI を追加することもできます。追加する CI を囲むようにボックスをドラッグし、ボックスを右クリックして [影響を受ける **CI** を追加] を選択します。
   CI はセキュリティインシデントの [影響を受ける CI] 関連リストに追加されます。

セキュリティインシデントの重大度の計算

事前定義された算出を使用して、セキュリティインシデントの重大度を計算できます。

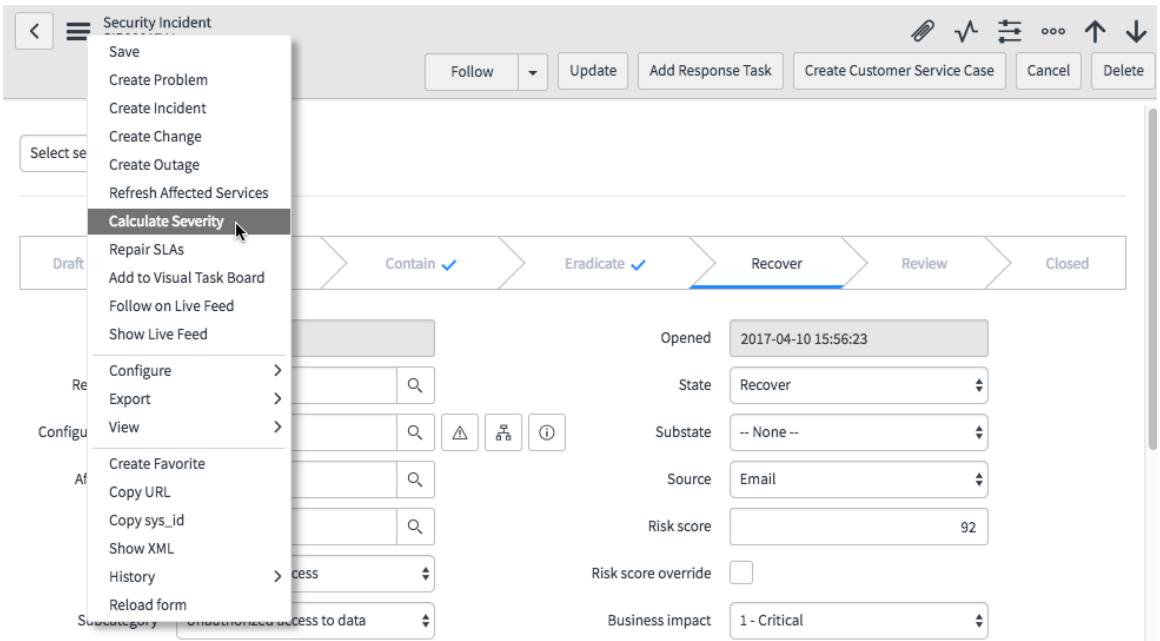
始める前に
必要なロール：sn_si.basic

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. まだ開いていない場合は、重大度を計算するセキュリティインシデントを開きます。
2. フォームヘッダーのコンテキストメニューをクリックし、[重大度の計算] を選択します。



重大度は、ベースとなる算出の事前定義されたルールに基づいて計算されます。詳細については、「セキュリティインシデント算出の理解」を参照してください。

フィッシングメールの検索と削除

フィッシングメールを削除すると、組織全体で特定の攻撃にさらされるリスクを低減できます。メールサーバーでフィッシングメールを管理するには、それらのメールの検索、承認の付与、および削除を行います。

始める前に

必要なロール：sn_sec_cmn.cap_email_read

セキュリティインシデントに関連付けられたメールレコードのクエリを実行することで、フィッシング攻撃のターゲットとなったユーザーの数を特定できます。

サポートされているソフトウェア：

- Microsoft® Exchange Server 2010

制限事項：メールの本文を検索する場合は、最大 1,500 個のメールボックスを検索できます。

このタスクについて

この機能は、Security Operations Integration - メールの検索と削除フロー でメールサーバーに対してクエリを実行するために使用されます。選択した検索条件に応じて、検索ではフィッシング攻撃内のすべてのメールが識別され、影響を受けたメールの合計数または影響を受けたメールの詳細が返されます。

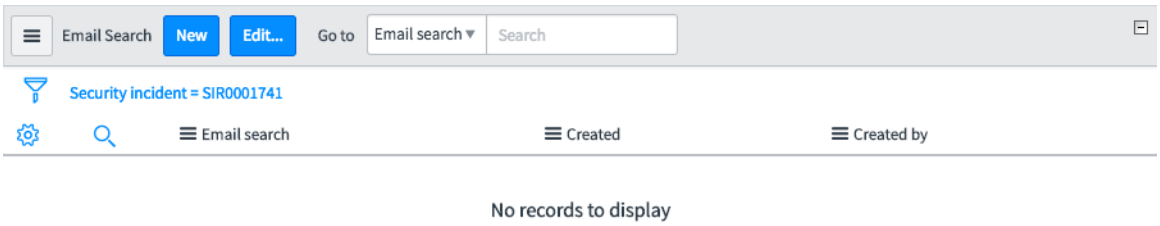
手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > オープンインシデントを表示.
2. セキュリティインシデントを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

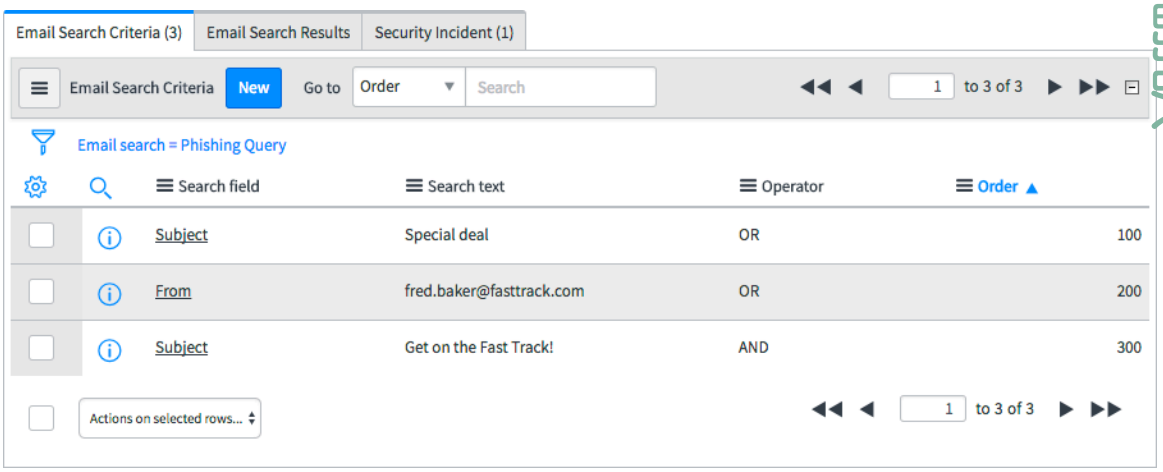
3. [メールの検索 **(Email Search)**] 関連リストが表示されない場合は、[すべての関連リンクを表示 **(Show All Related Links)**] 関連リンクをクリックします。
4. [メールの検索 **(Email Search)**] 関連リストをクリックします。



5. [新規] をクリックします。
6. 必要に応じてフィールドに入力します。

フィールド	説明
名前	検索クエリの名前
条件から生成されたクエリ	メールサーバーで実行されるクエリのプレビュー。関連付けられたすべてのアクティブな検索条件レコードから生成されます。
説明	検索クエリが何を探しているかを説明します。

7. フォームヘッダーを右クリックし、[保存] を選択します。



8. [メール検索基準] タブをクリックし、[新規] をクリックします。
9. 必要に応じてフィールドに入力するか、フィールドの内容を編集します。

フィールド	説明
メールの検索	メール検索の名前を表示します。これは必要に応じて変更できます。
検索フィールド	メールサーバー内を検索するフィールド。 検索フィールドには次の選択肢があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	件名 この条件は、[検索テキスト] フィールドで指定された件名テキストを含むメールを検索します。この検索条件を満たしているメールについて、フィッシングメールの合計数と、各メールの詳細 (受信したメールの日付、メール読み取りステータス、受信者、メッセージ ID など) が返されます。 送信元 この条件は、[検索テキスト] フィールドで指定された送信者の正確なメールアドレス (jane.doe@abc.com など) を含むメールを検索します。この検索条件を満たしているメールについて、フィッシングメールの合計数と、各メールの詳細 (受信したメールの日付、メール読み取りステータス、受信者、メッセージ ID など) が返されます。 **注:** 同じクエリで [送信元] フィールドと [受信者] フィールドを使用することはできません。 受信者 この条件は、[検索テキスト] フィールドで指定された受信者の完全なメールアドレス (john.doe@abc.com など) を含むメールを検索します。また、[宛先]、[CC]、および [BCC] フィールドでもメールを検索します。この検索条件を満たしているメールについて、フィッシングメールの合計数と、各メールの詳細 (受信したメールの日付、メール読み取りステータス、受信者、メッセージ ID など) が返されます。 **注:** 同じクエリで [送信元] フィールドと [受信者] フィールドを使用することはできません。 本文 この条件は、[検索テキスト] フィールドで指定された本文を含

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

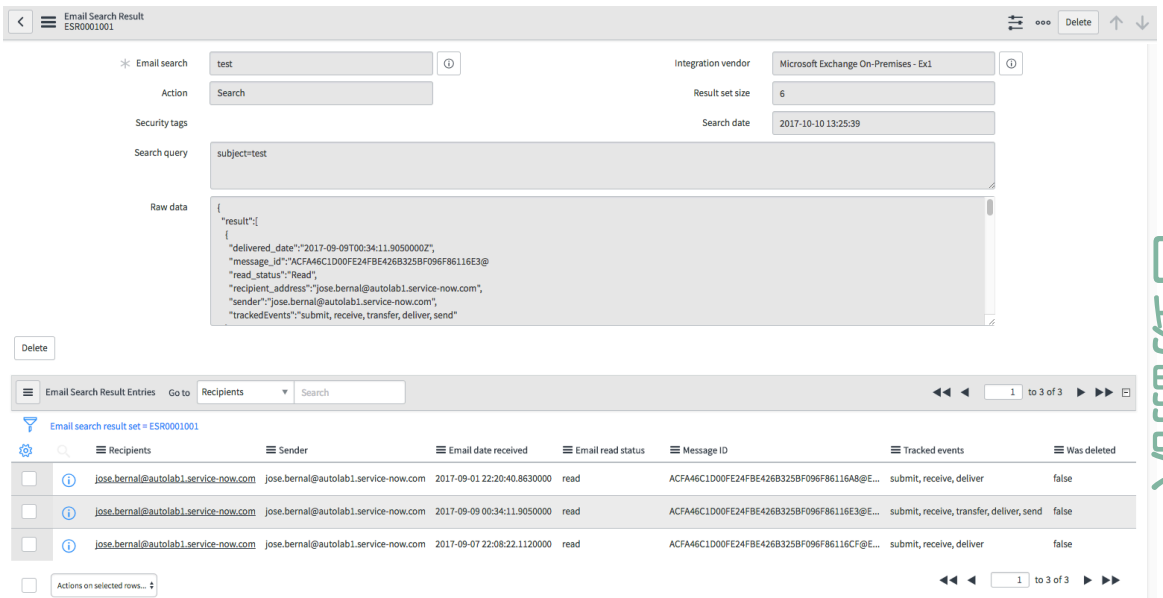
フィールド	説明
	むメールを検索します。この検索条件を満たしているメールについて、フィッシングメールの合計数が返されます。 **注:** メールの本文を検索する場合は、最大 1,500 個のメールボックスを検索できます。 CC： この条件は、[検索テキスト] フィールドで指定された CC の完全なメールアドレス (jane.doe@abc.com など) を含むメールを検索します。この検索条件を満たしているメールについて、フィッシングメールの合計数が返されます。 Bcc： この条件は、[検索テキスト] フィールドで指定された BCC の完全なメールアドレス (jane.doe@abc.com など) を含むメールを検索します。この検索条件を満たしているメールについて、フィッシングメールの合計数が返されます。 添付ファイル この条件は、[検索テキスト] フィールドで指定された添付ファイル名または添付ファイルのコンテンツを含むメールを検索します。この検索条件を満たしているメールについて、フィッシングメールの合計数が返されます。 **注:** 添付ファイルのコンテンツの検索では、プレーンテキスト形式の添付ファイルのみがサポートされています。 保持ポリシー この条件は、[検索テキスト] フィールドで指定された保持ポリシー番号を含むメールを検索します。この検索条件を満たしているメールについて、フィッシングメールの合計数が返されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

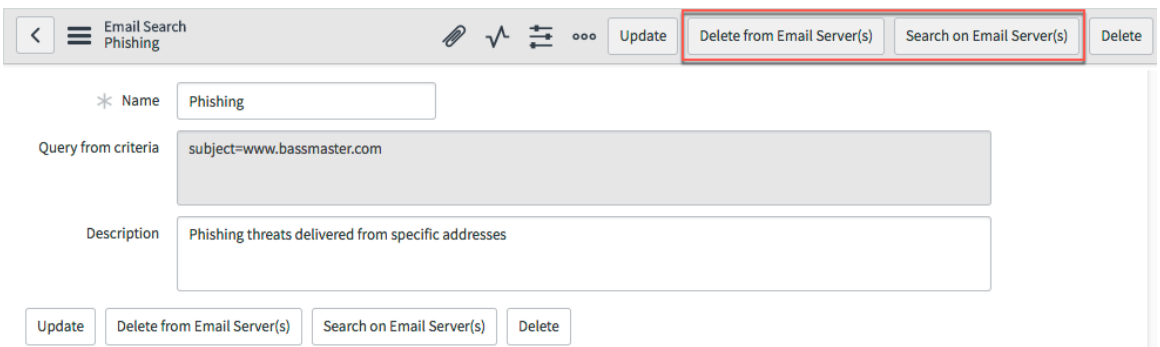
フィールド	説明
有効	このメール検索クエリをアクティブにするには、このチェックボックスをオンにします。
演算子	可能な値は、AND および OR です。メールサーバーで実行する検索条件をどのように組み合わせるかを定義できます。
順序	検索条件から検索クエリが作成される順番。
検索テキスト	検索するテキスト。一重引用符、二重引用符、およびコロンはサポートされていません。

10. **[Submit]** をクリックします。
11. 必要に応じて繰り返し、追加の検索条件を定義します。
12. [メールの検索結果] タブをクリックすると、検索の結果を表示できます。



[メールの検索結果エントリー] フォームの各行は個別のメールを表します。

13. 検索条件レコードを作成すると、[メールサーバーから削除] と [メールサーバーで検索] の 2 つのボタンが [メールの検索] フォームに表示されます。



14. 選択したサーバー内で、定義した検索条件に一致するメールを検索するには、[メールサーバーで検索] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントナレッジ記事の作成

セキュリティインシデントと応答タスクを処理すると、作業中のタスクについての関連情報を提供するナレッジ記事が自動的に表示されます。組織でセキュリティインシデントナレッジベースに記事を作成し、管理できます。

始める前に
必要なロール：sn.si.knowledge_admin

このタスクについて
ナレッジ記事はセキュリティ情報を共有し、組織が直面しているサイバー脅威のタイプを文書化し、これらの脅威に対する回答と対応方法を提供します。
必要に応じて、ナレッジ記事を Runbook に整理して、記事と特定のタスクを関連付けることができます。たとえば、フィッシング攻撃のセキュリティインシデントを作成するときに、フィッシングに関するナレッジベース記事が表示されるように、条件付きで Runbook を構成することができます。詳細については、「セキュリティインシデントレスポンス Runbook の作成」を参照してください。

Runbook のナレッジ記事は、プレイブックの特定のタスクに関連付けることもできます。詳細については、「ナレッジ記事とプレイブックタスクの関連付け」を参照してください。

ナレッジ記事には次のようなメリットがあります。

- 従業員は 1 つのソースから情報を簡単に検索できます。
- ナレッジ記事にはライフサイクル (作成、レビュー、更新、公開、廃止) が定義されているため、情報を常に最新の状態にしておくことができます。
- セキュリティ要求、インシデント、または応答タスクを手動で作成すると、簡単な説明を入力するに伴い関連記事のリストが表示されます。

> **注:**
> それぞれのセキュリティインシデントナレッジベースにナレッジマネージャーをアサインしてください。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > カタログとナレッジ > ナレッジ.
2. [記事の作成] アイコン ( ) をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

ナレッジ フォーム

フィールド	説明
数値	自動的に生成される KB 番号
ナレッジベース	この記事に対して選択されたナレッジ ベース。
カテゴリ	この記事のカテゴリ。
公開	このナレッジ記事が公開された日付。この値は記事が作成されたときに設定され、記事が公開されたときに更新されます。
有効期限	このナレッジ記事の有効期限が切れる日付。この日付以降、または日付が選択されていない場合、この記事は検索結果に表示されません。
画像	従来のナレッジポータルから検索するときに記事の横に表示される画像

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ワークフロー	[読み取り専用] [ドラフト]、[公開済み] などの記事の公開ステータス時期 既存の記事から新しい記事を挿入する と、新しい記事のステータスは [ドラフト] にリセットされます。
ソース	このナレッジ記事の作成の根拠であるタスク (存在する場合)。このフィールドは、タスク レコードからナレッジ記事を作成すると自動的に設定されます。
添付ファイルへ直接リンク	記事ビューを開く代わりに、ユーザーが記事にアクセスしたときに添付ファイルを自動的にダウンロードするためのチェックボックス。このオプションを使用するには、記事に添付ファイルを追加します。
添付ファイルの表示	このナレッジ記事を表示しているユーザーに添付ファイルを表示するためのチェックボックス。添付ファイルは記事テキストの下に表示されます。このオプションを使用するには、記事に添付ファイルを 1 つ以上追加します。
簡単な説明	記事のタイトル。このタイトルは、ナレッジを参照したり検索したりするときに、記事の上部に表示されます。
テキスト	記事のコンテンツ。WYSIWYG HTML エディターを使用してコンテンツを作成します。ナレッジを参照して検索するときにコンテンツのプレビューが表示されます。

注:
プレイブックタスクに関連付けるナレッジ記事を作成する場合は、[ナレッジベース] フィールドを [セキュリティインシデントレスポンス **Runbook]** に設定します。

4. [送信] をクリックして記事を作成します。

次のタスク
記事の公開に必要な追加手順 (承認など) は、 ナレッジベースの公開ワークフロー によって異なります。

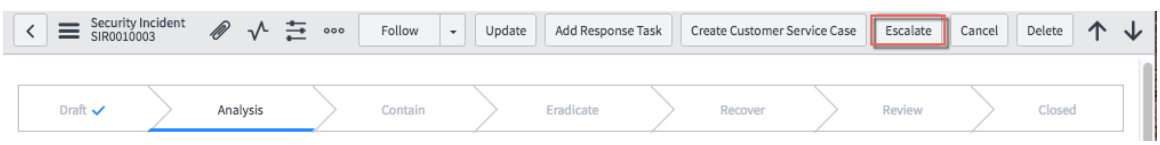
関連情報
セキュリティインシデントレスポンス Runbook の作成

セキュリティインシデントのエスカレーション

セキュリティインシデントにエスカレーションパスが存在する場合、セキュリティインシデントヘッダーで [エスカレート] ボタンを使用できます。

始める前に
必要なロール：sn_si.admin
このボタンが表示されるには、エスカレーショングループが作成されている必要があります。詳細については、「セキュリティオペレーション ユーザー定義のエスカレーショングループの作成」を参照してください。

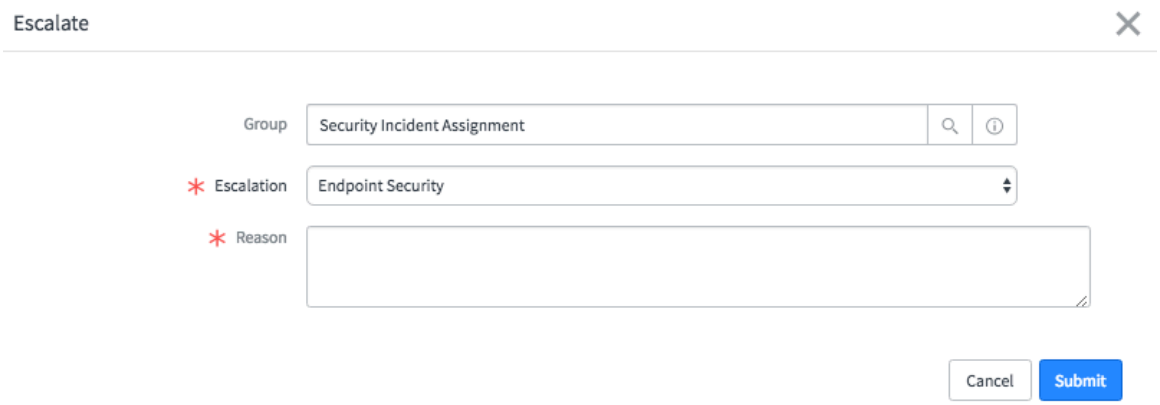
手順
1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > オープンインシデントを表示.
2. エスカレートするインシデントを開きます。
3. [エスカレート] ボタンをクリックします。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. エスカレーショングループを選択します。
5. エスカレーションの理由を入力します。



6. [送信] をクリックします。
   セキュリティインシデントの [アサイン先グループ] と [アサイン先] を更新します。

インシデントの事後アクティビティの管理

多くの場合、ビジネスの要件に基づいて作成元のレビューとセキュリティインシデントの処理が必要です。

ServiceNow のインシデントの事後レビュー機能では、このプロセスを自動化、追跡、監査、簡素化する多くのツールが利用できます。

このセクションでは、以下について説明します。

- インシデントの事後レビューのロールのアサイン
- アセスメントのトリガー条件の設定
- アンケートベースのインシデントの事後レビューの実施
- PIR アサインルールの作成
- インシデントの事後レビューレポート

インシデントの事後レビューのロールのアサイン

インシデントの事後レビュー (PIR) カテゴリにロールをアサインすることで、事前定義された特定のグループを質問の対象にすることができます。

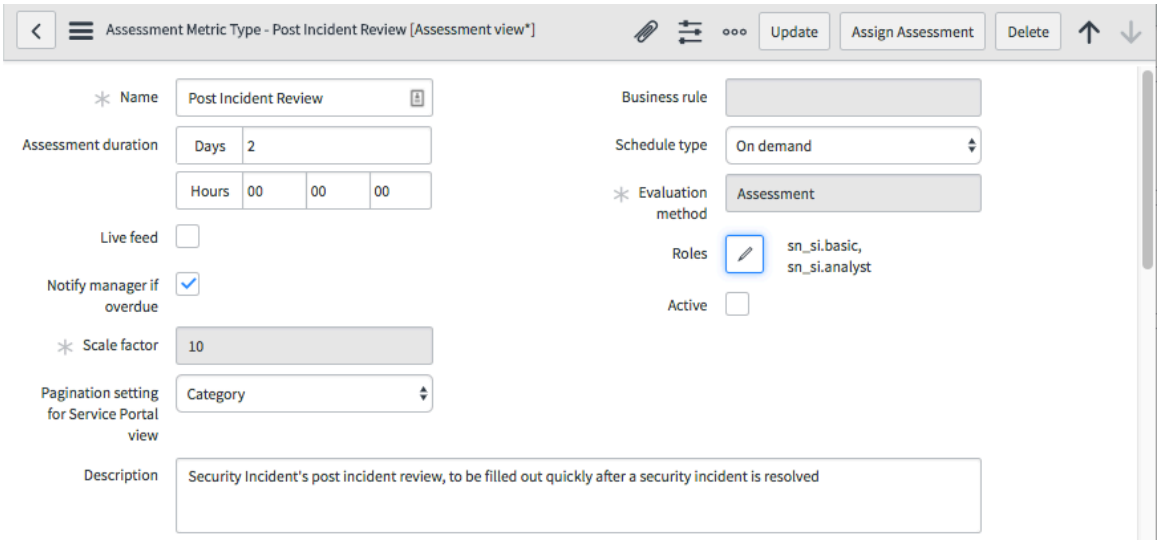
始める前に

必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > アセスメント > メトリクスの定義 > タイプ.
2. [タイプ] 列で、[インシデントの事後レビュー] レコードを検索します。
3. レコードを開きます。
4. この質問のカテゴリに 1 つ以上のロールをアサインします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. **[Update** (更新)] をクリックします。
6. 次のように移動する。 ユーザー管理 **(User Administration)** > ユーザー.
7. ユーザーを選択します。
8. ユーザーレコードに 1 つ以上のメトリクスタイプのロールを追加します。

> **注:**
> ロールは、[インシデントの事後レビュー] カテゴリでアサインされたロールに対応している必要があります。

インシデントの事後レビューレポート

インシデントの事後レビュー (PIR) レポート機能により、[インシデントの事後レビュー] タブを使用してインシデントの事後レビューレポートを設定およびダウンロードできます。

セキュリティアドミニストレーターは、レポートテンプレートを作成して構成し、レポート構成を使用してそれらのテンプレートをセキュリティインシデントにマッピングできます。セキュリティインシデントが解決され、ステータスが [レビュー] に更新された後で、セキュリティアナリストがレポートを表示またはダウンロードできます。

構成が正常に完了した後でセキュリティインシデントのステータスが [クローズ済み] に変わると、PDF レポートが生成されてセキュリティインシデントに添付されます。

> **注:**
> レポート機能は、Orlando Patch9 から適用およびサポートされています。

インシデントの事後レビューレポートをカスタマイズするには、次の構成を行う必要があります。

1. レポートテンプレート：次のレポートテンプレート機能をカスタマイズして設定し、補足情報をレポートに追加します。
   a. タイムライン
   b. 自社用カスタム設定
   c. テンプレートスクリプト
2. レポート構成

このセクションでは、構成手順を説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レポートテンプレート

[レポートテンプレート] セクションを使用して、インシデントの事後レビューレポートを生成するためにセキュリティインシデントに適用されるプライマリレポートテンプレートと追加のレポートテンプレートを作成します。要件に基づいてレポートの書式設定と構成を行うことができます。テンプレートは、アセスメントの詳細をテンプレートに組み込むときにも役立ちます。

テンプレートの作成中に実行できるいくつかのオプションの手順を次に示します。

1. ブランディング情報を構成します。
2. ページサイズとページマージンを設定します。
3. セキュリティインシデント関連フィールド (カスタムと標準の両方) を追加します。
4. 次の事前定義されたカスタムトークンを使用します。
   a. *$sessionUser*：ログインしているユーザー名を返します
   b. *$date*：現在の日付を返します
   c. *$if_not_null_start#&#$if_not_null_end* これらのタグがいずれかのフィールドに対して使用されている場合には、値が存在する場合にのみタグが表示されます。次に例を示します。
      - *${if_not_null_start:problem}*
      - *Problem Category: ${problem.category}*
      - *${if_not_null_end:problem}*
5. テンプレートスクリプトを使用して関連リストデータを含めます。詳細については、以下の「テンプレートスクリプト」セクションを参照してください。
6. タイムラインフィルターを使用してタイムライン情報を含めます。詳細については、以下の「タイムライン」セクションを参照してください。
7. 添付ファイル、テーブル、画像などのテンプレートコンテンツを管理し、書式設定します。

> **注:**
> 拡張レポートテンプレートツールバー機能は、Paris リリースバージョン以降でのみ使用できます。

レポートテンプレートの重要なポイント：

1. レポートテンプレートに添付された画像は、sys_attachment テーブルに含まれている場合にのみ、インシデントの事後レビューレポートに表示されます。

   > **注:**
   > db_image テーブルから選択された画像は、インシデントの事後レビューレポートには表示されません。

2. インシデントの事後レビューレポートではビデオはサポートされていません。
3. PDF 内の URL はクリックできません。URL を有効にするため、クリック不可 (.) は (ドット) として示されます。
4. レポートテンプレートのサイズが 50 MB を超えるている場合、レポートは生成されません。
5. レポートテンプレートコンテンツ用に選択されたフォントファミリーは、PDF ジェネレーターでサポートされていない場合、PDF には適用されません。

   > **注:**
   > 対応するフォントが存在しない場合、PDF ジェネレーターは最も近い代替フォントを特定して PDF を生成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

6. ページマージンの値を大きくすると、インシデントの事後レビューレポートの生成が失敗します。たとえば、上と下のマージンが 450 よりも大きい場合、および左と右のマージン が 450 よりも大きい場合などです
7. スペースのないレポートテンプレートに大きなテキストが含まれている場合、テキストが切り捨てられることがあります。テキストをプレビューし、必要に応じてテキストを変更します。

セキュリティアドミニストレーターは、[レポートテンプレート (Report Template)] ページで使用可能な [レポートをプレビュー] ボタンを使用してレポートをプレビューできます。

注:

[このテンプレートでレポートをプレビューするには、セキュリティインシデントを選択してください] オプションを選択して、[レポートをプレビュー] をクリックします。

自社用カスタム設定

レポートテンプレートの作成後に、レポートテンプレートにブランディングテンプレート名、ヘッダーとフッターの画像、ヘッダーとフッターのテキストを追加し、ページ番号を生成し、ブランディングレコードを含めることができます。

ブランディングレポート形式の例を次に示します。

レポートテンプレートのブランディングの重要なポイント：

1. ヘッダーとフッターの画像の最大サイズは 5 MB です。サイズが指定された制限を超えると、「画像の形式を認識できません (Image format cannot be recognized)」というエラーメッセージがセキュリティインシデントに表示されます。
2. フッターのテキストの長さは 100 文字に制限されています。
   a. プレビュー中にフッター画像とフッターテキストがレポートコンテンツに重なり合う場合は、ブランディングレコードを変更する必要があります。
   b. フッターテキストに URL リンクが含まれている場合、フッターテキストがフッター画像に重なり合う可能性があります。プレビューし、必要に応じて修正します。

タイムライン

タイムライン構成では、必要に応じてタイムラインフィルターを作成および変更できます。レポートに含めるアクティビティタイプをフィルタリングし、子タスクをレポートに含めるかまたは除外するかを設定し、画像をレポートに含めるかまたは除外するかを設定できます。

タイムライン構成を使用し、タイムライン構成を入力する場合は、タグを *${timeline:timeline name}* として追加する必要があります。この設定では、フィッシングレポートテンプレートとデフォルトレポートテンプレートで使用される 2 つのサンプルタイムライン構成が例として提供されています。これらの構成を変更して再利用できます。

テンプレートスクリプト

関連リストのデータ、日付とタイムスタンプ、および直接ドット連結可能でないその他のデータを含めるときに、テンプレートスクリプトを使用します。次に例を示します。

レポートテンプレートに関連リストを表示するテンプレートスクリプトを作成します。

1. 関連リストのデータを準備するには、PostIncidentReportUtils.fetchRelatedListDataForReport メソッドを呼び出します。
2. ステップ 1 のデータをテーブル形式とスタイルで表すには、ReportTemplateUtil.constructTablefunction メソッドを呼び出します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

テンプレートスクリプトを使用して入力する場合は、タグテンプレートスクリプトのタグを `${template_script:script name}` として追加する必要があります。

以下は、インシデントの事後レポートの設定と変更のために提供されているサンプルのテンプレートスクリプトです。

スクリプト名	説明
formatted_current_date	現地の現在の日時を DDMMYYYY 00.00 AM または PM 形式で返します。例：21 Jan 2021 3:51 PM PST
si_affected_users	影響を受けるユーザーを関連リストから表形式で返します。
si_assessments	インシデント事後アセスメントの結果を表形式で返します。
si_associated_phish_emails	関連フィッシングメールを関連リストから表形式で返します。
si_associated_phish_headers	関連フィッシングヘッダーを関連リストから表形式で返します。
si_business_criticality	ビジネス上の重要度の値を色分けされた形で返します。
si_malicious_observables	悪意のある観測事象を関連リストから表形式で返します。
si_observables	観測事象を関連リストから表形式で返します。
si_priority	優先度の値を色分けされた形で返します。
si_response_tasks	応答タスクを関連リストから表形式で返します。
si_time_to_identify	ドラフトと分析のステータスで費やされた期間を返します。
si_time_to_resolve	インシデントの解決にかかる時間を返します。

レポートテンプレートスクリプトの重要なポイント：

1. 列数が 5 列を超える関連リストが追加された場合、PDF の生成中にテーブルデータが切り捨てられます。各列の最小幅は 124px に設定されています。
2. 技術的な問題が原因でテンプレートスクリプトがレポートテンプレートのコンテンツをロードできない場合、「テンプレートスクリプトの評価中にエラーが発生しました (Error while evaluating the template script)」というエラーメッセージがレポートに表示されます。セキュリティアドミニストレーターは、スクリプトの正確性を評価して問題を解決する必要があります。
3. si_assessments：デフォルトでは、すべてのアセスメントカテゴリがレポートに追加されます。セキュリティアドミニストレーターは、必要に応じてテンプレートスクリプトを変更してデータをフィルタリングできます。`categories: sys_id1,# sys_id2;` パラメーターを追加して、データをフィルタリングします。
4. 解決時間とスクリプトの識別にかかる時間：メトリクス関連リストの一部である定義レコードを使用します。セキュリティインシデントで定義レコードが利用できない場合は、それらの定義レコードを作成または追加して、2 つのフィールドの値を入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

デフォルトでは、セキュリティアドミニストレーターにはテーブルのバージョンレコードを表示するためのアクセス権がありません。バージョンレコードにアクセスして以前のバージョンに戻すには、admin ロールを追加する必要があります。

レポート構成

[レポート構成] セクションを使用して条件を設定し、レポートテンプレートをセキュリティインシデントに適用します。1 つのプライマリレポートと 1 つ以上の追加のレポートテンプレートを同じ条件に追加できます。

以下は、フィッシングレポートテンプレートをフィッシングカテゴリインシデントに適用するための条件の例と、デフォルトレポートテンプレートをすべてのセキュリティインシデントに適用するための条件の例です。条件が満たされない場合、デフォルトレポートテンプレートがセキュリティインシデントに適用されます。

新しい実装をオフにする手順

1. 次のビジネスルールを非アクティブ化します。
   a. PIR PDF の生成 (Generate PIR PDF)
   b. 新規クローズ時にナレッジを作成 (Create Knowledge On Closure New)
2. 次のビジネスルールをアクティブ化します。
   a. レビューおよびクローズ時に PIR を生成 (Generate PIR when in Review and Close)
   b. クローズ時にナレッジを作成 (Create Knowledge On Closure)
   c. [クローズ/キャンセル/削除時に PIR を再生成 (Regen PIR on closure/cancel/delete)]
3. UI ルール *`Hide PIR field when empty`* をアクティブ化します。
4. セキュリティインシデントフォームのフォームレイアウトに移動します。[インシデントの事後レビュー] セクションで、次の手順を実行します。
   a. [PIR] セクションから PIR レポートピッカーを削除します
   b. [インシデントの事後レポート] フィールドを [PIR] セクションに追加します

子セキュリティインシデントのインシデントの事後レビュー **(PIR)** レポートプロパティの設定

子セキュリティインシデントに対して、次の 2 つの PIR レポートプロパティを設定するオプションがあります。

- **sn_si.generate_pir_report_for_child_si**
- **sn_si.include_child_si_timeline_in_pir**

注:
システムアドミニストレーター [admin] ロールを持つユーザーは、プロパティを表示できます。セキュリティアドミニストレーター [sn_si.admin] ロールを持つユーザーは、それらを変更できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

子セキュリティインシデントの **PIR** レポートプロパティの設定

プロパティ	使用法
sn_si.generate_pir_report_for_child_si	子セキュリティインシデントのインシデントの事後レビュー (PIR) レポートの生成を有効にするオプション。 • タイプ：true | false • デフォルト値：false • 場所：[すべて] > [システムプロパティ] > [すべてのプロパティ] に移動します。
sn_si.include_child_si_timeline_in_pir	親セキュリティインシデントの PIR レポートに子セキュリティインシデントのタイムラインを含めるオプション。 • タイプ：true | false • デフォルト値：false • 場所：[すべて] > [システムプロパティ] > [すべてのプロパティ] に移動します。

インシデント事後レビュー管理レポート **(Manage Post Incident Review Report)**

インシデント事後レビュー管理レポート (Manage Post Incident Review Report) には、セキュリティアドミニストレーターによって構成および適用された情報が含まれています。セキュリティアナリストは、実行時にタイムラインフィルターを変更してダウンロードできます。

始める前に

必要なロール：sn.si_analyst

このタスクについて

セキュリティアナリストは、利用可能なプライマリレポートテンプレートまたは追加のレポートテンプレートのいずれかを選択し、タイムラインフィルターを構成し、レポートをプレビューしてダウンロードできます。セキュリティアナリストは、最後に適用されたタイムライン構成を含むレポートを直接ダウンロードすることもできます。

セキュリティアナリストは、[インシデントの事後レビュー] タブからレポートにアクセスできます。

手順

1. [レビュー] ステータスのセキュリティインシデントに移動します。
2. [インシデントの事後レビュー] タブをクリックします。
3. セキュリティインシデントが [レビュー] ステータスの場合は、次のようになります。
   レポートテンプレート：
   - デフォルトでは、設定ページで構成されたプライマリレポートテンプレートがセキュリティインシデントに適用され、ダウンロードできるようになります。
   - アナリストは、ドロップダウンリストから他のレポートを選択して、そのレポートを構成およびダウンロードできます。
4. 設定/プレビュー：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティアナリストは、レポートテンプレート構成をプレビューして変更できます。現在の構成では、セキュリティアナリストはタイムラインフィルターのみを変更できます。

セキュリティインシデントがクローズされる前にプライマリレポートの構成が変更された場合、セキュリティインシデントに添付されているインシデントの事後レビューレポートは、セキュリティアナリストが行った変更に基づいて更新されます。クローズ後には、アナリストは構成を変更して外出先でレポートをダウンロードできるようになります。ただし、添付されるレポートはクローズ前の最後の構成に従っています。

レポートを構成/プレビューするには、次の手順を実行します。

a. [インシデントの事後レビュー] タブの [レポートテンプレート] ドロップダウンリストから目的のレポートテンプレートを選択します。

b. [設定/プレビュー] タブをクリックします。

c. 必要に応じてタイムラインフィルターを更新または構成します。

d. [イメージを表示] チェックボックスを使用して、タイムラインに画像を含めるかまたは除外します。オフにすると、画像の名前のみがタイムラインセクションに表示されます。

e. [子タスクを表示] チェックボックスを使用して、セキュリティインシデントに関連付けられているすべての子タスクを一覧表示します。

5. 構成を保存 し、[プレビュー]タブをクリックしてレポートをプレビューおよびダウンロードします。

6. [ダウンロード] をクリックして、レポートを直接ダウンロードします。

アセスメントのトリガー条件の設定

ルール条件を定義し、特定のセキュリティインシデントに対して必須およびオプションのアセスメントを生成します。

始める前に

必要なロール：sn_si.admin

注:
インシデントの事後レビューアセスメントのトリガー条件機能を使用するには、セキュリティインシデントレスポンス 11.0 にアップグレードする必要があります。アップグレードする前に、インシデントの事後レビューメトリクスタイプおよびトリガー条件に対して行われたカスタマイズを元に戻す必要があります。さらに、インシデントの事後レビューに固有のビジネスルールに対して行われたカスタマイズを元に戻すことが必要になる場合もあります。

- アセスメントを完了する必要があります。
- アサイニーを保存してください。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > アドミニストレーション > インシデントの事後レビュー：アセスメントセットアップ.

2. [アセスメントのトリガー条件の構成 **(Assessment Trigger Conditions Configure)]** セクションで、[構成] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[アセスメント構成] フォームの [アセスメント構成] セクション内では、[アセスメントを生成] チェックボックスがデフォルトでオンになっています。

- チェックボックスをオンにすると、すべてのセキュリティインシデントに対してオプションのアセスメントが作成されます。
- チェックボックスをオフにすると、アセスメントは生成されません。アセスメントルールは表示されず、セキュリティインシデントの条件を構成することはできません。

3. [アセスメント構成] フォームの [条件] セクションで、必要な情報を指定します。

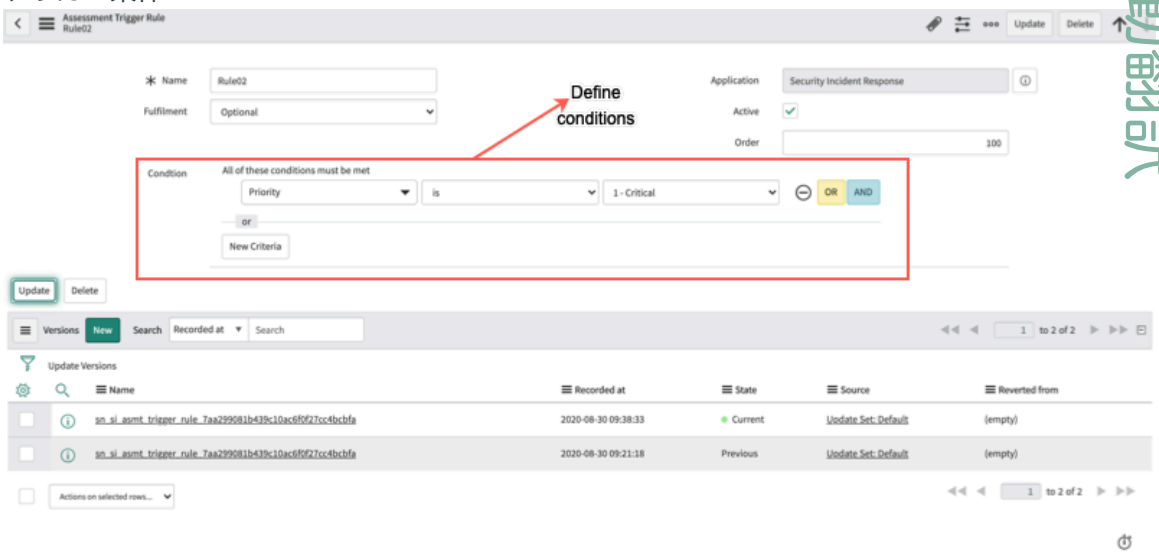
   a. [名前] フィールドで、ルール名を指定します。

   b. [履行 **(Fulfilment)**] フィールドで、履行タイプを指定します。

   c. 条件を設定するには、ルールレコードをクリックし、[条件] フィールドで条件を定義します。

   注:
   - [条件] フィールドで条件を定義せずにルールを作成すると、条件は true と評価され、そのルールはすべてのセキュリティインシデントに適用されます。
   - アセスメントを必須またはオプションにする特定のルールを定義できます。これにより、アセスメントは、定義されたルールに一致しない残りのセキュリティインシデントに対して生成されません。

   トリガー条件



アセスメントのトリガー条件の例

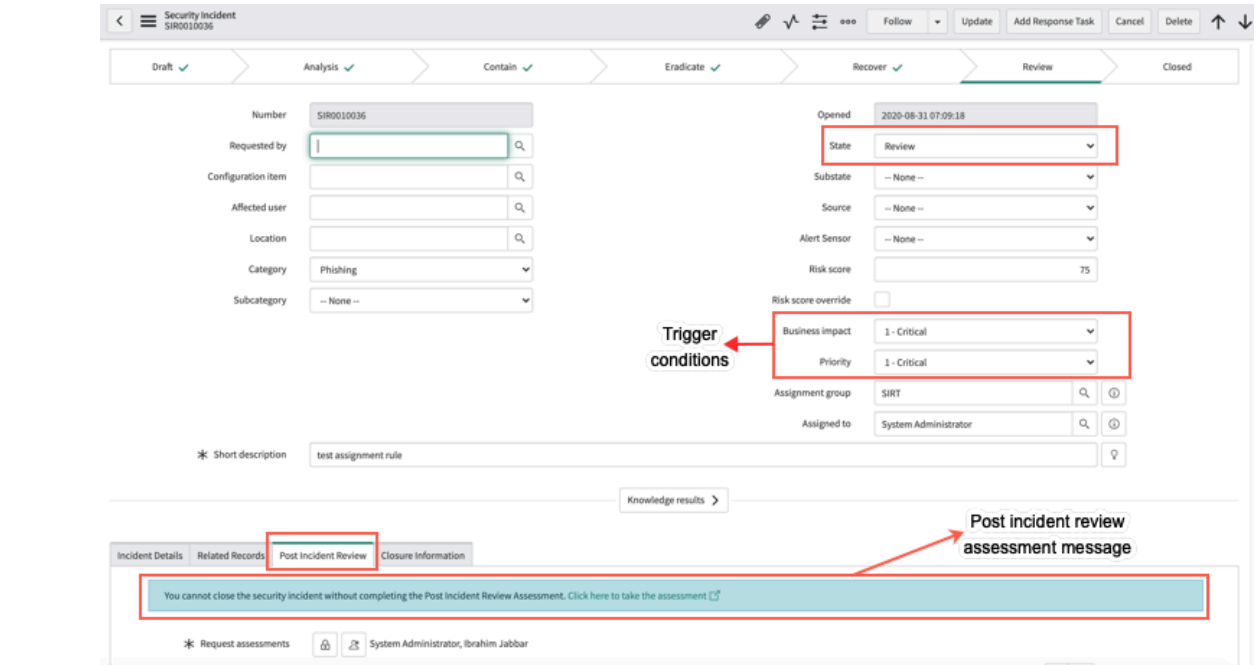
次の例は、必須およびオプションのアセスメントトリガー条件を生成する方法に関するさまざまなシナリオを示しています。

- [アセスメントトリガールール **(Assessment Trigger Rule)**] ページでセキュリティインシデントの [優先度] と [ビジネスインパクト] が [重大] に設定されている場合、[アセスメントトリガー条件] フォームで必須のアセスメントを生成します。このようなシナリオでは、セキュリティアナリストは必須のアセスメントが完了するまでインシデントをクローズできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

必須のアセスメントの例



- この例では、セキュリティインシデントが [レビュー] ステータスの場合、セキュリティアナリストは [インシデントの事後レビューアセスメント **(Post Incident Review Assessment)]** を完了せずにセキュリティインシデントをクローズすることはできません。インシデントにアサインされた (またはアセスメントを要求した) セキュリティアナリストは、アセスメントを行うためのアセスメントリンクを使用できます。
- セキュリティインシデントの [優先度] と [ビジネスインパクト] が [高] に設定されている場合、[アセスメントのトリガー条件] ページでオプションのアセスメントを生成します。この例では、セキュリティアナリストがアセスメントを完了せずにセキュリティインシデントをクローズすると、アセスメントは自動的にキャンセルされます。
- 必須またはオプションのアセスメントがセキュリティインシデントと一致しない場合、そのようなセキュリティインシデントに対してアセスメントは生成されません。セキュリティアナリストはインシデントの事後レビューアセスメントを完了せずにセキュリティインシデントをクローズできます。

アンケートベースのインシデントの事後レビューの実施

セキュリティインシデントの事後レビューが必要であると判断することがあります。インシデントの事後レビューでは、何が起こったかを記述し、なぜインシデントが発生したのかを判断し、どうすれば今後インシデントを回避または処理できるのかを特定します。

始める前に

必要なロール：sn_si.admin、sn_si.manager、sn_si.analyst

> **注:**
> インシデントの事後レビューのアンケートには、ロールに関係なくあらゆるユーザーが参加できます。レビューにはロールを割り当てることができます。

このタスクについて

ServiceNow セキュリティインシデントレスポンス アプリケーションでは、アンケートを使用して、セキュリティインシデントに関係するユーザー全員からインシデントの事後レビュー情報を自動収集できます。インシデントの事後レビューの一部としてアンケートを使用することにした場合、セキュリティインシデントに関連する質問のリストがユーザー定義の参加者リストに送信されます。各ユーザーがアンケートを完了すると、インシデントの事後レポートが自動的に生成されます。このレ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ポートでは、セキュリティインシデントに関連するすべての情報とインシデントの事後レビューに対するすべての回答がまとめられます。

最初の質問リストはベースシステムで提供されますが、カスタマイズ可能です。カテゴリを作成して新しい質問を追加したり、既存のカテゴリ内の個々の質問を改変したりすることができます。ロールに基づいて質問することができます。特定の質問をするタイミングを定義できます。たとえば、UNIX サーバーに関してのみ尋ねる質問や、犯罪行為がある場合のみ尋ねる質問があります。別の質問に対する回答、またはフォーム上のフィールドの値に応じて尋ねられる質問を定義できます。データベースに照会するだけで埋められる質問もあります。

セキュリティインシデントが解決され、[レビュー] ステータスに移行すると、アサインされたすべてのユーザーと [アセスメントを要求] リストから直接追加されたユーザーのアセスメントが生成されます。

アンケートは、さまざまなソースからセキュリティインシデントの処理に関する情報を収集するのに便利なツールです。

レビュー中は、ユーザーがまだアンケートの入力を開始していない限り、リストにさらにユーザーを追加したり、既存のユーザーをリストから削除したりすることができます。新しいユーザーをリストに追加すると、レコードが保存されたときにそのユーザーは質問を受け取ります。セキュリティインシデントは、すべてのアンケートが完了するまでクローズできません。各ユーザーがアンケートを完了すると、インシデントの事後レポートが自動的に生成 (および再生成) され、[インシデントの事後レビュー] タブに表示されます。

インシデントの事後レビューを開始するには：

手順

1. セキュリティインシデントを作成するか、次の場所に移動して既存のセキュリティインシデントを開きます セキュリティインシデント > インシデント > 自分にアサイン済み (またはチームにアサイン済みまたは未アサインのインシデント).
2. [インシデントの事後レビュー] タブをクリックします。
3. [アセスメントを要求] フィールドのデフォルト値は、[アサイン先] フィールドの個人です。
   他のユーザーをレビューリストに追加するには、ロックアイコンをクリックします。フィールドのロックを解除すると、複数のユーザーやロールを追加または削除するオプションや、ユーザーのメールアドレスを入力するオプションが利用可能になります。
4. 入力が完了したら、ロックアイコンをクリックしてフィールドをロックします。

   注:
   条件を定義して、セキュリティインシデントで条件が満たされたときに、そのセキュリティインシデントの [アセスメントを要求] フィールドに特定のユーザーが自動的に追加されるようにすることもできます。たとえば、セキュリティインシデントの [カテゴリ] が [フィッシング] に変更されたときに、フィッシングの脅威の専門知識を有する特定の個人をインシデントの事後レビューリストに追加することができます。詳細については、「PIR アサインルールの作成」を参照してください。

5. [更新] をクリックします。
   インシデントが [レビュー] ステータスになると (すでに [レビュー] ステータスの場合はただちに)、レビューリストの各ユーザーは最初のメール通知 を受け取ります。期日が近づくとリマインダーが送信されます。各ユーザーがメールリンクからアンケートにアクセスするか、 インシデントの事後レビュー > 自分のレビュー待ちの場合、表示される質問は、このセキュリティインシデントに適合するすべてのカテゴリから抽出されます。期日になる前に新しいユーザーがレビューリス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

トに追加された場合、セキュリティインシデントが保存されたときに新しいユーザーに通知が送信されます。

ユーザーがアンケートを完了すると、インシデントの事後レポートにデータがまとめられ、[インシデントの事後レビュー] タブにレポートが表示されます。アンケートデータは [結果] タブに表示されます。

インシデントの事後レビューのアンケートカテゴリを作成する

ベースシステムに含まれているアンケートカテゴリを使用することも、独自のカテゴリを作成することもできます。

始める前に
必要なロール：sn.si_admin

このタスクについて
質問の新しいカテゴリを作成するには：

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデントの事後レビュー.
2. [レビューの質問 **(Review Questions)]** をクリックします。
   カテゴリのリスト、その順序、質問がどのような条件の下で尋ねられるか (セキュリティインシデント カテゴリが [犯罪行為] の場合のみなど) を定義するフィルターが表示されます。各カテゴリはインシデントの事後レビューアンケートのセクションになります。各カテゴリの質問はセキュリティインシデントが [条件] フィルターに一致した場合のみ含まれます。たとえば、Linux サーバーにのみ適用される質問のカテゴリの場合、影響を受けるリソースタイプが Linux サーバーであるセキュリティインシデントを選択するフィルターを設定します。そのカテゴリで、セキュリティインシデントが Linux サーバーで発生した場合に必要なすべての質問を作成します。ベースシステムで提供されているカテゴリの 1 つを使用するか、新しいカテゴリを作成します。この手順では、質問を定義する前に新しいカテゴリを作成することを前提にしています。
3. カテゴリのリストで [新規] をクリックします。
4. 必要に応じて、フォームのフィールドに入力します。

セキュリティインシデント

フィールド	説明
名前	セキュリティインシデントアンケートに表示されるカテゴリの名前
タイプ	デフォルトは [インシデントの事後レビュー] です。
ステークホルダーの作成	セキュリティインシデントレスポンス では使用されていません。
テーブル	このフィールドは、フォームが送信されると自動的に割り当てられます。
フィルター	このカテゴリの質問をいつ使用するかを決定する条件を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	セキュリティインシデントレコードがこのフィルターに一致した場合、質問はそのセキュリティインシデントのインシデントの事後レビューに含まれます。フィルターには、このレコード、またはこのレコードにリンクされている他のレコードの任意のデータを使用できます。たとえば、要求ユーザーのマネージャーの部門などです。
アプリケーション	インシデントのスコープアプリケーション
重み付け	同じカテゴリの他のメトリクスと相対的にこのメトリクスの重要度を表す数値。デフォルトでは、重み付けは 10 です。
合計メトリクス	カテゴリで使用されるメトリクスの数
説明	アンケートの説明

5. [送信] をクリックしてカテゴリを保存します。

インシデントの事後レビューの質問の作成

ベースシステムに含まれている質問を使用することも、独自の質問を作成することもできます。

始める前に
必要なロール：sn_si.admin

このタスクについて
インシデントの事後レビュー情報は、質問の形式で収集することも、スクリプトを使用して自動的に収集することもできます。

質問は、他の質問に対する回答によって変えることもできます。たとえば、必要なすべてのログが利用可能かどうかを尋ねるとします。回答が「いいえ」の場合は、必要なログのどれが有効になっていないのかを確認するためにフォローアップの質問をします。

スクリプト化されたデータ収集はスクリプトメトリクスとも呼ばれ、自作のスクリプトを使用してセキュリティインシデントに関連するデータを収集します。このアクションは、セキュリティインシデントレコード自体のデータを大幅に超えて収集する可能性があります。たとえば、スクリプトメトリクスが、このセキュリティインシデントの影響を受けるサーバーの最近の機能停止時間を収集してしまう可能性があります。

最後に、この 2 つのタイプを混在させることができます。質問には、スクリプトから取得した、または単純にセキュリティインシデントレコードのフィールドから取得したデフォルト値を設定できます。[デフォルトの回答元…] タイプの質問を使用するときは、(デフォルト値を初期値として提供し) ユーザーが常に質問に回答するようにするか、スクリプトまたはフィールドが空だった場合のみユーザーに質問が尋ねられるようにするかを選択できます。

新しい質問を作成するには：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデントの事後レビュー.
2. 新しい質問を作成するカテゴリをクリックします。
3. [アセスメント評価指標] タブをクリックします。
4. [新規] をクリックします。
   既存の質問をクリックして変更することもできます。
5. 必要に応じて、フォームのフィールドに入力します。

メトリクスフォーム

フィールド	説明
名前	メトリクス (質問またはスクリプト) の名前。メトリクスがスクリプト化されたデータコレクションの場合、この名前がインシデントの事後レポートに表示されます。
カテゴリ	メトリクスが属するカテゴリ。[メトリクスカテゴリ] フォームから新しいメトリクスを作成すると、このカテゴリに値が自動的に入力されます。 **注:** [依存] フィールドが設定されている場合や、別のメトリクスがこのメトリクスに依存する場合、カテゴリを変更することはできません。
メソッド	メトリクスのタイプを次のように示します。 ○ *Assessment*：デフォルト値のない質問。[フィールドタイプ] タブの [データタイプ] フィールドでは、チェックボックス、選択リスト、テキスト入力など、いくつかのデータタイプを定義できます。 ○ *Script*：スクリプト化メトリクス。カスタム スクリプトを記述して値を取得します。*Script*手法は、[期間]、[番号]、および [パーセンテージ] データタイプと互換性があります。 ○ *Default answer from field*：デフォルトの回答が、選択したセキュリティインシデントのフィールドに由来する質問。このオプションを選択すると、[全般] タブに 2 つのフィールドが追加されます。 ▪ *Default answer*：セキュリティインシデントのフィールドから、質問に対するデフォルトの回答を含むものを選択します。たとえば、「このインシデントを最初に報告したのは誰ですか？」という質問の場合、[要求者] フィールドが候補になります。 ▪ *Ask question*：質問するタイミングを指定します。常時か、[デフォルトの回答] フィールドが空であった場合のみのいずれかです。上記の例であれば、質問は、[要求者] フィールドが空だった場合に尋ねられます。 ○ *Default answer from script*：デフォルトの回答がスクリプトに由来する質問。回答は、番号、文字列、またはパーセンテージです。[全般] タブにフィールドが 1 つ追加されます。 *Ask question*：質問するタイミングを指定します。常時か、スクリプトによってデフォルトの回答が提供されない場合のみのいずれかです。スクリプトは [フィールド タイプ] タブで定義されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: 選択した [手法] と互換性がない [データタイプ] を選択すると、[手法] がシステムによって自動的に互換性のある値に変更されます。
重み付け	[必須] 同じカテゴリの他のメトリクスと相対的にこのメトリクスの重要度を表す数値。デフォルトでは、重み付けは 10 です。 [データタイプ] が [日付]、[日付/時刻]、または [文字列] でなければ、このフィールドは表示され、必須です。これらのデータタイプは結果の計算に含まれません。
順序	[必須] アセスメントアンケートでのメトリクスの質問の順序を同じカテゴリの他のメトリクスの質問に相対的に決定する数値。順序値が最小のメトリクスは、カテゴリセクションの最初の質問として表示されます。デフォルトでは、順番は 100 です。 注: スクリプト手法を用いるメトリクスはアンケートに表示されないので、どの順序値を使用しても関係ありません。
有効	このメトリクスを使用するかどうかを決定するチェックボックス。チェックボックスがオフの場合、メトリクスレコードは存在しないものと見なされます。
必須	アセスメントアンケートでメトリクスの質問を必須 (選択) またはオプション (選択解除) にするチェックボックス。ユーザーは、赤色のフィールドステータスインジケーターで示される、必須のすべての質問に有効な回答を入力するまで、アンケートを送信することはできません。 このフィールドは、[依存] フィールドが空で、かつデータタイプが [チェックボックス] でない場合のみ表示されます。

6. [全般] タブをクリックし、必要に応じてフィールドに入力します。

[全般] タブ

フィールド	説明
質問	セキュリティインシデントレビューアンケートの質問として使用するテキスト。回答しやすい明確かつ直接的な質問を入力します (「インシデントをどのように阻止しましたか？」など)
説明	メトリクスとその評価対象についての情報。[*Method*] が [アセスメント] の場合、ユーザーが質問の回答方法を理解するのに役立つ詳細を含めます。ユーザーがアンケート上で質問テキストを指すと、このテキストがヒントとして表示されます。
[依存先] および [表示するタイミング]	[依存先] フィールドで、現在の質問が依存する質問を選択します。たとえば、「他にどのようなログが必要でしたか？」という質問は、「必要なログはすべてありましたか？」という質問に依存しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	次に、[表示するタイミング] フィールドを使用して、依存する質問をアンケートに表示するタイミングを指定します。たとえば、「必要なログはすべてありましたか？」に対してユーザーが「いいえ」と回答した場合のみ、依存する質問が尋ねられるようにしたい場合は、[表示するタイミング] フィールドで [いいえ] を選択します。 **注:** メトリクス間に再帰的な依存関係が作成されるのが防止されます。たとえば、メトリクス A がメトリクス B に依存する場合、メトリクス B はメトリクス A に依存できません。

7. [フィールドタイプ] タブをクリックし、必要に応じてフィールドに入力します。

[フィールドタイプ] タブ

フィールド	説明
データタイプ	選択した手法に利用可能なタイプのリストが依存する、予想される回答のデータタイプ。手法がアセスメントの場合、データタイプによって、ユーザーがアンケートで対応する質問にどのように回答するかが決まります。手法がスクリプトの場合、データタイプによって、アセスメント結果がどのように計算されるかが決まります。 **注:** 別のメトリクスがこのメトリクスに依存する場合、データタイプを変更することはできません。
選択肢のランダム表示	ユーザーがこの質問を含むアセスメントアンケートを開くたびに、このメトリクスの質問の回答オプションをランダムな順番で提示するかどうかを決定するチェックボックス。回答オプションが表示される順番によって、回答の優先傾向が影響を受けることがあります。このため、結果にバイアスがかかる可能性があります。回答の選択肢をランダムに表示すると、このバイアスがかかるのを防ぐのに役立ちます。 このフィールドは、[データタイプ] フィールドで、[リッカート尺度] または [選択肢] を選択した場合のみ表示されます。
依存プラグイン	[[*Method*] が [スクリプト] の場合は必須] スクリプトでクエリされるテーブルを含むプラグイン。プラグインが有効な場合のみ、メトリクススクリプトが実行されます。デフォルトで利用可能な値は、[資産管理]、**[CMDB]**、**[Core]**、[コスト管理]、[調達]、および [ソフトウェア資産管理] です。 このフィールドが表示されるのは、[*Method*] が [スクリプト] の場合のみです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: ○ Core のデフォルト値を使用している場合、スクリプトは常に実行されます。 ○ アドミンであれば、このフィールドにさらにプラグインの選択肢を追加できます。
スケール定義	アセスメント結果の計算で大きい数値と小さい数値のどちらのほうが良いスコアに等しいかを決定する設定。ベンダーの欠陥数を測定するメトリクスなど、数値が小さいほうがよい場合は、[低] を選択します。ユーザーの満足度を 1 から 5 の尺度で測定するメトリクスなど、数値が大きいほうがよい場合は、[高] を選択します。デフォルト値は [高] です。 [*Data type*] が [日付]、[日付/時刻]、または [文字列] でなければ、このフィールドは表示され、必須です。これらのデータタイプの結果は、結果の計算に含まれません。
最小	アセスメントの回答オプションとして、またはスクリプト化済みメトリクスのスケール値として使用される最小の数値。 このフィールドが表示されて必須なのは、特定のデータタイプが選択されている場合のみです。データタイプが [選択肢] または [リッカート尺度] の場合、このフィールドは読み込み専用であり、最小のメトリクスの定義 [*Value*] に基づいて自動的に設定されます。
最大	回答オプションまたはスケール値として使用する最も高い数値。 このフィールドが表示されて必須なのは、特定のデータタイプが選択されている場合のみです。データタイプが [選択肢] または [リッカート尺度] の場合、このフィールドは読み込み専用であり、最大のメトリクスの定義 [*Value*] に基づいて自動的に設定されます。
スクリプト	必要なシステム情報を取得するスクリプト。スクリプトには、セキュリティインシデント (プライマリ) の ID が設定される入力変数 1 つと、スクリプトによって設定される出力の可能性がある変数 3 つ (string_result、scaled_result、actual_result) があります。データタイプが [文字列] の場合は、string_result のみが必須です。 このフィールドは、[*Method*] が [スクリプト] の場合、またはデフォルト値がスクリプトから取得された場合に表示され、必須です。
テンプレート	質問に対して使用する、事前定義された一般的な回答のセット。たとえば、頻度テンプレートは通常、最初の値が「一度もない」で、最高値は「常時」になります。 このフィールドが表示されて必須になるのは、[*Data type*] が [テンプレート] の場合のみです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: 別のメトリクスがこのメトリクスに依存する場合は、テンプレートを変更できません。

8. オプション: 入力が完了したら、[更新] をクリックします。

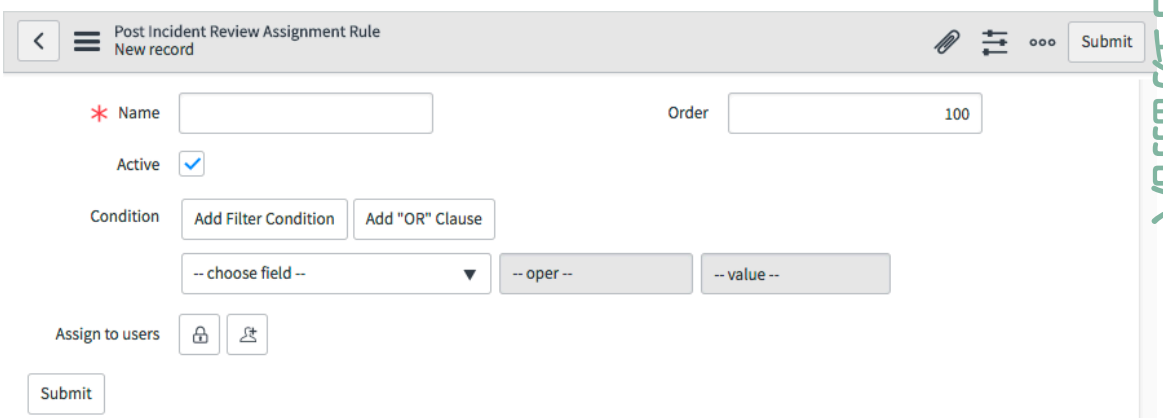
PIR アサインルールの作成

セキュリティインシデントのインシデントの事後レビューアセスメントリストにユーザーを手動で追加するだけでなく、ユーザーをリストに自動的に追加するためのアサインルールを定義することもできます。

始める前に
必要なロール：sn_si.admin、sn_si.manager、sn_si.analyst

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > アドミニストレーション > インシデントの事後レビュー：アセスメントセットアップ.
2. [ユーザーアサインルール] セクションにドリルダウンします。
3. [構成] をクリックします。
4. [新規] をクリックします。



5. 必要に応じて、フィールドに入力します。

フィールド	説明
名前	このアサインルールの名前。
有効	このルールをアクティブにするには、このチェックボックスをオンにします。
順序	数値を入力して、このルールをアサインルールのリスト内のどこに表示するかを指定します。番号が小さいほど、リストの上部に表示されます。 注: 最初に一致したアサインルールのみが実行され、そのルールで定義されたユーザーのみがアセスメントリストに追加されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

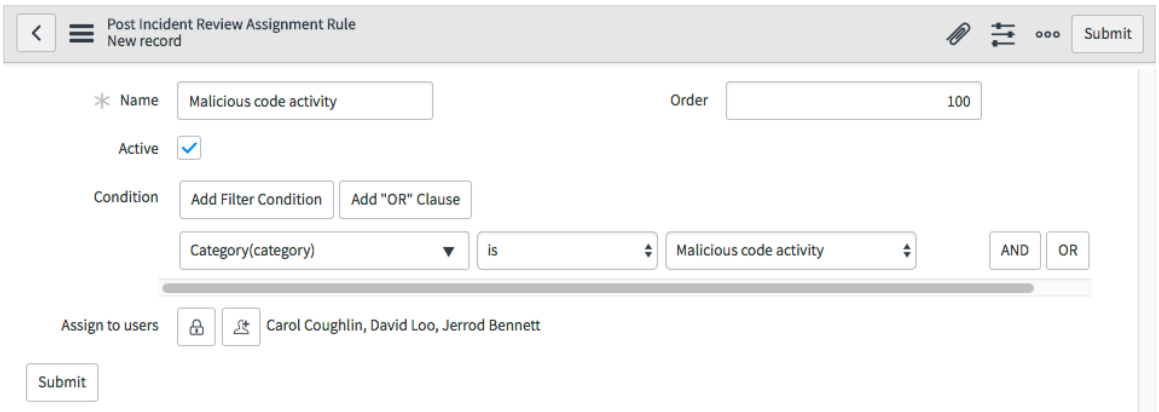
フィールド	説明
条件	次を使用： 条件ビルダー を使用して、このルールを実行するためにセキュリティインシデントで満たす必要がある条件を定義します。詳細については、以下の例を参照してください。
アサインするユーザー	ユーザーをレビューリストに追加するには、ロックアイコンをクリックします。フィールドのロックを解除すると、複数のユーザーやロールを追加または削除するオプションや、ユーザーのメールアドレスを入力するオプションが利用可能になります。

6. **[Submit]** をクリックします。

Example: 悪意のあるコードアクティビティ

ここに示したインシデントの事後レビューのアサインルールでは、[カテゴリ] フィールドが [悪意のあるコードアクティビティ] に設定されたセキュリティインシデントが [レビュー] ステータスに移行すると、識別された 3 人のユーザー (ここでは、悪意のあるコードアクティビティを処理するエキスパート) が、このセキュリティインシデントのインシデントの事後レビューアンケートを受け取るユーザーのリストに追加されます。

悪意のあるコードアクティビティ



セキュリティインシデントのクローズ

セキュリティインシデントが [レビュー] ステータスに移行したら、クローズして適切なクローズコードを入力することができます。クローズコードは後で検索して簡単に見つけることができます。

始める前に

必要なロール：sn_si.write

このタスクについて

注:
以前のバージョンの セキュリティインシデントレスポンス では、ユーザーがセキュリティインシデントまたは要求をスパムとしてクローズすることができました。Istanbul リリースでは、スパムオプションは使用できなくなりました。スパムセキュリティインシデントまたは要求は、必要に応じてキャンセルまたは削除できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. クローズするセキュリティインシデントがまだ開いていない場合は、次に移動します: セキュリティインシデント > インシデント > すべてのインシデントを表示をクリックし、クローズするセキュリティインシデントを見つけます。

   注:
   このセキュリティインシデントに対して完了していないインシデントの事後レビューアセスメントがある場合、このセキュリティインシデントをクローズすることはできません。戻るセキュリティインシデント > インシデントの事後レビュー > すべての未完了レビューで、不完全なレビューを見つけて、レビュー担当者にレビューを完了するように依頼するか、残りのアセスメントをキャンセルします。

2. [クローズ情報] タブをクリックし、必要に応じてフィールドに入力します。

   セキュリティインシデント

フィールド	説明
ナレッジ記事の作成	このフィールドを選択すると、インシデントの事後レビューの内容を含むナレッジベース記事のドラフトが自動的に作成されます。
終了コード	このセキュリティインシデントをクローズする理由を最も的確に表すクローズコードを選択します。 ○ 調査完了 ○ 脅威緩和 ○ 修正済みの脆弱性 ○ 無効な脆弱性 ○ 未解決 ○ 誤検出
クローズ担当者	レコードの更新後に、セキュリティインシデントをクローズしたユーザーを表示します。
クローズ済み	レコードの更新後に、クローズされた日付と時刻が表示されます。
クローズメモ	このセキュリティインシデントをクローズした結果を説明する追加のメモを入力します。

3. [更新] をクリックします。
4. アサインされたユーザーは、[ステータス **(State)]** を手動で [クローズ済み **(Closed)]** に変更できます。
   親インシデントがクローズされると、子インシデントに属するすべての応答タスクがキャンセルされます。他のタイプのタスクがない場合、子インシデントもクローズされます。

セキュリティインシデントへのクローズ情報の追加

セキュリティインシデントが [レビュー] または [クローズ済み] ステータスの場合は、クローズ情報を入力できます。

始める前に
必要なロール：sn_si.basic

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 更新するセキュリティインシデントがまだ開いていない場合は、これを開きます。
2. [関連レコード] タブをクリックします。
3. 必要に応じて、フィールドに入力します。

フィールド	説明
ナレッジ記事の作成	インシデントの事後レポートの内容を使用してナレッジ記事を生成するには、このチェックボックスをオンにします。
終了コード	セキュリティインシデントをクローズする理由を最も的確に表すクローズコードを選択します。
クローズ担当者	[読み取り専用] セキュリティインシデントをクローズしたユーザーを表示します。
クローズ済み	[読み取り専用] セキュリティインシデントがクローズされた日時を表示します。
クローズメモ	セキュリティインシデントがどのようにクローズされたか (得られた教訓、解決策など)。

4. セキュリティインシデントをさらに更新するには、次のいずれかのタブをクリックします。
   - インシデントの詳細
   - インシデントの事後レビュー
5. 入力が完了したら、[送信] をクリックします。

セキュリティインシデントへのアクセスの制限

機密情報を含むセキュリティインシデントへのアクセスを管理します。セキュリティインシデントの制限を適用して、特定のインシデントにアクセスできるユーザーを決定し、特定のユーザーまたはグループのみにアクセスを制限することができます。

始める前に

必要なロール：sn_si.admin

このタスクについて

セキュリティインシデント制限を使用すると、重大なセキュリティインシデントを非表示にして、特定の組織内の他のユーザーがこのようなインシデントにアクセスできないようにすることができます。この制限により、ユーザーがアクセスできるセキュリティインシデントをより詳細に制御できます。セキュリティインシデントの制限を適用するには、[制限の適用] チェックボックスをオンにし、特定のセキュリティインシデントへのアクセスを許可するユーザーまたはグループを選択します。

特定のセキュリティインシデントに対して制限を適用し、アクセスを特定のユーザーまたはグループに制限すると、組織内の他のすべてのユーザーは、制限が適用された特定のセキュリティインシデントを検索しても、これらのセキュリティインシデントにアクセスできません。

手順

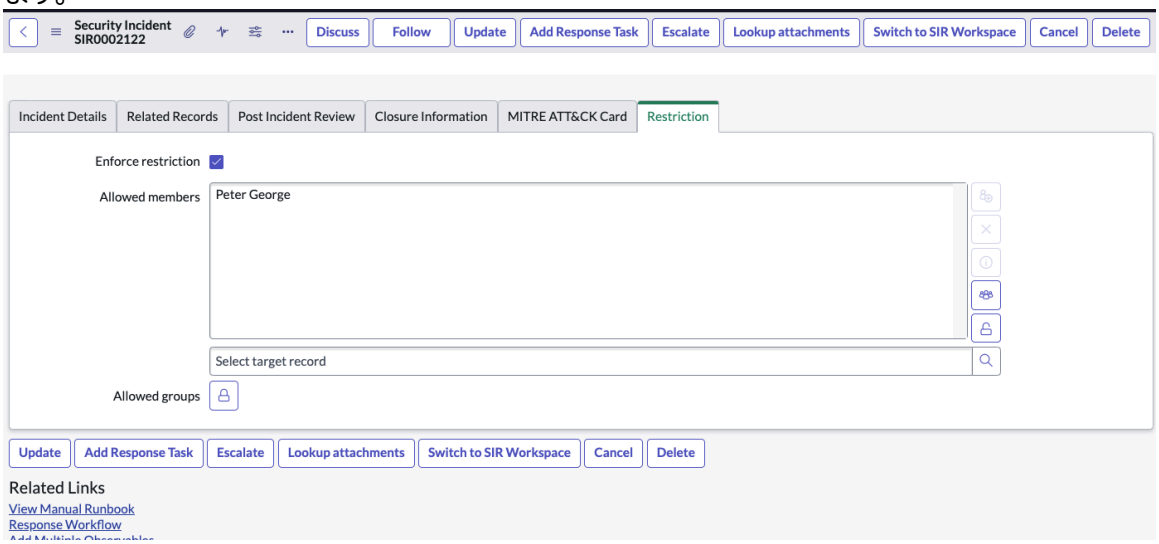
1. 制限するセキュリティインシデントを開きます。
2. クラシック UI を使用している場合は、次の手順を実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. [制限] タブをクリックします。

b. セキュリティインシデントの制限を有効にするには、[制限の適用] チェックボックスをオンにします。



c. [許可されたメンバー (Allowed members)] フィールドで アイコンをクリックして、セキュリティインシデントにアクセスできるユーザーを選択します。

d. アイコンを選択して、自分自身を許可されたユーザーとして追加します。

e. アイコンを選択して、ユーザーを追加または削除します。

f. [許可されたグループ (Allowed groups)] フィールドで アイコンをクリックして、セキュリティインシデントにアクセスできるグループを選択します。

g. アイコンを選択して、グループを追加または削除します。

> **注:**
> セキュリティインシデントの [制限を適用] チェックボックスをオンにすると、sn_si.admin および許可されたメンバーまたはグループのみがセキュリティインシデントにアクセスできるようになります。

h. [更新] をクリックします。

3. SIR ワークスペースを使用している場合は、次の手順を実行します。

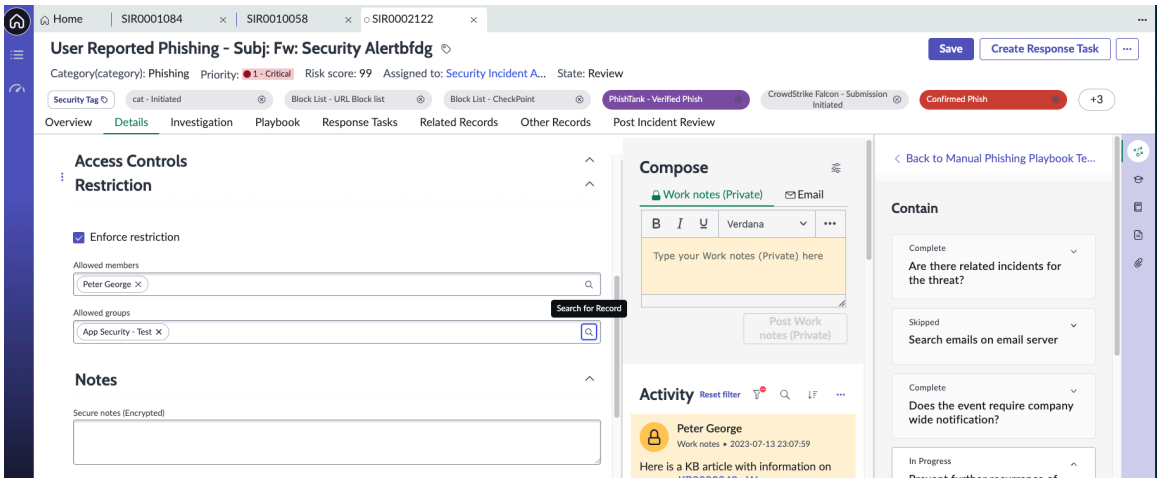
a. セキュリティインシデントで [詳細] タブをクリックします。

b. 下にスクロールして [制限] セクションをクリックします。

c. セキュリティインシデントの制限を有効にするには、[制限の適用] チェックボックスをオンにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



d. [許可されたメンバー (Allowed members)] フィールドで [検索] オプションを使用して、セキュリティインシデントにアクセスできるユーザーを選択します。

e. [許可されたグループ (Allowed groups)] フィールドで [検索] オプションを使用して、セキュリティインシデントにアクセスできるグループを選択します。

> **注:**
> セキュリティインシデントの [制限を適用] チェックボックスをオンにすると、sn_si.admin および許可されたメンバーまたはグループのみがセキュリティインシデントにアクセスできるようになります。

f. [保存] をクリックします。

セキュリティアナリストワークスペース を使用したセキュリティ上の脅威の管理

セキュリティインシデントレスポンス には、セキュリティアナリストワークスペース と呼ばれる新しいユーザーインターフェイスが含まれています。これには、プレイブック、ピークビュー、複数のセキュリティインシデントを処理するためのタブなど、分析を支援する強力なツールが含まれています。

セキュリティアナリスト向けにビルドされた セキュリティアナリストワークスペース の強力なツールを使用して、セキュリティインシデントに関連付けられた、増え続けるデータを分析できます。また、自動化されたアクションにより、攻撃を阻止できるか侵害を受けるかの分かれ道となるセキュリティインシデントの調査時間が大幅に短縮されます。

セキュリティアナリストワークスペース を使用する前に

セキュリティアナリストワークスペースの使用を開始する前に、インスタンスに少なくとも London パッチ 3 がインストールされていること、正しいロールが定義されていることを確認する必要があります。 からセキュリティインシデントレスポンス UI アプリケーションをダウンロードした ServiceNow Store.

> **注:**
> お使いのインスタンスで London パッチ 3 より前のバージョンを実行している場合は、HI Customer Service システムを介してセキュリティインシデントレスポンス UI プラグインを要求する必要があります。

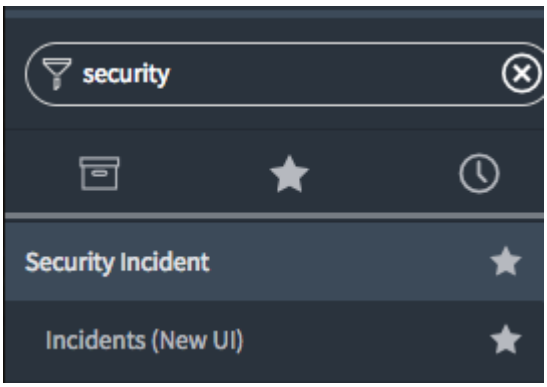
セキュリティアナリストワークスペース へのアクセス

この新しいワークスペースにアクセスするには、次に移動します: セキュリティインシデント > インシデント (新規 **UI**).

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

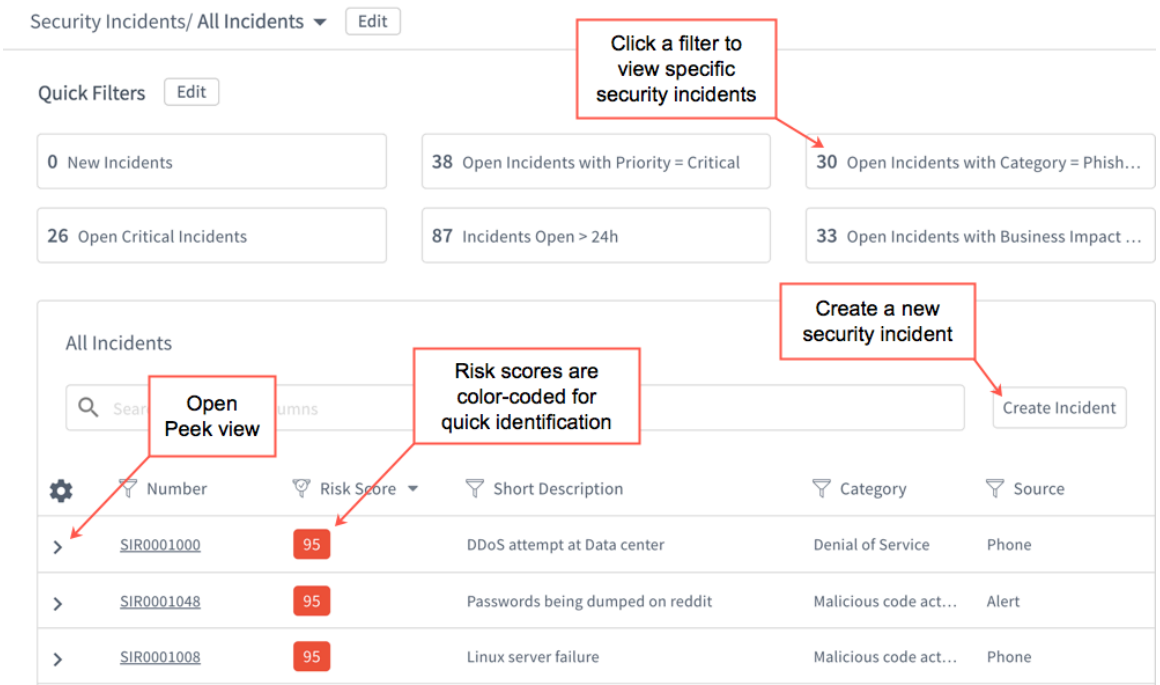
自動翻訳

セキュリティインシデント



ワークスペースが別のブラウザータブで開きます。

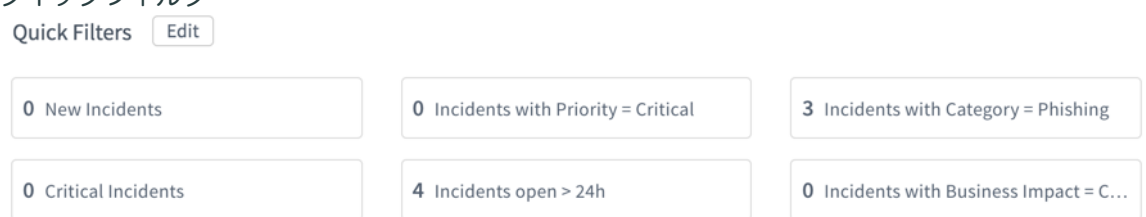
セキュリティインシデント



クイックフィルターを使用した分析対象セキュリティインシデントの検索

セキュリティアナリストワークスペース にはセキュリティインシデントのリストをフィルタリングするためのツールがいくつか用意されているため、分析するセキュリティインシデントをすばやく見つけることができます。クイックフィルターを使用すると、フィルターの基準に基づいてセキュリティインシデントのサブセットを選択できます。

クイックフィルター



使用するクイックフィルターをクリックするだけです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

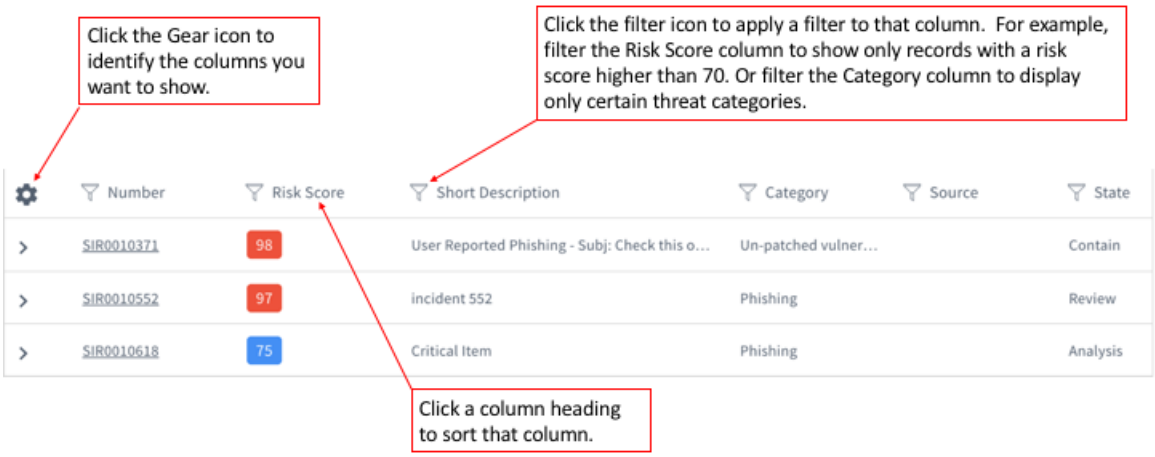
注:
[編集] ボタンをクリックすると、リスト画面に表示するクイックフィルターを指定できます。フィルターは、少なくとも 1 つ選択する必要があり、最大で 6 つ選択できます。

クラシック環境を使用すると、セキュリティアナリストワークスペース のプライマリフィルターに加えて、追加のクイックフィルターを定義できます。詳細については、「セキュリティアナリストワークスペースのプライマリフィルターとセカンダリフィルターの設定」を参照してください。

セキュリティインシデントリストのカスタマイズ

インスタンス内のすべてのリストと同様に、セキュリティアナリストワークスペース には、リストをカスタマイズし、表示される情報を分析のニーズに合わせてソートするためのツールが用意されています。

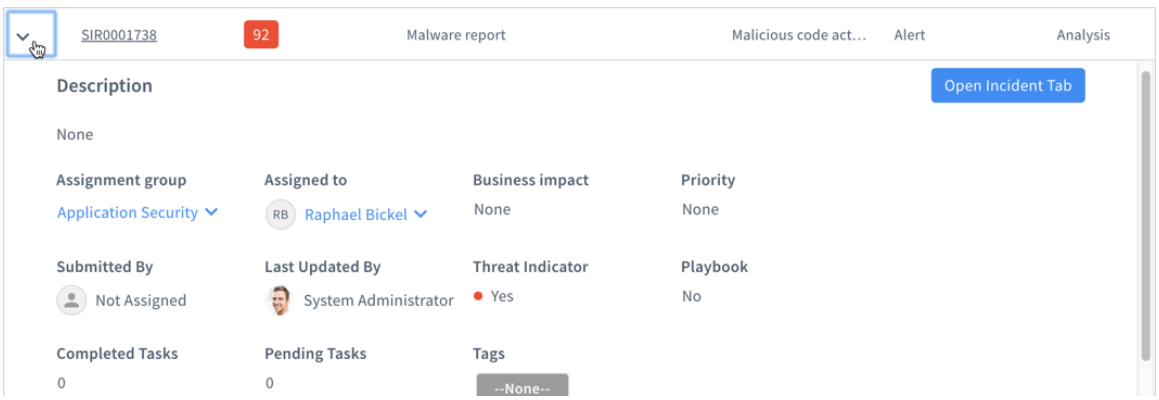
セキュリティインシデントリストのカスタマイズ



ピークビューによる時間の節約

セキュリティインシデントレコードを開く前に、ピークビューを使用して時間を節約できます。この機能を使用すると、ページ全体を再ロードしなくても重要なセキュリティアーティファクトをすばやく見つけることができます。セキュリティインシデント番号の左側にある > アイコンをクリックするだけで、内容を確認できます。

ピークビュー

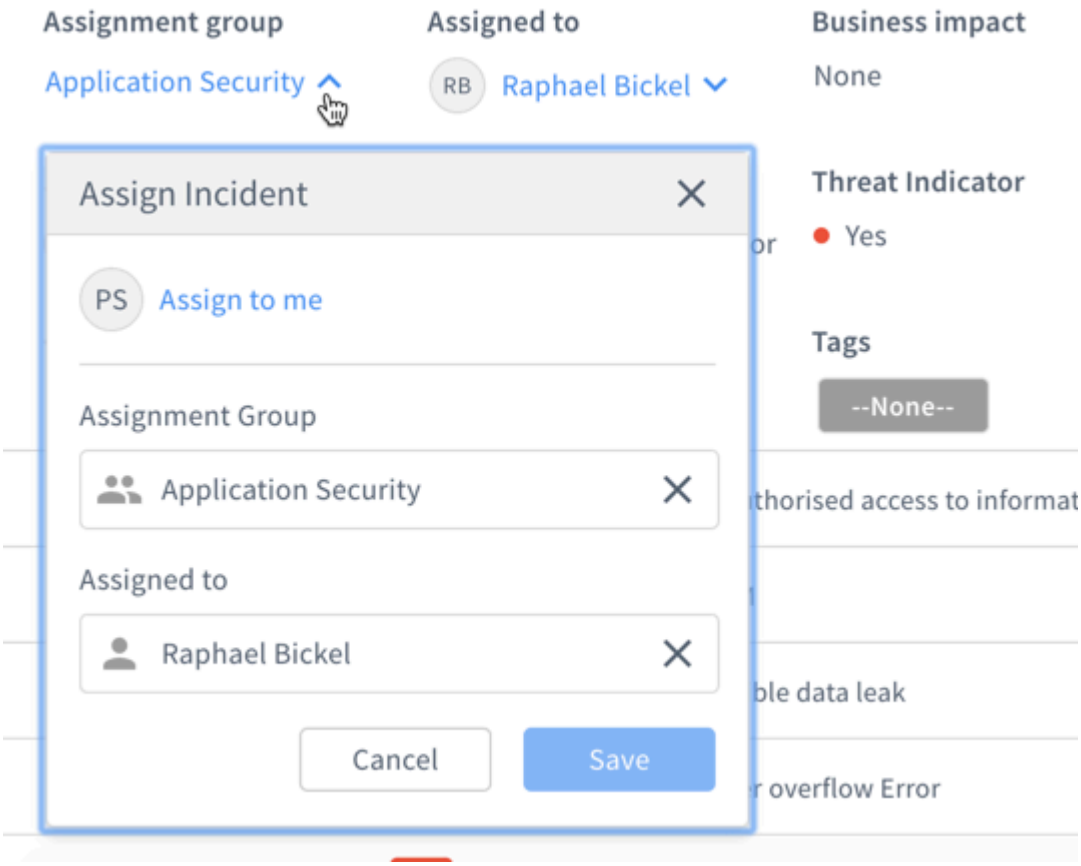


ピークビューは、重要な情報のスナップショットを 1 つのビューで提供します。このビューにより、複数のインシデントを処理する際に貴重な時間を節約できます。特定のフィールドの下矢印をクリックして、アサイン先グループや特定のアナリストのアサインなど、オンザフライでの更新を行うことができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ピークビューの詳細



セキュリティインシデントに対するクイックアクションの実行

特定のセキュリティインシデントを選択して開いた後、レコードに対して時間を節約するアクションを実行できます。

- セキュリティインシデントが開いている場合は、[レコードを編集] アイコンをクリックして、任意のフィールドをすばやく変更します。レコードが閉じている場合は、そのタグのみを変更できます。
- [添付ファイルを管理] をクリックして、セキュリティインシデントにファイルを添付します。添付ファイルをダウンロードまたは削除したり、添付ファイルに適用される暗号化を編集したりすることもできます。
- [メールの作成] をクリックして、同僚にクイックメールを送信します。自由形式のメールを送信することも、テンプレートのリストから選択した定型文メールを送信することもできます。送信されたメールと受信された返信は、インシデントタイムラインにキャプチャされます。

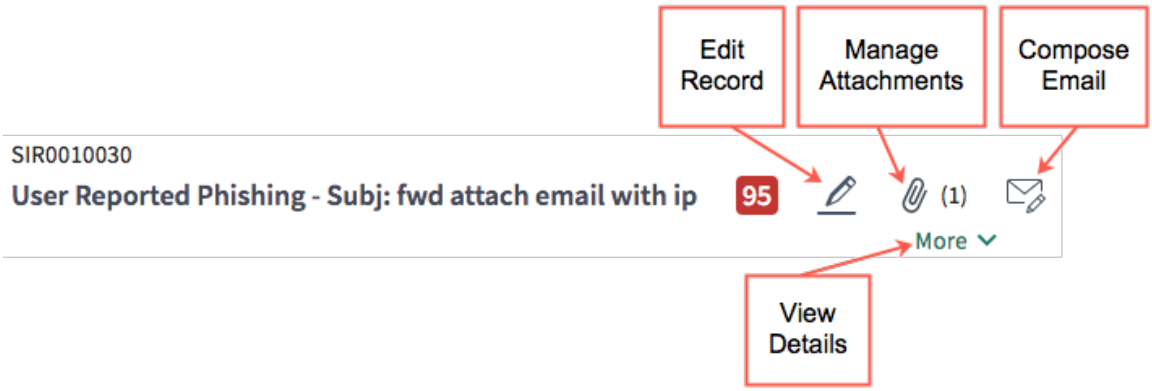
  注:
  メールとメール通知用に再利用可能なコンテンツを含むカスタムテンプレートを作成できます。変数を使用して、件名、優先度、脅威カテゴリなど、セキュリティインシデントまたはアラートに固有の情報を挿入することができます。セキュリティインシデントレスポンス に関連するメールおよびメール通知には、セキュリティインシデント [sn_si_incident] テーブルを使用します。詳細については、「Email templates (メールテンプレート)」を参照してください。

- [その他] をクリックすると、説明、ビジネスインパクト、優先度などのセキュリティインシデントのクイックスナップショットが表示されます。また、[アサイン先グループ] フィールドと [アサイン先] フィールドの下向き矢印をクリックすると、これらのフィールドをオンザフライで変更することができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

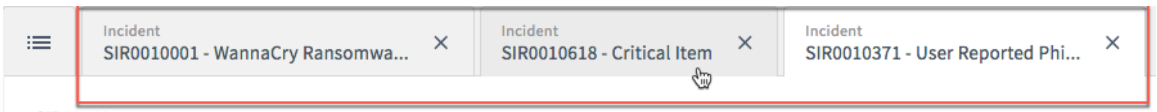
アサイン先グループ



複数のセキュリティインシデントの処理

タブ付きインターフェイスでは、複数のセキュリティインシデントを同時に開いておくことができるため、ワンクリックでそれらを切り替えることができます。これにより、時間を節約し、複数のソースからの脅威が特定されたときに全体像を把握できます。

複数のセキュリティインシデントの処理



セキュリティインシデントタブでの分析情報の表示

セキュリティインシデントレコードを開くと、次の 3 つのタブが表示されます。

- 概要
- 探索
- インシデントタイムライン

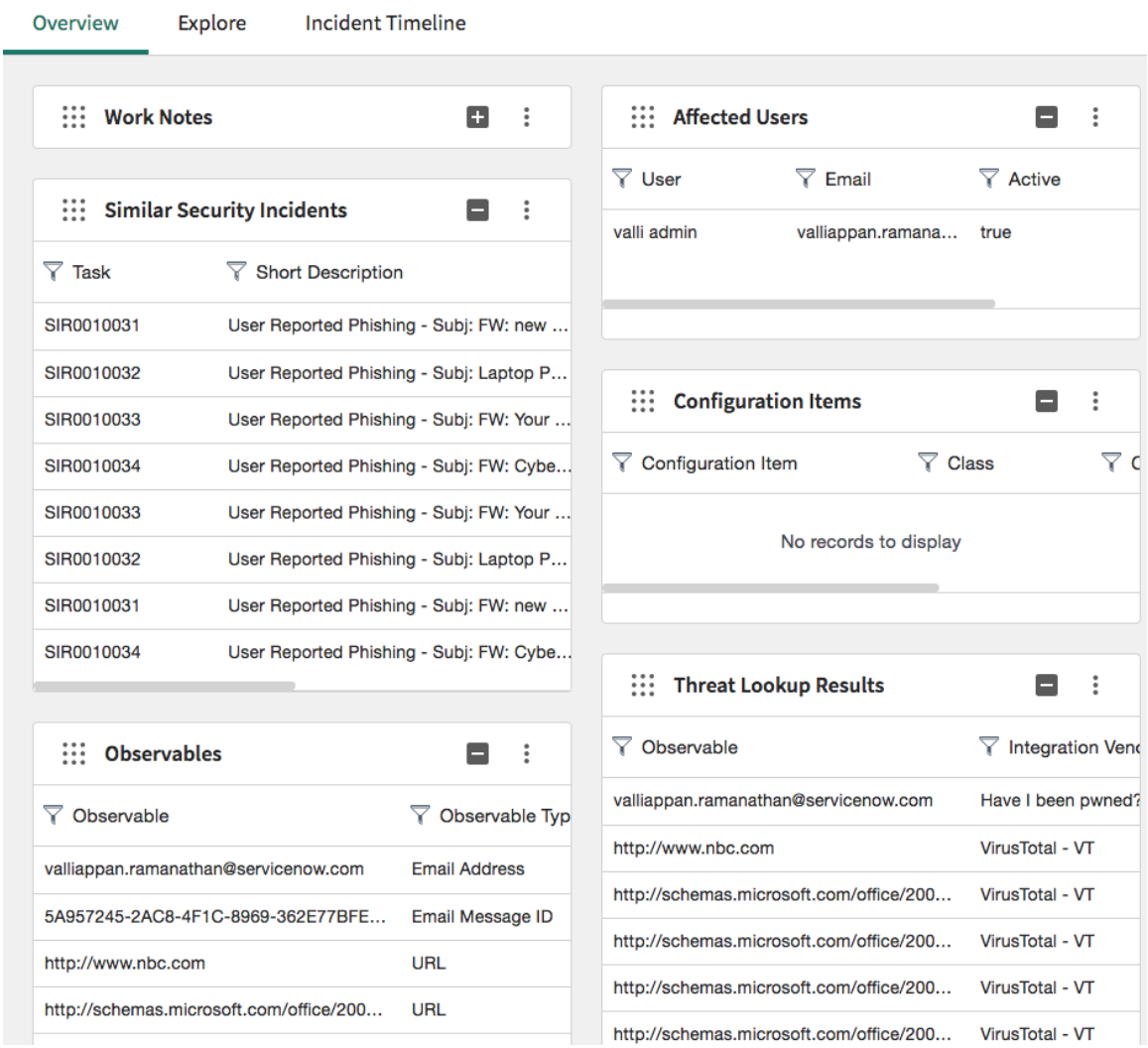
[概要] タブ

[概要] タブを使用して、セキュリティインシデントの情報を 1 か所に表示します。別のアプリケーションやコンソールを開く必要はありません。

自動翻訳

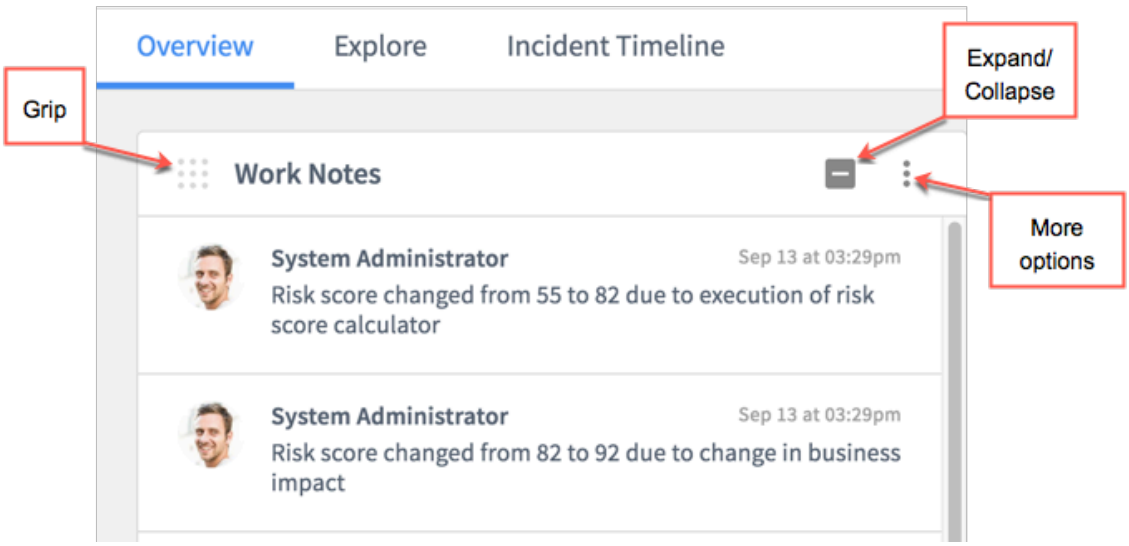
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

概要



[概要] タブに表示されるタイルはカスタマイズ可能です。これらは、必要に応じて折りたたんだり展開したりすることができます。また、グリップアイコンをドラッグして移動することもできます。その他のオプションアイコンをクリックすると、タイルを削除したり、その見出しテキストを変更したりできます。

[概要] タブ



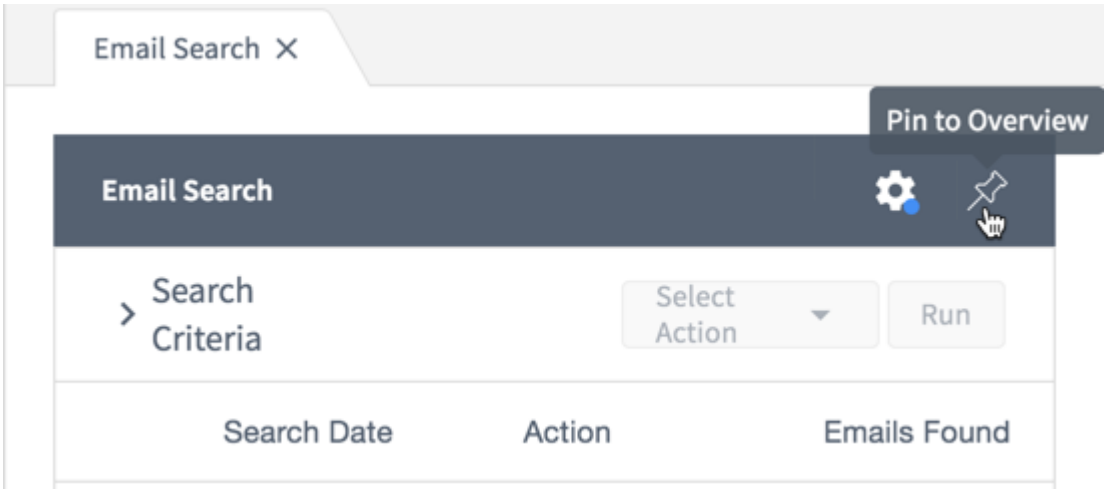
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[探索] タブ

[概要] タブに表示されるタイルを、[探索] タブを使用して構成します。表示するタイルを左側のペインから選択し、固定アイコンをクリックします。固定されたタイルは自動的に [概要] タブに表示されます。

[探索] タブ



[探索] タブの左側のペインには、[概要] タブに表示できるさまざまな情報が含まれています。たとえば、[観測事象] を展開すると、次の関連リストが表示されます。

- 観測事象
- 脅威のルックアップの結果
- セキュリティスキャン結果
- ドメインルックアップ
- 観測事象の拡張

[ユーザー]、[構成アイテム]、および [インシデント] に、追加の関連リストが用意されています。

[インシデントタイムライン] タブ

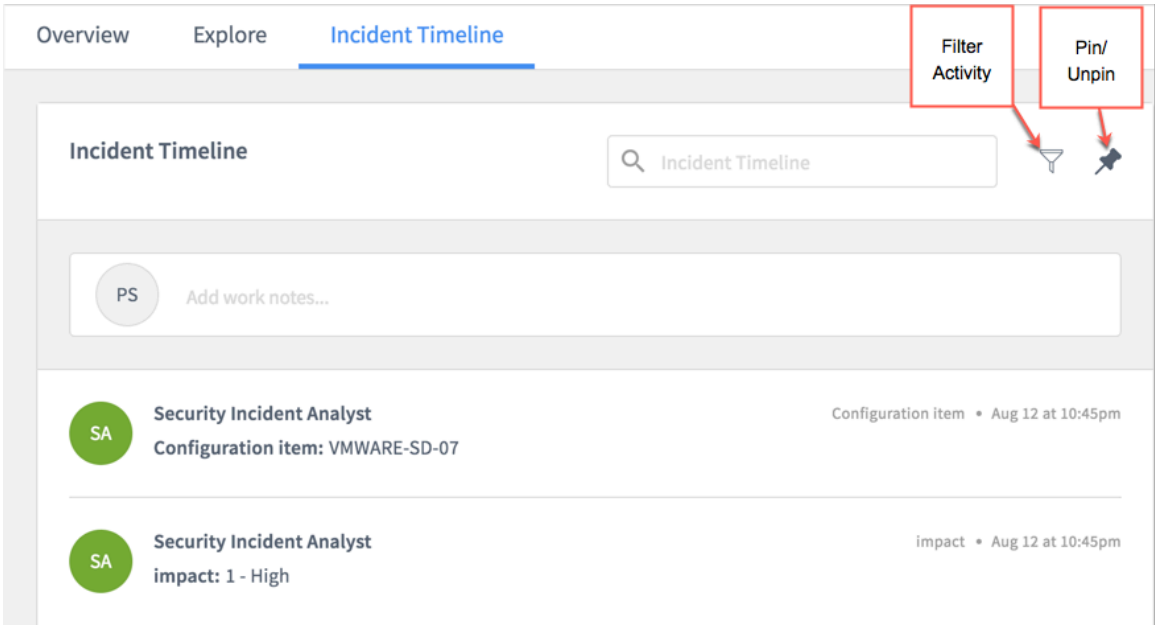
[インシデントタイムライン] タブは、追跡用に調査中に使用します。セキュリティインシデントに対して実行されたアクションは、そのつどシステムによってインシデントタイムラインに記録されます。

- [作業メモを追加] ボックスに作業メモを入力して [投稿] をクリックすることで、作業メモを手動でタイムラインに追加することもできます。
- 検索ボックスを使用して、特定のタイムラインアクティビティを検索できます。
- アクティビティをフィルターアイコンを使用すると、目的のタイプのタイムラインアクティビティのみ (たとえば、特定のアナリストによって作成されたインシデントのみ) を表示できます。
- 固定/固定解除アイコンを使用して、[概要] タブのインシデントタイムラインを追加または削除できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[インシデントタイムライン] タブ



プレイブックを使用したセキュリティインシデントの処理

ビルトインのセキュリティアナリスト向けプレイブックを使用して、特定のタイプのセキュリティ脅威を段階的な方法で解決します。たとえば、アナリストは、プレイブックを使用して、悪意のあるコードアクティビティによって発生するフィッシング攻撃および脅威を解決できます。詳細については、「プレイブックによるセキュリティの脅威の解決」を参照してください。

プレイブックによるセキュリティの脅威の解決

特定のタイプのセキュリティ脅威を段階的な方法で解決するためのプレイブックを使用します。たとえば、プレイブックを使用して、悪意のあるコードアクティビティによって発生するフィッシング攻撃および脅威を解決できます。

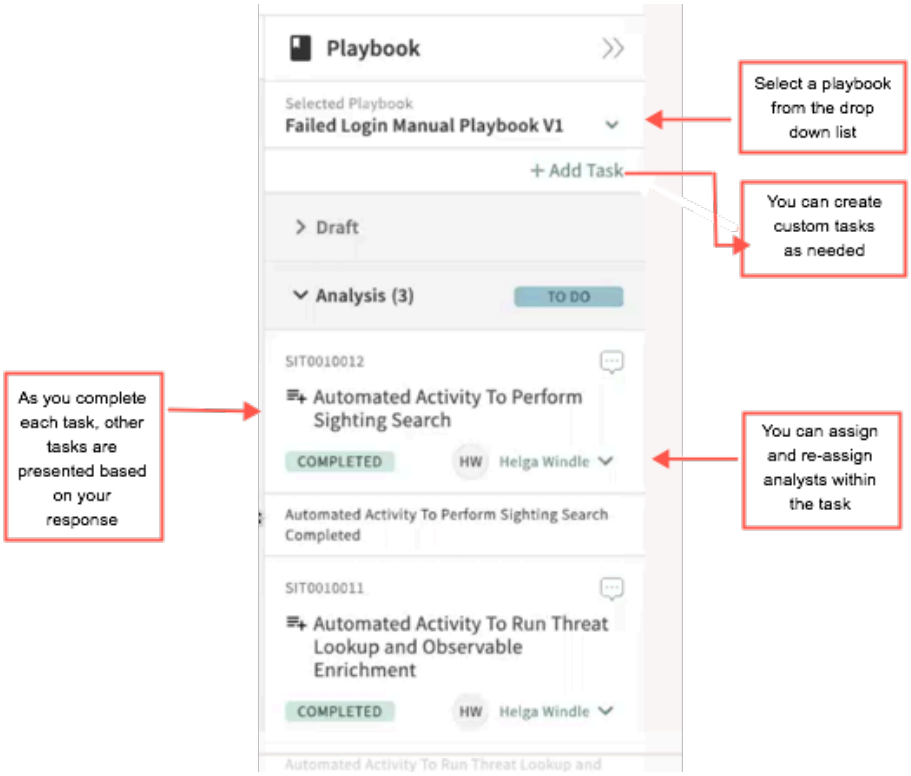
始める前に
必要なロール：sn_si.admin または admin

このタスクについて
各タスクグループ (アナリティクス、封じ込めなど) で、脅威を解決するための一連の質問および他のアクティビティを説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

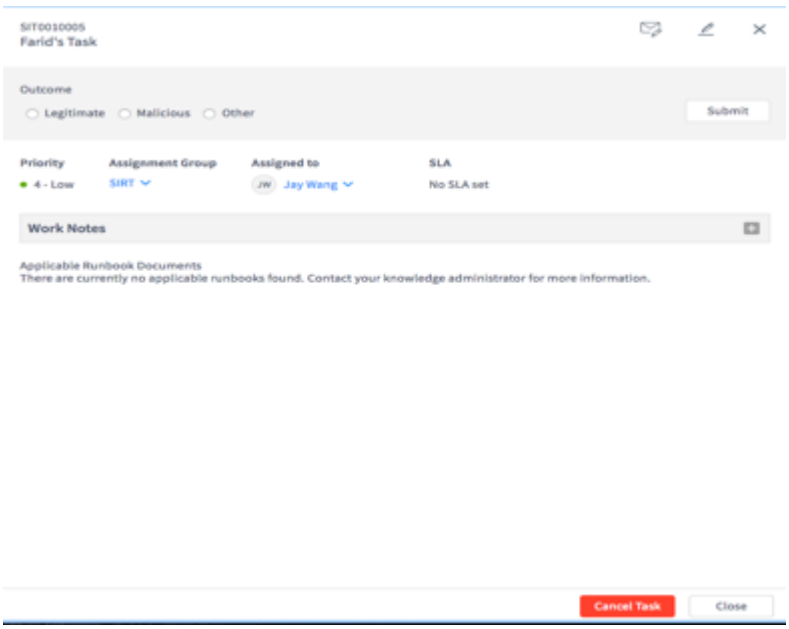
プレイブック



各タスクを進めるときに作業メモを入力しておくと、今後類似した攻撃を分析するのに役立ちます。脅威の特定後、プレイブックの情報を使用して脅威を隔離し、同様に影響を受ける資産を分離し、マルウェアを削除することもできます。

各タスクに含まれるナレッジ記事には、必要な手順を実行するためのヒントやその他の情報が記載されています。

ナレッジ記事



ベースシステムには、各プレイブックタスクのナレッジ記事が含まれています。ただし、独自のナレッジ記事を作成してプレイブックタスクに関連付けることができます。

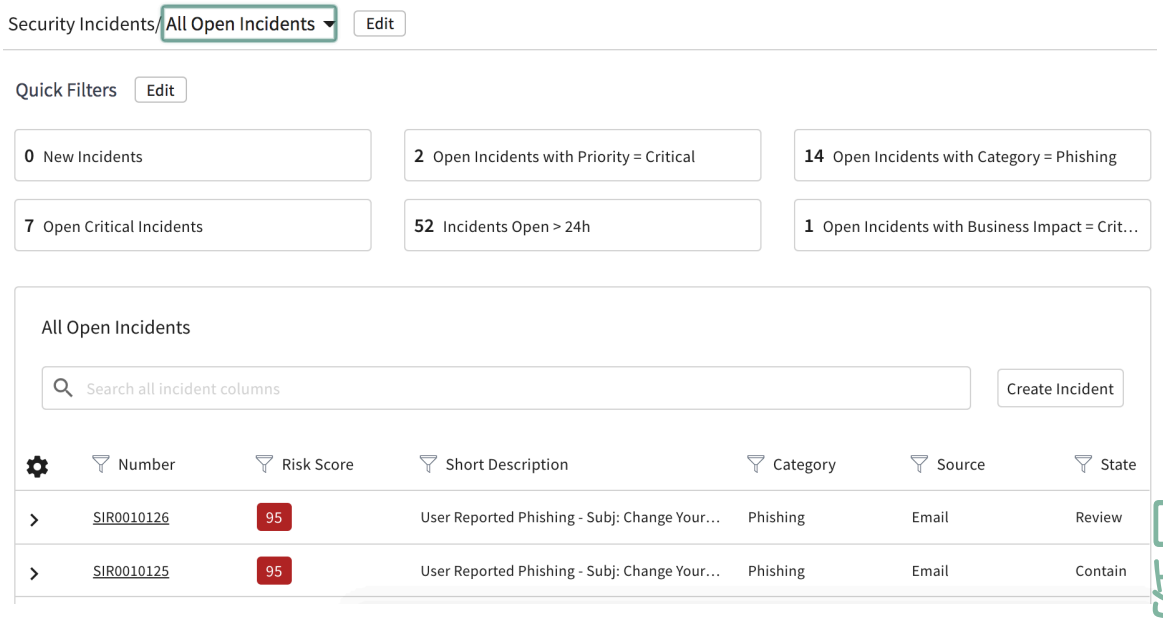
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
プレイブックを使用して特定の脅威を分析および解決する方法の例については、「プレイブックを使用したユーザーから報告されたフィッシング攻撃の解決」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデント (新規 **UI**).
[セキュリティインシデント] 画面には、自分にアサインされているセキュリティインシデントが表示されます。



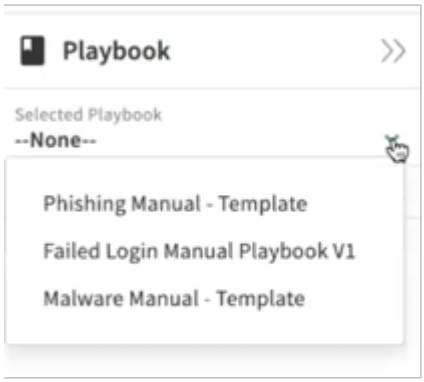
2. [自分にアサイン済み] 選択リストをクリックすると、すべてのオープンインシデントやすべての未アサインインシデントなどの別のフィルターを選択できます。
または、クイックフィルターのいずれかをクリックすると、最重要のインシデントなど、特定のタイプのセキュリティインシデントを表示できます。
3. 分析したいセキュリティインシデントをクリックします。

   リスクスコアが高いセキュリティインシデントを優先することを検討してください。

4. 画面の右端にあるプレイブックペインが閉じている場合は、プレイブックアイコン ( ) をクリックして開きます。
セキュリティインシデントにプレイブックが割り当てられていない場合は、次に示すように、[選択されたプレイブック] 選択リストからプレイブックを選択できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



セキュリティインシデントに別のプレイブックを割り当てることもできます。[選択されたプレイブック] 選択リストにプレイブックを追加したり、セキュリティインシデントのプレイブックを変更したりする方法については、「アナリスト向け Playbook の有効化」を参照してください。

セキュリティの脅威のタイプに固有のプレイブックが開きます。類似するタスクのカテゴリに分割されています。たとえば、[分析] グループのタスクを使用して、脅威の有効性と範囲を判断します。[封じ込め] グループには、脅威を特定のユーザーまたは資産に隔離するためのタスクが含まれています。[除去] グループのタスクは、マルウェアの削除またはホストの再イメージ化の手順を示します。

5. 最初のグループ ([アナリティクス]) をクリックしてから、プレイブックの最初のタスクをクリックします。
6. タスクのプロンプトに従います。
   - 一部のタスクでは、「メールはキャンペーンの一部ですか？(Is Email Part of Campaign?)」などの質問が尋ねられます。必要な分析を実行し、[はい] または [いいえ] を選択して質問に回答します。
   - ナレッジ記事を定義してプレイブックタスクに関連付けると、タスクの作業を開始したときに記事が表示されます。
   - 一部に過渡的なタスクもあります。それらは、観測事象をセキュリティインシデントに追加するなど、特定のアクションを実行するように指示するだけです。アクションを完了したら、[完了としてマーク] をクリックします。

   タスクを完了すると、行った選択に基づいて続きのタスクが提示されます。グレー表示されているグループ ([復旧]、[レビュー] など) も選択によってアクティブ化される場合があります。
7. すべてのタスクを完了し、脅威を解決してセキュリティインシデントをクローズするまで、提示された各タスクの作業を続けます。

関連情報

プレイブックへのカスタムタスクの追加

プレイブックを使用したユーザーから報告されたフィッシング攻撃の解決

フィッシングプレイブックは、会社の従業員の 1 人によって報告されたフィッシング攻撃を分析および解決するために必要なタスクをガイドします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

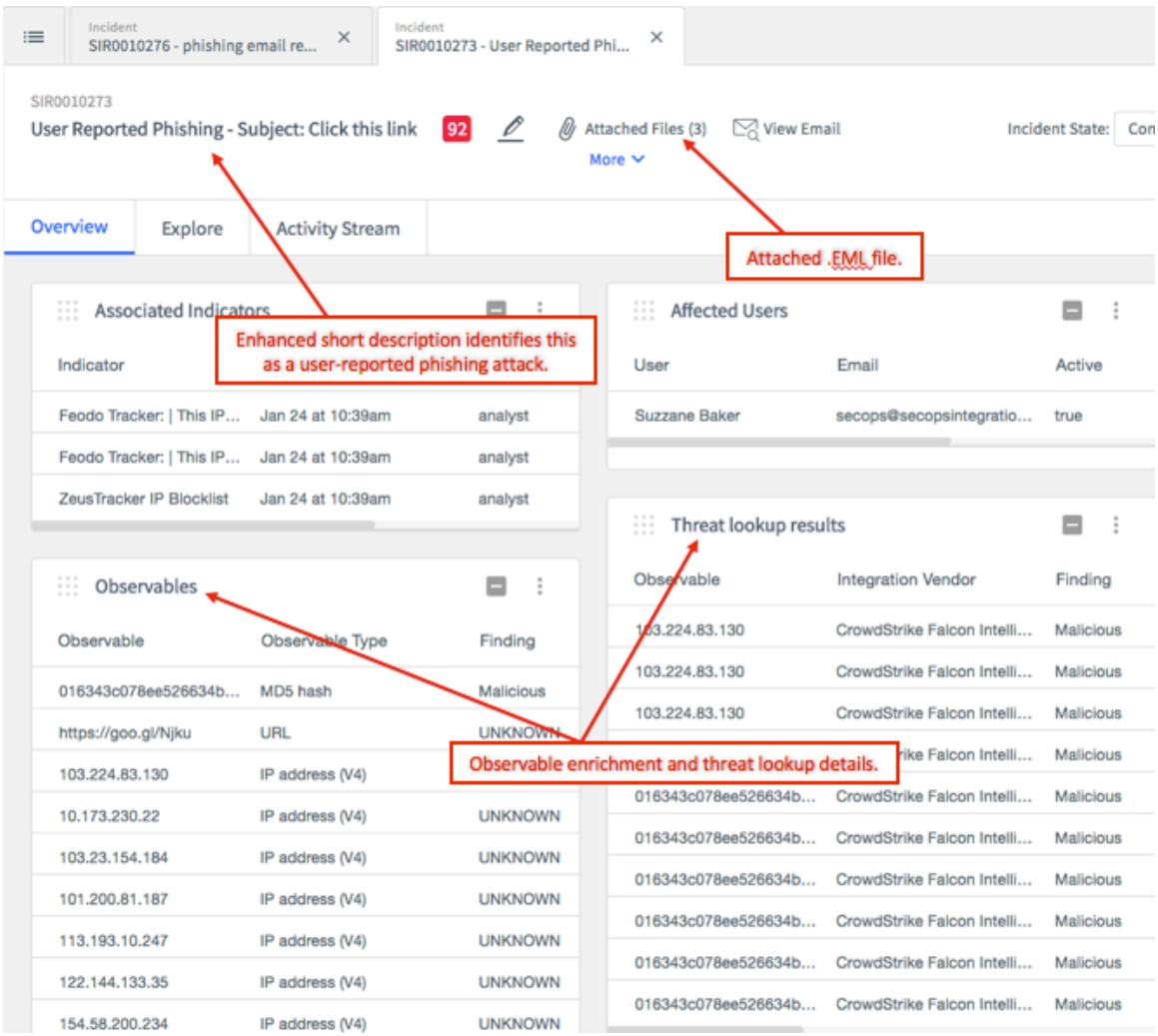
ユーザーから報告されたフィッシング攻撃からセキュリティインシデントを作成する方法

セキュリティインシデントレスポンスのセットアップ中、システムアドミニストレーターは、フィッシング攻撃の兆候を含むメールを特定できる一連のメール一致ルールを作成します。(セキュリティポリシーで定義されている) フィッシング攻撃の一般的な兆候を含む不審なメールを受信した場合、従業員は、それを組織で定義されたフィッシングメールアドレスに .EML 添付ファイルとして送信できます。

フィッシングメールアドレスでメールが受信されると、.EML 添付ファイルが解析され、その情報がメール一致ルールと比較されます。一致が見つかった場合、次の情報を含むセキュリティインシデントが作成されます。

- 簡単な説明には、「ユーザーから報告されたフィッシング (User Reported Phishing)」が含まれ、その後に送信元メールの実際の件名が続きます。
- .EML ファイルがセキュリティインシデントに添付されます。
- .EML に観測事象が含まれている場合は解析され、拡張と脅威のルックアップが自動的に実行されます。

ユーザーから報告されたフィッシング

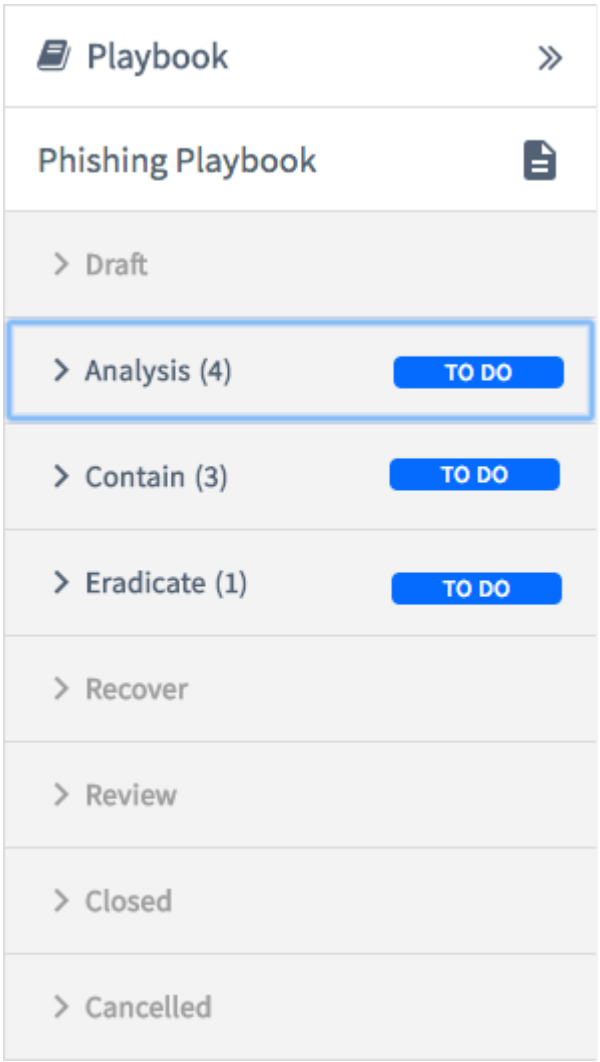


フィッシングカテゴリのセキュリティインシデントが開かれると、フィッシングプレイブックが自動的に利用可能になります。プレイブックアイコン ( ) をクリックするだけでプレイブックが開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィッシングプレイブック



フィッシングプレイブックには、フィッシングの脅威を分析、封じ込め、根絶するのに役立つタスクが含まれています。タスクは状況に整理されます (たとえば、[分析]、[封じ込め])。あるステータスのすべてのタスクが完了すると、プレイブックによって次のステータスにガイドされます。

セキュリティインシデントの詳細の分析

セキュリティインシデントのステータスが [分析] の場合は、次のようなインシデントの基本的な調査を実行するタスクが与えられます。

- インシデントの有効性を判断する。
- 潜在的な脅威の影響度を調査する。
- インシデントへの効果的な応答を調整する。

タスクを実行する場合：

- ナレッジ記事をよく理解する。
- メールの添付ファイルを開き、一般的なフィッシング要素の兆候を調べる。
- 脅威のルックアップの結果を確認する。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントの封じ込め

セキュリティインシデントのステータスが [封じ込め] の場合は、メールの詳細を確認するタスクが与えられます。脅威が組織に侵入できないようにするには、侵入防御システム (IDS) および侵入防止システム (IPS) の署名とルールの形でネットワーク防御を更新します。

タスクを実行する場合：

- 影響を受けたデバイスを隔離するなど、脅威の影響を制限するアクションを実行する。
- メールに添付された観測事象を確認する。
- いずれかのメールコンテンツが次を含む既知の脅威に関連付けられているかどうかを確認する。
  - URL
  - メール送信者
  - フィッシング URL
  - 送信者の SMTP サーバーの IP アドレス

マルウェアの根絶

更新された署名とルールをウイルス対策ソリューションに展開したら、[根絶] ステータスのタスクを使用して、マルウェアが存在するかどうかを判断し、それに応じて処理します。

タスクを実行する場合：

- 影響を受けるデバイスのエンドポイントをスキャンして、マルウェアの存在を確認する。
- 検出されたマルウェアを削除する。
- 最後の手段として、ホストデバイスをワイプして再イメージ化する。

セキュリティインシデントのレビュー

分析タスクの実行時にフィッシング攻撃が誤報であったと判断した場合、セキュリティインシデントは [レビュー] ステータスに移行します。この場合、メールの添付ファイルを開いても安全であることをユーザーに知らせる必要があります。

セキュリティインシデントのクローズ

プレイブックのすべてのタスクが完了すると、セキュリティインシデントは [クローズ] 状況に移行します。インシデントをクローズする前に、クローズコメントを入力する必要があります。

セキュリティインシデントのキャンセル

セキュリティインシデントのステータスが [レビュー] のときにメールが脅威ではないことをユーザーに正常に通知すると、[キャンセル] ステータスがアクティブになり、セキュリティインシデントをキャンセルできます。

注:
復旧タスクはフィッシングプレイブック では使用されません。

ナレッジ記事とプレイブックタスクの関連付け

組織で各タスクのナレッジ記事が定義されている場合、セキュリティインシデントレスポンス プレイブックを使用してセキュリティ上の脅威を分析すると、それらの記事を表示できます。ナレッジ記事が存在しない場合は、作成してプレイブックタスクに関連付けることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
セキュリティインシデントレスポンス で プレイブックを使用するときは、各タスクに関連付けられたテキストをメモします。たとえば、フィッシングカテゴリの最初のタスクは [従業員が送信したアラートでしたか？**(Was Alert Employee-Submitted?)]** です。これはタスクの簡単な説明です。ナレッジ記事をタスクに関連付けるには、このテキスト (プレイブックに表示されるとおりのテキスト) が必要です。

必要なロール：sn_sir.knowledge_admin、および sn_si.admin または admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > カタログとナレッジ > ナレッジ.
2. 特定のプレイブックタスクのナレッジ記事を作成して公開します。
3. 次のように移動する。 セキュリティインシデント > 手動 **Runbook** > 新しい **Runbook** を作成.
4. 次の情報を入力して Runbook を作成します。

フィールド	説明
ナレッジ記事	プレイブックタスクに関連付ける公開済みのナレッジ記事を選択します。
テーブル	セキュリティインシデントレスポンス タスク [sn_si_task] を選択します。
条件	条件ビルダーを次のように設定します。 ○ オプション：[簡単な説明] を選択します。 ○ 演算子：[次の値に等しい **(is)]** を選択します。 ○ 入力値：プレイブックに表示されるとおりに、タスクの簡単な説明を入力します。

5. **[Submit]** をクリックします。
次回プレイブックを実行してこのタスクを選択すると、関連付けられたナレッジ記事が表示されます。

関連情報

セキュリティインシデントナレッジ記事の作成

セキュリティインシデントレスポンス Runbook の作成

プレイブックへのカスタムタスクの追加

セキュリティアナリストワークスペースベースシステムには、各脅威カテゴリの一連のタスクが含まれています。システムまたは顧客の独自のニーズを満たすカスタムタスクを作成できます。

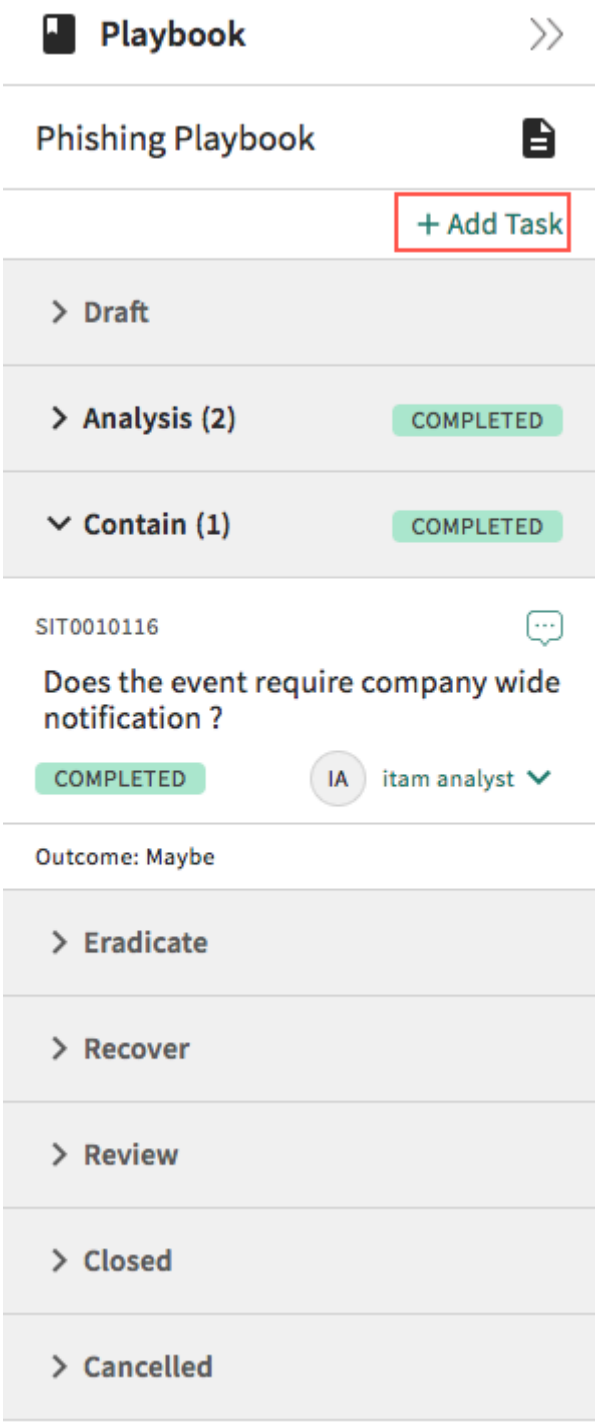
始める前に
必要なロール：sn_si.basic または security_admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

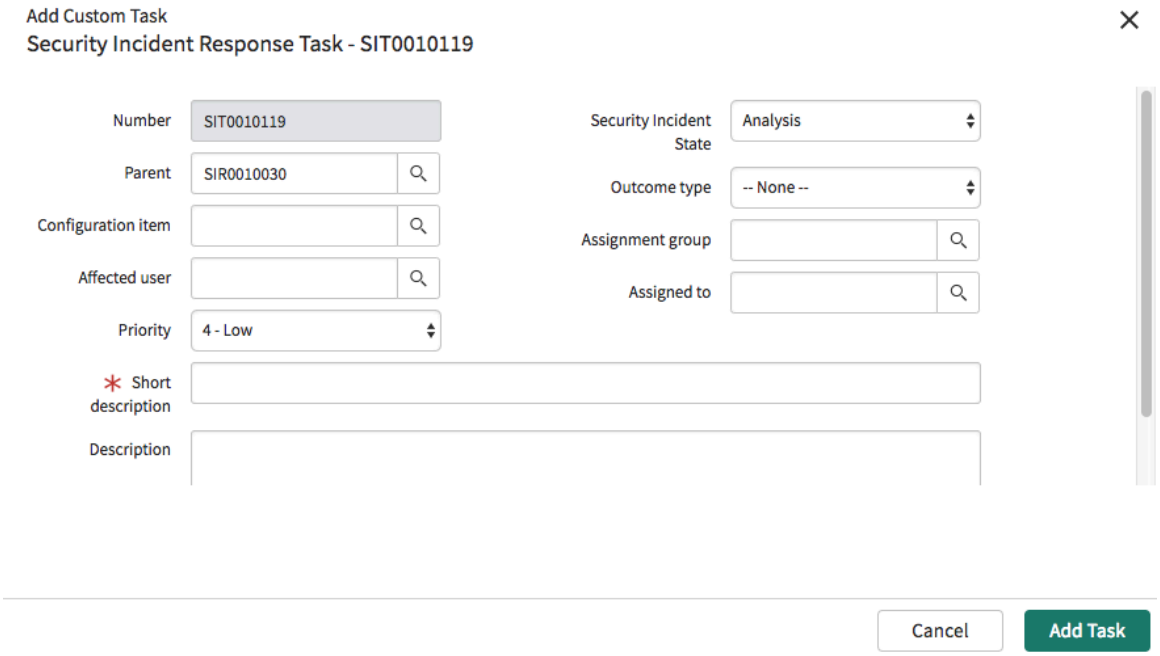
1. プレイブックを開いた状態で、[タスクを追加] をクリックします。



[カスタムタスクを追加] 画面が開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



2. 必要に応じて、フィールドに入力します。

フィールド	説明
数値	[読み取り専用] 自動的に生成されるセキュリティインシデントタスク番号。
親	関連するセキュリティインシデントの番号。
構成アイテム	セキュリティ上の問題の影響を受ける構成アイテム (存在する場合)。
影響を受けるユーザー	セキュリティ上の問題の影響を受けるユーザー (存在する場合)。
優先度	このタスクをいつ実行するかを決定するために使用される優先度を選択します。
セキュリティインシデントのステータス	セキュリティ応答タスクの現在のステータス。必要に応じて将来のステータスを選択できます。
結果タイプ	sn_si.basic ロールを持っている場合は、結果タイプとして [はい/いいえ] を選択します。 security_admin ロールを持っている場合は、複数のカスタム出力値を持つカスタム結果タイプを作成できます。たとえば、脅威カテゴリに基づく依存値を持つタスクを定義できます。詳細については、「選択リスト」を参照してください。
アサイン先グループ	アサインされるワーカーが選択されるアサイン先グループ。
アサイン先	タスクを実行するようアサインされる個人。
簡単な説明	セキュリティインシデントプレイブックタスクの説明。
説明	選択したタスクの説明を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 入力が完了したら、[タスクを追加] をクリックします。
   タスクは、現在のタスクに続いてプレイブックに挿入されます。

ユーザーから報告されたフィッシングおよびマルウェア攻撃のサイティング検索

メールまたは観測事象に対してサイティング検索を実行して、フィッシング攻撃や悪意のある IP や URL との通信などの特定のタイプの攻撃がネットワーク上でどの程度の頻度で発生しているのかを把握することができます。各発生は 1 回のサイティングと見なされます。観測事象のサイティング検索は、ログストアまたはセキュリティ情報およびイベント管理 (SIEM) に対して設定する必要があります。

サイティング検索機能を使用してフィッシングされたユーザーを特定し、ネットワーク上のログストア内でフィッシングとマルウェアの観測事象を追跡する方法。

サイティング検索機能を使用してフィッシングされたユーザーを特定し、ネットワーク上のログストア内でフィッシングとマルウェアの観測事象を追跡する方法については、この 3 分間のビデオをご覧ください。

ユーザーから報告されたフィッシング攻撃を説明するために次の用語が使用されます。

- フィッシングされたユーザー：フィッシングメールを受信したユーザー。
- 被害者ユーザー：(一般的にはフィッシングメールのリンクをクリックすることにより) フィッシング URL とのインタラクションを持ったユーザー。このアクションにより、認証情報が攻撃者に公開される可能性があります。

フィッシングインシデントの分析を始める際、メールサイティング検索を実行するか、観測事象のサイティング検索を実行して、同じフィッシング攻撃の影響を受けている組織内の他のユーザーを特定できます。ログストアを検索して、フィッシングされたユーザーと被害者ユーザーを特定します。影響を受けているユーザーのリストを特定したら、セキュリティインシデントレスポンス で利用可能なツールを使用して包括的なインシデント応答手順を実行するための子セキュリティインシデントを作成します。

注:
次のアプローチを使用してサイティング検索を実行することもできます。

- 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示 をクリックし、セキュリティインシデントをクリックします。
- [関連リンク] で **[IoC を表示]** をクリックします。観測事象のリストが表示されます。
- リストから観測事象を選択し、[アクション] リストから次のオプションのいずれかを選択します。
  - Web トラフィックのサイティング検索を実行する
  - メールトラフィックサイティング検索の実行
- 期間を指定し、[検索] をクリックしてサイティング検索を実行します。

保存済みのサイティング検索構成

サイティング検索を構成し、観測事象のインスタンスの SIEM または他のログストアの保存済みの構成を作成して、環境内の悪意のある観測事象の存在を確認します。

注:
保存された検索とインプレースクエリは、Splunk Integration でのみサポートされています。

関連情報

サイティング検索設定レコードの作成

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ユーザーから報告されたフィッシング攻撃のメールサイティング検索の実行

フィッシングメールを受信したユーザーを、メールの件名、送信者名、メッセージ ID などの観測事象に基づいて検索します。その後、これらのフィッシングメールを封じ込めて組織から根絶することができます。

始める前に
必要なロール：sn_si.analyst

このタスクについて
Splunk メールトラフィックログを検索して、不審なメールの受信者のリストを収集します。検索は、セキュリティインシデントで条件として関連付けられているメール送信者、メールメッセージ ID、またはメールの件名を使用して実行できます。

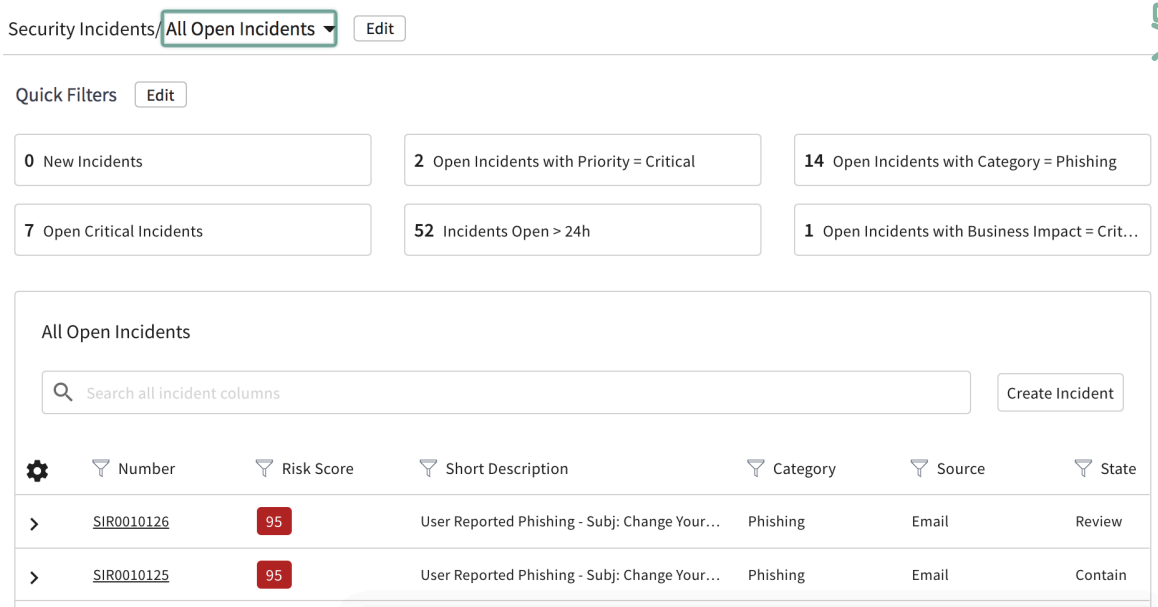
注:

- メールベースの観測事象のサイティング検索の実装は、Splunk Enterprise ログストアでのみテストされています。
- サイティング検索クエリで正確な結果を返すには、Splunk ログイベントが共通情報モデル (CIM) に準拠している必要があります。

手順

1. チームにアサインされたセキュリティインシデントを表示するには、次に移動します: セキュリティインシデント > インシデント (新規 **UI)**.
2. [セキュリティインシデント] リストから、いずれかのフィルター ([オープン中のインシデント]、[自分にアサインされているすべてのインシデント **(all incidents assigned to you)]**、[すべてのインシデント] など) を選択します。

   重大なインシデントやフィッシングメールなど、特定のタイプのセキュリティインシデントを表示するには、いずれかの [クイックフィルター] をクリックします。

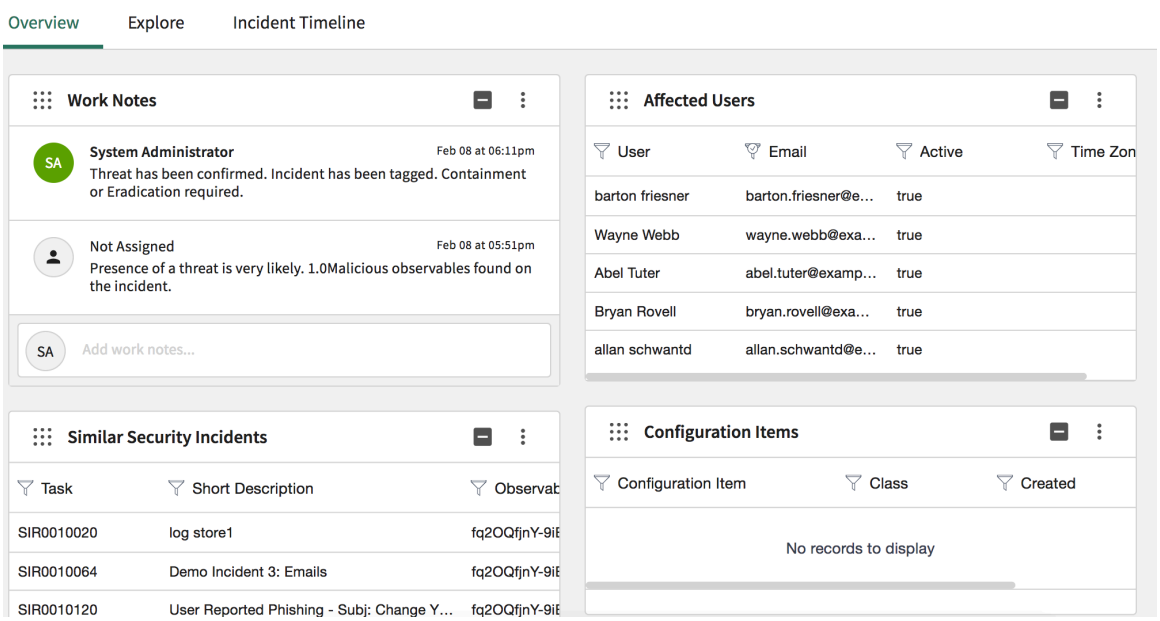


3. 分析するセキュリティインシデントをクリックします。

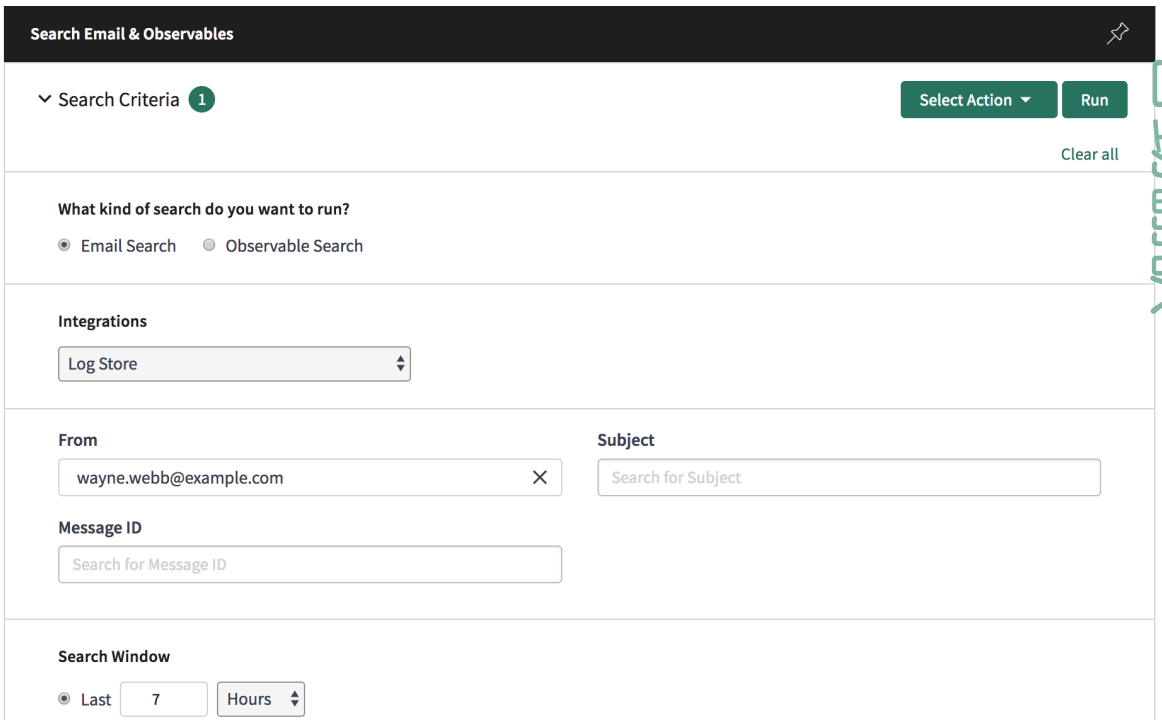
   [概要] タブで、観測事象のリスト、影響を受けるユーザー、および類似のセキュリティインシデントを含む、セキュリティインシデントの概要を確認できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [探索] タブをクリックします。
5. [インシデントデータ] で、 調査 > メールと観察事項を検索.



6. [検索条件] セクションを展開します。
7. 実行する検索のタイプとして [メールの検索] を選択し、残りの検索条件を指定します。

検索条件フォーム

フィールド	説明
統合	統合のタイプ。リストから [ログストア] を選択します。

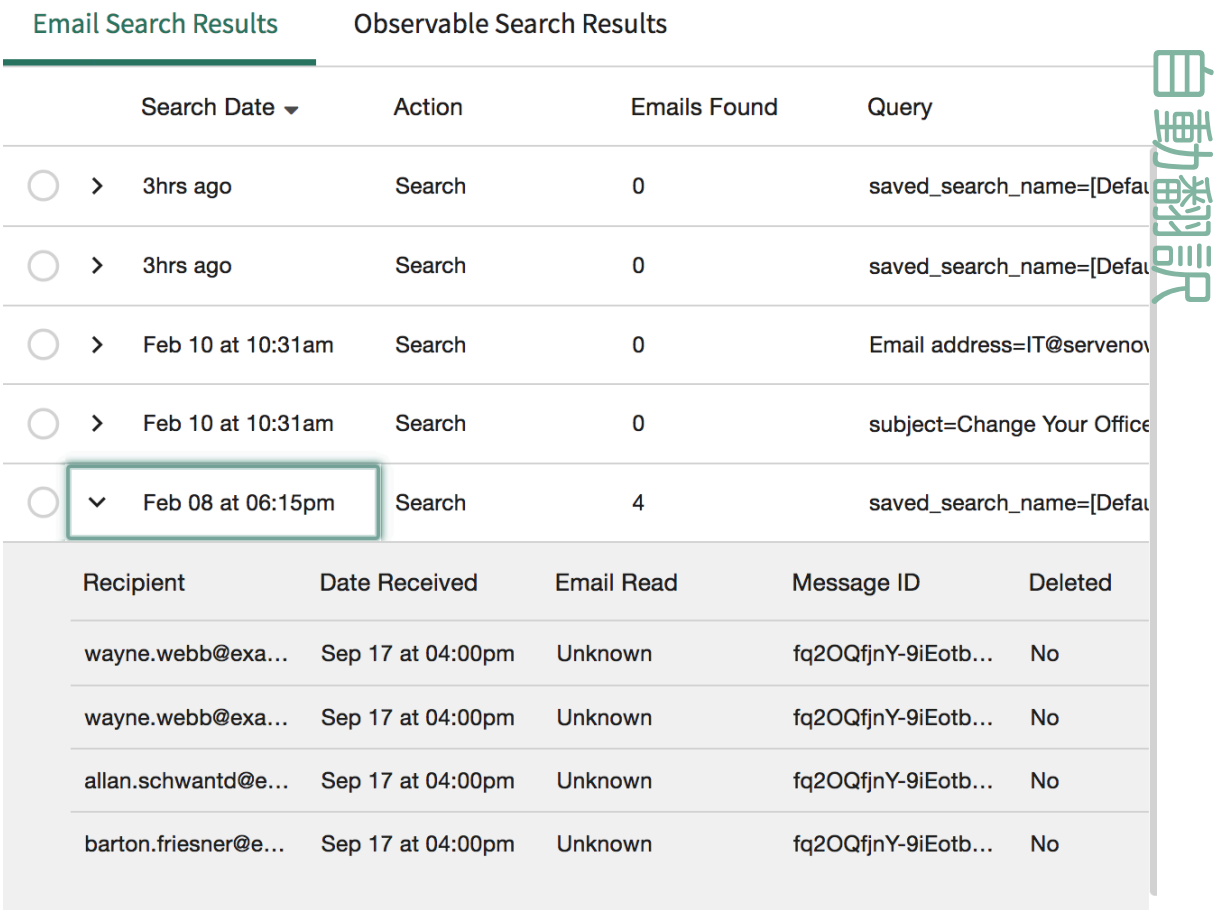
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: この機能は、Splunk ログストアでのみサポートされています。
送信元	送信者の正確なメールアドレス (jane.doe@example.com など)。
メッセージ ID	ログストアからのメールメッセージ ID。
件名	フィッシングメールの件名。
検索ウィンドウ	検索の期間 (過去 24 時間など)。

8. [アクションを選択] リストから [検索] を選択し、[実行] をクリックします。

   入力した条件を使用して Splunk ログストアが検索され、フィッシング攻撃のターゲットとなったユーザーが [メールの検索結果] タブに表示されます。フィッシングメールの合計数と、各メールの詳細 (受信したメールの日付、受信者、メッセージ ID など) が表示されます。

9. フィッシングメールを受信したユーザーのリストを表示するには、[検索日] 列で **[>]** 記号をクリックします。



10. メールを受信したユーザーのリストを表示するには、次の場所に移動します: ユーザー > 影響を受けるユーザー.

    [フィッシングされたユーザー] 列は、メールの受信者を示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[影響を受けるユーザー] ページには、ServiceNow インスタンスに存在するユーザーレコードのみが表示されます。

11. フィッシング攻撃のターゲットであるユーザーをさらに調査するには、次の手順を実行します。
    a. ユーザー名の横にあるチェックボックスをオンにします。
    b. リストから [子のセキュリティインシデントの作成] を選択し、[実行] をクリックします。
    子セキュリティインシデントが作成されたことを示すメッセージが表示されます。親インシデントに関連付けられた子セキュリティインシデントを表示するには、[探索] タブをクリックして インシデント > 子セキュリティインシデント.

タスクの結果
フィッシングされたユーザーのリストが表示されます。

ユーザーから報告されたフィッシングおよびマルウェア攻撃の観測事象サイティング検索の実行

観測事象のサイティング検索を実行して、特定の期間内に特定の悪意のある/不審な Web サイトを訪問したユーザーの数を確認します。

始める前に
必要なロール：sn_si.analyst

このタスクについて
セキュリティインシデントに関連付けられた URL、宛先ホスト、宛先 IP アドレスなどの観測事象のネットワークトラフィック検索を実行できます。

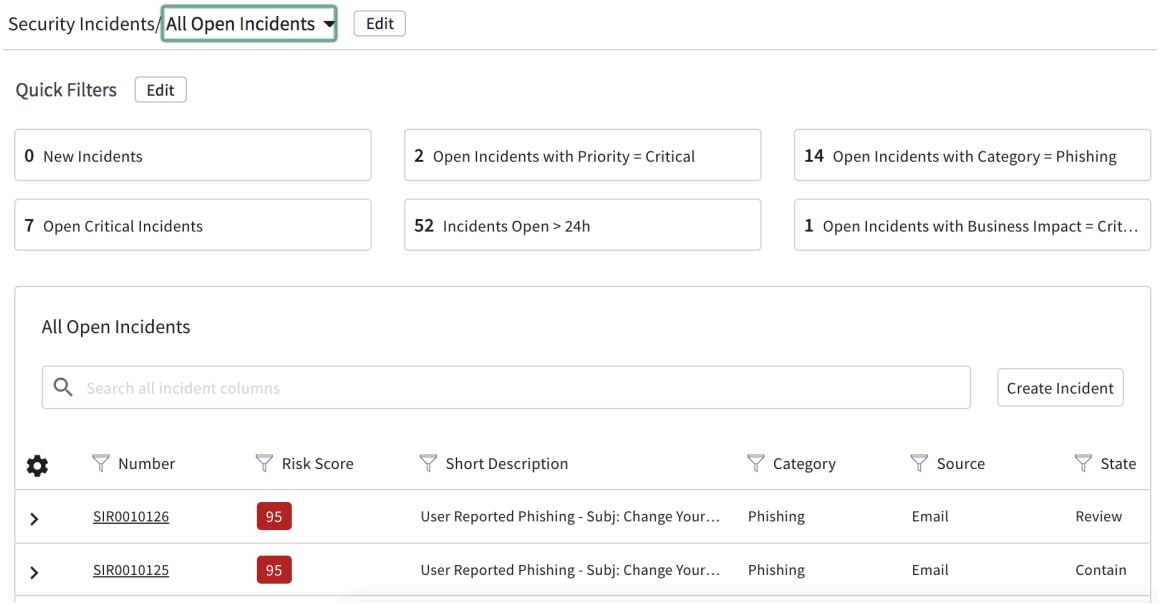
注:
- 観測事象のサイティング検索の実装は、Splunk Enterprise ログストアでのみテストされています。
- サイティング検索クエリで正確な結果を返すには、Splunk ログイベントが共通情報モデル (CIM) に準拠している必要があります。

手順
1. チームにアサインされているセキュリティインシデントを表示するには、次に移動します: セキュリティインシデント > インシデント (新規 **UI)**.
2. [セキュリティインシデント] リストから、すべての [自分に割り当てられたインシデント]、[すべてのオープンインシデント]、[すべてのインシデント] など、別のフィルターを選択します。

   重大なインシデントやフィッシングメールなど、特定のタイプのセキュリティインシデントを表示するには、いずれかの [クイックフィルター] をクリックします。

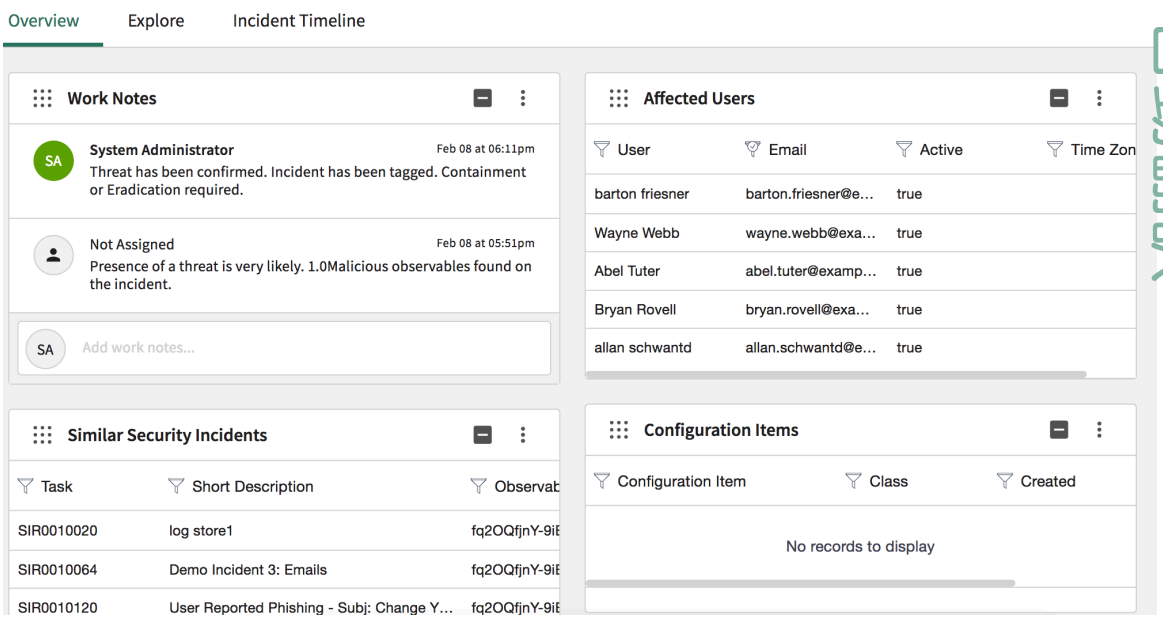
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. 分析するセキュリティインシデントをクリックします。

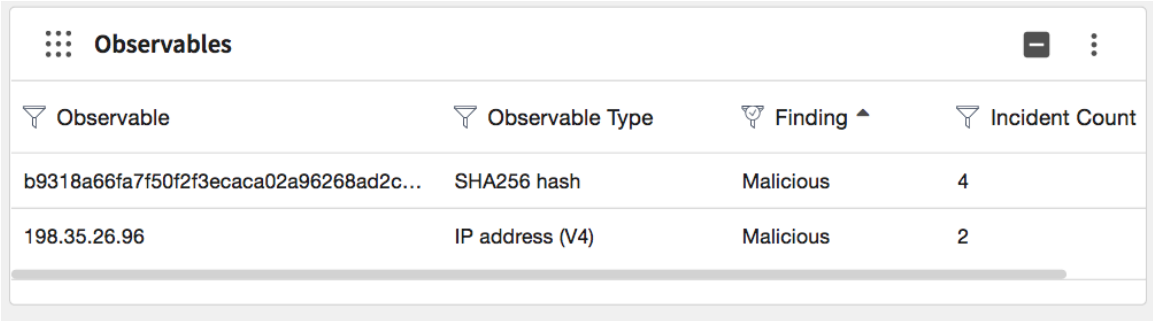
観測事象のリスト、影響を受けるユーザー、および類似のセキュリティインシデントを含む、セキュリティインシデントの概要を確認できます。



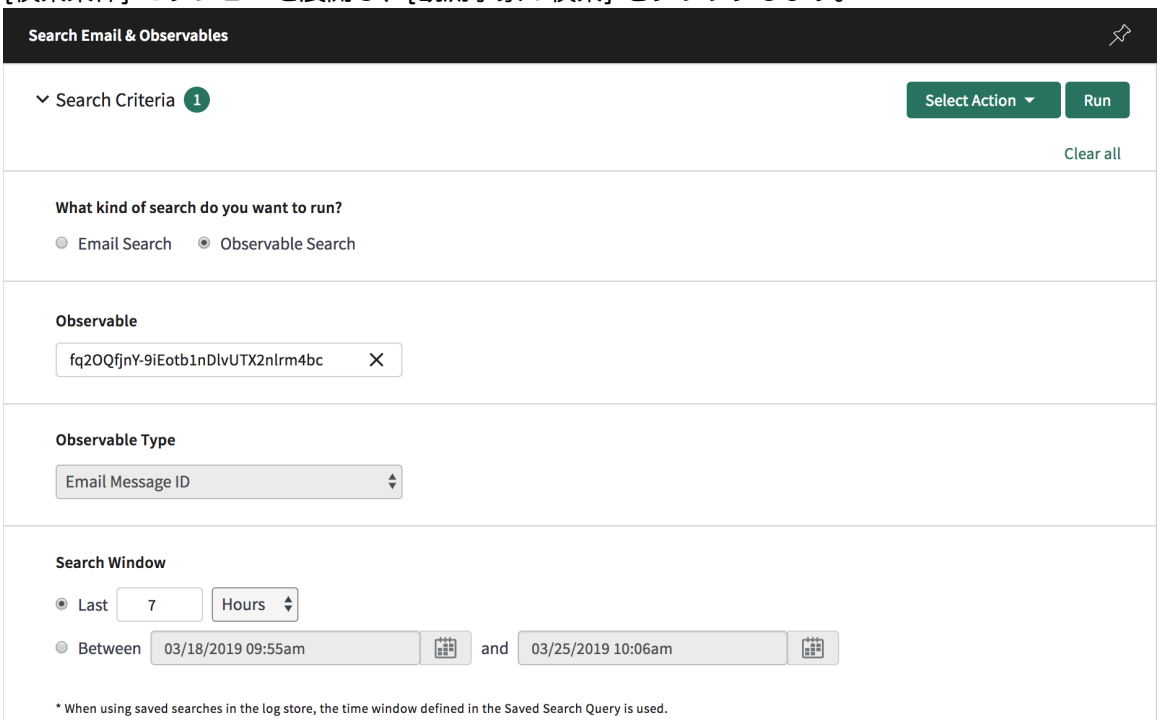
[観測事象 (Observables)] セクションで、[観測事象 (Observable)] 列にメールアドレス、件名、および URL が表示されていることを確認します。また、[結果] 列には、フィッシングメールが送信されたときにその URL が自動的にスキャンされ、既知の悪意のある URL であると判断されたことが表示されます。[インシデント数] 列には、同じ観測事象を共有する他のインシデントが表示されます。これらのアーティファクトは、組織内の何人のユーザーが影響を受けたかを判断するなど、このフィッシング攻撃の封じ込め手順に進む準備ができていることを示しています。

自動翻訳

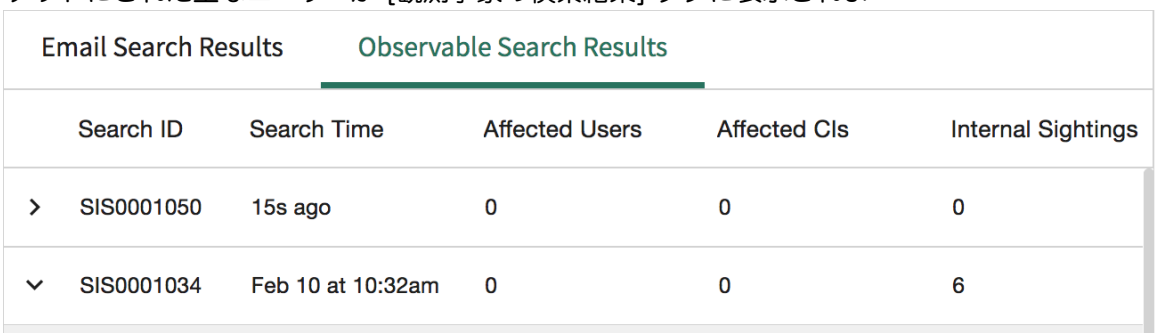
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. 次のように移動する。 探索 > 調査 > メールと観察事項を検索.
5. [検索条件] セクションを展開し、[観測事象の検索] をクリックします。



6. 検索する観測事象と、検索する期間 (「過去 24 時間」など) を入力します。
7. [アクションを選択] リストから [検索] を選択します。
   入力した条件を使用して Splunk ログストアが検索され、悪意のある攻撃のターゲットにされた主なユーザーが [観測事象の検索結果] タブに表示されます。



8. メールを受信したユーザーを表示するには、次の場所に移動します: ユーザー > 影響を受けるユーザー.

   [フィッシングされたユーザー] 列はフィッシングメールの受信者を識別し、[ユーザーのインタラクション] 列はフィッシング URL をクリックしたか、または不審なメールアドレスとやり取りを

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

したユーザーを識別します。[ユーザーのインタラクション] 列は、ユーザーが悪意のあるリンクまたは IP をクリックしたかどうかに応じて true または false に設定されます。

> **注:**
> [影響を受けるユーザー] ページには、ServiceNow インスタンスに存在するユーザーレコードのみが表示されます。

9. フィッシングメールをクリックし、認証情報を盗まれた可能性があるユーザーをさらに調査するには、次の手順を実行します。

   a. [フィッシングされたユーザー] 列と [ユーザーのインタラクション] 列の両方で、**[true]** と表示されているユーザー名の横のチェックボックスをオンにします。

   b. [子セキュリティインシデントの作成] をクリックし、[実行] をクリックします。
   子セキュリティインシデントが作成されたことを示すメッセージが表示されます。親インシデントに関連付けられた子セキュリティインシデントを表示するには、[探索] タブをクリックしてインシデント > 子セキュリティインシデント.

タスクの結果
フィッシングされたユーザーのリストが表示されます。

サイティング検索設定レコードの作成

複数のサイティング検索設定レコードを作成し、複数のログストアを照会したり、検索パラメーターを変更したりするときに使用します。

始める前に
必要なロール：sn_si.admin

- CIM アドオンが Splunk インスタンスにインストールされている必要があります。
- 保存された検索とインプレースクエリは、Splunk Integration でのみサポートされています。

このタスクについて
サイティング検索設定レコードを作成して、Splunk エンタープライズログストアで保存済みの検索 を呼び出すこともできます。

> **注:**
> 検索構成クエリは、Splunk 共通情報モデル (CIM) に準拠するために Splunk ログデータに依存しています。

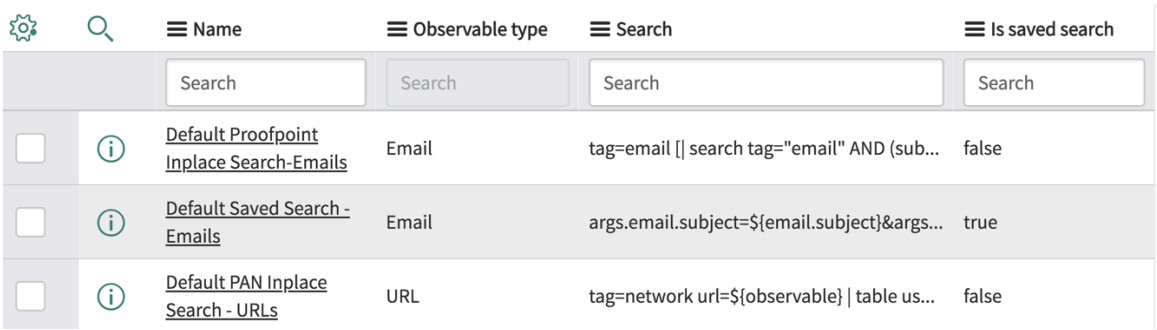
保存済みの検索構成を使用して、次のことができます。

- 複数のイベントレコードを組み合わせたカスタム検索の作成
- 設計効率に優れ、効果的な検索
- Splunk の保存済みの検索でパラメーター化された入力を使用

ベースシステムには、次の画像に示すサンプル構成が含まれています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

保存済みの検索の構成



	Name	Observable type	Search	Is saved search
	Search	Search	Search	Search
	Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
	Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
	Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

この保存済みの検索とインプレース構成クエリはサンプルクエリです。パラメーターは、お使いの環境に合わせて適宜置き換えてください。必要に応じて、保存済みの検索構成を追加で作成します。保存済みの検索構成を定義するときに、検索クエリの名前とパラメーターは、Splunk インスタンスで定義した保存済みの構成と一致させる必要があります。名前とパラメーターが同じでない場合、サイティング検索を実行しても正確な結果が表示されない可能性があります。

注:
Splunk インスタンスで、[検索、レポート、およびアラート (Searches, Reports, and Alerts)] ページに移動し、保存済みの検索クエリを見つけます。[権限 **(Permissions)]** リンクをクリックして [権限 (Permissions)] ページに移動します。[すべてのアプリ **(All Apps)]** ラジオボタンを選択し、[全員 **(Everyone)]** の [読み取り権限 **(Read Permission)]** オプションを有効にします。これにより、保存済みの検索クエリの [共有 (Sharing)] 列の値が [プライベート (Private)] から [アプリ (App)] に変更されます。これが設定されていない場合、保存済みの検索クエリが何も結果を返さない可能性があります。

保存済みの検索構成が Splunk インスタンスで定義した構成と一致するかどうかを確認するには、次の手順を実行します。

1. 次のように移動する。 設定 > 検索、レポート、およびアラート.
2. [アプリコンテキスト] を [すべて] に変更します。

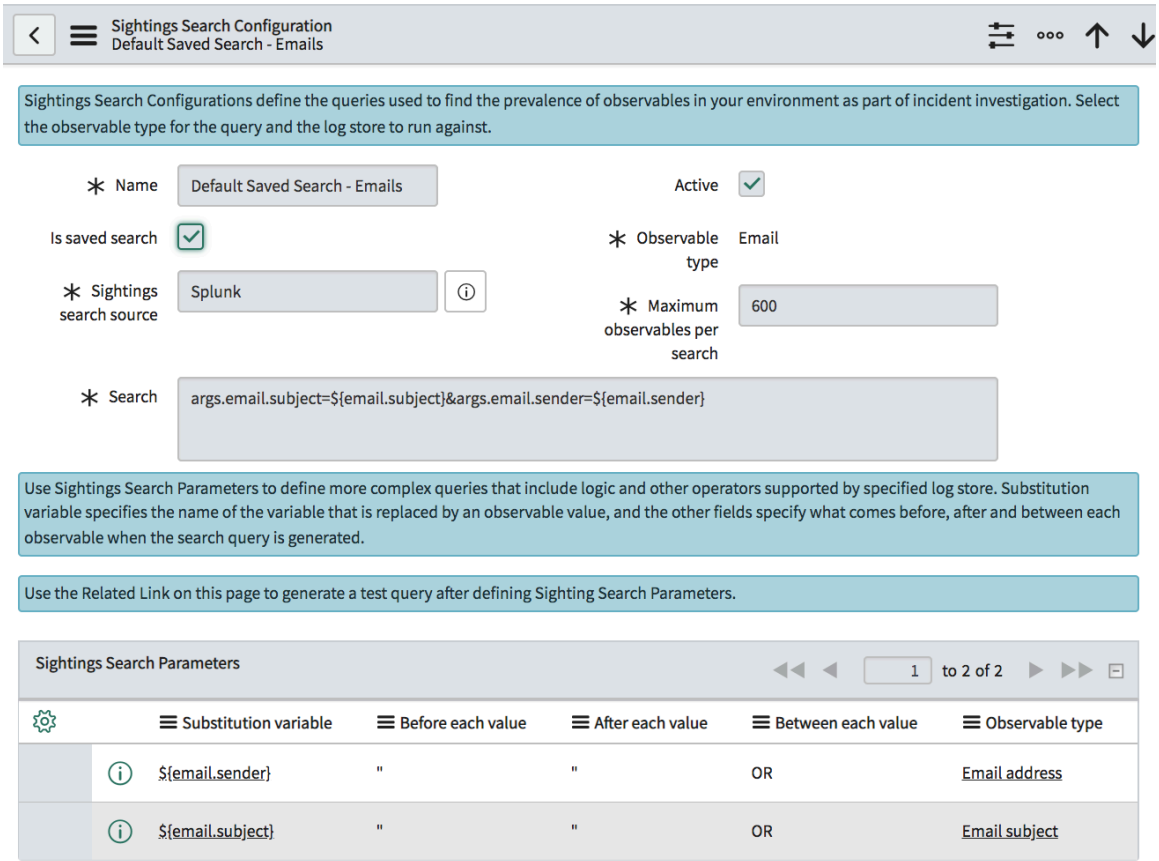
   検索レポートのリストが表示されます。
3. 保存済みの検索クエリがリストに存在することを確認します。

たとえば、[サイティング検索構成] フォームには、メールアドレスとメール送信者が検索パラメーターとして含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[サイティング検索構成] フォーム



Splunk インスタンスで、同じ「Default Saved Search - Emails (デフォルトの保存済みの検索 - メール)」という名前で、同じ検索パラメーター (メールアドレスとメールの件名) の保存済みの検索を定義します。名前と検索パラメーターが同じでない場合、サイティング検索で正確な結果が生成されない可能性があります。

手順

1. 次のように移動する。 セキュリティオペレーション > 統合 > サイティング検索構成 をクリックし、新しいレコードを作成します (フィールドの説明についてはテーブルを参照)。

[サイティング検索構成] フォーム

フィールド	説明
名前	構成の名前。
保存された検索	このオプションを選択すると、保存された検索構成が作成されます。
サイティング検索ソース	サイティング検索のソース。ソースとして Splunk ログストアを選択します。
有効	保存済みの検索ステータスのオプション。サイティング検索に使用できるのは、アクティブな検索構成だけです。
観測可能タイプ	[観測事象タイプ] には、IP、ハッシュ値、URL、ドメイン名などの任意の観測事象タイプを指定できます。
検索あたりの最大観測事象の数	検索から返される観測事象の最大数。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
検索	デフォルトの検索文字列は $(observable) ですが、Splunk ログストアでサポートされているパラメーターを指定することで、独自の検索クエリを定義できます。

2. **[Submit]** をクリックします。

タスクの結果
これでサイティング検索設定レコードを作成できました。

次のタスク
検索クエリを定義した後、[サイティング検索テストクエリを生成] をクリックし、観測事象値のリストを指定して、この保存済みの検索構成に基づいてテストクエリを生成します。

プレイブックリソース

セキュリティインシデントレスポンスには、プレイブック、サブフロー、およびアクションの包括的なライブラリを含む豊富なプレイブックリソースのセットが用意されています。複雑なコードを記述することなく、プレイブックを迅速かつ簡単に作成または構成できます。これらのプレイブックを使用して、ステップバイステップ方式でセキュリティ脅威を解決できます。

プレイブックリソースには次のものが含まれます。

セキュリティインシデントレスポンス Playbook	セキュリティインシデントレスポンスプレイブックアクション
ベースシステムで提供される Playbook は、複雑で日常的なタスクを自動化することで、セキュリティインシデント調査プロセスを迅速化するように設計されています。 Playbook は高度に構成可能であり、ServiceNow の Flow Designer 技術を使用してビルドされています。構成するには、ベースシステムで提供されているプレイブックをコピーし、シンプルなドラッグアンドドロップグラフィカルインターフェイスを使用して変更します。「セキュリティインシデントレスポンス Playbook」を参照してください。	Playbook のビルドに欠かせない複雑なアクションは、アクションライブラリとして利用できます。セキュリティアドミニストレーターは、これらのアクションライブラリを使用して、複雑なコードを記述せずにプレイブックを作成できます。「セキュリティインシデントレスポンスプレイブックアクション」を参照してください。

セキュリティインシデントレスポンス フローのアクティブ化

セキュリティアドミニストレーターとフローデザイナーは セキュリティインシデントレスポンス フローを使用して、組織内のセキュリティインシデントを解決するプロセスを自動化できます。

始める前に
必要なロール：sn_si.admin、action_designer、および flow_designer

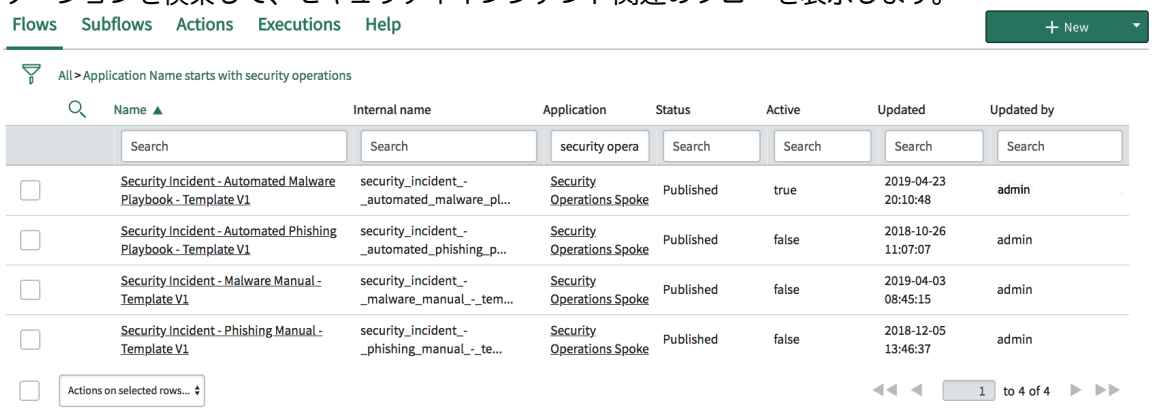
このタスクについて
ベースシステムで提供されるフローは非アクティブ状況です。これらのフローは、使用する前にアクティブ化してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

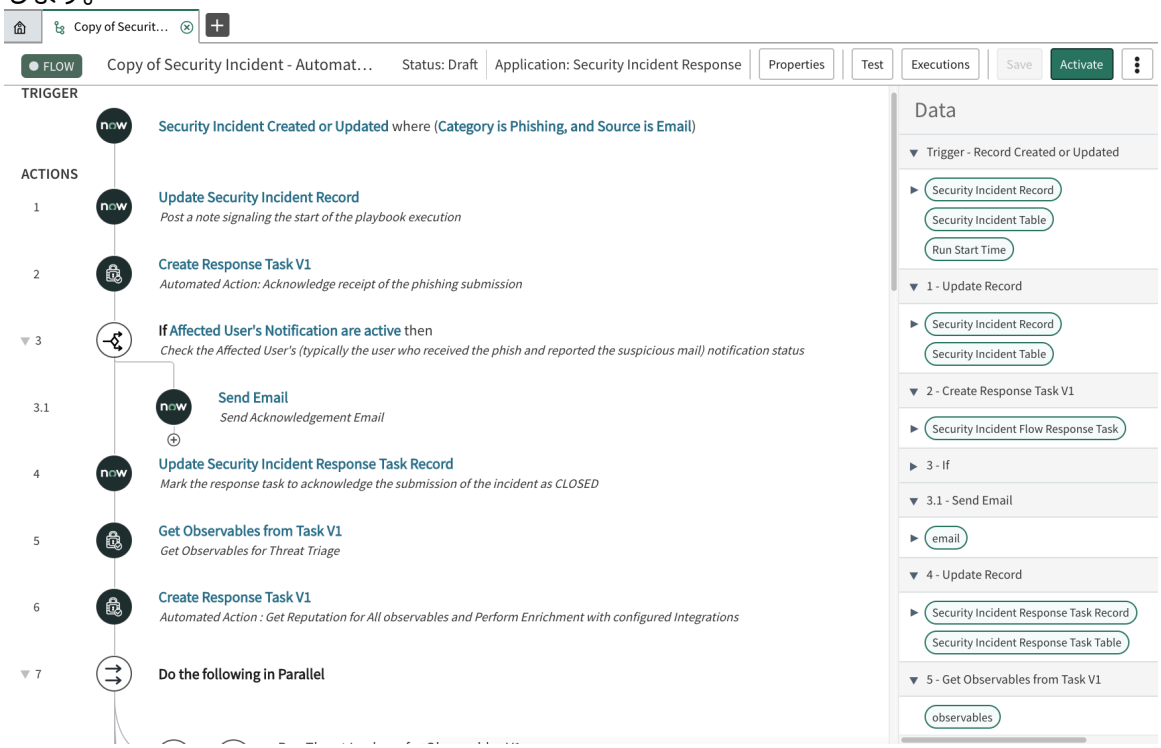
手順

1. セキュリティオペレーション スポークアプリケーションをダウンロードしてインストールします。このスポークアプリケーションでは、セキュリティインシデントレスポンス フローを定義するときに使用できるセキュリティ操作アクションが利用できます。
2. 次のように移動する。 **Flow Designer** > デザイナー セキュリティオペレーション スポークアプリケーションを検索して、セキュリティインシデント関連のフローを表示します。



フローのステータスは公開済みで、非アクティブであることに注意してください。

3. たとえば、自動マルウェアプレイブック フローをアクティブにする場合は、[セキュリティインシデント：自動化フィッシングプレイブック：テンプレート **V1]** リンクをクリックしてフローを表示します。



> **注:**
> ベースシステムで提供されているフローは読み取り専用フローであるため、編集できません。これらのフローをそのまま使用することも、コピーを作成して必要に応じて変更することもできます。

4. [アクティブ化] をクリックして、フローをアクティブ化します。

タスクの結果
自動フィッシングプレイブックフローがアクティブになり、使用する準備ができました。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンス Playbook

セキュリティインシデントのプレイブックフローを自動または手動で呼び出すことができます。

Playbook は、少なくとも 1 つのプレイブックがセキュリティインシデントに関連付けられている場合にのみ表示されます。プレイブックコンポーネントは、プロセスオートメーションデザイナー (PAD) でビルドされたプロセスでのみ機能し、フローデザイナーでビルドされたフローでは機能しません。既存のフローデザイナーが有効になっている場合は引き続き機能し、アクティビティは応答タスクとして引き続きレンダリングされます。

セキュリティインシデントレスポンス は、次の 2 種類のプレイブックをサポートしています。

- プロセスベースのプレイブック
- フローベースのプレイブック

リストされているプレイブックに加えて、Security Operations スポークには、フロープレイブックから呼び出すことができるサブフローもあります。ランサムウェアはそのサブフローの 1 つです。

これらのフローは、使用する前にアクティブ化してください。詳細については、「セキュリティインシデントレスポンスフローのアクティブ化)」を参照してください。

プロセスベースのプレイブック

プレイブックコンポーネントは、ワークフロースタジオでビルドされたプレイブックでのみ機能し、フローでは機能しません。ただし、既存のフローベースのプレイブックは引き続き機能し、アクティビティは応答タスクとして引き続きレンダリングされます。

セキュリティインシデントレスポンス は、ベースシステムで次のプレイブックを提供します。

手動フィッシング用プレイブック

手動フィッシングプレイブックには、フィッシングアクティビティにおける特定のタイプのセキュリティ上の脅威を手動で解決する方法について、アナリスト向けに詳細な手順が記載されています。

概要

手動フィッシングプレイブックテンプレートは、フィッシング応答タスクを手動で実行するように設計されており、トリガー条件を含む一連のアクションが含まれています。PAD テンプレートを使用してフィッシング対策の Playbook の手順を実行し、これらのインシデントを効率的に解決できます。

このプレイブックは、セキュリティインシデントが作成または更新された場合に使用できます。プロセスオートメーションデザイナー (PAD) で手動フィッシングプレイブックを有効にしてから、分析、封じ込め、除去、レビューなどのすべてのタスクを実行する必要があります。

プロセス定義のステージは次のとおりです。セキュリティインシデントのステータスに対応しています。

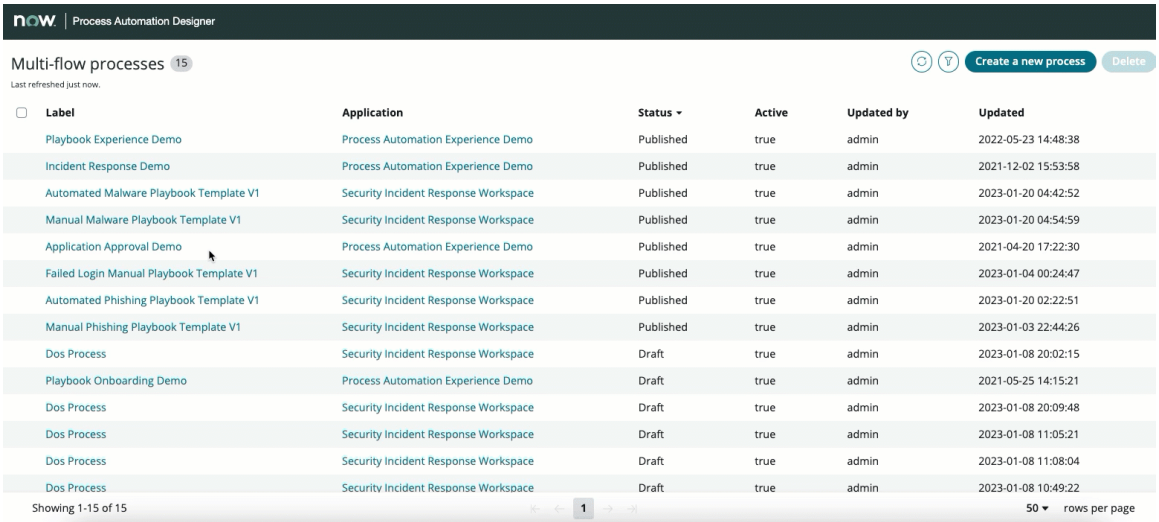
- 分析
- 封じ込め
- 根絶
- レビュー

各ステージにはアクティビティがあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手動フィッシングプレイブック



ステージ内のタスクを完了としてマークすると、次のタスクに移動できます。タスクはいつでも保存でき、後でプレイブックに戻ることができます。ステージ内のすべてのタスクを完了すると、次のステージに進むことができます。タスクとステージを完了していくに伴い、ステータスが左側のパネルに反映されます。プレイブックの右側にあるアクティビティログには、各タスクに入力したすべてのデータが表示されます。

すべてのタスクを完了すると、すべてのステージに入力した詳細を確認するように求められます。任意のフィールドを編集するか、[完了] をクリックしてエンタイトルメントの作成プロセスを完了することができます。

ワークフロースタジオでの手動フィッシングプレイブックの作成

次の手順を従って、ワークフロースタジオで手動フィッシングプレイブックを作成します。

始める前に

必要なロール：sn_si.admin または sn_si.manager

手順

1. クリックします **All** (すべて) > **Process Automation Designer** (プロセスオートメーションデザイナー) > > 新規 をクリックし、[プレイブック] を選択します。

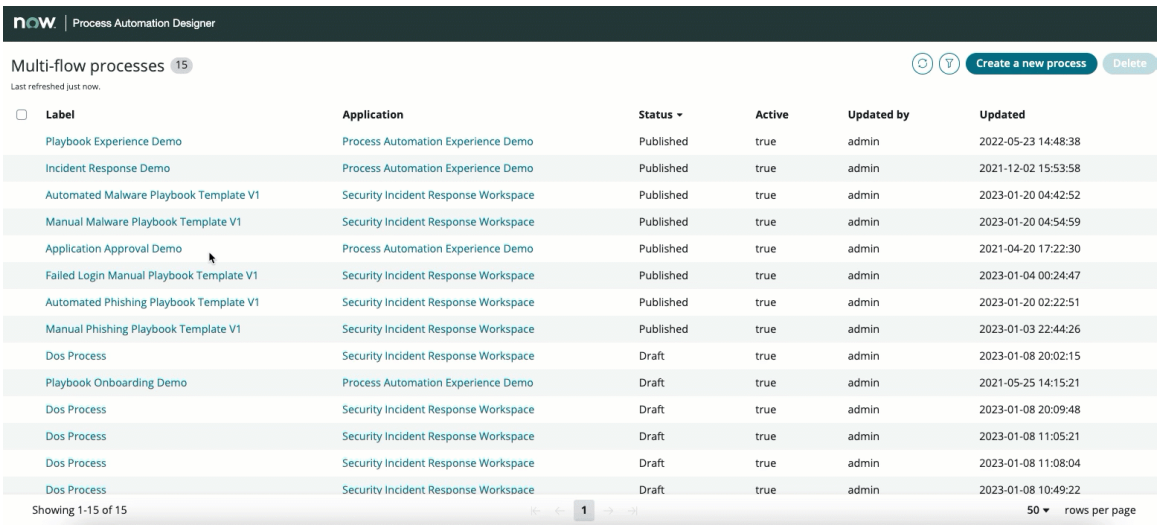
   例：手動フィッシングプレイブックテンプレート V1

2. プレイブックの名前、説明、プレイブックを作成するアプリケーションを入力します。
3. [トリガーを選択] をクリックします。
4. [プロセスを実行する独自の条件を定義します] を選択し、プレイブックを実行するトリガー条件を選択します。
5. [トリガー条件を設定] をクリックします。
6. テーブルを選択して条件を入力することで、プロセスの実行が必要になるタイミングを定義する条件を選択します。
   たとえば、カテゴリ [フィッシング] のセキュリティインシデントが作成されたときをトリガー条件にします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手動フィッシング

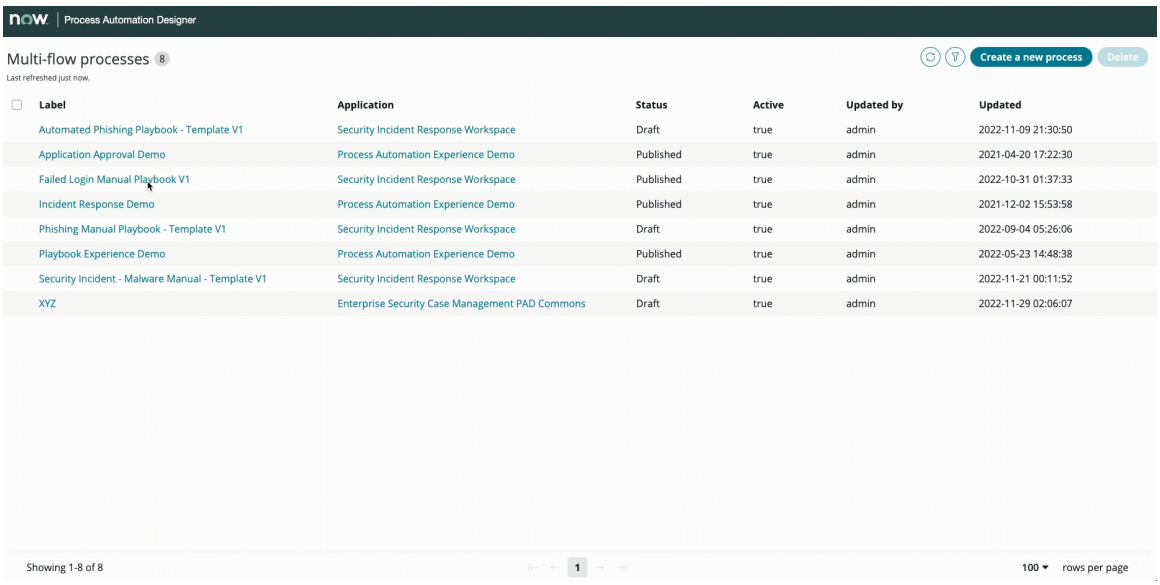


7. [デザイナーに移動] をクリックします。
8. [新しいステージを追加 **(Add a new stage)]** をクリックして、自動プロセスの設計を開始します。ステージのプロパティペインが UI の右側に表示されます。
9. ステージのプロパティペインで、[名前]、[説明]、[実行条件]、および [開始時期を指定 **(Indicate when to start)]** の詳細を入力します。
   [実行条件] および [開始時期を指定 **(Indicate when to start)]** フィールドは、ステージがいつ実行されるかを示します。
10. [保存して閉じる] をクリックします。
11. 別のステージを追加するには、[別のステージを追加 **(Add another stage)]** をクリックします。同様に、必要な数のステージを作成できます。この例では、それぞれ [分析]、[封じ込め]、[除去]、および [レビュー] のステージを作成できます。次の例では、[分析] ステージはすぐに開始され、実行条件はありません。[封じ込め] ステージは前のステージが完了した後に開始され、前のステージのアクティビティの結果に基づく実行条件を持ちます。
    ステージを追加した後、各ステージのプロセスアクティビティを追加する必要があります。
12. 特定のステージ (分析ステージなど) で [別のアクティビティを追加 **(Add another activity)]** をクリックします。
    [アクティビティを追加] ポップアップが開きます。
    a. [アクティビティを追加] ポップアップで、必要なアクティビティ定義を選択します。
13. [新しいアクティビティを作成] をクリックします。
    アクティビティ定義を追加した後、ステージと同様にさらに構成できます。同様に、各ステージの下に他のプロセスアクティビティを作成できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手動フィッシングアクティビティ



14. [アクティビティのプロパティ] ペインで実行条件を追加し、アクティビティを開始するタイミングを指定します。
15. 実行条件を追加し、開始するタイミングを指定します。
このアクティビティに必要なすべての入力 (構成されている自動化プランの入力を含む) が表示されます。値を上書きすることも、事前設定された値を使用することもできます。
16. [すべてのプロパティを表示] をクリックし、[詳細プロパティ] トグルを有効にすると、アクティビティ定義のすべてのアクティビティエクスペリエンスフィールドが表示されます。

並列アクティビティの追加

[開始時期 **(When to Start)]** フィールドが [前と同じ **(With Previous)]** に設定されている場合、並列アクティビティを開始できます。

あるステージから次のステージに移動する場合

実行条件が定義されていない場合、ステージとアクティビティは順番に実行されます。

実行条件を使用することで、アクティビティまたはステージをスキップできます。この例では、「メールに脅威インジケーターはありますか？」の結果が [はい] である場合に [封じ込め] ステージが開始されます。

あるステージから別のステージに移動するには、プラットフォームが提供する [アクティビティ定義 - レコードを更新 **(activity definition – Update Record)]** を使用します。これにより、セキュリティインシデントのステータスフィールドが更新され、次のステージでプレイブックの実行が再開されます。

ただし、このアクティビティ定義の課題は、プレイブックが [分析] ステージにあり、ユーザーがステータスを手動で [レビュー (review)] などに更新した場合、[レコードを更新] アクティビティによってステータスが再度 [封じ込め] に変更され、プレイブックの実行が続行されることです。これにより、手動で行った変更が上書きされます。

これを克服するために、ベースシステムには [タスクステータスを更新] と呼ばれるアクティビティ定義が用意されています。セキュリティの現在のステータスがプレイブックのステージよりも進んでいる場合、このアクティビティはセキュリティインシデント状況を上書きしません。

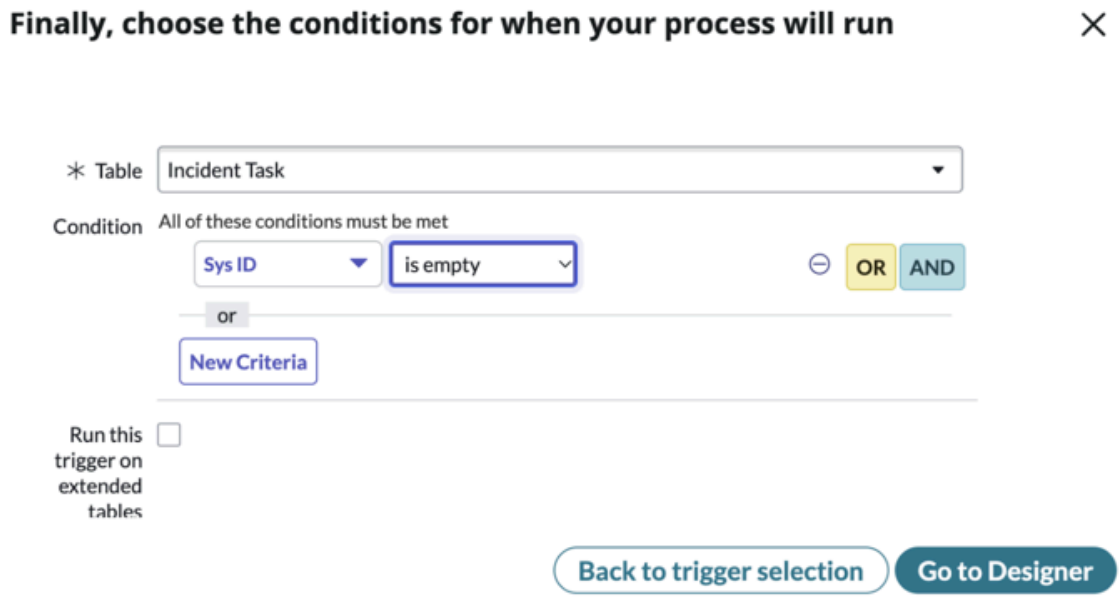
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ダミートリガー条件を使用したプロセス定義の作成

プロセス定義には必ずトリガー条件が必要です。ただし、プロセスをいつトリガーする必要があるかわからない場合は、ダミーのトリガー条件を使用してプロセス定義を作成できます。**[sys_id]** [は空] としてトリガー条件を設定します。この条件が満たされることはありません。

プロセス終了条件



自動翻訳

手動フィッシング プレイブック の使用

次のステップでは、SIR アナリストワークスペースでの手動フィッシングプレイブックの使用方法とその機能について説明します。

始める前に

必要なロール：sn_si.admin、sn_si.manager または sn_si.analyst

手順

1. SIR ワークスペースで、セキュリティインシデントを開きます。
2. **[Playbook]** タブをクリックします。

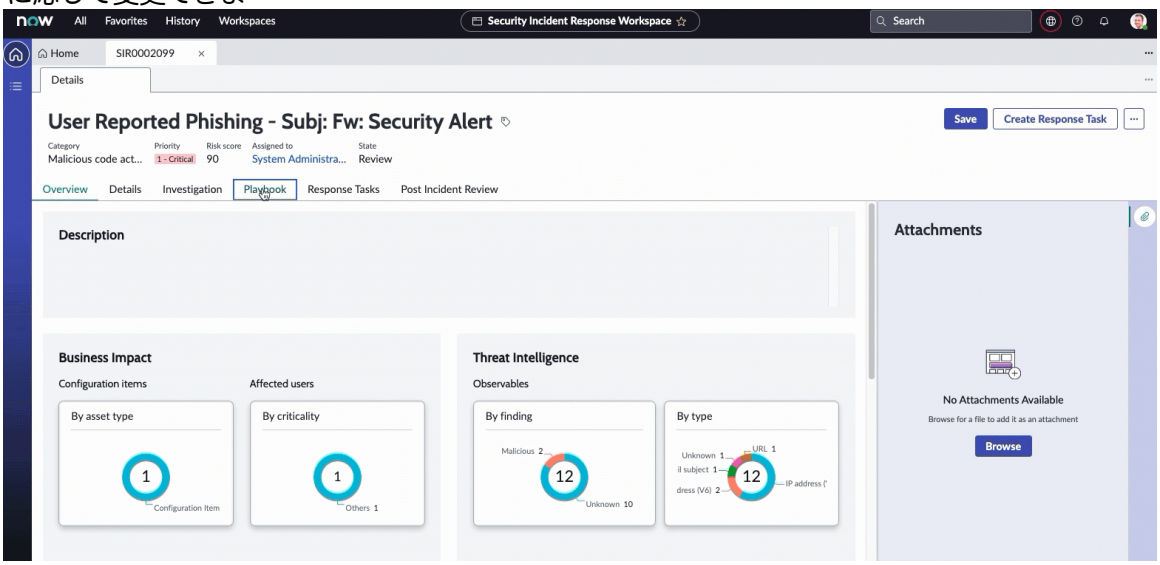
   セキュリティインシデントに対して有効になっているプレイブックを表示できます。セキュリティインシデントのカテゴリ、リスクスコアなどの詳細を表示することもできます。

   > **注:**
   > プレイブックがリストに表示されない場合は、PAD に移動して **[Playbook]** タブで表示できるようにする必要があります。

3. [手動フィッシングプレイブック] をクリックします。
4. 各ステージをクリックして、このプレイブックによって実行されたタスクを確認します。
5. [分析] をクリックすると、[分析] フェーズで実行されたアクティビティのリストが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

要件に応じて変更できま



す。

6. 同様に、[封じ込め]、 [除去]、および [レビュー] をクリックして、それぞれのフェーズで実行されたアクティビティのリストを表示できます。
要件に応じて変更できます。実行する必要があるアクティビティまたはユーザーアクションが残っている場合は、それぞれのフェーズに表示されます。
7. いずれかのフェーズで必要な残りのアクティビティまたはユーザーアクションがある場合は、それぞれのフェーズをクリックし、アクションを実行してアクティビティを完了します。

ワークスペースプレイブックサマリー

以下で、エンドポイントのプロセスフローについて説明します。

- 従来のフローベースの プレイブックを理解します。
- フローを分析した後、考えられるアクティビティとステージを一覧表示します。真のオーケストレーションを作成できるステップを探します。
- 各アクティビティを取得し、ベースシステム提供のアクティビティ定義がユースケースを満たすことができるかどうかを確認します。
- 新しいアクティビティ定義を実装する必要があるダウンアクティビティユースケースをリストします。インタラクティブ、非インタラクティブ、または自動に分類します。アクティビティ定義を作成するには
  - ユースケースのサブフローまたはアクションを作成します。
  - 関連データをフローデータテーブルまたはカスタムテーブルのどちらでキャプチャする必要があるかを決定します。
  - フローデータテーブルを使用する場合は、**sys_flow_data_definition** にフローデータ定義を作成します。サブフローでフローデータレコードを作成するときに、作成されたフローデータ定義を選択します。
  - アクティビティ定義を作成します。
  - 自動化プランをマッピングします。
  - アクティビティエクスペリエンスのプロパティを入力します。
  - [プレイブックアクション] の下にアクションを作成します。アクティビティ定義にアサインする既存のアクティビティアクションが必要です。
  - 選択したエクスペリエンスタイプに基づいてデフォルトのカードエクスペリエンスを上書きするには、アクティビティ UI のコンセプトを使用して Playbook の上書きを追加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 一部のアクティビティは、サブフローで [ユーザー入力待ち] フラグを使用して、自動とインタラクティブの両方を処理するように作成できます。この入力は、プロセス定義でアクティビティを構成するときに渡すことができます。
- プロセスに必要なすべてのアクティビティ定義を用意したら、ワークフロースタジオを使用してプロセス定義の構築を開始します。

自動フィッシングプレイブック

自動フィッシングプレイブックには、自動フィッシングアクティビティで特定のタイプのセキュリティ上の脅威を解決する方法について、アナリスト向けに詳細な手順が記載されています。

概要

自動フィッシングプレイブックテンプレートは、フィッシング応答タスクを自動で実行するように設計されており、トリガー条件などの一連のアクションを含んでいます。ワークフロースタジオでテンプレートを使用してフィッシング応答プレイブックの手順を自動化し、これらのインシデントを効率的に解決できます。このプレイブックテンプレートには、フィッシング攻撃に対応するように設計された一連の再利用可能なアクションが含まれています。各フローには、注釈を付けることができるトリガー (条件)、一連のアクション、およびサブフローがあります。

このプレイブックでは、セキュリティインシデントのカテゴリがフィッシングに設定されている場合、ユーザーインタラクションはありません。このプレイブックは、セキュリティインシデントが作成または更新された場合に使用できます。ワークフロースタジオで自動フィッシングプレイブックを有効にすると、このプレイブックで分析、封じ込め、除去、レビューなどのすべてのタスクが自動的に実行されます。

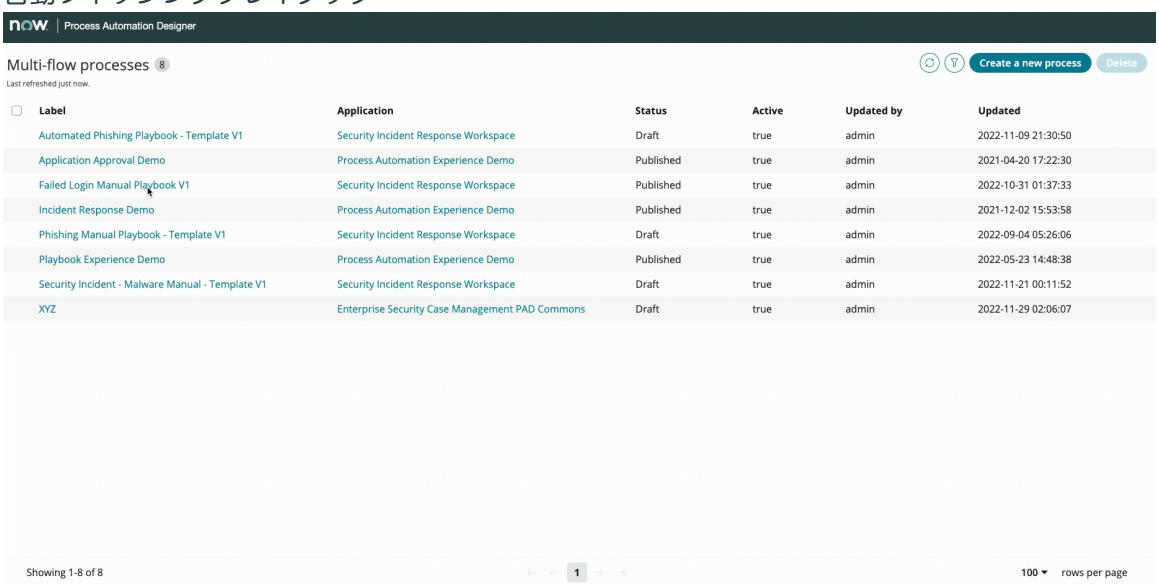
プロセス定義のステージは次のとおりです。セキュリティインシデントのステータスに対応しています。

- 分析
- 封じ込め
- 根絶
- レビュー

各ステージにはアクティビティがあります。

自動翻訳

自動フィッシングプレイブック



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ステージ内のタスクを完了としてマークすると、次のタスクに移動できます。タスクはいつでも保存でき、後でプレイブックに戻ることができます。ステージ内のすべてのタスクを完了すると、次のステージに進むことができます。タスクとステージを完了していくに伴い、ステータスが左側のパネルに反映されます。プレイブックの右側にあるアクティビティログには、各タスクに入力したすべてのデータが表示されます。

すべてのタスクを完了すると、すべてのステージに入力した詳細を確認するように求められます。任意のフィールドを編集するか、[完了] をクリックしてエンタイトルメントの作成プロセスを完了することができます。

PAD での自動フィッシングのプロセスの作成

プロセスオートメーションデザイナー (PAD) で自動フィッシングのプロセスを作成するには、次のステップに従います。

始める前に

必要なロール：sn_si.admin または sn_si.manager

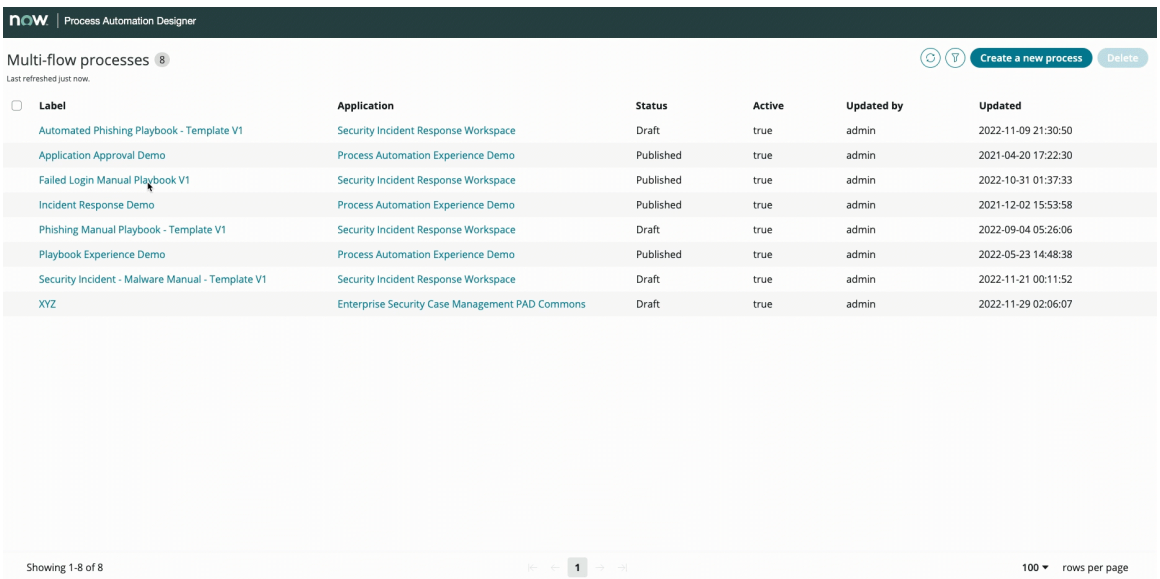
手順

1. クリックします すべて > **Process Automation Designer** (プロセスオートメーションデザイナー) > > 新しいプロセスを作成する.

   例：自動フィッシングプレイブックテンプレート V1

2. プロセスの名前、説明、およびプロセスを作成するアプリケーションを入力します。
3. [トリガーを選択] をクリックします。
4. [プロセスを実行する独自の条件を定義します] を選択し、プロセスを実行する必要があるタイミングに関するトリガー条件を選択します。
5. [トリガー条件を設定] をクリックします。
6. テーブルを選択して条件を入力することで、プロセスを実行する必要があるタイミングを定義する条件を選択します。
   たとえば、カテゴリ [フィッシング] のセキュリティインシデントが作成されたときをトリガー条件にします。

自動フィッシングプレイブック



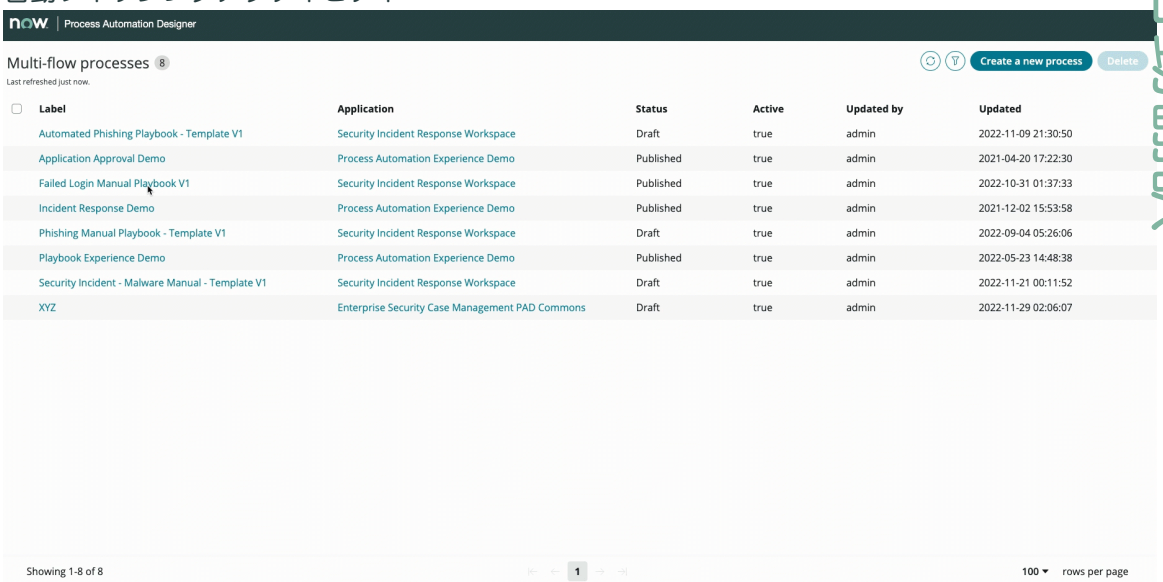
7. [デザイナーに移動] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[プロセスオートメーションデザイナー] ページが開きます。

8. [新しいステージを追加 **(Add a new stage)]** をクリックして、自動プロセスの設計を開始します。
ステージのプロパティペインが UI の右側に表示されます。
9. ステージのプロパティペインで、[名前]、[説明]、[実行条件]、および [開始時期を指定 **(Indicate when to start)]** の詳細を入力します。
[実行条件] および [開始時期を指定 **(Indicate when to start)]** フィールドは、ステージがいつ実行されるかを示します。
10. [保存して閉じる] をクリックします。
11. 別のステージを追加するには、[別のステージを追加 **(Add another stage)]** をクリックします。
同様に、必要な数のステージを作成できます。この例では、それぞれ [分析]、[封じ込め]、[除去]、および [レビュー] のステージを作成できます。次の例では、[分析] ステージはすぐに開始され、実行条件はありません。[封じ込め] ステージは前のステージが完了した後に開始され、前のステージのアクティビティの結果に基づく実行条件を持ちます。
ステージを追加した後、各ステージのプロセスアクティビティを追加する必要があります。
12. 特定のステージ (分析ステージなど) で [別のプロセスアクティビティを追加] をクリックします。
[アクティビティを追加] ポップアップが開きます。
    a. [アクティビティを追加] ポップアップで、必要なアクティビティ定義を選択します。
13. [新しいアクティビティを作成] をクリックします。
アクティビティ定義を追加した後、ステージと同様にさらに構成できます。同様に、各ステージの下に他のプロセスアクティビティを作成できます。

自動フィッシングアクティビティ



14. [アクティビティのプロパティ] ペインで実行条件を追加し、プロセスアクティビティを開始するタイミングを指定します。
15. 実行条件を追加し、開始するタイミングを指定します。
このアクティビティに必要なすべての入力 (構成されている自動化プランの入力を含む) が表示されます。値を上書きすることも、事前設定された値を使用することもできます。
16. [すべてのプロパティを表示] をクリックし、[詳細プロパティ] トグルを有効にすると、アクティビティ定義のすべてのアクティビティエクスペリエンスフィールドが表示されます。

自動フィッシングプレイブック 使用

次のステップでは、SIR アナリストワークスペースでの自動フィッシングプレイブックの使用方法とその機能について説明します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_si.admin、sn_si.manager または sn_si.analyst

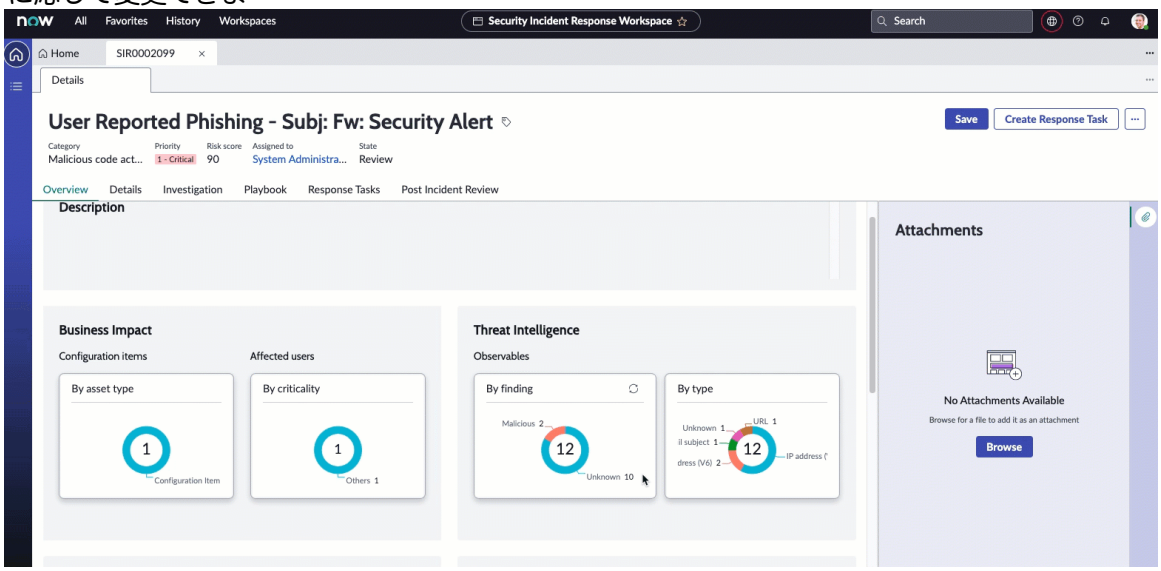
手順

1. SIR ワークスペースで、セキュリティインシデントを開きます。
2. **[Playbook]** タブをクリックします。

   セキュリティインシデントに対して有効になっているプレイブックを表示できます。セキュリティインシデントのカテゴリ、リスクスコアなどの詳細を表示することもできます。

   > 注:
   > プレイブックがリストに表示されない場合は、PAD に移動して **[Playbook]** タブで表示できるようにする必要があります。

3. [自動フィッシングプレイブック] をクリックします。
   自動フィッシングの場合、セキュリティインシデントに対してタスクが自動的に実行されます。
4. 各ステージをクリックして、このプレイブックによって実行されたタスクを確認します。
5. [分析] をクリックすると、[分析] フェーズで実行されたアクティビティのリストが表示されます。
   要件に応じて変更できま



す。

6. 同様に、[封じ込め]、 [除去]、および [レビュー] をクリックして、それぞれのフェーズで実行されたアクティビティのリストを表示できます。
   要件に応じて変更できます。実行する必要があるアクティビティまたはユーザーアクションが残っている場合は、それぞれのフェーズに表示されます。
7. いずれかのフェーズで必要な残りのアクティビティまたはユーザーアクションがある場合は、それぞれのフェーズをクリックし、アクションを実行してアクティビティを完了します。

手動マルウェアプレイブック

手動マルウェアプレイブックには、アナリストが手動でより効率的にマルウェアアラートを解決する方法についての詳細な手順が記載されています。

手動マルウェアプレイブック テンプレートは、エンドポイントまたはネットワークからのマルウェアアラートの処理に関連する手順を手動で実行するように設計されています。ワークフロースタジオでプレイブックテンプレートを使用して手動マルウェアプレイブックの手順を実行し、これらのアラートを効率的に解決できます。このプレイブックには、注釈を付けることができるトリガー (条件)、一連のアクション、およびサブフローがあります。このプレイブックには、マルウェア攻撃に

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

対応するように設計された一連の再利用可能なアクションが含まれています。各フローには、注釈に対するトリガー (条件)、一連のアクション、およびサブフローがあります。

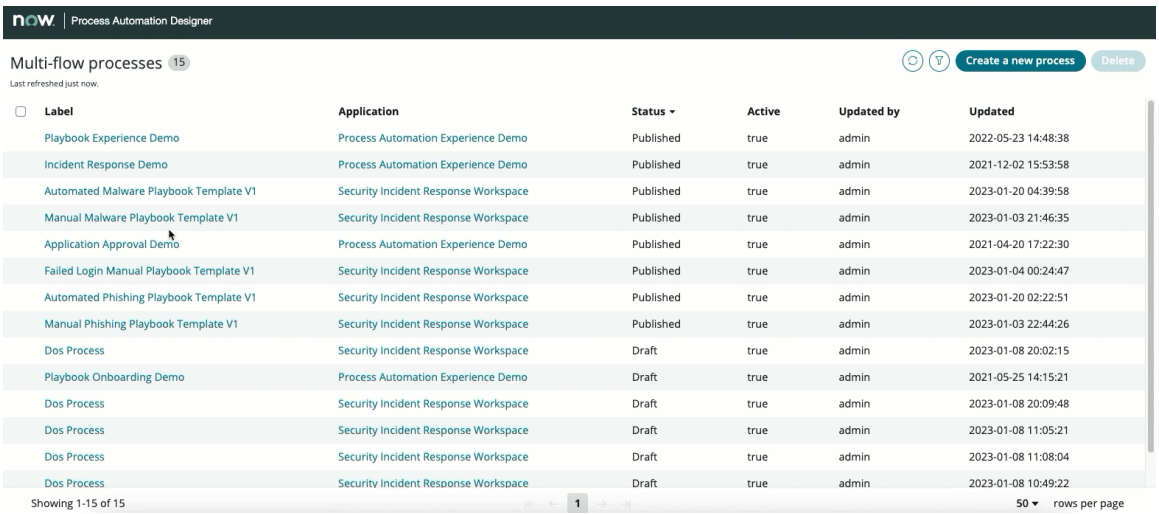
このプレイブックは、マルウェアが作成または更新された場合に使用できます。ワークフロースタジオで手動マルウェアプレイブックを有効にしてから、分析、封じ込め、除去、レビューなどのすべてのタスクを作成する必要があります。

プロセス定義のステージは次のとおりです。マルウェアアラートのステータスに対応しています。

- 分析
- 封じ込め
- 根絶
- レビュー

各ステージにはアクティビティがあります。

手動マルウェアプレイブック



ステージ内のタスクを完了としてマークすると、次のタスクに移動できます。タスクはいつでも保存でき、後でプレイブックに戻ることができます。ステージ内のすべてのタスクを完了すると、次のステージに進むことができます。タスクとステージを完了していくに伴い、ステータスが左側のパネルに反映されます。プレイブックの右側にあるアクティビティログには、各タスクに入力したすべてのデータが表示されます。

すべてのタスクを完了すると、すべてのステージに入力した詳細を確認するように求められます。任意のフィールドを編集するか、[完了] をクリックしてエンタイトルメントの作成プロセスを完了することができます。

PAD での手動マルウェアのプロセスの作成

プロセスオートメーションデザイナー (PAD) で手動マルウェアのプロセスを作成するには、次のステップに従います。

始める前に
必要なロール：sn_si.admin または sn_si.manager

手順

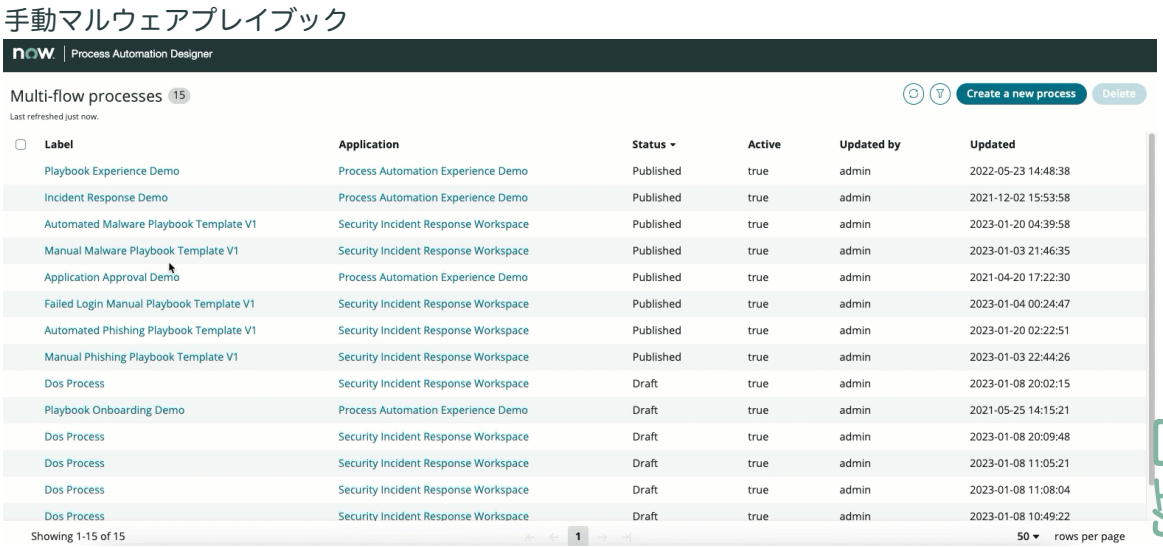
1. クリックします すべて > **Process Automation Designer** (プロセスオートメーションデザイナー) > > 新しいプロセスを作成する.

   例：手動マルウェアプレイブック テンプレート V1

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

2. プロセスの名前、説明、およびプロセスを作成するアプリケーションを入力します。
3. [トリガーを選択] をクリックします。
4. [プロセスを実行する独自の条件を定義します] を選択し、プロセスを実行する必要があるタイミングに関するトリガー条件を選択します。
5. [トリガー条件を設定] をクリックします。
6. テーブルを選択して条件を入力することで、プロセスを実行する必要があるタイミングを定義する条件を選択します。
   たとえば、カテゴリ [フィッシング] のセキュリティインシデントが作成されたときをトリガー条件にします。

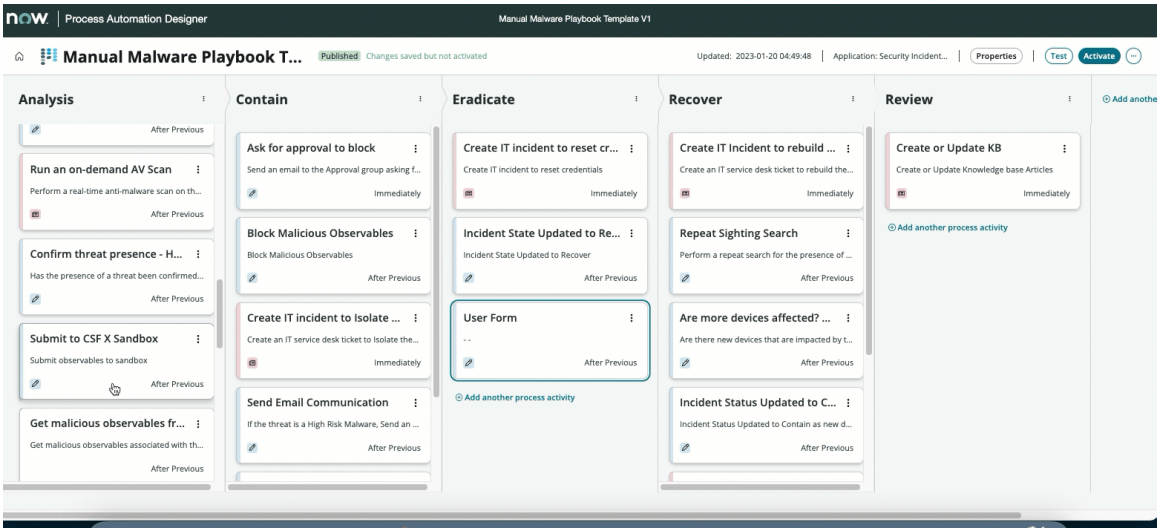


7. [デザイナーに移動] をクリックします。
   [プロセスオートメーションデザイナー] ページが開きます。
8. [新しいステージを追加 **(Add a new stage)**] をクリックして、自動プロセスの設計を開始します。
   ステージのプロパティペインが UI の右側に表示されます。
9. ステージのプロパティペインで、[名前]、[説明]、[実行条件]、および [開始時期を指定 **(Indicate when to start)**] の詳細を入力します。
   [実行条件] および [開始時期を指定 **(Indicate when to start)**] フィールドは、ステージがいつ実行されるかを示します。
10. [保存して閉じる] をクリックします。
11. 別のステージを追加するには、[別のステージを追加 **(Add another stage)**] をクリックします。
    同様に、必要な数のステージを作成できます。この例では、それぞれ [分析]、[封じ込め]、[除去]、および [レビュー] のステージを作成できます。次の例では、[分析] ステージはすぐに開始され、実行条件はありません。[封じ込め] ステージは前のステージが完了した後に開始され、前のステージのアクティビティの結果に基づく実行条件を持ちます。
    ステージを追加した後、各ステージのプロセスアクティビティを追加する必要があります。
12. 特定のステージ (分析ステージなど) で [別のプロセスアクティビティを追加] をクリックします。
    [アクティビティを追加] ポップアップが開きます。
    a. [アクティビティを追加] ポップアップで、必要なアクティビティ定義を選択します。
13. [新しいアクティビティを作成] をクリックします。
    アクティビティ定義を追加した後、ステージと同様にさらに構成できます。同様に、各ステージの下に他のプロセスアクティビティを作成できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手動マルウェアアクティビティ



14. [アクティビティのプロパティ] ペインで実行条件を追加し、プロセスアクティビティを開始するタイミングを指定します。
15. 実行条件を追加し、開始するタイミングを指定します。
このアクティビティに必要なすべての入力 (構成されている自動化プランの入力を含む) が表示されます。値を上書きすることも、事前設定された値を使用することもできます。
16. [すべてのプロパティを表示] をクリックし、[詳細プロパティ] トグルを有効にすると、アクティビティ定義のすべてのアクティビティエクスペリエンスフィールドが表示されます。

手動マルウェアプレイブック の使用

次のステップでは、SIR アナリストワークスペースでの手動マルウェアプレイブック の使用方法とその機能について説明します。

始める前に

必要なロール：sn_si.admin、sn_si.manager または sn_si.analyst

手順

1. SIR ワークスペースで、セキュリティインシデントを開きます。
2. **[Playbook]** タブをクリックします。

   セキュリティインシデントに対して有効になっているプレイブックを表示できます。セキュリティインシデントのカテゴリ、リスクスコアなどの詳細を表示することもできます。

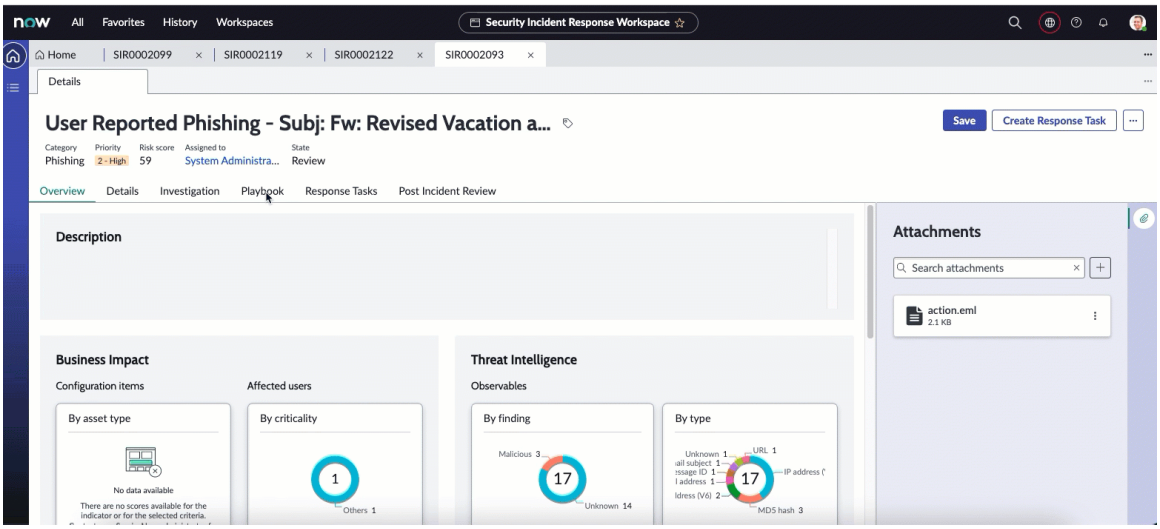
   > **注:**
   > プレイブックがリストに表示されない場合は、PAD に移動して **[Playbook]** タブで表示できるようにする必要があります。

3. [手動マルウェアプレイブック **(Manual Malware Playbook)]** をクリックします。
手動マルウェアの場合、セキュリティインシデントに対してタスクが自動的に実行されます。
4. 各ステージをクリックして、このプレイブックによって実行されたタスクを確認します。
5. [分析] をクリックすると、[分析] フェーズで実行されたアクティビティのリストが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

要件に応じて変更できま



す。

6. 同様に、[封じ込め]、 [除去]、および [レビュー] をクリックして、それぞれのフェーズで実行されたアクティビティのリストを表示できます。
   要件に応じて変更できます。実行する必要があるアクティビティまたはユーザーアクションが残っている場合は、それぞれのフェーズに表示されます。
7. いずれかのフェーズで必要な残りのアクティビティまたはユーザーアクションがある場合は、それぞれのフェーズをクリックし、アクションを実行してアクティビティを完了します。

自動マルウェアプレイブック

自動マルウェアプレイブックには、アナリストがより効率的にマルウェアアラートを解決するのに役立つ一連の自動化された手順が記載されています。

自動マルウェアプレイブック テンプレートは、エンドポイントまたはネットワークからのマルウェアアラートの処理に関連する手順を自動化するように設計されています。ワークフロースタジオでテンプレートを使用して自動マルウェアプレイブック の手順を自動化し、これらのアラートを効率的に解決できます。このプレイブックには、注釈を付けることができるトリガー (条件)、一連のアクション、およびサブフローがあります。このプレイブックには、マルウェア攻撃に対応するように設計された一連の再利用可能なアクションが含まれています。各フローには、注釈に対するトリガー (条件)、一連のアクション、およびサブフローがあります。

このプレイブックは、セキュリティインシデントが作成または更新された場合に使用できます。ワークフロースタジオで自動マルウェアプレイブックを有効にすると、このプレイブックで分析、封じ込め、除去、レビューなどのすべてのタスクが自動的に実行されます。

プロセス定義のステージは次のとおりです。セキュリティインシデントのステータスに対応しています。

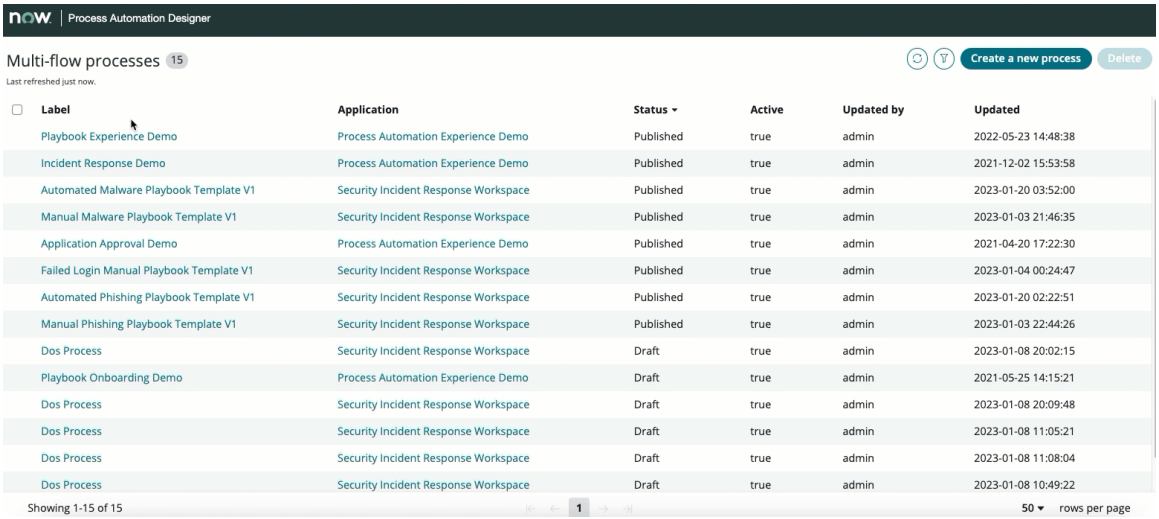
- 分析
- 封じ込め
- 根絶
- レビュー

各ステージにはアクティビティがあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動マルウェアプレイブック



ステージ内のタスクを完了としてマークすると、次のタスクに移動できます。タスクはいつでも保存でき、後でプレイブックに戻ることができます。ステージ内のすべてのタスクを完了すると、次のステージに進むことができます。タスクとステージを完了していくに伴い、ステータスが左側のパネルに反映されます。プレイブックの右側にあるアクティビティログには、各タスクに入力したすべてのデータが表示されます。

すべてのタスクを完了すると、すべてのステージに入力した詳細を確認するように求められます。任意のフィールドを編集するか、[完了] をクリックしてエンタイトルメントの作成プロセスを完了することができます。

PAD での自動マルウェアのプロセスの作成

プロセスオートメーションデザイナー (PAD) で自動マルウェアのプロセスを作成するには、次のステップに従います。

始める前に

必要なロール：sn_si.admin または sn_si.manager

手順

1. クリックします すべて > **Process Automation Designer** (プロセスオートメーションデザイナー) > > 新しいプロセスを作成する.

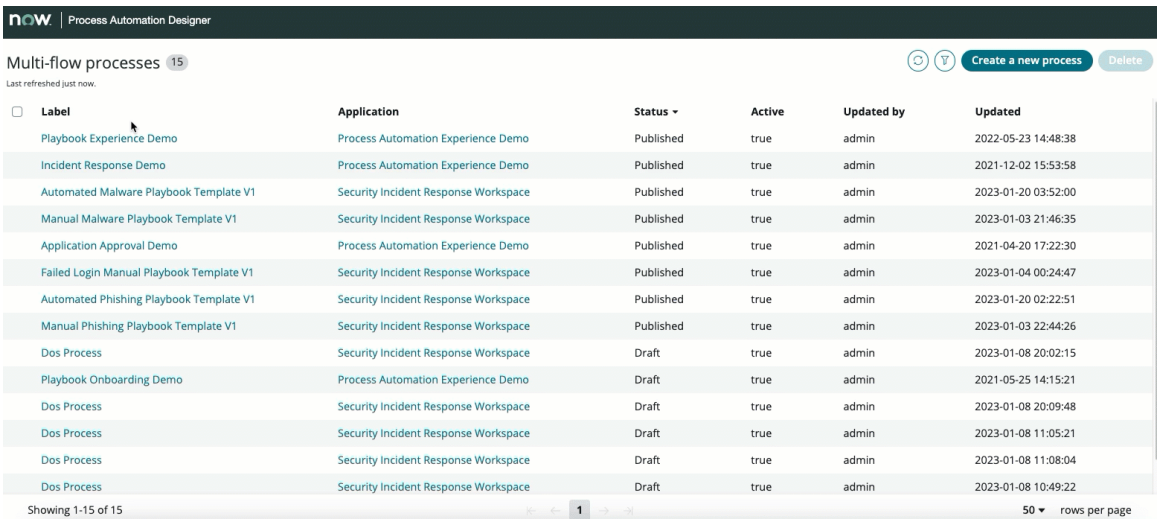
   例：自動マルウェアプレイブック テンプレート V1

2. プロセスの名前、説明、およびプロセスを作成するアプリケーションを入力します。
3. [トリガーを選択] をクリックします。
4. [プロセスを実行する独自の条件を定義します] を選択し、プロセスを実行する必要があるタイミングに関するトリガー条件を選択します。
5. [トリガー条件を設定] をクリックします。
6. テーブルを選択して条件を入力することで、プロセスを実行する必要があるタイミングを定義する条件を選択します。
   たとえば、カテゴリ [フィッシング] のセキュリティインシデントが作成されたときをトリガー条件にします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

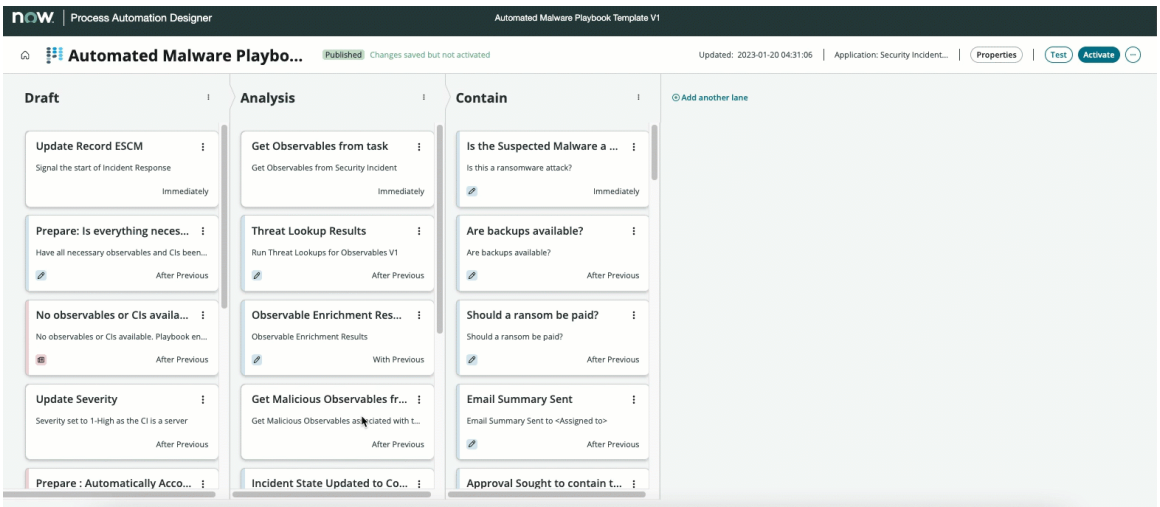
自動マルウェアプレイブック



7. [デザイナーに移動] をクリックします。
   [プロセスオートメーションデザイナー] ページが開きます。
8. [新しいステージを追加 **(Add a new stage)]** をクリックして、自動プロセスの設計を開始します。
   ステージのプロパティペインが UI の右側に表示されます。
9. ステージのプロパティペインで、[名前]、[説明]、[実行条件]、および [開始時期を指定 **(Indicate when to start)]** の詳細を入力します。
   [実行条件] および [開始時期を指定 **(Indicate when to start)]** フィールドは、ステージがいつ実行されるかを示します。
10. [保存して閉じる] をクリックします。
11. 別のステージを追加するには、[別のステージを追加 **(Add another stage)]** をクリックします。
    同様に、必要な数のステージを作成できます。この例では、それぞれ [分析]、[封じ込め]、[除去]、および [レビュー] のステージを作成できます。次の例では、[分析] ステージはすぐに開始され、実行条件はありません。[封じ込め] ステージは前のステージが完了した後に開始され、前のステージのアクティビティの結果に基づく実行条件を持ちます。
    ステージを追加した後、各ステージのプロセスアクティビティを追加する必要があります。
12. 特定のステージ (分析ステージなど) で [別のプロセスアクティビティを追加] をクリックします。
    [アクティビティを追加] ポップアップが開きます。
    a. [アクティビティを追加] ポップアップで、必要なアクティビティ定義を選択します。
13. [新しいアクティビティを作成] をクリックします。
    アクティビティ定義を追加した後、ステージと同様にさらに構成できます。同様に、各ステージの下に他のプロセスアクティビティを作成できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動マルウェアアクティビティ



14. [アクティビティのプロパティ] ペインで実行条件を追加し、プロセスアクティビティを開始するタイミングを指定します。
15. 実行条件を追加し、開始するタイミングを指定します。
このアクティビティに必要なすべての入力 (構成されている自動化プランの入力を含む) が表示されます。値を上書きすることも、事前設定された値を使用することもできます。
16. [すべてのプロパティを表示] をクリックし、[詳細プロパティ] トグルを有効にすると、アクティビティ定義のすべてのアクティビティエクスペリエンスフィールドが表示されます。

自動マルウェアプレイブック の使用

次のステップでは、SIR アナリストワークスペースでの自動マルウェアプレイブック の使用方法とその機能について説明します。

始める前に

必要なロール：sn_si.admin、sn_si.manager または sn_si.analyst

手順

1. SIR ワークスペースで、セキュリティインシデントを開きます。
2. **[Playbook]** タブをクリックします。

   セキュリティインシデントに対して有効になっているプレイブックを表示できます。セキュリティインシデントのカテゴリ、リスクスコアなどの詳細を表示することもできます。

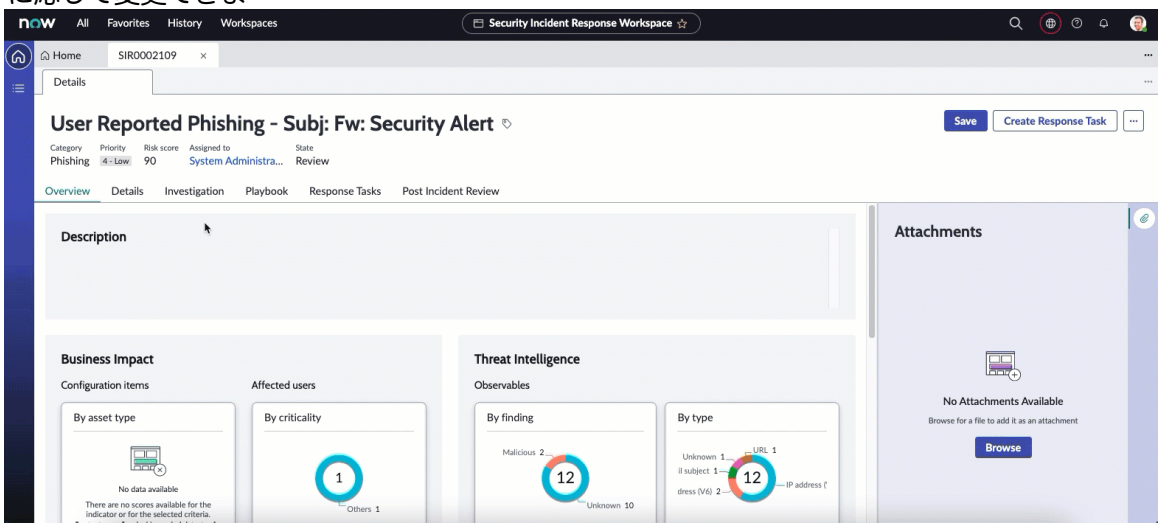
   > **注:**
   > プレイブックがリストに表示されない場合は、PAD に移動して [プレイブック] タブで表示できるようにする必要があります。

3. [自動マルウェアプレイブック **(Automated Malware Playbook)]** をクリックします。
自動マルウェアの場合、セキュリティインシデントに対してタスクが自動的に実行されます。
4. 各ステージをクリックして、このプレイブックによって実行されたタスクを確認します。
5. [分析] をクリックすると、[分析] フェーズで実行されたアクティビティのリストが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

要件に応じて変更できま



す。

6. 同様に、[封じ込め]、 [除去]、および [レビュー] をクリックして、それぞれのフェーズで実行されたアクティビティのリストを表示できます。
   要件に応じて変更できます。実行する必要があるアクティビティまたはユーザーアクションが残っている場合は、それぞれのフェーズに表示されます。
7. いずれかのフェーズで必要な残りのアクティビティまたはユーザーアクションがある場合は、それぞれのフェーズをクリックし、アクションを実行してアクティビティを完了します。

ログイン失敗手動プレイブック

ログイン失敗手動プレイブックはログイン失敗セキュリティインシデントを調査する上でのガイドとなり、調査の最適化にも役立ちます。

ユーザーが (SIM 構成に従って) 一定回数ログインに失敗すると、セキュリティインシデントが作成されます。これらの失敗したログイン試行は、誤検出であるか、ユーザーのメールアカウントへのアクセスを取得しようとする攻撃者の試みである可能性があります。

ワークフロースタジオでプレイブックテンプレートを使用して、ログイン失敗プレイブックの手順を実行することで、ログイン失敗セキュリティインシデントを効率的に解決できます。このプレイブックには、注釈を付けることができるトリガー (条件)、一連のアクション、およびサブフローがあります。このプレイブックには、ログイン失敗セキュリティインシデントに対応するように設計された一連の再利用可能なアクションが含まれています。各フローには、注釈に対するトリガー (条件)、一連のアクション、およびサブフローがあります。

このプレイブックは、ログイン失敗セキュリティインシデントが作成または更新された場合に使用できます。ワークフロースタジオでログイン失敗手動プレイブックを有効にしてから、分析、封じ込め、除去、レビューなどのすべてのタスクを作成する必要があります。

プロセス定義のステージは次のとおりです。セキュリティインシデントのステータスに対応しています。

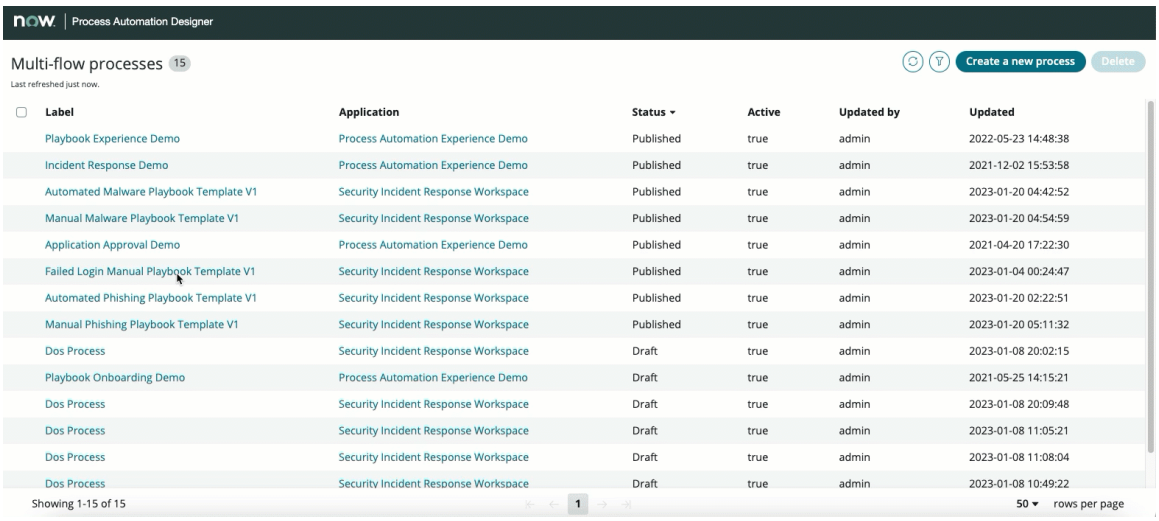
- 分析
- 封じ込め
- 根絶
- レビュー

各ステージにはアクティビティがあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログイン失敗手動プレイブック



ステージ内のタスクを完了としてマークすると、次のタスクに移動できます。タスクはいつでも保存でき、後でプレイブックに戻ることができます。ステージ内のすべてのタスクを完了すると、次のステージに進むことができます。タスクとステージを完了していくに伴い、ステータスが左側のパネルに反映されます。プレイブックの右側にあるアクティビティログには、各タスクに入力したすべてのデータが表示されます。

すべてのタスクを完了すると、すべてのステージに入力した詳細を確認するように求められます。任意のフィールドを編集するか、[完了] をクリックしてエンタイトルメントの作成プロセスを完了することができます。

PAD でのログイン失敗手動プロセスの作成

プロセスオートメーションデザイナー (PAD) でログイン失敗手動プロセスを作成するには、次のステップに従います。

始める前に

必要なロール：sn_si.admin または sn_si.manager

手順

1. クリックします すべて > **Process Automation Designer** (プロセスオートメーションデザイナー) > > 新しいプロセスを作成する.

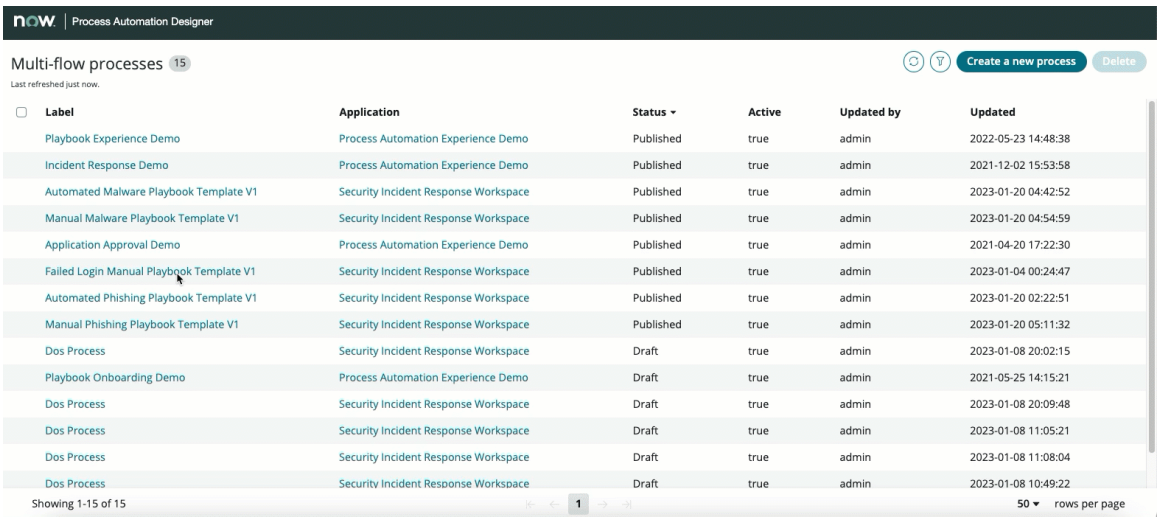
   例：ログイン失敗手動プレイブックテンプレート V1

2. プロセスの名前、説明、およびプロセスを作成するアプリケーションを入力します。
3. [トリガーを選択] をクリックします。
4. [プロセスを実行する独自の条件を定義します] を選択し、プロセスを実行する必要があるタイミングに関するトリガー条件を選択します。
5. [トリガー条件を設定] をクリックします。
6. テーブルを選択して条件を入力することで、プロセスを実行する必要があるタイミングを定義する条件を選択します。
   たとえば、カテゴリ [フィッシング] のセキュリティインシデントが作成されたときをトリガー条件にします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログイン失敗手動プレイブック

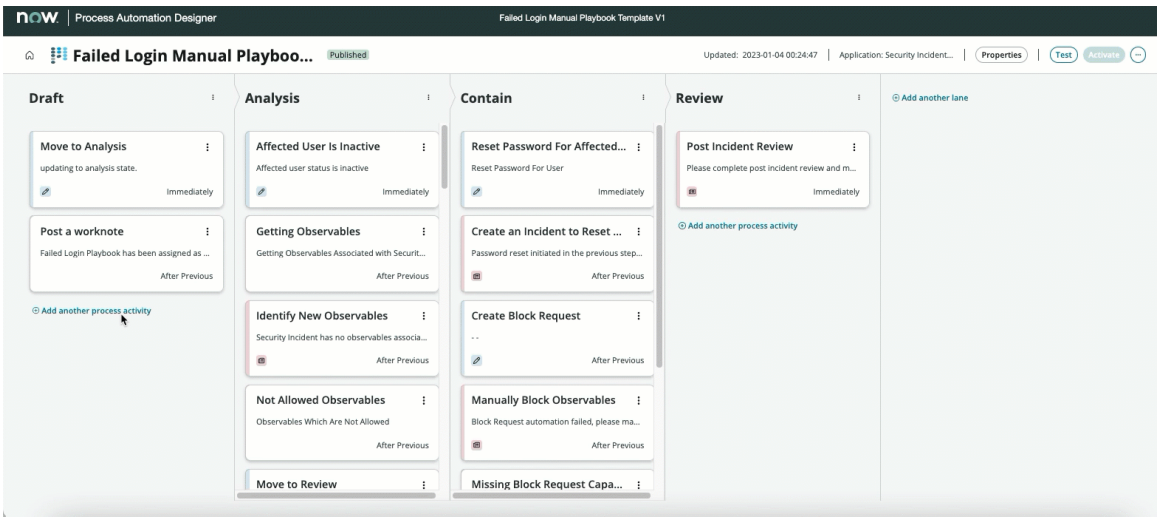


7. [デザイナーに移動] をクリックします。
   [プロセスオートメーションデザイナー] ページが開きます。
8. [新しいステージを追加 **(Add a new stage)**] をクリックして、自動プロセスの設計を開始します。
   ステージのプロパティペインが UI の右側に表示されます。
9. ステージのプロパティペインで、[名前]、[説明]、[実行条件]、および [開始時期を指定 **(Indicate when to start)**] の詳細を入力します。
   [実行条件] および [開始時期を指定 **(Indicate when to start)**] フィールドは、ステージがいつ実行されるかを示します。
10. [保存して閉じる] をクリックします。
11. 別のステージを追加するには、[別のステージを追加 **(Add another stage)**] をクリックします。
    同様に、必要な数のステージを作成できます。この例では、それぞれ [分析]、[封じ込め]、[除去]、および [レビュー] のステージを作成できます。次の例では、[分析] ステージはすぐに開始され、実行条件はありません。[封じ込め] ステージは前のステージが完了した後に開始され、前のステージのアクティビティの結果に基づく実行条件を持ちます。
    ステージを追加した後、各ステージのプロセスアクティビティを追加する必要があります。
12. 特定のステージ (分析ステージなど) で [別のプロセスアクティビティを追加] をクリックします。
    [アクティビティを追加] ポップアップが開きます。
    a. [アクティビティを追加] ポップアップで、必要なアクティビティ定義を選択します。
13. [新しいアクティビティを作成] をクリックします。
    アクティビティ定義を追加した後、ステージと同様にさらに構成できます。同様に、各ステージの下に他のプロセスアクティビティを作成できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログイン失敗手動アクティビティ



14. [アクティビティのプロパティ] ペインで実行条件を追加し、プロセスアクティビティを開始するタイミングを指定します。
15. 実行条件を追加し、開始するタイミングを指定します。
このアクティビティに必要なすべての入力 (構成されている自動化プランの入力を含む) が表示されます。値を上書きすることも、事前設定された値を使用することもできます。
16. [すべてのプロパティを表示] をクリックし、[詳細プロパティ] トグルを有効にすると、アクティビティ定義のすべてのアクティビティエクスペリエンスフィールドが表示されます。

ログイン失敗手動プレイブックの使用

次のステップでは、SIR アナリストワークスペースでのログイン失敗主導 Playbook の使用方法とその機能について説明します。

始める前に

必要なロール：sn_si.admin、sn_si.manager または sn_si.analyst

手順

1. SIR ワークスペースで、セキュリティインシデントを開きます。
2. **[Playbook]** タブをクリックします。

   セキュリティインシデントに対して有効になっているプレイブックを表示できます。セキュリティインシデントのカテゴリ、リスクスコアなどの詳細を表示することもできます。

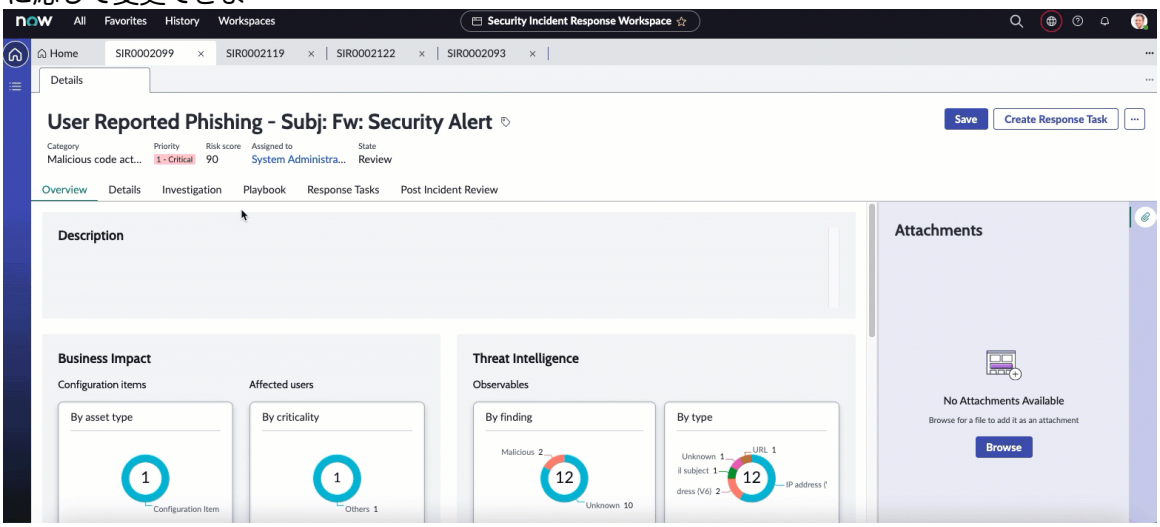
   > **注:**
   > プレイブックがリストに表示されない場合は、PAD に移動して **[Playbook]** タブで表示できるようにする必要があります。

3. [ログイン失敗手動プレイブック **(Failed Login Manual Playbook)]** をクリックします。
ログイン失敗手動の場合、セキュリティインシデントに対してタスクが自動的に実行されます。
4. 各ステージをクリックして、このプレイブックによって実行されたタスクを確認します。
5. [分析] をクリックすると、[分析] フェーズで実行されたアクティビティのリストが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

要件に応じて変更できま



す。

6. 同様に、[封じ込め]、 [除去]、および [レビュー] をクリックして、それぞれのフェーズで実行されたアクティビティのリストを表示できます。
   要件に応じて変更できます。実行する必要があるアクティビティまたはユーザーアクションが残っている場合は、それぞれのフェーズに表示されます。
7. いずれかのフェーズで必要な残りのアクティビティまたはユーザーアクションがある場合は、それぞれのフェーズをクリックし、アクションを実行してアクティビティを完了します。

フローベースのプレイブック

フローデザイナーを使用することで、セキュリティアドミニストレーターやフローデザイン作成者は、手動のプレイブックや文書化されていないプレイブックを、自動化された繰り返し可能なプレイブックへより簡単に移行できます。ドラッグアンドドロップ機能によって、オブジェクト、条件チェック、並列分岐、決定テーブルなどを柔軟に移動できます。

セキュリティインシデントレスポンス は、ベースシステムで次のプレイブックを提供します。

リストされているプレイブックに加えて、Security Operations スポークには、フロープレイブックから呼び出すことができるサブフローもあります。ランサムウェアはそのサブフローの 1 つです。

これらのフローは、使用する前にアクティブ化してください。詳細については、「セキュリティインシデントレスポンスフローのアクティブ化)」を参照してください。

自動フィッシングプレイブック

自動フィッシングプレイブックは、特定のタイプのセキュリティ脅威を段階的な方法で解決するのに役立ちます。フローデザイナーのテンプレートを使用することで、フィッシング応答プレイブックのステップを自動化し、インシデントを迅速かつ効率的に解決できます。

フローデザイナーで作成したテンプレートを使用して、フィッシング応答プレイブックのタスクを自動化し、組織内のフィッシング攻撃を分析および解決できます。

フィッシング応答プレイブックには、次のフローとサブフローが含まれています。

- セキュリティインシデント - 自動フィッシング応答テンプレート：このテンプレートは、フィッシング応答タスクを自動化するように設計されており、トリガーを含む一連のアクションを含みます。
- セキュリティインシデント - フィッシング手動テンプレート：このテンプレートは、既存の手動フィッシング応答ワークフローです。カテゴリを [フィッシング] に設定して、フローをアクティブ化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

これらのテンプレートには、フィッシング攻撃に応答するように設計された一連の再利用可能なアクションが含まれています。各フローには、トリガー (条件)、一連のアクション、サブフローがあります。これには、読みやすくするために注釈を付けることができます。これらのフローにアクセスするには、Security Operations スポーク をインストールする必要があります。

注:
これらのテンプレートは、使用する前にアクティブ化します。詳細については、「セキュリティインシデントレスポンス フローのアクティブ化」を参照してください。

- 観測事象の脅威ルックアップの実行：選択した観測事象の脅威のルックアップを実行します。
- 観測事象を拡張：さまざまなソースからの追加情報で観測事象を拡張できます。
- フィッシングメールの影響度の評価：フィッシングメールの影響を評価できます。このサブフローでは、フィッシングメールアドレスでメールを受信すると、.EML 添付ファイルが解析され、その情報がメール一致ルールと比較されます。
- フィッシングメールの撲滅：フィッシングメールを削除または根絶して、特定の攻撃へのエクスポージャーを減らすことができます。
- 観測事象のサイティング検索の実行：時間の経過に伴う脅威のまん延を判断したり、修復または根絶作業をテストしたりします。
- ブロック要求の作成：インシデントに関連付けられた観測事象との通信をブロックします。

これらのサブフローは、複数の Playbook で使用できる再利用可能操作のセットを表します。これらのサブフローを使用して、要件に従ってカスタムテンプレート (フロー) を定義できます。

カスタムテンプレート (フロー) を作成するには、「フロー 」の指示に従ってください。

自動フィッシング対応プレイブックフローの実行

フローデザイナーを使用して、プレイブックのタスクを定義して自動化し、組織に対するフィッシング攻撃を分析して解決します。

始める前に

- 必要なロール：sn_si.admin、flow_designer、および action_designer
- 適切な認証情報を使用して、次の統合をインストールして構成します。
  - ブロック要求 (セキュリティオペレーション Palo Alto Networks NGFW 統合)
  - 観測事象の拡張
  - サイティング検索
  - 脅威のルックアップ
  - Microsoft Office Exchange

このタスクについて

(セキュリティポリシーで定義されている) フィッシング攻撃の一般的な兆候を含む不審なメールを受信した場合、従業員は、それを組織で定義されたフィッシングメールアドレスに .EML 添付ファイルとして送信できます。自動フィッシングプレイブックフローで定義されたタスクを使用して、フィッシングの脅威をトリアージ、分析、封じ込め、および根絶できます。これらのタスクは、さまざまなインシデント状況 (分析、封じ込めなど) の一部として呼び出すことができます。フィッシングセキュリティインシデントが作成されると、自動フィッシングフローが自動的にトリガーされます。フローデザイナーを使用すると、さまざまなインシデント応答アクションが呼び出されたときにその詳細を表示できます。

自動翻訳

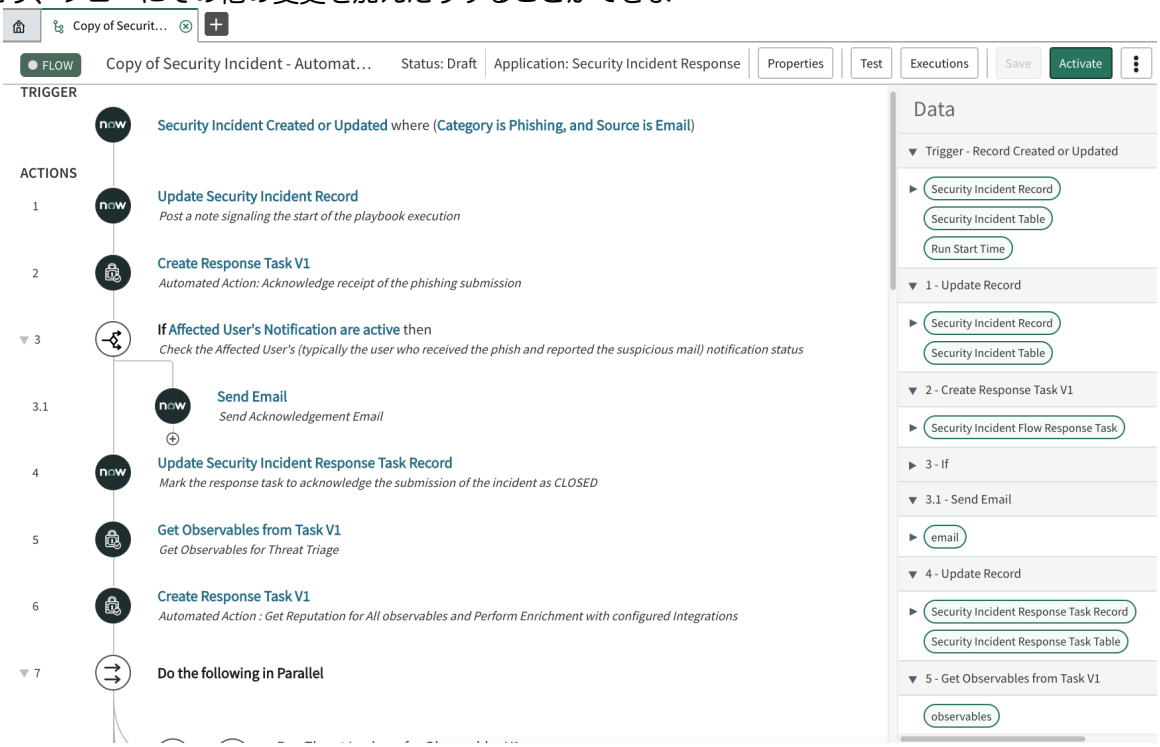
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[セキュリティインシデント - 自動フィッシング応答テンプレート V1 (Security Incident - Automated Phishing Response Template VI)] プレイブックフローは読み取り専用です。フローのコピーを作成し、必要に応じて変更を加えることができます。

この後のステップでは、フィッシングプレイブックテンプレートのコピーを作成する方法について説明し、フロー内のいくつかのタスクについて順を追って説明します。

手順

1. 次のように移動する。 **All** (すべて) > **Flow Designer** > デザイナー をクリックして、 セキュリティオペレーション スポークで利用可能なフローを表示します。
2. [セキュリティインシデント - 自動フィッシング応答テンプレート **VI (Security Incident - Automated Phishing Response Template VI)]** リンクをクリックします。
3. [フロー] ページで、 その他アイコン をクリックし、フローのコピーを作成して開き、使用できるようにします。
   トリガー条件を変更したり、アクションを追加または削除したり、フローにその他の変更を加えたりすることができます。

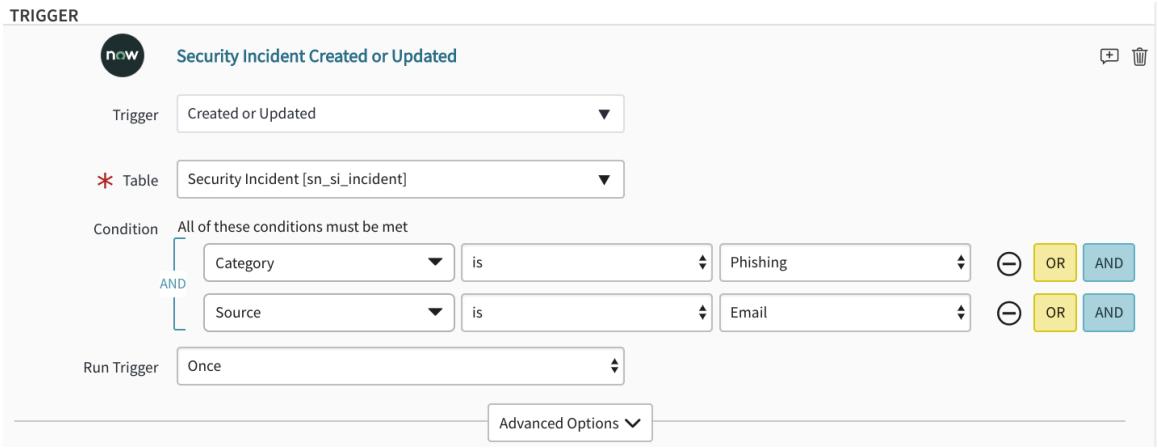


   この画像は、トリガー条件と、フローが実行するステップを示しています。右側のパネルにはデータフローが示されています。アイコンをクリックすると、ステップが展開され、詳細が表示されます。

4. [トリガー] アイコンをクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

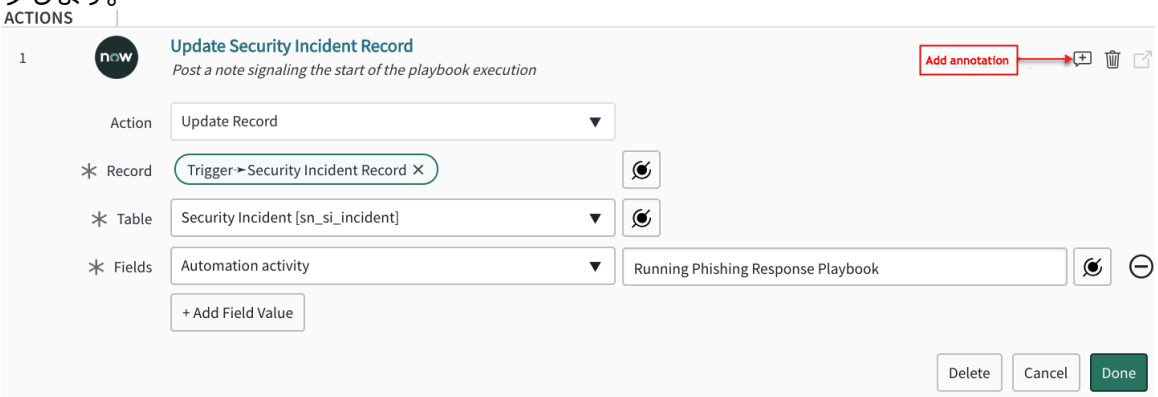
最初のステップでは、フローのトリガーを定義または設定します。トリガーの条件と、フローでトリガーを実行する頻度を指定しま



す。

フローで定義された条件 ([カテゴリ] が [フィッシング] で [ソース] が [メール] であること) がインシデントレコードで満たされると、自動フィッシングフローのタスクの実行が順次開始されます。トリガーの変更、注釈の追加、条件の追加または削除などを行うことができます。

5. [セキュリティインシデントレコードの更新 **(Update Security Incident Record)]** リンクをクリックします。

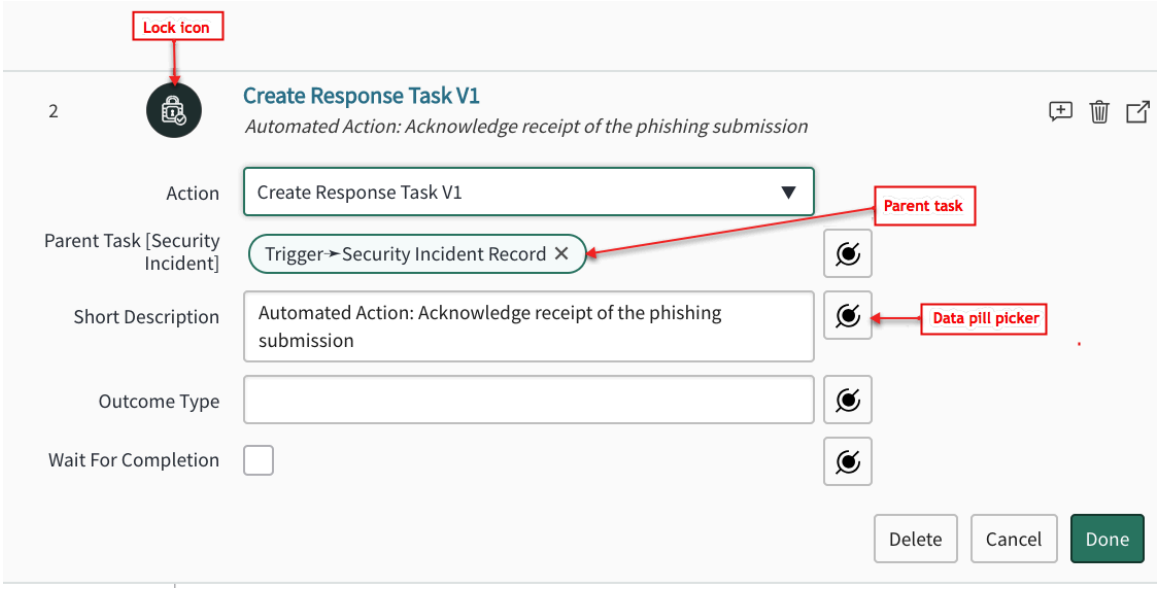


[セキュリティインシデントレコードの更新 (Update Security Incident Record)] が、フローの最初のステップです。注釈アイコン をクリックして、フィッシングインシデントが発生したこと、および自動フィッシングプレイブックフローの実行が開始されたことを示すセキュリティアナリスト向けのメモを追加します。

6. フローのステップ 2 に進み、[対応タスクを作成] リンクをクリックします。

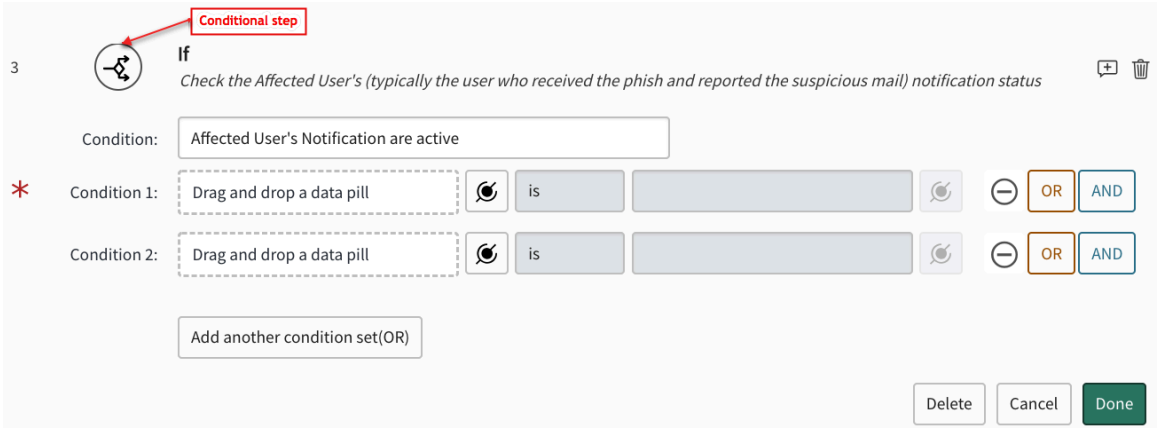
このステップでは、フローにより、インシデントの送信者または影響を受けるユーザーに受信確認を行う自動応答タスクが作成されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



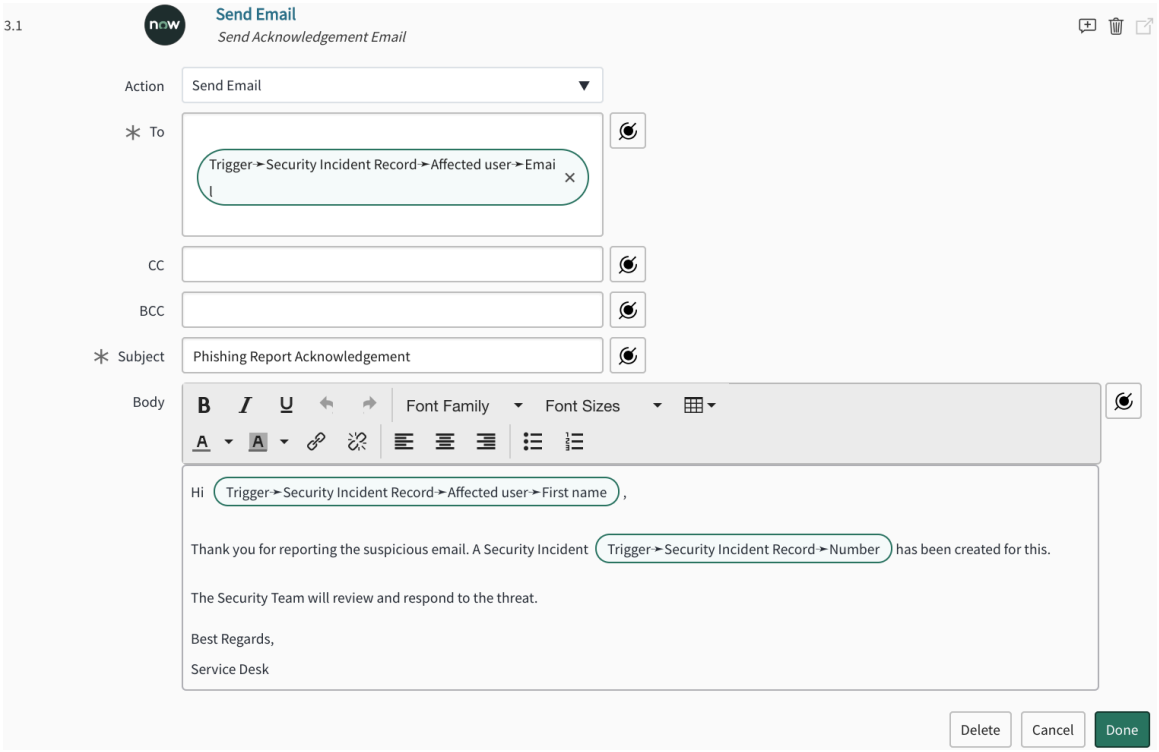
[親タスク [セキュリティインシデント]] フィールドは、このステップに関連付けられた親レコードを参照することに注意してください。データピルピッカーアイコン を使用するか、右側のパネルから関連する参照アイテムをドラッグして、参照レコードを選択できます。ロックアイコン を確認します。ロックアイコンは、ステップでユーザーの介入が必要ないことを示します。

7. ステップ 3 では、フローは通知を正常に送信できるように、影響を受けるユーザー (通常はインシデントを送信したユーザー) の詳細をさらに収集します。
影響を受けるユーザーのステータスがアクティブであり、ユーザーが通知を受信できるかどうかを確認する条件を指定できます。



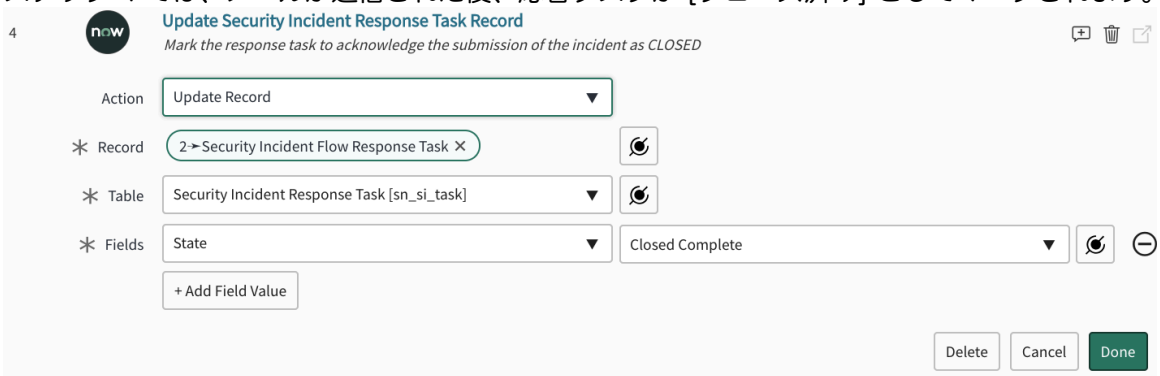
ステップ 3 の条件付きステップアイコン を確認します。フローは、指定された条件が満たされた場合にのみ次のステップ (3.1) を実行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

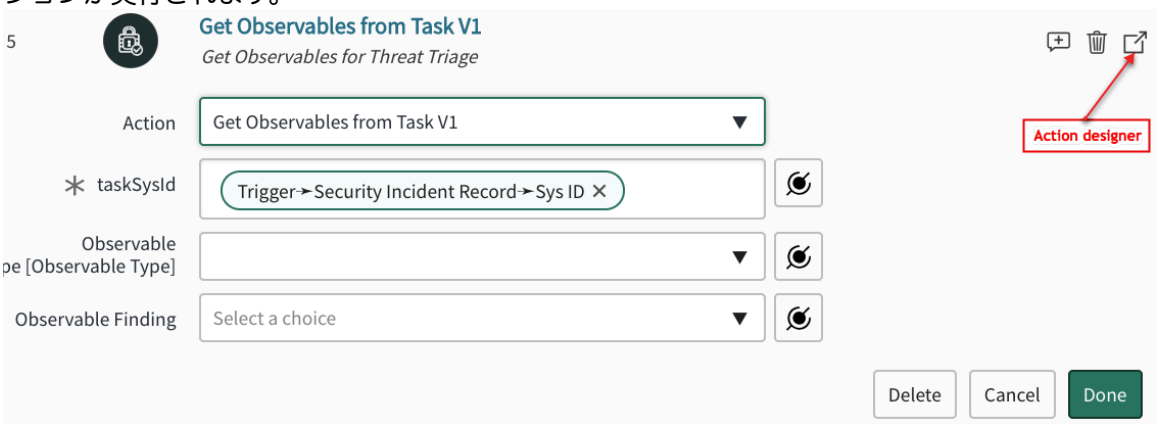


ステップ 3 で定義された条件が正常に満たされると、メールが送信されます。

8. ステップ 4 では、メールが送信された後、応答タスクが [クローズ済み] としてマークされます。



9. ステップ 5 では、インシデントに関連するすべての観測事象 (メールの件名、フィッシングメールの送信元のメールアドレス、フィッシング URL など) または選択したカテゴリに属する観測事象 (ハッシュ、ファイル、ドメイン) が収集され、後続の プレイブックステップで追加の自動アクションが実行されます。



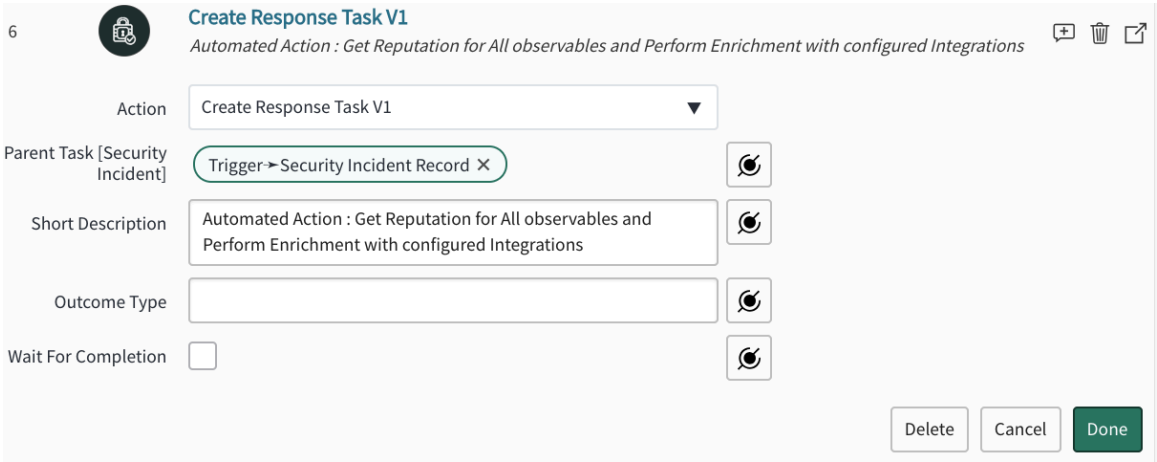
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクションデザイナーアイコン をクリックして、アクションの詳細ビューを表示します。

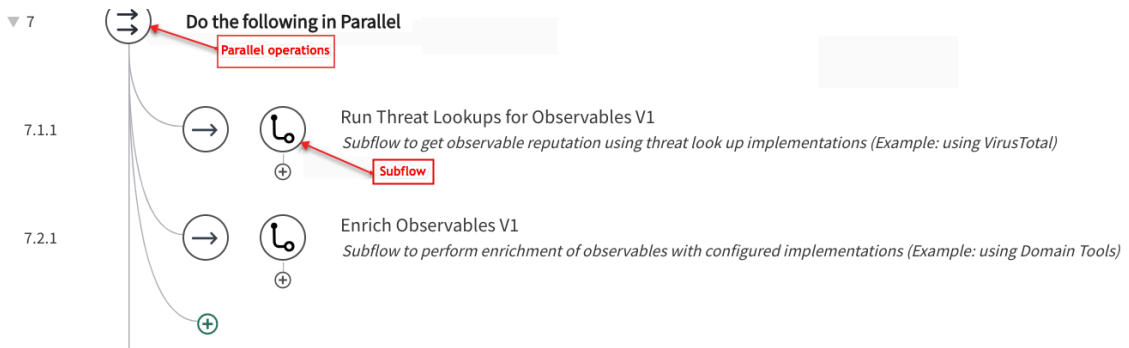
[アクションデザイナー] ページを表示するには、フローのステップを展開し、アクションデザイナーアイコンをクリックします。

10. ステップ 6 では、自動応答タスクが作成されます。
このタスクは、すべての観測事象の評判を取得し、構成された
統合を使用して拡張を実行するプロセスの開始をキャプチャしま

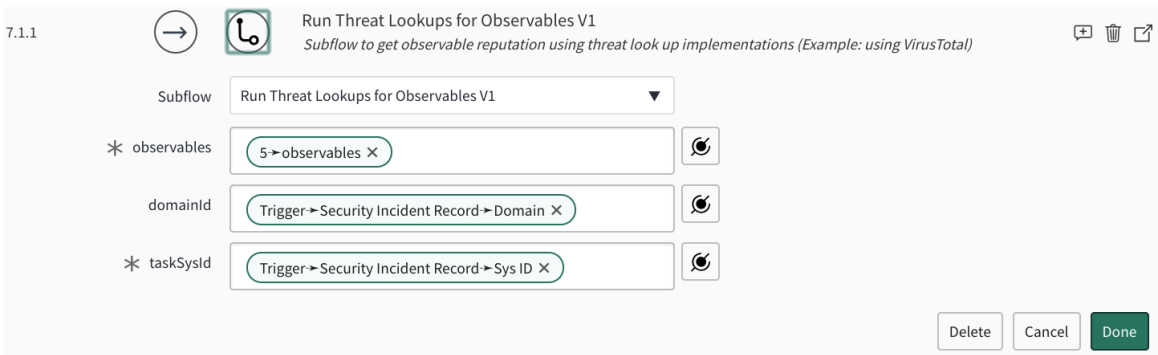


す。

11. ステップ 7 では、次の 2 つのサブフローが呼び出されます。
   - 観測事象の脅威ルックアップの実行：このサブフローは、脅威のルックアップ実装を使用してすべての観測事象の評判を取得するために使用されます。
   - 観測事象を拡張：このサブフローは、構成された実装で観測事象の拡張を実行するために使用されます。



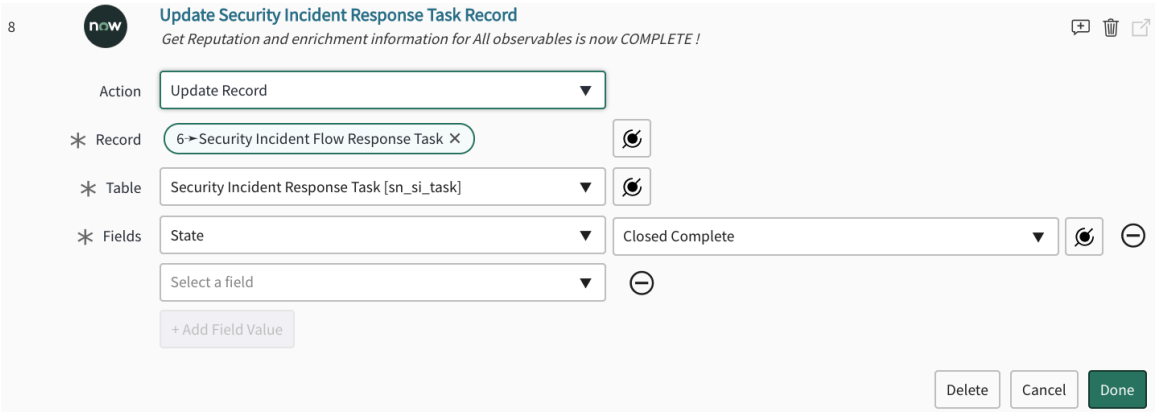
このタスクのアイコンを確認します。並列操作アイコン は、両方のタスクが並列に実行されることを示し、サブフローアイコン は、次に示すように、実行中のタスクがサブフローであることを示します。



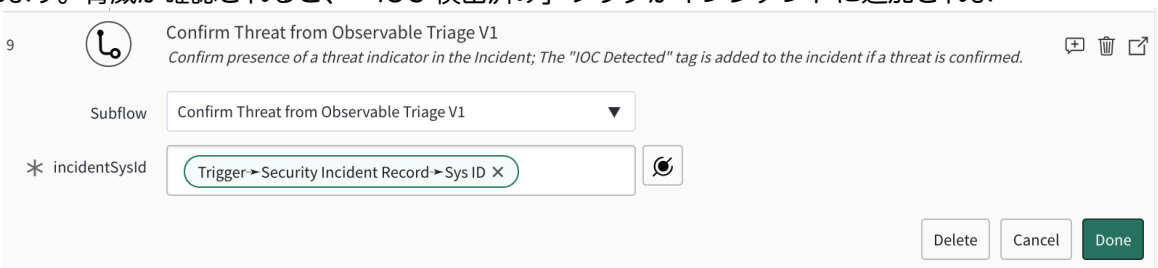
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[観測事象] フィールドの数字「5」に注目してください。これは、ステップ 5 で取得された観測事象に対して脅威のルックアップが実行されることを示しています。その結果、このサブフローは、サブフローデザイナーに示されているように、既存のワークフローとアクションを呼び出します。

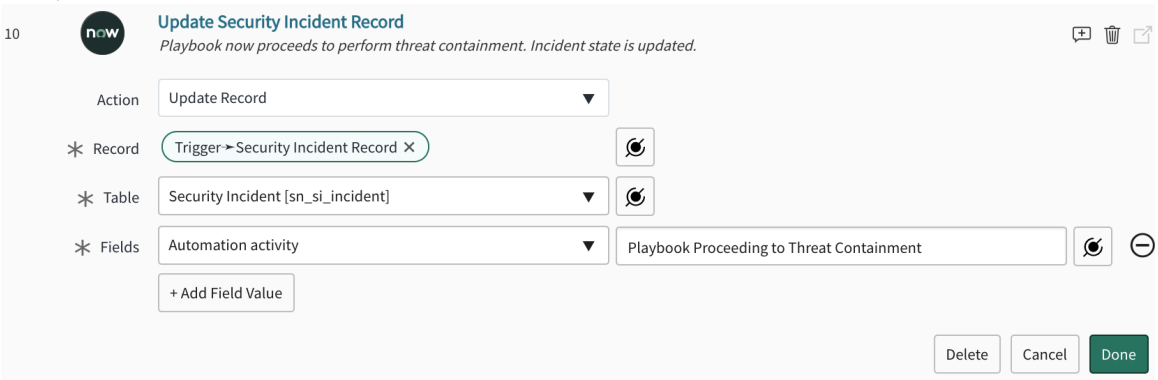
12. ステップ 8 では、サブフローが完了した後、応答タスクが [クローズ済み] としてマークされます。



13. ステップ 9 では、「観測事象トリアージからの脅威を確認」サブフローが呼び出されます。このサブフローは、インシデント内の脅威インジケーターの存在を確認するために使用されます。脅威が確認されると、「IOC 検出済み」フラグがインシデントに追加されます。

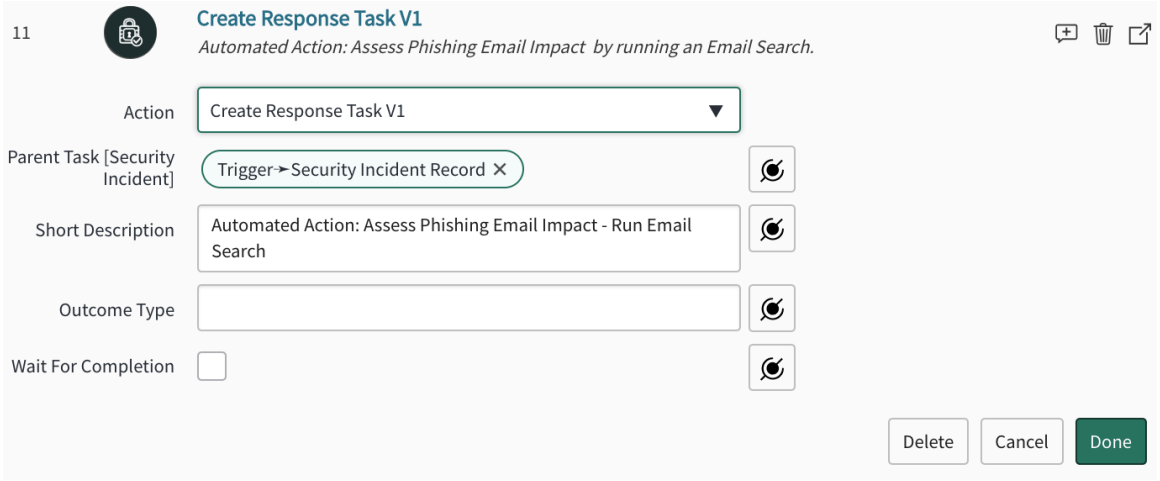


14. 脅威が確認されたら、ステップ 10 でセキュリティインシデントを更新して、脅威の封じ込めタスクが開始されることを示すメモを追加します。

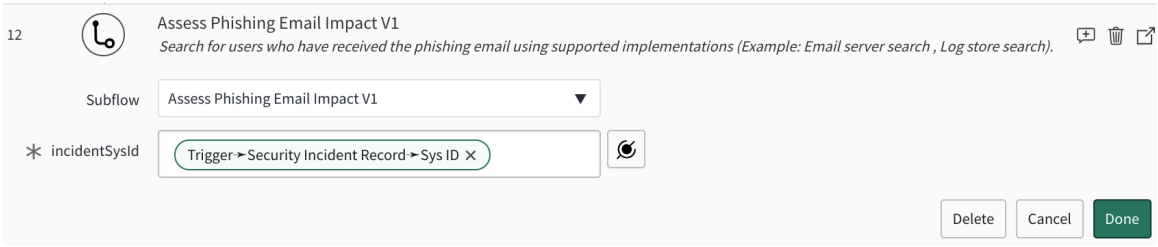


15. ステップ 11 は、フィッシングメールの影響を評価するために使用されるタスクの開始と完了をキャプチャする自動応答タスクです。

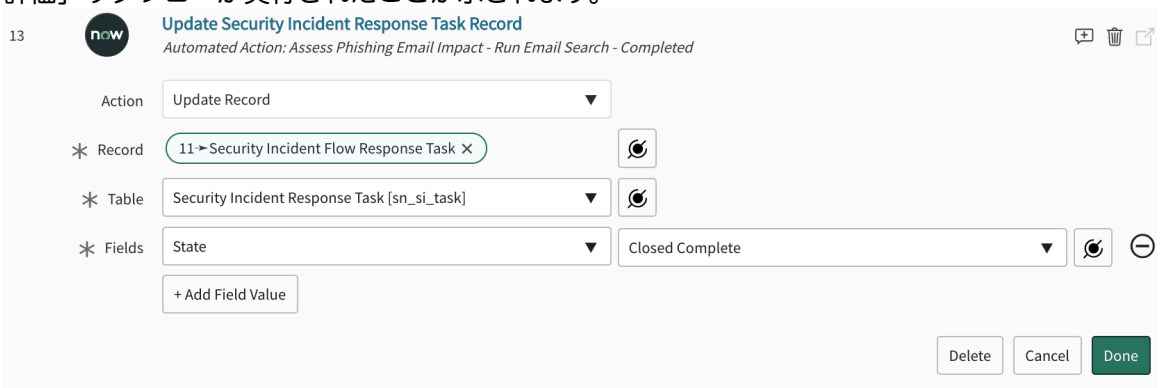
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



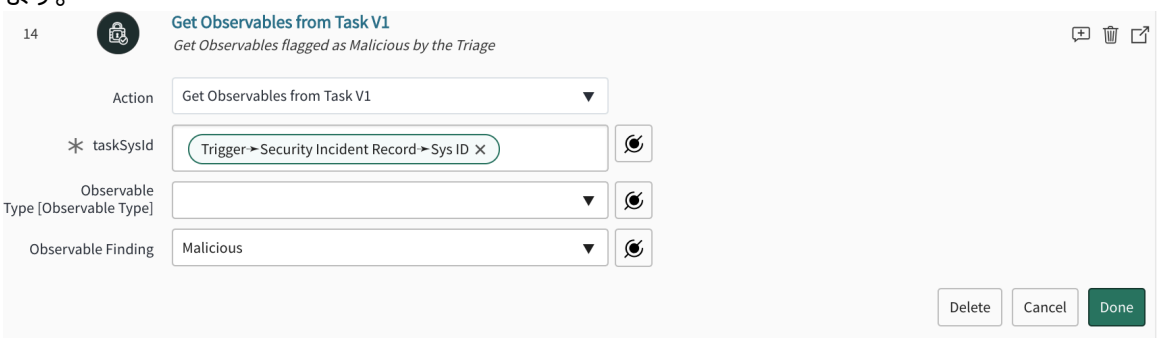
16. ステップ 12 では、「フィッシングメールの影響度の評価」サブフローが呼び出されます。このサブフローは、サポートされている実装を使用してフィッシングメールを受信したユーザーを検索するために使用されます。



17. ステップ 13 で、タスクは [クローズ済み] としてマークされ、「フィッシングメールの影響度の評価」サブフローが実行されたことが示されます。



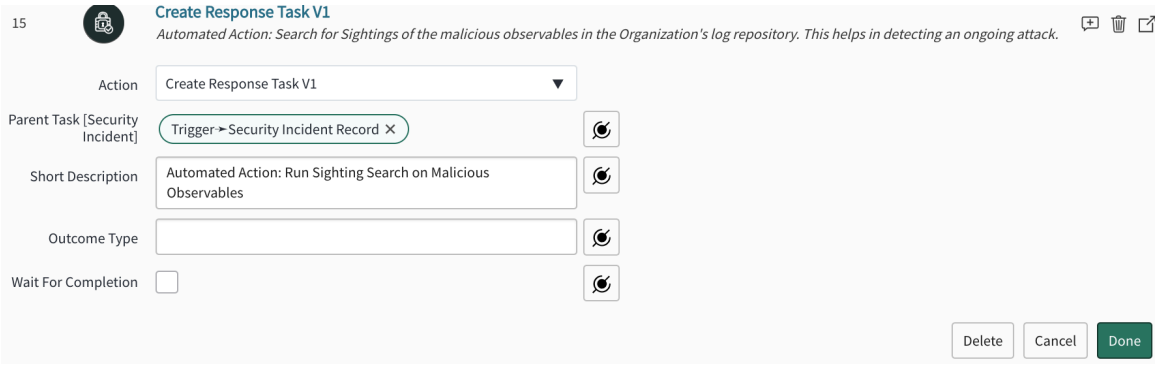
18. ステップ 14 は、悪意のある項目としてマークされたすべての観測事象を取得するために使用されます。



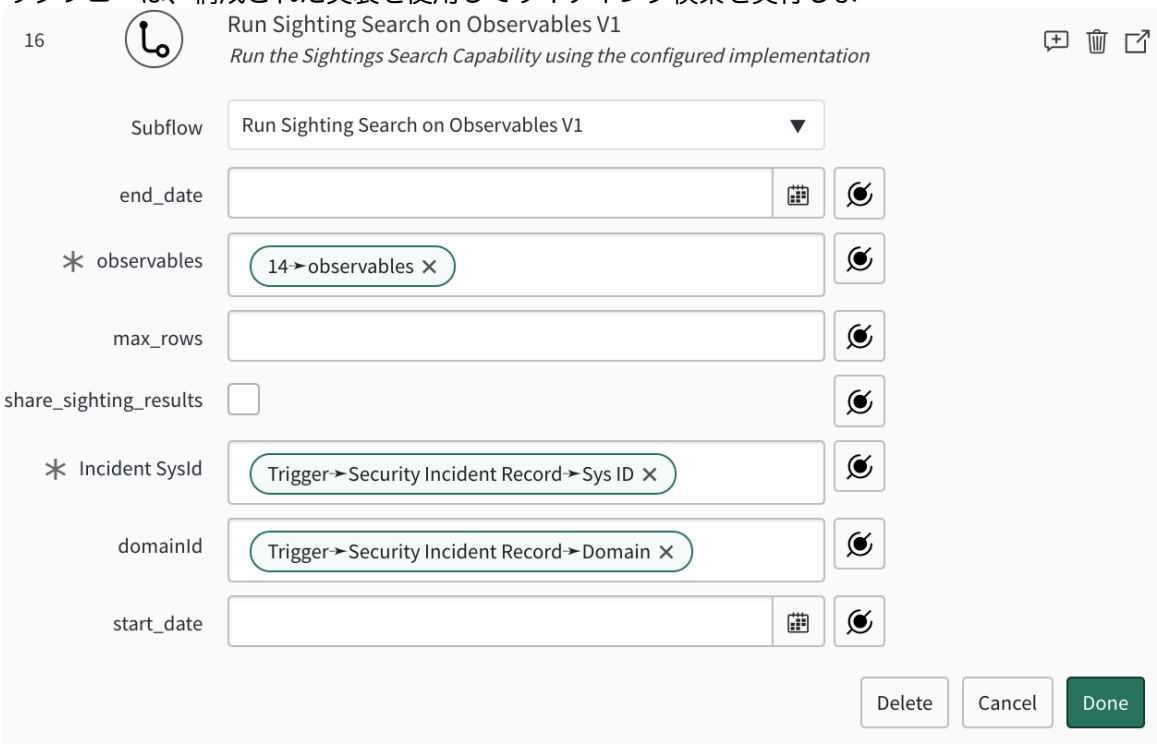
19. ステップ 15 は、観測事象タスクのサイティング検索の開始と完了をキャプチャする自動応答タスクです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

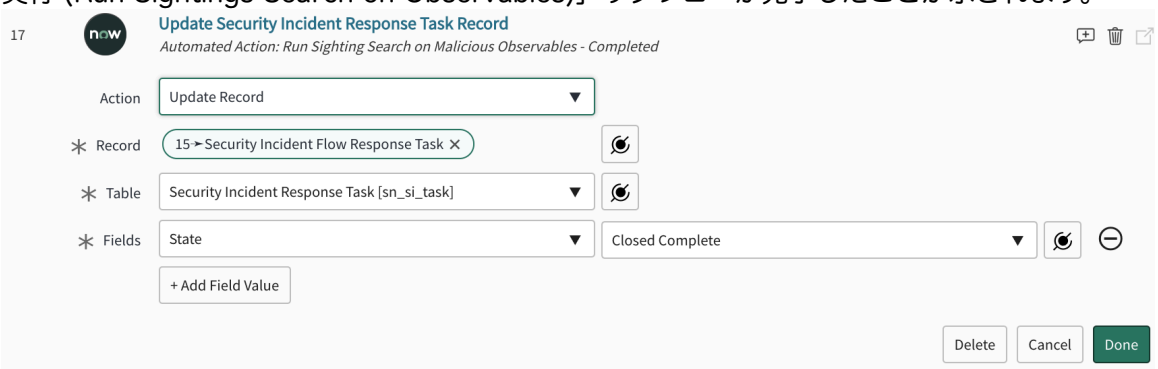


20. ステップ 16 では、「観測事象のサイティング検索を実行 (Run Sightings Search on Observables)」サブフローが呼び出されます。
このサブフローは、構成された実装を使用してサイティング検索を実行しま



す。

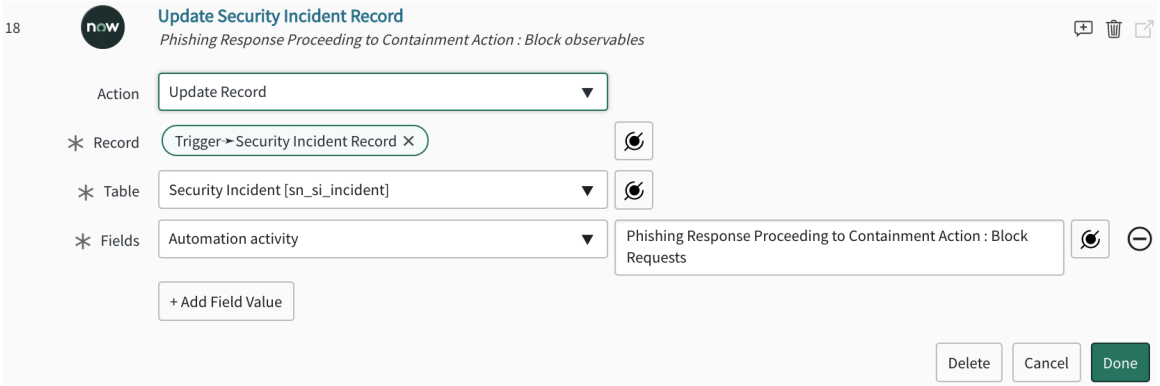
21. ステップ 17 で、タスクは [クローズ済み] としてマークされ、「観測事象のサイティング検索を実行 (Run Sightings Search on Observables)」サブフローが完了したことが示されます。



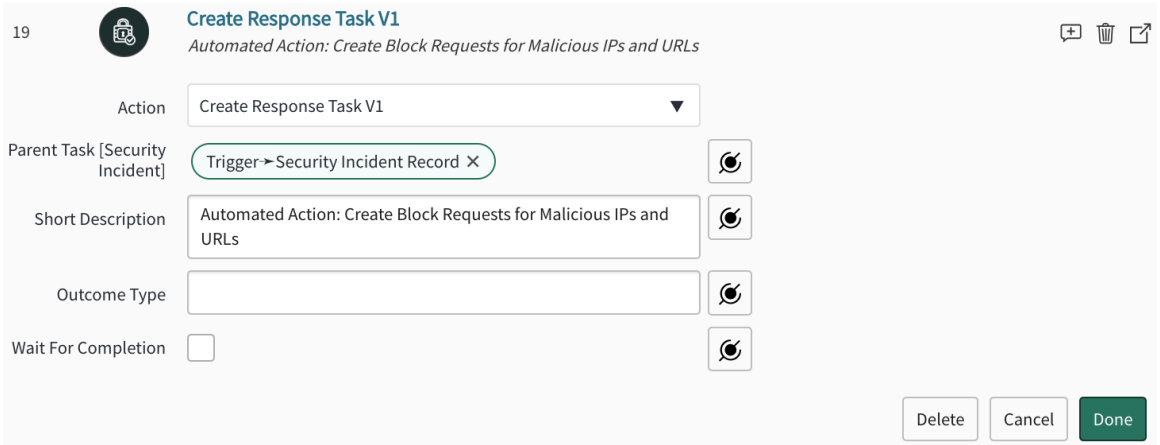
22. 悪意のある観測事象を特定したら、ステップ 18 でセキュリティインシデントレコードを更新して、封じ込めアクションが開始されることを示します。

自動翻訳

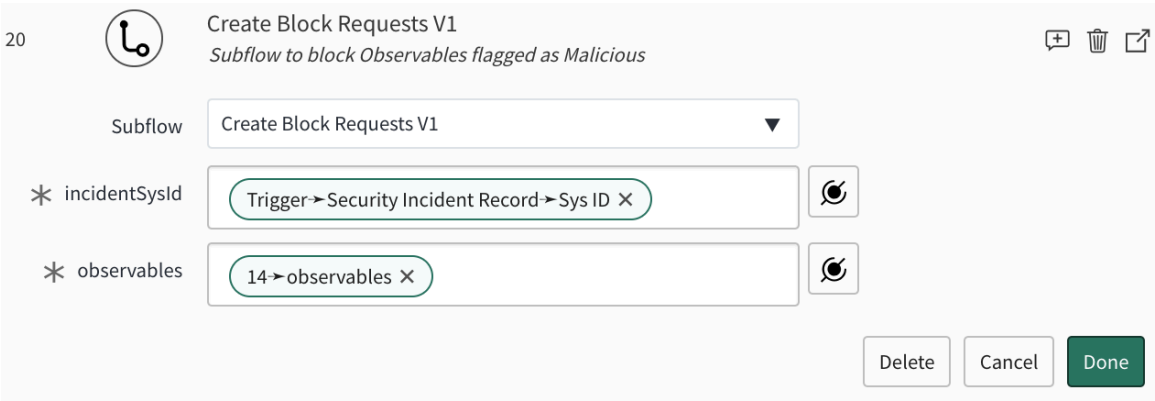
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



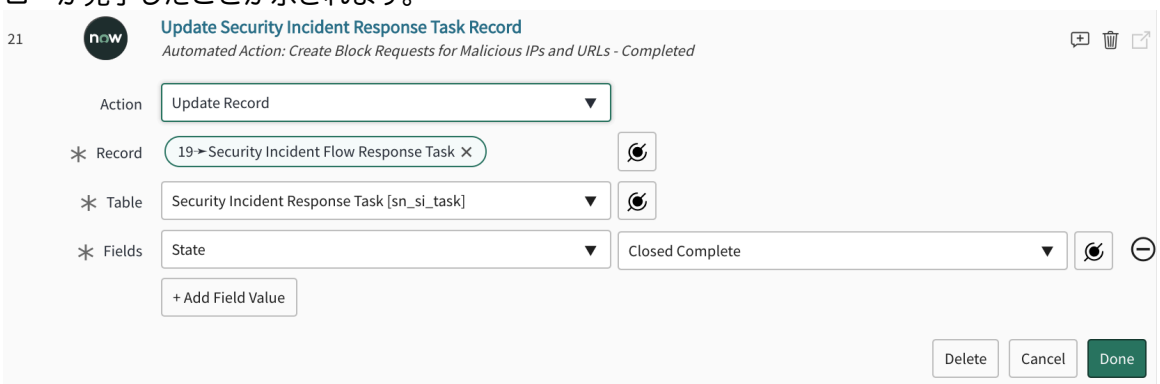
23. ステップ 19 は、ブロック要求タスクの開始と完了をキャプチャする自動応答タスクです。



24. ステップ 20 では、「ブロック要求の作成」サブフローが呼び出されます。このサブフローは、悪意のある観測事象をブロックするために使用されます。



25. ステップ 21 で、タスクは [クローズ済み] としてマークされ、「ブロック要求の作成」サブフローが完了したことが示されます。

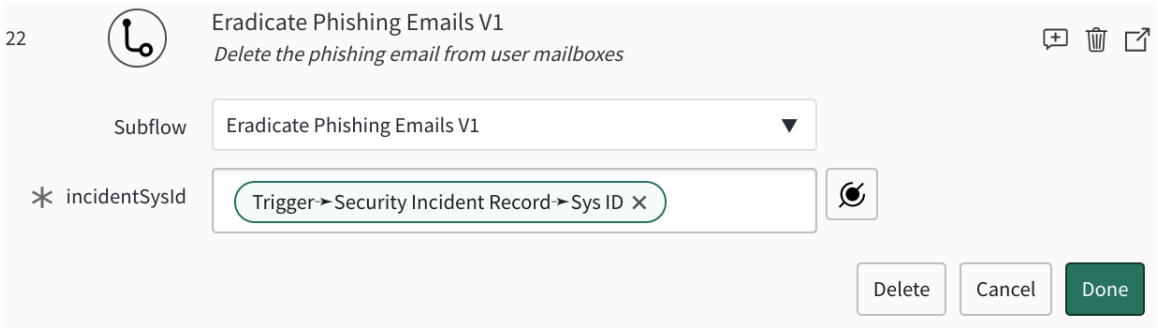


26. ステップ 22 では、「フィッシングメールの撲滅」サブフローが呼び出されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

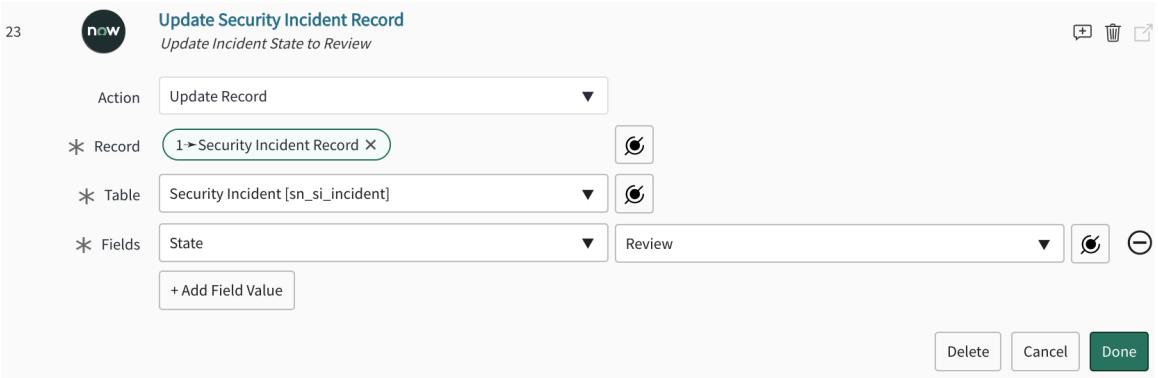
自動翻訳

このサブフローは、ユーザーのメールボックスからフィッシングメールを削除するために使用されま

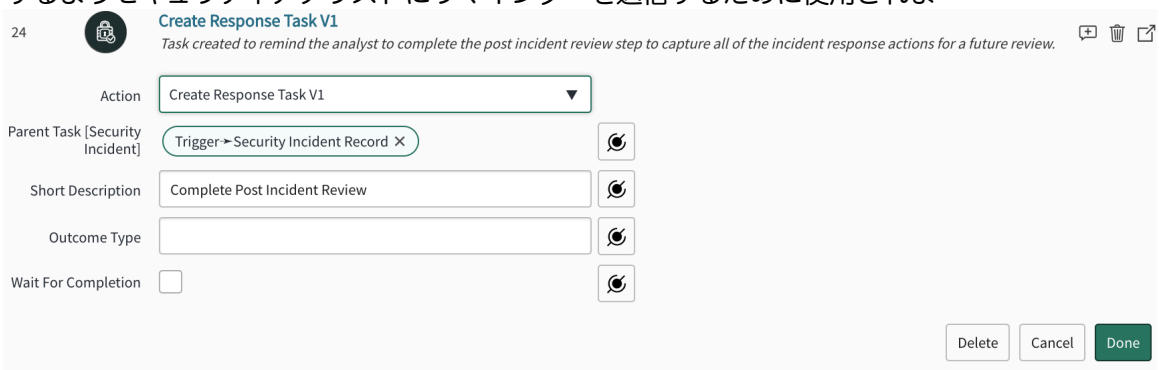


す。

27. フィッシングメールを削除した後、ステップ 23 でセキュリティインシデントレコードを更新して、インシデント状況を確認する必要があることを示します。



28. 最後のステップでは、フローにより自動応答タスクが作成されます。
このタスクは、今後のレビューのためにすべてのインシデント応答アクションを保存するようセキュリティアナリストにリマインダーを送信するために使用されま



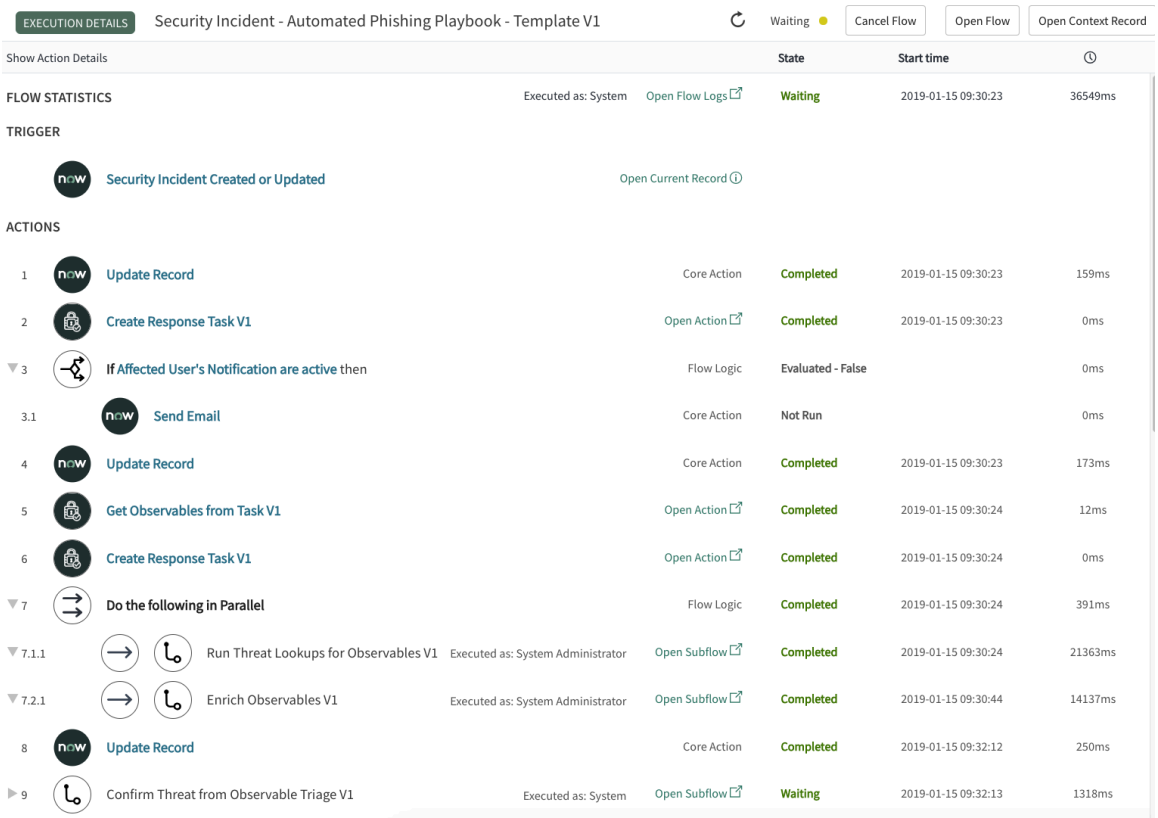
す。

次のタスク
[テスト] をクリックすると、公開する前にフロー内のアクションをシミュレートできます。フローをテストした後、[アクティブ化] をクリックしてフローをアクティブ化して、実行します。

[実行] をクリックして、フローの実行の詳細を表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳



自動翻訳

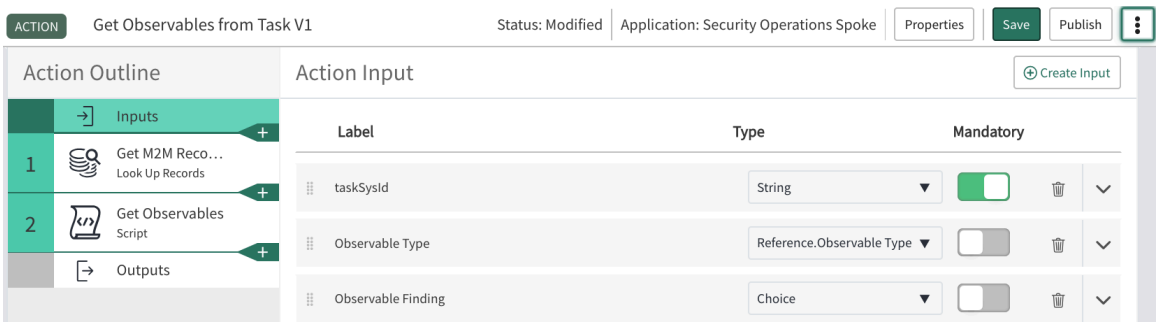
自動フィッシング対応プレイブックフローアクションデザイナーの表示

アクションデザイナーにドリルダウンして、自動フィッシング対応プレイブックフローの特定のステップで実行されているアクションに関する詳細情報を表示できます。

このページでは、[タスクから観測事象を取得] ステップの [アクションデザイナー] ページについて説明します。[アクションアウトライン] パネルでタスクをクリックして詳細を表示します。

アクションの入力

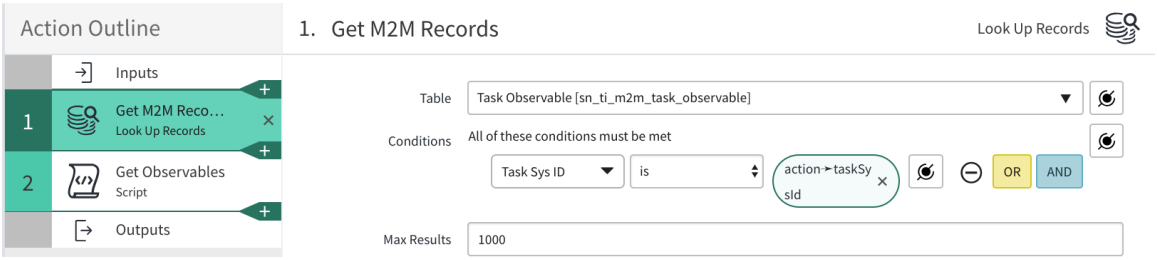
このセクションには、インシデント ID、観測事象のタイプ (ハッシュまたは IP)、観測可能結果 (悪意のあるメールのみ) など、アクションがどのように作成されたかについての詳細が表示されます。



M2M レコードを取得

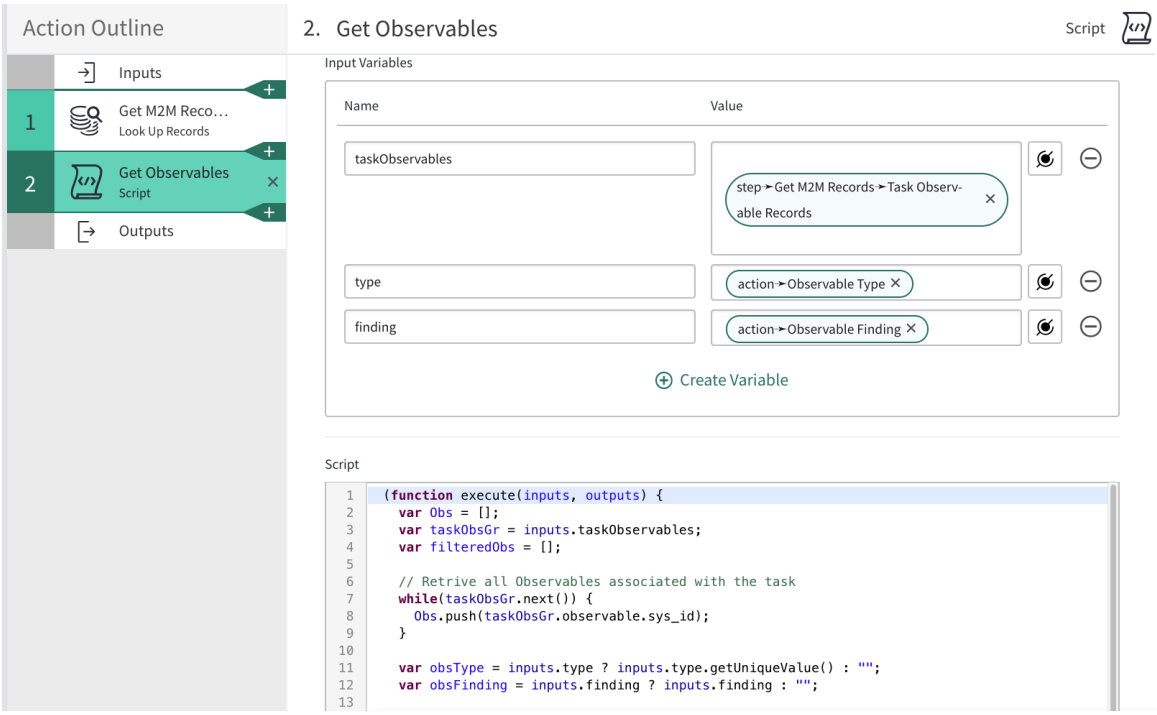
このセクションには、指定されたテーブル内の観測事象を検索するために定義された条件が表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



観測可能項目を取得

このセクションには、指定されたフィルター条件に基づいて観測事象を取得するために使用されるスクリプトが表示されます。最後に、この条件を満たす観測事象とカウントが表示されます。



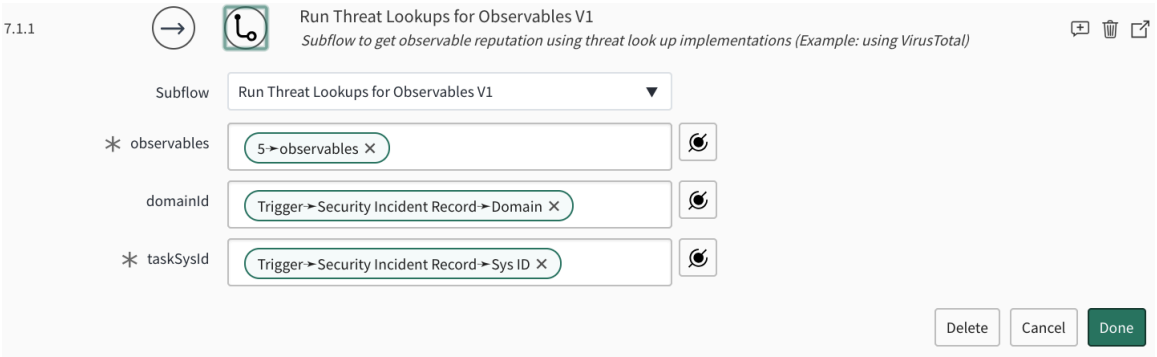
注:
このフローで定義されているすべてのアクションは再利用可能であり、要件に応じて変更できます。

自動フィッシング応答プレイブックサブフローデザイナーの表示

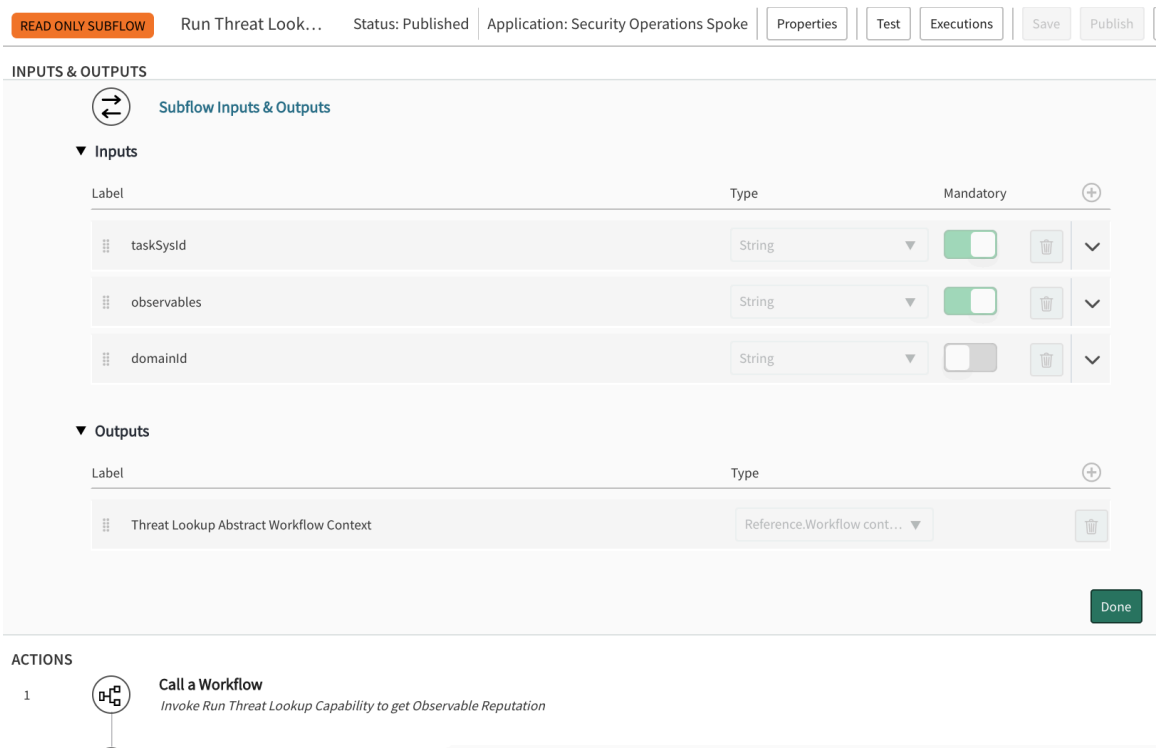
サブフローデザイナーにドリルダウンして、自動フィッシング応答プレイブックフローの一部として実行されているサブフローに関する詳細情報を表示できます。

サブフローデザイナーを起動して、サブフローの詳細を表示できます。ここでは、「観測事象の脅威ルックアップの実行」サブフローの [サブフローデザイナー] ページを示します。下の画像の アイコンをクリックすると、サブフローデザイナーが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[サブフローデザイナー] ページでは、このサブフローの入力と出力、および実行中の基礎となるワークフローアクションを確認できます。



注:
このサブフローは読み取り専用であり、編集できません。サブフローのステップへの追加や削除を行うことはできますが、サブフローを変更することはできません。

自動マルウェアプレイブック

自動マルウェアプレイブックには、マルウェアアラートを迅速かつ効率的に解決するのに役立つ一連の自動化された手順が記載されています。

マルウェアプレイブック フローを使用して、エンドポイントまたはネットワークからのマルウェアアラートの処理に関連する手順を自動化します。フローテンプレートには、読みやすい注釈が付けられたトリガー条件、一連のアクションとサブフローが含まれています。

これらのテンプレートには、フィッシング攻撃に応答するように設計された一連の再利用可能なアクションが含まれています。各フローには、読みやすい注釈が付けられたトリガー (条件)、一連のアクションとサブフローがあります。これらのフローにアクセスするには、Security Operations スポーク と Security Operations Palo Alto Networks - WildFire アプリを ServiceNow Store からインストールする必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
これらのテンプレートは、使用する前にアクティブ化する必要があります。

次のフローとサブフローが含まれています。

- セキュリティインシデント - 自動マルウェアプレイブック テンプレート：このテンプレートはマルウェアアラートへの対応を自動化するように設計されており、トリガーを含む一連のアクションが含まれています。
- セキュリティインシデント - マルウェア手動テンプレート：このテンプレートは、カテゴリが [悪意のあるコードアクティビティ] に設定されている場合にアクティブになる、既存の手動のマルウェア対応ワークフローです。

サブフロー

- 観測事象からの脅威を確認：観測事象が悪意のあるものであり、対処する必要があるかどうかを確認します。
- インシデントの重大度を設定：インシデントの重大度ステータスを設定します。
- ランサムウェアプレイブック：ランサムウェア攻撃かどうかを判断します。

これらのサブフローは、複数の Playbook で使用できる一連の再利用可能な操作を表します。これらのサブフローを使用して、要件に従ってカスタムテンプレート (フロー) を定義できます。

カスタムテンプレート (フロー) を作成するには、「フロー」の指示に従ってください。

自動マルウェアプレイブック フローの実行

このフローを使用してプレイブックのタスクを自動化し、組織に対するマルウェア攻撃を分析して解決します。

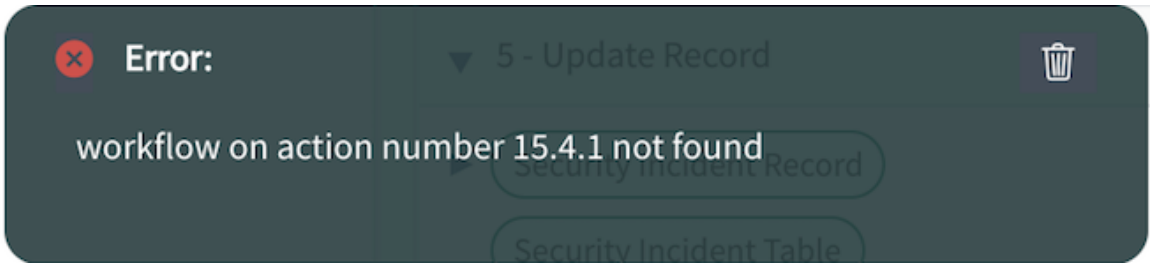
始める前に

- 必要なロール：sn_si.admin、flow_designer、および action_designer
- 正しい認証情報を使用して、次の統合をインストールして構成します。
  - Security Operations 用の Palo Alto Networks WildFire
  - サイティング検索 (Splunk)
  - ブロック要求
  - 脅威のルックアップ
  - 観測事象を拡張

  セキュリティインシデント - 自動マルウェアプレイブック テンプレートをアクティブ化する前に、これらの統合が正常に機能していることを確認します。
- Security Operations Palo Alto Networks Wildfire アプリ：自動マルウェアプレイブック フローにアクセスするには、Security Operations スポークと Security Operations Palo Alto Networks - WildFire アプリを ServiceNow Store からインストールする必要があります。Security Operations Palo Alto Networks Wildfire アプリがインストールされていない場合、次のような「アクション番号 15.4.1 のワークフローが見つかりません (workflow on action number 15.4.1 not found)」というエラーが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



このアプリをインストールしない場合は、自動マルウェアプレイブック フローからステップ 15.2、15.3、および **15.4** を削除します。

- 次の条件が満たされていることを確認します。
  - セキュリティインシデントが、適切な承認グループに属するセキュリティアナリストにアサインされている。
  - インシデントを処理するセキュリティアナリストは、有効なメールアドレスを持っている必要がある。
  - 必要な構成アイテムと観測事象がセキュリティインシデントに追加されている。
- ステップ **21** (承認を求める) で、グループを [セキュリティインシデントアサイン先 **(Security Incident Assignment)]** から希望するグループに変更します。
- フローのステップ 21 は、承認要求がアドミニストレーターに送信される必須のタスク承認ステップです。要求を承認するには、アドミニストレーターが [タスクの承認 (Task Approvals)] ページに移動し、[ステータス (State)] フィールドを [承認済み] に設定する必要があります。タスクが承認されない場合、フローデザイナーはそれ以上先に進むことができず、プロセスは終了します。

このタスクについて
悪意のあるコードアクティビティがネットワークで検出されると、セキュリティインシデントが作成され、自動マルウェアプレイブック フローが起動します。自動マルウェアプレイブック フローで定義されたタスクを使用して、脅威をトリアージ、分析、封じ込め、および根絶できます。

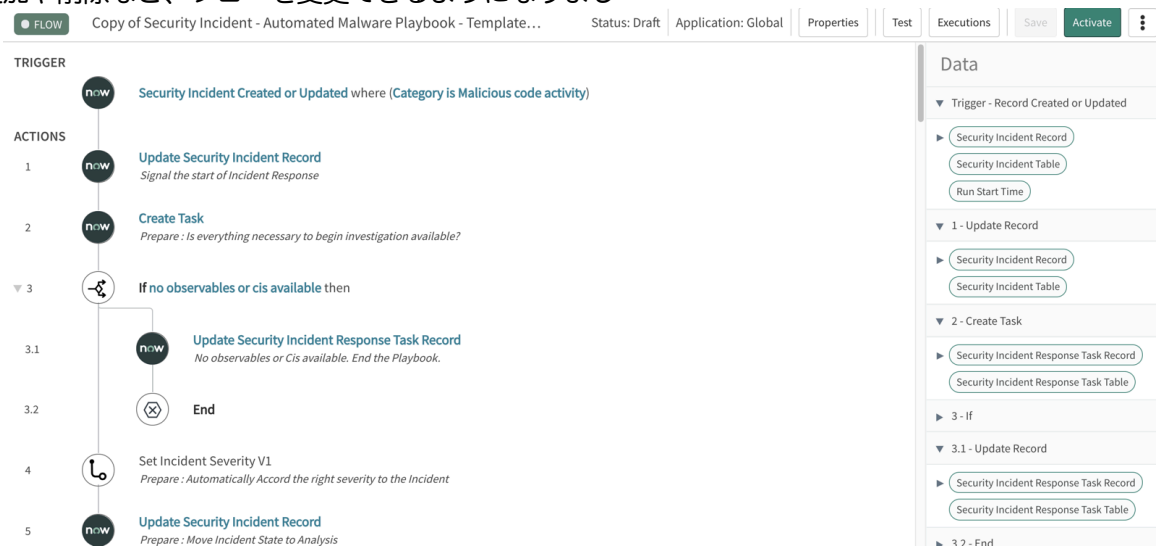
手順

1. 次のように移動する。 **All** (すべて) > **Flow Designer** > デザイナー をクリックして、Security Operations スポークで利用可能なフローを表示します。
2. [セキュリティインシデント：自動化マルウェアプレイブック：テンプレート **VI]** リンクをクリックします。
3. [フロー] ページで、 その他アイコン をクリックし、フローのコピーを作成して開き、使用できるようにします。

自動翻訳

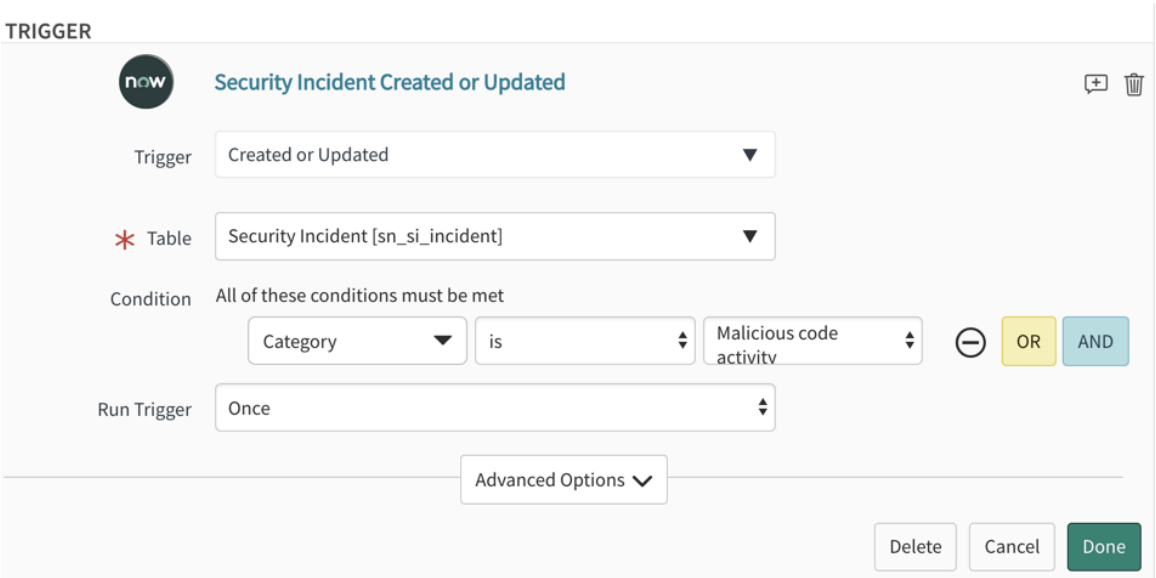
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

これで、トリガー条件やアクションの変更、アクションの追加や削除など、フローを変更できるようになりました。



これは、フローで実行されるトリガーおよびステップを示しています。右側のパネルにはデータフローが表示されています。アイコンをクリックすると、ステップが展開され、詳細が表示されます。

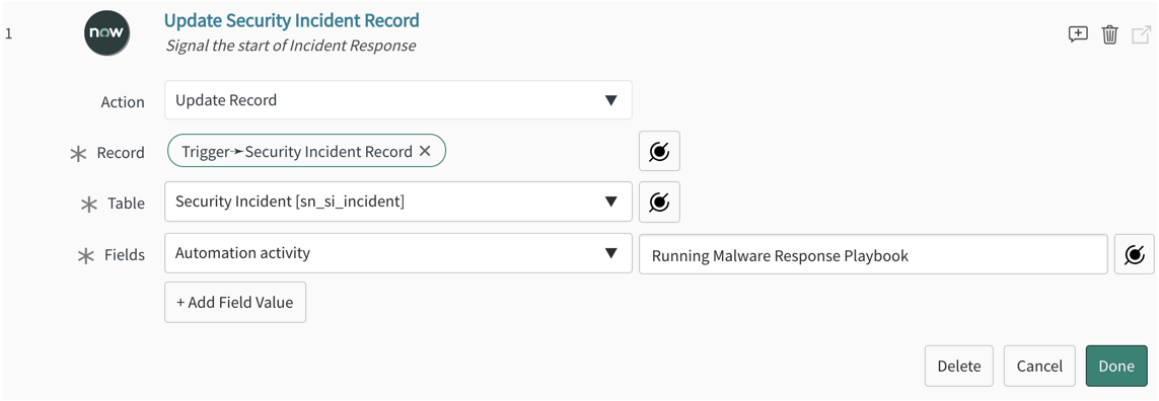
4. [トリガー] アイコンをクリックします。
最初のステップでは、フローのトリガーを定義または設定します。条件が満たされたときに実行されるトリガーとタスクの条件を指定します。



フローで定義された条件 ([カテゴリ] が [悪意のあるコードアクティビティ] であること) がインシデントレコードで満たされると、自動フィッシングフローのタスクの実行が順次開始されます。トリガーの変更、注釈の追加、条件の追加または削除などを行うことができます。

5. フローの最初のステップは、[セキュリティインシデントレコードの更新 **(Update Security Incident Record)]** です。

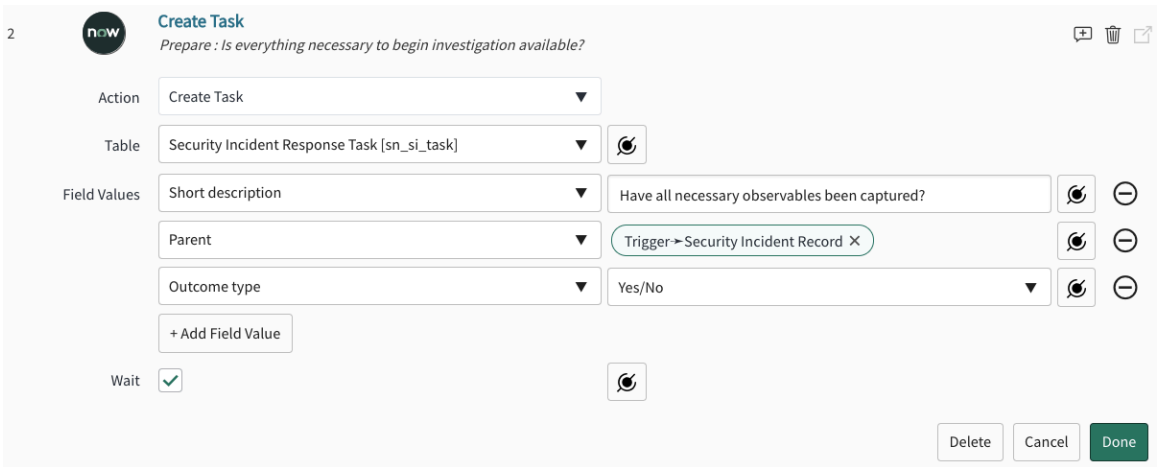
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



リンクをクリックし、 注釈アイコン をクリックして、悪意のあるコードアクティビティがあったこと、および自動マルウェア応答プレイブックフローの実行が開始されたことを示すセキュリティアナリスト向けのメモを追加します。

6. フローのステップ 2 に進み、[タスクの作成] リンクをクリックします。

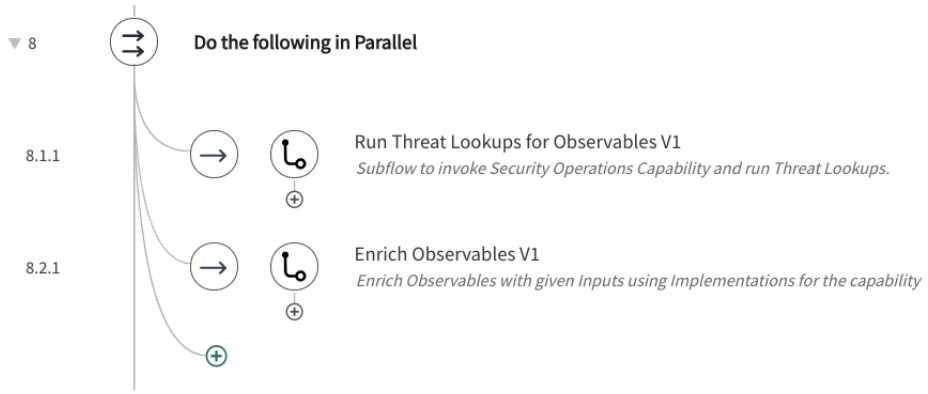
   このステップでは、必要なすべての観測事象がキャプチャされたかどうか、および調査を開始できるかどうかを確認する自動応答タスクが作成されます。



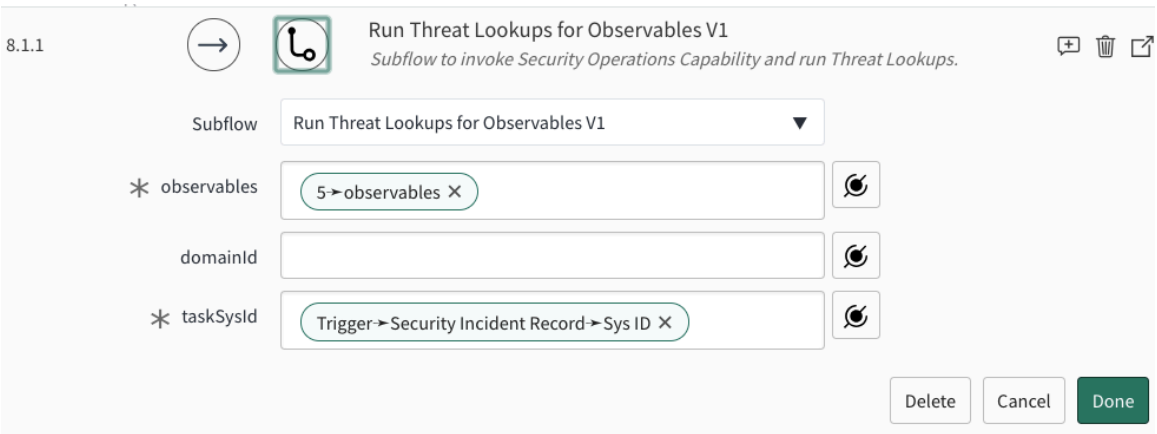
7. 結果タイプが [いいえ] の場合は、調査を開始するための観測事象と CI がないことを示します。セキュリティインシデントレコードを更新すると、プレイブックがそれ以上先に進むことができないことが示されます。
8. 結果タイプが [はい] の場合、「インシデント重大度を設定」サブフローは、正しい重大度をセキュリティインシデントに自動的にアサインします。
9. 次のステップで、セキュリティインシデントレコードが更新されます。
10. 次のステップでは、インシデントまたは選択したカテゴリに関連するすべての観測事象が収集され、後続のプレイブックステップで追加の自動アクションが実行されます。
11. 次のステップでは、自動応答タスクが作成されます。
    このタスクは、すべての観測事象の評判を取得し、構成された統合を使用して拡張を実行するプロセスの開始をキャプチャします。
12. ステップ 8 では、次の 2 つのサブフローが呼び出されます。
    - 観測事象の脅威ルックアップの実行：このサブフローは、脅威のルックアップ実装を使用してすべての観測事象の評判を取得するために使用されます。
    - 観測事象を拡張：このサブフローは、構成された実装で観測事象の拡張を実行するために使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



このタスクのアイコンを確認します。並列操作アイコン は、両方のタスクが並列に実行されることを示し、サブフローアイコン は、次に示すように、実行中のタスクがサブフローであることを示します。



[観測事象] フィールドの数字「5」に注目してください。これは、ステップ 5 で取得された観測事象に対して脅威のルックアップが実行されることを示しています。その結果、このサブフローは既存のワークフローとアクションを呼び出します。

13. 次のステップで、[レコードの検索を実行 (Run the Look Up Records)] アクションが実行されます。
このアクションは、親ワークフローが次のいずれかになるワークフローコンテキストレコードを検索するために使用されます。
    - 脅威ルックアップの抽象ワークフロー コンテキスト
    - 観測可能拡張の抽象ワークフロー コンテキスト
14. 次のステップでは、8 つのレコードごとに評判とエンリッチメント結果がレビューされます。
15. 後続ステップのレビューを続行します。
    a. セキュリティインシデントレコードの更新 (Update Security Incident Record)：評判のルックアップと拡張アクティビティが完了したことを示すように、セキュリティインシデントレコードを更新します。
    b. タスクから観測事象を取得：セキュリティインシデントに関連付けられた悪意のあるすべての観測事象を取得します。
    c. タスクの作成：自動トリアージの実行が成功したかどうかをチェックして確認します。
16. 悪意のある項目としてフラグが付けられた観測事象がある場合：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. セキュリティインシデントレコードの更新 (Update Security Incident Record)：脅威が検出されたことを示す作業メモを投稿します。

b. 観測事象から入力クエリを作成：10 件を超える観測事象に悪意のある項目としてフラグが付けられている場合、(Splunk または Carbon Black 上で)「観測事象でのサイティング検索」サブフローが実行されます。

17. 観測事象に悪意のある項目としてフラグが付けられていない場合、フローは後続のステップに進みます。

a. セキュリティインシデントレコードの更新 (Update Security Incident Record)：脅威が検出されていないことを示す作業メモを投稿します。

b. タスクから観測事象を取得：インシデントからのすべての SHA256 ハッシュ ID を識別します。

c. 観測事象レコードを検索 (Look Up Observable Records)：この条件を満たすレコードを検索します。

18. 後続ステップのレビューを続行します。

a. 悪意のある観測事象ごとに、**[Security Operations Palo Alto Networks - Wildfire** データ拡張の取得 **(Security Operations Palo Alto Networks - Get Wildfire Data Enrichment)]** ワークフローが実行されます。

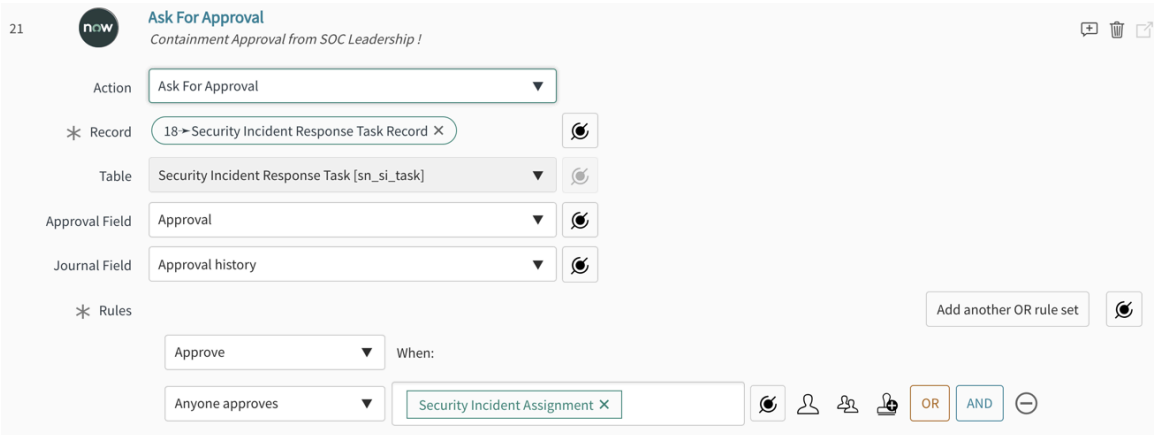
b. 調査結果が満足のいくものであるかどうかを確認します。
疑わしいマルウェアがランサムウェア攻撃であるかどうかを確認するための応答タスクが作成されます。「はい」の場合、ランサムウェアプレイブックサブフローが実行されます。

c. 次のステップでは、分析のサマリと封じ込め手順を開始するための承認要求を含むメールが送信されます。

d. 要求された承認の詳細をキャプチャするタスクが作成されます。

e. 次のステップは、セキュリティインシデントレコードの更新です。
承認要求が行われたことをセキュリティアナリストに知らせる作業メモを投稿します。

f. SOC マネージャーにマルウェア攻撃を封じ込めるための承認を要求します。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
フローによって承認要求が生成されると、作業メモは次のメッセージで更新されます。

<task id> の承認要求が行われました。封じ込めを続行します。(An Approval request has been made for <task id> proceeding with containment.) このタスクを承認するには、SOC マネージャーとして次の手順を手動で実行します。

- [タスクの承認 (Task Approvals)] ページに移動します。
- 承認のリストが表示されます。承認する <task id> をクリックします。
- ステータスを [承認] に変更して、更新された <task id> を保存します。

g. 次のステップでは、セキュリティインシデントレコードが更新され、承認ステータスが追跡されます。

h. 次に、封じ込め手順を開始するためのタスクが作成されます。

i. 「悪意のある観測事象のブロック要求の作成の実行 (Run the Create Block Requests for Malicious Observables)」サブフローが実行され、感染したデバイスとその資産を再ビルドする要求を含むインシデントレコードが作成されます。

j. 次に、サイティング検索を実行して環境が安全かどうかを確認するタスクが作成されます。サイティング検索は、サイティングが見つからなくなるまで繰り返されます。

k. 次に、セキュリティインシデントレコードでレビューの準備ができていることを示すタスクが作成されます。

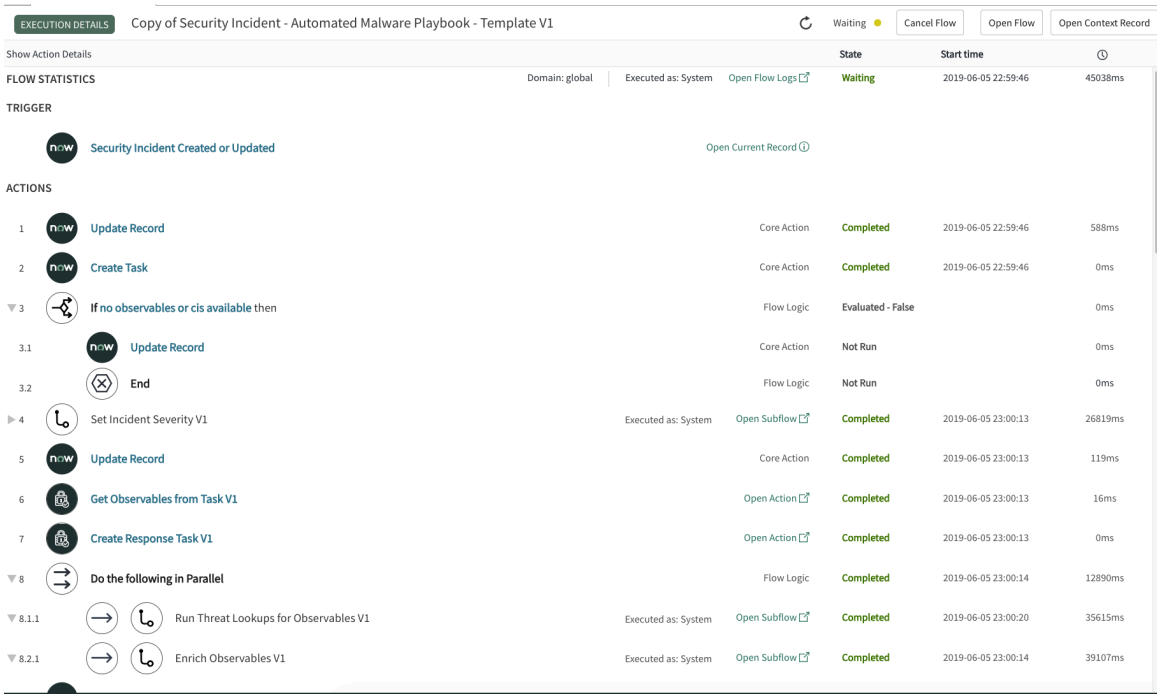
l. 最後に、レコードが更新され、[レビュー] ステージに移行します。

次のタスク
[テスト] をクリックすると、公開される前にフロー内のアクションをシミュレートできます。フローをテストした後、[アクティブ化] をクリックしてフローをアクティブ化して、実行できるようにします。

[実行] をクリックして、フローの実行の詳細を表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



ログイン失敗手動プレイブック

ユーザーが (SIM 構成に従って) 一定回数ログインに失敗すると、セキュリティインシデントが作成されます。

これらの失敗したログイン試行は、誤検出であるか、ユーザーのメールアカウントへのアクセスを取得しようとする攻撃者の試みである可能性があります。このようなシナリオでは、ログイン失敗手動プレイブック は、ガイダンスを提供し、失敗したログインセキュリティインシデントの調査を最適化するのに役立ちます。

必須条件

必要なロール：

- sn_si.admin
- flow_designer

スポーク：Security Operations スポークのインストール (sn_sec_spoke)

主な機能

ログイン失敗プレイブックには、セキュリティインシデントを調査するための次の機能が含まれています。

1. 影響を受けるユーザーがアクティブ/非アクティブユーザーであるかどうかを確認する。
2. 許可リスト観測事象をフィルタリングする。
3. 観測事象を拡張する。
4. 自動脅威ルックアップを実行する。
5. 失敗したログイン試行を確認する自動メールをユーザーに送信する。
6. ユーザーアクセスを調査するタスクをアナリストにアサインする。
7. 悪意のある観測事象とブロック IP および URL を特定する。
8. ユーザーパスワードをリセットする。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

9. セキュリティインシデントのステータスを更新する。
10. インシデントの事後レビューを処理するタスクをセキュリティアナリストにアサインする。

必要な機能

- 脅威のルックアップ (Virus Total、ハイブリッド分析)
- 観測事象を拡張 (Whois、ReverseWhois)
- サイティング検索 (Splunk、QRadar)
- 観測事象のブロック (CheckPoint、Palo Alto)

詳細については、ServiceNow Store を参照してください。

セキュリティアナリストエクスペリエンス

セキュリティ上の脅威を段階的に解決する方法を理解するには、「プレイブックによるセキュリティの脅威の解決」を参照してください。

フローデザイナーの機能を使うログイン失敗プレイブックの使用

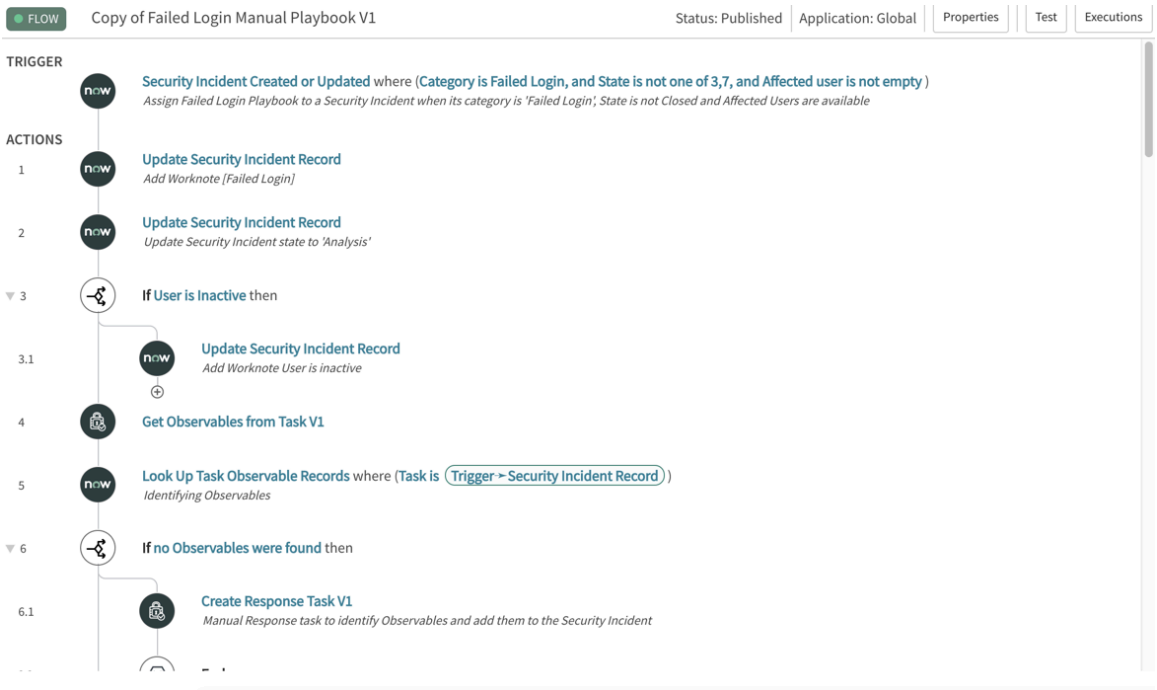
はじめに

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **Flow Designer** > デザイナー をクリックし、 ログイン失敗 プレイブックをクリックします。
3. 次のフローのコピーを作成して、ログイン失敗プレイブックをコピーし、必要な変更を行います(これはオプションのステップです。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します)。
   - ログイン失敗手動プレイブック V1
   - ログイン失敗：ユーザーの返信を解析し、応答タスクを更新 V1
4. 要件に応じて必要な変更を行います。(これはオプションのステップです。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します)。
5. プレイブックをアクティブ化します。
   - ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   - 要件に応じて変更を加えた後、コピーしたフローをアクティブ化します。

次の画像は、ログイン失敗手動プレイブック のコピーを示しています。以下の手順では、プレイブックでのさまざまなアクションについて説明しています。

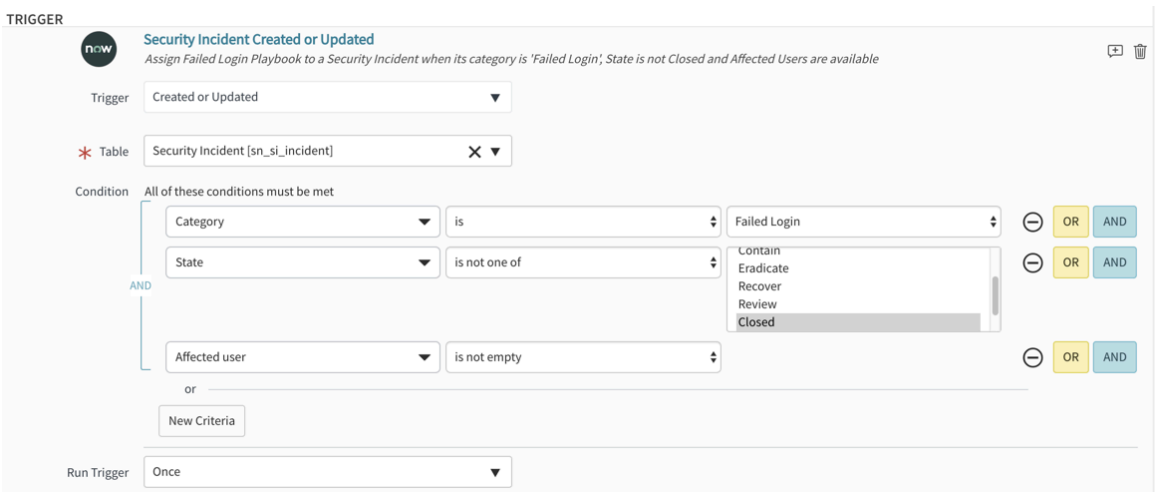
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



このプレイブックは、次の条件が満たされるとトリガーされ、セキュリティインシデントに関連付けられます。

- カテゴリが [ログイン失敗] である。
- 影響を受けるユーザーが 1 人以上いる。
- セキュリティインシデントがクローズまたはキャンセルされていない。

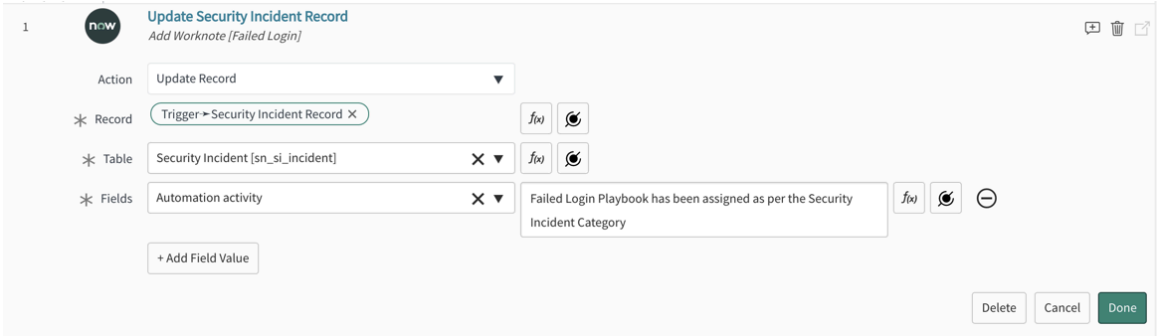


次のステップでは、ログイン失敗手動プレイブック で利用可能なアクション、タスク、およびサブフローについて説明します。

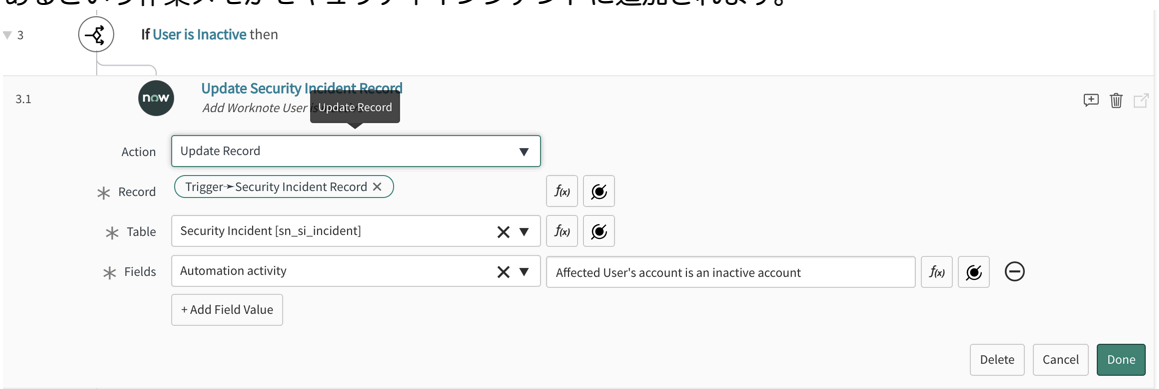
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. プレイブックの実行が開始されると、ステップ 1 で、ログイン失敗カテゴリのセキュリティインシデントがアサインされたことを示す作業メモでプレイブックが自動的に更新されます。



2. ステップ 2 では、プレイブックが更新され、[分析] ステータスに移行します。
3. ステップ 3 で、プレイブックは、影響を受けるユーザーがアクティブ/非アクティブユーザーであるかどうかを確認します。ユーザーが非アクティブの場合、ユーザーアカウントが非アクティブであるという作業メモがセキュリティインシデントに追加されます。

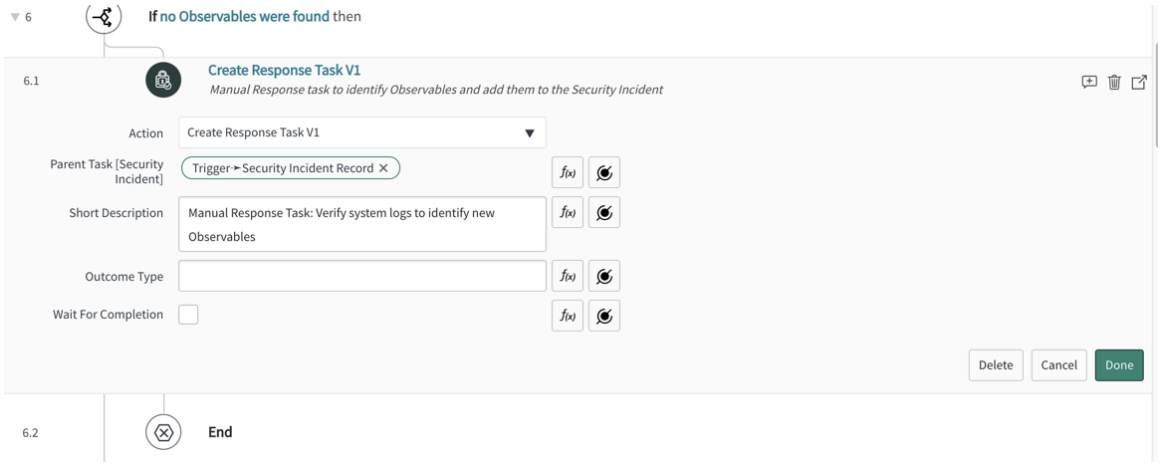


> **注:**
> フローのステップ 3 では、ServiceNow で利用可能な *sn_si_incident* テーブル内の非アクティブなユーザーを確認します。このステップは指針として提供されており、特定の環境に合わせて変更する必要があります。この機能を使用する場合は、お使いの環境で Active Directory 統合を設定することをお勧めします。Active Directory 統合を使用してユーザーステータスを確認し、応答に応じてプレイブックの次のステップを設計できます。
>
> Active Directory 統合を設定していない場合は、セキュリティアナリストが IT チームと協力してユーザーをブロックし、プレイブックの残りの手順を進めるために、このステップを手動タスクで置き換えます。

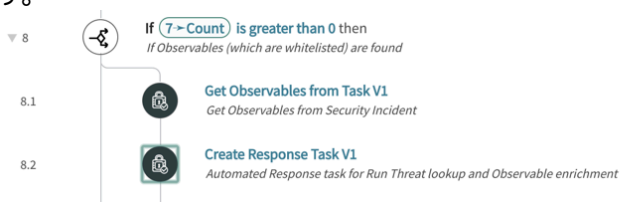
4. ステップ 4 では、セキュリティインシデントの観測事象が取得されます。
5. ステップ 5 では、観測事象が特定されます。
6. 観測事象が見つからない場合は、ステップ 6 で手動応答タスクが作成され、フローが終了します。

自動翻訳

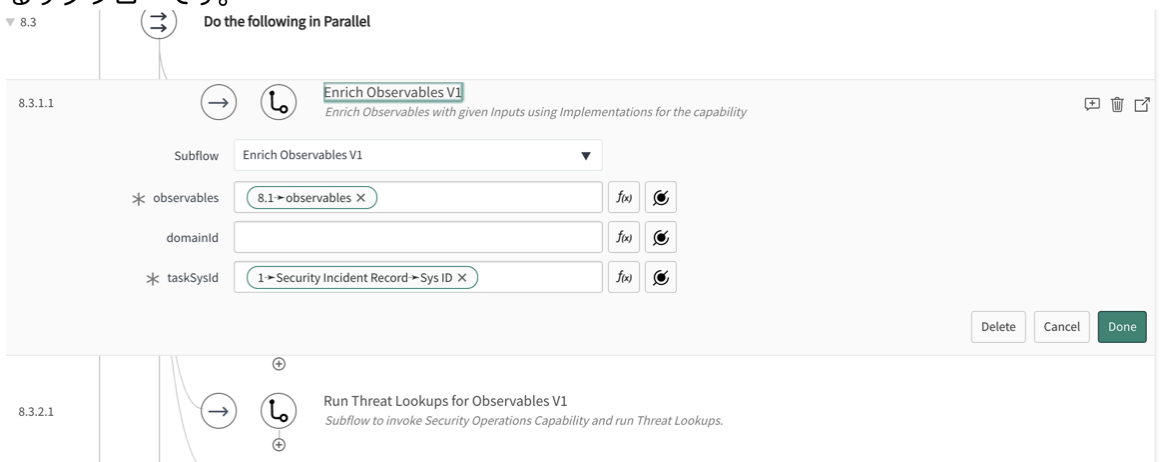
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



7. ステップ 7 で観測事象が見つかった場合、許可リストにない観測事象が特定されます。
8. 少なくとも 1 つの観測事象が許可リストにない場合、次のステップが実行されます。
   a. ステップ 8.1 および 8.2 が実行されます。観測事象が取得され、自動応答タスクが開始されます。



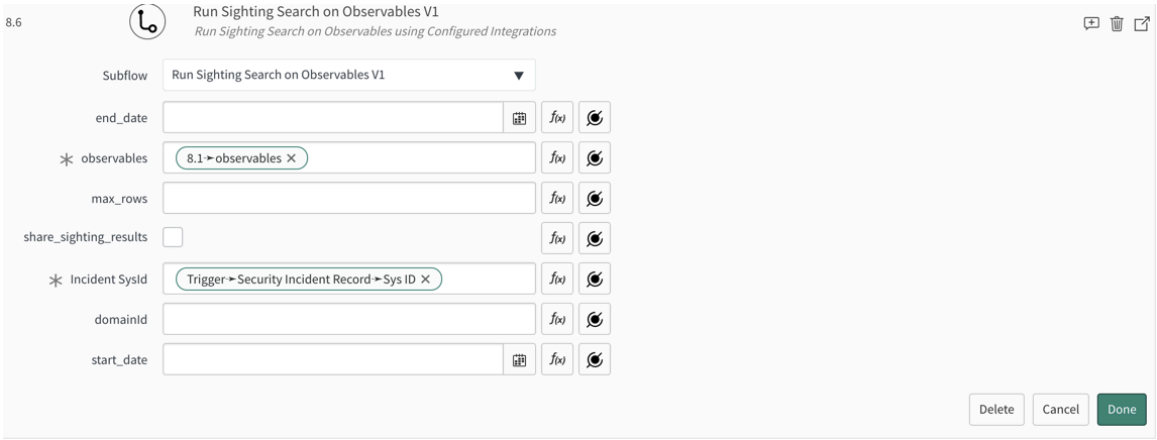
   b. 自動タスクが作成された後、ステップ 8.3 (8.3.1.1 および 8.3.2.1) が実行され、「観測事象を拡張」および「脅威のルックアップ」統合が実行されます。これらはプレイブックに含まれているサブフローです。



   c. ステップ 8.4 で、統合が完了した後、セキュリティインシデントレコードが更新されます。
   d. ステップ 8.5 で、次に実行される自動タスクを示す新しい応答タスクが作成されます。
   e. ステップ 8.6 で、観測事象に対してサイティング検索統合が実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



f. サイティング検索サブフローが完了した後、ステップ 8.7 でセキュリティインシデントが更新されます。

g. ステップ 8.8 で、観測事象が悪意のあるものかどうかが確認されます。

h. 観測事象が悪意のあるものでなく、ユーザーアカウントがアクティブな場合、ログイン試行の失敗を再確認するために自動メールがユーザーに送信されます。観測事象を特定してセキュリティインシデントに追加するために、手動応答タスクが作成されます。プレイブックはこのステージで終了します。

i. 観測事象が悪意のあるものである場合、次の 3 つの応答タスクが作成されます。

i. ログイン試行の失敗を確認するための自動メールがユーザーに送信されます (「はい」または「いいえ」)。ユーザーが「はい」と応答した場合：

1. セキュリティインシデントのステータスが [封じ込め] に更新されます。
2. パスワードをリセットするためのメールがユーザーに送信されます。
3. 「パスワードのリセット」サブフローが開始され、タスクが完了するとメールがユーザーに送信されます。

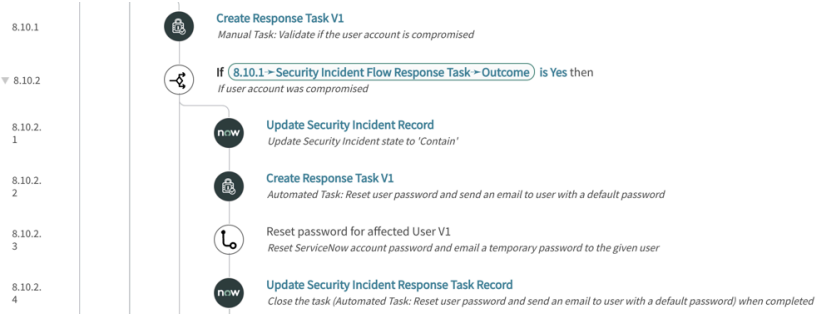
> **注:**
> 「パスワードのリセット」ステップは指針として提供されています。フローのステップでは、ServiceNow システムのユーザーアカウントのパスワードをリセットします。ただし、パスワードをリセットするプロセスは環境によって異なる場合があります。Active Directory 統合を確認して、ユーザーのパスワードを自動的にリセットできます。Active Directory 統合を設定していない場合は、各タスクの完了時に、セキュリティアナリストが IT チームと協力してユーザーのパスワードをリセットし、プレイブックの残りの手順を進めるために、このステップを手動タスクで置き換えます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ii. ユーザーが「いいえ」と応答した場合、応答を再確認するために自動メールがユーザーに送信されます。セキュリティアナリストは、手動で適切なアクションを実行する必要があります。

iii. ユーザーが自動メールに応答しない場合、セキュリティアナリストは、手動でセキュリティインシデントを更新し、応答を提供する必要があります。ユーザーアカウントが侵害されているかどうかを検証するための手動タスクが作成されます。



9. ステップ 8.10.3 で、セキュリティインシデントのステータスが更新されます。
10. ステップ 8.10.4 で、悪意のある IP および URL に対するブロック要求の作成機能の実装が利用可能かどうかを確認する自動タスクが作成されます。機能実装が利用可能な場合は、「ブロック要求の作成」サブフローが実行されます。これを利用できない場合、セキュリティインシデントが更新され、機能実装を利用できないことを示す作業メモが投稿されます。
11. ステップ 9 で、セキュリティインシデントが更新され、ステータスが [レビュー] に更新されます。
12. ステップ 10 で、タスクをクローズする前にインシデントの事後レビューを完了するための応答タスクが作成されます。

子セキュリティインシデント自動化のプレイブック

重複するセキュリティインシデントは子セキュリティインシデントとして分類され、親セキュリティインシデントにロールアップされます。

子セキュリティインシデント自動化プレイブックは、重複するセキュリティインシデントの調査とクローズに必要な時間を短縮するのに役立ちます。このプレイブックは、子セキュリティインシデントの特定の一意のアーティファクト (観測事象、影響を受けるユーザー、CI) を親セキュリティインシデントに自動的にロールアップします。

必須条件

必要なロール：

- sn_si.admin
- flow_designer

スポーク：Security Operations スポークのインストール (sn_sec_spoke)

主な機能

子自動化プレイブックは次の機能をカバーしています。

1. セキュリティインシデントを分析ステージに移動する。
2. 重複を排除し、影響を受けるユーザーと CI を親セキュリティインシデントに追加 (ロールアップ) する。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 子インシデントから親セキュリティインシデントに観測事象を追加する。
4. 親セキュリティインシデントがクローズされたときに、子セキュリティインシデントをクローズまたはキャンセルする。

必要な機能

詳細については、ServiceNow Store を参照してください。

セキュリティアナリストエクスペリエンス

セキュリティ上の脅威を段階的に解決する方法を理解するには、「プレイブックによるセキュリティの脅威の解決」を参照してください。

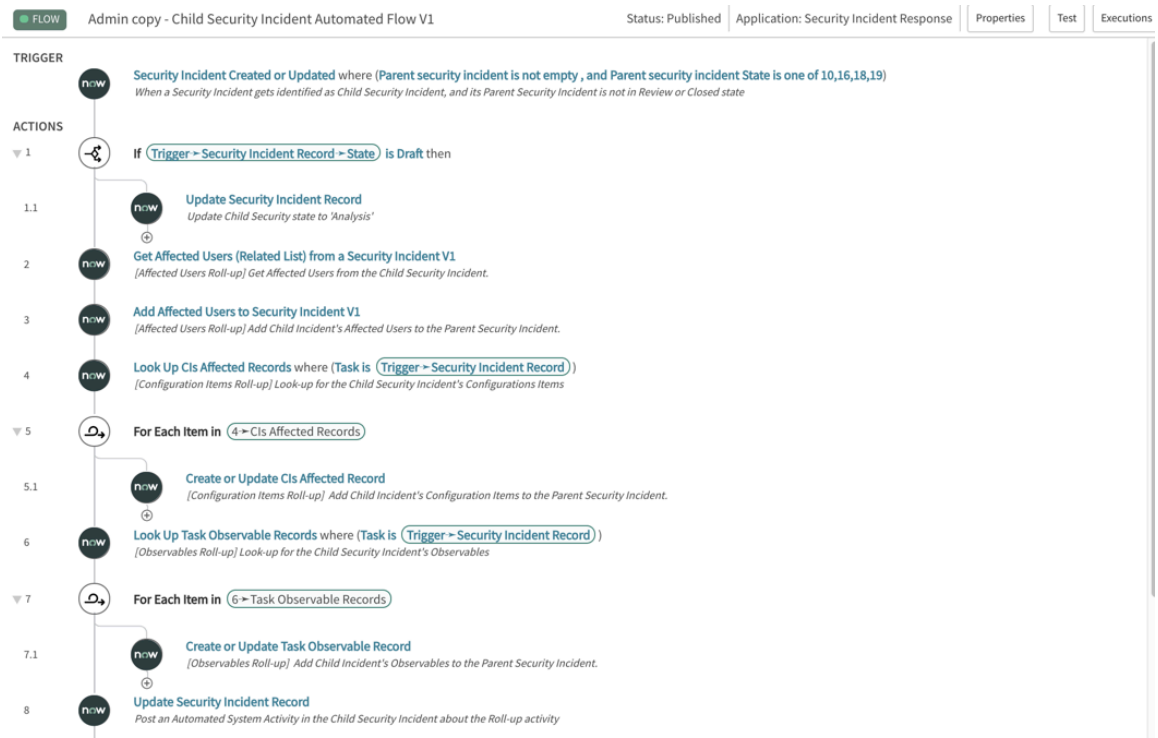
フローデザイナーの機能を使用した子セキュリティインシデント自動化プレイブックの詳細

はじめに

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **Flow Designer** > デザイナー をクリックし、ログイン失敗プレイブックをクリックします。
3. 子セキュリティインシデント自動化プレイブックのコピーを作成し、必要な変更を行います。(これはオプションのステップです。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します)。
4. 要件に応じて必要な変更を行います。(これはオプションのステップです。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します)。
5. プレイブックをアクティブ化します。
   - ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   - 要件に応じて変更を加えた後、コピーしたフローをアクティブ化します。

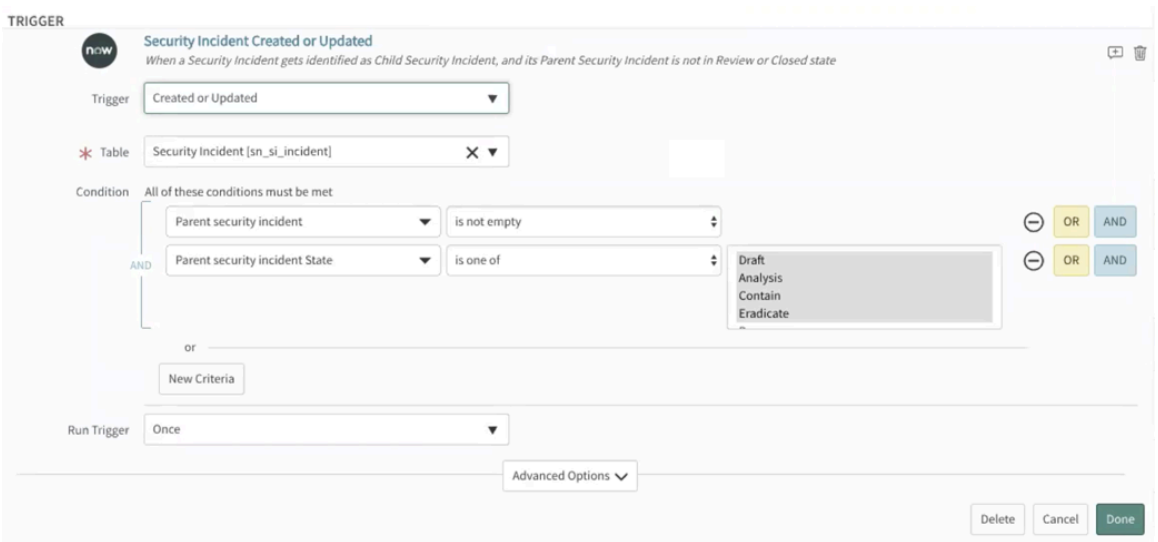
次の画像は、子セキュリティインシデント自動化プレイブックのコピーを示しています。以下の手順では、プレイブックでのさまざまなアクションについて説明しています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



このプレイブックは、次の場合にトリガーされます。

- 親セキュリティインシデントフィールドが空でない。
- 親セキュリティインシデントのステータスが [ドラフト]、[分析]、[封じ込め]、または [根絶] である。

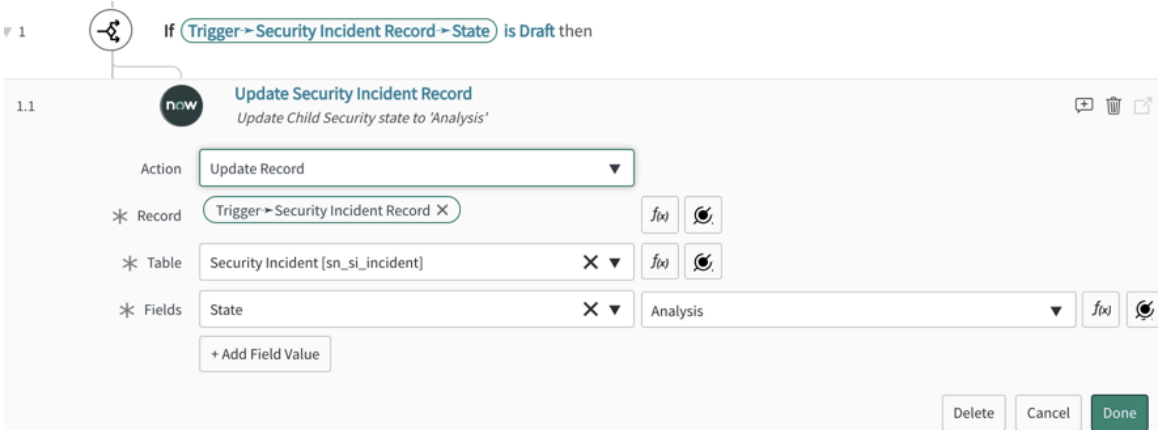


次のステップでは、子セキュリティインシデント自動化プレイブックで利用可能なアクションおよびタスクについて説明します。

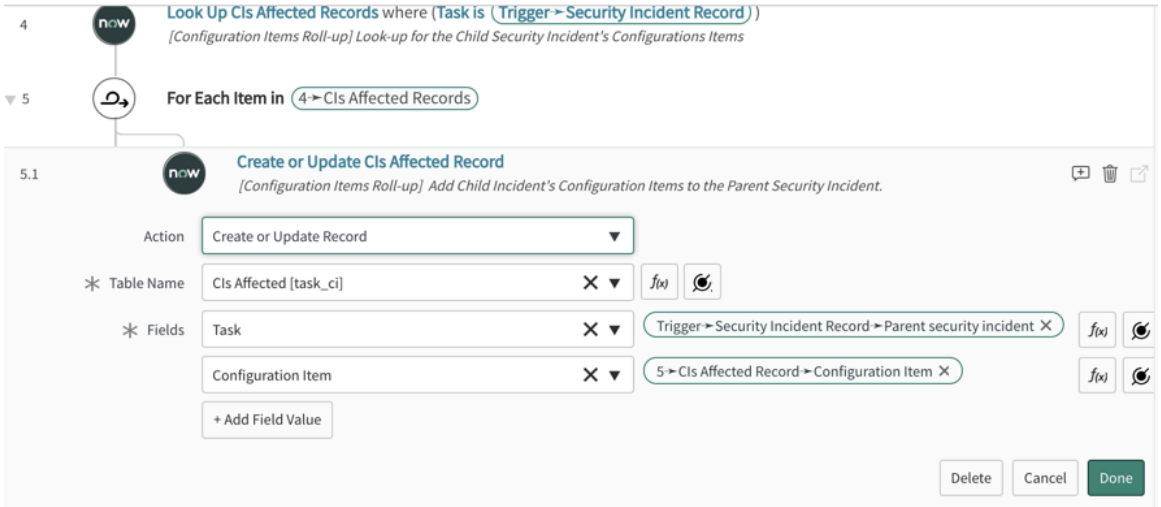
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. プレイブックの実行が開始されると、ステップ 1 でセキュリティインシデントが [ドラフト] ステータスの場合は、更新されて [分析] ステータスに設定されます。



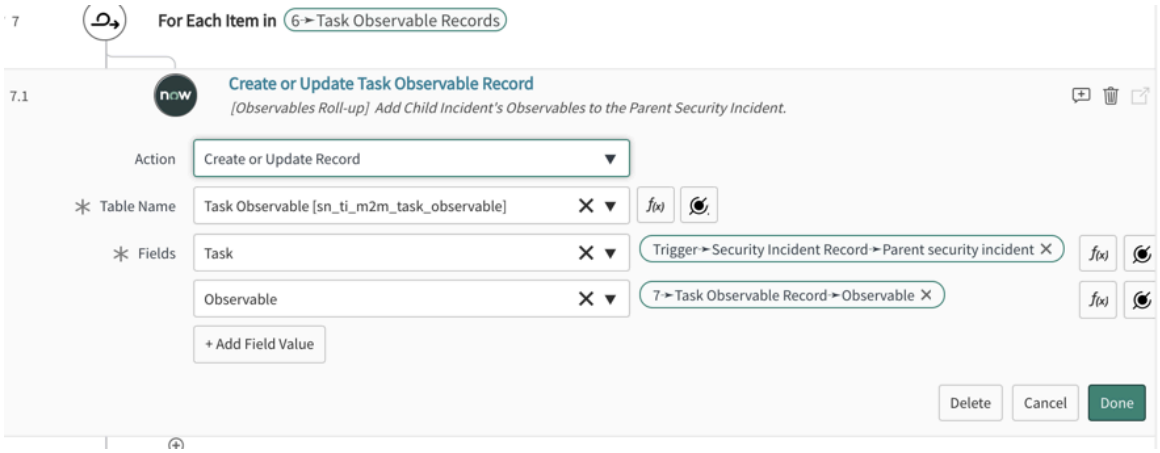
2. ステップ 2 および 3 では、セキュリティインシデントの影響を受けるユーザーが取得され、親セキュリティインシデントにロールアップされます。重複するユーザーは削除されます。
3. ステップ 4 および 5 では、子セキュリティインシデントに関連付けられた構成アイテムが取得され、一意の CI が親セキュリティインシデントにロールアップされます。



4. ステップ 6 および 7 では、子セキュリティインシデントに関連付けられた観測事象が取得され、一意の観測事象が親セキュリティインシデントにロールアップされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. ステップ 8 および 9 では、影響を受けるユーザー、構成アイテム、および観測事象が子セキュリティインシデントから親セキュリティインシデントにロールアップされたことを示す自動作業メモが親および子のセキュリティインシデントに投稿されます。

Office 365 - 悪意のあるファイル検出のプレイブック

このプレイブックでは、Office 365 で検出された悪意のあるファイルを調査するための体系的な修復手順について説明します。

Office 365 で悪意のあるファイルが検出された場合は、フローデザイナーの 365 - 悪意のあるファイル検出プレイブックを手引きとして使用し、これらの悪意のあるファイルの調査を最適化することができます。

Office 悪意のあるファイル検出プレイブックの設定

Office 悪意のあるファイル検出プレイブックを設定するには、次の手順に従います。

始める前に
必要なロール：

- sn_si.admin
- flow_designer

Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

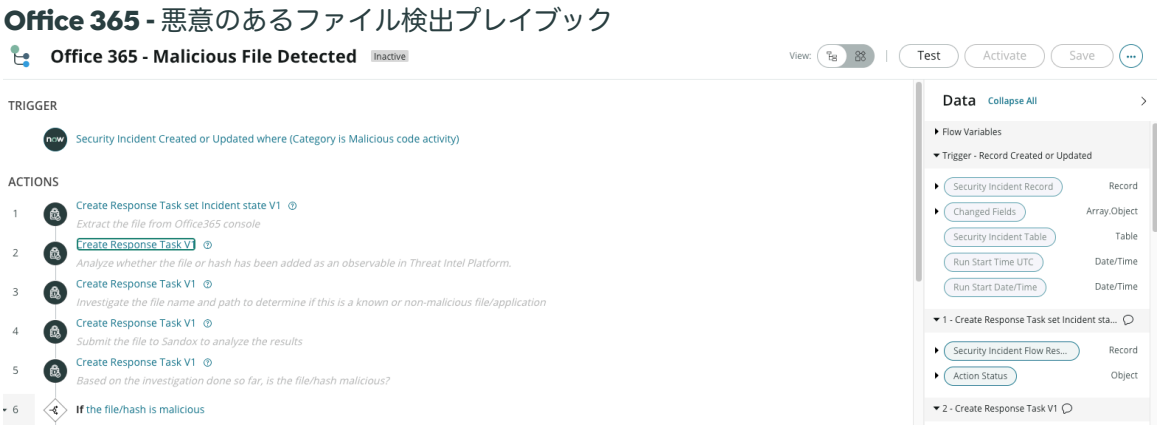
手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 **Office 365 -** 悪意のあるファイル検出 プレイブックを選択します。
3. オプション: Office 365 - 悪意のあるファイル検出プレイブックのフローのコピーを作成し、必要な変更を加えることができます。

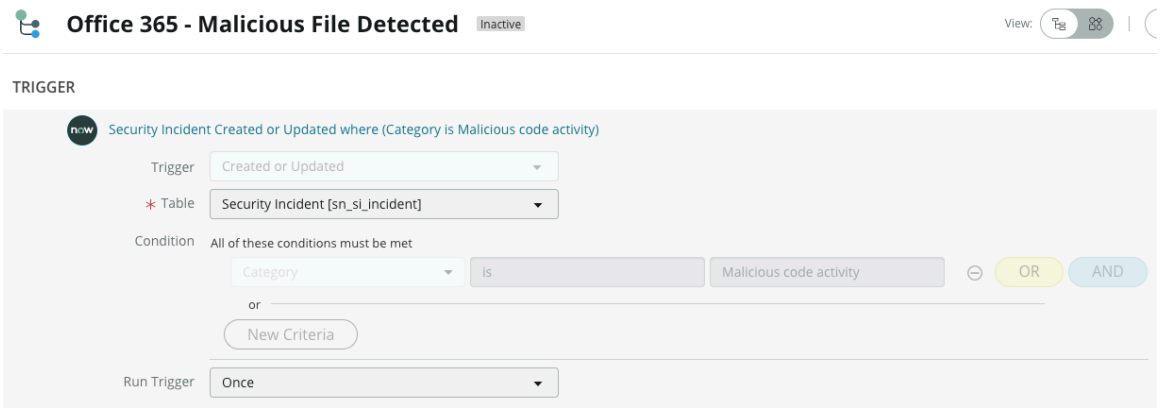
   プレイブックのフローのコピーを作成するには、 アイコンをクリックし、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. プレイブックをアクティブ化します。
   - ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   - 必要な変更を行った後、コピーしたフローをアクティブ化します。
5. プレイブックの [トリガー条件] を設定します。
   このプレイブックは、[カテゴリ] が [悪意のあるコードアクティビティ **(Malicious code activity)**] である場合にトリガーされ、セキュリティインシデントに関連付けられます。



Office 365 - 悪意のあるファイル検出プレイブックを使用する

このプレイブックを使用して、Office 365 で検出された悪意のあるファイルを調査します。以下に示すステップは、Office 365 - 悪意のあるファイル検出プレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

手順

1. プレイブックがトリガーされて実行が開始されたら、アクション 1 で、Office 365 コンソールから悪意のあるファイルを抽出する必要があります。
2. アクション 2 では、ファイルまたはハッシュが脅威インテリジェンスプラットフォームに観測可能として追加されているかどうかを分析する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

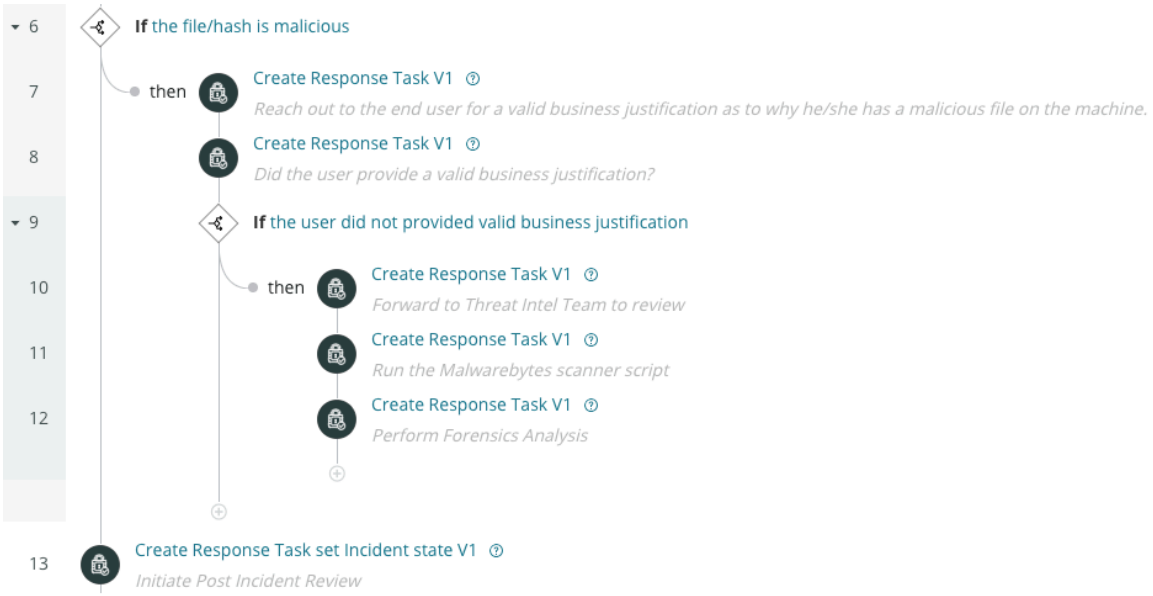
3. アクション 3 では、ファイル名とパスを調査して、既知のファイル/アプリケーションまたは悪意のないファイル/アプリケーションかどうかを判断する必要があります。

4. アクション 4 では、結果を分析するためにファイルをサンドボックスに送信する必要があります。
5. アクション 5 では、これまでに行った調査に基づいて、ファイルまたはハッシュが悪意のあるものかどうかを確認する必要があります。
   ファイルまたはハッシュが悪意のあるものでない場合は、アクション 5 で手動応答タスクが作成され、フローが終了します。
6. アクション 6 では、ファイルまたはハッシュが悪意のあるものである場合に、アクション 7 および 8 が実行されます。
7. アクション 7 では、デバイス上に悪意のあるファイルがある理由について、有効なビジネス上の根拠をエンドユーザーに問い合わせる必要があります。
   ファイルまたはハッシュが悪意のあるものである場合は、プレイブックの既存のメールテンプレートを使用して、エンドユーザーにメールを送信して説明を求めることができます。
8. アクション 8 では、エンドユーザーが有効なビジネス上の根拠を提供したかどうかを確認する必要があります。
   エンドユーザーが有効なビジネス上の根拠を提供した場合は、アクション 5 で、手動応答タスクが作成され、フローが終了します。
9. アクション 9 では、ユーザーが有効なビジネス上の根拠を提供しなかった場合に、アクション 10、11、および 12 が実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

悪意のあるファイルのビジネス上の根拠



10. アクション 10 では、有効なビジネス上の根拠がなかったため、悪意のあるファイルまたはハッシュを確認のために脅威インテリジェンスチームに転送することができます。
11. アクション 11 では、マルウェアバイトスキャナースクリプトを実行して、ファイルまたはハッシュが悪意のあるものかどうかを確認する必要があります。
12. アクション 12 では、フォレンジック分析を実行して、ファイルまたはハッシュが悪意のあるものであるかどうかを確認する必要があります。
13. アクション 13 では、タスクをクローズする前にインシデントの事後レビューを完了するための応答タスクが作成されます。

反復検出のプレイブック

このプレイブックは、インシデント応答が過去にそのものまたは類似のフィッシングレポートで提供されたかどうか、および同じように新しいレポートでも自動的に機能するかどうかを判断するのに役立ちます。

反復検出プレイブックは、新しく報告されたフィッシングインシデントが過去のインシデントに類似しているかどうかを確認します。反復検出が特定されると、一致したセキュリティインシデントと解決の詳細がアナリストに提供され、アナリストはそれを新たに報告されたインシデントで使用できるため、セキュリティインシデントを迅速に修復できます。

反復検出プレイブックの設定

反復検出プレイブックを設定するには、次の手順に従います。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。次のシステムプロパティを変更するオプションがあります。

- *sn_sec_spoke.similarphish.earlyterminationscore*
- *sn_sec_spoke.similarphish.lookbackdays*

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

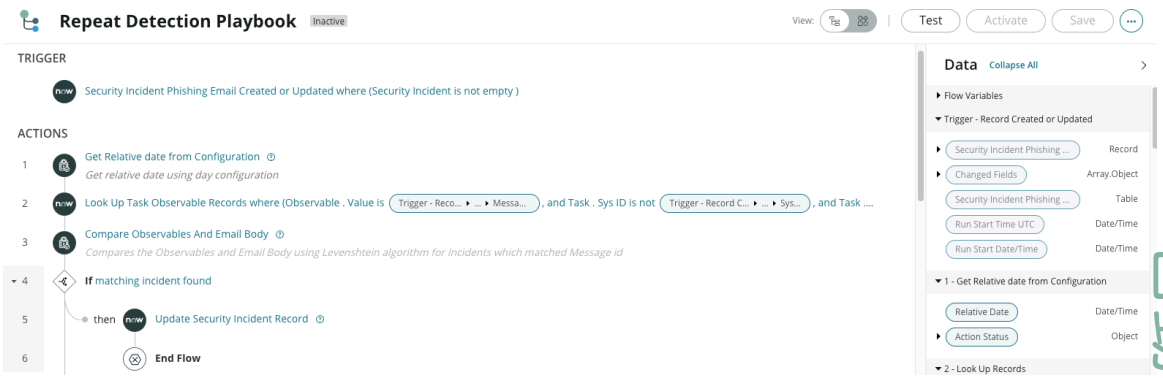
- *sn_sec_spoke.similarphish.maxcomparisonsize*
- *sn_sec_spoke.similarphish.minmatchscore*

手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 反復検出 プレイブックを選択します。
3. オプション: 反復検出プレイブックのフローのコピーを作成し、必要な変更を加えることができます。

   プレイブックのフローのコピーを作成するには、 アイコンをクリックし、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

   反復検出プレイブック

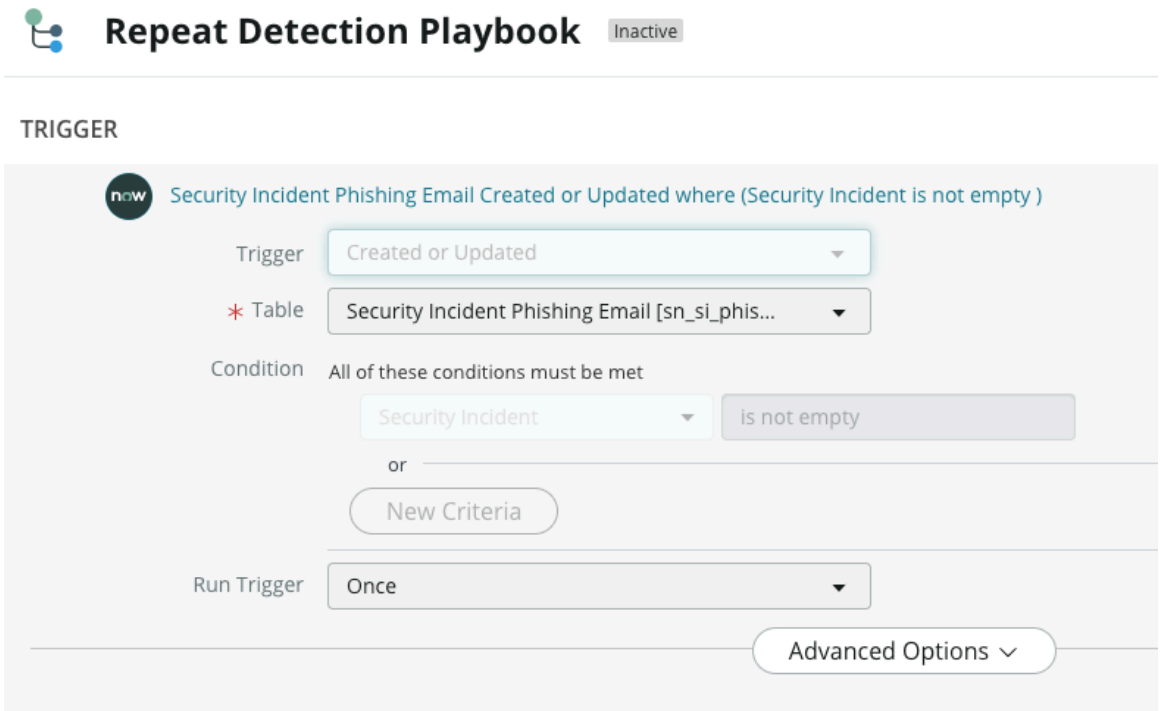
   

4. プレイブックをアクティブ化します。
   - ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   - 必要な変更を行った後、コピーしたフローをアクティブ化します。
5. プレイブックの [トリガー条件] を設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このプレイブックは、[セキュリティインシデント] が [空でない **(is not empty)]** 場合にトリガーされます。



反復検出プレイブックを使用する

このプレイブックを使用して、インシデントレスポンスが過去にそのものまたは類似のフィッシングレポートで提供されたかどうか、および同じように新しいレポートでも自動的に機能するかどうかを調査します。以下に示すステップは、反復検出プレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

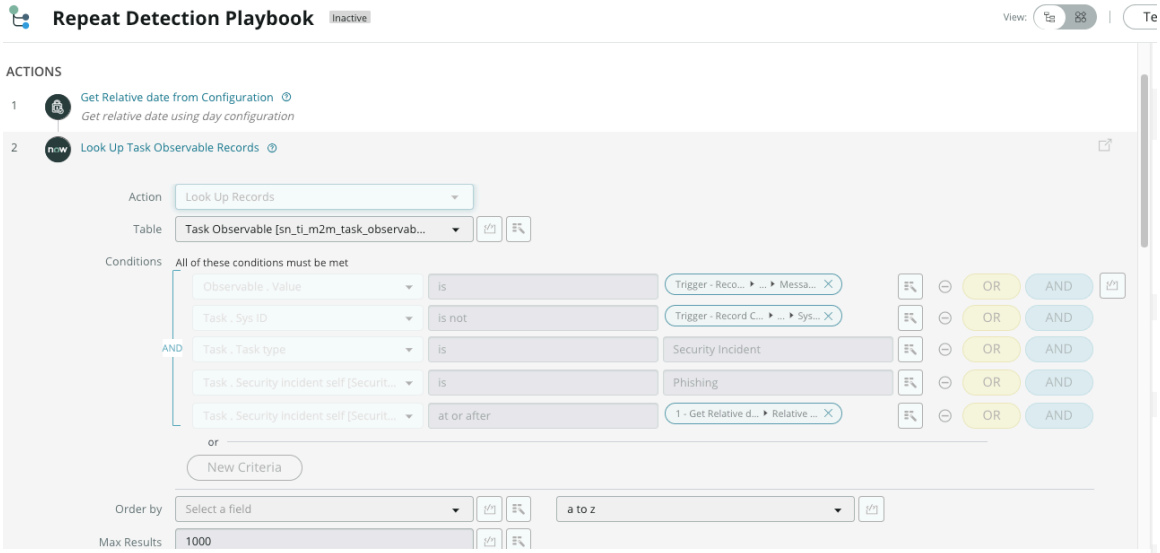
手順

1. プレイブックがトリガーされて実行が開始されると、アクション 1 で、プレイブックは日の構成を使用してセキュリティインシデントの相対日付を取得します。
2. アクション 2 では、プレイブックはメッセージ ID に基づいてインシデントと一致するテーブル *sn_ti_m2m_task_observable* のタスク観測可能レコードを検索します。

自動翻訳

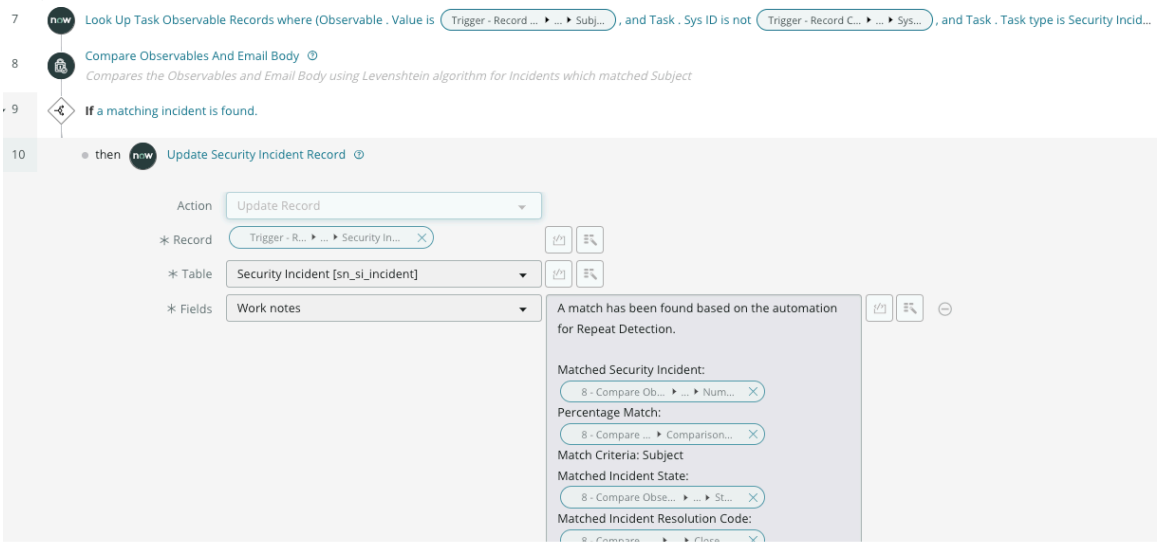
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

反復検出プレイブック



3. アクション 3 では、プレイブックは、メッセージ ID と一致したインシデントのレーベンシュタインアルゴリズムを使用して、タスク観測事象とメール本文を比較します。
4. アクション 4 では、これまでに行った調査に基づいて、プレイブックはメッセージ ID に基づいて一致するインシデントが見つかったかどうかを確認します。
   アクション 5 では、一致するインシデントが見つかった場合に、プレイブックは繰り返し検出の自動化に基づいて一致が見つかった作業メモを自動的に更新します。アクション 6 で、フローは終了します。
5. 一致するインシデントが見つからなかった場合に、アクション 7 で、プレイブックは件名に基づいてインシデントと一致するテーブル *sn_ti_m2m_task_observable* のタスク観測可能レコードを検索します。
6. アクション 8 では、プレイブックは、件名と一致したインシデントのレーベンシュタインアルゴリズムを使用して、タスク観測事象とメール本文を比較します。
7. アクション 9 では、プレイブックは一致するインシデントが見つかったかどうかを確認します。
   アクション 10 では、一致するインシデントが見つかった場合に、プレイブックは繰り返し検出の自動化に基づいて一致が見つかった作業メモを自動的に更新します。アクション 11 で、フローは終了します。

一致するインシデント



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

8. アクション 12 では、プレイブックはアドレスに基づいてインシデントと一致するテーブル *sn_ti_m2m_task_observable* のタスク観測可能レコードを検索します。
9. アクション 13 では、プレイブックは、アドレスと一致したインシデントのレーベンシュタインアルゴリズムを使用して、タスク観測事象とメール本文を比較します。
10. アクション 14 では、プレイブックはアドレスに基づいて一致するインシデントが見つかったかどうかを確認します。
アクション 15 では、一致するインシデントが見つかった場合に、プレイブックは繰り返し検出の自動化に基づいて一致が見つかった作業メモを自動的に更新します。アクション 16 で、フローは終了します。

なりすましメール (同じ表示名を使用) のプレイブック

このプレイブックでは、なりすまし名が用いられたメールが組織の従業員に送信されたときにトリガーされる、なりすましメールを調査するための体系的な修復手順について説明します。

なりすましメールプレイブックの設定

なりすましメールプレイブックを設定するには、次の手順に従います。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

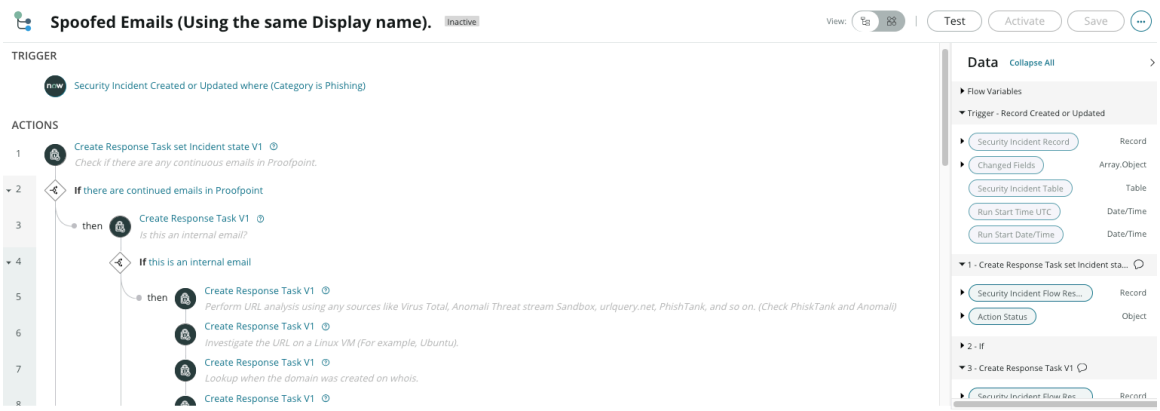
Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 なりすましメール (同じ表示名を使用) プレイブックを選択します。
3. オプション: 反復検出プレイブックのフローのコピーを作成し、必要な変更を加えることができます。

   プレイブックのフローのコピーを作成するには、 アイコンをクリックし、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

   なりすましメールプレイブック

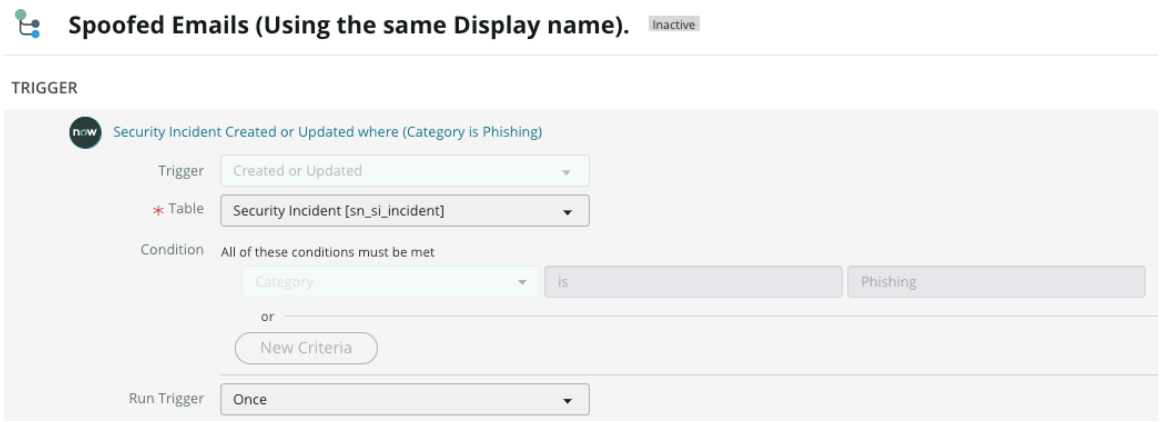
4. プレイブックをアクティブ化します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
- 必要な変更を行った後、コピーしたフローをアクティブ化します。

5. プレイブックの [トリガー条件] を設定します。

   このプレイブックは、[カテゴリ] が [フィッシング] である場合にトリガーされ、セキュリティインシデントに関連付けられます。



なりすましメール (同じ表示名を使用) プレイブックを使用する

このプレイブックを使用して、なりすまし名が用いられたメールが組織の従業員に送信されたときにトリガーされる、なりすましメールを調査します。以下に示すステップは、なりすましメール (同じ表示名を使用) プレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

手順

1. プレイブックがトリガーされて実行が開始されたら、アクション 1 で、Proofpoint に継続的なないなりすましメールがないかどうかを確認する必要があります。
2. アクション 2 では、Proofpoint に継続的なメールがある場合に、それが内部のなりすましメールであるかどうかを確認します。
3. アクション 3 では、それが内部のなりすましメールである場合に、次のアクションを実行します。

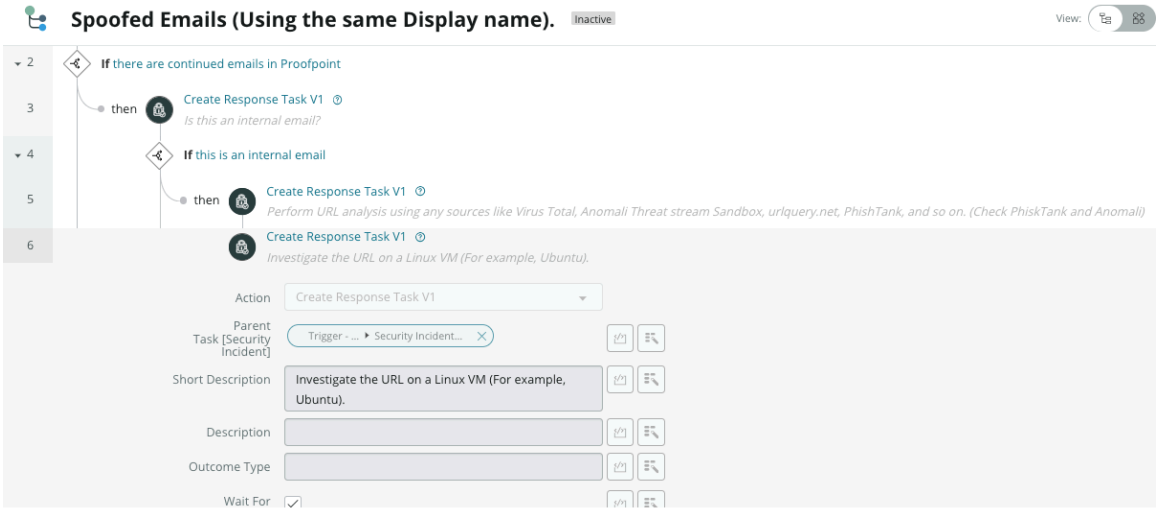
   a. アクション 5 では、Virus Total、Anomali Threat Stream Sandbox、urlquery.net、PhishTank などのソースを使用して URL 分析を実行する必要があります (たとえば、PhiskTank と Anomali を確認します)。

   b. アクション 6 では、Linux VM (Ubuntu など) 上の URL を調査する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

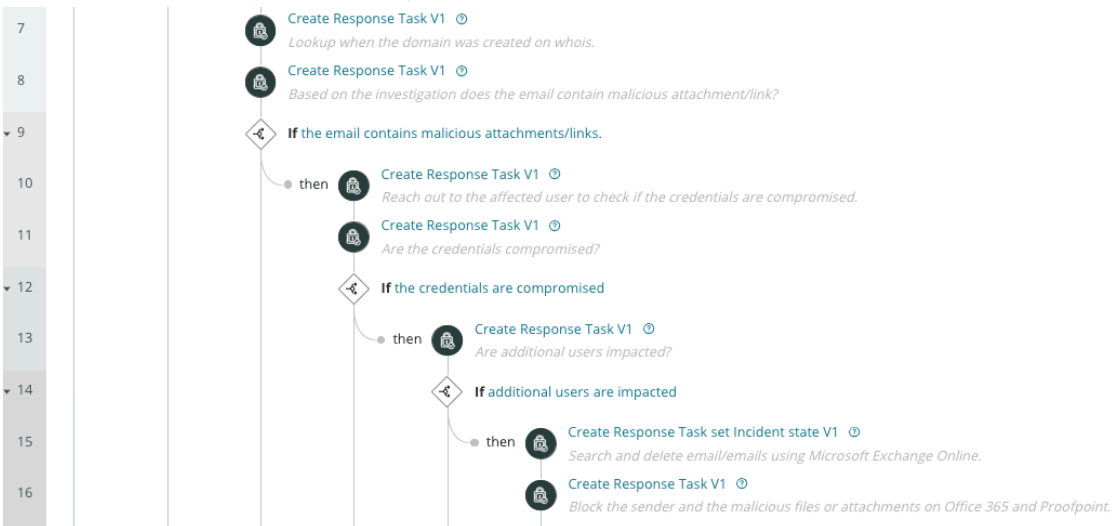
なりすましメール (同じ表示名を使用) プレイブック



c. アクション 7 では、WHOIS でドメインがいつ作成されたかを調べる必要があります。疑わしくフィッシング攻撃の可能性が高い、最近 (先週内に) 登録されたドメインを探します。

d. アクション 8 では、これまでに行われた調査に基づいて、このメールに悪意のある添付ファイルまたはリンクが含まれているかどうかを確認する必要があります。
このメールに悪意のある添付ファイルまたはリンクが含まれていない場合、フローは終了します。

なりすましメールに悪意のある添付ファイルまたはリンクが含まれている



e. アクション 9 では、メールに悪意のある添付ファイルまたはリンクが含まれている場合に、次のアクションを実行します。

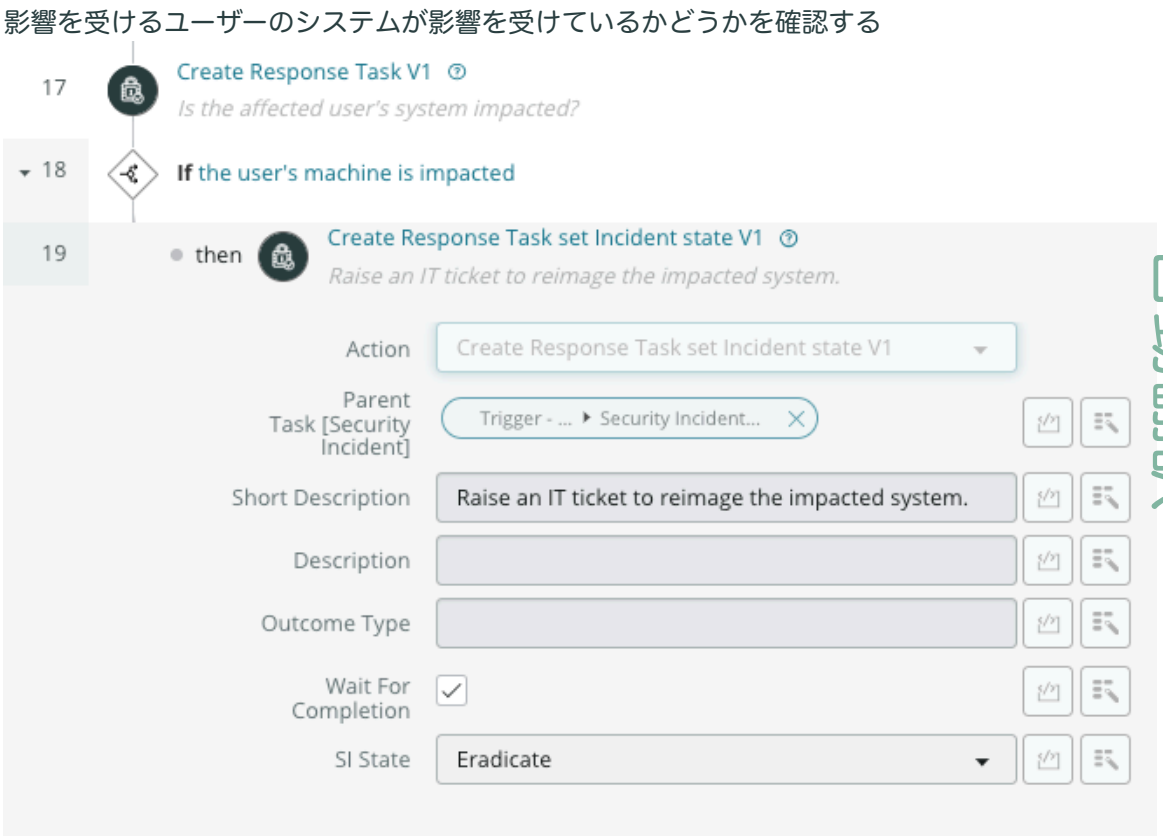
i. アクション 10 では、影響を受けているユーザーに連絡して、認証情報が侵害されていないかどうかを確認する必要があります。提供されたメールテンプレートを使用して、影響を受けるユーザーに連絡できます。

ii. アクション 11 では、メールの応答に基づいて、認証情報が侵害されているかどうかを確認する必要があります。認証情報が侵害されていなければ、フローは終了します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. アクション 12 では、認証情報が侵害されていた場合に、アクション 13 で、さらに別のユーザーが影響を受けているかどうかを確認する必要があります。別のユーザーが影響を受けていない場合、フローは終了します。
2. アクション 14 では、別のユーザーが影響を受けていた場合に、次のアクションを実行します。
   a. アクション 15 では、Microsoft Exchange Online を使用してメールを検索および削除する必要があります。
   b. アクション 16 では、Office 365 と Proofpoint の送信者と悪意のあるファイルまたは添付ファイルをブロックする必要があります。

4. アクション 17 では、これが内部のなりすましメールでない場合に、影響を受けるユーザーのシステムが影響を受けているかどうかを確認する必要があります。
5. アクション 18 では、ユーザーのシステムが影響を受けている場合に、アクション 19 で、IT チケットを発行して、影響を受けるシステムを再イメージ化します。



6. アクション 20 では、タスクをクローズする前にインシデントの事後レビューを完了するための応答タスクが作成されます。

エンドポイント検出のプレイブック

このプレイブックでは、ホストまたはエンドポイントでトリガーされたマルウェアアラート (悪意のあるファイルの検出など) を調査するための体系的な修復手順について説明します。

ホストまたはエンドポイントで CrowdStrike アラートがトリガーされた場合は、フローデザイナーのエンドポイント検出プレイブックを手引きとして使用し、これらの悪意のあるファイルの調査を最適化することができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エンドポイント検出プレイブックの設定

エンドポイント検出プレイブックを設定するには、次の手順に従います。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

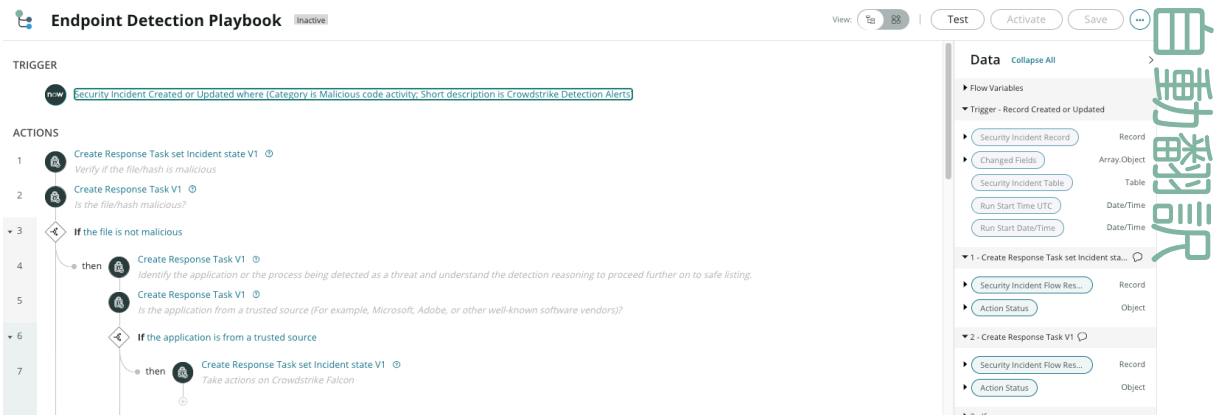
Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 エンドポイント検出 プレイブックを選択します。
3. オプション: エンドポイント検出プレイブックのフローのコピーを作成し、必要な変更を加えることができます。

   プレイブックのフローのコピーを作成するには、 アイコンをクリックし、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

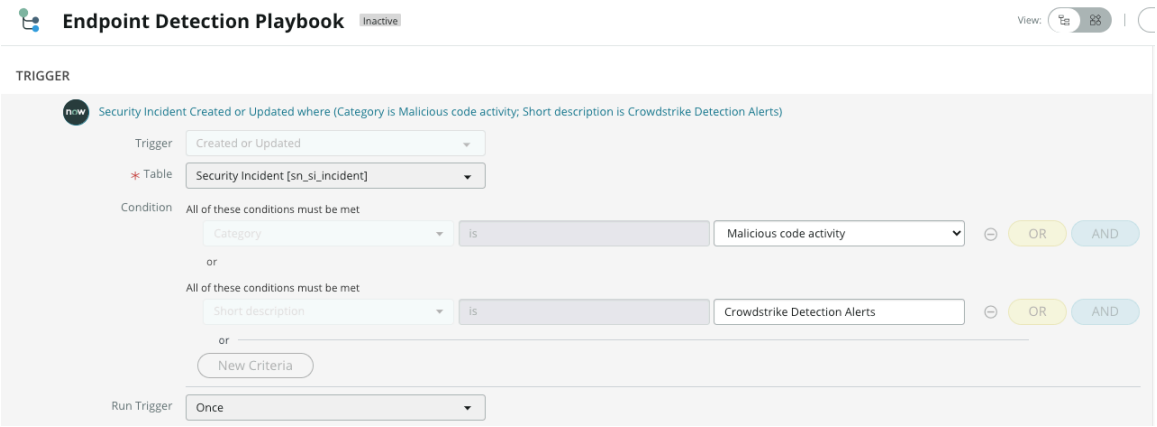
   エンドポイント検出プレイブック

4. プレイブックをアクティブ化します。
   - ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   - 必要な変更を行った後、コピーしたフローをアクティブ化します。
5. プレイブックの [トリガー条件] を設定します。
   このプレイブックは、次の条件が満たされるとトリガーされ、セキュリティインシデントに関連付けられます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [カテゴリ] が [悪意のあるコードアクティビティ] である。
- [簡単な説明] が **[CrowdStrike** 検出アラート **(CrowdStrike Detection Alerts)]** である。



エンドポイント検出プレイブックを使用する

このプレイブックを使用して、ホストまたはエンドポイントでトリガーされたマルウェアアラートを調査します。以下に示すステップは、エンドポイント検出プレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

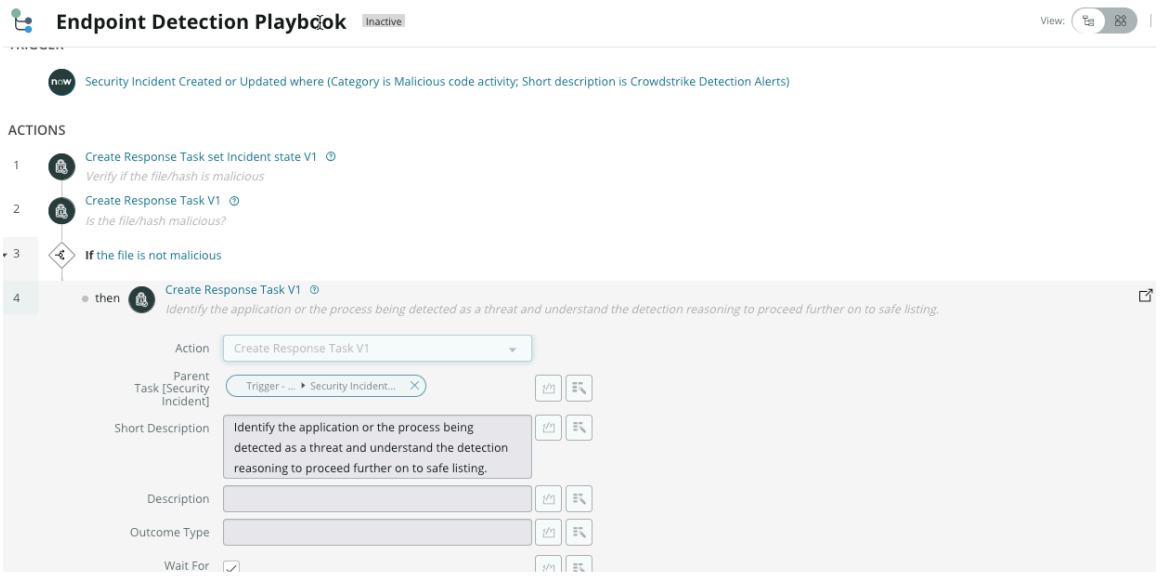
1. プレイブックがトリガーされて実行が開始されたら、アクション 1 で、SIR で脅威のルックアップの結果を分析し、VirusTotal、WildFire、ThreatCrowd などから情報を収集して、ファイルまたはハッシュが悪意のあるものかどうかを確認する必要があります。
2. アクション 2 では、ファイルまたはハッシュが悪意のあるものかどうかを確認する必要があります。
3. アクション 3 では、ファイルまたはハッシュが悪意のあるものであった場合に、次のアクションを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. アクション 4 では、検出されたアプリケーションまたはプロセスを脅威と特定し、検出の理由に関する情報を収集して、セーフリストに進む必要があります。

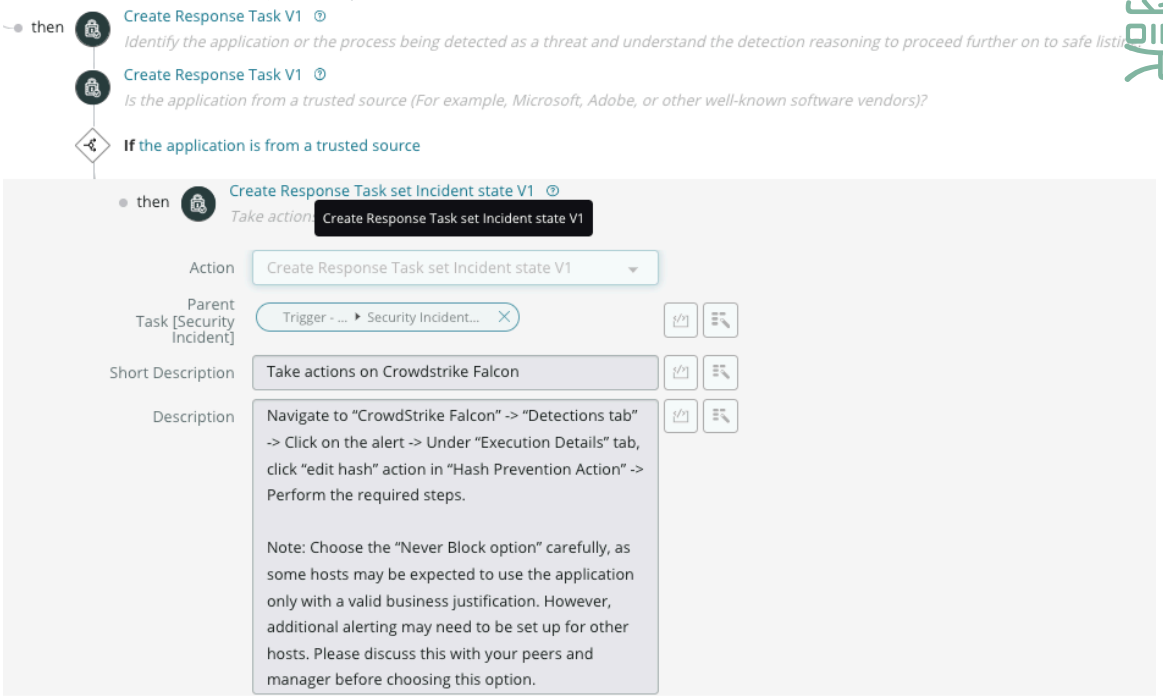
エンドポイント検出プレイブック



b. アクション 5 では、アプリケーションが信頼できるソース (Microsoft、Adobe、またはその他の有名なソフトウェアベンダーなど) からのものであるかどうかを確認する必要があります。

c. アクション 6 では、アプリケーションが信頼できるソースからのものである場合に、CrowdStrike Falcon アラートに対してアクションを実行する必要があります。

CrowdStrike Falcon アラート



d. アクション 7 で、次のアクションを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

i. 次のように移動する。 **CrowdStrike Falcon** > 検出 学習します。

ii. CrowdStrike Falcon アラートをクリックします。

iii. [実行の詳細] タブで、[ハッシュ防止アクション (Hash Prevention Action)] の [ハッシュの編集 **(Edit Hash)]** アクションをクリックします。

iv. 必要な手順を実行します。

> **注:**
> 特定のホストにしか有効なビジネス上の根拠があるアプリケーションの使用が許可されなくなる可能性があるため、[ブロックしない **(Never Block)]** オプションは慎重に選択してください。ただし、他のホストに対して追加のアラートを設定することが必要な場合があります。

e. アクション 8 では、アプリケーションが信頼できるソースからのものでない場合に、デバイスからファイルまたはアプリケーションをローカルで放棄するかどうかを選択する必要があります。
アクション 10 では、デバイスからファイルまたはアプリケーションをローカルで放棄する場合に、次のアクションを実行します。

i. アクション 11 では、[隔離されたファイル] タブに移動し、デバイス名を検索してエンドポイントをフィルタリングします。

ii. ローカルで放棄する必要があるファイルを選択し、[リリース] をクリックします。

> **注:**
> - ファイルは引き続きこの特定のエンドポイントで実行されます。ただし、検出と隔離は他のすべてのホストで引き続き実行されます。
> - 複数のホストで隔離ファイルを一括解放するには、適切なファイル名とステータスを選択します。[選択] をクリックし、[リリース] を選択します。

アクション 12 で、デバイスからローカルにファイルまたはアプリケーションを放棄しない場合は、承認されたアプリケーションのインストールを要求するためにユーザーを IT サポートにリダイレクトできます。

4. アクション 14 では、ファイルまたはハッシュが悪意のあるものであった場合に、次のアクションを実行します。

a. アクション 15 では、ユーザーのロール (機密情報を処理する部署または役職)、アプリケーションの種類 (ランサムウェア、ルートキットなど)、およびアプリケーションの影響 (影響を受けたユーザーの数) に基づいて、ファイル/ハッシュが高リスクか低リスクかを判断する必要があります。

b. アクション 16 では、ファイルが高リスクファイルの場合に、次のアクションを実行します。

i. アクション 17 では、脅威インテリジェンスチームとともに結果を確認します。

ii. アクション 18 では、ファイルに対してマルウェアバイトスキャンを実行します。

iii. アクション 19 では、フォレンジック分析を開始します。

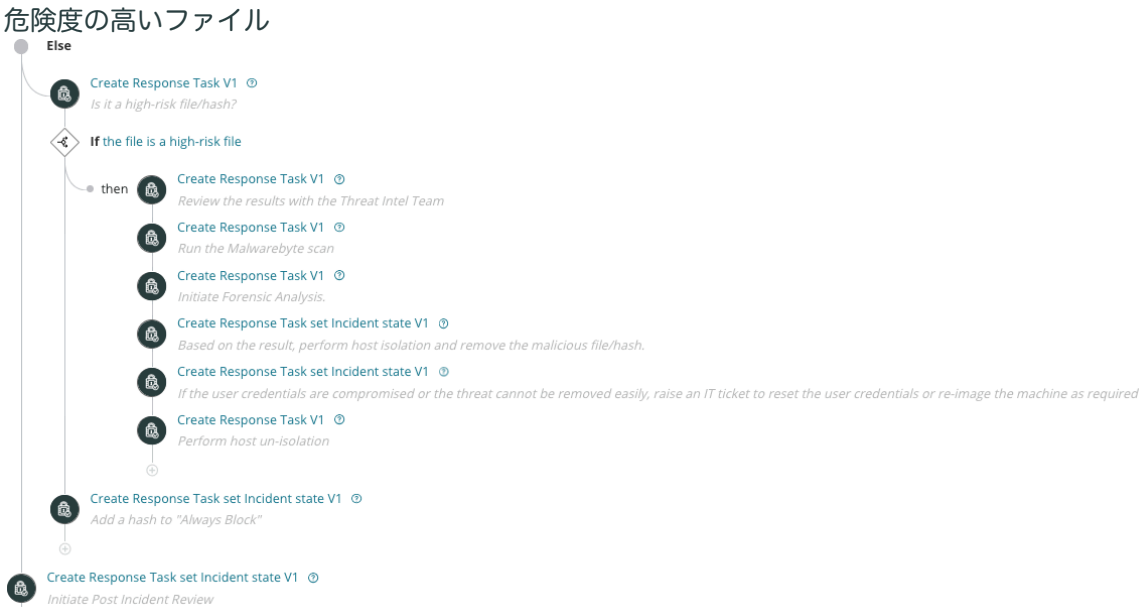
iv. アクション 20 では、フォレンジック分析の結果に基づいてホストの隔離を実行し、悪意のあるファイル/ハッシュを削除します。

v. アクション 21 では、ユーザー認証情報が侵害された場合、または脅威を簡単に除去できない場合に、IT チケットを発行してユーザー認証情報をリセットするか、必要に応じてマシンを再イメージ化します。

vi. アクション 22 では、ホストの隔離解除を実行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳



c. アクション 23 では、ファイルが高リスクファイルの場合に、次のアクションを実行します。

i. 次のように移動する。 **CrowdStrike Falcon** > 構成 学習します。

ii. [構成] タブから、 防止ハッシュ > > アップロードハッシュ > ハッシュの追加.

iii. 必要な OS を選択し、[常にブロック **(Always Block)]** を選択します。

5. アクション 24 で、タスクをクローズする前にインシデントの事後レビューを完了するための応答タスクが作成されます。

パスワードスプレーの可能性のプレイブック

このプレイブックでは、複数のログイン失敗 (同じユーザーの複数の IP アドレスからの認証失敗が多すぎる) によってトリガーされたパスワードスプレーアラートを調査するための体系的な修復手順について説明します。

パスワードスプレーの可能性プレイブックの設定

パスワードスプレーの可能性プレイブックを設定するには、次の手順に従います。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。

2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 パスワードスプレーの可能性プレイ ブックを選択します。

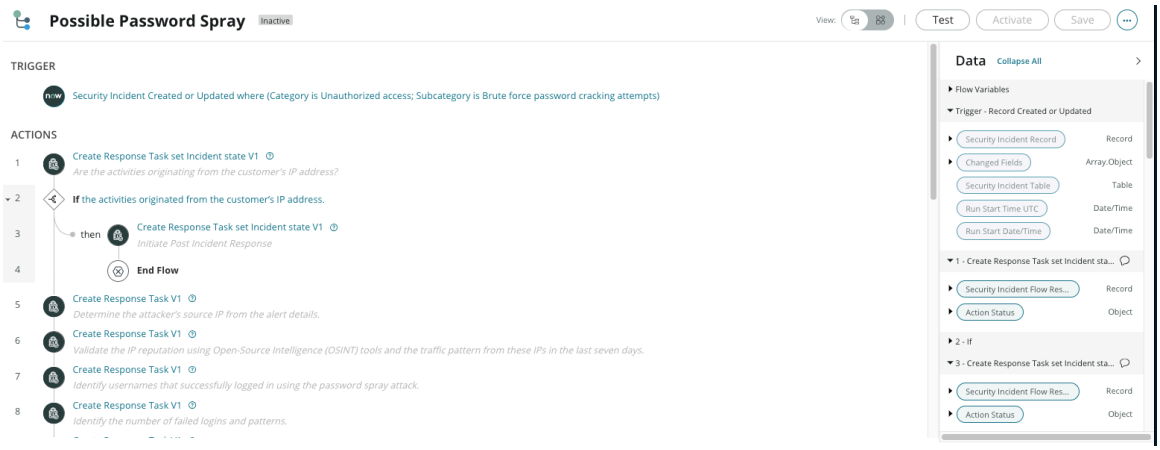
3. オプション: パスワードスプレーの可能性プレイブックのフローのコピーを作成し、必要な変更を加えることができます。

自動翻訳

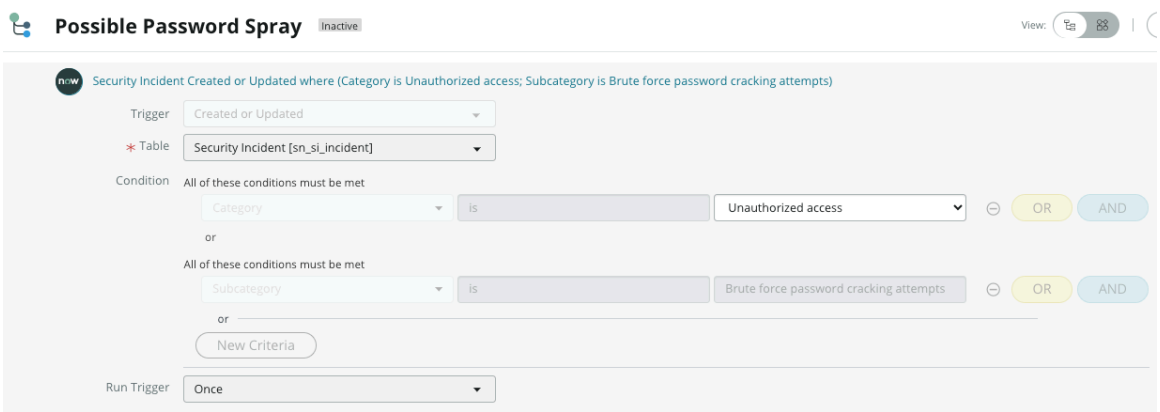
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プレイブックのフローのコピーを作成するには、 アイコンをクリックし、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

パスワードスプレーの可能性プレイブック



4. プレイブックをアクティブ化します。
   - ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   - 必要な変更を行った後、コピーしたフローをアクティブ化します。
5. プレイブックの [トリガー条件] を設定します。
   このプレイブックは、次の条件が満たされるとトリガーされ、セキュリティインシデントに関連付けられます。
   - [カテゴリ] は [無許可のアクセス] です。
   - [サブカテゴリ] は [総当たりパスワード攻撃の試行] です。



パスワードスプレーの可能性プレイブックを使用する

このプレイブックを使用して、複数のログイン失敗 (同じユーザーの複数の IP アドレスからの認証失敗が多すぎる) によってトリガーされたパスワードスプレーアラートを調査します。以下に示すステップは、パスワードスプレーの可能性プレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に
必要なロール：

- sn_si.admin
- flow_designer

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

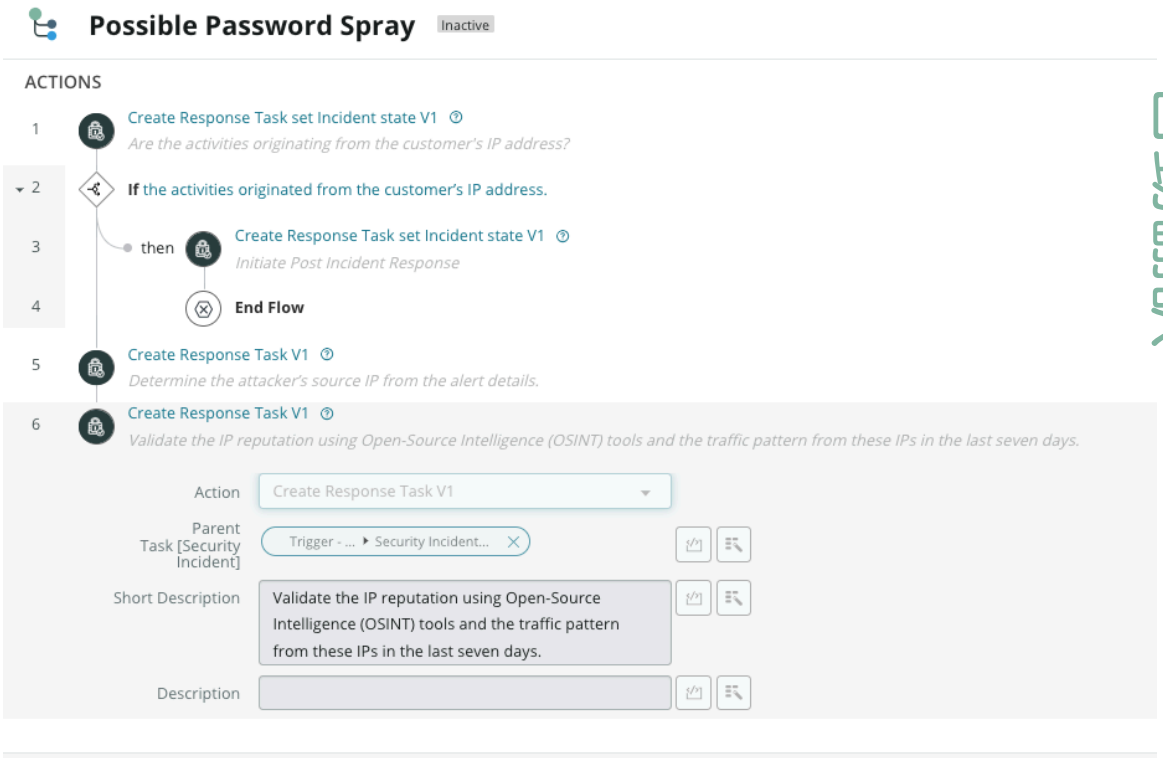
自動翻訳

Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

1. プレイブックがトリガーされて実行が開始されたら、アクション 1 で、アクティビティが顧客の IP アドレスから発信されているかどうかを確認する必要があります。
   パスワードスプレー攻撃を実行している IP アドレスを特定します。たとえば、アラートの TXID (トランザクション ID) を使用して、F5 ログと照合します。
2. アクション 2 では、アクティビティが顧客の IP アドレスから発信された場合に、次のアクションを実行します。
   a. アクション 3 では、パスワードスプレー攻撃の可能性に関するインシデント後のレビューを開始する必要があります。
   b. アクション 4 で、フローは終了します。
3. アクション 5 では、アクティビティが顧客の IP アドレスから発信されていない場合に、アラートの詳細から攻撃者のソース IP を特定します。
4. アクション 6 では、オープンソースインテリジェンス (OSINT) ツールを使用して IP レピュテーションを検証し、さらに過去 7 日間のこれらの IP からのトラフィックパターンを検証する必要があります。

パスワードスプレーの可能性プレイブック



5. アクション 7 では、パスワードスプレー攻撃を使用して正常にログインしたユーザー名を特定する必要があります。
6. アクション 8 では、失敗したログイン数とパターンを特定する必要があります。
7. アクション 9 では、真陽性のインジケーターを特定する必要があります。
   - 過去 60 日間のソース IP からのトラフィックを確認します。履歴トラフィックは、真陽性のインジケーターにはなりません。
   - 認証失敗があるユーザー名パターンとカウントを確認します。カウントが大きいほど、真陽性である確率が高くなります。

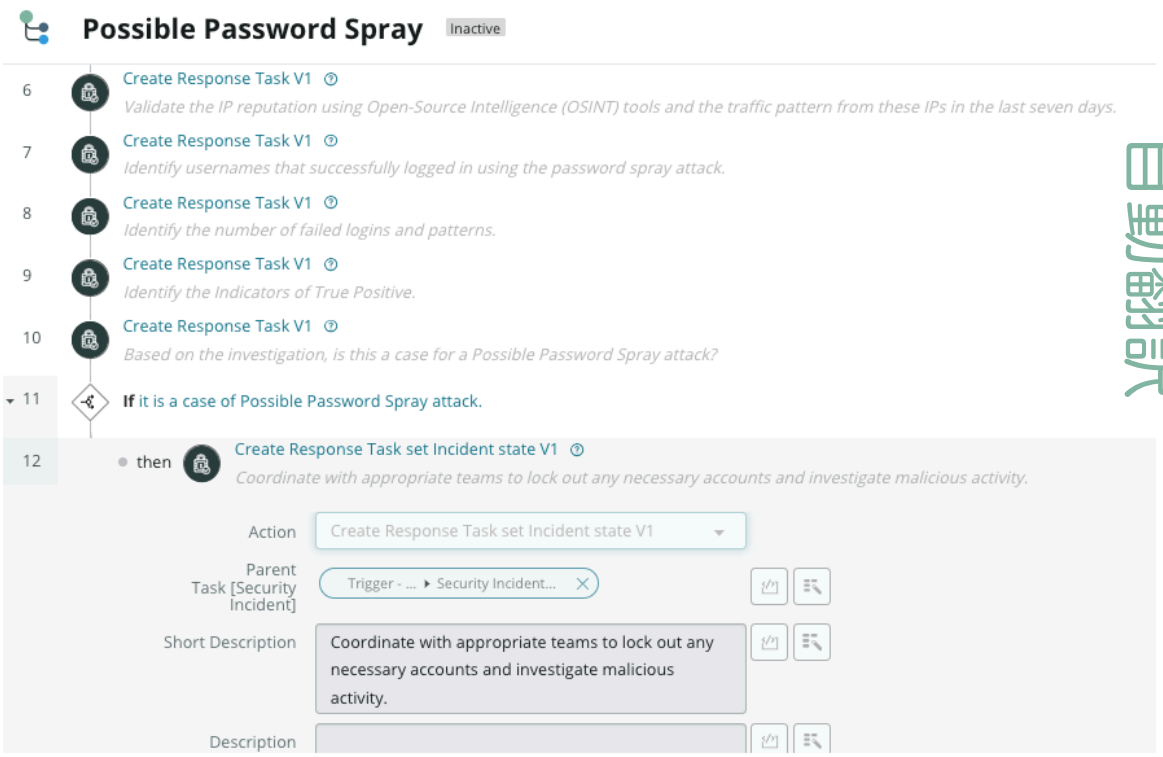
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ユーザー名は辞書ベースのように表示され (A ～ Z 順の並び) 、admin、sysadmin、root などの一般的なアドミン名が示されている場合があります
- スプレー攻撃では同じユーザー名でもさまざまなパターンがあり、同じアラートも john.doe、johnd、jdoe、john_doe、jdoe7 などでは失敗する可能性があります。これは、攻撃者が一般的なユースケースに基づいてユーザー名パターンを推測していることを示しています。
- 上記のステップの F5 ログのユーザーエージェントと URI に注目し、IOC が Red Condor アラートに関連しているかどうかを確認します。それらが一致した場合、それは真陽性のイベントです。

8. アクション 10 では、これまでに行われた調査に基づいて、これがパスワードスプレー攻撃の可能性があるケースかどうかを確認する必要があります。
9. アクション 11 で、これが「パスワードスプレー攻撃の可能性」である場合は、次のアクションを実行します。

   a. アクション 12 では、適切なチームと連携して、必要なアカウントをロックアウトし、悪意のあるアクティビティを調査する必要があります。

パスワードスプレーの可能性プレイブック



   b. アクション 13 では、パスワードスプレー攻撃の可能性に関するインシデント後のレビューを開始する必要があります。

   c. アクション 14 で、フローは終了します。

10. アクション 15 では、これがパスワードスプレー攻撃の可能性があるケースでないかどうかを確認する必要があります。
11. アクション 16 で、これが「パスワードスプレー攻撃の可能性」でない場合は、次のアクションを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. アクション 17 で、これまでの検索結果を文書化する必要があります。

b. アクション 18 では、パスワードスプレー攻撃の可能性に関するインシデント後のレビューを開始する必要があります。

c. アクション 19 で、フローは終了します。

12. アクション 20 では、同僚および GIR マネージャーに問い合わせてガイダンスを求める必要があります。

13. アクション 21 では、タスクをクローズする前にインシデントの事後レビューを完了するための応答タスクが作成されます。

T1003 - 認証情報ダンピング検出ツールのプレイブック

このプレイブックでは、認証情報のダンピングアクティビティに関連するインシデントを調査するための体系的な修復手順について説明します。

T1003 - 認証情報ダンピング検出ツールプレイブックの設定

T1003 - 認証情報ダンピング検出ツールプレイブックを設定するには、次の手順に従います。

始める前に
必要なロール：

- sn_si.admin
- flow_designer

Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

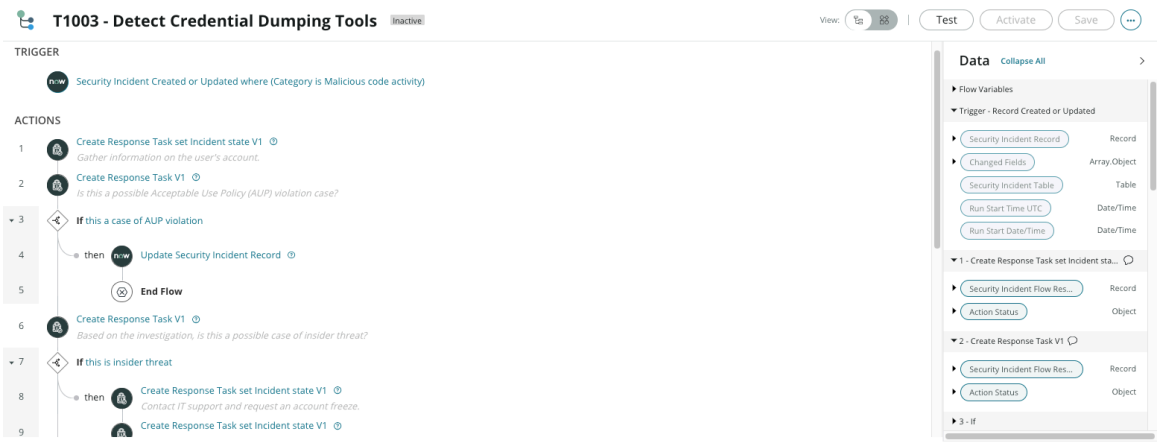
1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。

2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 **T1003 -** 認証情報ダンピング検出ツール プレイブックを選択します。

3. オプション: T1003 - 認証情報ダンピング検出ツールプレイブックのフローのコピーを作成し、必要な変更を加えることができます。

プレイブックのフローのコピーを作成するには、 アイコンをクリックし、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

T1003 - 認証情報ダンピング検出ツールプレイブック



4. プレイブックをアクティブ化します。

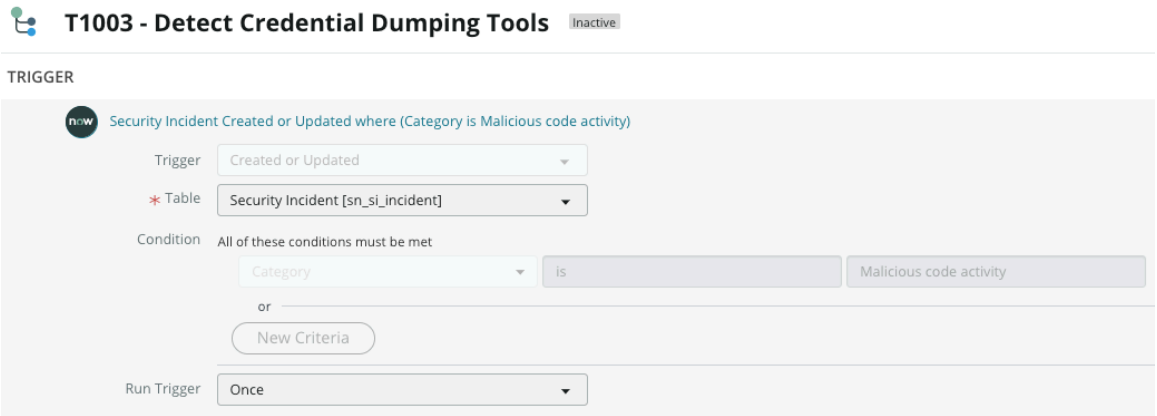
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
- 必要な変更を行った後、コピーしたフローをアクティブ化します。

5. プレイブックの [トリガー条件] を設定します。

   このプレイブックは、[カテゴリ] が [悪意のあるコードアクティビティ **(Malicious code activity)**] である場合にトリガーされ、セキュリティインシデントに関連付けられます。



T1003 - 認証情報ダンピング検出ツールプレイブックを使用する

このプレイブックを使用して、認証情報ダンピングアクティビティに関連するインシデントを調査します。以下に示すステップは、T1003 - 認証情報ダンピング検出ツールプレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

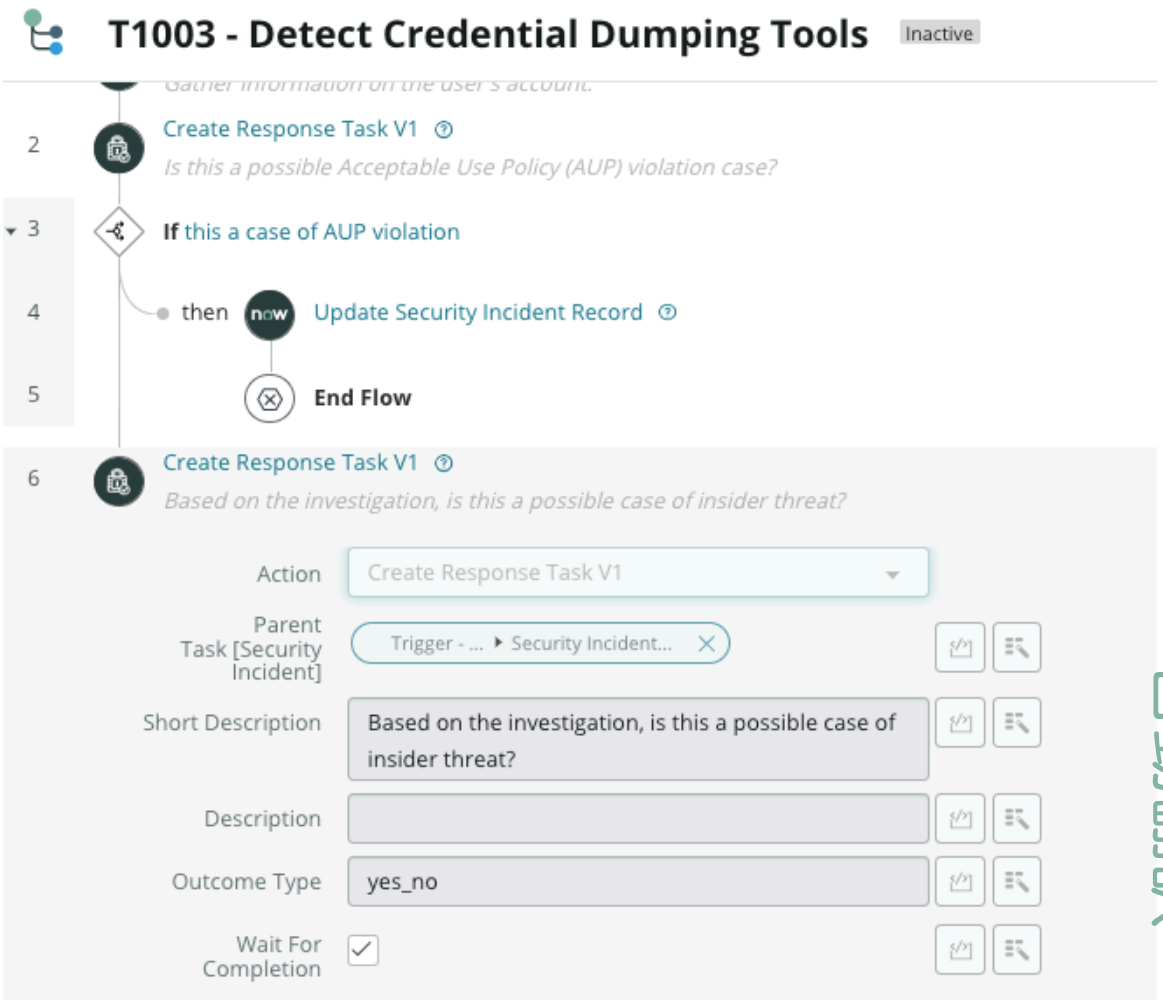
1. プレイブックがトリガーされて実行が開始されたら、アクション 1 で、ユーザーのアカウントに関する情報を収集する必要があります。
   - ホストのアクティビティをチェックして、疑わしいアクティビティを探す必要があります。
   - サーバー/エンドポイント/VM の所有者を特定し、ツールに関連するデータをキャプチャする必要があります。
   - ユーザーの他のアカウントに関する情報を収集する必要があります。
2. アクション 2 では、これが利用規定 (AUP) 違反の可能性があるかどうかを確認する必要があります。
   収集した証拠でピアレビューを行い、そのユーザーに連絡するかどうかを地域のインシデントマネージャーに相談できます。
3. アクション 3 では、利用規定 (AUP) 違反の場合に、次のアクションを実行します。
   a. アクション 4 では、これが利用規定 (AUP) 違反のケースであるセキュリティインシデントを更新する必要があります
   b. アクション 5 で、フローは終了します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. アクション 6 では、これまでに行った調査に基づいて、これが内部関係者の脅威の可能性があるかどうかを確認する必要があります。

T1003 - 認証情報ダンピング検出ツールプレイブック



5. アクション 7 では、これが内部関係者の脅威の場合に、次のアクションを実行します。

   a. アクション 8 では、IT サポートに連絡してアカウントの凍結を要求します。

   b. アクション 9 では、悪意のある IP をブロックする必要があります。

   c. アクション 10 では、社内の従業員にメールで連絡する必要があります。
   提供されたメールテンプレートを使用して、社内従業員に連絡できます。

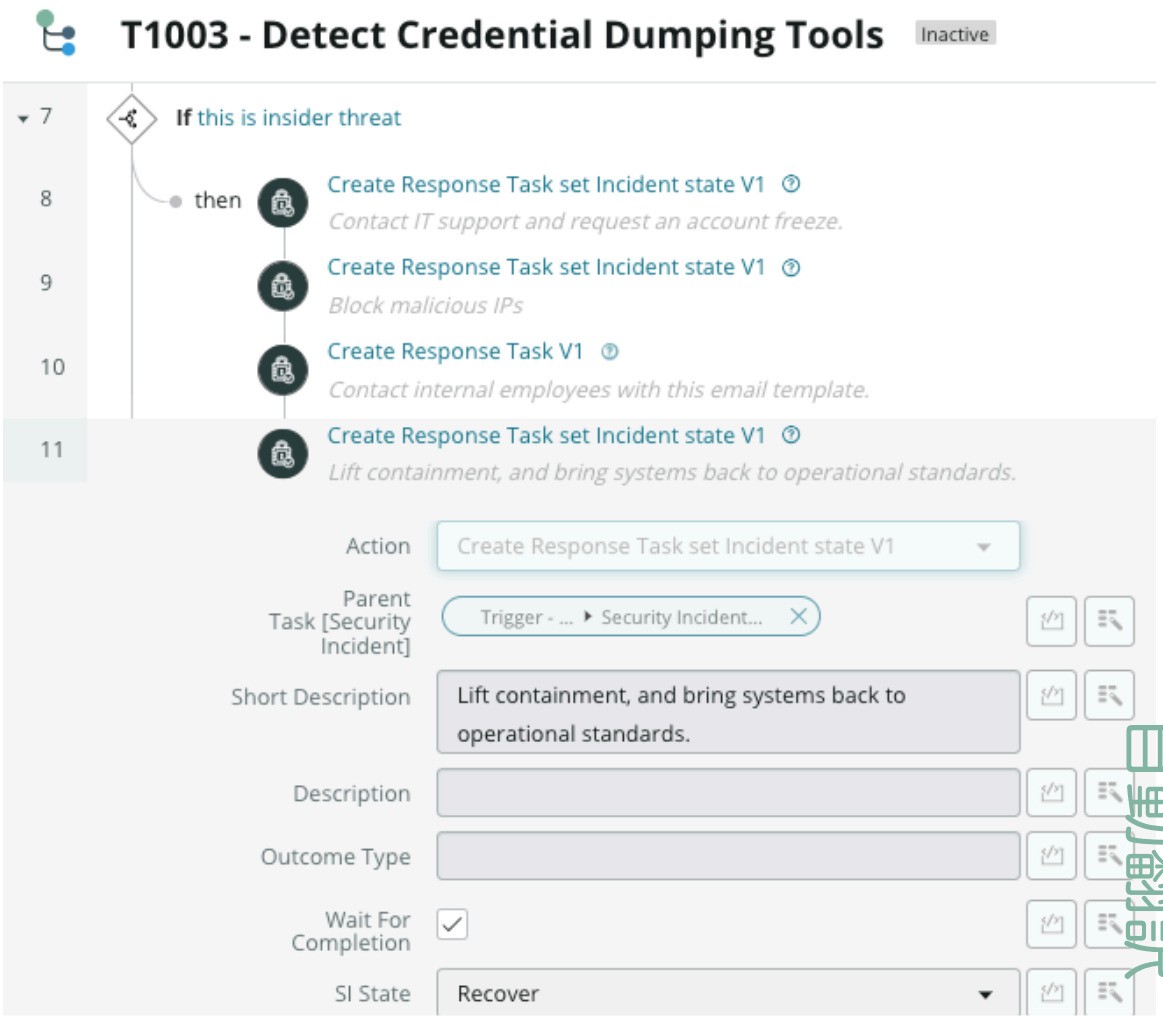
   d. アクション 11 では、封じ込めを解除し、システムを運用標準に戻す必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フローが終了します。

封じ込めを解除するための対応タスク



6. アクション 12 では、これが内部関係者の脅威でない場合に、アクション 13 で、ピアレビューを実行して、これを除外リストに追加する必要があるかどうかを判断する必要があります。フローが終了します。
7. アクション 14 では、タスクをクローズする前にインシデントの事後レビューを完了するための応答タスクが作成されます。

メールドメインなりすまし検出のプレイブック

このプレイブックは、フィッシング攻撃者のメールアドレスにそっくりに見せかけたドメインが使用されている可能性をアナリストに警告することで、ユーザーから報告されたフィッシング送信の初期段階でのトリアージを支援します。

メールドメインなりすまし検出プレイブックは、フィッシング攻撃者の送信元メールドメインと、観測可能リポジトリに存在する信頼できるドメイン名との類似性の一致を探します。なりすまし送信者のメールドメインの一致がプレイブックによって特定されると、アナリストはタグでアラートを受け取ります。

ワークフローは既存のプレイブックに基づいて作成され、インシデント調査のための一貫した効率的なアプローチを提供します。プレイブックの各意思決定ポイントは結果主導型タスクに変換され、そのようなタスクの結果に基づいてフローの方向が変わります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

メールのなりすまし検出プレイブックの設定

メールのなりすまし検出プレイブックを設定するには、次の手順に従います。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

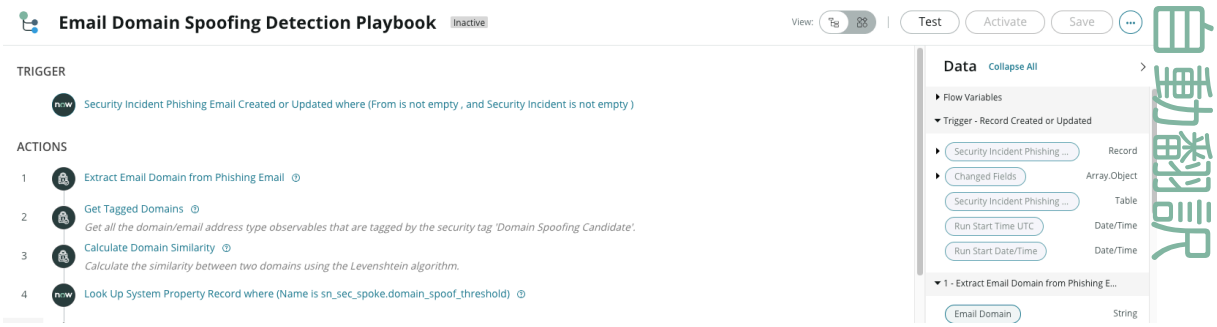
Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 メールドメインなりすまし検出プレイブック プレイブックを選択します。
3. オプション: メールドメインなりすまし検出プレイブックのフローのコピーを作成し、必要な変更を加えることができます。

   プレイブックのフローのコピーを作成するには、 アイコンをクリックし、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

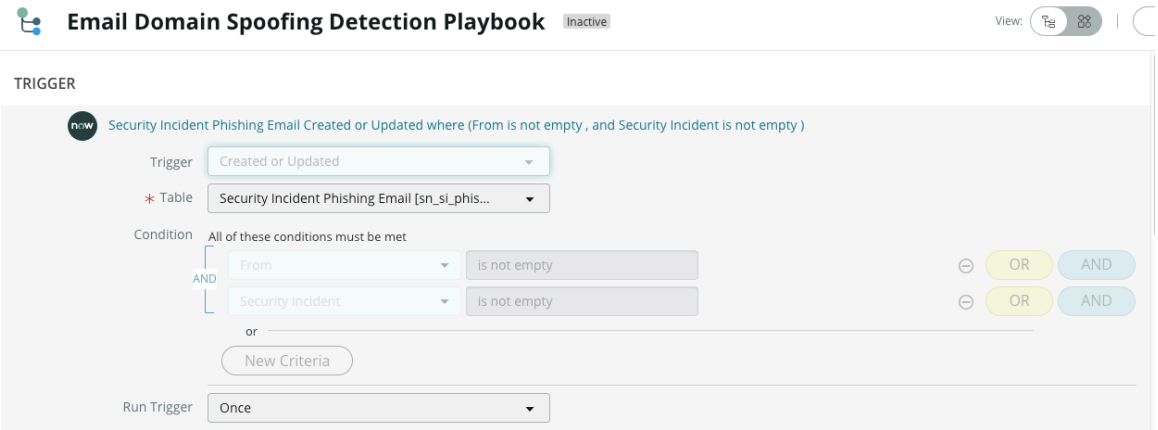
   メールドメインなりすまし検出プレイブック

4. プレイブックをアクティブ化します。
   - ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   - 必要な変更を行った後、コピーしたフローをアクティブ化します。
5. プレイブックの [トリガー条件] を設定します。
   このプレイブックは、次の条件が満たされるとトリガーされ、セキュリティインシデントに関連付けられます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [送信元 **(From)**] が空でない **(is not empty)**。
- [セキュリティインシデント] が空でない **(is not empty)**。



メールドメインなりすまし検出プレイブックを使用する

このプレイブックを使用して、フィッシング攻撃者の送信元メールドメインと、観測可能リポジトリに存在する信頼できるドメイン名との類似性の一致を探します。以下に示すステップは、メールドメインなりすまし検出プレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

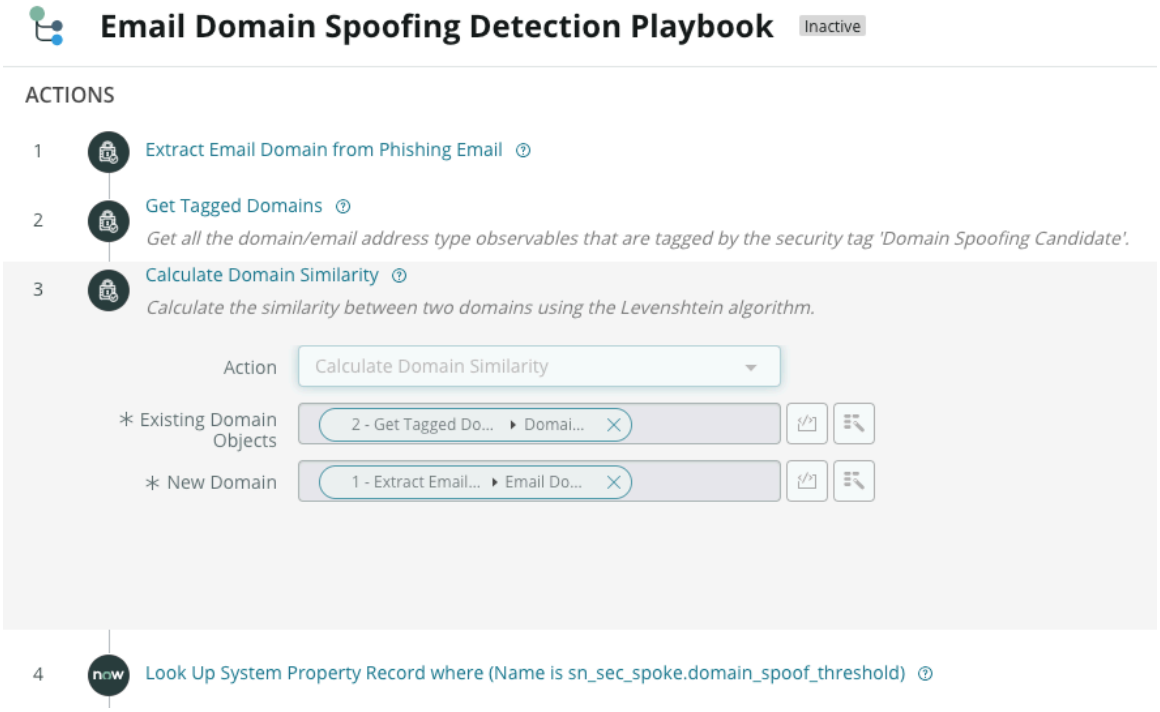
手順

1. プレイブックがトリガーされて実行が開始されると、アクション 1 で、プレイブックはフィッシングメールからメールドメインを抽出します。
2. アクション 2 では、プレイブックはセキュリティタグ「ドメインスプーフィング候補」でタグ付けされたすべてのドメイン/メールアドレスタイプの観測事象を取得します。
3. アクション 3 で、プレイブックはレーベンシュタインアルゴリズムを使用して、タグ付きドメインとメールドメイン間の類似度を計算します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

メールドメインなりすまし検出プレイブック

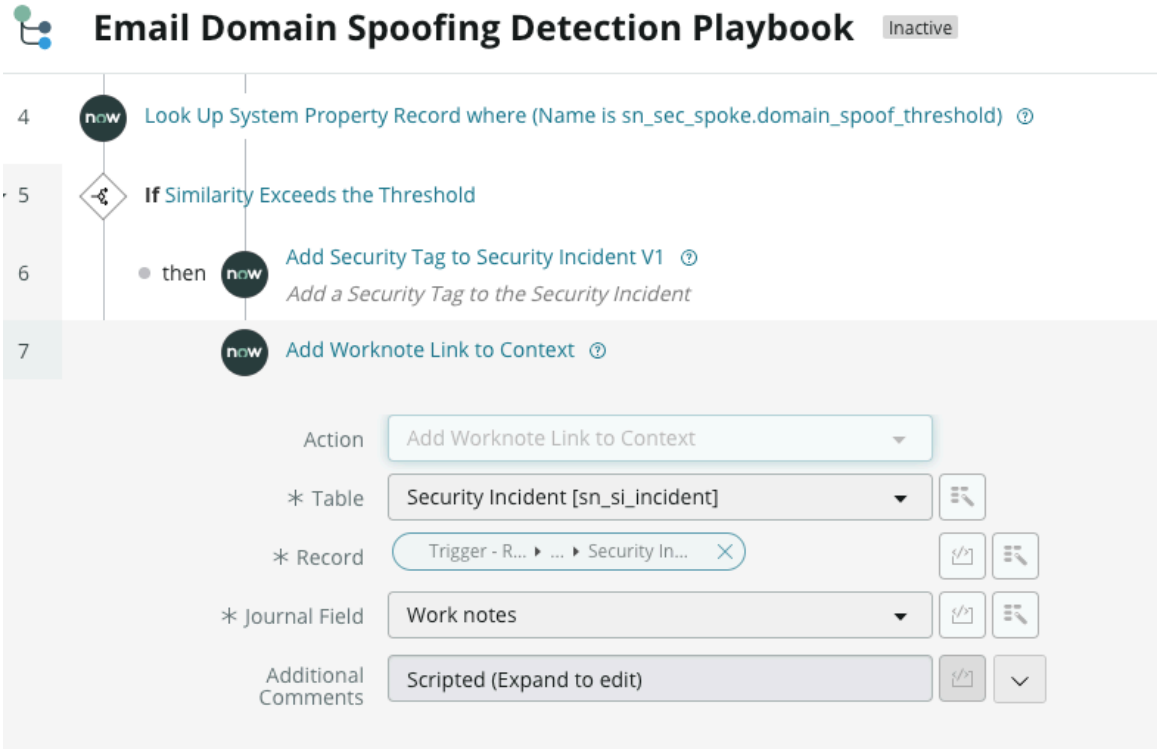


4. アクション 4 では、プレイブックは次のいずれかの条件に基づいてシステムプロパティレコードを検索します。
   - 名前は sn_sec_spoke.domain_spoof_threshold。
   - 名前は a ～ z で、複数のレコードが見つかった場合、最初のレコードのみが返される。
5. アクション 5 では、これまでに行った調査に基づいて、プレイブックは 2 つのドメインの類似性がしきい値を超えているかどうかを確認します。
   2 つのドメインの類似性がしきい値を超えない場合、アクション 5 で、手動応答タスクが作成され、フローが終了します。2 つのドメインの類似性がしきい値を超えると、アクション 6 と 7 が実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

類似性がしきい値を超える



6. アクション 6 では、プレイブックはメールドメインなりすましセキュリティタグをセキュリティインシデントに追加します。
7. アクション 7 では、プレイブックはスクリプトオプションを使用して作業メモリンクをコンテキストに追加します。
8. アクション 8 で、フローは終了します。

タイポスクワッティングドメインのプレイブック

このプレイブックには、スペルミスのあるドメインを調査し、削除のために組織の法務部門と協力するための体系的な手順が記載されています。タイポスクワッティングドメインは、正当なドメイン名によく似せた意図的に正しくないスペルを用いているドメイン名です。攻撃者はその正しくないスペルで見間違いをさせて、金融搾取やその他の悪意のある活動のために、悪事を意図した Web サイトに誘導します。

タイポスクワッティングドメインは、デジタルリスク保護ソリューション (Digital Shadows) や脅威インテリジェンスプラットフォーム (Anomali Threatstream) などのさまざまなソースから Security Operations チームに報告されます。セキュリティインシデントが作成された後、このソリューションは、そのドメインが本当にタイポスクワッティングドメインであるかどうかを識別するのに役立ちます。タイポスクワッティングドメインの場合、アナリストはそれを法務部門に報告して、さらにアクションを実行できます。

ワークフローは既存のプレイブックに基づいて作成され、インシデント調査のための一貫した効率的なアプローチを提供します。プレイブックの各意思決定ポイントは結果主導型タスクに変換され、そのようなタスクの結果に基づいてフローの方向が変わります。

タイポスクワッティングドメインプレイブックの設定

タイポスクワッティングドメインプレイブックを設定するには、次の手順に従います。

始める前に
必要なロール：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- sn_si.admin
- flow_designer

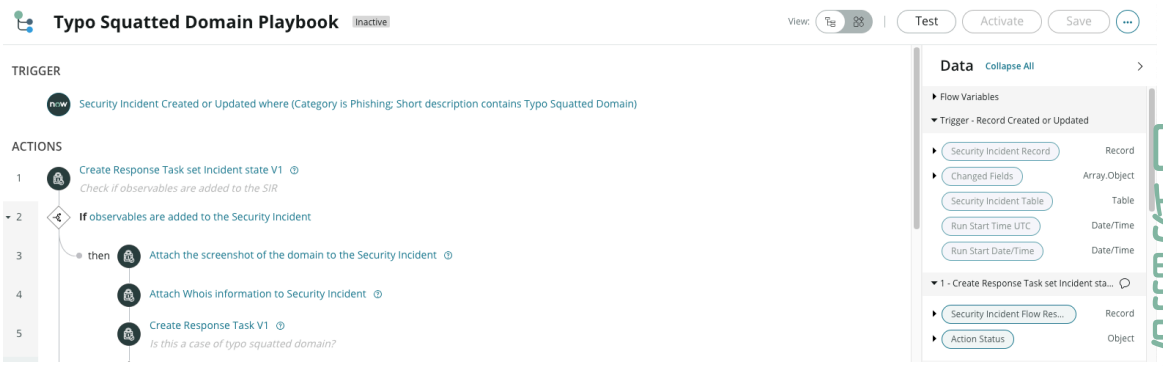
Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 タイポスクワッティングドメイン プレイブックを選択します。
3. オプション: タイポスクワッティングドメインプレイブックのフローのコピーを作成し、必要な変更を加えることができます。

   (Optional) プレイブックのフローのコピーを作成するには、 アイコンをクリックし、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

   タイポスクワッティングドメインプレイブック

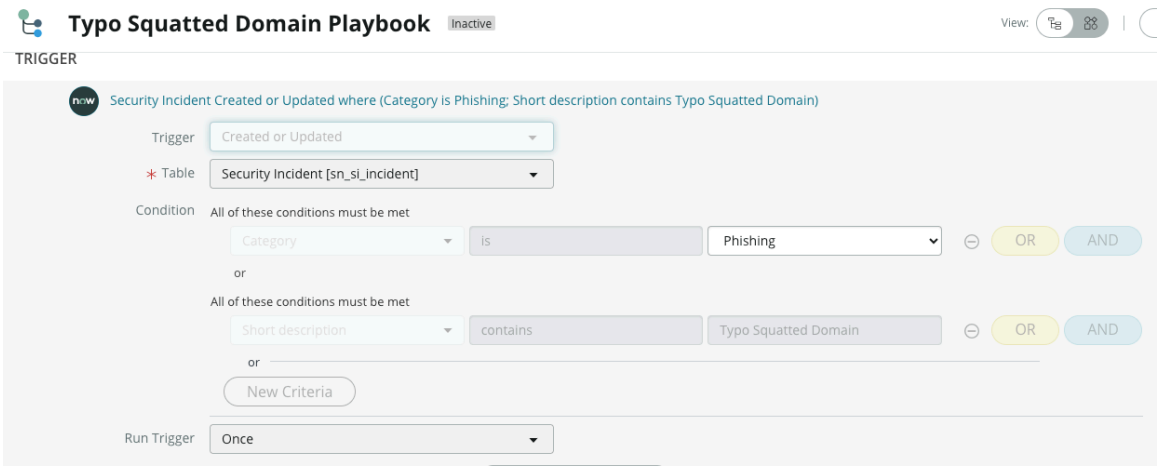
   

4. プレイブックをアクティブ化します。
   - ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   - 必要な変更を行った後、コピーしたフローをアクティブ化します。
5. プレイブックの [トリガー条件] を設定します。

   このプレイブックは、次の条件が満たされるとトリガーされ、セキュリティインシデントに関連付けられます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [カテゴリ] は [フィッシング] です。
- [簡単な説明] に [タイポスクワッティングドメイン **(Typo Squatted Domain)]** が含まれています。



タイポスクワッティングドメインプレイブックを使用する

このプレイブックを使用して、スペルミスのあるドメインを調査し、組織の法務部門と協力して削除を行います。以下に示すステップは、タイポスクワッティングドメインプレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に
必要なロール：

- sn_si.admin
- flow_designer

Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

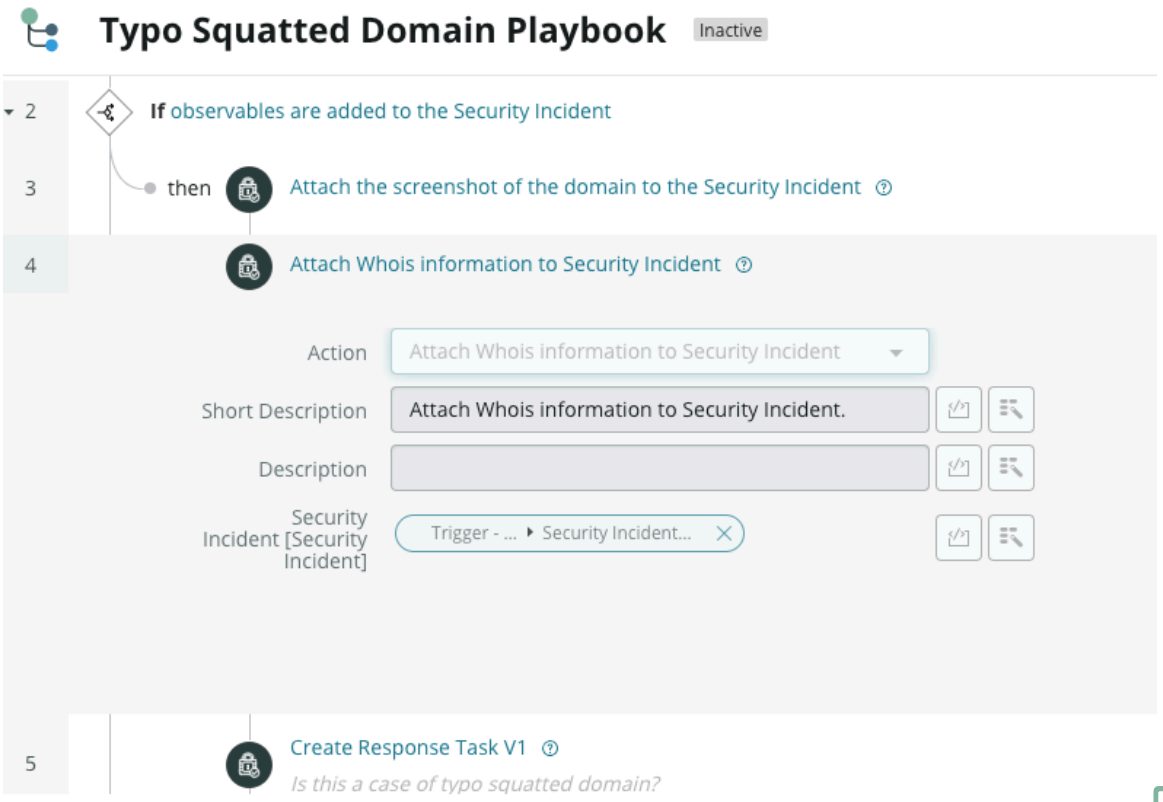
手順

1. プレイブックがトリガーされて実行が開始されたら、アクション 1 で、観測事象がセキュリティインシデントレスポンス (SIR) に追加されているかどうかを確認する必要があります。
   観測事象が SIR に追加されていない場合は、続行する前に観測事象を追加してください。観測事象が利用できない場合は、アクション 10 が実行され、セキュリティインシデントがクローズされます。
2. アクション 2 では、観測事象がセキュリティインシデントに追加された場合に、次のアクションが実行されます。
3. アクション 3 では、セキュリティインシデントへのタイポスクワッティングドメインのスクリーンショットを添付する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タイポスクワッティングドメインプレイブック



4. アクション 4 では、セキュリティインシデントに Whois 情報を添付する必要があります。
5. アクション 5 では、これまでに行った調査に基づいて、プレイブックはこれがタイポスクワッティングドメインのケースであるかどうかを確認します。
これがタイポスクワッティングドメインのケースでない場合は、アクション 5 で手動応答タスクが作成され、フローが終了します。
6. アクション 6 では、これがタイポスクワッティングドメインである場合に、アクション 7 が実行されます。
7. アクション 7 では、これがタイポスクワッティングドメインのケースであることを法務チームおよびその他の必要なチームにメール送信して通知し、それを根絶するために必要なアクションを実行する必要があります。
これがタイポスクワッティングドメインのケースでない場合は、アクション 5 で手動応答タスクが作成され、フローが終了します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タイポスクワッティングドメインのケース

8. アクション 9 では、タスクをクローズする前にインシデントの事後レビューを完了するための応答タスクが作成されます。

認証情報スニッフィングのプレイブック

このプレイブックでは、ServiceNow インスタンスの *sys_installation_exit* テーブルを介して実行される認証情報スニッフィングアクティビティに関連するインシデントを調査するための、システム修復手順について説明します。

認証情報スニッフィングプレイブックには、*sys_installation_exit* テーブルのレコードを使用してデータベース (DB) ログイン、シングルサインオン (SSO)、LDAP (ライトウェイトディレクトリアクセスプロトコル) を処理するためのスクリプトフィールドがあります。これらの特権スクリプトフィールドを使用すると、ログイン中にインスタンスに対するユーザー要求とパラメーター (ユーザー名とパスワードといったユーザー認証情報など) をリッスンできます。

悪意のあるユーザーがユーザー要求をリッスンし、これらの要求をインスタンスに記録するスクリプトを作成する可能性があります。インスタンスの *sys_installation_exit* テーブルは、そのインスタンス上のすべてのユーザーのログイン/ログアウトアクティビティを処理するルールを定義します。

認証情報スニッフィングプレイブックを設定する

認証情報スニッフィングプレイブックを設定するには、以下の手順に従います。

始める前に

必要なロール：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- sn_si.admin
- flow_designer

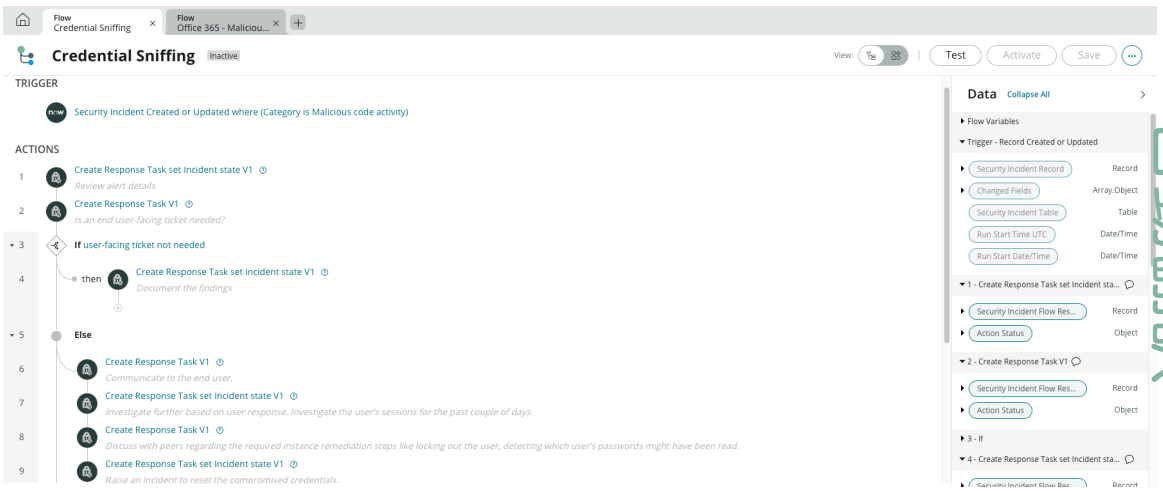
Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 認証情報スニッフィング プレイブックを選択します。
3. オプション: 認証情報スニッフィングプレイブックのフローのコピーを作成し、必要な変更を加えます。

   (Optional) プレイブックのフローのコピーを作成するには、 アイコンを選択し、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

   認証情報スニッフィングプレイブック

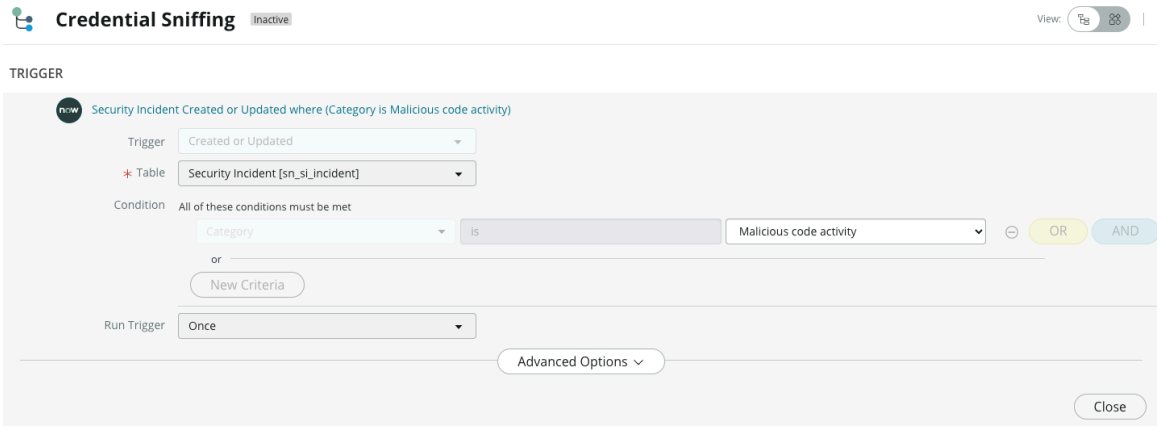
   

4. プレイブックをアクティブ化します。
   a. ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   b. 必要な変更を行った後、コピーしたフローをアクティブ化します。
5. プレイブックの [トリガー条件] を設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このプレイブックは、[カテゴリ] が [悪意のあるコードアクティビティ **(Malicious code activity)**] である場合にトリガーされ、セキュリティインシデントに関連付けられます。

認証情報スニッフィングプレイブックのトリガー条件



認証情報スニッフィングプレイブックを使用する

このプレイブックを使用して、ServiceNow インスタンスの *sys_installation_exit* テーブルを介して実行される認証情報スニッフィングアクティビティに関連するインシデントを調査します。以下に示すステップは、認証情報スニッフィングプレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

手順

1. プレイブックがトリガーされて実行が開始されたら、アクション 1 で、次のアラートの詳細を確認します。
   - インスタンス
   - セッション ID
   - トランザクション ID
   - _raw：スクリプト全体を提供します。

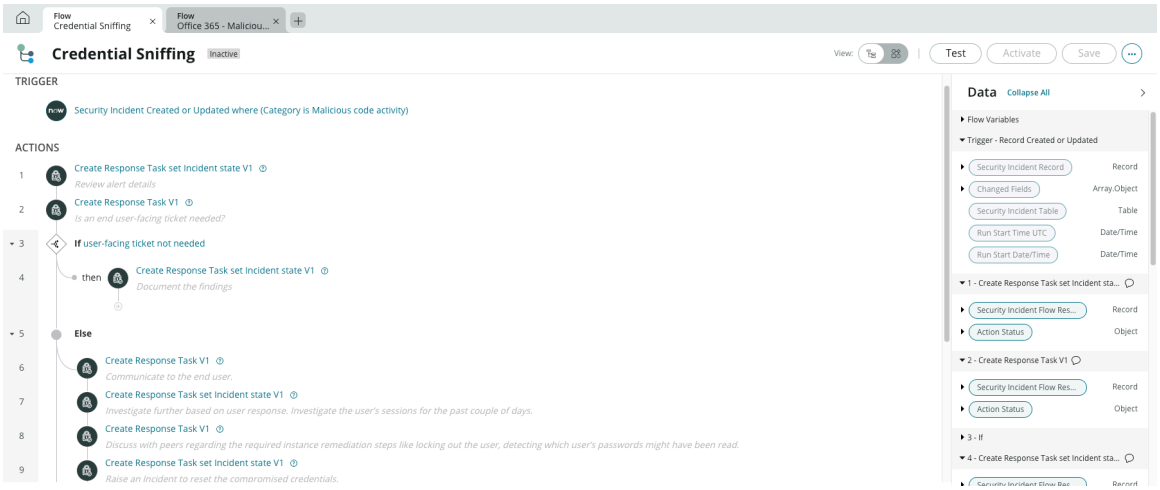
     スクリプト例：

     ```
     Var pass= request.getParameter(“user_password”);
     Gs.log(pass);
     ```

2. アクション 2 では、これまでに収集されたデータに基づいて、このアラートにエンドユーザーチケットが必要かどうかを確認します。
3. アクション 3 では、アラートがエンドユーザーチケットを必要としない場合に、アクション 4 で、これまでの結果を文書化します。
   フローが終了します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

認証情報スニッフィングプレイブック



4. アクション 5 では、アラートにエンドユーザーチケットが必要な場合に、次の手順を実行します。

   a. アクション 6 では、アラートにエンドユーザーチケットが必要であることをエンドユーザーに通知します。

   b. アクション 7 では、過去数日間のユーザーの応答とユーザーのセッションに基づいて、さらに調査します。

   c. アクション 8 では、ユーザーのロックアウトや、どのユーザーのパスワードが読み取られた可能性があるかの検出など、インスタンスの修復手順について同僚と話し合います。

   d. アクション 9 では、インシデントまたはチケットを生成して、侵害されたユーザーの認証情報をリセットします。

   e. アクション 10 では、封じ込めを解除し、システムを運用標準に戻します。フローが終了します。

5. アクション 11 では、タスクをクローズする前にインシデントの事後レビューを完了します。

T1070 - クリアされた Windows イベントログのプレイブック

このプレイブックには、ユーザーがセキュリティログを削除するイベントタイプを追跡するインシデントを調査するための修復手順が記載されています。セキュリティログがクリアされるたびに、監査システムイベントポリシーの状態に関係なく、イベント 517 と 1102 がログに記録されます。

このアラートでは、次のタイプのイベントを追跡できます。

- イベント **517**： [プライマリユーザー名 (Primary username)] フィールドと [クライアントユーザー名 (Client username)] フィールドは、ログをクリアしたユーザーを特定します。プライマリユーザー名はシステムに対応し、クライアントユーザー名はログをクリアしたユーザーを示します。
- イベント **1102**： [アカウント名] フィールドと [ドメイン名] フィールドは、ログをクリアしたユーザーを特定します。ログオン ID を使用すると、ログオンイベントおよび同じログオンセッション中にログに記録された他のイベントに逆方向の関連付けを行うことができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

T1070 - クリアされた Windows イベントログプレイブックを設定する

T1070 - クリアされた Windows イベントログプレイブックを設定するには、以下の手順に従います。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

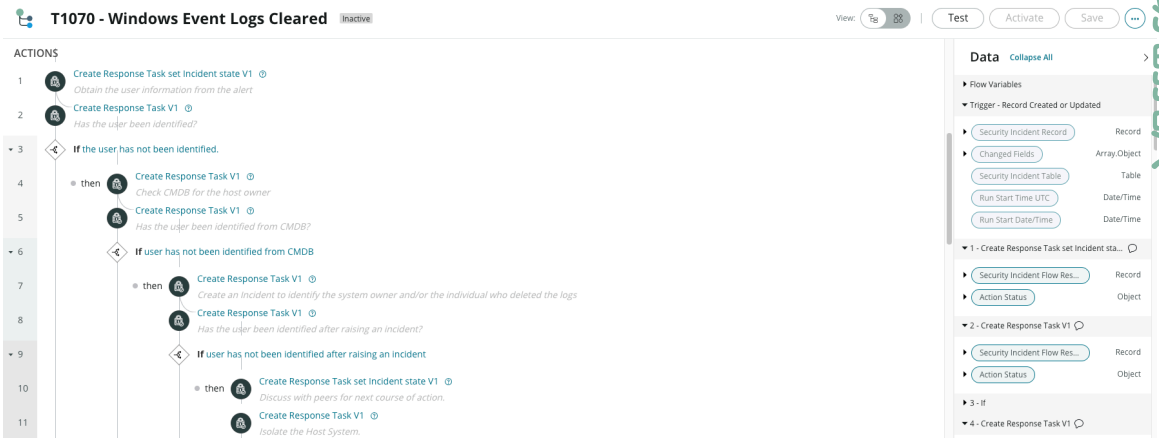
Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、[**T1070 -** クリアされた **Windows** イベントログ] プレイブックを選択します。
3. オプション: T1070 - クリアされた Windows イベントログプレイブックのフローのコピーを作成し、必要な変更を加えます。

   (Optional) プレイブックのフローのコピーを作成するには、 アイコンを選択し、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

   T1070 - クリアされた **Windows** イベントログプレイブック

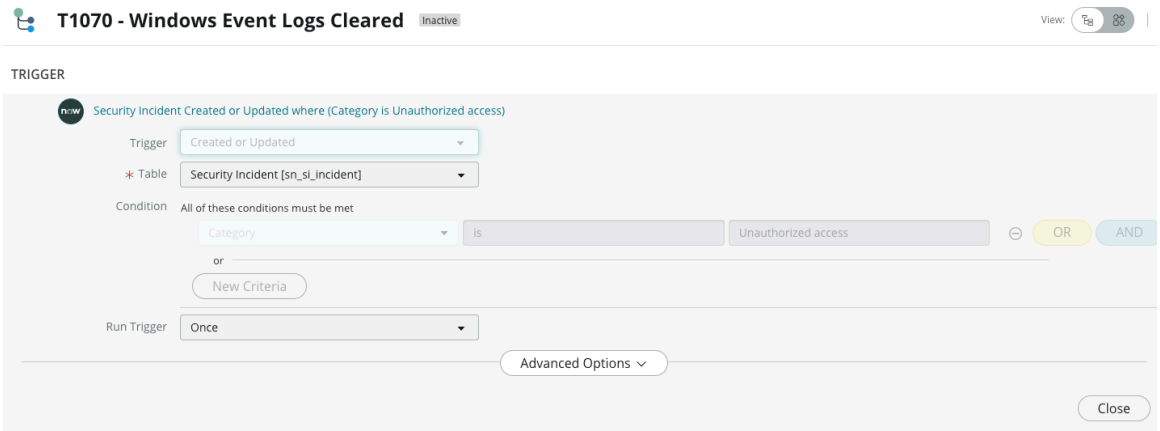


4. プレイブックをアクティブ化します。
   a. ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   b. 必要な変更を行った後、コピーしたフローをアクティブ化します。
5. プレイブックの [トリガー条件] を設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このプレイブックは、[カテゴリ] が [無許可のアクセス] である場合にトリガーされ、セキュリティインシデントに関連付けられます。

T1070 - クリアされた **Windows** イベントログプレイブックのトリガー条件



T1070 - クリアされた **Windows** イベントログプレイブックを使用する

このプレイブックを使用して、ユーザーがセキュリティログを削除するイベントタイプを追跡するインシデントを調査します。以下に示すステップは、T1070 - クリアされた Windows イベントログプレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

手順

1. プレイブックがトリガーされて実行が開始されたら、アクション 1 でアラートからユーザーの詳細を取得します。
2. アクション 2 では、ユーザーが識別されているかどうかを確認します。
3. アクション 3 では、ユーザーが識別されていない場合に、次の手順を実行します。

   a. アクション 4 では、CMDB (構成管理データベース) でホスト所有者の詳細を確認します。

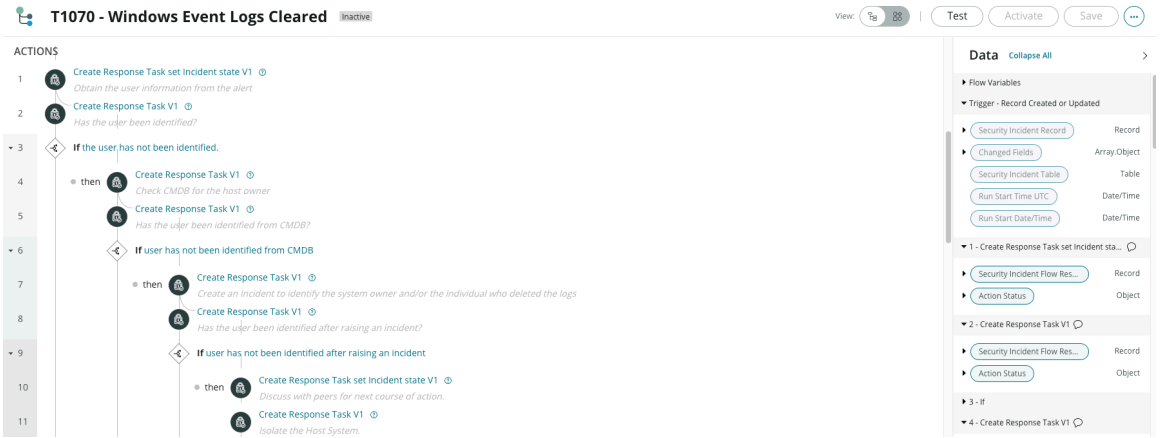
   b. アクション 5 では、CMDB からユーザーが識別されているかどうかを確認します。

   ユーザーが CMDB から特定された場合は、アクション 5 で手動応答タスクが作成され、フローが終了します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

T1070 - クリアされた **Windows** イベントログプレイブック



c. アクション 6 では、ユーザーが CMDB から識別されていない場合に、次の手順を実行します。

i. アクション 7 では、インシデントを作成して、システム所有者と、ログを削除した個人を特定します。

ii. アクション 8 では、インシデントを発生させた後に、ユーザーが特定されているかどうかを確認します。

インシデントの発生後にユーザーが特定された場合は、アクション 8 で手動応答タスクが作成され、フローが終了します。

iii. アクション 9 では、インシデントの発生後にユーザーが特定されていない場合に、次の手順を実行します。

1. アクション 10 では、次に取るべき対処措置について同僚と話し合います。

2. アクション 11 で、ホストシステムを分離します。

3. アクション 12 では、作成された可能性のある不要なファイルを削除し、不正なアカウントを削除します。

4. アクション 13 では、封じ込めを解除し、システムを運用標準に戻します。

5. アクション 14 では、タスクをクローズする前にインシデントの事後レビューを完了します。

アクション 15 で、フローは終了します。

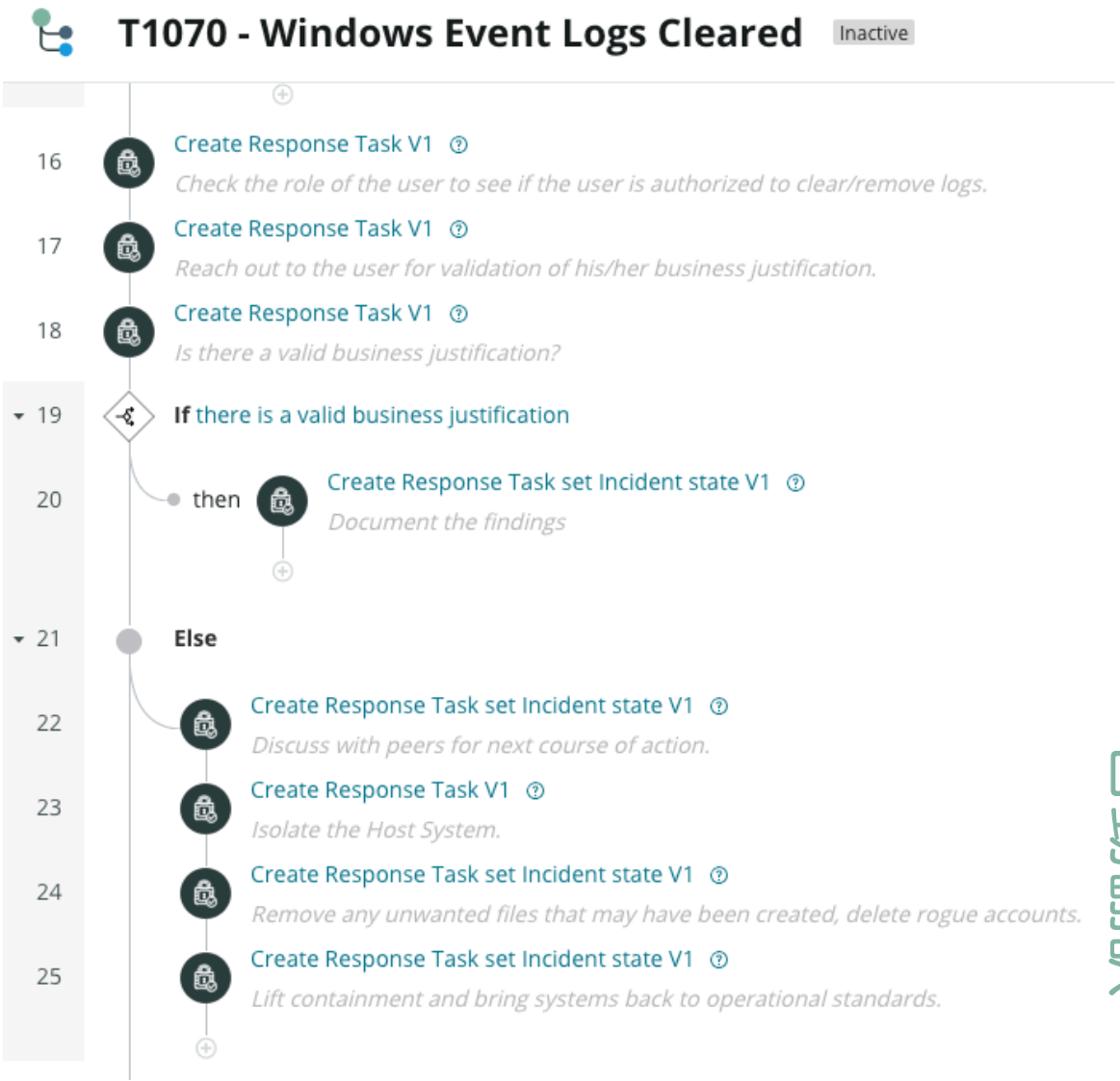
4. アクション 16 では、ユーザーが特定されている場合に、ユーザーのロールをチェックして、ユーザーがログをクリアまたは削除することを許可されているかどうかを確認します。

5. アクション 17 では、ビジネス上の根拠を検証するためにユーザーに連絡します。
提供されたメールテンプレートを使用して、ユーザーに連絡できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

T1070 - クリアされた **Windows** イベントログプレイブックの使用



自動翻訳

6. アクション 18 では、有効なビジネス上の根拠が提供されているかどうかを確認します。
7. アクション 19 では、有効なビジネス上の根拠が提供された場合に、アクション 20 で、これまでの結果を文書化します。
   フローが終了します。
8. アクション 21 では、有効なビジネス上の根拠が指定されていない場合に、次の手順を実行します。

   a. アクション 22 では、次に取るべき対処措置について同僚と話し合います。

   b. アクション 23 で、ホストシステムを分離します。

   c. アクション 24 では、作成された可能性のある不要なファイルを削除し、不正なアカウントを削除します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

d. アクション 25 では、封じ込めを解除し、システムを運用標準に戻します。
フローが終了します。

9. アクション 26 では、タスクをクローズする前にインシデントの事後レビューを完了します。

/etc/hosts ファイル内の外部アドレスの OSquery のプレイブック

このプレイブックでは、内部ホスト名またはドメインが Linux サーバーのローカル DNS (/etc/hosts) の外部 IP アドレスに割り当てられていることを示すインシデントを調査するための体系的な修復手順について説明します。

/etc/hosts ファイル内の外部アドレスの OSquery プレイブックを設定する

/etc/hosts ファイル内の外部アドレスの OSquery プレイブックを設定するには、以下の手順に従います。

始める前に
必要なロール：

- sn_si.admin
- flow_designer

Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

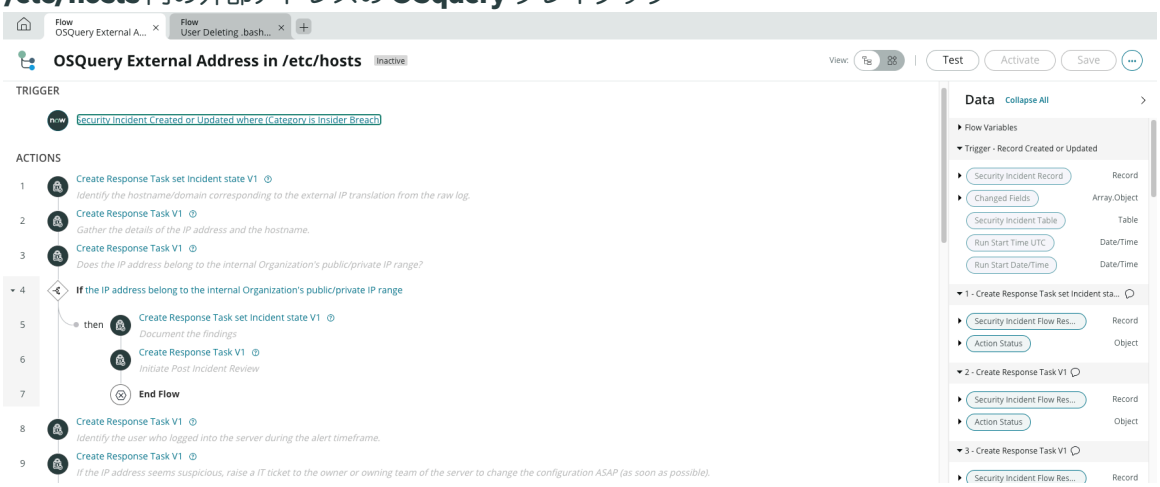
1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。

2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 **/etc/hosts** 内の **OSquery** 外部アドレス プレイブックを選択します。

3. オプション: /etc/hosts 内の外部アドレスの OSquery プレイブックのフローのコピーを作成し、必要な変更を加えます。

(Optional) プレイブックのフローのコピーを作成するには、 アイコンを選択し、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

/etc/hosts 内の外部アドレスの OSquery プレイブック



4. プレイブックをアクティブ化します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

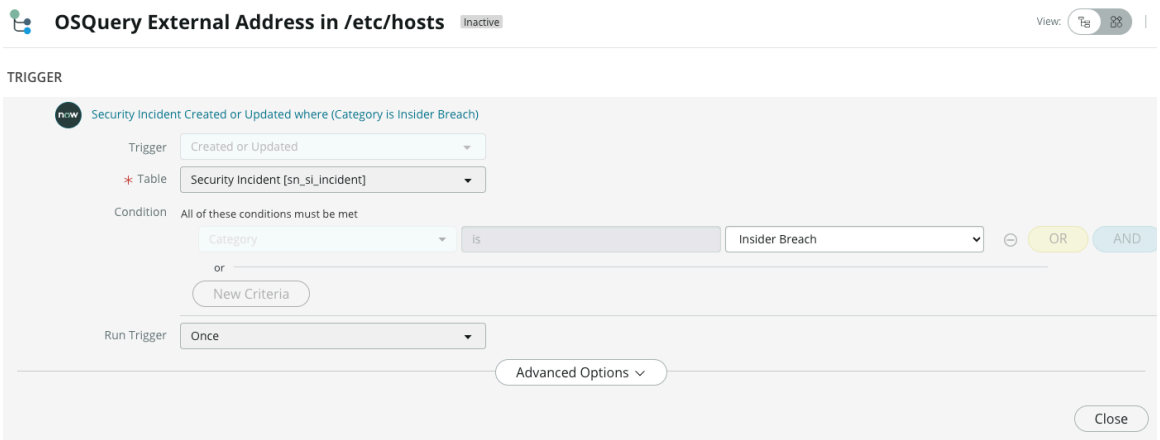
a. ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。

b. 必要な変更を行った後、コピーしたフローをアクティブ化します。

5. プレイブックの [トリガー条件] を設定します。

このプレイブックは、[カテゴリ] が [内部違反 **(Insider Breach)]** である場合にトリガーされ、セキュリティインシデントに関連付けられます。

/etc/hosts ファイル内の外部アドレスの **OSquery** プレイブックのトリガー条件



/etc/hosts ファイル内の外部アドレスの OSquery プレイブックを使用する

このプレイブックを使用して、内部ホスト名またはドメインが Linux サーバーのローカル DNS (/etc/hosts) の外部 IP アドレスに割り当てられていることを示すインシデントを調査します。以下に示すステップは、/etc/hosts ファイル内の外部アドレスの OSquery プレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

手順

1. プレイブックがトリガーされて実行が開始されたら、アクション 1 で、生のログからの外部 IP 変換に対応するホスト名またはドメイン名を特定します。

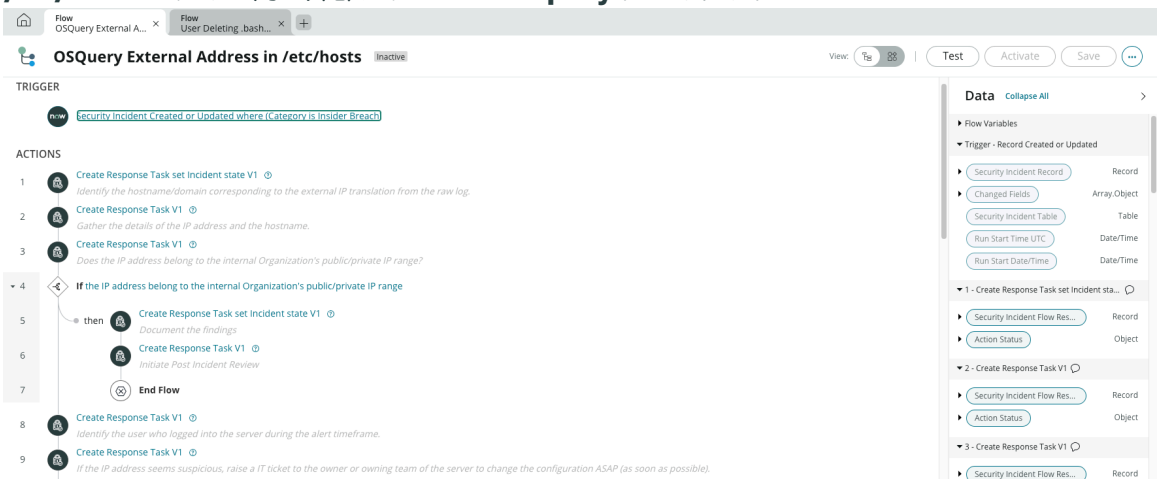
2. アクション 2 では、IP アドレスとホスト名の詳細を収集します。

3. アクション 3 では、この IP アドレスが内部組織のパブリック/プライベート IP 範囲に属しているかどうかを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

/etc/hosts ファイル内の外部アドレスの OSquery プレイブック



4. アクション 4 では、IP アドレスが内部組織のパブリック/プライベート IP 範囲に属している場合に、次の手順を実行します。

   a. アクション 5 では、これまでの結果を文書化します。

   b. アクション 6 では、インシデントの事後レビューを開始します。
   アクション 7 では、インシデントの事後レビューの後、フローが終了します。

5. IP アドレスが内部組織のパブリック/プライベート IP 範囲に属していない場合は、アクション 8 で、アラートの期間中にサーバーにログインしたユーザーを特定します。
6. アクション 9 では、IP アドレスが疑わしいと思われる場合に、所有者またはサーバーのチームに IT チケットを発行して、できるだけ早く構成を変更します。
7. アクション 10 では、DNS エントリを追加する前と後に、サーバーに悪意のあるアクティビティがあったかどうかを確認します。
8. アクション 11 では、サーバーから外部 IP アドレスへの接続を確認します。
9. アクション 12 では、これまでの結果を文書化します。
10. アクション 13 では、所有者またはチームの情報が利用可能かどうかを確認します。
11. アクション 14 では、所有者またはチームの情報が使用可能な場合に、次の手順を実行します。

    a. アクション 15 では、所有者またはサーバーのチームに連絡して、アクティビティを認識しているかどうかを確認します。
    提供されたメールテンプレートを使用して、所有者またはサーバーのチームに連絡できます。

    b. アクション 16 では、所有者またはチームが有効なビジネス上の根拠を提供したかどうかを確認します。

    c. アクション 17 では、指定された所有者またはチームが有効なビジネス上の根拠を提供しなかった場合に、フローが終了します。
    しかし、所有者またはチームが有効なビジネス上の根拠を提供した場合には、次の手順を実行します。

自動翻訳

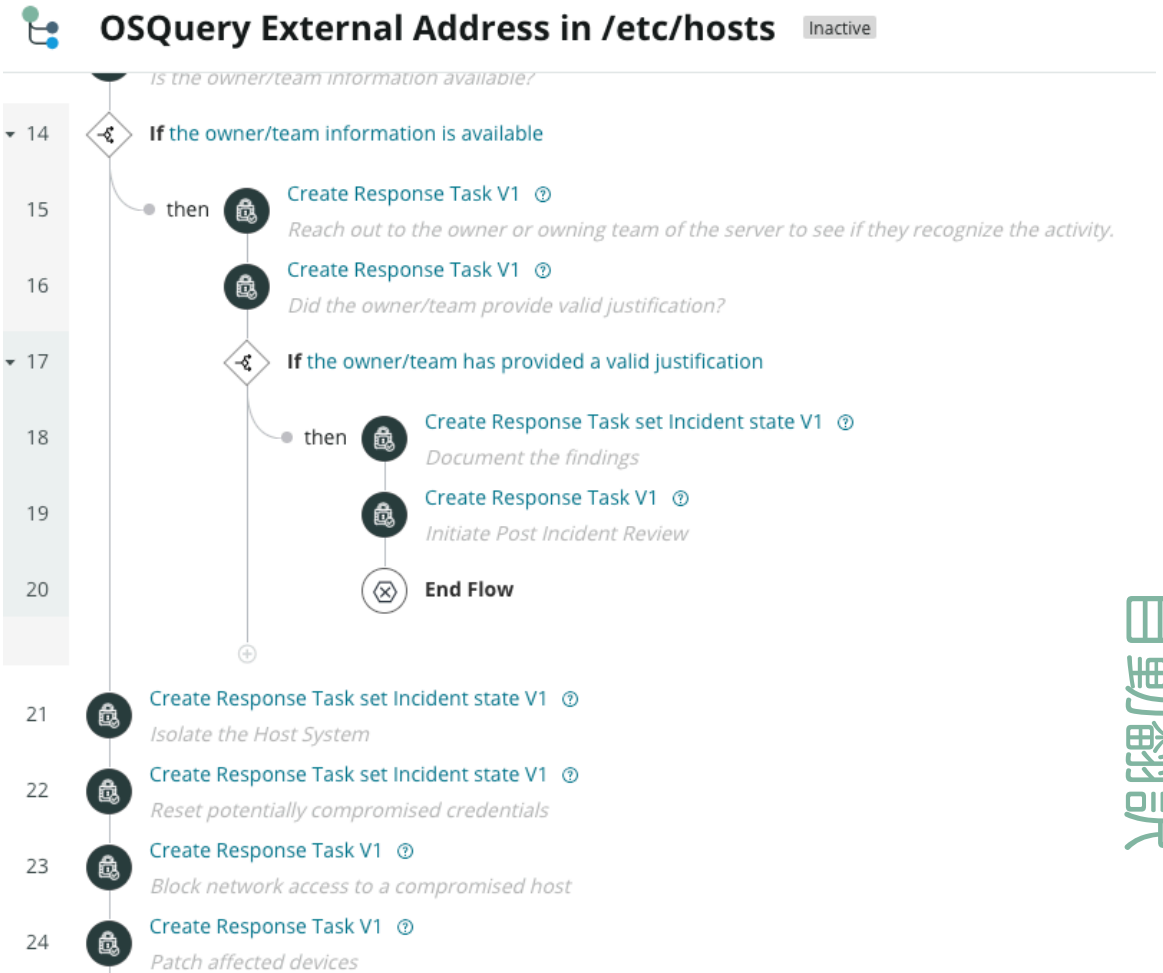
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

i. アクション 18 では、これまでの結果を文書化します。

ii. アクション 19 では、インシデントの事後レビューを開始します。

アクション 20 では、インシデントの事後レビューの後、フローが終了します。

/etc/hosts ファイル内の外部アドレスの **OSquery** プレイブックの使用



12. アクション 21 では、所有者またはチームの情報が使用できない場合に、ホストシステムを分離します。
13. アクション 22 では、侵害された可能性のある認証情報をリセットします。
14. アクション 23 では、侵害されたホストへのネットワークアクセスをブロックします。
15. アクション 24 では、影響を受けるデバイスにパッチを適用します。
16. アクション 25 では、封じ込めを解除し、システムを運用標準に戻します。
17. アクション 26 では、タスクをクローズする前にインシデントの事後レビューを完了します。

bash 履歴を削除するユーザー - クラウドのプレイブック

このプレイブックには、誰かが Linux サーバーから bash 履歴 (`.bash_history`) ファイルを削除しようとしたかどうかを示すインシデントを調査するための体系的な修復手順が記載されています。

注:
このアラートがトリガーされることはめったにないものの、インサイダーの脅威の可能性を示すため、このアラートの緩和は慎重に行う必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

bash 履歴を削除するユーザープレイブックを設定する

bash 履歴を削除するユーザープレイブックを設定するには、以下の手順に従います。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

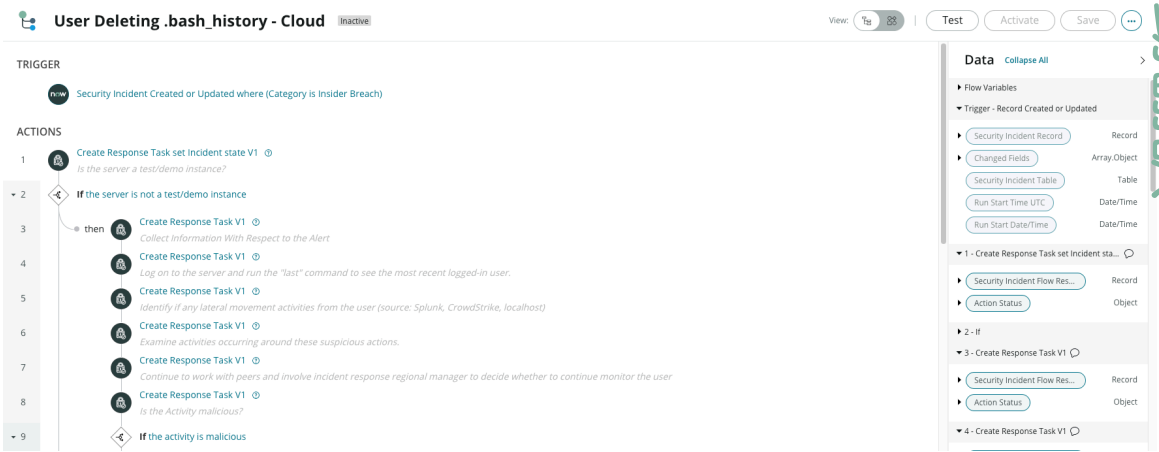
Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 ユーザーによる.bash_historyの削除 - クラウド プレイブックを選択します。
3. オプション: .bash_history を削除するユーザー - クラウドプレイブックのフローのコピーを作成し、必要な変更を加えます。

   (Optional) プレイブックのフローのコピーを作成するには、 アイコンを選択し、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

   bash 履歴を削除するユーザー - クラウドプレイブック

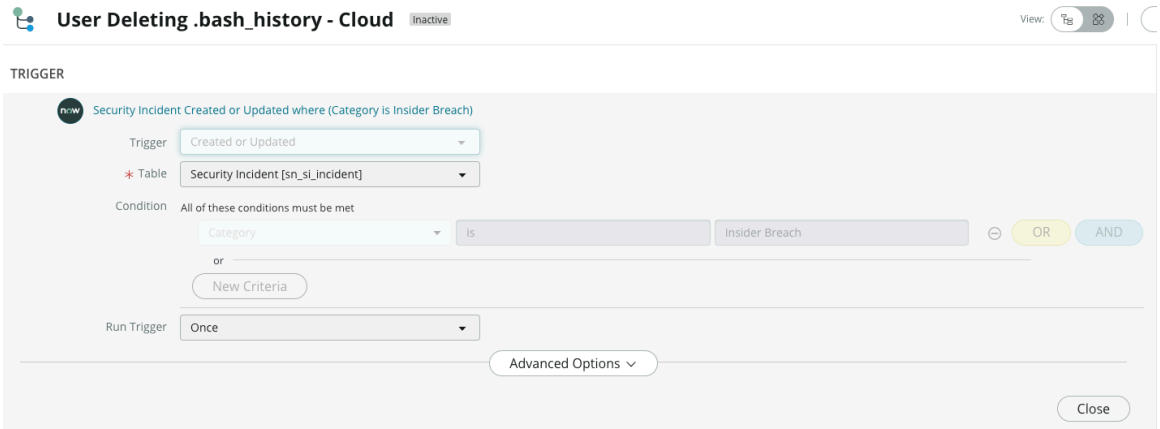
   

4. プレイブックをアクティブ化します。
   a. ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   b. 必要な変更を行った後、コピーしたフローをアクティブ化します。
5. プレイブックの [トリガー条件] を設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このプレイブックは、[カテゴリ] が [内部違反 **(Insider Breach)]** である場合にトリガーされ、セキュリティインシデントに関連付けられます。

bash 履歴を削除するユーザー - クラウドプレイブックのトリガー条件



bash 履歴を削除するユーザープレイブックを使用する

このプレイブックを使用して、誰かが Linux サーバーから bash 履歴ファイルを削除しようとしたかどうかを示すインシデントを調査します。以下に示すステップは、bash 履歴 (*.bash_history*) を削除するユーザープレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

手順

1. プレイブックがトリガーされて実行が開始されたら、アクション 1 で、サーバーがテストインスタンスであるかデモインスタンスであるかを確認します。
2. アクション 2 では、サーバーがテストインスタンスまたはデモインスタンスでない場合に、次の手順を実行します。

   a. アクション 3 では、アラートについての次の情報を収集します。
      - ユーザー名
      - IP アドレス
      - bash 履歴を削除しようとする悪意のあるコマンド
      - ユーザーが実行したすべてのコマンド (CrowdStrike ログから入手可能な場合)。

   b. アクション 4 では、サーバーにログインし、*last* コマンドを実行して、最後にログインしたユーザーを表示します。

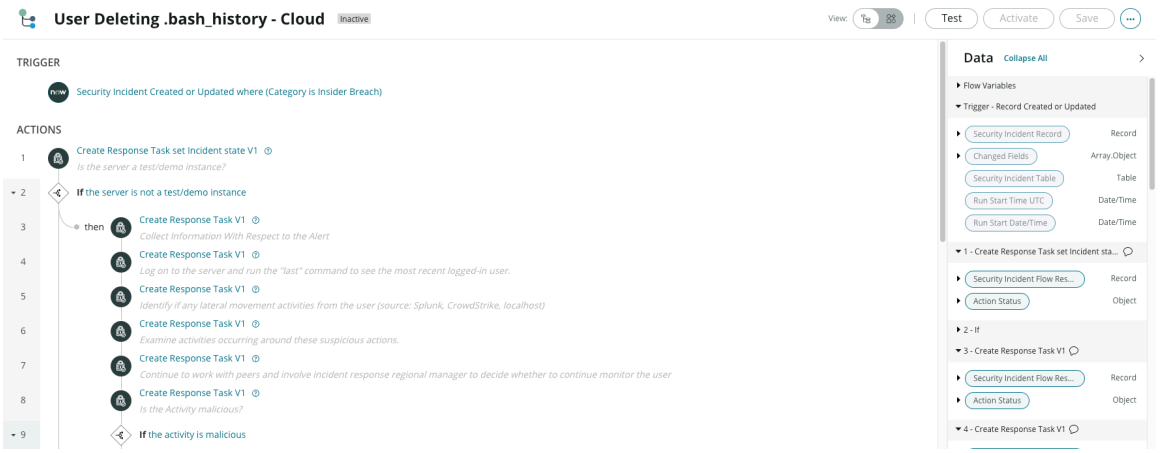
   c. アクション 5 では、ユーザーからの横方向移動アクティビティがあったかどうかを特定します (ソース：Splunk、CrowdStrike、localhost)。

   d. アクション 6 では、これらの疑わしいアクションの周囲で発生しているアクティビティを調べます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

bash 履歴を削除するユーザープレイブック



e. アクション 7 では、同僚との作業を続行し、インシデント応答地域マネージャーを関与させて、ユーザーの監視を継続するかどうかを決定します。

f. アクション 8 では、アクティビティが悪意のあるものであるかどうかを判断します。

g. アクション 9 では、アクティビティが悪意のあるものであった場合に、次の手順を実行します。

i. アクション 10 では、調査中に IT サポートに連絡してアカウントの凍結を要求します。

ii. アクション 11 では、インスタンスが通常の状態に復元され、悪意のあるアクティビティがないことを確認します。

iii. アクション 12 では、封じ込めを解除し、システムを運用標準に戻します。

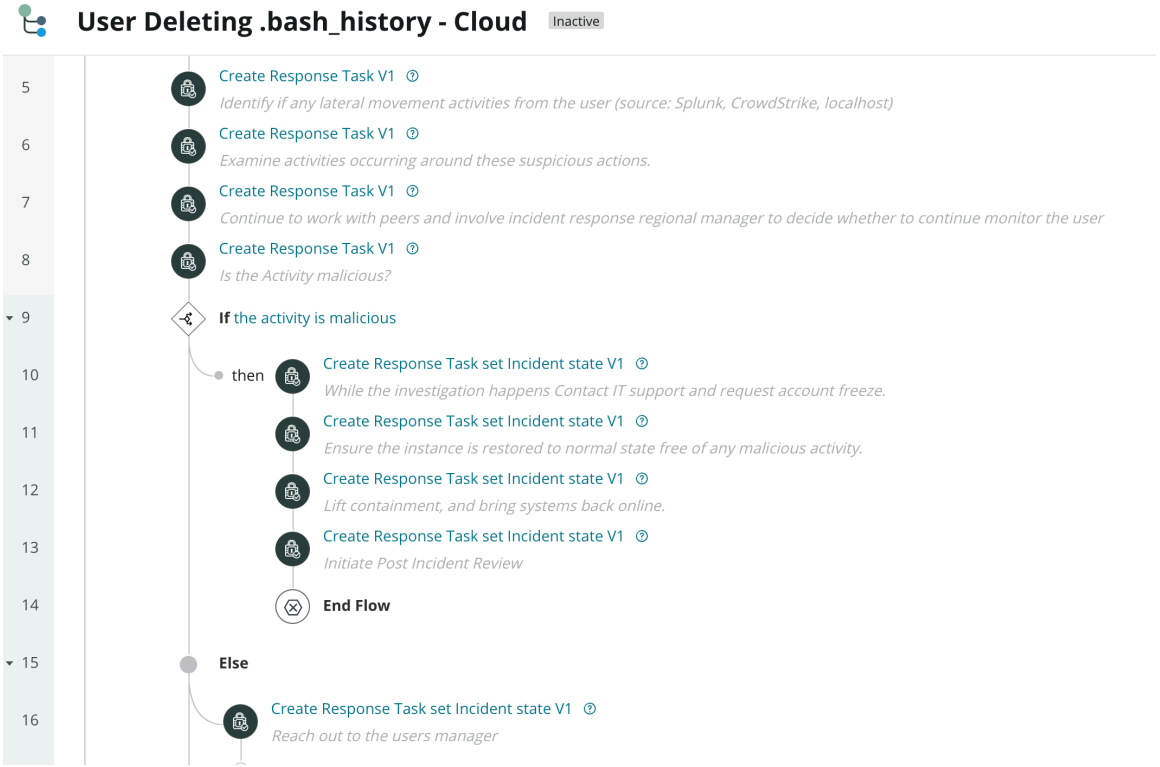
iv. アクション 13 では、インシデントの事後レビューを開始します。

アクション 14 では、インシデントの事後レビューの後、フローが終了します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

bash 履歴を削除するユーザープレイブックの使用



h. アクション 15 では、アクティビティが悪意のあるものでない場合に、アクション 16 で、ユーザーのマネージャーに連絡します。
提供されたメールテンプレートを使用してユーザーのマネージャーに連絡し、推奨されるアプローチについて知らせることができます。

3. アクション 17 では、これまでの結果を文書化します。

4. アクション 18 では、タスクをクローズする前にインシデントの事後レビューを完了します。

サービスアカウントからの正常な **VPN** 試行 **-** 企業/クラウドのプレイブック

このプレイブックでは、VPN を介したサービスアカウントからの成功したログイン試行を追跡するインシデントを調査するための体系的な修復手順が提供されます。サービスアカウントでは VPN からのログインイベントは想定されておらず、そのようなイベントはブルートフォースまたはアカウントの認証情報の公開の可能性のいずれかを示している可能性があります。

サービスアカウントからの正常な **VPN** 試行プレイブックを設定する

サービスアカウントからの正常な VPN 試行プレイブックを設定するには、以下の手順に従います。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

自動翻訳

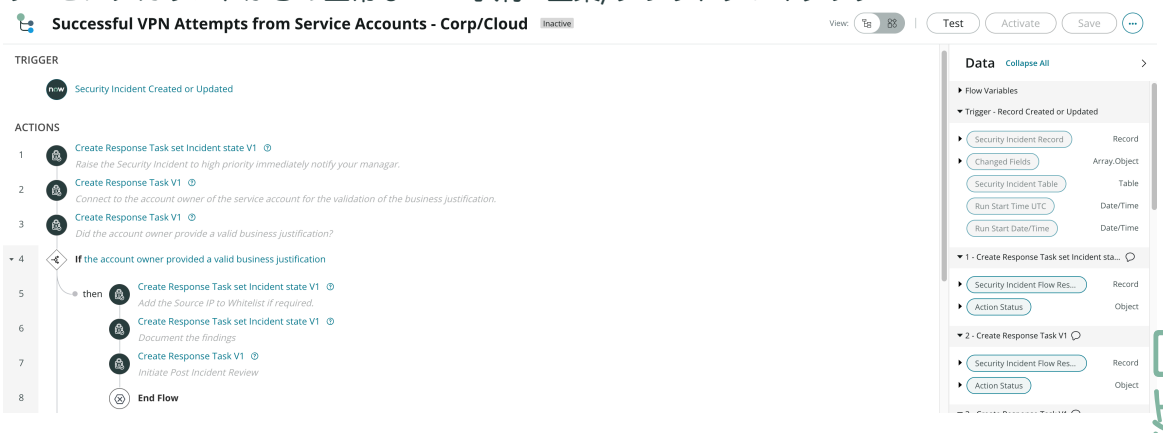
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 サービスアカウントからの正常な **VPN** 試行 プレイブックを選択します。
3. オプション: サービスアカウントからの正常な VPN 試行プレイブックのフローのコピーを作成し、必要な変更を加えます。

   (Optional) プレイブックのフローのコピーを作成するには、 アイコンを選択し、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

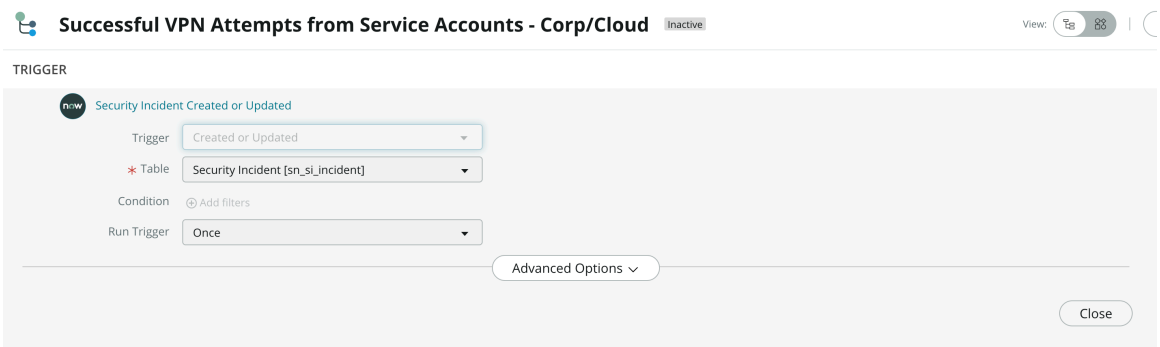
   サービスアカウントからの正常な **VPN** 試行 **-** 企業/クラウドプレイブック



4. プレイブックをアクティブ化します。
   a. ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   b. 必要な変更を行った後、コピーしたフローをアクティブ化します。
5. プレイブックの [トリガー条件] を設定します。

   このプレイブックは、必要な条件に基づいてセキュリティインシデントが作成または更新されると、トリガーされ、セキュリティインシデントに関連付けられます。たとえば、[カテゴリ] が [内部違反] である場合などです。

   サービスアカウントからの正常な **VPN** 試行 **-** 企業/クラウドプレイブックのトリガー条件



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サービスアカウントからの正常な **VPN** 試行プレイブックを使用する

このプレイブックを使用して、VPN を介したサービスアカウントからの成功したログイン試行を追跡するインシデントを調査します。以下に示すステップは、サービスアカウントからの正常な VPN 試行プレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に

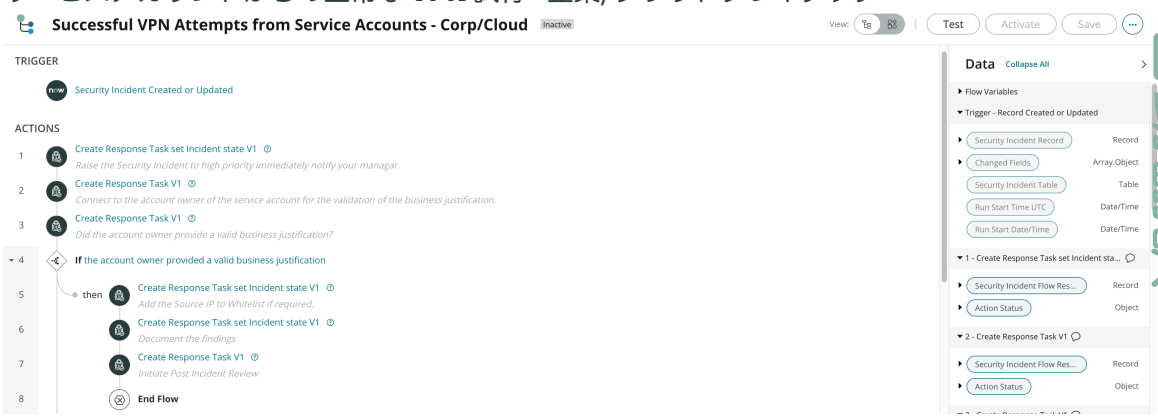
必要なロール：

- sn_si.admin
- flow_designer

手順

1. プレイブックがトリガーされて実行が開始されたら、アクション 1 で、セキュリティインシデントを優先度「高」に引き上げ、すぐにマネージャーに通知します。
2. アクション 2 では、ビジネス上の根拠を検証するためにサービスアカウントの所有者に連絡します。
   提供されたメールテンプレートを使用して、サービスアカウントの所有者に連絡し、ビジネス上の根拠を検証することができます。
3. アクション 3 では、サービスアカウントオーナーが有効なビジネス上の根拠を提供したかどうかを確認します。

サービスアカウントからの正常な **VPN** 試行 **-** 企業/クラウドプレイブック



4. アクション 4 では、サービスアカウント所有者が有効なビジネス上の根拠を提供した場合に、次の手順を実行します。

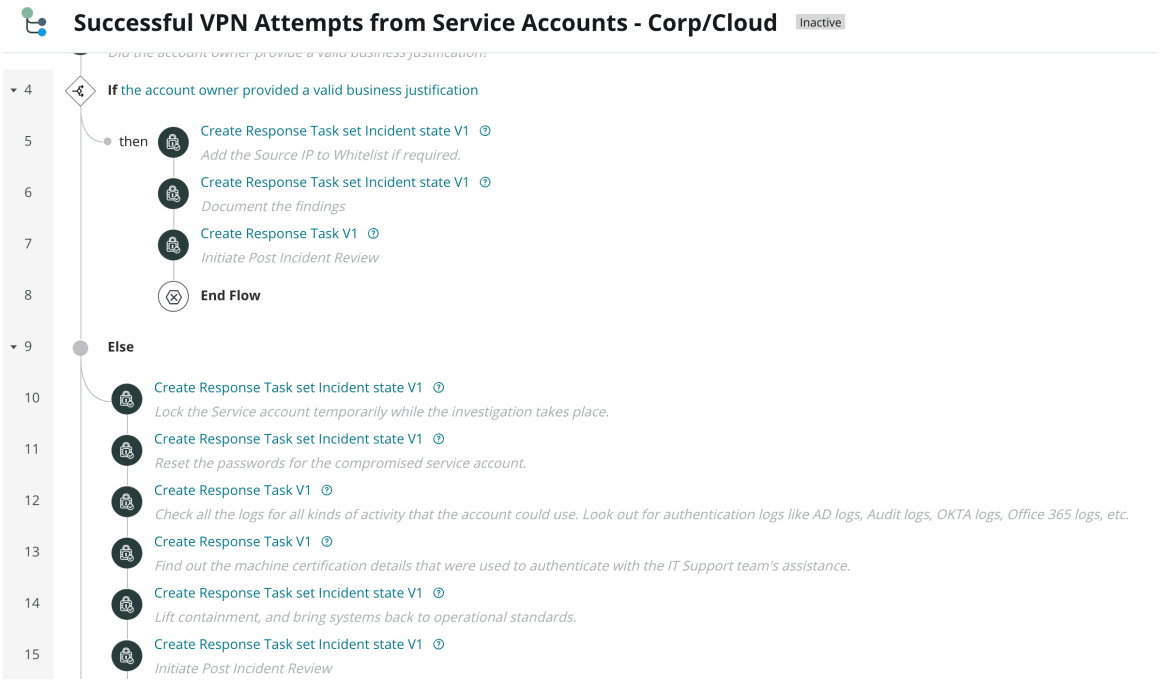
   a. アクション 5 では、必要に応じてソース IP を許可リストに追加します。

   b. アクション 6 では、これまでの結果を文書化します。

   c. アクション 7 では、インシデントの事後レビューを開始します。
      アクション 8 では、インシデントの事後レビューの後、フローが終了します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サービスアカウントからの正常な **VPN** 試行 **-** 企業/クラウドプレイブックの使用



5. アクション 9 では、サービスアカウント所有者が有効なビジネス上の根拠を提供しなかった場合に、次の手順を実行します。

   a. アクション 10 では、調査の実行中にサービスアカウントを一時的にロックします。

   b. アクション 11 では、侵害されたサービスアカウントのパスワードをリセットします。

   c. アクション 12 では、アカウントが使用できるあらゆる種類のアクティビティのログを確認します。
   Active Directory ログ、監査ログ、Okta ログ、Office 365 ログなどの認証ログを探します。

   d. アクション 13 では、IT サポートチームの支援による認証に使用されるマシン認定の詳細を見つけます。

   e. アクション 14 では、封じ込めを解除し、システムを運用標準に戻します。

   f. アクション 15 では、タスクをクローズする前にインシデントの事後レビューを完了します。

非アクティブ化されたアカウントへのアクセス試行用のプレイブック

このプレイブックは、アカウントが終了、無効化、または分離されている従業員が認証情報を使用してログインしようとするとトリガーされます。Sailpoint でのユーザーの ID 状態は、通常は終了日に更新され、無効になります。

終了日から 30 日というのが、分離された状態へと更新されるのに理想的な期間です。Sailpoint でビジネスロジックを使用して RSA アカウントを削除し、30 日後に Active Directory (AD) グループメンバーシップを削除できます。

非アクティブ化されたアカウントへのアクセス試行プレイブックを設定する

非アクティブ化されたアカウントへのアクセス試行プレイブックを設定するには、以下の手順に従います。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：

- sn_si.admin
- flow_designer

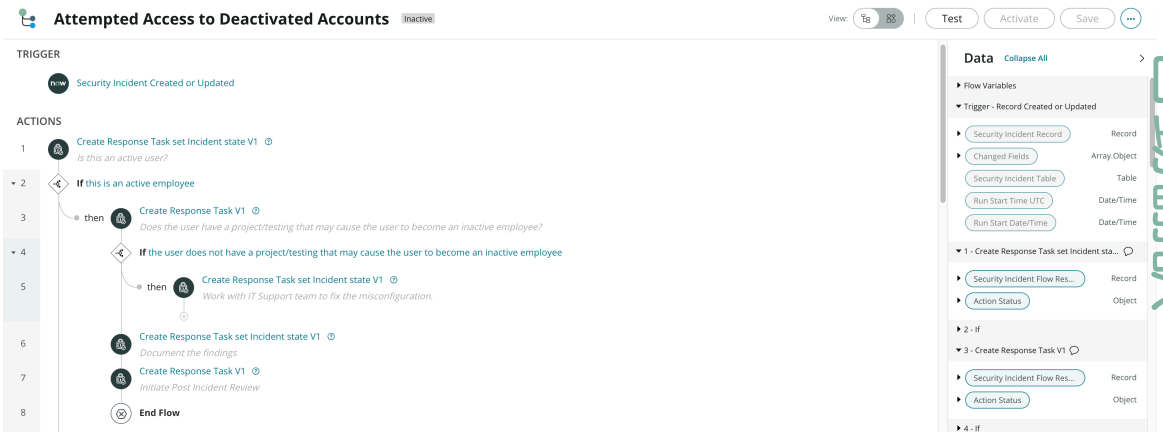
Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 非アクティブ化されたアカウントへのアクセス試行 プレイブックを選択します。
3. オプション: 非アクティブ化されたアカウントへのアクセス試行プレイブックフローのコピーを作成し、必要な変更を加えます。

   (Optional) プレイブックのフローのコピーを作成するには、 アイコンを選択し、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

   非アクティブ化されたアカウントへのアクセス試行プレイブック

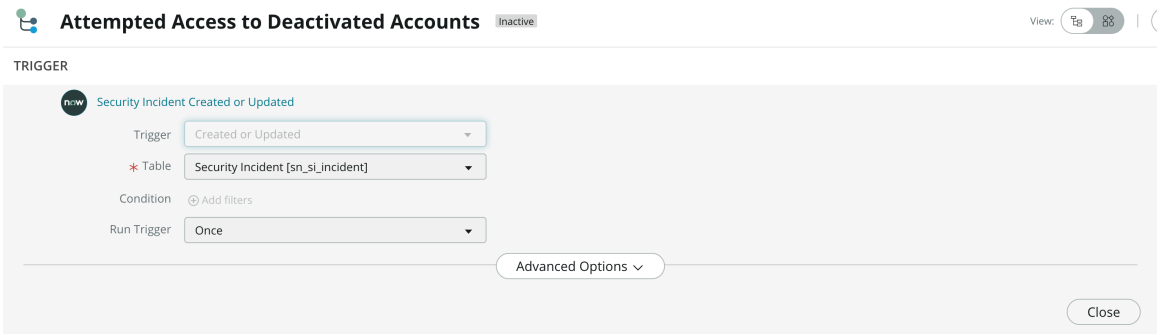
   

4. プレイブックをアクティブ化します。
   a. ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   b. 必要な変更を行った後、コピーしたフローをアクティブ化します。
5. プレイブックの [トリガー条件] を設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このプレイブックは、必要な条件に基づいてセキュリティインシデントが作成または更新されるとトリガーされます。たとえば、[カテゴリ] が [内部違反] である場合などです。

非アクティブ化されたアカウントへのアクセス試行プレイブックのトリガー条件



非アクティブ化されたアカウントへのアクセス試行プレイブックを使用する

このプレイブックは、アカウントが終了、無効化、または分離されている従業員が認証情報を使用してログインしようとする場合に使用します。以下に示すステップは、非アクティブ化されたアカウントへのアクセス試行プレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に

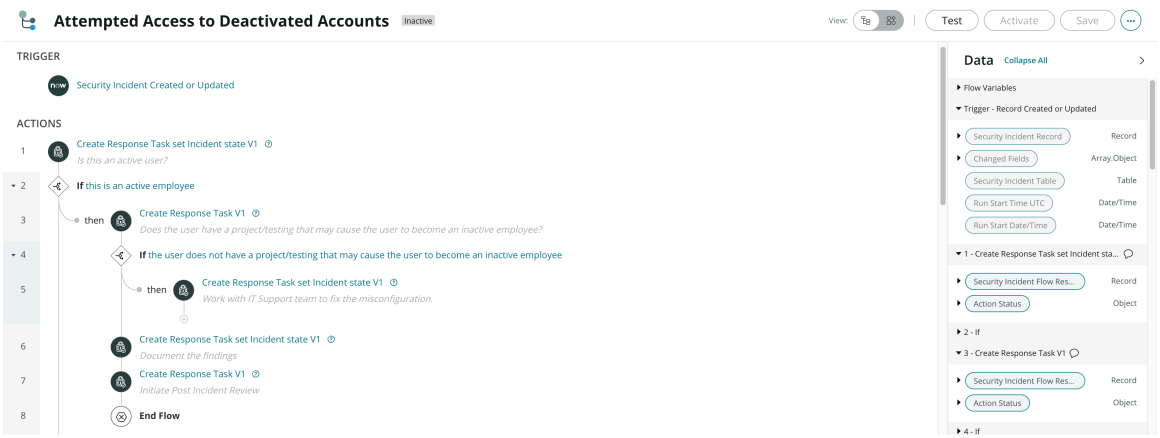
必要なロール：

- sn_si.admin
- flow_designer

手順

1. プレイブックがトリガーされて実行が開始されたら、アクション 1 で、非アクティブ化されたアカウントへのアクセスの試行がアクティブなユーザーによって行われたかどうかを確認します。
2. アクション 2 では、非アクティブ化されたアカウントへのアクセスの試行がアクティブな従業員によって行われたかどうかを確認します。

非アクティブ化されたアカウントへのアクセス試行プレイブック



3. 非アクティブ化されたアカウントへのアクセスの試行がアクティブな従業員によって行われた場合は、次の手順を実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. アクション 3 では、ユーザーに非アクティブな従業員となる原因となったプロジェクトまたはテストケースがあったかどうかを確認します。

b. アクション 4 では、ユーザーに非アクティブな従業員となる原因となったプロジェクトまたはテストケースがなかった場合に、IT サポートチームと協力して構成ミスを修正します。フローが終了します。

c. アクション 5 では、ユーザーに非アクティブな従業員となる原因となったプロジェクトまたはテストケースがあった場合に、次の手順を実行します。

i. アクション 6 では、これまでの結果を文書化します。

ii. アクション 7 では、インシデントの事後レビューを開始します。

アクション 8 では、インシデントの事後レビューの後、フローが終了します。

4. アクション 9 では、非アクティブ化されたアカウントへのアクセスの試行がアクティブな従業員によって行われた場合に、次の手順を実行します。

a. アクション 10 では、ユーザーのログインが成功したかどうかを確認します。

b. アクション 11 では、従業員がいつオフボーディングされたかを確認します。

c. アクション 12 では、Splunk のイベントを調査して、期間中のユーザーのアクティビティを調べます。

d. アクション 13 では、これまでの調査に基づいて、ユーザーがデータを盗み出したかどうかを判断します。

e. アクション 14 では、ユーザーがデータを盗み出していない場合に、次の手順を実行します。

i. アクション 15 では、IT サポートチームと協力してアクティブなセッションを終了し、アカウントを無効にします。

ii. アクション 16 では、これまでの結果を文書化します。

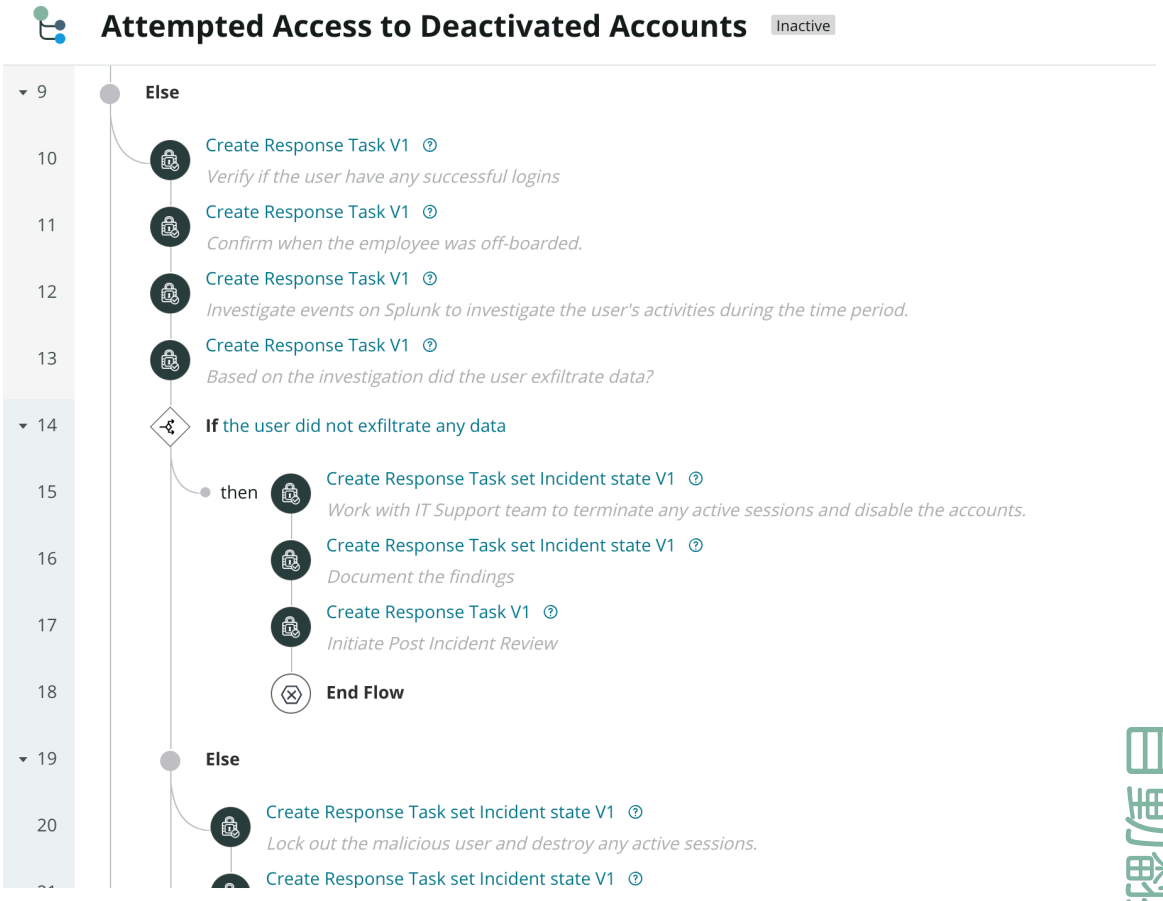
iii. アクション 17 では、インシデントの事後レビューを開始します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクション 18 では、インシデントの事後レビューの後、フローが終了します。

非アクティブ化されたアカウントへのアクセス試行プレイブックの使用



5. アクション 19 では、ユーザーがデータを盗み出していた場合に、次の手順を実行します。

a. アクション 20 では、悪意のあるユーザーをロックアウトし、アクティブなセッションをすべて破棄します。

b. アクション 21 では、IT サポートチームと協力してすべてのアカウントを無効にします。

c. アクション 22 では、リソースが通常の状態に復元され、悪意のあるアクティビティがないことを確認します。
必要に応じて、リソースを再イメージ化できます。

d. アクション 23 では、封じ込めを解除し、システムを運用標準に戻します。

e. アクション 24 では、タスクをクローズする前にインシデントの事後レビューを完了します。

T1003 - 防御回避 **- Mimikatz DCShadow** プレイブック

このプレイブックでは、Mimikatz DCShadow が原因と疑われるインシデントを調査するための体系的な修復ステップについて説明します。DCShadow は Mimikatz の機能であり、ドメインコントローラー (Active Directory を制御するサーバー) の動作をシミュレートして、標準のセキュリティコントロール (SIEM を含む) のほとんどをバイパスして独自のデータを挿入します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Mimikatz DCShadow は、攻撃者が Active Directory (AD) の一部となる不正なドメインコントローラー (DC) を設定する足がかりとなります。登録されると、正当な DC として機能し、損害を発生させる可能性があります。

T1003 - 防御回避 - Mimikatz DCShadow プレイブックを設定する

T1003 - 防御回避 - Mimikatz DCShadow プレイブックを設定するには、以下の手順に従います。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

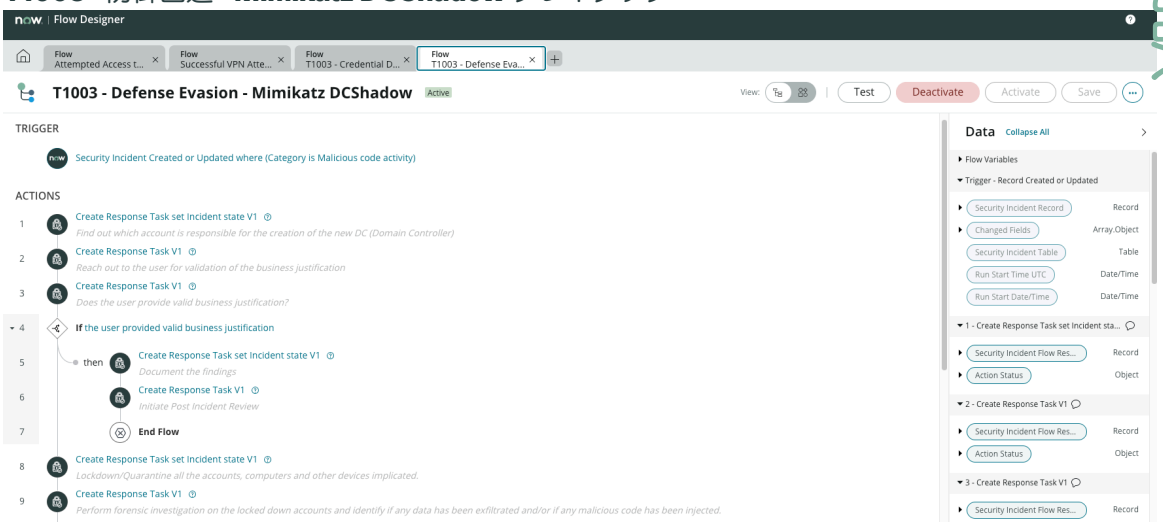
Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 **T1003 - 防御回避 - Mimikatz DCShadow** プレイブックを選択します。
3. オプション: T1003 - 防御回避 - Mimikatz DCShadow プレイブックのフローのコピーを作成し、必要な変更を加えます。

   (Optional) プレイブックのフローのコピーを作成するには、 アイコンを選択し、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

   T1003 - 防御回避 - Mimikatz DCShadow プレイブック

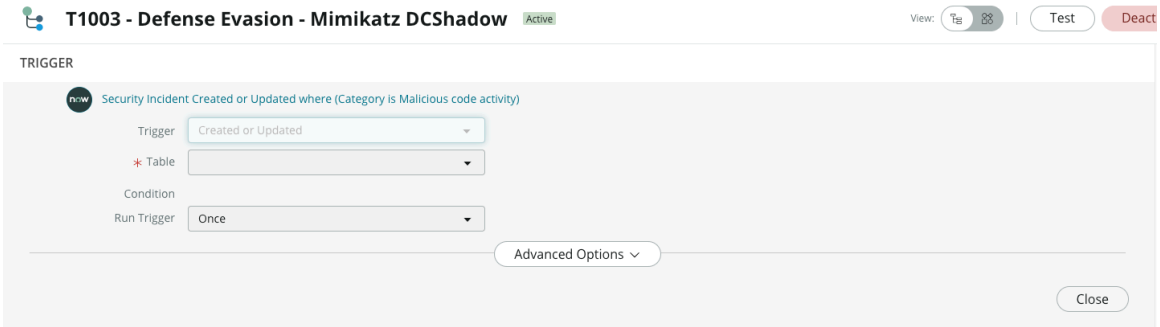


4. プレイブックをアクティブ化します。
   a. ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   b. 必要な変更を行った後、コピーしたフローをアクティブ化します。
5. プレイブックの [トリガー条件] を設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このプレイブックは、[カテゴリ] が [悪意のあるコードアクティビティ **(Malicious code activity)**] である場合にトリガーされ、セキュリティインシデントに関連付けられます。

T1003 - 防御回避 **- Mimikatz DCShadow** プレイブックのトリガー条件



T1003 - 防御回避 **- Mimikatz DCShadow** プレイブックを使用する

このプレイブックを使用して、Mimikatz DCShadow が原因と疑われるセキュリティインシデントを調査します。以下に示すステップは、T1003 - 防御回避 - Mimikatz DCShadow プレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

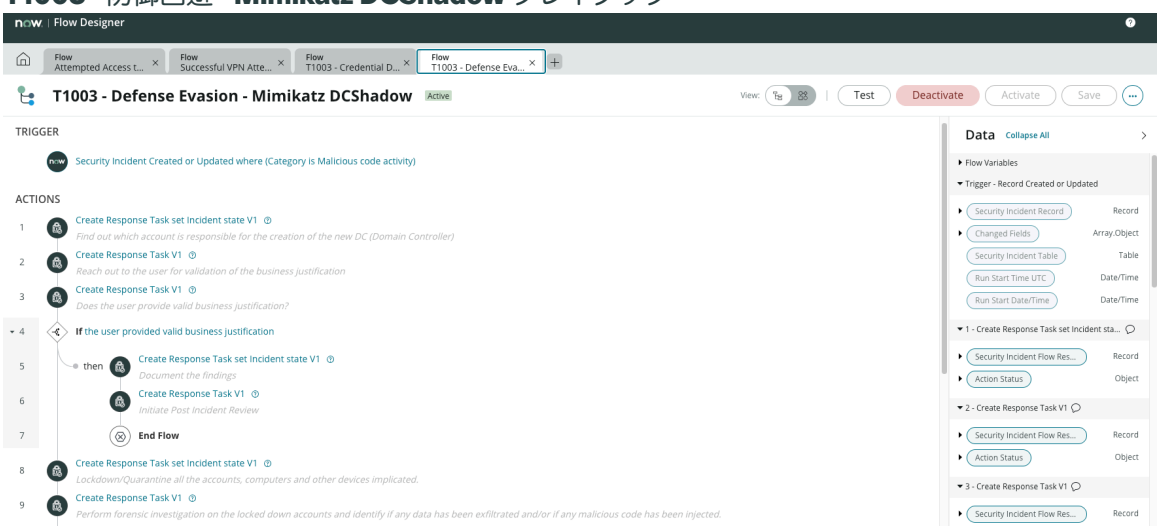
始める前に
必要なロール：

- sn_si.admin
- flow_designer

手順

1. プレイブックがトリガーされて実行が開始されたら、アクション 1 で、新しい DC (ドメインコントローラー) の作成を担当するアカウントを見つけます。
2. アクション 2 では、ビジネス上の根拠を検証するためにユーザーに連絡します。
   提供されたメールテンプレートを使用して、ユーザーに連絡できます。
3. アクション 3 では、ユーザーが有効なビジネス上の根拠を提供したかどうかを確認します。
4. アクション 4 で、ユーザーが有効なビジネス上の根拠を提供した場合は、次の手順を実行します。

T1003 - 防御回避 **- Mimikatz DCShadow** プレイブック



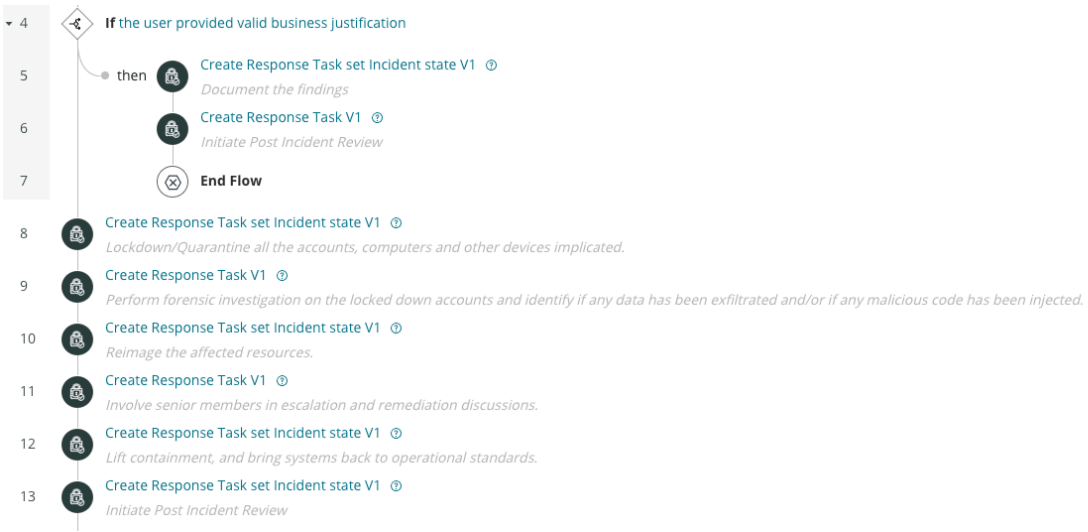
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. アクション 5 では、これまでの結果を文書化します。

b. アクション 6 では、インシデントの事後レビューを開始します。
アクション 7 では、インシデントの事後レビューの後、フローが終了します。

5. アクション 8 では、ユーザーが有効なビジネス上の正当な理由を提供しなかった場合に、次の手順を実行します。

T1003 - 防御回避 - Mimikatz DCShadow プレイブックを使用する



a. アクション 9 では、関連するすべてのアカウント、コンピューター、およびその他のデバイスをロックダウンまたは隔離します。

b. アクション 10 では、ロックダウンされたアカウントについてフォレンジック調査を実行し、データが盗み出されていないか、悪意のあるコードが挿入されていないかを特定します。

c. アクション 11 では、影響を受けるリソースを再イメージ化します。

d. アクション 12 では、封じ込めを解除し、システムを運用標準に戻します。

e. アクション 13 では、タスクをクローズする前にインシデントの事後レビューを完了します。

T1003 - 認証情報ダンピング **- Mimikatz DCSync** のプレイブック

このプレイブックでは、Mimikatz DCSync が原因と疑われるインシデントを調査するための体系的な修復ステップについて説明します。このプレイブックは、Mimikatz 関数 (`lsadump::d csync`) のいずれかが使用されたときにトリガーされます。この関数は通常、攻撃対象のドメインコントローラー (DC) で使用されます。

Mimikatz は、攻撃対象のシステムから機密データを取得するコマンドを発行できる一般的なハッキングツールです。機密データには、パスワードやハッシュなどが含まれます。

注:
これは忠実度の高いアラートであり、まれにしかトリガーされないと想定されています。トリガーされたら、上級チームメンバーまたはマネージャーにすぐに通知する必要があります。

T1003 - 認証情報ダンピング **- Mimikatz DCsync** プレイブックを設定する

T1003 - 認証情報ダンピング - Mimikatz DCsync プレイブックを設定するには、以下の手順に従います。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：

- sn_si.admin
- flow_designer

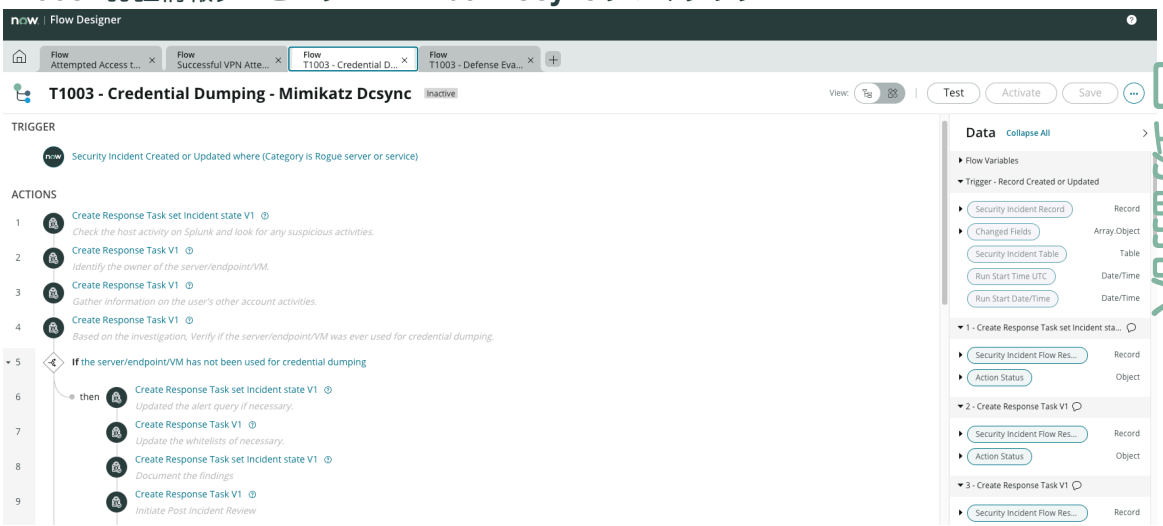
Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 **T1003 -** 認証情報ダンピング **- Mimikatz DCsync** プレイブックを選択します。
3. オプション: T1003 - 認証情報ダンピング - Mimikatz DCsync プレイブックのフローのコピーを作成し、必要な変更を加えます。

   (Optional) プレイブックのフローのコピーを作成するには、 アイコンを選択し、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

   T1003 - 認証情報ダンピング **- Mimikatz DCSync** プレイブック

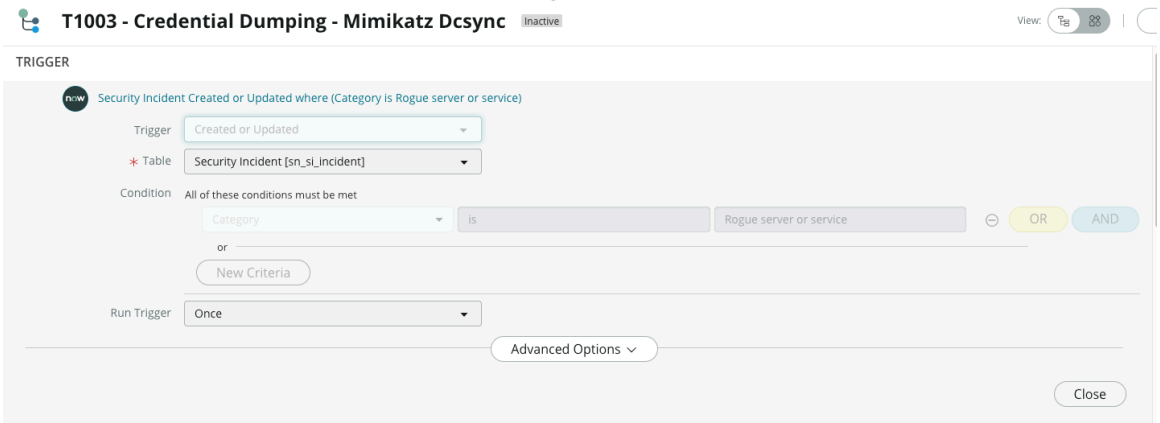


4. プレイブックをアクティブ化します。
   a. ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   b. 必要な変更を行った後、コピーしたフローをアクティブ化します。
5. プレイブックの [トリガー条件] を設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このプレイブックは、[カテゴリ] が [不正サーバーまたはサービス] である場合にトリガーされ、セキュリティインシデントに関連付けられます。

T1003 - 認証情報ダンピング **- Mimikatz DCSync** プレイブックのトリガー条件



T1003 - 認証情報ダンピング **- Mimikatz DCsync** プレイブックを使用する

このプレイブックを使用して、Mimikatz DCSync が原因と疑われるインシデントを調査します。以下に示すステップは、T1003 - 認証情報ダンピング - Mimikatz DCsync プレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に
必要なロール：

- sn_si.admin
- flow_designer

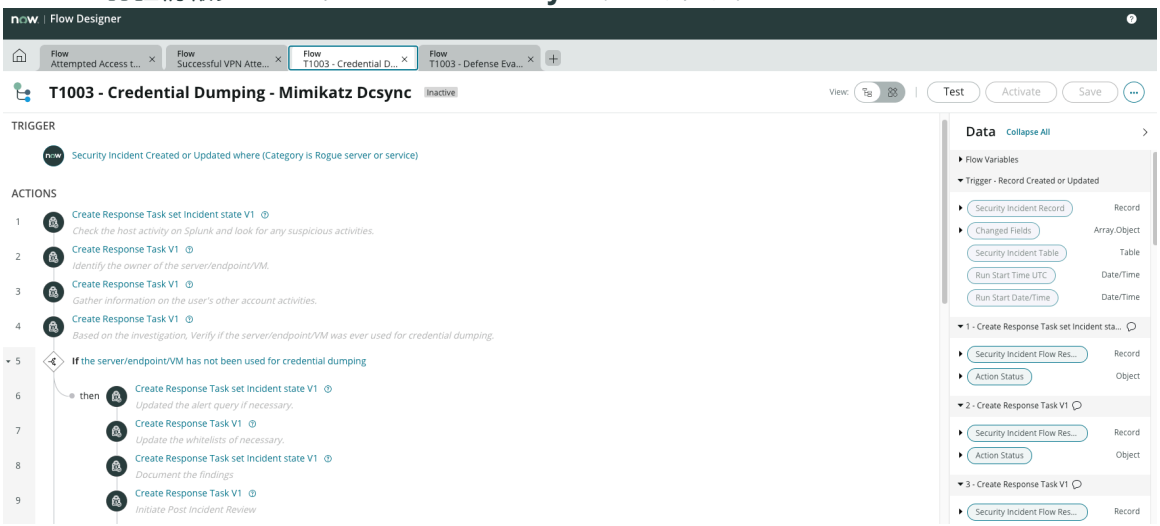
手順

1. プレイブックがトリガーされて実行が開始されたら、アクション 1 で Splunk のホストアクティビティを確認し、疑わしいアクティビティを探します。
2. アクション 2 では、サーバー/エンドポイント/VM の所有者を特定します。
   ユーザーがオンラインの場合は、CrowdStrike EDR を実行して、さらに広い範囲のシステムのアクティビティを収集します。
3. アクション 3 では、ユーザーの他のアカウントアクティビティに関する情報を収集します。
4. アクション 4 では、調査に基づいて、サーバー/エンドポイント/VM が認証情報ダンピングに使用されたことがあるかどうかを確認します。
5. アクション 5 では、サーバー/エンドポイント/VM が認証情報ダンピングに使用ていなかった場合に、次のアクションを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

T1003 - 認証情報ダンピング - Mimikatz DCsync プレイブック



a. アクション 6 では、必要に応じてアラートクエリを更新します。

b. アクション 7 では、必要に応じて許可リストを更新します。

c. アクション 8 では、これまでの結果を文書化します。

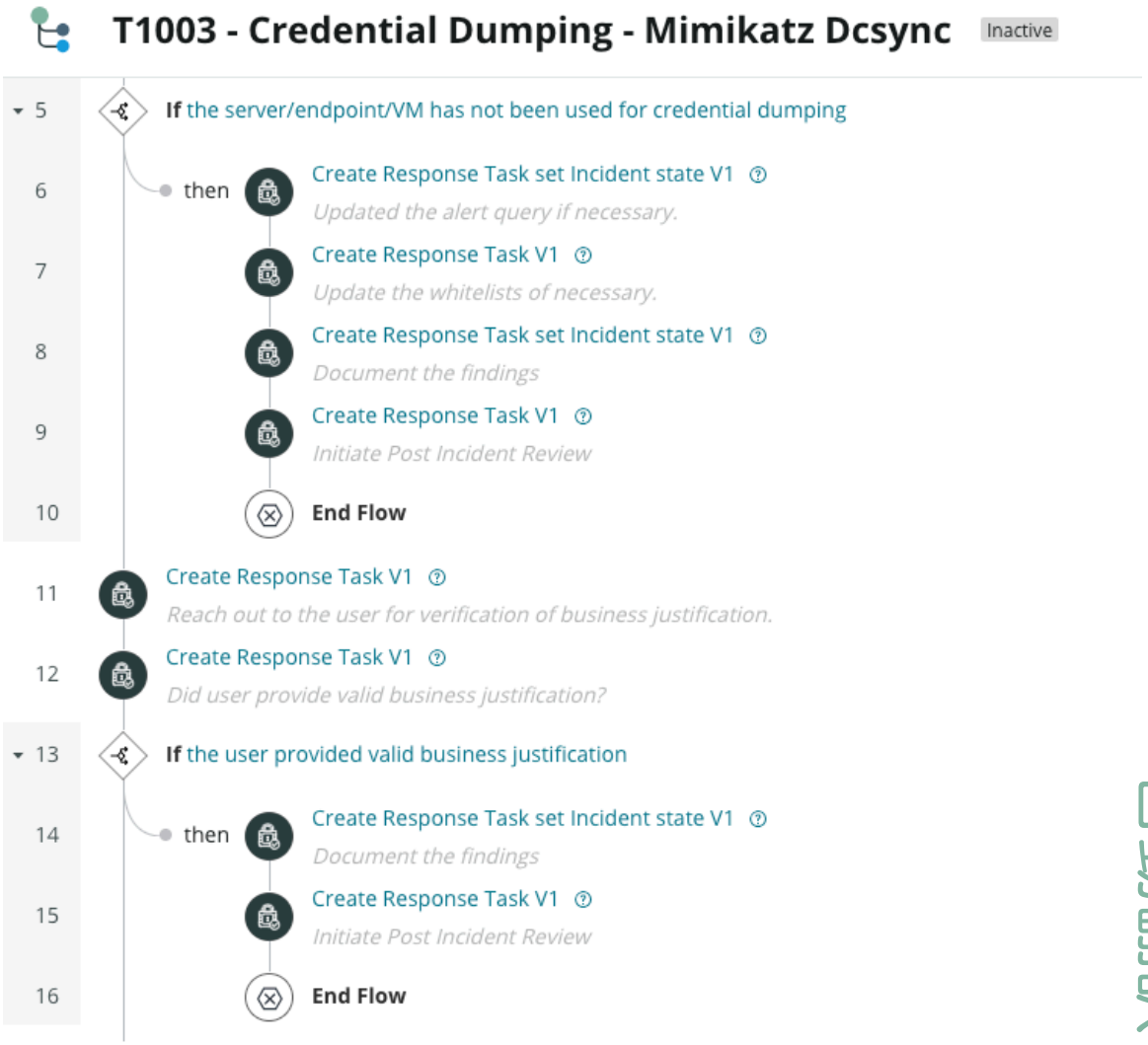
d. アクション 9 では、インシデントの事後レビューを開始します。
アクション 10 で、フローは終了します。

6. サーバー/エンドポイント/VM が認証情報ダンピングに使用されていた場合は、アクション 11 でユーザーに連絡します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

T1003 - 認証情報ダンピング **- Mimikatz DCsync** プレイブックの使用



自動翻訳

7. アクション 12 では、ビジネス上の根拠を検証するためにユーザーに連絡します。
8. アクション 13 では、ユーザーが有効なビジネス上の根拠を提供した場合に、次のアクションを実行します。

   a. アクション 14 では、これまでの結果を文書化します。

   b. アクション 15 では、インシデントの事後レビューを開始します。
   アクション 16 で、フローは終了します。

9. ユーザーが有効なビジネス上の根拠を提供しなかった場合には、アクション 17 でシステムを検疫します。
10. アクション 18 では、不正なアカウントによって作成または削除された可能性のある不要なファイルを削除します。
11. アクション 19 では、封じ込めを解除し、システムを運用標準に戻します。
12. アクション 20 では、タスクをクローズする前にインシデントの事後レビューを完了します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

複数の IP からの Okta ユーザーログイン失敗のプレイブック

このプレイブックでは、Okta でのユーザーログイン失敗のインシデントを調査するための体系的な修正手順について説明します。

複数の IP からの Okta ユーザーログイン失敗プレイブックには、Okta で複数の ServiceNow 以外の IP からの ServiceNow アカウントエラーが観察された場合のアラートの分析について説明しています。このプレイブックに関連するアラートについては、Okta ログを確認します。ServiceNow 以外の IP 範囲から ServiceNow ユーザー ID のログインに 1 時間以内に 3 回を超えて失敗した場合、アラートがトリガーされます。

複数の IP からの Okta ユーザーログイン失敗プレイブックを設定する

複数の IP からの Okta ユーザーログイン失敗プレイブックを設定するには、以下の手順に従います。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

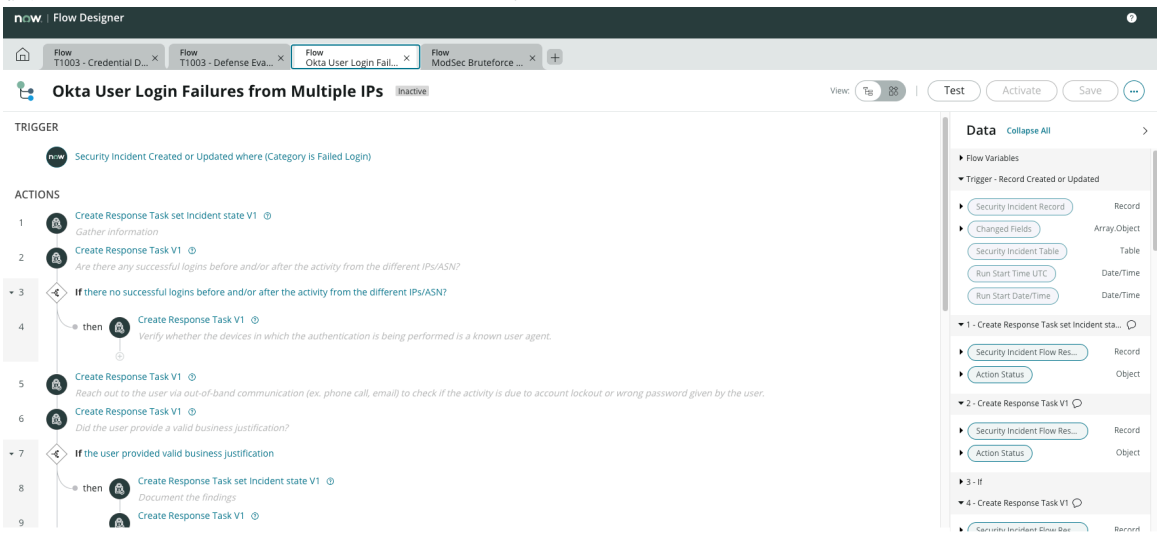
Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 複数の **IP** からの **Okta** ユーザーログイン失敗 プレイブックを選択します。
3. オプション: 複数の IP からの Okta ユーザーログイン失敗プレイブックのフローのコピーを作成し、必要な変更を加えます。

   (Optional) プレイブックのフローのコピーを作成するには、 アイコンを選択し、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

   複数の **IP** からの **Okta** ユーザーログイン失敗プレイブック



4. プレイブックをアクティブ化します。

自動翻訳

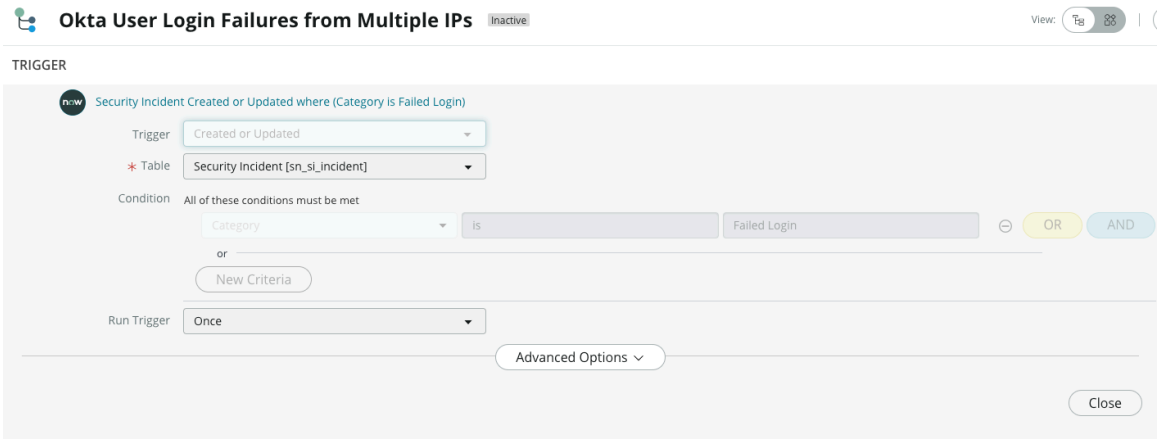
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。

b. 必要な変更を行った後、コピーしたフローをアクティブ化します。

5. プレイブックの [トリガー条件] を設定します。
このプレイブックは、[カテゴリ] が [失敗したログイン] である場合にトリガーされ、セキュリティインシデントに関連付けられます。

複数の **IP** からの **Okta** ユーザーログイン失敗プレイブックのトリガー条件



複数の **IP** からの **Okta** ユーザーログイン失敗プレイブックを使用する

このプレイブックを使用して、Okta でのユーザーログイン失敗のセキュリティインシデントを調査します。以下に示すステップは、複数の IP からの Okta ユーザーログイン失敗プレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に

必要なロール：

- sn_si.admin
- flow_designer

手順

1. プレイブックがトリガーされて実行が開始されたら、アクション 1 で次のタスクを実行します。
   - ターゲットとされているユーザーアカウントを特定します。
   - IP サブネットを確認し、すべてが同じ自律システム番号 (ASN) の所有者に属しているかどうかを確認します。

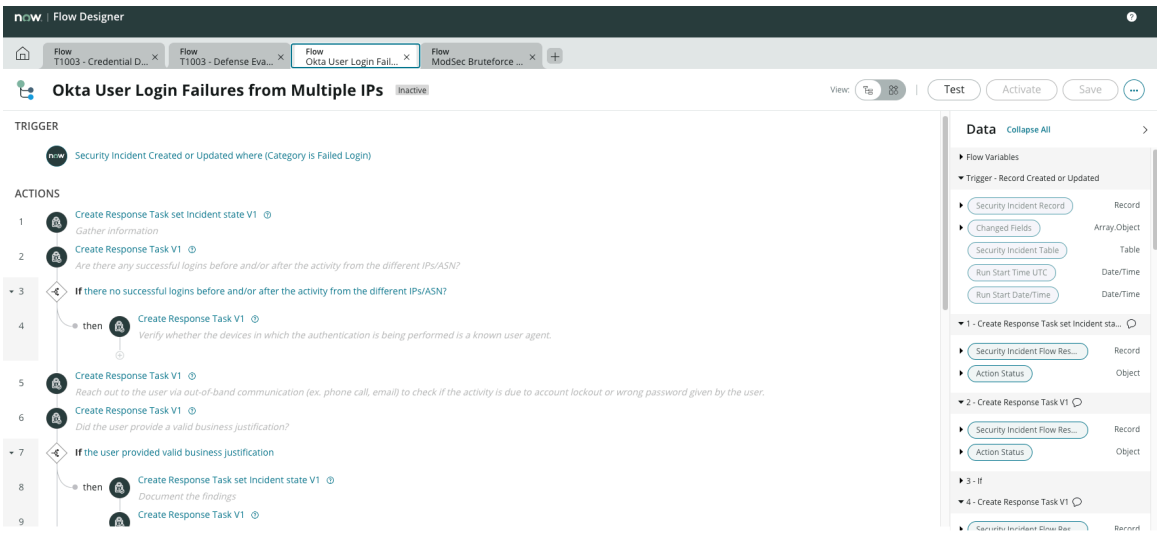
2. アクション 2 では、異なる IP/ASN からのアクティビティの前後に成功したログインがあったかどうかを確認します。

3. アクション 3 では、異なる IP/ASN からのアクティビティの前後にログインが成功しなかった場合に、アクション 4 で、認証が実行されているデバイスが既知のユーザーエージェントであるかどうかを確認します。
デバイスが既知のユーザーエージェントによって認証されると、フローは終了します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

複数の **IP** からの **Okta** ユーザーログイン失敗プレイブック



4. アクション 5 では、調査に基づいて、帯域外通信 (電話や電子メールなど) を使用してユーザーに連絡し、アクティビティがアカウントのロックアウトによるものか、ユーザーが提供したパスワードの誤りによるものかを確認します。
5. アクション 6 では、ユーザーが有効なビジネス上の根拠を提供したかどうかを確認します。
6. アクション 7 では、ユーザーが有効なビジネス上の根拠を提供した場合に、次のタスクを実行します。

   a. アクション 8 では、これまでの結果を文書化するための応答タスクを作成します。

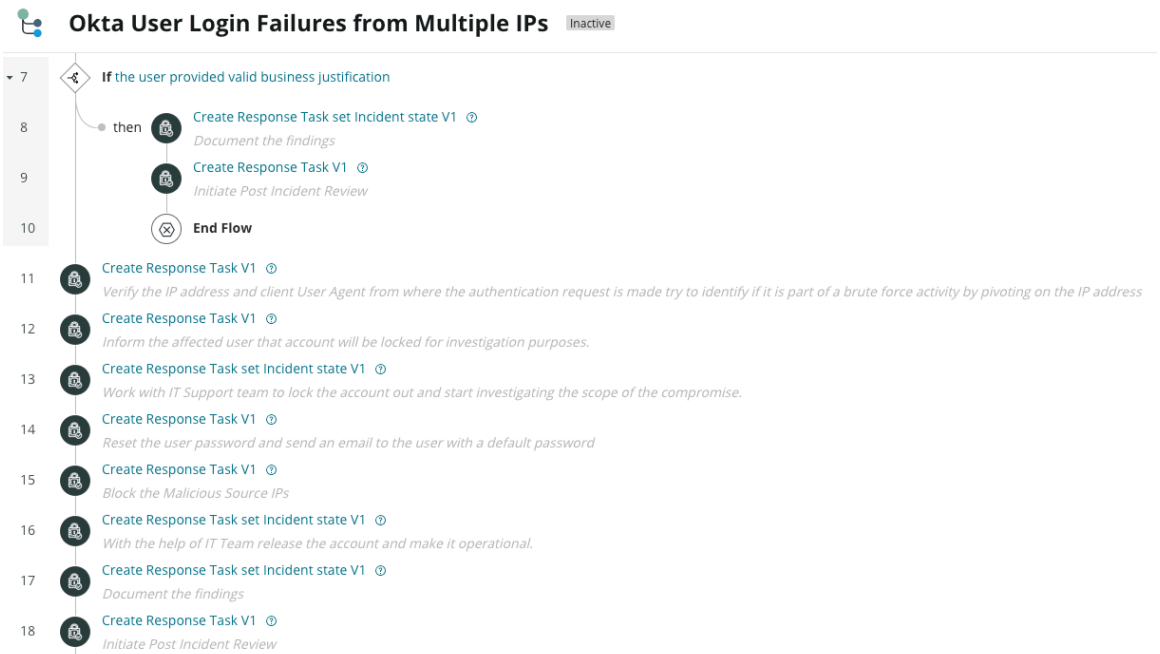
   b. アクション 9 では、インシデントの事後レビューを開始するための応答を作成します。
   アクション 10 で、フローは終了します。

7. アクション 11 では、認証要求が行われた IP アドレスとクライアントユーザーエージェントを確認し、IP アドレスをピボットしてブルートフォースアクティビティの一部であるかどうかを識別します。
8. アクション 12 では、影響を受けるユーザーに、調査目的でアカウントがロックされることを通知します。
   提供されたメールテンプレートを使用して、影響を受けるユーザーに通知できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

複数の **IP** からの **Okta** ユーザーログイン失敗プレイブックの使用



9. アクション 13 では、IT サポートチームと協力してアカウントをロックし、侵害の範囲の調査を開始します。
10. アクション 14 では、ユーザーパスワードをリセットし、デフォルトのパスワードを使用してユーザーにメールを送信します。
11. アクション 15 では、悪意のあるソース IP をブロックします。
12. アクション 16 では、アカウントを解放して運用標準に戻すための支援を IT サポートチームから受けます。
13. アクション 17 では、これまでの結果を文書化します。
14. アクション 18 では、タスクをクローズする前にインシデントの事後レビューを完了します。

自動翻訳

IP バーストによる **ModSec** ブルートフォースのプレイブック

このプレイブックでは、ModSec によって検出された複数の IP からのログインページでのブルートフォース試行のインシデントを調査するための、体系的な修復手順について説明します。イベント条件は ModSec ポリシー自体で設定でき、ModSec でイベントが作成されると Splunk でアラートが発生します。

このプレイブックは、ログインページの異常なトラフィックカウントを検出するのに役立ちます。この例では、50 ヒット/分を超える 2 つの連続したバーストは、1 つの IP からログインページに対するものであり、これはブルートフォースによるログイン試行を示します。

IP バーストによる **ModSec** ブルートフォースプレイブックを設定する

IP バーストによる ModSec ブルートフォースプレイブックを設定するには、以下の手順に従います。

始める前に
必要なロール：

- sn_si.admin
- flow_designer

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

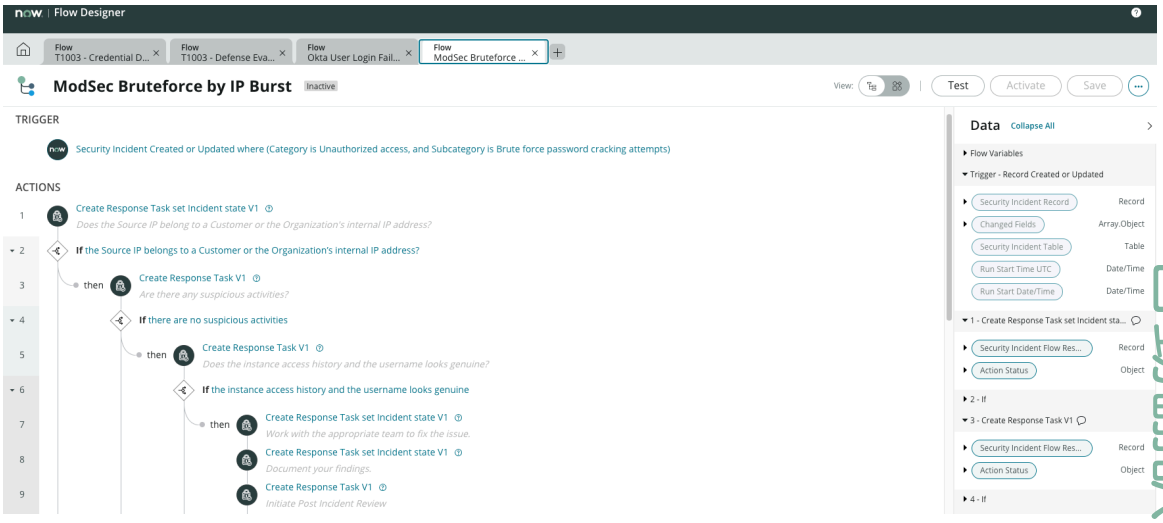
Security Operations スポーク (*sn_sec_spoke*) がインストールされていることを確認します。

手順

1. sn_si.user および flow_designer ロールを持つユーザーとしてログインします。
2. 次のように移動する。 **All** (すべて) > **Flow Designer** をクリックし、 **IP** バーストによる **ModSec** ブルートフォース プレイブックを選択します。
3. オプション: IP バーストによる ModSec ブルートフォースプレイブックのフローのコピーを作成し、必要な変更を加えます。

   (Optional) プレイブックのフローのコピーを作成するには、その他のアクションメニューアイコン ( ) を選択し、[コピーフロー] を選択します。フローをカスタマイズまたは変更する場合にのみ、このステップを実行します。

   IP バーストによる **ModSec** ブルートフォースプレイブック

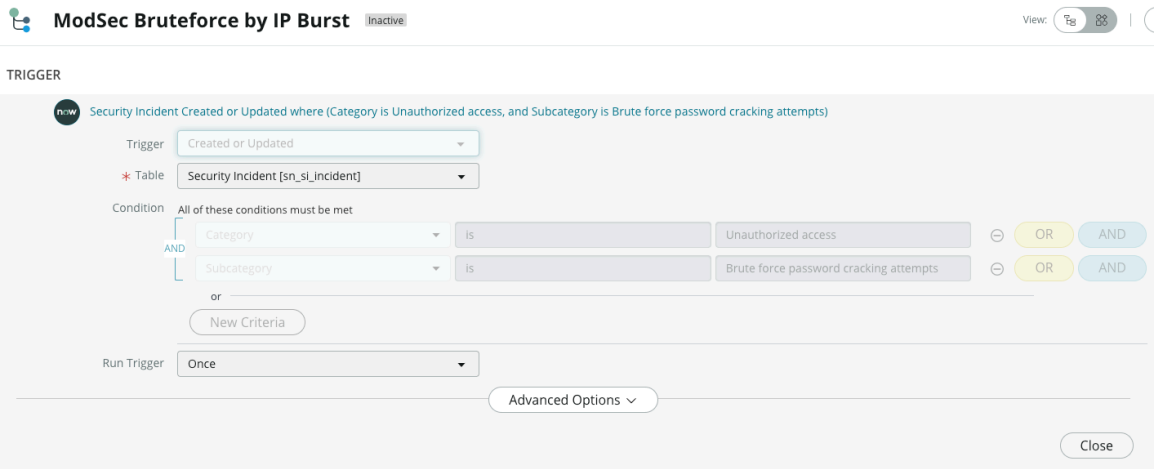


4. プレイブックをアクティブ化します。
   a. ベースシステムで利用可能なプレイブックを使用するには、メインフローをアクティブ化します。
   b. 必要な変更を行った後、コピーしたフローをアクティブ化します。
5. プレイブックの [トリガー条件] を設定します。
   このプレイブックは、次の条件が満たされるとトリガーされ、セキュリティインシデントに関連付けられます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [カテゴリ] は [無許可のアクセス] です。
- [サブカテゴリ] は [総当たりパスワード攻撃の試行] です。

IP バーストによる **ModSec** ブルートフォースプレイブックのトリガー条件



IP バーストによる **ModSec** ブルートフォースプレイブックを使用する

このプレイブックを使用して、ModSec によって検出された複数の IP からのログインページでのブルートフォース試行のインシデントを調査します。以下に示すステップは、IP バーストによる ModSec ブルートフォースプレイブックで使用できるアクション、タスク、サブフローの段階的な説明です。

始める前に

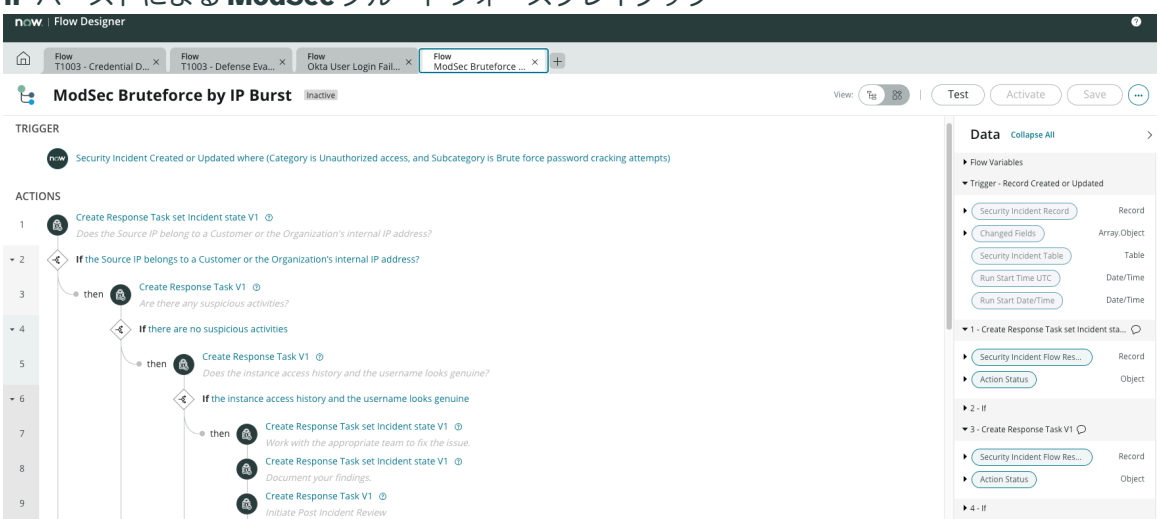
必要なロール：

- sn_si.admin
- flow_designer

手順

1. プレイブックがトリガーされて実行が開始されたら、アクション 1 で、ソース IP が顧客に属しているのか、組織の内部 IP アドレスに属しているのかを確認します。
2. アクション 2 では、ソース IP が顧客または組織の内部 IP アドレスに属している場合に、次の手順を実行します。

IP バーストによる **ModSec** ブルートフォースプレイブック



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. アクション 3 では、疑わしいアクティビティがあったかどうかを確認します。

- 過去数日間のソース IP からのアクティビティを確認します。IP のトラフィックがごくわずかである場合は、実際の攻撃を示しています。
- スプレーのユーザー名を確認します。たとえば、ユーザー名がアルファベット順に並んでいるかどうかを確認します。
- 関連する汎用アカウント名を探します。たとえば、admin、sysadmin、root、administrator、およびその他のアプリケーションアカウント名です。

不審なアクティビティがない場合、フローは終了します。

b. ステップ 4 では、不審なアクティビティがあった場合に、アクション 5 で、インスタンスのアクセス履歴とユーザー名が本物に見えるかどうかを確認します。

Appnode ログに障害の兆候がないか確認します。SAML、SSO、または LDAP 障害イベントが発生する可能性があります。これは運用上の問題が原因である可能性があります。

インスタンスのアクセス履歴とユーザー名が本物に見えない場合、フローは終了します。

c. アクション 6 では、インスタンスのアクセス履歴とユーザー名が本物に見える場合に、次の手順を実行します。

i. アクション 7 では、適切なチームと連携して問題を解決します。

ii. アクション 8 では、これまでの結果を文書化します。

iii. アクション 9 では、タスクをクローズする前にインシデントの事後レビューを完了します。

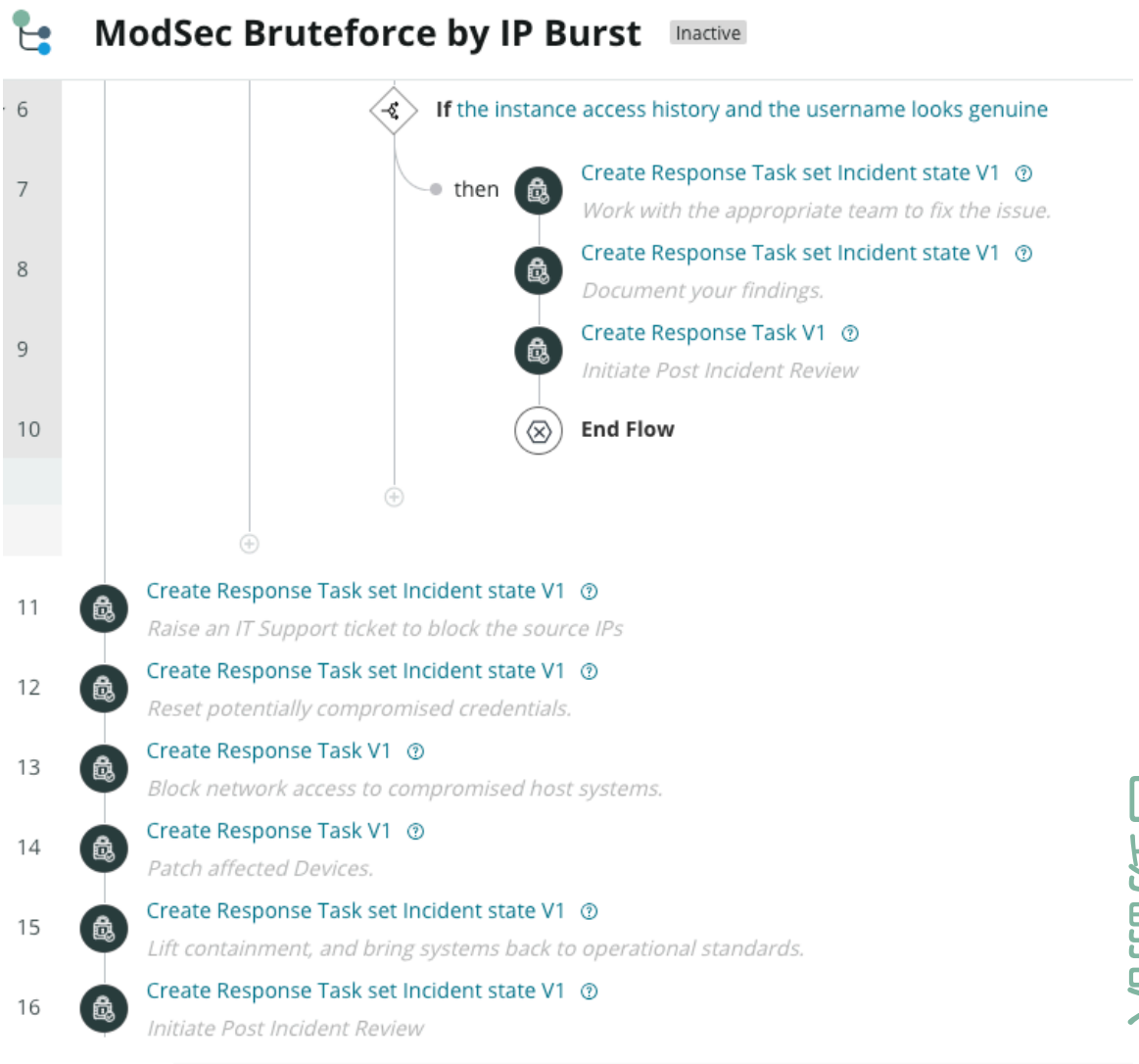
アクション 10 で、フローは終了します。

3. ソース IP が顧客または組織の内部 IP アドレスに属していない場合は、アクション 11 で、ソース IP をブロックする IT サポートチケットを発行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

IP バーストによる ModSec ブルートフォースプレイブックの使用



自動翻訳

4. アクション 12 では、侵害された可能性のある認証情報をリセットします。
5. アクション 13 では、侵害されたホストシステムへのネットワークアクセスをブロックします。
6. アクション 14 では、影響を受けるデバイスにパッチを適用します。
7. アクション 15 では、封じ込めを解除し、システムを運用標準に戻します。
8. アクション 16 では、タスクをクローズする前にインシデントの事後レビューを完了します。

セキュリティインシデントレスポンスプレイブックアクション

このセクションでは、フローデザイナーアクションライブラリで提供されるアクションについて説明します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクション名	説明	シナリオの例	
セキュリティインシデントにセキュリティタグを追加	このアクションを使用して、フローデザイナーロジックを使用してセキュリティタグを自動的に追加します。	フローが IOC を検出した場合、このアクションを使用して「**IOC** 検出済み」タグを自動的に追加できます。 **Flow**：	• 入力：セキュリティインシデント、セキュリティタグ • 出力：適用外
セキュリティインシデントに観測事象を追加 (Add observables to the security incident)	このアクションを使用して、選択したセキュリティインシデントに観測事象を追加します。 • デフォルトでは、観測事象のリストはカンマ (,) 区切り文字で区切られます。ただし、この文字は変更できます。別の単一の特殊文字を区切り文字として指定できます。観測事象を追加する際、タイプ (URL、IP アドレス、ハッシュ) が自動的に設定されます。 • 観測事象がセキュリティインシデントに追加されると、タイプ (URL、IP アドレス、ハッシュ) が自動的に設定されます。 • 観測事象が追加されると、[許可リスト観測事象をフィルター] オプションによって許可リスト観測事象が識別され、セキュリティインシデントの観測事象関連リストから除外されます。これらの観測事象が削除されたことを示すために、自動システムアクティビティ (応答) が追加されます。		• 入力： ○ セキュリティインシデント ○ 観測事象 ○ 区切り文字 ○ 許可リスト観測事象をフィルターし、アクティビティメモを投稿 • 出力：適用外

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクション名	説明	シナリオの例	
複数のセキュリティインシデント V1 から影響を受けるユーザー (関連リスト) を取得	指定されたセキュリティインシデントについて、[影響を受けるユーザー] 関連リストに記載されているすべての影響を受けるユーザーを取得します。	複数の子セキュリティインシデントを持つ親セキュリティインシデントがある場合があります。このアクションを使用して、影響を受けるユーザーを、すべての子セキュリティインシデントから対応する親セキュリティインシデントにロールアップします。影響を受ける一意のユーザーのみがロールアップされ、すべての重複が排除されます。	• 入力：セキュリティインシデント • 出力： ○ 影響を受けるユーザー ○ カウント
複数のセキュリティインシデントから影響を受けるユーザーを取得	指定されたセキュリティインシデントの影響を受けるプライマリユーザーを取得します。[影響を受けるユーザー] 関連リストの影響を受けるユーザーは含まれません。	• フィッシングセキュリティインシデントの調査中に、(フィッシングインシデントを報告した) 影響を受けるプライマリユーザーにメールを送信して、ユーザーがフィッシングメール内の悪意のあるリンクをクリックしたかどうかを確認します。 • 影響を受けるプライマリユーザーの数に基づいて、親セキュリティインシデントの重大度またはリスクスコアを更新します。	• 入力：セキュリティインシデント • 出力： ○ 影響を受けるユーザー ○ カウント
セキュリティインシデントから影響を受けるユーザー (関連リスト) を取得	指定されたセキュリティインシデントについて、[影響を受けるユーザー] 関連リストに記載されているすべての影響を受けるユーザーを取得します。		• 入力：セキュリティインシデント • 出力： ○ 影響を受けるユーザー ○ カウント

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクション名	説明	シナリオの例	

影響を受けるユーザーをセキュリティインシデントに追加	影響を受けるすべてのユーザーをセキュリティインシデントに追加します。	複数の子セキュリティインシデントを持つ親セキュリティインシデントがある場合、このアクションを使用して、影響を受けるユーザーを、すべての子セキュリティインシデントから対応する親セキュリティインシデントにロールアップできます。影響を受ける一意のユーザーのみがロールアップされ、すべての重複が排除されます。	• 入力：
			  ○ セキュリティインシデント
			  ○ ユーザー
			• 出力：適用外

影響を受けるユーザーの構成アイテムを取得	影響を受けるすべてのユーザーの構成アイテムを取得します。	フィッシングまたはマルウェアのシナリオでは、このアクションを使用して、[影響を受ける構成アイテム (CI)] 関連リストを更新し、CI を調査できます。特定された CI の数に基づいて、セキュリティインシデントの重大度またはリスクスコアを更新できます。	• 入力：ユーザー
			• 出力：
			  ○ 構成アイテム
			  ○ カウント

セキュリティインシデントのすべての子セキュリティインシデントを取得	特定の親セキュリティインシデントに関連するすべての子セキュリティインシデントを取得します。	シナリオ例：このアクションを使用して、次のことを行います。
		• 対応する親セキュリティインシデントのステータスが更新されたときに、子セキュリティインシデントのステータスを更新します。
		• 子セキュリティインシデントの数に基づいて、セキュリティインシデントの重大度またはリスクスコアを更新します。
			• 入力：
			  ○ セキュリティインシデント
			  ○ インシデント状況
			• 出力：
			  ○ 子セキュリティインシデント
			  ○ カウント

観測事象の構成アイテムを取得 (IP アドレスタイプ) (Get configuration items	IP アドレスタイプの観測事象のすべての構成アイテム (CI) を取得します。	IP アドレス観測事象は、構成アイテムに関連付けることができます。たとえば、サーバーの IP アドレスで	• 入力：観測事象 IP アドレス • 出力：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクション名	説明	シナリオの例	
for the observables (type IP address))		す。このアクションを使用すると、サーバーの情報を取得できます。	○ 構成アイテム ○ カウント
悪意がある観測事象 (Is observable malicious)	観測事象のセット内に 1 つ以上の悪意がある観測事象が存在するかを示します。	脅威のルックアップが完了し、悪意のある観測事象の存在を特定したら、セキュリティインシデントの重大度またはリスクスコアを上げることができます。	• 入力：セキュリティインシデント • 出力：悪意がある (true/false)
メールを送信してユーザーのインタラクションを確認 (Send email to confirm user interaction)	ユーザーの応答に応答してメールを送信します。	ユーザーがアプリケーションへのログインを複数回試行して失敗すると、ログイン失敗シナリオが発生します。この場合、ユーザーがログインを試行したかどうかを確認するメールがユーザーに送信されます。ユーザーの応答 (「はい」または「いいえ」) に応じて、さまざまなアクションを実行できます。 フロー：ログイン失敗手動プレイブック	
許可リスト観測事象をフィルター	このアクションを使用して、指定された観測事象のセットから許可リスト観測事象を除外します。	観測事象のセットから無視できる特定の観測事象を特定できます。これらの観測事象は、セキュリティインシデントの解決時に考慮されません。	• 入力：セキュリティインシデント • 出力： ○ 許可リスト観測事象 ○ カウント
影響を受けるユーザーのパスワードをリセット	このアクションを使用して、影響を受けるユーザーのパスワードをリセットします。	ユーザーアカウントがハッキングされた場合、またはユーザーがパスワードのリセットを要求した場合、パスワードをリセットするためのメールがユーザーに送信されます。 フロー：ログイン失敗手動プレイブック	
影響を受けるユーザーのユーザーグループを取得	影響を受けるユーザーのユーザーグループの詳細を取得します。	組織内で 2 人以上のユーザーがフィッシングメールを報告した場	• 入力：ユーザー • 出力：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクション名	説明	シナリオの例	
		合、そのユーザーが属するグループを特定し、影響を受けているユーザーがほかにいるかどうかを特定できます。	○ ユーザーグループ ○ カウント

セキュリティインシデントレスポンスレポート

セキュリティマネージャーは、高度なグラフィカルインターフェイスを使用して、問題のある領域を特定できます。

セキュリティインシデントレスポンスエクスプローラーへのアクセス

セキュリティインシデントレスポンス Explorer ダッシュボードにアクセスしてセキュリティインシデントアクティビティを表示することで、懸念のある領域を即座に特定し、問題を迅速に解決できます。

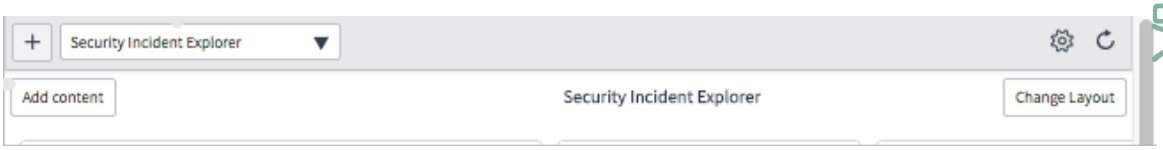
始める前に

必要なロール：

- sn_si.admin (書き込み用)
- sn_si_basic (読み取り用)

手順

1. 次のように移動する。 **All** (すべて) > セルフサービス > ホームページ または、 セルフサービス > ダッシュボード.
2. レポートリストから [Security Incident Explorer] を選択します。



セキュリティインシデントレスポンス の概要

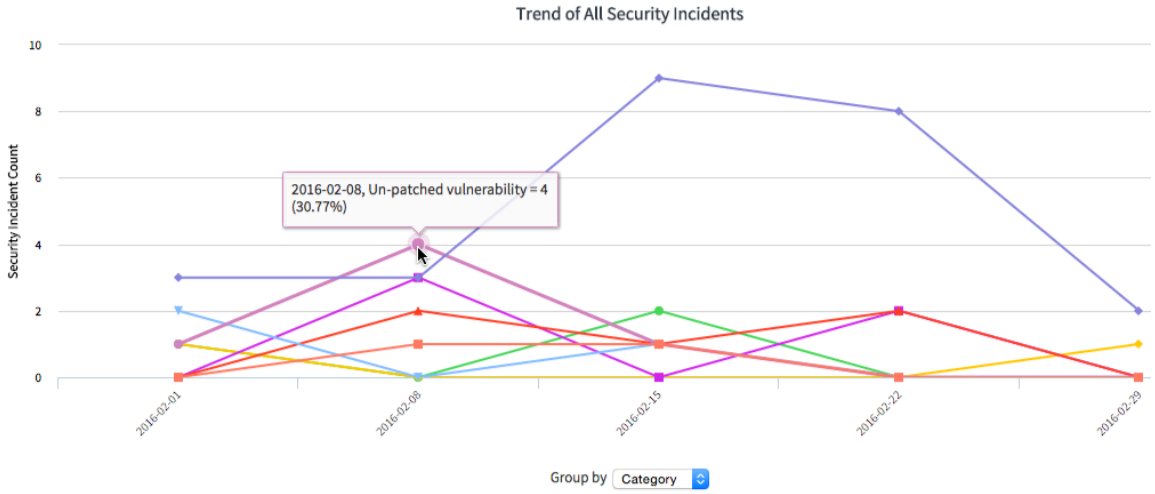
セキュリティインシデントレスポンス の概要では、セキュリティインシデントアクティビティのエグゼクティブビュー、傾向とレポート、および特定のデータへのドリルダウンが利用できます。

概要モジュールには、ユーザーのロールに合わせたセキュリティインシデント情報が表示されます。チャートの任意の部分 (棒、円、データポイント、ヒートマップなど) をポイントして、その部分に固有の一般的なデータを表示できます。次の画像を参照してください。レポートの任意の部分をクリックすると、詳細な情報を提供するリストが開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

すべてのセキュリティインシデントの傾向



セキュリティインシデントマネージャー概要

セキュリティインシデントアドミニストレーターおよびセキュリティインシデントマネージャーのロールを持つユーザーは、セキュリティインシデントマネージャーの概要を表示します。ベースシステムに次のレポートが含まれます。

セキュリティインシデントマネージャー概要レポート

名前	ビジュアル	説明
チームの重大なセキュリティインシデント	単一スコア	チームにアサインされた重大なセキュリティインシデントの数
チームの高セキュリティインシデント	単一スコア	チームにアサインされた高セキュリティインシデントの数
24 時間以内に期限切れになる SLA	単一スコア	次の 24 時間以内に期限切れになる SLA の数
リスクと重大度	ヒートマップ	チームにアサインされたセキュリティインシデントのリスクと重大度別の分布
CI クラス別のセキュリティインシデント、過去 3 か月	棒グラフ	チームにアサインされた構成アイテムクラス別のセキュリティインシデントの数
すべてのセキュリティインシデントの傾向	傾向図	受信したセキュリティインシデントの数をカテゴリまたは優先度別にプロットします。
不正アクセスのセキュリティインシデント	棒グラフ	受信したセキュリティインシデントカテゴリのタイプを時系列で表示します。
平均封じ込め時間	単一スコア	すべてのセキュリティインシデントを封じ込めるのに要する平均時間
平均封じ込め時間 (重大)	単一スコア	すべての重大なセキュリティインシデントを封じ込めるのに要する平均時間
識別までの平均時間	単一スコア	すべてのセキュリティインシデントを識別するのに要する平均時間

セキュリティアナリスト概要

セキュリティインシデントアナリストロールを持つユーザーは、セキュリティアナリスト概要を表示します。ベースシステムに次のレポートが含まれます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティアナリスト概要レポート

名前	ビジュアル	説明
自分の重大な優先度の作業	単一スコア	自分にアサインされた重大なセキュリティインシデントの数
自分の優先度の高い作業	単一スコア	自分にアサインされた高セキュリティインシデントの数
24 時間以内に期限切れになる自分の SLA	単一スコア	自分にアサインされた次の 24 時間以内に期限切れになる SLA の数
自分にアサインされたセキュリティインシデント	棒グラフ	インシデントのステータスおよびカテゴリ別の自分にアサインされたセキュリティインシデント
自分にアサインされたタイプ別の作業	棒グラフ	タイプまたは優先度別の自分にアサインされたセキュリティタスク (インシデント、タスク、または要求)
自分にアサインされたセキュリティインシデント、要求、タスク	リスト	自分にアサインされたすべてのセキュリティインシデント、セキュリティ要求およびタスクのリスト
セキュリティインシデントの場所	マップ	セキュリティインシデントの地域の場所。
カウント	マップ	地域ごとのセキュリティインシデントの数
最小/最大数	カラースペクトラムバー	カラースペクトラムバーで表される、地域ごとのセキュリティインシデントの最小数と最大数。
カウントの割合	マップ	地域ごとの合計インシデント数の割合

セキュリティインシデントアナリティクスをアクティブ化したセキュリティインシデント **CISO** の概要

セキュリティインシデントアナリティクス プラグインがアクティブになっている場合、セキュリティインシデント CISO およびシステムアドミニストレーターロールを持つユーザーは、セキュリティインシデント CISO の概要を表示できます。ベースシステムには次の CISO レポートがあります。

(セキュリティインシデントアナリティクスをアクティブ化した) セキュリティインシデント **CISO** 概要レポート

名前	ビジュアル	説明
今週の新規セキュリティインシデント	単一スコア	今週受信した新規セキュリティインシデントの数
今週クローズされたセキュリティインシデント	単一スコア	今週クローズされたセキュリティインシデントの数
新規セキュリティインシデント (連続 7 日間合計)	単一スコア	過去 7 日間にオープンされたセキュリティインシデントの数
クローズされたセキュリティインシデント (連続 7 日間合計)	単一スコア	過去 7 日間にクローズされたセキュリティインシデントの数
新規セキュリティインシデントとクローズされたセキュリティインシデント (日別)	傾向図	新規およびクローズされたセキュリティインシデントの数 (日別)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(セキュリティインシデントアナリティクスをアクティブ化した) セキュリティインシデント **CISO** 概要レポート (続く)

名前	ビジュアル	説明
新規セキュリティインシデントとクローズされたセキュリティインシデント (週次)	傾向図	新規およびクローズされたセキュリティインシデント (週次)
セキュリティインシデントクローズコード	傾向図	経時的なクローズコードの全数
セキュリティインシデントのビジネスインパクト	ツリーマップ	ビジネス上の重要度別にグループ化されたセキュリティインシデントを含むビジネスサービス
平均封じ込め時間 (週次)	傾向図	セキュリティインシデントを封じ込めるのに要する 7 日間の平均時間 (時系列)
平均除去時間 (週次)	傾向図	セキュリティインシデントを除去するのに要する 7 日間の平均時間 (時系列)
平均識別時間 (週次)	傾向図	セキュリティインシデントを識別するのに要する 7 日間の平均時間 (時系列)
セキュリティインシデントの場所	マップ	セキュリティインシデントの地域の場所。
カウント	マップ	地域ごとのセキュリティインシデントの数
最小/最大数	カラースペクトラムバー	カラースペクトラムバーで表される、地域ごとのセキュリティインシデントの最小数と最大数。
カウントの割合	マップ	地域ごとの合計インシデント数の割合

セキュリティインシデントアナリティクスをアクティブ化しないセキュリティインシデント **CISO** の概要

セキュリティインシデントアナリティクス プラグインがアクティブになっていない場合、セキュリティインシデント CISO およびシステムアドミニストレーターロールを持つユーザーは、セキュリティインシデント CISO レポートの概要を表示できます。ベースシステムには次の CISO レポートがあります。

(セキュリティインシデントアナリティクスをアクティブ化しない) セキュリティインシデント **CISO** 概要レポート

名前	ビジュアル	説明
今週の新規セキュリティインシデント	単一スコア	今週オープンされた新規セキュリティインシデントの数
今週クローズされたセキュリティインシデント	単一スコア	今週クローズされたセキュリティインシデントの数
新規セキュリティインシデント (連続 7 日間合計)	単一スコア	過去 7 日間にオープンされたセキュリティインシデントの数

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(セキュリティインシデントアナリティクスをアクティブ化しない) セキュリティインシデント **CISO** 概要レポート (続く)

名前	ビジュアル	説明
クローズされたセキュリティインシデント (連続 7 日間合計)	単一スコア	過去 7 日間にクローズされたセキュリティインシデントの数
新規セキュリティインシデント (週次)	傾向図	オープンされた新規セキュリティインシデント (週次)
クローズされたセキュリティインシデント (週次)	傾向図	クローズされたセキュリティインシデント (週次)
セキュリティインシデントクローズコード	傾向図	セキュリティインシデントクローズコード (時系列)
セキュリティインシデントのあるビジネスサービス - ビジネスインパクト	ツリーマップ	ビジネス上の重要度別にグループ化されたセキュリティインシデントを含むビジネスサービス
平均封じ込め時間	単一スコア	すべてのセキュリティインシデントを封じ込めるのに要する平均時間
平均封じ込め時間 (重大)	単一スコア	すべての重大なセキュリティインシデントを封じ込めるのに要する平均時間
識別までの平均時間	単一スコア	すべてのセキュリティインシデントを識別するのに要する平均時間

自動翻訳

注:
セキュリティインシデントレスポンス ベースシステムには、事前設定されたベストプラクティスダッシュボードを表示するためのパフォーマンスアナリティクスソリューションが含まれます。ダッシュボードには、新しいセキュリティインシデントやオープンセキュリティインシデントの平均経過時間など、セキュリティインシデントレスポンスプロセスを分析する上で重要なメトリクスが表示されます。詳細と手順については、以下を参照してください。 セキュリティインシデントレスポンス プラットフォームアナリティクスソリューション。

セキュリティインシデントマップ

セキュリティインシデントマップは、地理的な場所別のデータを提供します。世界地図でインシデントが発生するすべてのエリアがハイライト表示されます。セキュリティインシデントアナリティクスプラグインがアクティブになると、セキュリティインシデントマップを セキュリティインシデントレスポンス の概要に追加できます。追加されたマップは、マップフィルターを変更して設定できます。

セキュリティインシデントレスポンス 概要へのマップの追加

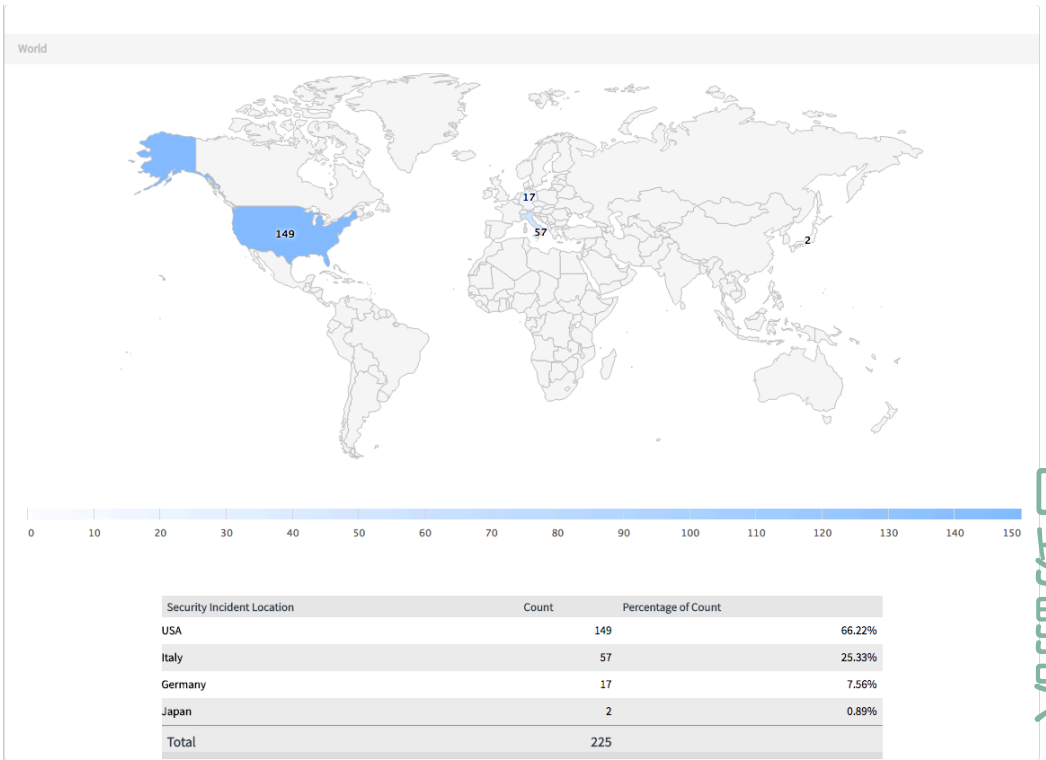
セキュリティインシデントレスポンス 概要にマップを追加して、地理的な場所別にセキュリティインシデントデータを表示できます。マップを使用すると、場所ごとにセキュリティインシデント情報にドリルダウンできます。

始める前に
必要なロール：sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > 概要.
2. ページの左上隅にある [コンテンツを追加] をクリックして、ウィジェット選択コントロールを開きます。
3. 最初の選択ボックスで、[レポート] をクリックします。
4. 2 番目の選択ボックスで、[セキュリティインシデント] をクリックします。
5. 3 番目の選択ボックスで、[セキュリティインシデントマップ] をクリックします。



Security Incident Location	Count	Percentage of Count
USA	149	66.22%
Italy	57	25.33%
Germany	17	7.56%
Japan	2	0.89%
Total	225	

6. 画面の下部で、レポートに追加する画面上の場所をクリックします。
7. [コンテンツを追加] ボックスを閉じます。

セキュリティインシデントマップの変更

グローバルドメインのアドミニストレーターは、フィルターを使用してセキュリティインシデントマップがセキュリティインシデントをどのように処理するかを変更できます。

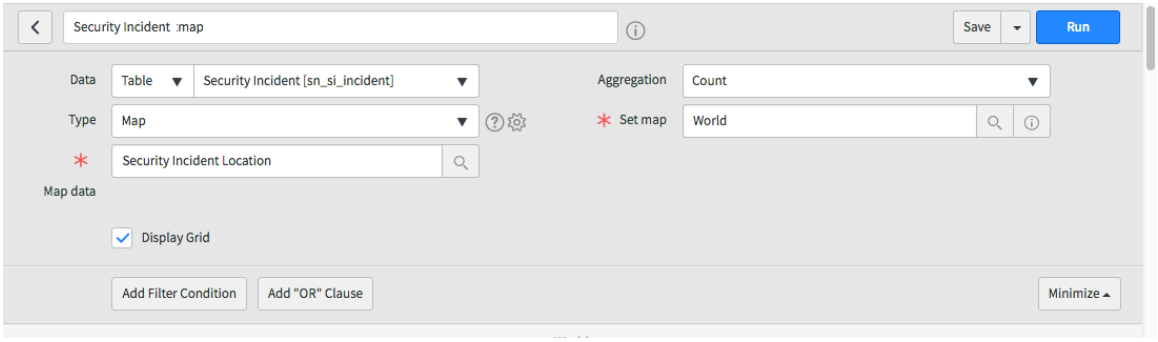
始める前に

必要なロール：sn_si.admin

手順

1. 次のように移動する。 レポート > アドミニストレーション > **All** (すべて).
2. 「セキュリティインシデントマップ」を検索します。
3. [レポートを編集] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [フィルター条件の追加] をクリックしてフィルターを追加または編集します。
5. [実行] をクリックして、適用された変更を確認します。
6. [保存] をクリックします。

セキュリティインシデントツリーマップ

セキュリティインシデントアナリティクス プラグインがアクティブになると、セキュリティインシデント - サービスへの影響度とセキュリティインシデント - リアルタイムツリーマップを セキュリティインシデントレスポンス 概要に追加できます。追加した後、ツリーマップカテゴリとインジケーターを変更してツリーマップを構成できます。

セキュリティインシデントレスポンス概要へのツリーマップの追加

ツリーマップは、(ツリー構造の) 階層データをネストされた矩形の集合として表示します。ツリーの各ブランチは矩形で、サブブランチを表す小さな矩形がタイル状になっています。ツリーマップを使用すると、セキュリティインシデント情報を動的で人目を引く方法で表示できます。

始める前に
必要なロール：sn_si.admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > 概要.
2. ページの左上隅にある [コンテンツを追加] をクリックして、ウィジェット選択コントロールを開きます。
3. 最初の選択ボックスで、[ツリーマップ] をクリックします。
4. 2 番目の選択ボックスで、挿入するツリーマップを次のリストから選択します。
   - セキュリティインシデント - サービスへの影響
   - セキュリティインシデント - リアルタイム
   - セキュリティインシデント - ビジネスインパクト
   - 脆弱性重要度 (Vulnerability Significance)

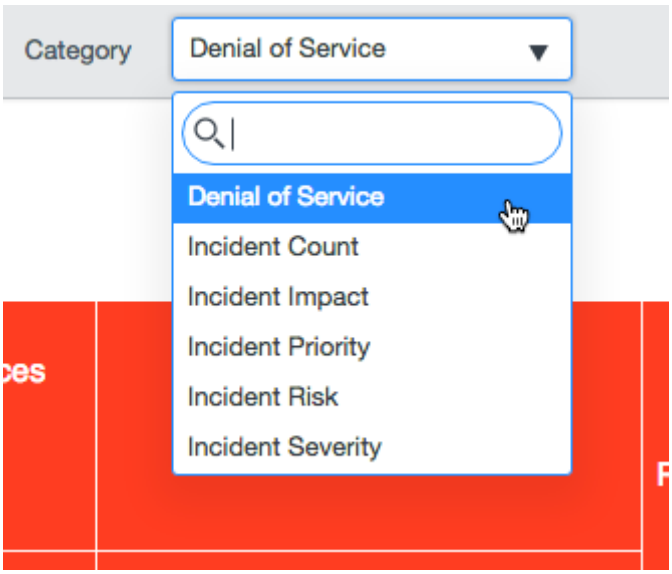
   注:
   [ビジネスインパクト] ツリーマップは、セキュリティインシデントレスポンス ホームページにデフォルトで表示されます。[サービスへの影響度] および [リアルタイム] ツリーマップを使用するには、セキュリティインシデントアナリティクスプラグインがアクティブになっている必要があります。

5. 3 番目の選択ボックスで、選択したツリーマップについて、取得したい情報の粒度レベルを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[セキュリティインシデント - サービスへの影響] ツリーマップの場合、3 番目の選択ボックスで [セキュリティインシデント] を選択します。この選択により、複数のデータカテゴリを含むドロップダウンリストが表示されます。



6. 画面の下部で、ゲージに追加する画面上の場所をクリックします。
7. [コンテンツを追加] ボックスを閉じます。

ツリーマップカテゴリの作成または更新

必要に応じて、セキュリティインシデントツリーマップに事前定義されたカテゴリを変更するか、カテゴリを作成できます。

始める前に
必要なロール：sn_si.admin

ツリーマップは、データソースとしてパフォーマンスアナリティクスを使用します。パフォーマンスアナリティクスモジュールには独立したプラグインが必要です。

このタスクについて
ベースシステムには、インシデントリスク、サービス拒否、インシデントの重大度などのツリーマップカテゴリが含まれています。必要に応じて、これらのカテゴリを変更するか、さらにカテゴリを定義することができます。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > アドミニストレーションをクリックし、カテゴリを構成するツリーマップ定義を開きます。
   - サービス重要度レポートの定義
   - リアルタイム定義
2. オプション: ツリーマップ定義名を変更します。
   ベースシステムでは、サービスへの影響ツリーマップ定義のデフォルト名は「セキュリティインシデント」です。リアルタイムツリーマップ定義のデフォルト名は、「セキュリティインシデント - リアルタイム」です。
3. カスタムビルトのツリーマップを使用する場合を除き、**[PA** インジケーターグループ] の値を変更しないでください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. ツリーマップ定義を非アクティブ化するには、[有効] チェックボックスをオフにします。
たとえば、システム影響度ダッシュボードから [サービス拒否] カテゴリを非アクティブ化した場合、そのツリーマップカテゴリは使用できなくなります。
5. [ツリーマップカテゴリ] 関連リストで、変更するカテゴリを選択するか、[新規] をクリックして新しいカテゴリを作成します。
6. フィールドに入力します。

[ツリーマップカテゴリ] フォーム

フィールド	説明
名前	ツリーマップの上にある [カテゴリ] リストのカテゴリに表示される名前
順序	ツリーマップの上にある [カテゴリ] リストにカテゴリが表示される順序
ツリーマップ	このカテゴリを使用するツリーマップの名前
色	ツリーマップでこのカテゴリに表示される色
有効	このカテゴリをアクティブにする場合に選択します。
説明	カテゴリの説明
全てのロールに公開	ロールに関係なく、このカテゴリをすべてのユーザーに表示する場合に選択します。
ロール	[全てのロールに公開] チェックボックスをオンにしなかった場合に、このカテゴリを表示できるロールを選択します。

7. [送信] または [更新] をクリックします。

ツリーマップインジケーターの作成または更新

ツリーマップカテゴリに事前定義されたインジケーターを変更するか、新しいインジケーターを作成することができます。インジケーターごとにデータソースを設定し、インジケーターで表示されるツリーマップからセキュリティインシデントのリストを開く方法を指定できます。

始める前に
必要なロール：sn_si.admin

ツリーマップは、データソースとしてパフォーマンスアナリティクスを使用します。パフォーマンスアナリティクスモジュールには独立したプラグインが必要です。

手順

1. インジケーターを設定するツリーマップ定義を開きます。
2. [ツリーマップカテゴリ] 関連リストで、インジケーターを設定するカテゴリを選択します。
3. [ツリーマップインジケーター] 関連リストで、変更するインジケーターを選択するか、[新規] をクリックして新しいインジケーターを作成します。
4. フィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[ツリーマップインジケーター] フォーム

フィールド	説明
名前	サービスへの影響ダッシュボードの [インジケーター] リストに表示される名前
簡単な説明	ツリーマップの上にある [インジケーター] リストのインジケーターに表示される説明
結果制限	許容される結果の最大数。上限は 100 です。
結果の精度	小数点以下の表示桁数。 このフィールドは、リアルタイムツリーマップ定義の場合のみ表示されます。
有効	このインジケーターをアクティブ化するチェックボックス
カテゴリ	前の画面で入力されたカテゴリ名
方向	ツリーマップ上のタイルを最小化するか最大化するかを指定します。 このフィールドは、リアルタイムツリーマップ定義の場合のみ表示されます。
単位	このメトリクスに使用する測定単位。 このフィールドは、リアルタイム定義の場合のみ表示されます。
自動リフレッシュ間隔	ツリーマップを更新する頻度
順序	ツリーマップの上の [インジケーター] リストにインジケーターが表示される順序

5. [データソース構成] タブをクリックし、次のデータソースオプションのいずれかをインジケーターに設定します。

6. [クリックスルー] タブをクリックし、セキュリティインシデントのリストをツリーマップから開く方法を指定します。
   a. [クリックスルー **URL** ナビゲーションタイプ] フィールドで、セキュリティインシデントのリストを新しいウィンドウで開くか、同じウィンドウで開くか、ダイアログボックスで開くかを選択します。
   b. オプション: [クリックスルー **URL** スクリプト] フィールドで、必要に応じてサンプルスクリプトを変更します。
7. [送信] または [更新] をクリックします。

概要への脆弱性重要度チャートの追加

脆弱性対応 プラグインがアクティブになっている場合は、脆弱性重要度定義チャートやその他の可視化を概要に追加できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_si.admin

手順

1. 脆弱性重大度ゲージを追加する [概要] ページに移動します。
2. ページの左上隅にある [コンテンツを追加] をクリックして、ウィジェット選択コントロールを開きます。
3. 3 つの選択ボックスで、追加するゲージ (ツリーマップまたはスコアレポート) に応じて選択します。
   - [脆弱性重要度 (Vulnerability Significance)] ツリーマップを追加するには、次の選択を行います。
     - ツリーマップ
     - 脆弱性重要度 (Vulnerability Significance)
     - 脆弱性重要度 (Vulnerability Significance)
   - [脆弱性重要度 (Vulnerability Significance)] スコアレポートを追加するには、次の選択を行います。
     - パフォーマンスアナリティクス
     - スコア
     - Services with Vulnerability Significance (脆弱性重要度ありのサービス)
4. ゲージに追加する画面上の場所をクリックします。
5. [コンテンツを追加] ボックスを閉じます。

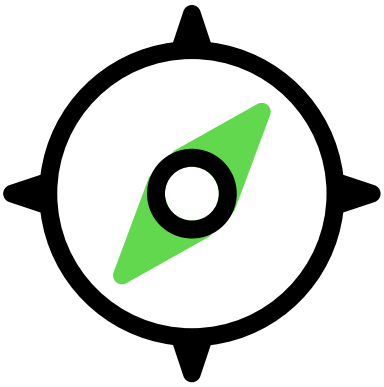
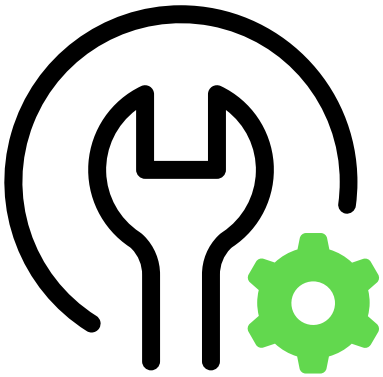
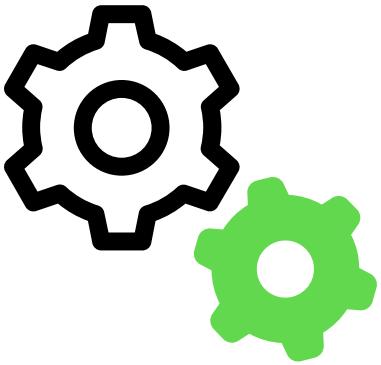
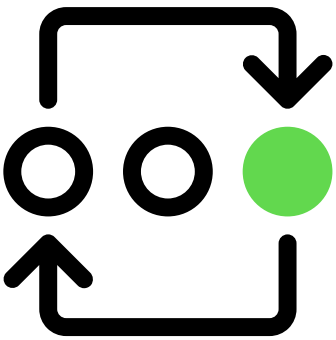
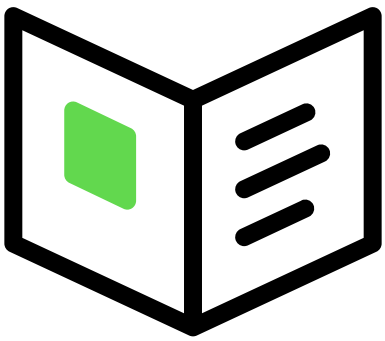
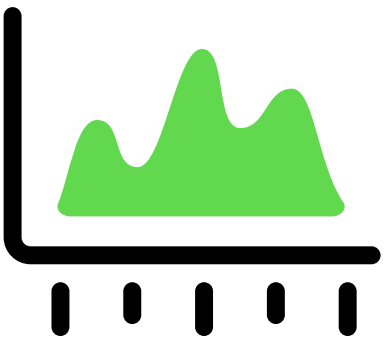
重大セキュリティインシデント管理

ServiceNow® 重大セキュリティインシデント管理 アプリケーションは、検出から分析、セキュリティインシデントの提案、昇格、リンク、およびクローズまでの、重大セキュリティインシデント (MSI) の進行状況を追跡します。

重大セキュリティインシデント管理

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

探索	構成	統合
		
アナリスト、アドミン、およびマネージャーが重大セキュリティインシデント管理 (MSIM) を使用する方法について説明します	実装の計画と構成	他の Microsoft アプリケーションとの統合による MSIM 機能の拡張
管理	**使用**	**ステータスレポート**
		
インシデントレコードにタグを付け、ラベルを設定する方法に関する管理タスク	ワークスペース管理による重大なセキュリティインシデントレコードの提案、昇格、リンク、および却下	インシデント関連タスクを監視し、メトリクス、傾向図、およびレポートを通じてプロセスを改善します

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

その他の機能 レコードをロールアップするための情報の構成		

ストアでアプリを要求

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアに要求を送信する方法について確認してください。リリースされたすべてのアプリのリリースメモ情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

ストアで セキュリティオペレーション アプリを要求する

Rome 以降の新規セキュリティオペレーションのお客様の場合は、 ServiceNow Store Web サイトで利用可能なアプリと、ストアに要求を送信する方法に関する情報を表示します。

トラブルシューティングとサポート

- 重大セキュリティインシデント管理 フォーラム ServiceNow コミュニティ.
- セキュリティオペレーションリソースライブラリ
- セキュリティオペレーションコミュニティ
- 既知のエラーポータルで既知のエラー記事を検索する
- 連絡先 カスタマーサービス & サポート

重大セキュリティインシデント管理の詳細

重大セキュリティインシデント管理 に関する詳細な説明を読んで、組織への脅威として識別された優先度の高い重大なセキュリティインシデントをこのアプリケーションがどのように追跡するかを理解します。

このセクションでは、重大なセキュリティインシデントのレコードの操作に関与する主な機能や各種ロールについて学習します。このセクションは、アプリケーションの開始方法、前提条件、およびアプリケーションの操作に必要なプラグインを理解するのにも役立ちます。

重大セキュリティインシデント管理

重大セキュリティインシデント管理を使用して、重大なセキュリティインシデントの解決の一環でよく行われるさまざまなアクティビティを追跡および管理します。インシデントマネージャーおよびインシデント担当者は、直感的なワークスペースを使用して、インシデントを提案して重大なインシデントに昇格させ、重大なセキュリティインシデントのアクティビティを追跡し、同僚と簡単に共同作業を行うことができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

概要

重大セキュリティインシデント管理の機能は、既存のセキュリティインシデントレスポンス製品の機能と連携して機能します。連携先の機能としては、セキュリティアナリストが標準的なセキュリティインシデントを重大なセキュリティインシデントにエスカレートすることで、新しい製品機能を使用して修復プロセスをサポートできるようにする機能などがあります。

ServiceNow インスタンスに重大セキュリティインシデント管理をインストールすると、セキュリティインシデントアナリストは次のことができます。

- 重大なセキュリティインシデント候補としてセキュリティインシデントを提案し、重大なセキュリティインシデントの作成が必要であればレビューのプロセスを開始する。
- 追加のレビュープロセスを必要とすることなく、セキュリティインシデントを重大なセキュリティインシデントに直接昇格させる。
- 重大なセキュリティインシデント (MSI) として提案されたセキュリティインシデントを拒否する。
- セキュリティインシデントを子インシデントとして重大なセキュリティインシデント (MSI) にリンクして、すべてのセキュリティインシデントを処理できるようにする。

主な機能

重大セキュリティインシデント管理 (MSIM) は、次の機能で、重大なセキュリティインシデントの修復プロセスを改善します。

- 重大なセキュリティインシデントマネージャーのユーザーロール向けに設計された、重大なセキュリティインシデントを管理する専用のワークスペース。
- 複数の「子」セキュリティインシデントの応答タスクを整理する。
- 重大なセキュリティインシデントが作成された後、コラボレーションフォルダーとチャットコミュニケーションチャネルの作成を自動化し、インシデントクローズ時にアーカイブを作成する。
- Microsoft SharePoint の統合を介して、重大なセキュリティインシデントに関連するアーティファクト (ファイル) のコレクションを整理して追跡するためのファイルエクスプローラーコンポーネント。
- Microsoft Teams の統合を介して、複数のセキュリティ、IT、機能グループ間のコミュニケーションを管理するためのチャットチャネルマネージャーとアクティビティストリームコンポーネント。

ワークスペースのコンポーネント

重大セキュリティインシデント管理製品には、主な機能を提供する新しいワークスペースコンポーネントとユーザーインターフェイスページがいくつか含まれています。

- 重大セキュリティインシデントマネージャーのユーザーロールに特化して設計された、重大なセキュリティインシデントを管理する専用のワークスペース。
- 複数の子セキュリティインシデントの応答タスクを整理する。
- 重大なセキュリティインシデントが作成された後、コラボレーションフォルダーとチャットコミュニケーションチャネルの作成を自動化し、インシデントクローズ時にアーカイブを作成する。
- Microsoft SharePoint の統合を介して、重大なセキュリティインシデントに関連するアーティファクト (ファイル) のコレクションを整理して追跡するためのファイルエクスプローラーコンポーネント。
- Microsoft Teams の統合を介して、複数のセキュリティ、IT、機能グループ間のコミュニケーションを管理するためのチャットチャネルマネージャーとアクティビティストリームコンポーネント。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サポートされている重大セキュリティインシデント管理のバージョン

重大セキュリティインシデント管理 (MSIM) には Now Platform® Rome バージョンが必要です。

この機能は、Microsoft Office 365 スイートに入っている、チャットを中心としたワークスペースである Microsoft Teams をサポートしています。以前は、Microsoft Teams は Microsoft Office 365 アプリケーションと別にインストールする必要がありました。

サポートされている **Now Platform** のバージョン

この機能は Rome 以降のリリースでサポートされています。

次の セキュリティオペレーション アプリケーションが標準のセキュリティインシデントレスポンスプラグインです。既に セキュリティインシデントレスポンス (SIR) を使用していれば、これらのプラグインはほとんどのユーザーのマシンにインストールされていると考えられます。インストールされていない場合は、ServiceNow Store からプラグインをインストールしてアクティブ化する必要があります。スムーズにインストールするには、一度に 1 つのアプリケーションを、以下の順序でインストールしてアクティブ化します。

1. セキュリティインシデントレスポンス：com.snc.si_dep が依存プラグインです。このプラグインをインストールすることで、他の SecOps アプリケーションが有効になります。
2. Security Integration Framework
3. Security Support Common
4. Security Support Common Orchestration

MSIM を開始するには

重大セキュリティインシデント管理 の作業を開始する前に、次の情報を確認します。

必要なロール：sn_msi.workspace_admin

重大セキュリティインシデント管理 アプリケーションのインストールと構成を容易に行うには、次のプラグインがアクティブになっているかどうかを確認する必要があります。

重要:
構成の簡単なセットアップでユーザーを支援する更新セット (KB1289784) は、「重大セキュリティインシデント管理クイックスタートガイド」にあります。アプリケーションのインストールの後にこの更新セットをインポートする必要があります。ServiceNow Store にある MSIM アプリケーション内の [補足ドキュメント (Supporting documents)] セクションにある「クイックスタートガイド」 (ステップ 2) に記載されている手順に従います。

必須条件

タスク	説明
アプリケーションの使用を開始する前に、必要な依存プラグインがあることを確認します。	最初のステップとして、以下のプラグインをインストールします。 • ServiceNow IntegrationHub Installer (com.glide.hub.integrations) • ServiceNow® 統合ハブ Runtime (com.glide.hub.integration.runtime) • ServiceNow® 統合ハブ Action Step - REST (com.glide.hub.action_step.rest)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

必須条件 (続く)

タスク	説明
	• ServiceNow 統合ハブアクション テンプレート - データストリーム (com.glide.hub.action_type.datastream) • ServiceNow 統合ハブ フロー デザイナー - Dynamic Inputs (com.glide.hub.dynamic_inputs) **注:** リストされている ServiceNow 統合ハブ プラグインのいずれかに必要な権限がない場合は、これらの必須アプリケーションをインストールするためのサポートチケットを作成してください。
Microsoft SharePoint スポークと Microsoft Teams Graph スポークのインストールに必要なアクセス権があることを確認します。 **注:** 上記に挙げたのは、重大セキュリティインシデント管理 の使用を開始するための主な依存アプリケーションです。	Microsoft SharePoint スポークと Microsoft Teams Graph スポークをインストールする前に、ServiceNow 統合ハブ アプリケーションへの必要なアクセス権があることを確認してください。 **注:** Microsoft SharePoint スポークと Microsoft Teams Graph スポークは ServiceNow 統合ハブ アプリケーションに依存するアプリケーションです。

MSIM セットアップのチェックリスト

ServiceNow 重大セキュリティインシデント管理 (MSIM) アプリケーションを使用する前に、ServiceNow Store からアプリケーションをダウンロードします。

次のテーブルに記載されたセットアップ、インストール、および構成の進捗状況を追跡します。

注: 重大セキュリティインシデント管理 アプリケーションにアサインされるロールは、この後のセクションにリストされています。詳細については、「重大セキュリティインシデント管理 ロール」を参照してください。

次のチェックリストを使用して、重大セキュリティインシデント管理 アプリケーションをインストールして構成するためのエンドツーエンドの手順を示します。

チェックリスト

セットアップタスク	説明
重大セキュリティインシデント管理 アプリケーションが ServiceNow Store からインストールされ、アクティブ化されていることを確認します。	重大セキュリティインシデント管理 v1.1.1 は ServiceNow Store で入手可能です。 次の手順に従います。 からのアプリケーションのダウンロード ServiceNow Store.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

チェックリスト (続く)

セットアップタスク	説明
次のアプリケーションが記載された順序でインストールされていることを確認します。	現在のアプリケーションリリースバージョンでは 重大セキュリティインシデント管理 アプリケーションをインストールした後、デフォルトで次のアプリケーションがインストールされます。 • File Explorer Core for Security Operations v1.1.1 • Microsoft SharePoint File Explorer Connector for セキュリティオペレーション v1.1.1 • File Explorer Component for セキュリティオペレーション v1.0.0 • Microsoft Teams Chat Connector for Security Operations v1.0.0 • Chat core for セキュリティオペレーション v1.0.0 • 重大セキュリティインシデント Response v1.1.1 • Collab Chat EVAM card for MSIM workspace v1.0.0 (このアプリケーションは、重大セキュリティインシデント管理 ワークスペースのアプリケーションバックグラウンドでの UI 可視化用にのみ設定されます) • Task Organizer UI Component for 重大セキュリティインシデント管理 workspace 1.0.0 • セキュリティインシデントレスポンス v12.8.1
ユーザーロールが必要に応じて「重大セキュリティインシデント」にアサインされていることを確認します。	重大セキュリティインシデント修復プロセスのインシデントライフサイクル全体に関連するロールは次のとおりです。 • MSI アドミニストレーター [sn_msi.workspace_admin] • MSI マネージャー [sn_msi.workspace_manager] • MSI レスポンダー [sn_msi.workspace_responder 各ロールの詳細については、「重大セキュリティインシデント管理 ロール」を参照してください。
Microsoft SharePoint v1.0.0 構成が正常にセットアップされていることを確認します。	Microsoft SharePoint は、Microsoft SharePoint 内のサイト、フォルダー、ファイル、グループ、およびユーザーを管理します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト (続く)

セットアップタスク	説明
	Microsoft SharePoint データを ServiceNow インスタンスに追加します。これを行うには、Graph および REST 接続をセットアップする必要があります。 REST および Graph 接続構成の設定方法については、Microsoft SharePoint Spoke v1.1.2 のドキュメントを参照してください。 Microsoft SharePoint から ServiceNow インスタンスに接続するための Graph および REST 接続を確立します。
ドキュメントライブラリを作成するための Microsoft SharePoint サイトが作成されていることを確認します。	必要に応じて Microsoft SharePoint サイトを作成します。または、既存のサイトを使用してドキュメントライブラリを作成することもできます。
Microsoft SharePoint サイトの下にドキュメントライブラリが作成されていることを確認します。	新規または既存の Microsoft SharePoint サイトの下に専用のドキュメントライブラリを作成します。
Microsoft SharePoint で必要な権限がユーザーに提供され、必要なユーザーグループにアサインされていることを確認します。	Microsoft SharePoint サイトからさまざまなユーザーおよびユーザーグループへのアクセスを管理します。
Microsoft SharePoint ドライブおよび必要な構成設定が作成され構成されていることを確認します。	ドライブ構成を確認するには、Microsoft SharePoint File Explorer Connector、フォルダーとファイルのアクション、およびフォルダーテンプレートをセットアップします。 • ファイルエクスプローラーのリポジトリドライブの構成：Microsoft SharePoint から ServiceNow インスタンスへの接続を作成します。 • フォルダーとファイルのアクション設定の構成：ファイルエクスプローラーコンポーネントに表示される個々のフォルダーとファイルのアクションを構成および制御します。 • フォルダーテンプレートの作成：さまざまな重大なセキュリティインシデントタイプに対して一意のフォルダーを作成するように構成します。
Microsoft Teams Chat Connector アプリケーションへの接続が正常に確立されていることを確認します。	ServiceNow インスタンスとの Microsoft Teams Chat Connector アプリケーション接続を確立するには、「Now Platform での MS Teams Graph 接続の確立」で説明されている手順に従います。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト (続く)

セットアップタスク	説明
Now Platform® インスタンスを使用して Microsoft Teams が構成され、接続と資格情報の構成が作成されていることを確認します。	ServiceNow® インスタンスを使用した Microsoft Teams 構成を確認するには、次の項目で説明する手順に従います。 • Now Platform での MS Teams Graph 接続の確立 • チャットチャネルテンプレートの作成
[重大なセキュリティインシデントの管理 - 構成 (Major Security Incident Administration - Configuration)] 設定が正常であることを確認します。	MSI アドミニストレーターは、次のことを実行できる必要があります。 • セキュリティアナリストがインシデントを提案および昇格し、他のセキュリティインシデントをリンクできるかどうかを判断する。 • インシデントが提案または昇格されたときの通知を有効または無効にする。デフォルトのテンプレートメッセージを編集できる。 • 重大なセキュリティインシデント候補として提案された、または重大なセキュリティインシデントに昇格されたインシデントを区別するために、セキュリティアナリストインターフェイスに表示されるセキュリティタグを設定する。
[重大なセキュリティインシデントの管理 - 通知 (Major Security Incident Administration - Notifications)] 設定が正常であることを確認します。	MSI アドミニストレーターは、セキュリティインシデントが提案された時点でメール通知をトリガーし、通知リストに設定されているすべてのユーザーとグループに通知が送信されます。詳細については、「MSIM の通知設定」を参照してください。

重大セキュリティインシデント管理 ロール

ロールをアサインして、必要なすべてのアクションをユーザーが MSIM アプリケーション内で実行できるようにします。

重大インシデント管理 のロール

ロールタイプ	ロール	説明
MSI アドミニストレーター	sn_msi.workspace_admin	重大インシデント管理 をインストールして構成し、File Explorer (FE)、Microsoft Teams とチャットチャネルの構成、ワークスペースのセットアップ、および MSI 管理 (構成と通知のセットアップ) などの依存アプリケーションを設定できるかどうか。 設定方法：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重大インシデント管理 のロール (続く)

ロールタイプ	ロール	説明
		• ファイルエクスプローラー (FE) コンポーネント： ○ ファイルリポジトリを設定する。 ○ 重大セキュリティインシデント管理ワークスペースの [コラボレーション] タブのファイルエクスプローラーコンポーネントで実行可能なファイルとフォルダーのアクションを構成します。 ○ ルートフォルダーとサブフォルダーを作成し、サブフォルダーへのアクセス権を設定します。 • チャットチャネルの管理 ○ Microsoft Teams の接続を検証して、Microsoft Teams をアクティブ化して設定します。 ○ チャットチームとチャットチャネルを作成し、ユーザーを追加して、さまざまなユーザーグループにユーザーをアサインします。 • MSI 管理： ○ 構成：セキュリティアナリストのアクション、インシデントの提案および昇格時に送信される通知、およびセキュリティインシデントに対する表示タグを構成します。 ○ 通知：セキュリティインシデントが重大なセキュリティインシデントとして提案または昇格されたときのメール通知プロセスとユーザー通知を自動化します。
MSI マネージャー	sn_msi.workspace_manager	• 重大セキュリティインシデント管理の構成設定ページへのアクセス権を表示します。構成設定の変更については制限されています。 • 重大インシデント管理 ワークスペースの [詳細]、[コラ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重大インシデント管理 のロール (続く)

ロールタイプ	ロール	説明
		ボレーション]、および [タスクオーガナイザー] タブで、インシデントレコードデータを表示および編集します。 • セキュリティインシデントを重大なセキュリティインシデントに昇格します。 • 重大インシデント管理 ワークスペースの [コラボレーション] タブのファイルエクスプローラーコンポーネントで実行可能なファイルとフォルダーのアクションを構成します。 • ワークスペースから重大なセキュリティインシデントに追加レコードをリンクおよびリンク解除する。
MSI レスポンダー	sn_msi.workspace_responder	• で重大なセキュリティインシデントを表示、編集、応答するためのオプションのロール 詳細 AND タスク 重大インシデント管理のタブ。 • ワークスペースから重大なセキュリティインシデントに追加レコードをリンクおよびリンク解除する。

自動翻訳

重大セキュリティインシデント管理 の統合

Microsoft アプリケーションと統合することで、重大セキュリティインシデント管理 の機能を拡張し、Now Platform インスタンスと接続します。

重要:
構成の簡単なセットアップでユーザーを支援する更新セット (KB1289784) は、「重大セキュリティインシデント管理クイックスタートガイド」にあります。アプリケーションのインストールの後にこの更新セットをインポートする必要があります。ServiceNow Store にある MSIM アプリケーション内の [補足ドキュメント (Supporting documents)] セクションにある「クイックスタートガイド」(ステップ 2) に記載されている手順に従います。

Microsoft SharePoint ドキュメントライブラリの設定

Microsoft SharePoint で実行する必要がある、必要な設定を確認します。

始める前に
次の設定手順が完了していることを確認します。

必要なロール：システムアドミニストレーター、sn_msi.workspace_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 新規または既存の Microsoft SharePoint サイトに新しいドキュメントライブラリを作成し、重大セキュリティインシデント管理 ファイルリポジトリ構成の構成時に同じサイトを使用します。
2. アプリケーションを Microsoft に登録して接続を確立し、Microsoft SharePoint Rest API を使用して Microsoft SharePoint と通信します。
   アプリケーションを登録すると、アプリと Microsoft の間に接続が確立されます。詳細については、docs.microsoft.com ポータルの「Set up app-only access to SharePoint (SharePoint へのアプリ専用アクセスの設定)」を参照してください。

   アプリケーションを Microsoft SharePoint に登録するには、次の 2 つの方法があります。

   a. Azure AD アプリのみを介したアクセスの許可

   b. を使用したアクセスの許可 Microsoft SharePoint アプリ専用

   > **重要:**
   > Microsoft SharePoint アプリのみを使用したアクセスの許可は従来のアプローチですが、非常に関連性が高く設定が簡単です。

   ファイルエクスプローラー Microsoft SharePoint コネクタの REST 接続を設定するときに、上記の手順で生成されたクライアント ID とクライアントシークレットを使用します。
3. Microsoft にもう 1 つのアプリを登録し、Microsoft Graph API を使用して Microsoft SharePoint と通信します。
   詳細については、「アプリケーションを Microsoft ID プラットフォームに登録する」を参照してください **Azure** 上の新しいアプリケーションを **Now Platform** インスタンスに登録する

   a. Microsoft アカウントを使用して Azure ポータルにサインインします。

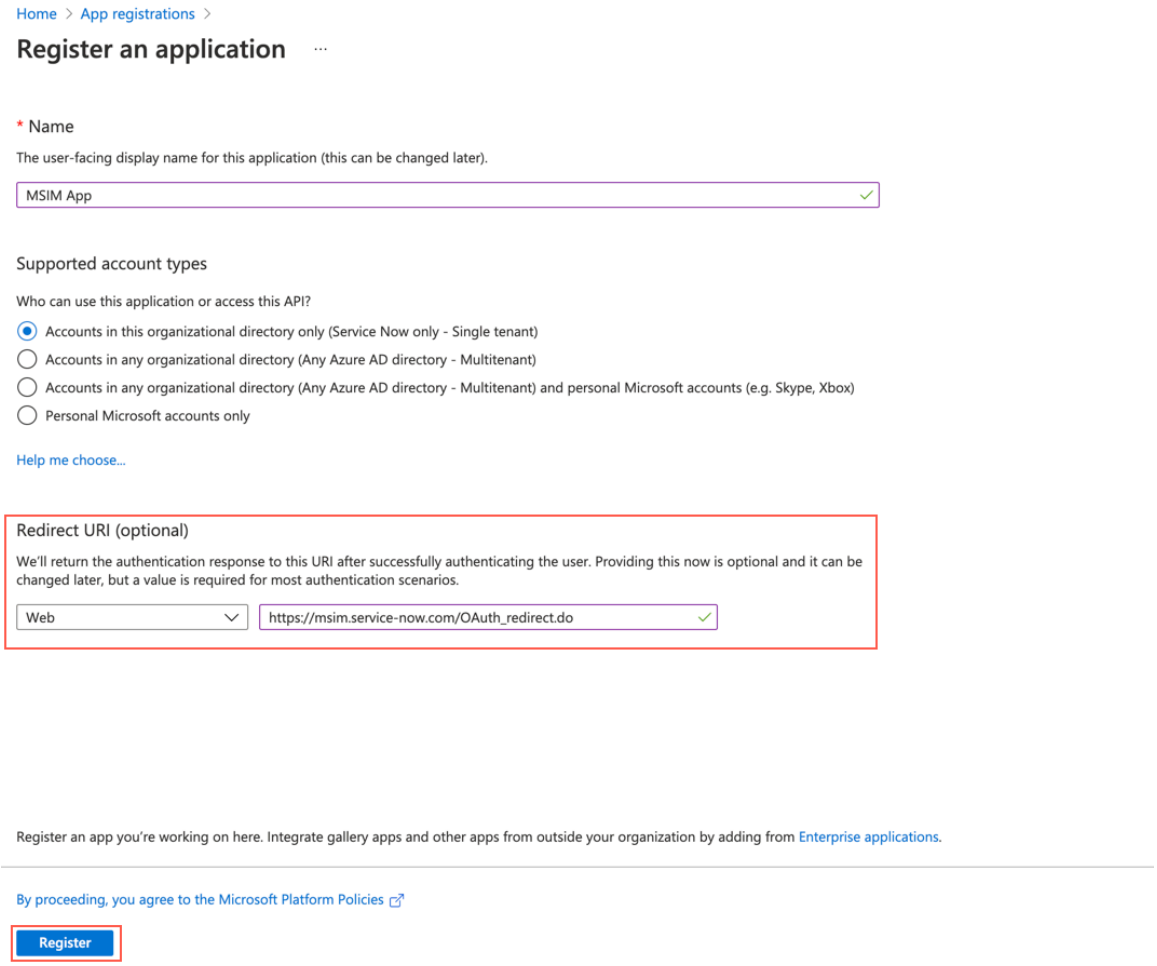
   b. Microsoft ポータルに示された指示に従います。

   c. 許可されるリダイレクト URL のフィールドに Now Platform® インスタンスのリダイレクト URL を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

例：msim.service-now.com/OAuth_redirect.do



d. 登録 必要があります

e. [証明書とシークレット **(Certificates & secrets)]** セクションに移動し、新しいクライアントシークレットを作成します。

> **注:**
> クライアント証明書をアップロードすることもできます。生成されたサムプリントの値を必ずコピーして保存してください。

f. ServiceNow® インスタンスでの OAuth アプリケーションレジストリの設定時に必要になるため、生成されたクライアントシークレットを別の場所にコピーして保存します。

4. [API 権限] で、Microsoft Graph 権限を追加します。

a. [アクセス許可の追加] をクリックします。

b. [Microsoft Graph] を選択します。

c. [委任されたアクセス許可] を選択します。

d. [サイト] リストから、**[Sites.ReadWrite.All]** 権限を選択します。

e. [ユーザー] リストから、**[User.Read]** 権限を選択します。

f. [アクセス許可の追加] をクリックします。

5. [API 権限] で、SharePoint 権限を追加します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. [アクセス許可の追加] をクリックします。

b. **[SharePoint]** を選択します。

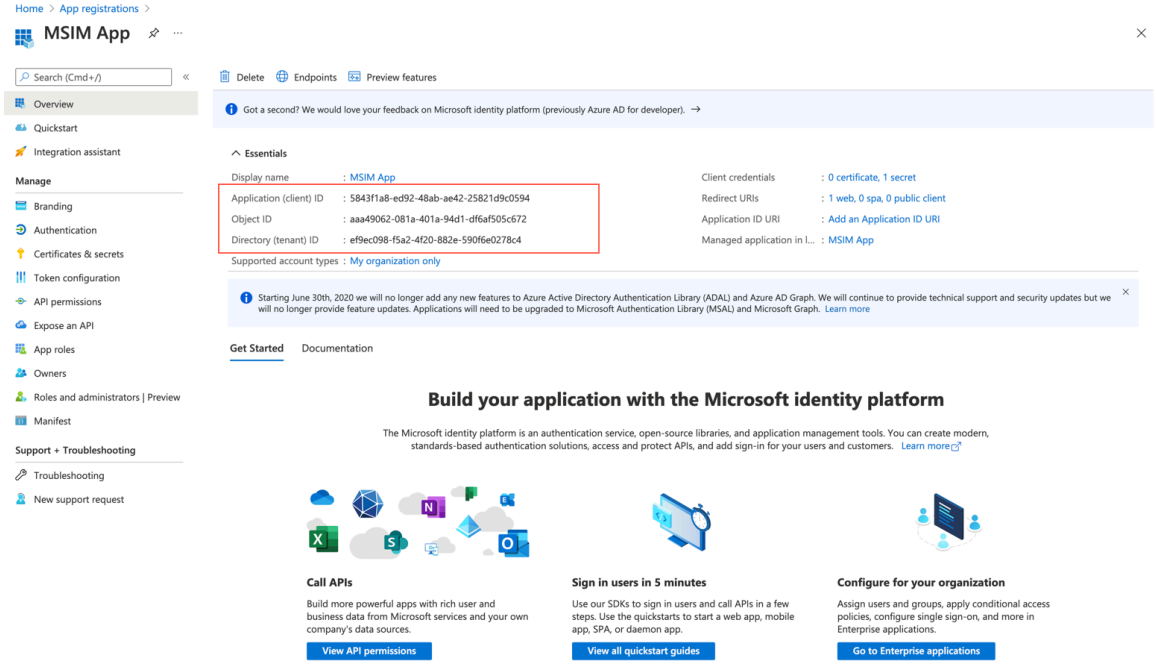
c. [アプリケーションの権限 **(Application Permissions)]** を選択します。

d. [サイト] リストから、**[Sites.FullControl.All]** 権限を選択します。

e. [アクセス許可の追加] をクリックします。

6. 権限を追加した後、[アドミンの同意を付与する **(Grant admin consent)]** をクリックします。

7. ファイルエクスプローラー Microsoft Teams コネクタの Graph 接続を構成するときに、このアプリケーションレジストリから生成された同じクライアント ID とクライアントシークレットの値 ([概要] セクションで入手可能) を使用します。



Now Platform での **Graph** および **REST** 接続の確立

Microsoft SharePoint と通信できるように Now Platform インスタンス上で Graph および REST 接続を構成します。

Microsoft SharePoint でカスタム OAuth アプリケーションを作成して Now Platform インスタンスと Microsoft SharePoint を統合し、Now Platform 要求を認証します。

MS SharePoint 用の **REST** 接続の設定

Now Platform のインスタンスで、Microsoft SharePoint と通信するための REST 接続を設定します。

始める前に
必要なロール：admin

手順

1. 新しいテナントレコードを設定し、エイリアスレコードとして **[MicrosoftSharepointOnline]** を選択します。
詳細については、「Define Microsoft SharePoint tenants (Microsoft SharePoint テナントの定義)」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. **MicrosoftSharepointOnline** 接続および資格情報エイリアスを構成するには、。
3. 上記のステップ 2 で作成したテナントレコードを次のように選択します。 **REST** 接続 ファイルリポジトリ構成フォームへの入力中に

MS SharePoint 用のグラフ接続の設定

Now Platform のインスタンスで、Microsoft SharePoint と通信するためのグラフ接続を設定します。

始める前に
必要なロール：admin

手順

1. クライアントシークレットを使用して「接続および資格情報エイリアス」グラフを構成するには、「」を参照してください。
   クライアント証明書を使用してグラフ接続および資格情報エイリアスを設定するには、以下の手順に従います。

   > **注:**
   > デフォルトでは、前の REST 接続で設定された JWT プロバイダー、JWT キー、および証明書がこの手順で使用されます。詳細については、「MS SharePoint 用の REST 接続の設定」を参照してください。

   a. 次のように移動する。 **All** (すべて) > 接続 **&** 認証情報 > 接続および資格情報エイリアス.

   b. レコード **MicrosoftSharePointGraph** を開きます。

   c. [新しい接続および資格情報の作成] 関連リンクをクリックします。

   d. フォームで、詳細を入力します。

フィールド	説明
OAuth エンティティ名	OAuth アプリケーションレジストリレコードを識別する名前。
OAuth クライアント ID	クライアント ID
OAuth クライアントシークレット	任意の値を入力できます。 **注:** 証明書ベースの認証を使用するため、この値は重要ではありません。
OAuth 認証 URL	認証 URL のフォーマット：`https://login.microsoftonline.com/<tenant-id>/oauth2/v2.0/authorize?response_mode=query`
OAuth トークン URL	トークン URL のフォーマット：`https://login.microsoftonline.com/<tenant-id>/oauth2/v2.0/token`

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
トークン失効 URL	トークン失効 URL のフォーマット：https://login.microsoftonline.com/<tenant-id>/oauth2/v2.0/token
OAuth リダイレクト URL	ServiceNowリダイレクト URL のフォーマット：https://empipaas.service-now.com/oauth_redirect.do

注:
要件に応じてデフォルト値を変更できます。

e. **[OAuth** トークンを作成して取得] をクリックします。
「401- unauthorized」というエラーメッセージが表示されます。

f. フォームを再ロードし、[接続] 関連リストのレコードを開きます。

g. [属性] セクションの [エンコードされたサムプリント値 **(Encoded Thumbprint Value)]** 属性に、Base64 でエンコードされた [サムプリント] の値を入力します。

注:
[サムプリント] の値は 16 進値です。16 進値から Base64 への (Hex to Base64) 変換ツールを使用して、[サムプリント] の値を Base64 値にエンコードできます。

h. 次のように移動する。 システム **OAuth** > アプリケーションレジストリー.

i. この手順のステップ d に記載の、**[OAuth** エンティティ名]と同じ名前のレコードを開きます。

j. OAuth API スクリプトを **OAuthUtilJWTFESPGraph** に変更します。

k. 次のように移動する。 接続 **&** 認証情報 > 認証情報.

l. レコード **Microsoft SharePoint Graph Credential** を開きます。

m. [関連リンク] セクションで **[OAuth** トークンを取得] をクリックします。

2. OAuth エンティティスコープを更新します。

a. 次のように移動する。 システム **OAuth** > アプリケーションレジストリー.

b. ステップ 1 で生成した OAuth アプリケーションレジストリレコードを開きます。

c. **[OAuth** エンティティスコープ] 関連リストを選択します。

d. **[OAuth** スコープ] フィールドを次の **offline_access** 値に置き換えます。

```
https://graph.microsoft.com/Sites.ReadWrite.All
```

注:
クライアント証明書を追加する場合は、ステップ 2 を無視して次のステップに進んでかまいません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. 新しいテナントレコードを設定し、ステップ 1 で作成したエイリアスレコードを選択します。詳細については、「Define Microsoft SharePoint tenants (Microsoft SharePoint テナントの定義)」を参照してください。
4. ステップ 3 で作成したテナントレコードを次のように選択します。 グラフ接続 ファイルリポジトリ構成フォームへの入力中に

Now Platform での MS Teams Graph 接続の確立

Microsoft Teams Graph 接続を確立して、Now Platform インスタンスと Microsoft Teams アカウントを統合します。

始める前に

必要に応じて、SharePoint 用に作成したものと同じアプリケーションを使用して、Microsoft Teams Graph 接続を確立できます。

必要なロール：admin、Azure admin

Azure での Microsoft Teams Graph 接続用の新しいアプリケーションの登録

手順

1. Microsoft アカウントを使用して Azure ポータルにサインインします。
2. 次のように移動する。 **Azure** サービス > アプリケーション登録 > 新規登録.
3. アプリケーションの名前を入力します。
   たとえば、Microsoft Teams Graph などです。
4. 組織に該当するそれぞれの [サポートされているアカウントの種類 **(Supported account types)**] オプションを選択します。
   たとえば、[この組織のディレクトリ内のアカウントのみ **(Service Now** のみ **-** シングルテナント) **(Accounts in this organizational directory only (Service Now only - Single tenant))**] オプションを選択します。

   > **注:**
   > サポートされているアカウントの種類の詳細については、「アプリケーションを Microsoft ID プラットフォームに登録する」を参照してください。

5. [リダイレクト URL] の下のドロップダウンリストから **[Web]** タイプを選択します。
6. 許可されるリダイレクト URL のフィールドに Now Platform インスタンスのリダイレクト URL を入力します。
   例：https://<<InstanceName>>.service-now.com/oauth_redirect.do
7. [登録] をクリックして新しいアプリケーションを登録し、ページに [概要] セクションが表示されていることを確認します。

証明書を使用した認証

証明書の認証情報を使用してアクセストークンを要求します。

始める前に

1. 自己署名証明書も CA 発行の証明書も使用できます。「アプリ専用アクセス用の Azure AD アプリの設定 (Setting up an Azure AD app for app-only access)」で説明されているように、PowerShell スクリプトを実行して、自己署名証明書を作成できます。このスクリプトは、.PFX ファイルと .CER ファイルの 2 つのファイルを生成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> 秘密鍵を暗号化して .PFX ファイルと .CER ファイルを生成するために使用されるパスワードを知っていることを確認してください。

2. Java Key Store (JKS) ファイルを作成するには、.PFX ファイルを使用します。

> **注:**
> JKS ファイルを .PFX ファイルから生成するために使用されるパスワードを知っていることを確認してください。

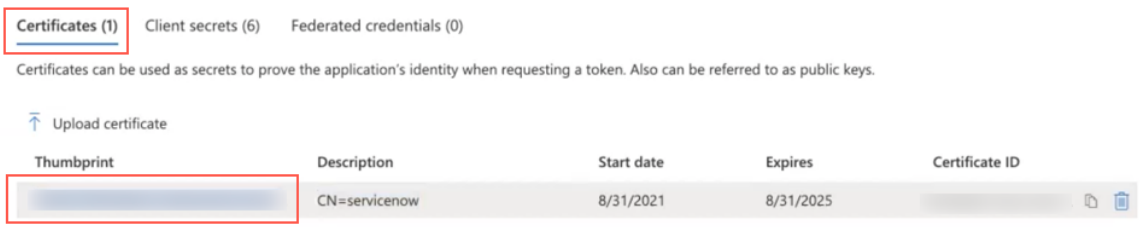
必要なロール：admin

手順

1. Azure AD ポータルで、[アプリの登録 **(App registrations)]** に移動します。
2. [管理] セクションから [証明書とシークレット **(Certificates & secrets)]** をクリックします。
3. [証明書] タブで、[証明書のアップロード **(Upload Certificate)]** をクリックします。
4. フォームに、これらの値を入力します。

フィールド	説明
.cer、.pem、.crt のいずれかのファイルタイプで証明書 (公開鍵) をアップロードします。	PowerShell スクリプトを使用して生成した .CER ファイル。
説明	証明書の説明。

5. [追加] をクリックします。
   証明書がアップロードされ、その詳細が [証明書] タブに表示されます。
6. アップロードした証明書の **[Thumbprint]** 値をコピーします。
   [サムプリント] の値は 16 進値です。



7. [サムプリント] の値を Base64 値にエンコードして記録し、後で使用できるようにします。

> **注:**
> 16 進値から Base64 への (Hex to Base64) 変換ツールを使用して、[サムプリント] の値を Base64 値にエンコードできます。

MS Teams 用の Java Key Store 証明書の添付

有効な Java Key Store (JKS) 証明書を添付して、JWT ベアラー権限許可トークン認証を有効にします。

始める前に
ServiceNow インスタンスにログインして、次の手順を実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 有効な Java Key Store 証明書
- 必要なロール：admin

手順

1. 次のように移動する。 システム定義 > 証明書.
2. **[Microsoft Teams Connector** 証明書 **(Microsoft Teams Connector Certificate)]** レコードを開きます。
   必ず、デフォルトのレコードである **Microsoft Teams Connector** 証明書のみを使用してください。
3. JKS ファイルに関連付けられたパスワードを [キーストアパスワード] に入力します。
4. 添付ファイルアイコン ( ) をクリックし、生成した JKS 証明書を添付します。
   詳細については、「」を参照してください。
5. [ストア/証明書を検証] をクリックします。
6. [更新] をクリックします。

MS Teams 用の **JWT** 署名キーの構成

Java Key Store 証明書に割り当てる JSON Web トークン (JWT) 署名キーを作成します。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 システム **OAuth** > **JWT** キー.
2. **[Microsoft Teams Connector JWT (Microsoft Teams Connector JWT)]** レコードを開きます。
3. 秘密鍵を暗号化し、.PFX ファイルと .CER ファイルを生成するために使用するパスワードを、[署名キーパスワード] に入力します。
4. [更新] をクリックします。

MS Teams 用の **JWT** プロバイダーの構成

JSON Web トークン (JWT) プロバイダーを ServiceNow インスタンスに追加します。

始める前に

- Azure ポータルに登録したアプリケーションの [アプリケーション (クライアント) **ID]** と [ディレクトリ (テナント) **ID]** の値をコピーして記録します。

- 必要なロール：admin

手順

1. 次のように移動する。 システム **OAuth** > **JWT** プロバイダー.
2. **[MS Teams Connector JWT** プロバイダー **(MS Teams Connector JWT Provider)]** というレコードを開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. [標準要求] 関連リストで、**[iss]**、**[sub]**、および **[aud]** の各値を入力します。

フィールド	値
aud	次の形式の Microsoft Online URL：https://login.microsoftonline.com/<tenant-id>/oauth2/token。<tenant-id> を、Azure ポータルにアプリケーションが登録した [ディレクトリ (テナント)] の値と置き換えます。
iss	Azure ポータルに登録したアプリケーションの [アプリケーション (クライアント) ID]。
sub	Azure ポータルに登録したアプリケーションの [アプリケーション (クライアント) ID]。

4. [更新] をクリックします。

証明書を使用した接続の確立

証明書を使用して、新しく作成された Microsoft Teams グラフアプリケーション間の接続を確立します。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 接続 **&** 認証情報 > 接続および資格情報エイリアス.
2. **Microsoft Teams Spoke**を開きます。
3. フィールド値 [構成テンプレート：**MSIM Microsoft Teams** コネクタ承認コードテンプレート **(Configuration Template: MSIM Microsoft Teams ConnectorAuthorization Code Template)]** を変更して、フォームを保存します。

   注:
   このテンプレートには、MSTeams 統合に必要な委任 API 権限が含まれています。

4. [関連リンク] セクションから、[新しい接続および資格情報の作成] をクリックします。

5. **[OAuth** トークンを作成して取得] をクリックします。
   「401- unauthorized」というエラーメッセージが表示されます。
6. フォームを再ロードし、[接続] 関連リストのレコードを開きます。
7. [属性] セクションの [エンコードされた証明書のサムプリント] 属性に、Base64 でエンコードされた [サムプリント] の値を入力します。

   注:
   [サムプリント] の値は 16 進値です。16 進値から Base64 への (Hex to Base64) 変換ツールを使用して、[サムプリント] の値を Base64 値にエンコードできます。

8. 次のように移動する。 システム **OAuth** > アプリケーションレジストリー
9. **MSIM Microsoft Teams Connector** 認証コード **(MSIM Microsoft Teams Connector Authorization Code)** レコードを開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

10. OAuth API スクリプト **OAuthUtilJWTMSTeamsConnector** を変更します。
11. 次のように移動する。 接続 **&** 認証情報 > 認証情報.
12. **[Microsoft Teams Connector** 認証情報 **(MSIM Microsoft Teams Connector Credential)]** レコードを開きます。
13. [関連リンク] から、**[OAuth** トークンの取得] をクリックします。
成功すると、次の API 権限が Azure アプリケーションに追加されます。

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

クライアントシークレット値の使用

クライアントシークレット値を使用して、Graph アプリケーションのレジストリレコードを設定できます。

始める前に
必要なロール：admin

手順

1. Azure AD ポータルで、[アプリの登録 **(App registrations)]** に移動します。
2. [管理] セクションから [証明書とシークレット **(Certificates & secrets)]** をクリックします。
3. [新しいクライアントシークレット **(New client secret)]** をクリックします。
4. 作成された [値] フィールドのクライアントシークレットをコピーしてメモします。

クライアントシークレットを使用した接続の確立

新しく作成した Microsoft Teams グラフアプリケーションと Now Platform インスタンス間の接続を確立します。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 接続 **&** 認証情報 > 接続および資格情報エイリアス.
2. **Microsoft Teams Spoke**を開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. フィールド値 [構成テンプレート：**MSIM Microsoft Teams** コネクタ承認コードテンプレート **(Configuration Template: MSIM Microsoft Teams ConnectorAuthorization Code Template)**] を変更して、フォームを保存します。

   注:
   このテンプレートには、MSTeams 統合に必要な委任 API 権限が含まれています。

4. [関連リンク] セクションから、[新しい接続および資格情報の作成] をクリックします。

5. **[OAuth** トークンを作成して取得] をクリックします。
   成功すると、次の API 権限が Azure アプリケーションに追加されます。

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

自動翻訳

MS Teams Graph Spoke ユーザーのための **MS Teams** チャットコネクタのアクティブ化

既存のユーザーの場合は、このセクションの手順に従って Microsoft Teams チャットコネクタをアクティブ化してください。

始める前に
必要なロール：admin

手順

Microsoft Teams Graph Spoke の既存ユーザーの場合は、次の手順に従います。

- Microsoft Teams Graph Spoke で使用される Azure ポータルの登録済みアプリケーションに移動します。
- **[API** 権限] セクションに移動して、必要な API 権限を設定します。
- [アクセス許可の追加] をクリックします。
- **[Microsoft Graph]** を選択します。
- Microsoft Teams Connector アプリケーションを使用するには、Azure ポータルからアプリケーションに委任された 2 つの権限「ChannelMember.ReadWrite.All」と「TeamMember.ReadWrite.All」を追加する必要があります。
- 前述の必要な権限を追加した後、[アドミンの同意を付与する] をクリックします。

既存のユーザーの **Now Platform** インスタンスで **MS Teams** を設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [接続および資格情報エイリアス] に移動します。
- **Microsoft Teams** スポークレコードを選択します。
- Microsoft Teams Spoke に関連付けられた認証情報レコードを選択します。
- **[OAuth** トークンを取得 **(Get OAuth Token)]** をクリックします。OAuth Refresh トークンが利用可能である旨の確認メッセージが表示されます。

既存のユーザーとして、Microsoft Teams チャットコネクタアプリケーションと Microsoft Teams Graph API の統合を完了しました。

重大セキュリティインシデント管理カンファレンスコールの統合

重大セキュリティインシデント管理カンファレンスコールの統合では、MSIM アプリケーションから Microsoft Teams、Cisco Webex、または Zoom のビデオおよび画面共有オプションを使用して、顧客やピアエージェントと協力して顧客の問題を解決できます。

重大セキュリティインシデント管理カンファレンスコール統合は、重大セキュリティインシデント管理アプリケーションから直接 Microsoft Teams、Cisco Webex、または Zoom 会議を管理および開始することで、カンファレンスコミュニケーションチャネルと通知コミュニケーションチャネルを統合できます。

MSI マネージャーは、MSIM カンファレンスコール統合を使用して、Microsoft Teams、Cisco Webex または Zoom 会議を開始できます。重大セキュリティインシデント管理カンファレンスコールをコミュニケーションチャネルとしてサードパーティサービスプロバイダーと統合し、重大なセキュリティインシデントを解決するためにステークホルダーと会議ができます。

主な機能

重大セキュリティインシデント管理カンファレンスコールの統合は、次の主要な機能を提供します。

- MSI マネージャーは、重大なセキュリティインシデントから直接、Microsoft Teams、Cisco Webex、または Zoom カンファレンスコールを開始できます。
- 追加の参加者をコールに招待します。
- コール記録とチャットの詳細を表示します。
- メールと Microsoft Teams チャットを介して参加者に招待状を送信します。

カンファレンスの開始

1 人または複数のユーザーがカンファレンスコールに参加するように招待することで、タスクまたは重大なセキュリティからカンファレンスコールを開始します。カンファレンスコールは、2 人以上の参加者が参加したときのみ開始されます。

始める前に

必要なロール：sn_msi.workspace_manager

ServiceNow® インスタンスで以下が実行済みであることを確認してください。

- 通知プラグイン (com.snc.notify) をインストールして有効化している。
- 構成可能ワークスペースアプリの通知 UI コンポーネントをインストールしている。
- ビジュアルタスクボードプラグイン (com.devsnc.snb_vtb) をインストールして有効にしている。

詳細については、「統合ハブの要求」を参照してください。

このタスクについて

会議参加者には、次のものを含めることができます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

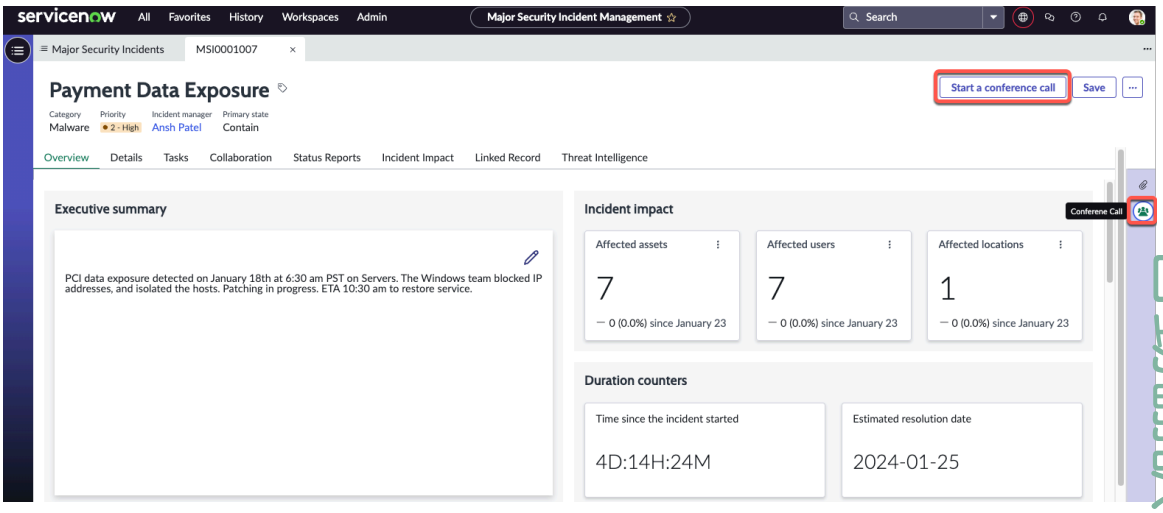
自動翻訳

- 特定の責務をアサインされたユーザー。
- アドホックまたはオンデマンドの連絡先
- その他のサードパーティ連絡先

手順

1. 次のように移動する。 ワークスペース > 重大セキュリティインシデント管理.
2. [重大なセキュリティインシデント] リストから、重大なセキュリティインシデントを選択します。
3. Select the **Start a conference call** action.
4. You can also start a conference call by selecting the icon on the right-context menu and selecting the + icon.
   [カンファレンスコールを開始] ポップアップが表示されます。

MSIM カンファレンスコール



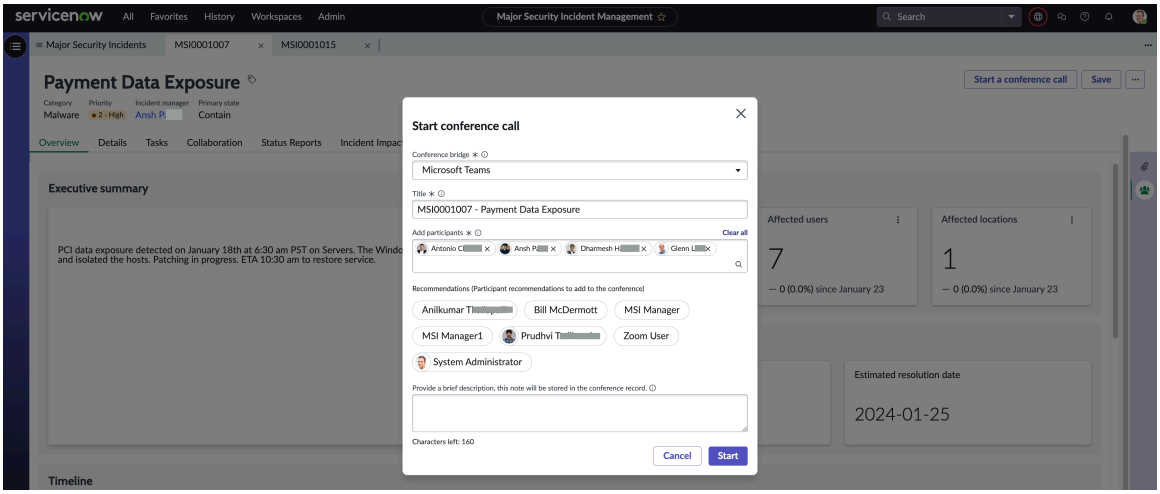
5. [会議ブリッジ] フィールドで、接続元の会議ブリッジを選択します。
   例：Microsoft Team、Zoom、Cisco Webex など。
6. [タイトル] フィールドに、カンファレンスコールの理由を説明するタイトルを入力します。
7. [参加者を追加] フィールドで、カンファレンスコールの参加者を選択します。
   検索オプションを使用して必要な参加者を検索して追加することも、[推奨事項] リストから参加者を選択して参加者を追加することもでき、これにより、カンファレンスコールに追加する参加者の推奨事項が表示されます。

   カンファレンスコールを開始したユーザー (ホスト) は、選択済み参加者のリストに追加されます。重大なセキュリティインシデントに関連付けられているすべてのユーザーは、デフォルトで [推奨事項] リストに表示されます。

   注:
   選択した参加者が有効なメールアドレスを持っていることを確認してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

カンファレンスの開始



8. 参加者を選択したら、[説明] フィールドにカンファレンスコールを開始する理由についての簡単な説明を入力します。
   入力した説明が会議レコードに追加されます。
9. 参加者リストが完成したら、[開始 **(Start)]** を選択します。
   選択した会議ブリッジでカンファレンスコールが開始されます。すべての参加者にはメールで通知され、選択されたそれぞれの会議ブリッジを介しても通知されます。
10. 重大なセキュリティインシデントの上部にある [ここをクリック] オプションを選択して、カンファレンスコールに参加します。
    参加者は、メール通知からのリンクまたは選択した会議ブリッジからの通知を使用して、コールに参加できます。
11. 関連する重大なセキュリティインシデントを開いて、カンファレンスコールの詳細を表示します。
    最後の参加者が会議を退出すると、カンファレンスコールが終了するか、[コールを終了] を選択してカンファレンスコールを終了します。

カンファレンスへの参加者の追加

[カンファレンスコールを開始] ポップアップの検索オプションを使用してカンファレンスコールに参加者を追加し、必要な参加者を検索して追加します。[推奨事項] リストから参加者を選択して参加者を追加することもできます。これにより、カンファレンスコールに追加する参加者の推奨事項が表示されます。

始める前に

必要なロール：sn_msi.workspace_manager

このタスクについて

カンファレンスコールを開始したユーザー (ホスト) は、選択済み参加者のリストに追加されます。重大なセキュリティインシデントに関連付けられているすべてのユーザーは、デフォルトで [推奨事項] リストに表示されます。

会議参加者には、次のものを含めることができます。

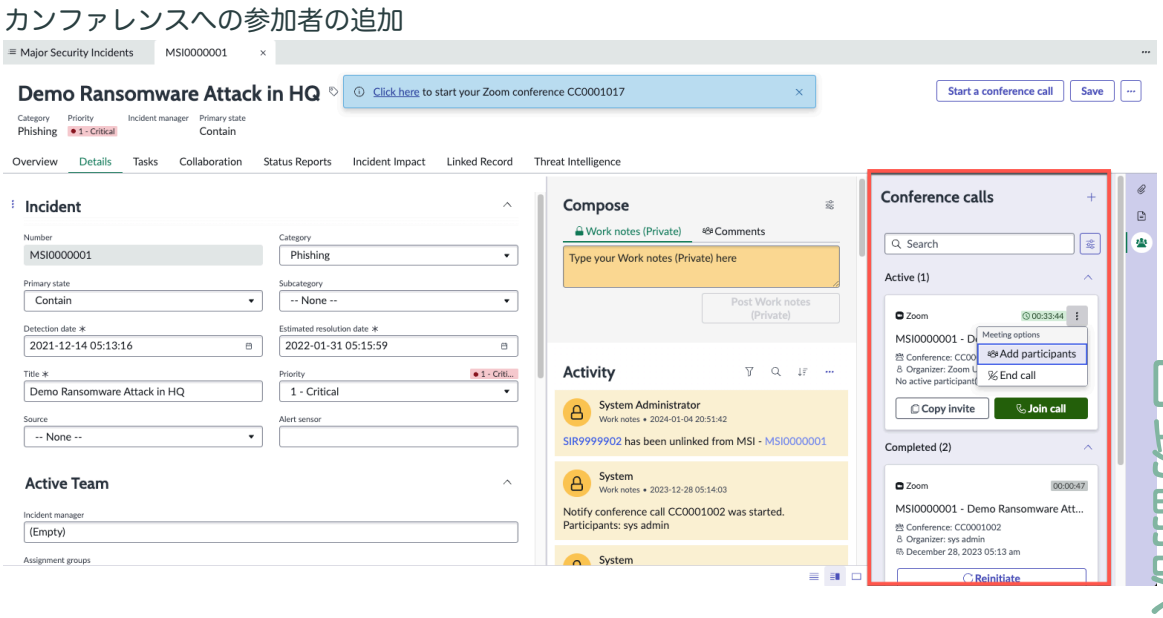
- 特定の責務をアサインされたユーザー。
- アドホックまたはオンデマンドの連絡先
- その他のサードパーティ連絡先

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 重大セキュリティインシデント管理.
2. [重大なセキュリティインシデント] リストから、カンファレンスコールで解決しようとしている重大なセキュリティインシデントを選択します。
3. 右側のコンテキストメニューで アイコンを選択すると、カンファレンスコールの詳細が表示されます。
   これには、会議ブリッジ名、主催者名、日付、時刻、コール期間、アクティブな参加者と非アクティブな参加者などの詳細が含まれます。
4. アクティブなカンファレンスコールの横にある を選択し、[参加者を追加] オプションを選択します。



5. 検索オプションを使用して必要な参加者を検索して追加することも、[推奨事項] リストから参加者を選択して参加者を追加することもでき、これにより、カンファレンスコールに追加する参加者の推奨事項が表示されます。
6. 参加者を選択したら、[説明] フィールドにカンファレンスコールを開始する理由についての簡単な説明を入力します。
   すべての参加者にはメールで通知され、選択されたそれぞれの会議ブリッジを介しても通知されます。参加者は、メール通知からのリンクまたは選択した会議ブリッジからの通知を使用して、コールに参加できます。
7. または、右側のコンテキストメニューの [カンファレンスコール] セクションで [招待をコピー **(Copy invite)]** オプションを選択して参加者を追加し、必要な参加者と共有することもできます。

カンファレンスコールで参加者をミュート状態にする

MSI マネージャーまたはカンファレンスコールのホストは、カンファレンスコールの特定の参加者またはすべての参加者をミュートにすることができます。

始める前に

必要なロール：sn_msi.workspace_manager

この手順を開始する前に、1 人以上の参加者がいるアクティブなカンファレンスコールが行われていることを確認してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 重大セキュリティインシデント管理.
2. [重大なセキュリティインシデント] リストから、カンファレンスコールで解決しようとしている重大なセキュリティインシデントを選択します。
3. 右側のコンテキストメニューで アイコンを選択すると、カンファレンスコールの詳細が表示されます。
4. アクティブな会議ブリッジで [電話に参加] を選択します。
5. カンファレンスコールに参加した後、ミュートする参加者を選択し、会議ブリッジで [ミュート] を選択します。
6. カンファレンスコールの参加者全員をミュートするには、会議コントロールで [参加者] を選択し、[すべてミュート] を選択します。

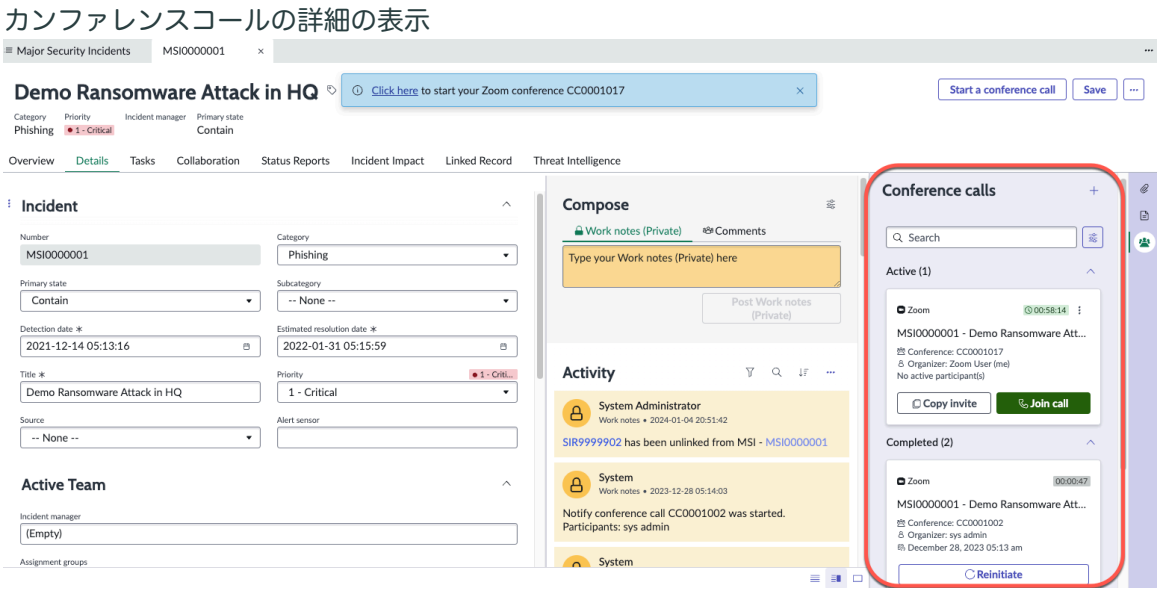
カンファレンスコールの詳細の表示

カンファレンスコールは、重大なセキュリティインシデントの [アクティビティ] セクションにシステムアクティビティとしてリストされ、[カンファレンスコール] 関連リストにもリストされます。会議ブリッジ名、主催者名、日付、時刻、コールの期間、アクティブな参加者および非アクティブな参加者などの詳細を含みます。

始める前に
必要なロール：sn_msi.workspace_manager

手順

1. 次のように移動する。 ワークスペース > 重大セキュリティインシデント管理.
2. [重大なセキュリティインシデント] リストから、カンファレンスコールで解決しようとしている重大なセキュリティインシデントを選択します。
3. 右側のコンテキストメニューで アイコンを選択すると、カンファレンスコールの詳細が表示されます。
   これには、会議ブリッジ名、主催者名、日付、時刻、コール期間、アクティブな参加者と非アクティブな参加者などの詳細が含まれます。



4. 検索オプションを使用して、特定のカンファレンスコールを検索できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

同じ重大なセキュリティインシデントに対して複数のコールが発生する可能性があります。

5. カンファレンスコールに参加者を追加するには、アクティブなカンファレンスコールの横にある ⋮ を選択し、[参加者を追加] オプションを選択します。
6. [招待をコピー **(Copy invite)]** オプションを使用して参加者を追加し、必要な参加者とリンクを共有することもできます。
7. カンファレンスコールに参加するには、[アクティブ] セクションに移動し、必要なカンファレンスコールの [電話に参加] オプションを選択します。
8. カンファレンスコールを終了するには、アクティブなカンファレンスコールの横にある ⋮ を選択し、[コールを終了] オプションを選択します。
9. カンファレンスコールを再開するには、[完了] セクションに移動し、必要なカンファレンスコールの [再開始 **(Reinitiate)]** オプションを選択します。

MSIM カンファレンスコールの Microsoft Teams との統合

カンファレンスコールの Microsoft Teams との統合を使用すると、重大なセキュリティインシデントから直接 Microsoft Teams カンファレンスコールを管理および開始できます。

主な機能

- 重大なセキュリティインシデントから直接 Microsoft Teams カンファレンスコールを開始および終了するか、重大なセキュリティワークベンチからタスクを開始および終了します。
- 参加者を追加または削除して Microsoft Teams カンファレンスコールを管理します。

必須条件

ServiceNow インスタンスに以下の統合ハブプラグインをインストールしていることを確認します。

- 通知 プラグイン (com.snc.notify)
- Microsoft Teams Communications スポークプラグイン (sn_msteams_com_spk)
- Azure Active Directory ユーザーマッピングプラグイン (sn_now_azure)
- 構成可能ワークスペースの通知 UI コンポーネント

詳細については、「Request IntegrationHub (統合ハブの要求)」を参照してください。

構成

- 事前構成済みアプリを使用して MSIM カンファレンスコール Microsoft Teams 統合を構成するには、「Integrate Notify connector pre-published app with Microsoft Teams」を参照してください。
- 自己構成済みアプリを使用して MSIM カンファレンスコール Microsoft Teams 統合を構成するには、「Integrating Notify connector self-configured app with Microsoft Teams」を参照してください。

MSIM カンファレンスコール Microsoft Teams 統合の使用

次の手順は、重大なセキュリティインシデントから直接 Microsoft Teams カンファレンスコールを管理および開始する方法のウォークスルーを示しています。

始める前に

必要なロール：sn_msi.workspace_manager

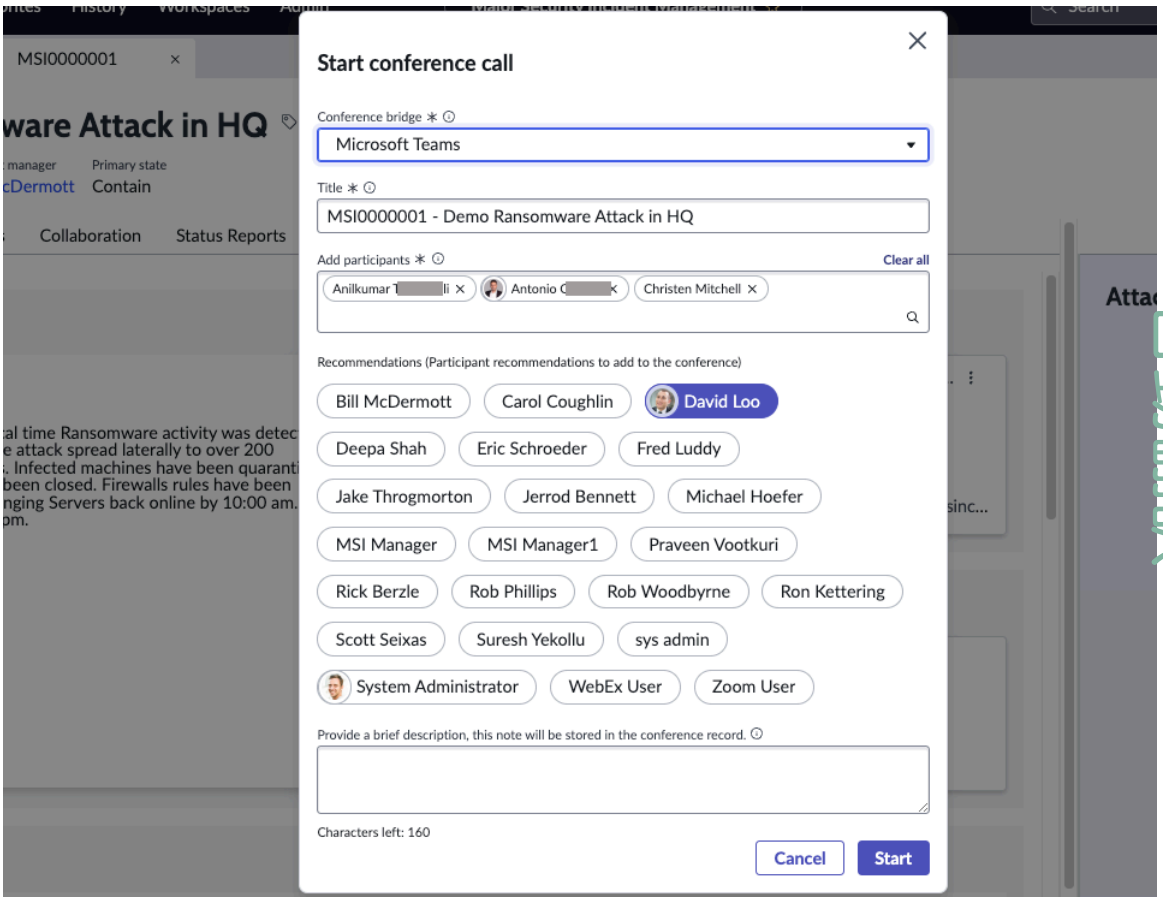
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 重大セキュリティインシデント管理.
2. [重大なセキュリティインシデント] リストから、重大なセキュリティインシデントを選択します。
3. Select the **Start a conference call** action.
4. You can also start a conference call by selecting the icon on the right-context menu and selecting the + icon.
   [カンファレンスコールを開始] ポップアップが表示されます。
5. 接続元の会議ブリッジとして **Microsoft Teams** を選択します。
6. [タイトル] フィールドに、Microsoft Teams カンファレンスコールの理由を説明するタイトルを入力します。

カンファレンスコール **Microsoft Teams** データ連携の使用



7. [参加者の追加] フィールドで、Microsoft Teams カンファレンスコールの参加者を選択します。検索オプションを使用して必要な参加者を検索して追加することも、[推奨事項] リストから参加者を選択して参加者を追加することもでき、これにより、Microsoft Teams カンファレンスコールに追加する参加者の推奨事項が表示されます。

   Microsoft Teams カンファレンスコールを開始したユーザー (ホスト) は、選択済み参加者のリストに自動的に追加されます。重大なセキュリティインシデントに関連付けられているすべてのユーザーは、デフォルトで [推奨事項] リストに表示されます。

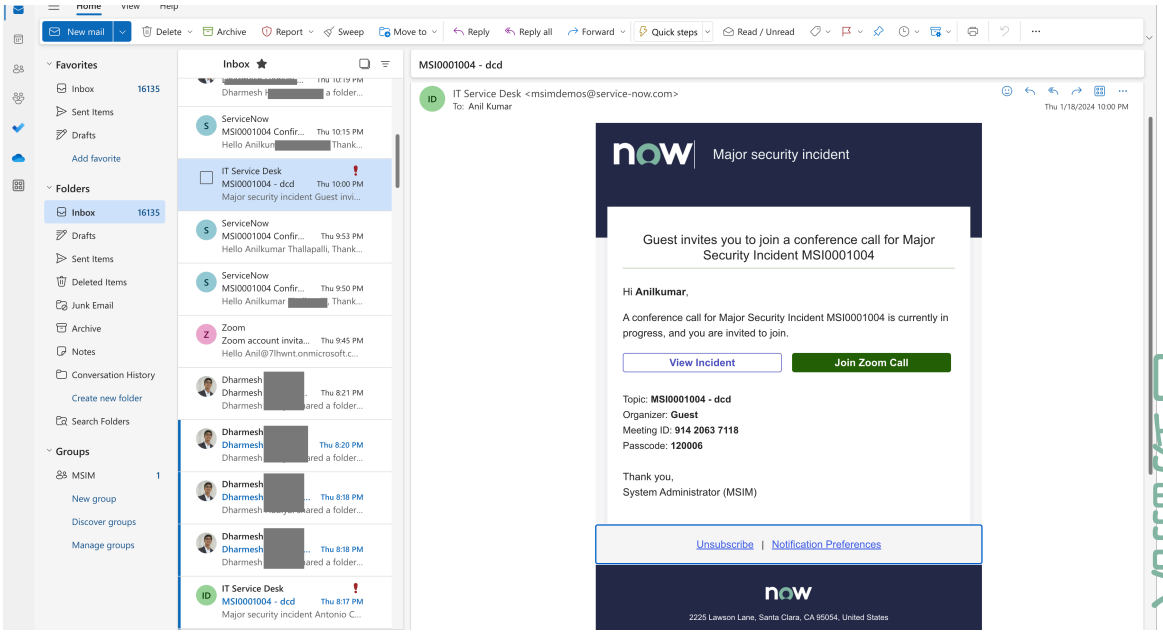
   注:
   選択した参加者が有効なメールアドレスを持っていることを確認してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

8. 参加者を選択したら、[説明] フィールドにカンファレンスコールを開始する理由についての簡単な説明を入力します。
入力した説明が会議レコードに追加されます。
9. 参加者リストが完成したら、[開始 **(Start)]** を選択します。
カンファレンスコールが Microsoft Teams アプリで開始されます。すべての参加者は MSIM アプリからメールで通知され、他の通知は Microsoft Teams アプリのボットを介して送信されます。
10. 重大なセキュリティインシデントの上部にある [ここをクリック] オプションを選択して、Microsoft Teams アプリでカンファレンスコールに参加します。
参加者は、MSIM メール通知からのリンクまたは Microsoft Teams アプリからの通知を使用して、コールに参加できます。

メール通知



11. MSIM ワークスペースで関連する重大なセキュリティインシデントを開いて、カンファレンスコールの詳細を表示します。

    最後の参加者が会議を退出すると、カンファレンスコールが終了するか、[カンファレンスコール] セクションで [コールを終了] を選択してカンファレンスコールを終了します。

MSIM カンファレンスコールの **Zoom** との統合

カンファレンスコールの Zoom との統合を使用すると、重大なセキュリティインシデントから直接 Zoom カンファレンスコールを管理および開始できます。

主な機能

- 重大なセキュリティインシデントや変更などの任意のタスクレコードから、または重大なインシデントワークベンチから、Zoom 会議を直接開始および終了します。
- 参加者を追加または削除して Zoom 会議を管理します。
- さらに分析するために、会議の期間や出席者などの会議の詳細を追跡して報告します。

必須条件

ServiceNow インスタンスに以下の統合ハブプラグインをインストールしていることを確認します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 通知 プラグイン (com.snc.notify)
- Zoom スポーク (sn_zoom_spoke)
- 通知 Zoom (sn_notify_zoom)
- 構成可能ワークスペースの通知 UI コンポーネント

詳細については、「Request IntegrationHub (統合ハブの要求)」を参照してください。

構成

通知コミュニケーションチャネルを使用して MSIM カンファレンスコール Zoom 統合を構成するには、「Configure Notify Zoom connector in Notify」を参照してください。

MSIM カンファレンスコール Zoom 統合の使用

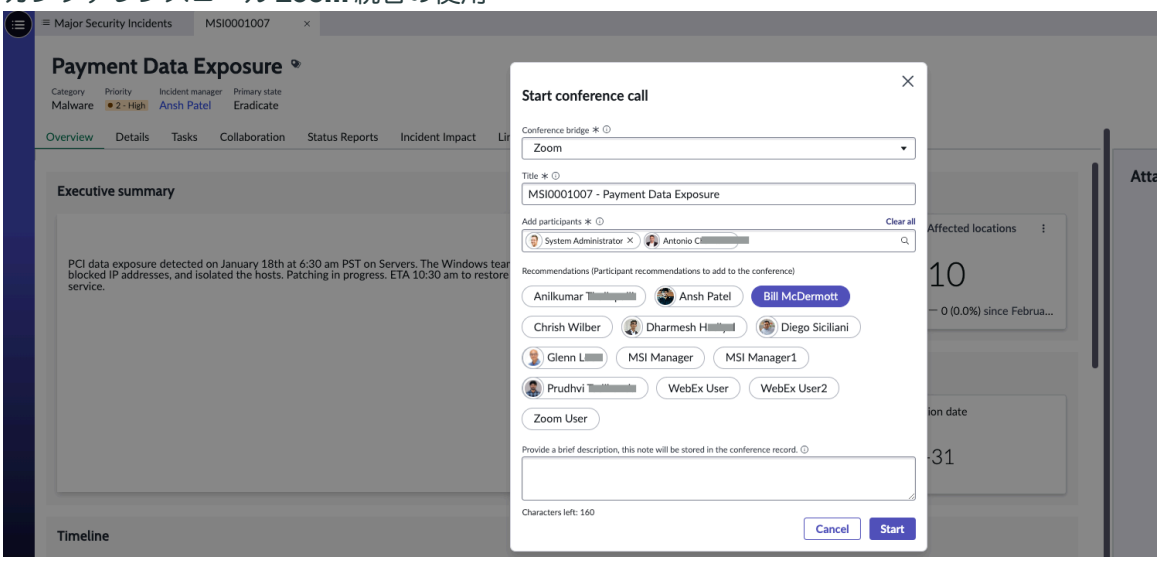
次の手順は、重大なセキュリティインシデントから直接 Zoom カンファレンスコールを管理および開始する方法のウォークスルーを示しています。

始める前に
必要なロール：sn_msi.workspace_manager

手順

1. 次のように移動する。 ワークスペース > 重大セキュリティインシデント管理.
2. [重大なセキュリティインシデント] リストから、重大なセキュリティインシデントを選択します。
3. [カンファレンスコールを開始] アクションをクリックします。
4. また、右側のコンテキストメニューの アイコンをクリックし、+ アイコンを選択して、カンファレンスコールを開始することもできます。
   [カンファレンスコールを開始] ポップアップが表示されます。
5. 接続元の会議ブリッジとして **[Zoom]** を選択します。
6. [タイトル] フィールドに、Zoom カンファレンスコールの理由を説明するタイトルを入力します。

カンファレンスコール Zoom 統合の使用



7. [参加者を追加] フィールドで、Zoom カンファレンスコールの参加者を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

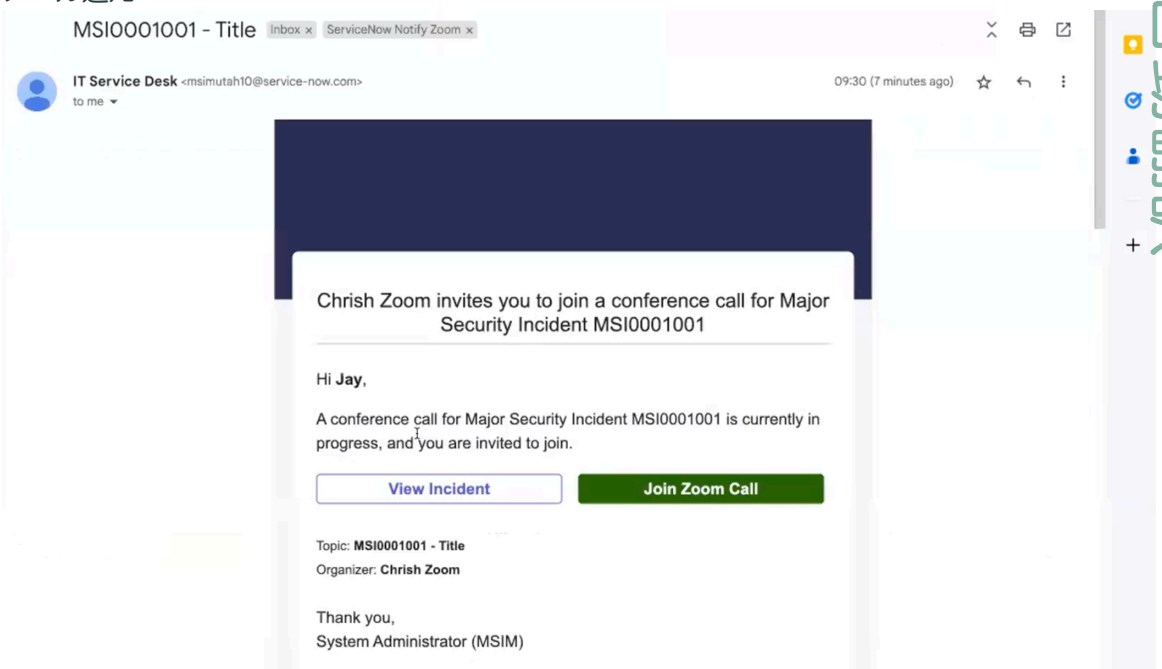
検索オプションを使用して必要な参加者を検索して追加することも、[推奨事項] リストから参加者を選択して参加者を追加することもでき、これにより、Zoom カンファレンスコールに追加する参加者の推奨事項が表示されます。

Zoom カンファレンスコールを開始したユーザー (ホスト) は、選択済み参加者のリストに追加されます。重大なセキュリティインシデントに関連付けられているすべてのユーザーは、デフォルトで [推奨事項] リストに表示されます。

> **注:**
> 選択した参加者が有効なメールアドレスを持っていることを確認してください。

8. 参加者を選択したら、[説明] フィールドにカンファレンスコールを開始する理由についての簡単な説明を入力します。
   入力した説明が会議レコードに追加されます。
9. 参加者リストが完成したら、[開始 **(Start)]** をクリックします。
   カンファレンスコールが Zoom アプリで開始されます。すべての参加者には 2 通のメールで通知されます。1 通のメールは MSIM アプリから参加者に送信され、もう 1 通のメールは Zoom 会議ブリッジから送信されます。
10. 重大なセキュリティインシデントの上部にある [ここをクリック] オプションを選択して、Zoom アプリでカンファレンスコールに参加します。
    参加者は、MSIM メール通知からのリンクまたは Zoom アプリからの通知を使用して、コールに参加できます。

メール通知



11. MSIM ワークスペースで関連する重大なセキュリティインシデントを開いて、カンファレンスコールの詳細を表示します。

    最後の参加者が会議を退出すると、カンファレンスコールが終了するか、[カンファレンスコール] セクションで [コールを終了] を選択してカンファレンスコールを終了します。

    カンファレンスが記録された場合、しばらくすると、関連する重大なセキュリティインシデントの [カンファレンス] セクションで録音が利用可能になります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MSIM カンファレンスコールと Cisco Webex との統合

MSIM カンファレンスコール Cisco Webex 統合では、重大なセキュリティインシデントから直接 Cisco Webex カンファレンスコールを管理および開始できます。

主な機能

- 重大なセキュリティインシデントから直接 Cisco Webex 会議を開始および終了します。
- 参加者を追加または削除して Cisco Webex 会議を管理します。

必須条件

ServiceNow インスタンスに以下の統合ハブプラグインをインストールしていることを確認します。

- 通知 プラグイン (com.snc.notify)
- 通知 Cisco Webex コネクタ (sn_notify_webex)
- Cisco Webex Teams スポーク (sn_cisco_teams_spk)
- 構成可能ワークスペースの通知 UI コンポーネント

詳細については、「Request IntegrationHub (統合ハブの要求)」を参照してください。

構成

通知コミュニケーションチャネルを使用して MSIM カンファレンスコール Cisco Webex 統合を構成するには、「Configure Notify Cisco Webex Connector」を参照してください。

カンファレンスコール Cisco Webex 統合の使用

次の手順は、重大なセキュリティインシデントから直接 Cisco Webex カンファレンスコールを管理および開始する方法のウォークスルーを示しています。

始める前に
必要なロール：sn_msi.workspace_manager

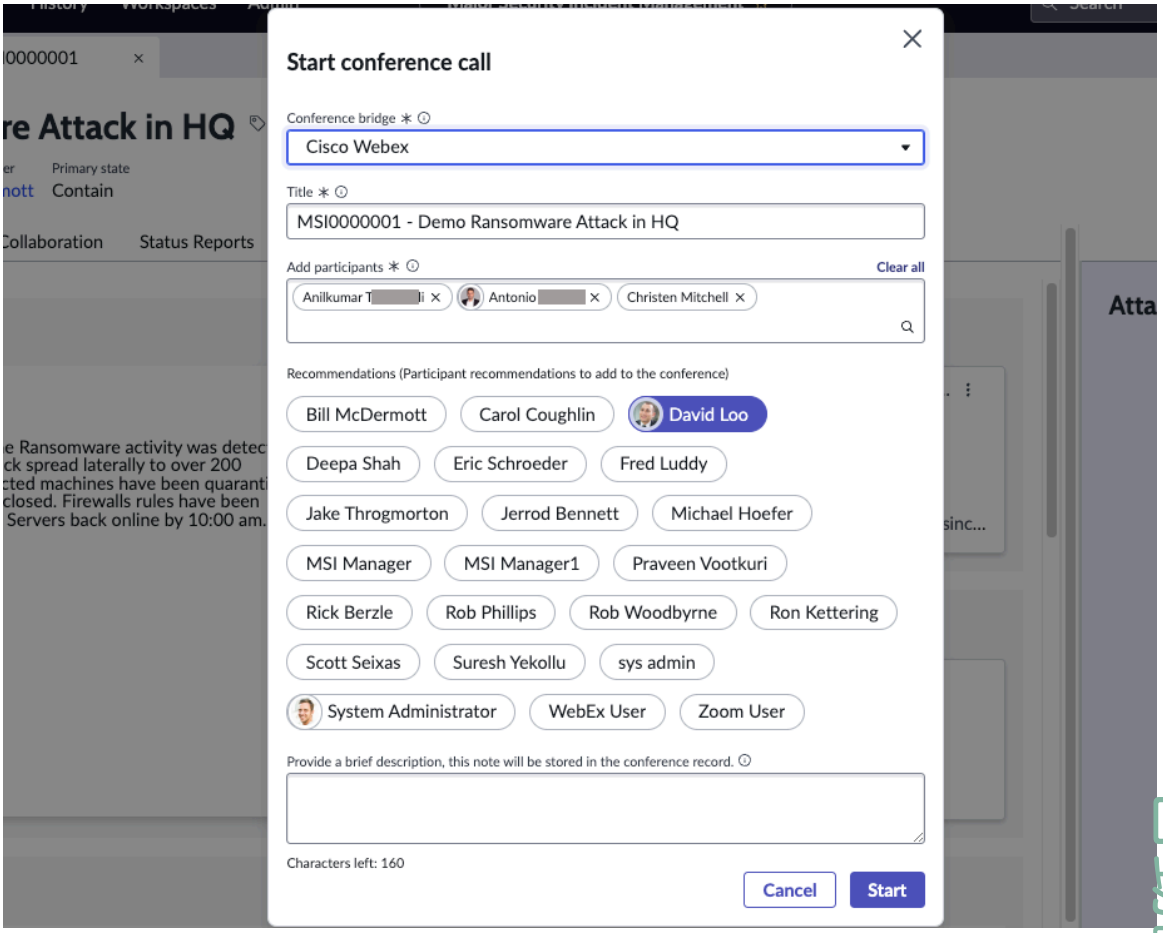
手順

1. 次のように移動する。 ワークスペース > 重大セキュリティインシデント管理.
2. [重大なセキュリティインシデント] リストから、重大なセキュリティインシデントを選択します。
3. Select the **Start a conference call** action.
4. You can also start a conference call by selecting the icon on the right-context menu and selecting the + icon.
   [カンファレンスコールを開始] ポップアップが表示されます。
5. 接続元の会議ブリッジとして **[Cisco Webex]** を選択します。
6. [タイトル] フィールドに、Cisco Webex カンファレンスコールの理由を説明するタイトルを入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

カンファレンスコール **Cisco Webex** 統合の使用



7. [参加者を追加] フィールドで、Cisco Webex カンファレンスコールの参加者を選択します。
検索オプションを使用して必要な参加者を検索して追加することも、[推奨事項] リストから参加者を選択して参加者を追加することもでき、これにより、Cisco Webex カンファレンスコールに追加する参加者の推奨事項が表示されます。

   Cisco Webex カンファレンスコールを開始したユーザー (ホスト) は、選択済み参加者のリストに追加されます。重大なセキュリティインシデントに関連付けられているすべてのユーザーは、デフォルトで [推奨事項] リストに表示されます。

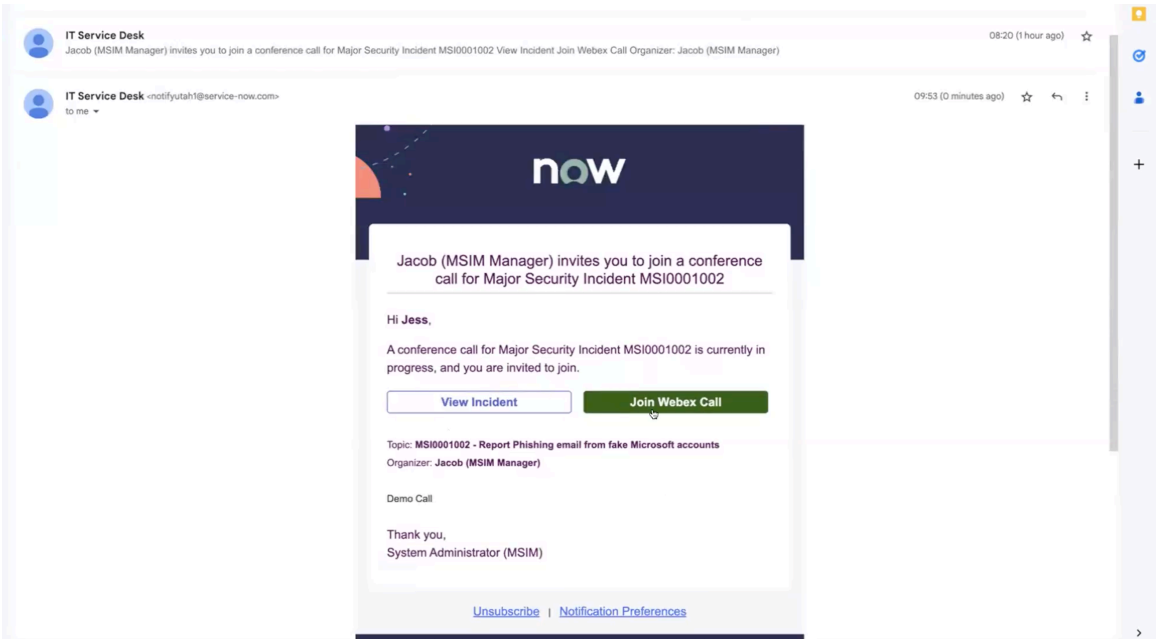
   注:
   選択した参加者が有効なメールアドレスを持っていることを確認してください。

8. 参加者を選択したら、[説明] フィールドにカンファレンスコールを開始する理由についての簡単な説明を入力します。
入力した説明が会議レコードに追加されます。
9. 参加者リストが完成したら、[開始 **(Start)]** を選択します。
カンファレンスコールが Cisco Webex アプリで開始されます。すべての参加者には 2 通のメールで通知されます。1 通のメールは MSIM アプリから参加者に送信され、もう 1 通のメールは Cisco Webex 会議ブリッジから送信されます。
10. 重大なセキュリティインシデントの上部にある [ここをクリック] オプションを選択して、Cisco Webex アプリでカンファレンスコールに参加します。
参加者は、MSIM メール通知からのリンクまたは Cisco Webex アプリからの通知を使用して、コールに参加できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

メール通知



11. MSIM ワークスペースで関連する重大なセキュリティインシデントを開いて、カンファレンスコールの詳細を表示します。

    最後の参加者が会議を退出すると、カンファレンスコールが終了するか、[カンファレンスコール] セクションで [コールを終了] を選択してカンファレンスコールを終了します。

    カンファレンスが記録された場合、しばらくすると、関連する重大なセキュリティインシデントの [カンファレンス] セクションで録音が利用可能になります。

重大セキュリティインシデント管理 の構成

重大セキュリティインシデント管理 アプリケーションをインストールして構成します。

重要:

- 重大セキュリティインシデント管理の構成をすぐに開始するには、ServiceNow Store の「Major Security Incident Management (MSIM) Quick Start Guide (重大セキュリティインシデント管理 (MSIM) クイックスタートガイド)」を参照してください。
- 重大セキュリティインシデント管理アプリをインストールした後、KB1289784 に更新セットをインポートして、部分的に事前設定されたファイルをロードしてください。

このセクションでは、他の外部 Microsoft アプリケーションと統合して ServiceNow インスタンスとの接続を確立することによって、重大セキュリティインシデント レコードを操作するために必要な構成を設定する方法について説明します。

ファイルエクスプローラーコンポーネントの構成

ファイルエクスプローラーワークスペースコンポーネントは、重大なセキュリティインシデントに関連するアーティファクト (ファイル) のコレクションを整理および追跡します。これは、重大セキュリティインシデント管理 ワークスペースで Microsoft SharePoint などのサードパーティのファイルホスティングプロバイダーとの統合をサポートするように設計されています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- File Explorer コンポーネント：ファイルシステムを表示し、ユーザーがファイル操作を実行できるようにするためのグラフィカルユーザーインターフェイスを提供します。
- File Explorer コア：外部リポジトリとの通信に使用される基礎となるコネクタについて知ることなく、ファイルエクスプローラーコンポーネントでファイルシステムを表示し、さまざまなファイル操作を実行できるようにするための抽象化レイヤーを提供します。
- File Explorer Microsoft SharePoint コネクタアプリケーション：Microsoft SharePoint ドキュメントライブラリからファイル/フォルダーのメタデータを追跡およびフェッチし、ファイル操作を実行するために必要な実装モジュールを提供します。

File Explorer コアコンポーネントは、さまざまなファイル共有コネクタアプリケーションが接続プロパティを定義するために必要な基本インフラストラクチャを提供します。

ファイルホスティングプロバイダーの場所からファイルのメタデータをプルするための接続プロパティを追加して、ファイルリポジトリドライブとファイルリポジトリプロバイダーをインストールして構成する必要があります。

File Explorer の現在のバージョンの場合、これらの手順には、Microsoft SharePoint のファイルとフォルダーの更新、ファイル操作、ファイルアクティビティのログ記録など、ファイルメタデータの取得操作の構成と登録が含まれます。重大なセキュリティインシデントに固有の個々のフォルダーを作成するには、指定された Microsoft SharePoint ドキュメントライブラリと関連するドライブ構成が必要です。

File Explorer は Microsoft SharePoint のようなコネクタアプリケーションも使用できます。この例を使用して、次のようなファイル操作の実装を構成できます ダウンロード または 名前の変更 フォルダーとファイルのアクションは、ファイルエクスプローラーワークスペースコンポーネントで有効になります。これらのアクションは、統合された フローデザイナーサブフローを使用して有効化され、実行されます。詳細については、「Folder and File Action Settings (フォルダーとファイルのアクション設定)」を参照してください。

File Explorer 構成には、次のセットアップが含まれます。

- ファイルエクスプローラーのリポジトリドライブの構成
- フォルダーとファイルのアクション設定の構成
- フォルダーテンプレートの作成

ファイルエクスプローラーの使用を開始する

File Explorer コンポーネントの作業を開始する前に、次の情報を確認します。

Microsoft SharePointとの接続を確立し、フォルダーとファイルのアクションを作成し、ファイルエクスプローラーコンポーネントのフォルダーテンプレートを作成する前に、次の情報を確認してください。

必須条件

名前	説明
ServiceNow® IntegrationHub. 用の Microsoft SharePoint スポーク、バージョン 2.0.2	Microsoft SharePoint スポークを検索してインストールするには **sn_sp_spoke** というプラグイン ID を使用します。 このプラグインをインストールすると、コラボレーション、ドキュメント管理、およびユーザーアクセス権限を自動化するフローとアク

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

必須条件 (続く)

名前	説明
	ションが Microsoft SharePoint に提供されます。
ファイルエクスプローラーコンポーネント v1.1.0	ファイルエクスプローラーコンポーネント v1.1.0 を検索してインストールするには、**sn_file_exproller** というプラグイン ID を使用します。 このプラグインをインストールすると、File Explorer Core で利用可能な、ファイルシステムを参照するためのグラフィカルユーザーインターフェイスが提供されます。
File Explorer Core for Security Operations v1.1.1	File Explorer Core を検索してインストールするには、**sn_fe** というプラグイン ID を使用します。 このプラグインをインストールすると、サードパーティのファイルホスティングプロバイダーと統合するための基本インフラストラクチャが提供されます。
Microsoft SharePoint File Explorer Connector for Security Operations v1.1.1	Microsoft SharePoint File Explorer Core を検索してインストールするには、**sn_fe_sharepoint** というプラグイン ID を使用します。 このプラグインをインストールすると、ファイルエクスプローラーを使用する Microsoft SharePoint ファイル/フォルダーが管理されます。

自動翻訳

ファイルエクスプローラーのリポジトリドライブの構成

Microsoft SharePoint コネクタは、ファイルのメタデータを管理および追跡することで Microsoft SharePoint ファイルエクスプローラー機能に実装されるさまざまな機能を提供します。

始める前に

必要なロール：sn_msi.workspace_admin

手順

1. 次のように移動する。 **All** (すべて) > 重大なセキュリティインシデント > ファイルエクスプローラー > ファイルリポジトリ構成.
2. 次の表の説明に従って、次の各フィールドに入力します。

フィールド名	フィールドの説明
名前	使用状況を識別するファイルリポジトリレコードの名前。例：MSIM。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド名	フィールドの説明
プロバイダー	サードパーティのファイルホスティングリポジトリプロバイダーであるプロバイダーの名前。例：Microsoft SharePoint。
プロパティ	
サイト URL パス	特定のサイトパスを含む Microsoft SharePoint URL を入力します。 サイトへの相対パスのみを指定します。完全なサイト URL は必要ない場合があります。例：Sites/MSIM。
ドキュメントライブラリ名	Microsoft SharePoint サイトの下にドキュメントライブラリを作成し、ここで同じドキュメントライブラリ名を指定します。 これは、Microsoft SharePoint コネクタドライブのセットアップで作成したものと同じドキュメントライブラリです。
グラフ接続	[ファイルエクスプローラー] の [グラフ] テナントレコードを選択します。 テナント接続構成の詳細については、「Microsoft SharePoint スポーク」を参照してください。
REST 接続	[ファイルエクスプローラー] の [REST] テナントレコードを選択します。 テナント接続構成の詳細については、「Microsoft SharePoint スポーク」を参照してください。

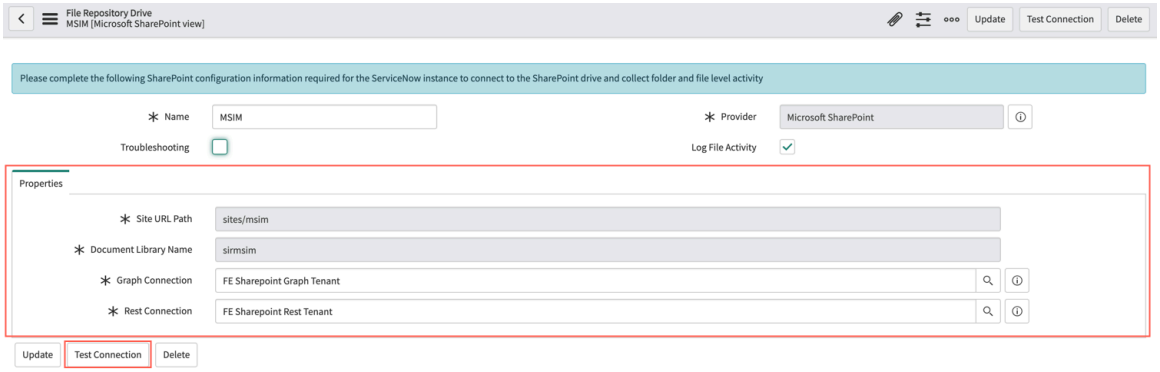
3. **[Save** (保存)] を選択します。
4. クリックします テスト接続 タブで接続をテストし、ファイルリポジトリドライブ構成プロパティを検証します。

   注:
   ファイルリポジトリをアクティブにする前に、Microsoft SharePoint の対応するドキュメントライブラリにフォルダーまたはファイルデータがないことを確認してください。

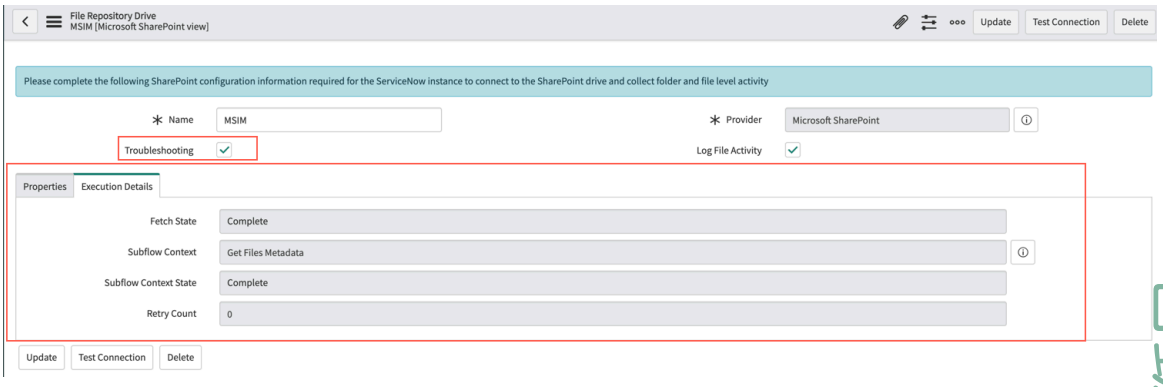
5. [アクティブ化] をクリックして、ファイルリポジトリをアクティブ化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



6. [トラブルシューティング] チェックボックスをオンにして、ファイルリポジトリの [実行の詳細] を確認し、 フェッチステータス が完了し、 Microsoft SharePoint ドライブサブスクリプション が作成され、ステータスが完了していることを確認します。



注:
[テスト接続] ボタンを使用すると、MSI アドミニストレーターまたは MSI マネージャーはファイルリポジトリ構成のみを検証できます。

自動翻訳

フォルダーとファイルのアクション設定の構成

[重大セキュリティインシデント管理] ワークスペースのファイルエクスプローラーコンポーネントから使用できるようにするフォルダーとファイルのアクションを、[フォルダーとファイルのアクション設定] セットアップページを使用して構成します。MSI アドミニストレーターは、ファイルエクスプローラーコンポーネントに表示される個々のフォルダーとファイルのアクションを制御できます。

始める前に

ServiceNow® フローデザイナーを使用して、ファイルエクスプローラーコンポーネントに実装されているファイル操作の機能は次のとおりです。

ファイル操作の機能

ファイル操作	説明
Microsoft SharePoint で開く	新しいブラウザータブを開き、Microsoft SharePoint ドキュメントライブラリファイルビューを表示します。
フォルダーを作成	重大なセキュリティインシデントが作成された後に追加のアドホックフォルダーを作成できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ファイル操作の機能 (続く)

ファイル操作	説明
フォルダーの名前を変更	作成されたフォルダーの名前を変更できます。
ファイルを移動	ワークスペースのファイルエクスプローラーコンポーネント内のフォルダー間でファイルを移動することで、Microsoft SharePoint のファイルを移動できます。
ファイルを検索 (Locate File)	を使用するときにフォルダーの場所を表示します 最近 ファイルエクスプローラーのビュー。
Delete File	ファイルを削除します。
フォルダーを削除	フォルダーを削除します。
ファイルのダウンロード	既存の MSIM ワークスペースブラウザータブ内でファイルをダウンロードして、すばやく表示できます。
ファイルの名前を変更 (Rename File)	ファイルの名前を変更します。

注:

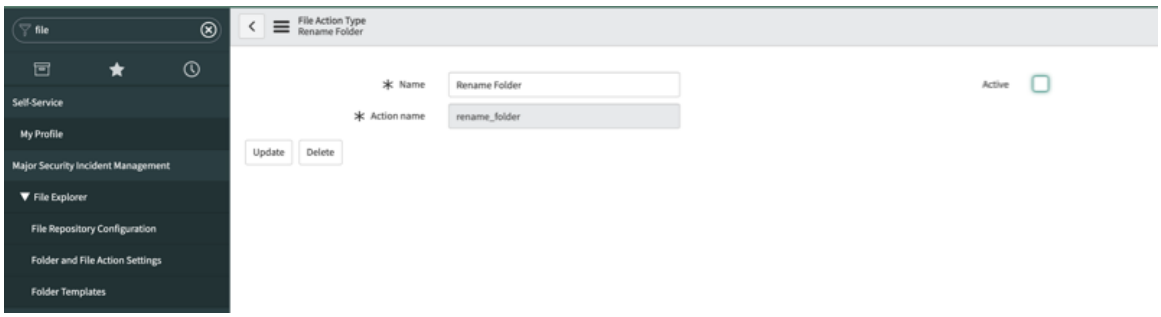
1. リストされているすべてのアクションは、現在デフォルトで有効になっています。次を編集する必要があります: ファイルアクション設定 特定のアクションを表示しない場合。現在、すべての設定はすべてのユーザーに対してグローバルです。これは、特定のロールを持つユーザーのサブセットに対してアクションを有効にすることはできないことを意味します。
2. ユーザーアクセスを取り消す AND 権限を追加 アクションはシステム関連のアクションです。これらのファイルアクションは変更しないことをお勧めします。

次のサンプル手順は、ファイルエクスプローラーリポジトリの構成中に特定のフォルダーとファイルのアクションを無効にするファイル操作機能 の 1 つを示しています。この手順は、編集が必要な可能性がある他のすべてのアクションに適用されます。

必要なロール：sn_msi.workspace_admin

手順

1. 次のように移動する。 重大セキュリティインシデント管理 > ファイルエクスプローラー > フォルダーとファイルのアクション設定.
2. 目的のレコードを選択して、フォルダーまたはファイルのアクションをそれぞれ有効または無効にします。
3. 選択を解除 アクティブ フォルダーとファイルのアクションを無効にするチェックボックス。

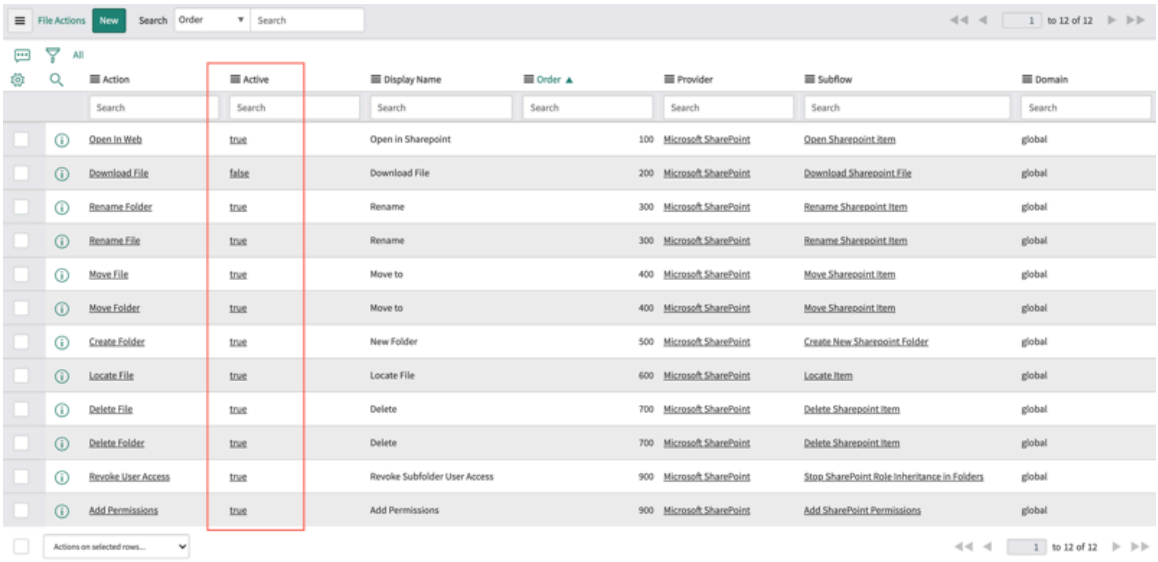


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

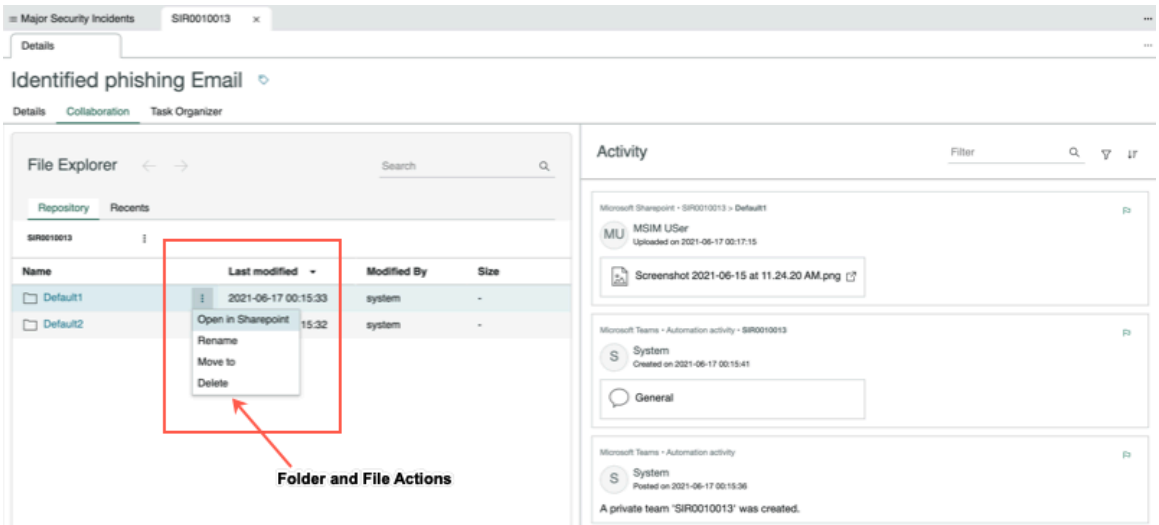
4. ドライブレコードを更新 します。

注:
また、表示されたファイル操作のリストからファイルアクションを直接実行することもできます。 アクティブ 列の値を True または False に設定しま



す。

実行されたファイルアクションが無効になっている場合、アクションは コラボレーション のタブ 重大セキュリティインシデント管理 できるようになります



フォルダーテンプレートの作成

フォルダーテンプレートを使用すると、さまざまな重大なセキュリティインシデントタイプに対して一意のフォルダーを自動的に作成できます。ファイルエクスプローラーコンポーネント内のフォルダーテンプレートは、Microsoft SharePoint 内のセキュリティインシデントのベースフォルダー構造を作成するために使用されます。

始める前に

MSI アドミニストレーターは、さまざまなインシデントレスポンダーグループ間のコラボレーションを可能にするために必要な初期フォルダー構造を定義し、サブフォルダーレベルで適切なアクセス権限をアサインします。特定の 重大セキュリティインシデント フィールド値の条件ビルダーを使用して、さまざまな 重大セキュリティインシデント タイプに対して複数の構成を作成できます。これには、各サブフォルダーレベルでのさまざまなユーザーとユーザーグループへのアクセス許可が含まれます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> これらのフォルダーテンプレートは、条件ビルダーで指定された条件を満たすすべての重大なセキュリティインシデントで使用されます。インシデント番号やカテゴリなどのインシデントフィールド変数を使用して、一意のルートフォルダー名の作成を検討することが推奨されます。一意のルートフォルダー名により、1 つの重大なセキュリティインシデントの共通のフォルダー名を持つ一連のサブフォルダーを、別の重大なセキュリティインシデントの一部であるこれらの名前を持つ類似するフォルダーと区別します。

定義されたフォルダーテンプレート構成は、条件に一致した場合にのみ重大なセキュリティインシデントに適用されます。

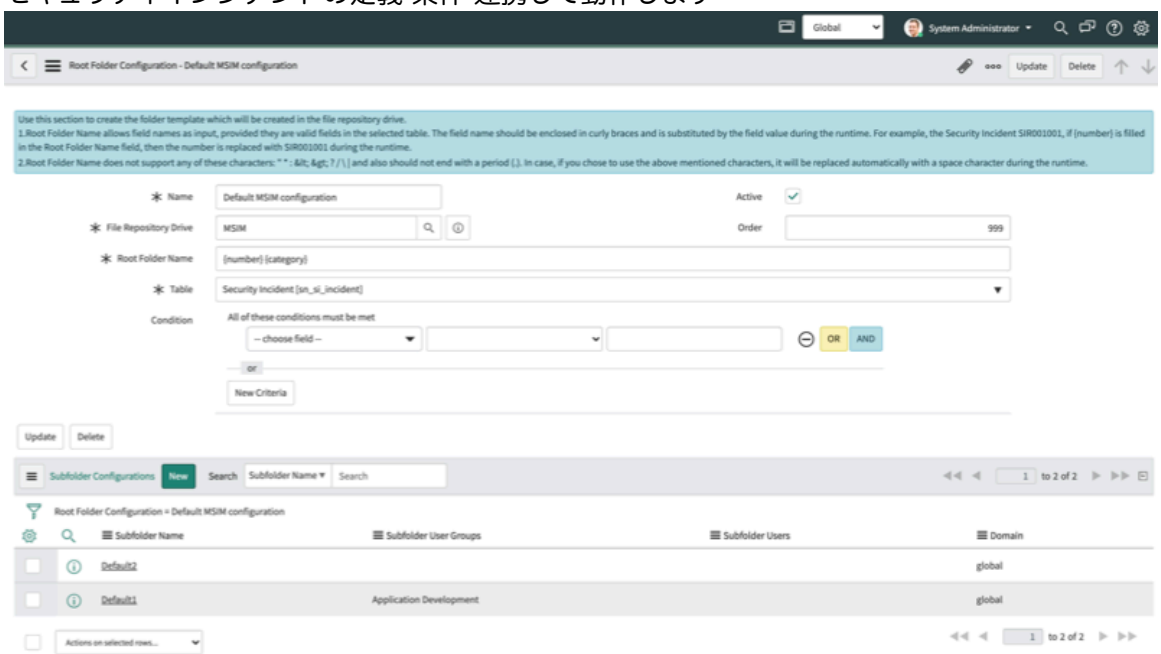
> **注:**
> ベースシステム構成 (サブフォルダーなし) がすべてのセキュリティインシデントに適用されます。このデフォルト構成を編集して特定のサブフォルダーを含めるか、重大なセキュリティインシデントフィールド値の指定されたセットに基づいて新しい構成を作成することができます。例：カテゴリが [悪意のあるコードアクティビティ] である。

必要なロール：sn_msi.workspace_admin

手順

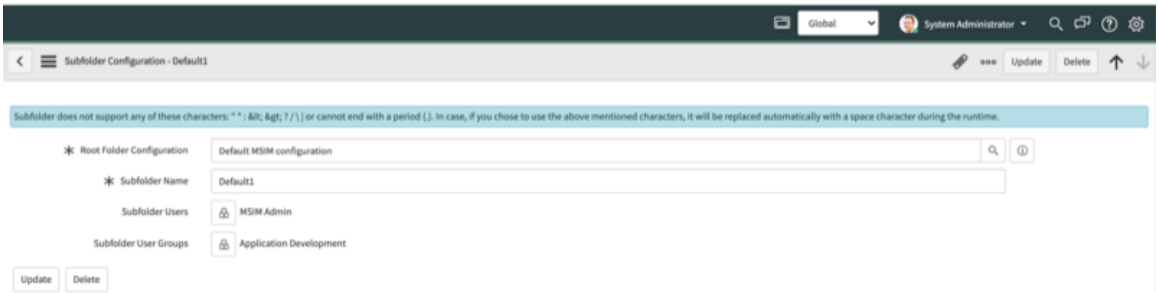
1. 次のように移動する。 **All** (すべて) > 重大セキュリティインシデント管理 > ファイルエクスプローラー > フォルダーテンプレート.
2. クリックします 新規 Root Folder Configuration (ルートフォルダー構成)
3. フォームの各フィールドに入力します。

4. セキュリティインシデントの定義 条件 連携して動作します



5. 更新 します。
   定義された値でサブフォルダーが作成されます。
6. 目的のサブフォルダーをクリックします。
   適切な名前でサブフォルダーを作成しないと、サブフォルダー名は デフォルト の サブフォルダー構成

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



節。

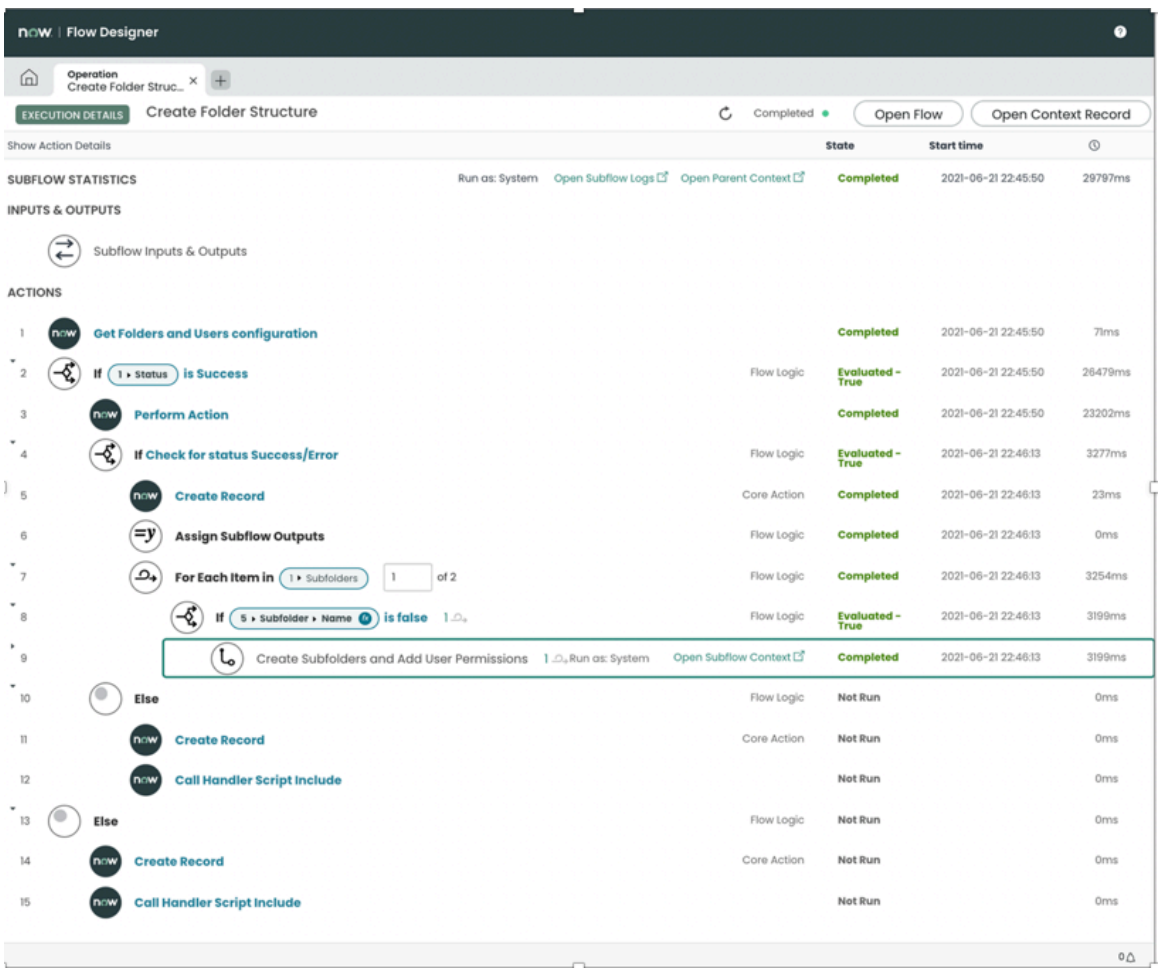
。

で構成されているのと同じアクセス権限を使用して、同じフォルダー構造が Microsoft SharePoint に自動的に作成されます フォルダーテンプレート ページ

注:

- [ルートフォルダー名] では、フィールド変数名を入力にできます (選択したテーブル内の有効なフィールドである場合)。フィールド名は中括弧で囲む必要があり、フロー実行時にフィールド値に置き換えられます。たとえば、セキュリティインシデント SIR001001 があり、[ルートフォルダー名] フィールドで {number} 変数が設定されている場合、number は実行時に SIR001001 に置き換えられます。
- ルートフォルダー名 は、" * : < > ? / \ | の文字をサポートしていません。また、末尾をピリオド (.) にすることもできません。上記の文字を使用すると、実行時に自動的にスペース文字に置き換えられます。
- [ルートフォルダー] と [サブフォルダー] の名前が定義された制限 (256 文字) を超えた場合、フォルダー名は切り捨てられます。

「フォルダー構造を作成」サブフローのランタイム実行は次のとおりです。



自動翻訳

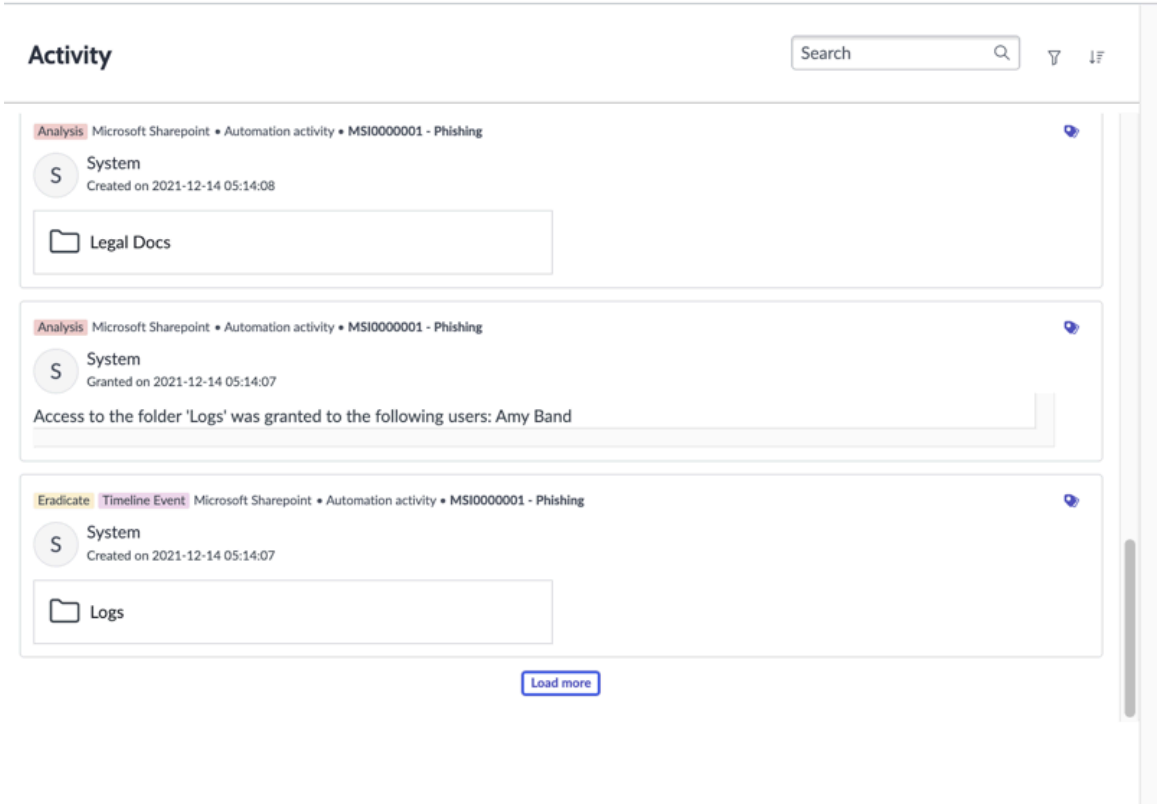
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ワークスペース内での **File Explorer** アクティビティストリーム

重大セキュリティインシデント管理 ワークスペースの [ファイルエクスプローラー] セクションを使用して、Microsoft SharePoint ドキュメントライブラリで作成されたフォルダーとファイルを作成された順に表示します。

重大セキュリティインシデント の解決中にフォルダーとファイルのアクティビティやログが発生するたびに、すべての自動化アクティビティの投稿がアクティビティストリームに一覧表示されます。アクティビティストリームの構造は、作成されたフォルダーと、そのフォルダーにアサインされたユーザーやユーザーグループを示す Microsoft SharePoint ライブラリと同じ形式に揃えられます。

ワークスペースマネージャーと他のユーザーやユーザーグループがアクティビティストリームを使用することで、連絡や共同作業の効率化を図ったり、Microsoft SharePoint フォルダーやファイルで実行されたアクティビティを一覧表示したり、インシデントのステータスを監視したり、インシデントレコードにメモを投稿したり、コメントを追加したりすることが可能になります。ワークスペースマネージャーは最後に更新されたアクティビティをピックアップし、それに基づいて作業できま



す。

File Explorer のトラブルシューティング

トラブルシューティングのセクションは、File Explorer コンポーネントのセットアップ時に発生する可能性のある技術的な問題の解決に役立ちます。

スケジュール済みジョブ、システムのプロパティ、および File Explorerフローデザイナーサブフローの詳細については、次のセクションを参照してください。

File Explorer のスケジュール済みジョブ

スケジュール済みジョブは、Microsoft SharePoint からの通知を処理し、ServiceNow インスタンスにファイルのメタデータを取り込んで、定期的にファイルリポジトリのサブスクリプションを更新するために実行される、自動化されたジョブです。

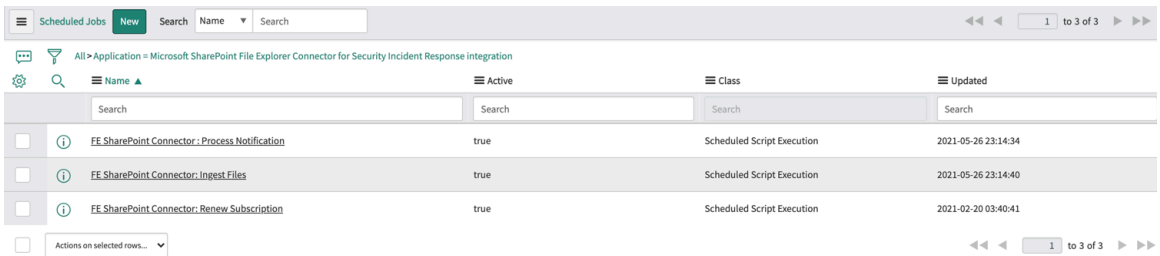
スケジュール済みジョブは、バックグラウンドで次の動作を行う自動化されたジョブです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- Microsoft Microsoft SharePoint からの通知を処理する。
- ファイルのメタデータを Now Platform インスタンスに取り込む。
- 通知を受信するように、Microsoft SharePoint ドキュメントライブラリのサブスクリプションを更新する。

ジョブ	説明
Microsoft SharePoint File Explorer Connector：通知の処理	30 秒ごとに実行され、登録されているドキュメントライブラリで変更が発生したことを示す通知を読み取り、ドライブのステータス (sn_fe_file_repo_drive) を処理待ちとしてマークします。
Microsoft SharePoint File Explorer Connector：ファイルの取り込み	30 秒ごとに実行され、処理待ちステータスのドライブ (sn_fe_file_repo_drive) の処理を主に行い、前回のプル以降に構成された Microsoft SharePoint ドキュメントライブラリからデルタファイルの変更をプルします。
Microsoft SharePoint File Explorer：サブスクリプションの更新	10 分ごとに実行され、有効期限の 1 日前に Microsoft SharePoint ドキュメントライブラリのサブスクリプションを更新します。通常、サブスクリプションは 30 日で期限切れになります。



利用可能なファイルエクスプローラーのシステムプロパティ

Microsoft SharePoint ファイルエクスプローラーで利用可能なコネクタのシステムプロパティは次のとおりです。

システムプロパティ

プロパティ名	説明
sn_fe_sharepoint.max_retry_count	障害が発生したドライブのプルや、失敗したサブスクリプションの更新を、Microsoft SharePoint コネクタアプリケーションが試行する頻度を制御します。頻度のデフォルト値は 50 に設定されています。
sn_fe_sharepoint.retry_after_seconds	障害が発生したドライブのプルまたはサブスクリプションの更新を試行する時間間隔。デフォルト値は 900 秒または 15 分に設定されています。
sn_fe_sharepoint.max_subscription_expiration_time	Microsoft SharePoint のサブスクリプションの最大有効期限 (日数)。デフォルトの有効期限は 30 日に設定されています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

File Explorer フローデザイナーのサブフロー

Microsoft SharePoint File Explorer コネクタと一緒にインストールされるフローデザイナーサブフローは次のとおりです。

サブフロー

名前	説明
Microsoft SharePoint 権限の追加	特定のユーザーに特定のフォルダーの編集権限を付与します。
ドライブサブスクリプションを作成	構成された Microsoft SharePoint ドキュメントライブラリに登録して、ドキュメントライブラリで発生した更新に関する通知を受け取ります。
新しい Microsoft SharePoint フォルダーを作成	所定の親フォルダーの下に新しい Microsoft SharePoint フォルダーを作成します。
Microsoft SharePoint のアイテムを削除	Microsoft SharePoint のファイルとフォルダーを削除します。
Microsoft SharePoint ファイルをダウンロード	Microsoft SharePoint ファイルのダウンロード URL を返します。
ファイルメタデータを取得	Microsoft SharePoint ドキュメントライブラリに登録して変更をプルします。
Microsoft SharePoint のアイテムを移動	Microsoft SharePoint のファイル/フォルダーを移動先フォルダーに移動します。
Microsoft SharePoint のアイテムを開く	ブラウザーで開く Microsoft SharePoint ファイル/フォルダーの Web URL を返します。
ドライブサブスクリプションを更新	Microsoft SharePoint ドキュメントライブラリのサブスクリプションを更新します。
フォルダー構造を作成	フォルダーテンプレート構成に従い、Microsoft SharePoint ドキュメントライブラリにフォルダー構造を作成します。

Microsoft Teams の構成

Microsoft Teams と簡単に統合して連携し、重大セキュリティインシデントを解決して、Collaboration Chat アクティビティを表示してフィルタリングします。

Microsoft Teams チャット環境の構成と登録、指定されたチャネル内からのチャット会話の取得、および Team と関連チャネルのアーカイブが、インシデントクローズプロセスの一部として含まれます。重大セキュリティインシデントに固有の個々のチャネルを作成するには、指定された Microsoft Teams 環境と関連する Microsoft Teams Graph API 構成が必要です。

Microsoft Teams を構成するには、チャットプロバイダーとして Teams をアクティブ化します。これにより、さまざまなステークホルダーやグループがアクティビティについてやり取りするためのチャットチャネルを作成し、チャットの会話を追跡して重大セキュリティインシデントを解決できます。Microsoft Teams および Microsoft Graph API 構成には次のものが含まれます。

- Now Platform での MS Teams Graph 接続の確立
- チャットプロバイダーとしての MS Teams のアクティブ化
- チャットチャネルテンプレートの作成
- チャットメッセージアクティビティの表示

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Microsoft Teams を開始するには

コネクタアプリケーションとしての Microsoft Teams の作業を開始する前に、次の情報を確認します。

Microsoft Teams のセットアップ接続の確立、アクティブ化、および検証を開始する前に、次のプラグインがインストールされていることを確認してください。

必須のプラグイン

名前	説明
Chat integration with Security Incident Management	Microsoft Teams チャットを検索してインストールするには、**sn_chat_collab_core** というプラグイン ID を使用します。 このプラグインをインストールすることで、Microsoft Teams (または Slack その他サードパーティ製チャットアプリケーション) などのサードパーティ製アプリケーションのチャットアクティビティを追跡できます。
Microsoft Teams チャットコネクタのセキュリティインシデント管理統合	Microsoft Teams Chat Connector for Major Security Incident Management を検索してインストールするには、**sn_ms_teams_connector** というプラグイン ID を使用します。 このプラグインをインストールすることで、Microsoft Teams に固有のコラボレーションコンポーネントを使用してチャットアクティビティを追跡できるようになります。
Microsoft Teams Graph スポーク	このプラグインをインストールすると、Microsoft Teamsとの Graph スポーク接続が確立されます。詳細については、「Microsoft Teams Graph Spoke」を参照してください。

チャットプロバイダーとしての MS Teams のアクティブ化

Microsoft Teams 接続を検証して、Microsoft Teams をアクティブ化します。

始める前に

必要なロール：sn_msi.workspace_admin

接続がアクティブ化され、検証されると、プロバイダー接続が正常に検証されたことを示す情報メッセージが表示されます。ユーザーを追加および削除し、場合によってはチャネルを追加したり、既存のチャネルの名前を変更したりして、チャネル構成を変更できます。

手順

1. 次のように移動する。 重大セキュリティインシデント管理 > チャットプロバイダー構成.
2. **[Microsoft Teams** レコード **(Microsoft Teams record)]** を選択します。
3. [接続を検証] をクリックします。
   プロバイダー接続が正常に検証されたことを示す確認メッセージが表示されます。
4. [アクティブ] チェックボックスを選択して、プロバイダーレコードをアクティブ化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロバイダー接続が正常に検証されたことを示す確認メッセージが表示されます。

5. チャットプロバイダー構成をアクティブ化した後、フォームを [保存] します。
これにより、Microsoft Teams と Now Platform インスタンス間の接続が正常に確立されます。

チャットチャネルテンプレートの作成

チャットチームとチャネルテンプレートを構成して、共同作業を行うチャットチームとチャネルを作成し、チャットの会話を追跡し、そのチャットチャネルにユーザーとユーザーグループを追加します。チャネルテンプレートは、重大なセキュリティインシデントが昇格すると Microsoft Teams 内に作成されます。

始める前に
必要なロール：sn_msi.workspace_admin

手順

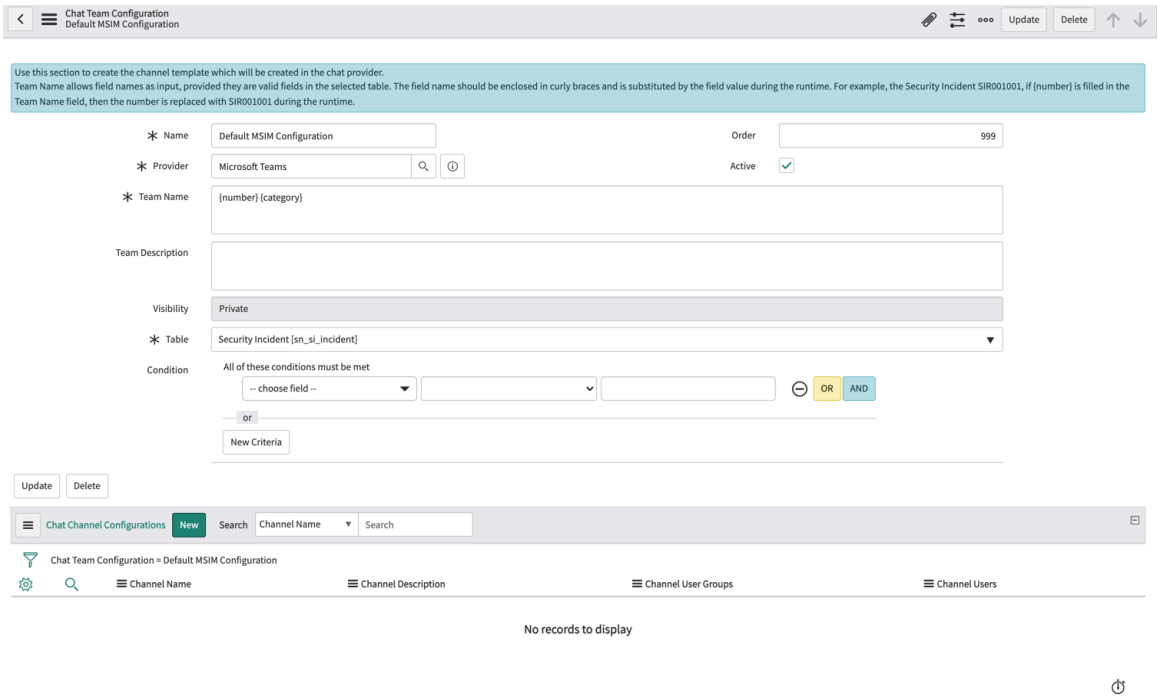
1. 次のように移動する。 重大セキュリティインシデント管理 > チャットチャネル > チャネルテンプレート.
2. [チャットチャネル構成] フォームで、フォームヘッダーの [新規] をクリックします。
3. フォームのフィールドに入力します。

[チャットチーム構成] フォーム

フィールド	説明
名前	フォルダーの名前。
プロバイダー	Microsoft Teams。
チーム名	チームの名前 ({number}-{category} など)。 **注:** ここで指定したチーム名は、重大なセキュリティインシデントのすべてのレコードで使用されます。実際の Microsoft チーム名が MS Teams アプリケーションに表示され、異なる重大なセキュリティインシデントに対してそれぞれ一意の名前の値を持つようにするには、インシデント番号 - {number} などの一意のインシデントフィールド値を使用することをお勧めします。スクリーンショットの例で示すように、{number} の後にセパレーター「-」が続き、Microsoft Teams の作成目的となる重大なセキュリティインシデントの一意の番号と説明 (例：{number} - {category}) が、{category} フィールド変数で示されます。
チームの説明	(オプション) チームの説明。
テーブル	重大なセキュリティインシデント (sn_msi_incident)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [送信] をクリックします。
5. [チャットチャネル構成] セクションに移動します。
6. クリックします 新規 をクリックして、新しいチャットチャネル構成を作成します。
7. 入力 チャットチーム構成 AND チャネル名.

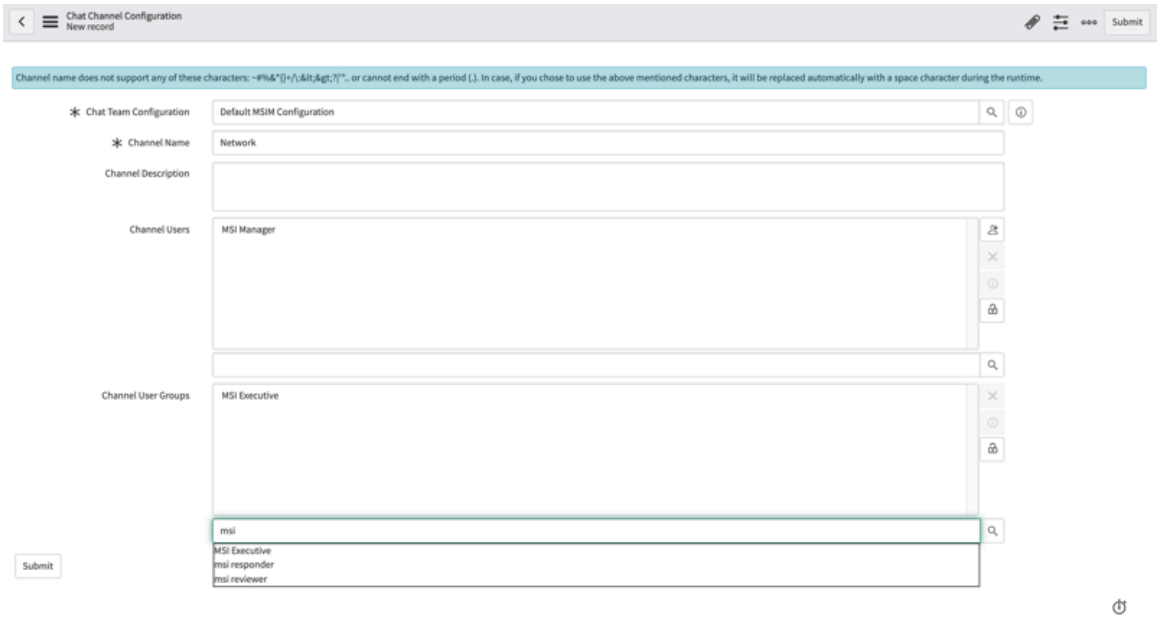
   注:
   ここで作成した新しいチャネルは、Microsoft Teams のチャネル名にもなります。同じチャネルを検索して会話を追加できます。

8. Catalogs List に [チャネルユーザー AND チャネルユーザーグループ 検索リストから

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

9. 送信 新しいチャットチャネル設定レコード。



タスクの結果
これでチャットチャネルが作成され、ユーザーがチャットチャネルグループにアサインされました。コラボレーションチャットアクティビティは、Microsoft Teams と MSIM ワークスペースのコラボレーションアクティビティストリームのいずれでも、チャットチャネルプロバイダー構成で設定された体系的なチャットチャネル階層構造の形式で表示できます。

チャットメッセージアクティビティの表示

チャットメッセージアクティビティは記録され、重大セキュリティインシデント管理ワークスペースの [コラボレーション] タブに表示されます。

チャットメッセージアクティビティには、参加者や異なるユーザーグループ間で発生したすべてのチャット会話が含まれます。

MSIM の **MS Teams** チャットコネクタのトラブルシューティング

スケジュール済みジョブ、システムプロパティ、および Microsoft Teams フローデザイナーのサブフローについては、Microsoft Teams チャットコネクタのトラブルシューティングに関するセクションを参照してください。

コラボレーションチャットメッセージが Microsoft Teams および MSIM ワークスペースの外部コラボレーションアクティビティストリームに投稿されない場合は、チャットコネクタプロセスのスケジュール済みジョブを確認します。

Microsoft Teams のスケジュール済みジョブ

スケジュール済みジョブは、Microsoft Teams Chat Connector からの通知を処理し、繰り返しスケジュールで Microsoft Teams サブスクリプションを更新するために実行される、自動化されたジョブです。

必要なロール：admin

- **MS Teams** チャットコネクタ:通知の処理

  チャットメッセージイベントごとに、テーブルに保存されているリソース ID と通知を含む通知が送信されます。未処理の通知を選択するスケジュールジョブが 30 秒ごとに実行され、Microsoft

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Teams API のクエリを実行して実際のメッセージコンテンツが取得されます。これらのメッセージは、さらに別のテーブルに保存されます。

- **MS Teams Chat Connector:**サブスクリプションを更新

  チーム内のチャネルごとに、作成、更新、および削除されたイベントの通知を取得するサブスクリプションが作成されます。このサブスクリプションは 60 分間のみアクティブです。サブスクリプションは、「Microsoft Teams Connector：通知の更新 (Microsoft Teams Connector: Renew Notification)」スケジュールジョブによって 25 分ごとに更新されます。

Microsoft Teams Chat Connector の機能フロー

このセクションを確認して、重大なセキュリティインシデントからのチャットチャネルの作成とユーザーアクセスを管理するために使用される Microsoft Teams 関連のフローデザイナーサブフローを理解します。

始める前に
必要なロール：sn_msi.workspace_admin

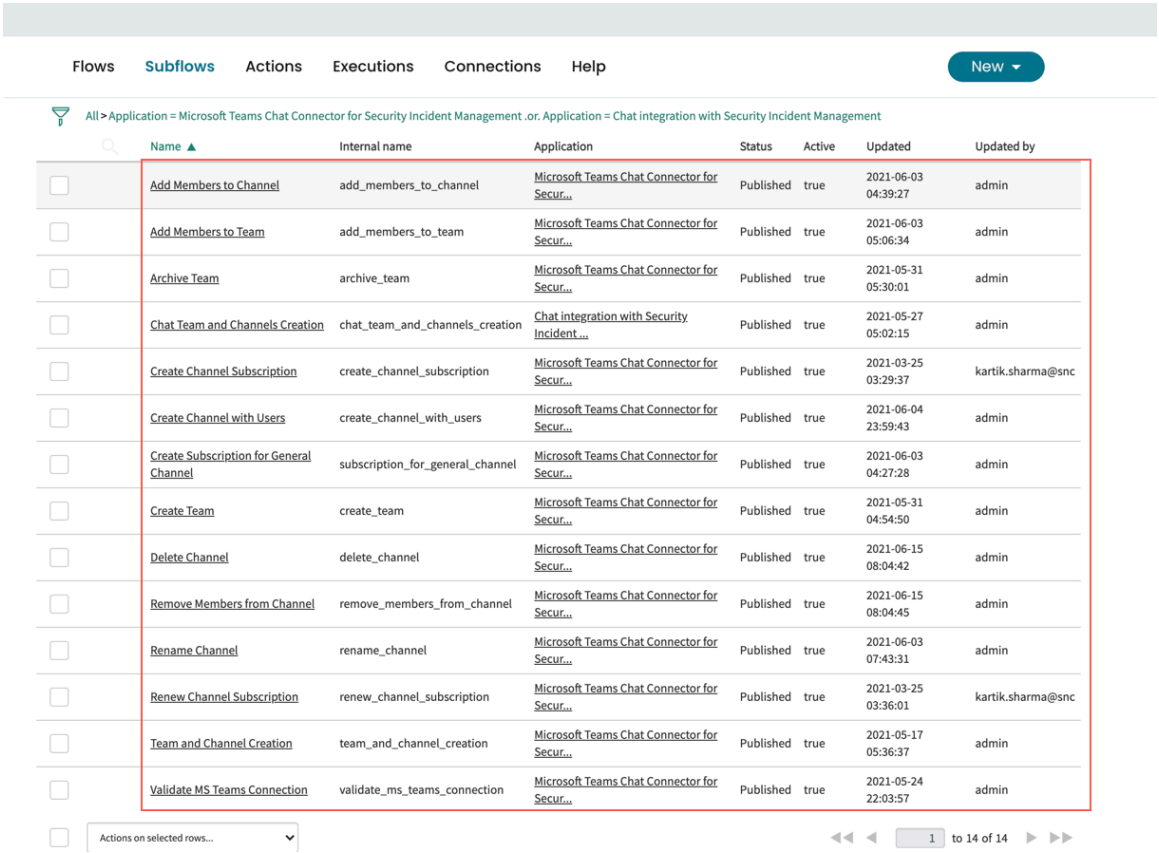
手順

1. 次のように移動する。 **All** (すべて) > **Flow Designer**.
2. チャネルにメンバーを追加
3. チームにメンバーを追加
4. チームをアーカイブ
5. チャットチームとチャネルの作成
6. チャネルのサブスクリプションを作成
7. ユーザーを含むチャネルを作成
8. 一般チャネルのサブスクリプションを作成
9. チームを作成
10. チャネルを削除
11. チャネルからメンバーを削除
12. チャネルの名前を変更
13. チャネルサブスクリプションを更新
14. チームとチャネルの作成

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

15. MS Teams 接続の検証



重大なセキュリティインシデントに対する **Slack** チャットコネクタを構成する

Slack と統合して連携し、重大なセキュリティインシデントを解決して、Collaboration Chat アクティビティを表示およびフィルタリングします。

Slack チャット環境の構成と登録、指定されたチャネル内からのチャット会話の取得、および Slack と関連チャネルのアーカイブが、インシデントクローズプロセスの一部として含まれます。重大セキュリティインシデントに固有の個々のチャネルを作成するには、指定された Slack 環境と関連する Slack API 構成が必要です。

Slack を設定するには、Slack をチャットプロバイダーとしてアクティブ化します。これにより、さまざまなステークホルダーやグループがアクティビティについてやり取りするためのチャットチャネルを作成し、チャットの会話を追跡して重大セキュリティインシデントを解決できます。Slack および Slack の API 構成には次のものが含まれます。

- Slack チャットコネクタ構成の開始
- チャネルプロバイダーとして Slack をアクティブ化する
- Slack のチャットチャネルテンプレートを作成する
- Slack でのチャットメッセージアクティビティの表示

Slack チャットコネクタ構成の開始

コネクタアプリケーションとしての Slack の作業を開始する前に、次の情報を確認します。

Slack のセットアップ接続の確立、アクティブ化、および検証を開始する前に、次のプラグインがインストールされていることを確認してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

必須のプラグイン

名前	説明
セキュリティインシデント管理用の Slack チャットコネクタ	重大セキュリティインシデント管理用の Slack チャットコネクタを検索してインストールするには、**sn_ms_teams_connector** プラグイン ID を使用します。 このプラグインをインストールすることで、Slack に固有のコラボレーションコンポーネントを使用してチャットアクティビティを追跡できるようになります。
Slack スポーク	このプラグインをインストールすると、Slack とのスポーク接続が確立されます。詳細については、「Slack Spoke」を参照してください。

Slack のチャットチャネルテンプレートを作成する

チャットチームとチャネルテンプレートを構成して、共同作業を行うチャットチームとチャネルを作成し、チャットの会話を追跡し、そのチャットチャネルにユーザーとユーザーグループを追加します。チャネルテンプレートは、重大なセキュリティインシデントが昇格すると、Slack 内に作成されます。

始める前に

必要なロール：sn_msi.workspace_admin

このタスクについて

作成した新しいチャネルは、Slack のチャネル名にもなります。同じチャネルを検索して会話を追加できます。

手順

1. 次のように移動する。 **All** (すべて) > 重大セキュリティインシデント管理 > チャットチャネル > チャネルテンプレート.
2. **[Slack** チャネル構成 **(Slack channel configuration)]** を選択して、Slack 構成の詳細を表示します。
3. [アクティブ] チェックボックスをオンにすると、Slack チャットチャネル構成がアクティブ化されます。
4. [チーム名] フィールドに、MSI 番号とコード名を入力します。

   デフォルトでは、すべての Slack チャネルにインシデント番号がプリフィックスとして付きます。たとえば、`MSI000000 - {チャネル名}` ですプリフィックスは、`{field_name}` の形式で任意のフィールドに変更できます。

   > **注:**
   > ここで指定したチーム名は、重大なセキュリティインシデントのすべてのレコードで使用されます。実際の Slack が Slack アプリケーションに表示され、異なる重大なセキュリティインシデントに対してそれぞれ一意の名前の値を持つようにするには、`MSI000000 - {チャネル名}` などの一意のインシデントフィールド値を使用することをお勧めします。

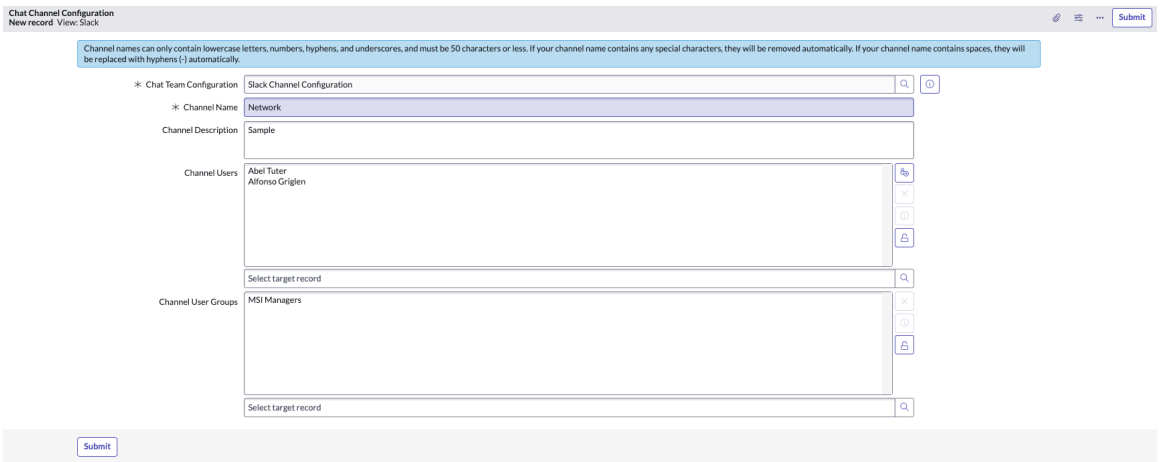
5. 構成を右クリックして、[保存] を選択します。
6. [チャットチャネル構成] セクションに移動します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. 選択 新規 をクリックして、新しいチャットチャネル構成を作成します。
8. フォームの各フィールドに入力します。

Slack チャットチャネル構成



9. [送信] を選択します。

タスクの結果

これでチャットチャネルが作成され、ユーザーがチャットチャネルグループにアサインされました。コラボレーションチャットアクティビティは、Slack と MSIM ワークスペースのコラボレーションアクティビティストリームのいずれでも、チャットチャネルプロバイダー構成で設定された体系的なチャットチャネル階層構造の形式で表示できます。

チャネルプロバイダーとして **Slack** をアクティブ化する

Slack 接続を検証して、Slack をアクティブ化します。

始める前に

必要なロール：

- sn_msi.workspace_admin - 書き込み
- sn_msi.chat_collab_provider - 読み取り

接続がアクティブ化され、検証されると、プロバイダー接続が正常に検証されたことを示す情報メッセージが表示されます。ユーザーを追加および削除し、場合によってはチャネルを追加したり、既存のチャネルの名前を変更したりして、チャネル構成を変更できます。

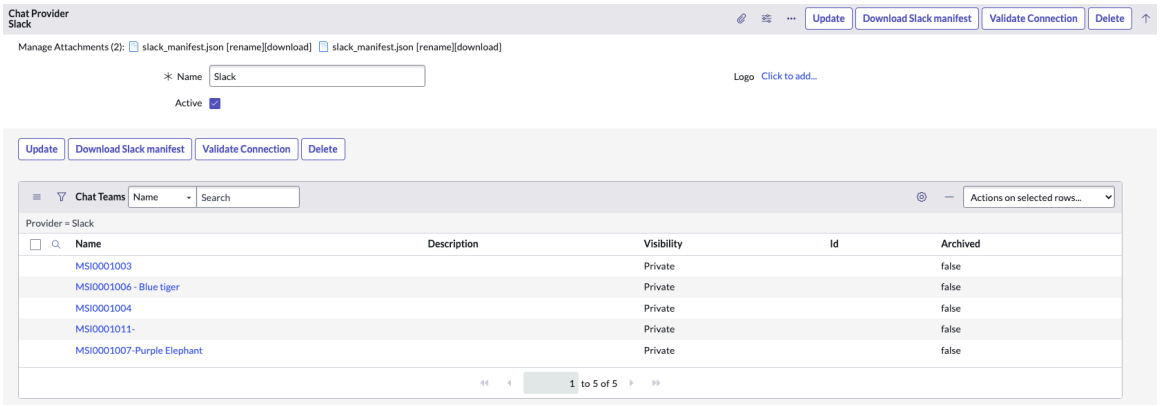
手順

1. 次のように移動する。 **All** (すべて) > 重大セキュリティインシデント管理 > チャットチャネル > チャットプロバイダー構成.
2. **[Slack]** を選択して、Slack チャットプロバイダー構成を開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Slack チャットプロバイダー構成



3. **[Slack** マニフェストをダウンロード **(Download Slack manifest)]** を選択して、slack_manifest.json ファイルをダウンロードします。
   slack_manifest.json ファイルには、Slack セットアップの完全な構成が含まれており、Slack を自動的に構成することができます。この JSON ファイルを Slack 構成にアップロードする必要があります。
4. slack_manifest.json ファイルを開き、次の手順を実行します。
   a. Web ブラウザーで URL api.slack.com/apps に移動します。
   b. [新しいアプリを作成 **(Create New App)]** アクションを選択します。
   c. [アプリを作成] ポップアップで、[アプリマニフェストから **(From an app manifest)]** オプションを選択します。
   d. [アプリを開発するワークスペースを選択 (Pick a workspace to develop your app)] ポップアップで、リストからワークスペースを選択し、[次へ] を選択します。
   例：MSIM Slack ワークスペース。
   e. [以下のアプリマニフェストを入力 (Enter app manifest below)] ポップアップで、**[JSON]** タブを選択し、slack_manifest.json ファイルからコードをコピーして貼り付けます。
   f. [次へ] を選択します。
   g. [概要を確認してアプリを作成 (Review summary & create your app)] ポップアップで、[作成] を選択します。
   これでアプリが作成されました。
   h. [基本情報] ページで、[ワークスペースにインストール **(Install to Workspace)]** を選択します。
   Slack 統合ボットは、MSIM Slack ワークスペースにアクセスする権限を要求します。
   i. [許可] を選択します。
   j. [アプリの資格情報] セクションで、ServiceNow インスタンスに戻って詳細を入力します。
   k. 選択 **All** (すべて) > **Slack** 構成.
   このアクションには sn_msi.workspace_admin ロールが必要です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

l. [署名シークレット] プロパティを選択します。

m. 署名シークレットをコピーして、Slack の [アプリの資格情報] セクションに貼り付けます。

n. ServiceNow インスタンスで、 **All** (すべて) > **Flow Designer**.

o. 次のように移動する。 接続 > **Slack** > 詳細を表示する > 構成.

p. フォームの各フィールドに入力します。

フィールド	説明
接続名	この接続の名前。例：Slack。
接続 URL	この接続の URL。例：https://slack.com
認証情報名	認証情報の名前。例：Slack 認証情報。
OAuth 名	OAuth の名前。例：Slack OAuth。
OAuth クライアント ID	Slack で作成したアカウントに生成されたクライアント ID。
OAuth クライアントシークレット	Slack で作成したアカウントのクライアントシークレット。
OAuth リダイレクト URL	OAuth リダイレクトインスタンス名。 例：msimslack.service-now.com/oauth_redirect.do

q. **[OAuth** トークンを設定して取得] を選択します。
Slack 統合ボットは、MSIM Slack ワークスペースにアクセスする権限を要求します。

r. [許可] を選択します。
OAuth アクセストークンが利用可能で、<YYYY-MM-DD> <HH:MM:SS> に有効期限が切れます。

5. 次のように移動する。 **All** (すべて) > 重大セキュリティインシデント管理 > チャットチャネル > チャットプロバイダー構成.
6. [アクティブ] チェックボックスを選択して、チャットプロバイダーレコードをアクティブ化します。
7. [接続を検証 **(Validate Connection)]** を選択して、接続をテストします。
プロバイダー接続が正常に検証されたことを示す確認メッセージが表示されます。
8. レコードを右クリックして、[保存] を選択します。
その後、Slack と Now Platform インスタンス間の接続が正常に確立されます。
9. 次のように移動する。 **api.slack.com/apps** > 機能 > **OAuth** と権限.

a. すべてのスコープが正しいかどうかを確認します。

b. 次のように移動する。 機能 > イベントサブスクリプション.

c. [要求 URL] フィールドで、[再試行] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

確認済みのメッセージが表示されます。

d. [保存] を選択します。

Slack でのチャットメッセージアクティビティの表示

チャットメッセージアクティビティは記録され、重大セキュリティインシデント管理ワークスペースの [コラボレーション] タブに表示されます。

始める前に
必要なロール：sn_msi.workspace_admin

このタスクについて
チャットメッセージアクティビティには、参加者や異なるユーザーグループ間で発生したすべてのチャット会話が含まれます。詳細については、「Slack を使用してチャットチャネルの通信を管理する」を参照してください。

重大セキュリティインシデント管理 管理

重大セキュリティインシデント管理 の実装を計画し構成します。

重大セキュリティインシデント管理 の管理機能を、次の点から構成できます。

重大なセキュリティインシデントの提案、昇格、およびリンクの有効化

インシデントを重大なセキュリティインシデントとして提案または昇格することをユーザーが決定できるようにします。セキュリティインシデントを親または子インシデントにリンクできるようにすることで、重大なセキュリティインシデントに関連するすべてのインシデントを簡単に追跡できます。

始める前に
必要なロール：sn_msi.workspace_admin

手順

1. 次のように移動する。 **All** (すべて) > 重大セキュリティインシデント管理 > **MSI** 管理 > 構成.
2. [SIR/VR ワークスペースアクション (SIR/VR Workspace Actions)] セクションの [重大なセキュリティインシデントを提案] チェックボックスをオンにして、ユーザーがセキュリティインシデントを重大なセキュリティインシデントに提案できるようにします。
3. [重大なセキュリティインシデントに昇格] チェックボックスをオンにして、ユーザーがセキュリティインシデントを重大なセキュリティインシデントに昇格できるようにします。
4. [重大なセキュリティインシデントへのリンク] チェックボックスをオンにして、重大なセキュリティインシデントへのセキュリティインシデントのリンクを可能にし、まとめて追跡できるようにします。
5. [更新] を選択します。

セキュリティインシデントを重大なセキュリティインシデントとしてタグ付けする

インシデントの提案または昇格時に、セキュリティインシデントまたは脆弱なレコードを重大なセキュリティインシデントとしてタグ付けまたはラベル付けします。セキュリティインシデントが提案されると、そのインシデントレコードは重大なセキュリティインシデント候補と呼ばれます。セキュリティインシデントが昇格されると、そのインシデントレコードは、ステータスが「承認済み」の重大なセキュリティインシデントと呼ばれます。

始める前に
必要なロール：sn_msi.workspace_admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 重大セキュリティインシデント管理 > **MSI** 管理 > 構成.
2. [ラベル名：候補として提案] ルックアップフィールドを選択することで、[ラベルの表示] チェックボックスを有効にして提案されたインシデント候補に重大なセキュリティインシデントのラベルを付けて、**[SIR/VR** ワークスペースラベル **(SIR/VR Workspace Labels)]** セクションで [重大なセキュリティインシデント候補] を選択します。
3. [ラベル名 **-** 重大なセキュリティインシデントに昇格] ルックアップフィールドを選択することで、[ラベルの表示] チェックボックスを有効にして昇格されたインシデント候補に重大なセキュリティインシデントのラベルを付けて、**[SIR/VR** ワークスペースラベル **(SIR/VR Workspace Labels)]** セクションで [重大なセキュリティインシデント] を選択します。
4. [更新] を選択します。

重大なセキュリティインシデントのラベルの設定

重大なセキュリティインシデント管理のラベルを設定して、カスタムラベルを作成し、アクティビティストリームの外部コラボレーションアクティビティとタスクをフィルタリングします。実装されているラベルのタイプは、ステータスラベルとタイムラインラベルです。

始める前に
必要なロール：sn_msi.workspace_admin

手順

1. 次のように移動する。 **All** (すべて) > 重大セキュリティインシデント管理 > **MSI** 管理 > 構成.
2. [ラベルの表示] チェック ボックスを有効にすると、**[MSIM** ワークスペースラベル (コラボレーションアクティビティおよびタスクの表示) **(MSIM Workspace Labels (Display on Collaboration Activities and Tasks))]** セクションで、分析、封じ込め、除去、復旧、レビュー、タイムラインイベントなどのさまざまなインシデント状況にラベルを付けることができます。
3. [更新] を選択します。

重大なセキュリティインシデントのラベルの設定

より適切にフィルタリングを行ってインシデント状況を示すための、さまざまなタイプのラベルを設定します。重大なセキュリティインシデントのラベルを使用すると、インシデントレコードのコラボレーションアクティビティとタスクに柔軟性をもってラベルを付けることができます。

始める前に
必要なロール：sn_msi.workspace_admin

ラベルの選択および選択解除は、MSIM ワークスペースの [コラボレーション] および [タスクオーガナイザー] セクションの [アクティビティストリーム] セクションで使用可能なラベルアイコンを使用して行うことができます。

手順

1. 次のように移動する。 **All** (すべて) > 重大セキュリティインシデント管理 > **MSI** 管理 > **MSI** ラベル.
2. [新規] をクリックして新しいラベルを作成します。
3. フォームに [ラベル名] と [ラベルの色] を入力します。
4. [ラベルを作成] をクリックします。
5. ベースシステムの一部として、各インシデント状況に対して設定されているラベルは次のとおりです。ラベルの名前や色を変更することはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 分析
- 封じ込め
- 根絶
- レビュー
- 復旧
- タイムラインイベント

> **注:**
> カスタムのラベルとそのプロパティは変更可能です。

重大なセキュリティインシデントのタイムラインカテゴリを設定する

[概要] タブの [タイムライン] セクションを使用して、脅威、対応、カスタムなどのタイムラインカテゴリを設定し、重大なセキュリティインシデントにアサインします。

始める前に

必要なロール：sn_msi.workspace_admin

手順

1. 次のように移動する。 **All** (すべて) > 重大セキュリティインシデント管理 > **MSI** 管理 > タイムラインカテゴリ.
   ベースシステムの一部として、次のタイムラインが提供されます。
   - カスタム。
   - 応答。
   - 脅威。
2. 既存のタイムラインイベントカテゴリを変更するには、次の手順を実行します。
   a. リストからタイムラインイベントカテゴリを選択します。
   b. タイムラインイベントカテゴリの名前を変更できます。
   c. イベントの色を変更したり、タイムラインイベントカテゴリに別の色を選択したりできます。
   d. [更新] を選択します。
3. 新しいタイムラインイベントカテゴリを作成するには、次の手順を実行します。
   a. [新規] を選択します。
   b. [名前] フィールドで、タイムラインイベントカテゴリの名前を入力します。
   c. [イベントの色] フィールドで、ドロップダウンリストを使用してイベントタイムラインカテゴリの色を選択します。
   d. [送信] を選択します。

MSIM の通知設定

セキュリティインシデントが重大なセキュリティインシデント候補として提案または昇格されたときのメール通知プロセスを自動化してユーザーに通知します。

必要なロール：sn_msi.workspace_admin

通知は、セキュリティインシデントが提案されたときにのみトリガーされ、通知リストに設定されているすべてのユーザーとグループに送信されます。デフォルトでは、メール通知は、セキュリティインシデントを重大なセキュリティインシデント候補として提案したユーザーに送信されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

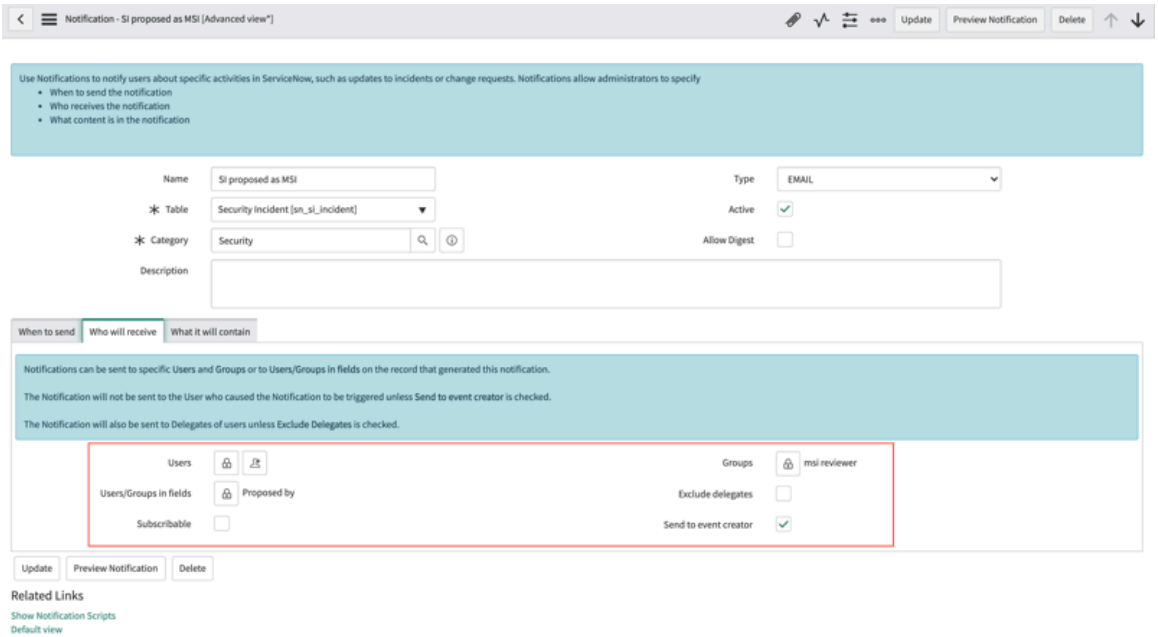
通知:重大なセキュリティインシデント **(MSI)** として提案されたセキュリティインシデント **(SI)**

受信者：

- デフォルトでは、 **MSI** レビュー担当者 グループ名が作成され、このグループに追加されたすべてのユーザーに、 **MSIM** マネージャー そのグループのユーザーは通知メールを受信します。
- に追加されている特定のユーザー ユーザー リストにも通知メールが送信されます。

内容：

メールの本文などのメールコンテンツ (件名やメッセージ HTML を含む) を変更する場合は、システムアドミニストレーターロールアクセス権を持っているか、または MSI アドミニストレーターではなくシステムアドミニストレーターとしてアサインされている必要があります。



通知:重大なセキュリティインシデント **(MSI)** として昇格されたセキュリティインシデント **(SI)**

この通知は、セキュリティインシデントが昇格されたとき、およびファイルエクスプローラーと Microsoft Teams 基本構造が作成されたときにトリガーされます。デフォルトでは、この通知は、セキュリティインシデントを重大なセキュリティインシデントに昇格したユーザーに送信されます。

受信者

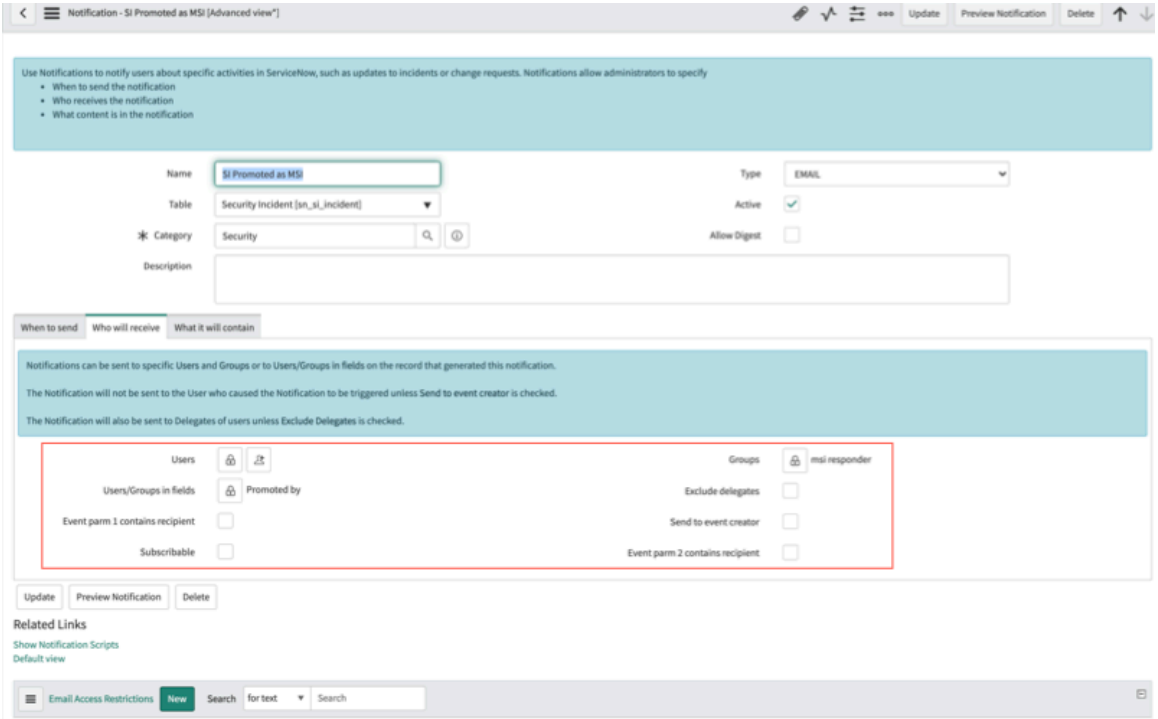
- デフォルトでは、 グループ 名前別 **MSI** レスポンダー が作成され、このグループに追加されたすべてのユーザーに、 **MSIM** レスポンダー ロールとそのグループのすべてのユーザーに通知メールが送信されます。
- に追加されている特定のユーザー ユーザー リストにも通知メールが送信されます。

内容

メールの本文などのメールコンテンツ (件名やメッセージ HTML を含む) を変更する場合は、システムアドミニストレーターロールアクセス権を持っているか、または MSI アドミニストレーターではなくシステムアドミニストレーターとしてアサインされている必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



MSI クローズのアクティビティの設定

重大なセキュリティインシデントがクローズされたときに自動的に発生するアクションを設定します。解決情報を含むフォルダーへのアクセスを自動的にアーカイブして削除することで、セキュリティを強化します。

始める前に
必要なロール：sn_msi.workspace_admin

手順

1. 次のように移動する。 **All** (すべて) > 重大セキュリティインシデント管理 > **MSI** 管理 > 構成.
2. [自動クローズアクション (Automated Closure Actions)] セクションの [コラボレーションチャネルのアーカイブ] チェックボックスをオンにして、インシデントの解決に関連するチャットのやり取りをアーカイブします。
3. [コラボレーションフォルダーを削除 **(Remove Collaboration Folders)**] チェックボックスをオンにして、インシデントの解決に関連する資料を含むフォルダーを削除します。
4. [更新] を選択します。

重大セキュリティインシデント管理 ワークスペース

重大セキュリティインシデント管理 には、重大セキュリティインシデント マネージャーに特化して設計された、重大なセキュリティインシデントの管理専用のワークスペースがあります。

ファイルやフォルダーの共有と表示、インシデントタスクの確認と更新、専用のチャットチャネルを介したインシデントに関する作業者とのコミュニケーションを行うことで、重大なセキュリティインシデントの解決に役立つアクティビティの共同作業を簡単に行うことができます。

重大セキュリティインシデント管理 (MSIM) は、重大なセキュリティインシデントを追跡して解決するメカニズムです。セキュリティインシデントや脆弱性に対応する既存の製品の機能と連携して機能し、重大なセキュリティインシデントの修復プロセスを次の機能によって改善します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 重大なセキュリティインシデントマネージャーのユーザーロールに特化して設計された、重大なセキュリティインシデントを管理する専用のワークスペース。
- 重大なセキュリティインシデント応答タスク (リンクされたセキュリティインシデントおよび脆弱性グループで追跡されるタスクなど) を整理する。
- 重大なセキュリティインシデントが作成された後、コラボレーションフォルダーとチャットコミュニケーションチャネルの作成を自動化し、インシデント終了時にアーカイブを作成する。
- Microsoft SharePoint の統合を介して、重大なセキュリティインシデントに関連するアーティファクト (ファイル) のコレクションを整理して追跡するためのファイルエクスプローラーコンポーネント。
- Microsoft Teams の統合を介して、複数のセキュリティ、IT、機能グループ間のコミュニケーションを管理するためのチャットチャネルマネージャーとアクティビティストリームコンポーネント。
- 影響を受ける資産、ユーザー、場所、およびチームリソースのロールアップや、インシデントの重要なマイルストーンのタイムラインを含む、重大なセキュリティインシデントの影響度と進行状況のメトリクスのサマリーのレポート。

MSIM のワークスペースを使用して、重大なセキュリティインシデントを次の手順で追跡および解決します。

1. 重大なセキュリティインシデントの傾向図と進行状況を表示します。
2. MSIM のワークスペースで、Microsoft SharePoint ファイルのアクティビティを追跡および整理します。
3. MSIM のワークスペースで、Microsoft Teams のチャットのアクティビティを追跡および整理します。
4. MSIM ワークスペースで、インシデントの詳細を確認および更新します。
5. MSIM ワークスペースのアクティビティストリームのコラボレーションアクティビティをフィルタリングします。

重大セキュリティインシデント管理 の使用

マネージャーは、 重大セキュリティインシデント管理 ワークスペースを使用して、提案、昇格、リンク、および却下されたインシデントレコードを表示し、関連するアクティビティを追跡できます。

インシデントレコードの提案、昇格、およびリンク

インシデントが組織に対する重大な脅威として識別された場合は、セキュリティインシデントを重大なセキュリティインシデントとして提案するか昇格させます。

重大セキュリティインシデント管理を ServiceNow インスタンスにインストールすると、セキュリティインシデントから重大なインシデントへの移行を次のように処理できます。

- レビュープロセスを開始するために、セキュリティインシデントを重大なセキュリティインシデント候補として提案する。
- レビュープロセスなしで、セキュリティインシデントを重大なセキュリティインシデントに昇格させる。
- 重大なセキュリティインシデントとして提案されたセキュリティインシデントを却下する。

また、セキュリティインシデントを子インシデントとして重大なセキュリティインシデントにリンクして、すべての関連するセキュリティインシデントを一緒に追跡できるようにすることもできます。

重大セキュリティインシデント として提案する

重大なセキュリティインシデントにセキュリティインシデントを提案します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > セキュリティインシデント > **Lists** (リスト).
2. 重大なセキュリティインシデントとして提案する、関連カテゴリ内のセキュリティインシデントを選択します。
3. [その他のアクション] アイコンを選択し、[重大なセキュリティインシデントとして提案 **(Propose as Major Security Incident)]** を選択します。
4. [重大なセキュリティインシデントとして提案 (Propose as Major Security Incident)] ダイアログボックスで、フィールドに入力します。
   a. 検出日：重大なセキュリティインシデントが最初に作成または提案された日付。
   b. 理由：インシデントを提案する理由を入力します。
   c. 潜在的な影響：インシデントの影響を指定します。
5. [提案] を選択します。

タスクの結果
インシデントが提案され、次のアクションが発生します。

- セキュリティインシデントレコードで、検証バナーメッセージが表示され、定義された重大なセキュリティインシデントのタグが表示されます。
- インシデントレコードの [重大なセキュリティインシデント] 関連リストにレコードが [提案済み] ステータスで表示され、MSIM ワークスペースの [候補] リストにも表示されます。
- MSIM ワークスペースの [アクティビティ] セクションに、セキュリティインシデントが重大なセキュリティインシデントとして昇格されるように提案されたことが表示されます。
- インシデントレコードへのリンクとインシデントの [詳細] タブを含むメッセージが、定義された通知リストに送信されます。

重大セキュリティインシデント への昇格

重大セキュリティインシデント管理 (MSIM) ワークスペースを使用して、セキュリティインシデントを重大なセキュリティインシデントに昇格させたり、昇格された提案を却下したりします。

始める前に
必要なロール：sn_msi.workspace_admin

手順

1. 次のように移動する。 ワークスペース > セキュリティインシデントレスポンスワークスペース > セキュリティインシデント > **Lists** (リスト).
2. 重大なセキュリティインシデントとして昇格する、関連カテゴリ内のセキュリティインシデントを選択します。
   [詳細] セクションでセキュリティインシデントの詳細を確認するか、[詳細を表示] をクリックして別のタブでインシデントレコードの詳細を表示します。
3. [その他のアクション] アイコンを選択し、[重大なセキュリティインシデントに昇格] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [重大なセキュリティインシデントの昇格 (Promote Major Security Incident)] ダイアログボックスで、フィールドに入力します。

   a. 検出日：重大なセキュリティインシデントが最初に作成または提案された日付。

   b. 推定解決日：重大なセキュリティインシデントが解決されると推定される日付。

   c. コード名：重大なセキュリティインシデントのコード名を選択します。
   例：Blue Tiger。

   d. カテゴリ：重大なセキュリティインシデントのカテゴリを選択します。
   例：構成ミス。

   e. 理由：インシデントを提案する理由を入力します。

   f. 潜在的な影響：インシデントの影響を指定します。

5. [提案] を選択します。
6. セキュリティインシデントを昇格するか、昇格提案を却下します。
   - インシデントを昇格するには、[重大なセキュリティインシデントに昇格] をクリックします。
   - 昇格提案を却下するには、[重大なセキュリティインシデントを却下] をクリックします。
7. [保存] を選択します。

タスクの結果

- 昇格提案を却下した場合、インシデントは昇格されず、インシデントのエントリは [却下] タブに移動します。
- インシデントを昇格させた場合、インシデントエントリは [オープン] タブに移動し、重大なセキュリティインシデントであることを示すタグがセキュリティレコードに表示されます。
- この決定は、MSIM ワークスペースの [アクティビティ] セクションに一覧表示されます。

インシデントが昇格されると、デフォルトの構成が適用されます。

- フォルダーテンプレートの構成に基づいてフォルダー構造が作成されます。
- チャネル構成に基づいてチャットチャネルが作成されます。
- 指定されたユーザーにメールメッセージが送信されます。デフォルトの通知には、重大なセキュリティインシデントへのリンクとインシデントの詳細が記載されています。指定されたユーザーはコラボレーションリソースにもアクセスできるようになります。そのため通知には、Microsoft チーム名と、インシデントに関連する Microsoft SharePoint フォルダーへのリンクも記載されます。

重大セキュリティインシデント へのリンク

セキュリティインシデントを重大なセキュリティインシデントにリンクさせます。

始める前に

必要なロール：sn_msi.workspace_admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデント > すべてのインシデントを表示.
2. 重大なセキュリティインシデントにリンクする、関連カテゴリ内のセキュリティインシデントを選択します。
3. [他のアクション] アイコンを選択し、[重大なセキュリティインシデントへのリンク] を選択します。
4. リンクする重大なセキュリティインシデントを選択します。
   a. ダイアログボックスで、[リストから参照] アイコンを選択します。
   b. リンク先の重大なセキュリティインシデントを選択します。
   c. **[OK]** を選択します。
5. [提案] を選択します。

タスクの結果
提案が送信され、次のアクションが発生します。

- セキュリティインシデントレコードで、検証バナーメッセージが表示され、定義された重大なセキュリティインシデントのタグが [セキュリティタグを選択] フィールドの横に表示されます。
- 両方のインシデントが、重大セキュリティインシデント管理 の重大なセキュリティインシデントの [詳細] タブにあるレコード番号のドロップダウンリストに入っています。
- インシデントレコードの [重大なセキュリティインシデント] 関連リストに、レコードが [提案済み] ステータスで表示されます。
- インシデントレコードへのリンクとインシデントの [詳細] タブを含むメッセージが、定義された通知リストに送信されます。
- MSIM ワークスペースの [アクティビティ] セクションに、セキュリティインシデントが子セキュリティインシデントとして重大なセキュリティインシデントにリンク付きで追加されていることが表示されます。

MSIM ワークスペースでの **MSI** リストビューの使用

MSIM ワークスペースのリストビューでは、提案、昇格、却下された重大なセキュリティインシデントを表示できます。

始める前に
必要なロール：sn_msi.workspace_manager

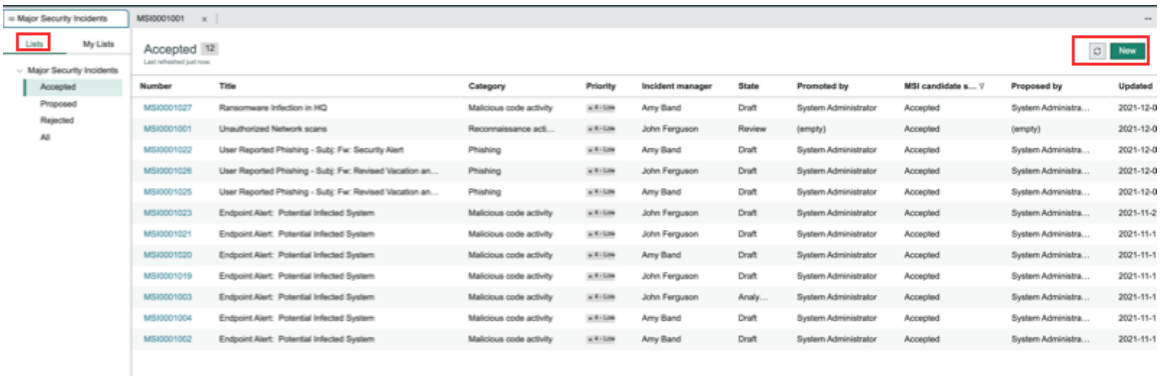
ワークスペースの右上隅にある [新規] ボタンを使用して、新しいインシデントを作成することもできます。

手順

1. 次のように移動する。 重大セキュリティインシデント管理 > **MSIM** ワークスペース.
2. [リスト] タブを選択して [リスト] ビューを表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳



3. [自分のリスト] を選択して、重大なセキュリティインシデントの独自のリストを作成します。
4. リストビューから実行できる操作については、次の表を参照してください。

タスク	説明
自分のリスト	新しい MSI レコードリストを作成し、作成したリストを表示します。
リストの列のフィルターを設定する	列を選択し、縦ドットメニューを展開すると、列のデータをさらにフィルタリングするオプションが表示されます。
アイテムを除外する、または列内の行のアイテムと一致させる	列のセルを選択し、次のいずれかを選択して表示されるデータを絞り込みます。 ○ この値で絞り込み：列内の選択したアイテムに一致するアイテムのみを表示します。 ○ 除外：それぞれの列で選択したアイテムに一致する列のアイテムを除外します。
リストを更新	リストを更新し、更新された完全なリストを表示します。
新規	新しい MSI レコードを作成します。

重大セキュリティインシデント の影響のメトリクスの表示

重大なセキュリティインシデントの影響度と進行状況に関する最新のサマリーレポートを提供します。これは、新しいワークスペースを使用した重大なセキュリティインシデントの管理における重要な作業となります。

[概要] タブには、影響を受ける資産、ユーザー、場所、およびチームリソースのロールアップなど、インシデントの範囲と進行状況を管理するための対応する影響度メトリクスのほか、重大なインシデントのマイルストーンのタイムラインが表示されます。

タイムラインには、特定の重大なセキュリティインシデントの解決の一環で発生した主要なイベントとマイルストーンの水平ビューが示されます。タイムラインコンポーネントは、すべての重大セキュリティインシデント管理ワークスペースのタブの上部に表示され、必要に応じて折りたたんだり展開したりすることができます。指定されたマイルストーンイベントやマイルストーンが追加または更新されるたびに、表示されるイベントデータが更新されます。

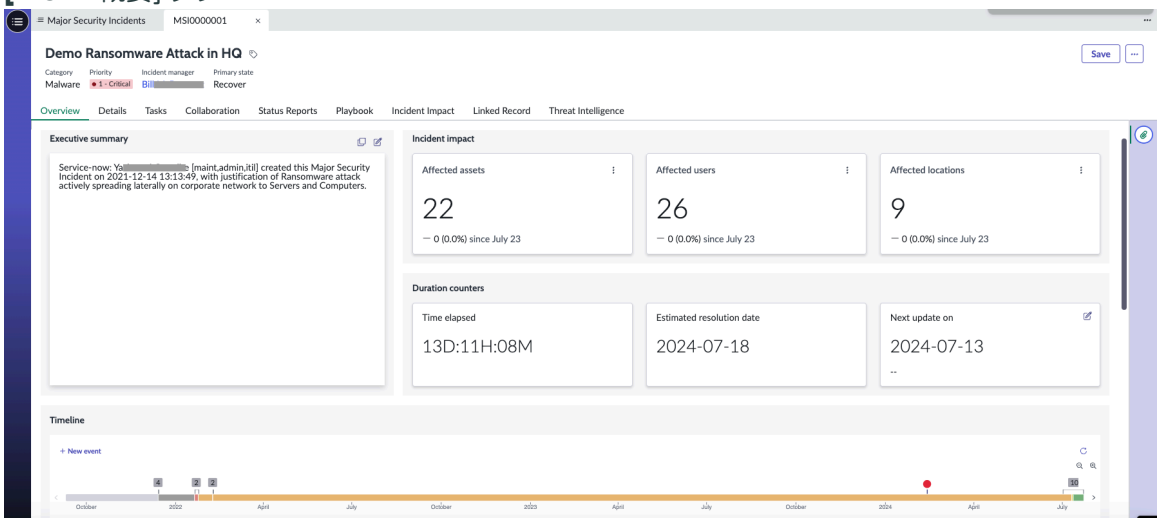
イベントやマイルストーンがそれぞれ異なるタイムラインイベントタイプオプションで示され、それによってイベントやマイルストーンの数とタイプを識別できます。たとえば、NOW レコードの更新やコラボレーションアクティビティなどです。さらに、重大なセキュリティインシデント状況の期間

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

が別個に自動的に追跡され、各インシデント状況の期間と一緒に、範囲ごとに色分けされて表示されます。

[MSIM 概要] タブ



エグゼクティブサマリーとインシデントの影響度

タスク	説明
エグゼクティブ サマリー	重大なセキュリティインシデントの簡単なサマリーをはじめ、ユーザー名、ユーザーロール、タイムスタンプの詳細。 • [編集] アイコンを選択すると、[エグゼクティブサマリー] を変更できます。必要な変更を行った後、[更新] オプションを選択します。 • エグゼクティブサマリーをコピーして重大セキュリティインシデントにペーストするには、[コピー] アイコンを選択して、必要な重大セキュリティインシデントにサマリーをペーストします。
インシデントの影響度	これらの各コンポーネントは、すべてのアクティブなタスクのロールアップと、特定された資産、ユーザー、場所、およびアサインされたチームメンバーにリンクされたインシデントに基づいて、影響を受けるリソースを表示します。影響を受けるリソースは次のとおりです。 • 影響を受ける資産 • 影響を受けるユーザー • 影響を受ける場所 数値を選択すると、影響を受ける資産、ユーザー、場所の詳細にドリルダウンして移動できるようになります。移動すると、ワークスペースの [インシデントの影響度] タブに関連タスクが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エグゼクティブサマリーとインシデントの影響度 (続く)

タスク	説明
	選択したインシデントの影響度のタイプのリンクに基づいて、タスクタイプとその説明、アサイン先グループ、インシデント状況などの関連インシデントの詳細が インシデントの影響度 MSIM ワークスペースのタブ。
期間カウンター	これらのコンポーネントには、重大セキュリティインシデントの期間が表示されます。影響を受けるリソースは次のとおりです。 • 経過時間：重大なセキュリティインシデントが検出されてからの経過時間が表示されます。 • 推定解決日：重大なセキュリティインシデントが解決されると推定される日付が表示されます。 • 次の更新日：重大なセキュリティインシデントを解決するための次回の更新日時。例：2024 年 3 月 25 日午後 5:00 (東部標準時)。 [編集] アイコンを選択すると、次の更新日を変更できます。新しい日付と時刻を選択し、[更新] を選択します。

フィルター切り替えボタンを使用して、タイムラインインジケーターとタイムライン範囲の両方に対して特定のイベントタイプの表示を有効または無効にすることができます。

タイムライン

タイムラインコンポーネントで利用可能なその他の機能については、以下の表を参照してください。

タイムラインコンポーネントのその他の機能

タスク	説明
新しいイベント	新しいカスタムイベントを作成し、そのイベントを MSI レコードに関連付けます。この機能は、タイムラインにデフォルトで表示されるラベル付きのタスク、レコードステータスの変更、またはラベル付きのコラボレーションアクティビティを介してでないと取得できない、過去と未来の日付のイベントを作成するのに役に立ちます。
リフレッシュ	タイムラインイベントを更新して、最新の更新を表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タイムラインコンポーネントのその他の機能 (続く)

タスク	説明
タイムラインインジケーター	[Now レコード (Now Record)] フィールドの変更や、ラベル付きコラボレーションアクティビティ (Labelled Collaboration Activities)、その他 (カスタム) などのさまざまなタイプのイベントが、各イベントタイプインジケーターについて発生したイベントの合計数およびアイコンとともに一覧表示されます。 スライドインジケーターを使用して、特定のイベントタイプのすべてのイベントを有効または無効にすることができます。
凡例を表示	選択すると、凡例がドロップダウンで表示され、さまざまなタイプのタイムラインインジケーターが示されます。
[タイムライン] 進行状況バー	インシデントの全体的な進行状況を、タイムラインに表示されるさまざまな範囲内で発生した、指定のタイムラインイベントまたはマイルストーンで表示します。 イベントタイプとイベントカテゴリをリンクさせることもできます。リンクさせると、両方においてタイムライン上でのイベントの詳細が更新されます。
タイムライン範囲	重大なセキュリティインシデントのライフサイクル全体を通じたインシデントの進行に伴う、さまざまなインシデントのステータスタイプと期間を表示します。 インシデントのステータスに基づいて、特定のイベントを有効または無効にします。

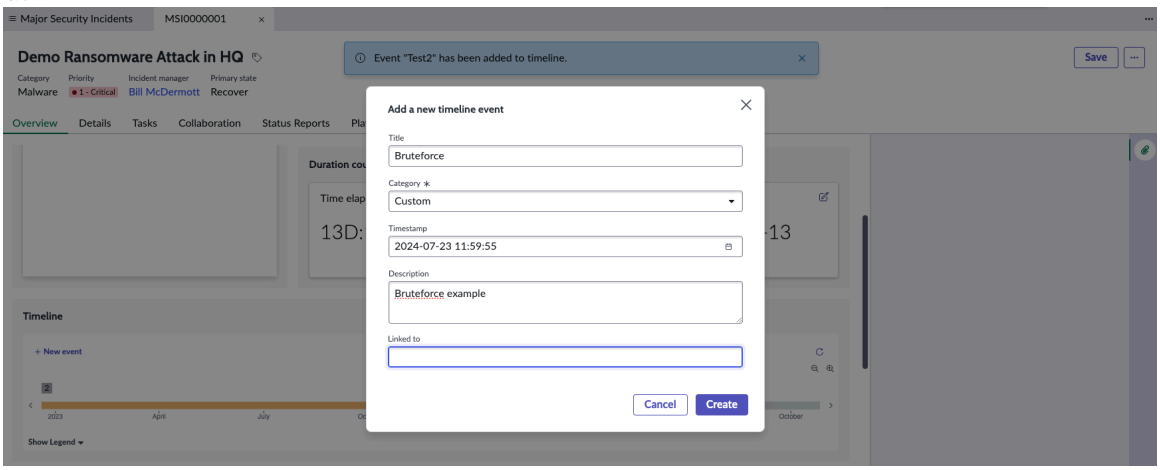
自動翻訳

タイムラインイベントを作成

新しいタイムラインイベントを作成するには、次の手順を実行します。

1. [概要] タブで、[タイムライン] セクションに移動します。
2. 選択 + 新しいイベント.
3. [新規タイムラインイベントを追加] ポップアップのフィールドを入力します。

新規タイムラインイベント



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスク	説明
タイトル	タイムラインイベントのタイトルを入力します。
カテゴリ	タイムラインイベントのカテゴリを選択します。 次のカテゴリはベースシステムの一環として提供され、要件に応じて選択することができます。 ○ カスタム。 ○ 応答。 ○ 脅威。 タイムラインイベントカテゴリの追加や構成については、「重大なセキュリティインシデントのタイムラインカテゴリを設定する」を参照してください。
タイムスタンプ	タイムスタンプカレンダーを使用して、タイムラインイベントの日時を選択します。開始日前後のタイムラインにイベントを追加することができます。
説明	タイムラインイベントに関する簡単な説明を入力します。
リンク先	タイムラインイベントを重大セキュリティインシデントレコードにリンクさせるオプション。

4. 選択 作成/挿入.
5. [ズームイン] および [ズームアウト] アイコンでタイムラインの進行状況バーを拡大または縮小できます。直近のいくつかのイベントを表す数字が表示される場合は、個々のイベントも表示されます。

   デフォルトのズームレベルを追加して、すべてのイベントを表示することもできます。
6. [リフレッシュ] アイコンを選択して、最新のタイムラインイベントを表示します。

重大セキュリティインシデント の傾向図の確認

棒グラフとチャートで可視化された重大なセキュリティインシデントの影響度の進行状況のメトリクスを表示します。

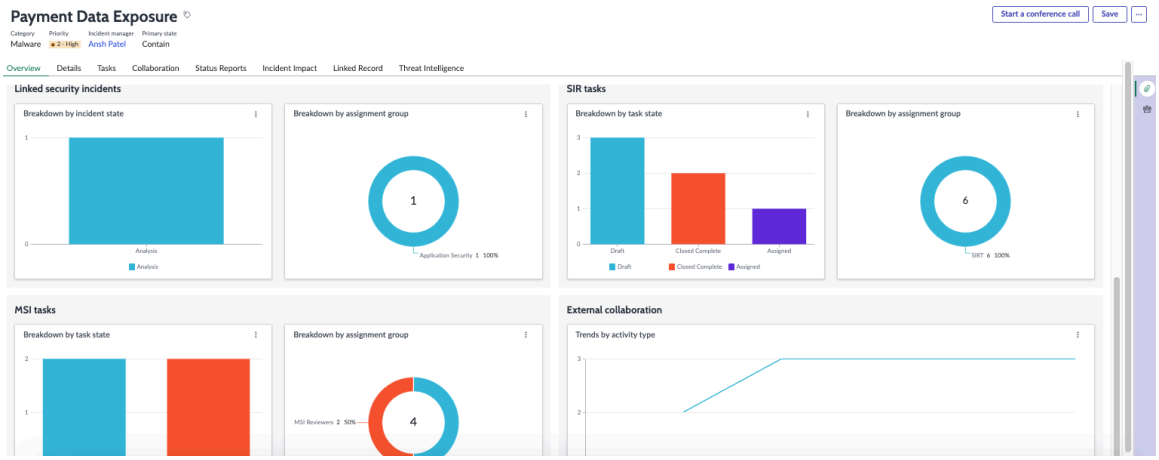
インシデントのタイムラインと進捗の傾向チャートによる可視化に加えて、 概要 タブには、影響を受ける資産、ユーザー、場所、およびチームリソースのロールアップなど、インシデントの変化する範囲を管理するための関連する影響度メトリクスが表示されます。

可視化コンポーネントに表示される数は、リンクされたセキュリティインシデントレスポンス (SIR) のインシデントのアクティブなタスクに基づいて決まります。タスクがオープンまたはクローズされると、重大なセキュリティインシデントに対して計画されている残りのアクティビティの性質と量に従ってこの数が変化し、傾向図の可視化コンポーネントに傾向が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[MSIM の概要] タブの影響度メトリクス



から実行できる UI アクションについては、次の表を参照してください 概要] セクション：

[概要] の各 **UI** セクション

タイトル	説明
時間	重大なセキュリティインシデントがアクティブになってからの期間が合計日数で表示されます。 時間は、 検出日 に入力されました 詳細 ワークスペースのタブ。 [検出日] は多くの場合、重大なセキュリティインシデントが最初に作成または提案されたときに最初にキャプチャされます。この日付が変更されるたびに、時間が自動的に計算されて更新され、「日: 時間: 分」の形式で表示されます (例：20D: 13H: 58M)。 推定解決日:インシデントが解決されると推定される日付。この日付は多くの場合、重大なセキュリティインシデントが最初に作成または昇格されたときに最初にキャプチャされます。 日付は、で指定された推定日付に基づいて更新されます。 詳細 ワークスペースのタブ。 [詳細] セクションに予定日が指定されていない場合、このセクションには日付の値なしでハイフンが表示されます。
アクティブチーム	重大なセキュリティインシデントおよび関連タスクに積極的に取り組んでいるさまざまな応答チームと各チームのメンバーを表示します。 アクティブチーム 傾向:重大なセキュリティインシデントおよび関連タスクに定期的に積極的に取り組んでいる各チームとそのチームメンバーの傾向図を表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[概要] の各 **UI** セクション (続く)

タイトル	説明
	注: からアサインされたアクティブなグループを表示する 詳細 ワークスペースのタブ。
リンクされた **SIR** インシデント	インシデントステータス別:分析、封じ込め、除去、復旧、レビューなどのインシデントステータスに基づいて、リンクされたセキュリティインシデントの分布を表示します。 インシデントステータス別の傾向:インシデントのステータスに基づいて、リンクされたインシデントの数の進行状況の傾向ビューを詳細に示します。 各インシデント状況リンクを選択すると、リンクされたセキュリティインシデントの詳細を リンクされた **SI/VI** ワークスペースのタブ。 このセクションは、基礎的なインシデントに変更が発生するたびに自動的に更新されます。
SIR タスク	SIR インシデントを介して MSI レコードにリンクされているアクティブなタスクの合計を表示します。 • タスクステータス別:インシデント応答タスクを、[ドラフト]、[アサイン済み]、[対応中]、[完了してクローズ] などのインシデントステータスに基づいて表示します。この分布図では、アサイン先グループ別に、さらに細かく分布を分類できます。各タスクステータスを選択すると、インシデントタスクステータス別にフィルタリングされたリストを表示できます。 タスク ワークスペースのタブ。フィルタリングされたビューで、個々のタスクの詳細を表示および更新できます。 • インシデントステータスラベル別の対応中タスク:タスクオーガナイザーコンポーネントで適用する必要があるインシデントステータスラベルに基づいて、アクティブなタスクとグループを表示します。デフォルトのラベルには、関連するタスクの性質を示す、[分析]、[封じ込め]、[除去]、[復旧]、[レビュー] などの値があります。 • 期限切れ:期日を過ぎたアクティブなセキュリティインシデントレスポンスタスクを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[概要] の各 **UI** セクション (続く)

タイトル	説明
	すべての期限切れタスクの詳細を表示するには、[期限切れ] の合計数を選択します。すると、[タスク] タブに自動的に移動します。 • タスクステータス別の傾向:インシデント期間にわたる対応中タスクとクローズ済み応答タスクの両方の進捗傾向を表示します。 **注:** 傾向図のグラフは、スケジュール済みジョブに基づいて最新のデータを取得します。必要に応じて、データ取得の時間間隔を設定または変更できます。
MSI タスク	MSI レコードで直接作成されたアクティブなタスク (リンクされた応答タスクではない) を、次のようにまとめて表示します。 タスクステータス別: 重大なセキュリティインシデントで作成されたタスク、アサイン済みタスク、およびその関連情報を表示します。 各タスクステータスを選択すると、インシデントタスクステータス別にフィルタリングされたリストを表示できます。 タスク ワークスペースのタブ。フィルタリングされたビューで、個々のタスクの詳細の表示および更新が可能になります。
外部コラボレーション	コラボレーションアクティビティストリームのすべてのラベル付きコラボレーションアクティビティを、次のようにまとめて表示します。 • インシデントステータスラベル別:Microsoft TeamsおよびMicrosoft SharePointのファイルとフォルダーで調整され、ワークスペースの [コラボレーション] タブから [分析]、[封じ込め]、[除去]、[復旧] などのインシデントステータスラベルを使用してラベル付けされたインシデントコラボレーションアクティビティデータを表示します。 • アクティビティタイプ別の傾向:インシデント期間中の Microsoft Teams および Microsoft SharePoint のファイルとフォルダーのアクティビティの数の傾向グラフを表示します。

重大セキュリティインシデント の詳細の更新

インシデントレコードの詳細、アクティブなチームの参加者、対応するアクティビティログなど、重大なセキュリティインシデントに関連する特定の詳細情報を表示および更新します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

重大なセキュリティインシデントの詳細な関連情報はすべて、ワークスペースの [詳細] タブのフォームの各セクションに表示されます。このタブでは、インシデントレコードの詳細、アクティブなチームの参加者、対応するアクティビティログなどの詳細情報を表示します。リンクされた SIR インシデント、脆弱性グループのレコードの詳細、およびすべてのリンクされたインシデントレコードへのアクティビティの投稿をブロードキャストする機能も表示されます。

[詳細] タブには主に次の情報が記載されます。

1. [重大なセキュリティインシデント] フォームのフィールドとインシデント関連の UI セクション。
2. アクティビティストリーム

次の表で、[重大なセキュリティインシデント] フォームの各フィールドの詳細について説明します。

[重大なセキュリティインシデント] フォームのセクション

フィールド	説明
インシデント	
番号	重大なセキュリティインシデントのレコード番号。
プライマリステータス	重大なセキュリティインシデントレコードのプライマリステータス。
検出日	重大なセキュリティインシデントが最初に作成または提案された日付。 [詳細] タブで [検出日] を変更するたびに、MSI の日時が自動的に計算されて更新され、 時間 > インシデントが開始されてからの時間 ワークスペースの [概要] セクションのセクション。
Title (役職)	重大なセキュリティインシデントのタイトル。
コード名	重大なセキュリティインシデントのコード名。例：Blue Tiger。
次の更新日	重大セキュリティインシデントを解決するための次回の更新日時。例：2024 年 3 月 25 日午後 5:00 (東部標準時)。
カテゴリ	重大なセキュリティインシデントのカテゴリ。
サブカテゴリ	重大なセキュリティインシデントのサブカテゴリタイプ。
推定解決日	インシデントの解決予定日。デフォルト値は、重大なセキュリティインシデントの作成時点から 7 日です。
優先度	重大なセキュリティインシデントの優先度。
アラートセンサー	重大なセキュリティインシデントのアラートセンサー。たとえば、「ユーザーから報告されたフィッシング」などです。
ソース	重大なセキュリティインシデントのソース。
アクティブチーム	
インシデントマネージャー	インシデントマネージャーの名前。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[重大なセキュリティインシデント] フォームのセクション (続く)

フィールド	説明
アサイン先グループ	重大なセキュリティインシデントに積極的に取り組んでいるさまざまな応答チームと各チームのチームメンバーを示します。
候補	
MSI 候補ステータス	提案済みや昇格済みなど、重大なセキュリティインシデント候補のステータスを示します。インシデントが昇格された場合、ステータスは [承認済み] と表示されます。
昇格者	重大なセキュリティインシデントを昇格したユーザー。
昇格日時	重大なセキュリティインシデントが昇格された日付。
理由	重大なセキュリティインシデントの理由。理由には、MSI 番号とコード名を含める必要があります。
潜在的な影響	重大なセキュリティインシデントの潜在的な影響と重大度。潜在的な影響には、MSI 番号とコード名を含める必要があります。
制限	
制限の適用	特定の重大なセキュリティインシデントの制限に制限を適用するには、このオプションを選択します。制限を適用して、表示または変更アクセスを特定のユーザーまたはグループのみに制限できます。 詳細については、「特定の重大なセキュリティインシデントへのアクセスの制限」を参照してください。
許可されたメンバー	重大なセキュリティインシデントにアクセスできるユーザーのリスト。
許可されたグループ	重大なセキュリティインシデントにアクセスできるグループのリスト。
その他のアクション	
添付ファイル	重大なセキュリティインシデントに関連する添付ファイル。 [選択] オプションを選択して、添付ファイルをインシデントに追加します。
カンファレンスコール	カンファレンスコールをコミュニケーションチャネルとしてサードパーティサービスプロバイダーと使用し、重大なセキュリティインシデントを解決するためにステークホルダーと会議ができます。詳細については、「重大セキュリ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[重大なセキュリティインシデント] フォームのセクション (続く)

フィールド	説明
	ティインシデント管理カンファレンスコールの統合」を参照してください。

アクティビティ：

[アクティビティ] セクションを使用して、作業メモやコメントを追加したり、アクティビティを非公開で投稿したり、必要に応じて [作成] セクションを使用してコメントを追加したりすることができます。作業メモとコメントを投稿した後にアクティビティを保存すると、追加されたアクティビティまたは作業メモが [アクティビティ] セクションに表示されます。

注:
[詳細を表示] リンクを選択すると、その重大なセキュリティインシデントに関連付けられている特定のセキュリティインシデントレコードの詳細が表示されます。

次のような関連アクティビティを表示する設定を行います。

1. フィルター：[フィルターセット] アイコンを選択してフィルターを設定します。

   作業メモ、メール、タイムライン、その他のコメントに追加されたアクティビティなど、アクティビティに関する会話を表示するためのフィルターを設定します。

2. フラグ付き: [フラグ付き] アイコンを選択して、アクティビティにフラグを設定します。

   重要なアクティビティの会話にフラグを付けて、手元に置いておきます。

特定の重大なセキュリティインシデントへのアクセスの制限

誰が機密情報を含む重大なセキュリティインシデントを表示または変更できるかを管理します。重大なセキュリティインシデントの制限を適用して、特定の重大なセキュリティインシデントレコードと関連リストを表示または変更するアクセス権を誰が持つかを決定し、読み取りまたは書き込みアクセスを特定のユーザーまたはグループのみに制限できます。

始める前に
必要なロール：sn_msi.workspace_manager

このタスクについて
重大なセキュリティインシデント制限を使用すると、最重要な重大なセキュリティインシデントを非表示にして、特定の組織内のすべてのユーザーまたはグループがこのようなインシデントにアクセスまたは変更できないようにすることができます。この制限により、ユーザーまたはグループが表示または変更できるセキュリティインシデントをより詳細に制御できます。重大なセキュリティインシデントの制限を適用するには、[制限の適用] チェックボックスをオンにし、特定の重大なセキュリティインシデントの表示または変更を許可するユーザーまたはグループを選択します。

重大なセキュリティインシデントまたは関連リストに対する制限を特定のユーザーまたはグループに適用すると、組織内の残りのすべてのユーザーまたはグループは、これらの重大なセキュリティインシデントまたは関連リストを表示または変更できなくなります。

手順

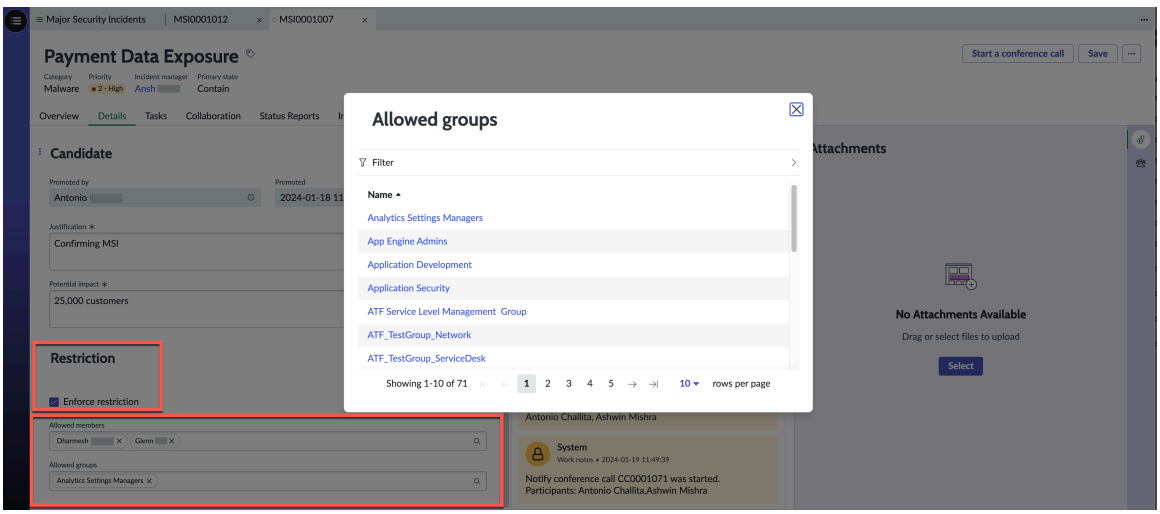
1. 次のように移動する。 ワークスペース > 重大セキュリティインシデント管理 > 重大なセキュリティインシデント.
2. [リスト] ビューを選択します。
3. 必要な重大なセキュリティインシデントレコードを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [詳細] タブを選択します。
5. 下にスクロールして [制限] セクションを選択します。
6. 重大なセキュリティインシデントの制限を有効にするには、[制限の適用] チェックボックスをオンにします。

重大なセキュリティインシデントへのアクセスの制限



7. [許可されたメンバー (Allowed members)] フィールドで [検索] オプションを使用して、重大なセキュリティインシデントを表示または変更できるユーザーを選択します。
8. [許可されたグループ] フィールドで [検索] オプションを使用して、重大なセキュリティインシデントを表示または変更できるグループを選択します。

> **注:**
> 重大なセキュリティインシデントの [制限を適用] チェックボックスをオンにすると、sn_msi.workspace_manager および許可されたメンバーまたはグループのみが重大なセキュリティインシデントを表示または変更できるようになります。

9. [保存] を選択します。

追加レコードの 重大セキュリティインシデント へのリンク

ワークスペースで、レコードのリンク機能を使用して、関連するセキュリティインシデントレコードとその子セキュリティインシデント、Vulnerability Response で示された修復タスク、および脅威インテリジェンスで示されたセキュリティケースを 重大セキュリティインシデント (MSI) レコードにリンクします。

始める前に

必要なロール：sn_msi.workspace_manager および sn_msi.workspace_responder

手順

1. 次のように移動する。 **Security Incident Response** > **MSIM** ワークスペース.
2. ワークスペースの左ペインに表示される [リスト] ビューに移動します。
3. [承認済み] をクリックして、昇格された重大なセキュリティインシデントレコードを選択します。
4. 昇格されたレコードのリストから、リンクする必要があってクローズ済みステータスでないインシデントレコードを選択します。
5. [リンクされたレコード] タブをクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

他のリンクされたレコードのテーブルを選択するためのドロップダウンリストが表示されます。
[リンクされたレコード] セクションに、重大なセキュリティインシデントにリンクされたレコードとその関連レコードが表示されます。

6. [セキュリティインシデント]、[修復タスク] (脆弱性一致アイテム)、または [セキュリティケース] など、目的のテーブルビューをリストから選択します。
選択したタイプのレコードのテーブルビューに基づいて、重大なセキュリティインシデントレコードにリンクされたレコードが表示されます。
7. どの MSI レコードにもリンクされていない [オープン] ステータスのレコードをリンクする場合は、そのレコードを選択し、ページの右上にある [レコードをリンク] ボタンをクリックします。

   注:
   [クローズ済み] ステータスの場合、インシデントレコードを MSI レコードにリンクすることはできません。

8. リンクするレコードを選択し、[リンク] ボタンをクリックします。
レコードが正常にリンクされ、関連レコードのロールアップがバックグラウンドで処理されることを示す確認メッセージが表示されます。

   注:
   レコードがリンクされると、リストビューが自動的に更新され、インシデントレコードの更新済みリストが表示されます。

関連情報

重大セキュリティインシデント からのレコードのリンク解除

重大セキュリティインシデント からのレコードのリンク解除

重大セキュリティインシデント管理ワークスペースを使用して、[リンクされたレコード] セクションから重大なセキュリティインシデントレコードのリンクを解除します。

始める前に

必要なロール：sn_msi.workspace_manager および sn_msi.workspace_responder

注:
リンク解除できるレコードは一度に 1 つのみです。レコードのリンクを解除すると、関連するロールアップ情報がワークスペースの [インシデントの影響度] および [脅威インテリジェンス] セクションから削除されます。このアクションを取り消すことはできません。

ロールアップレコードの詳細については、「MSIM のロールアップフレームワーク」を参照してください。

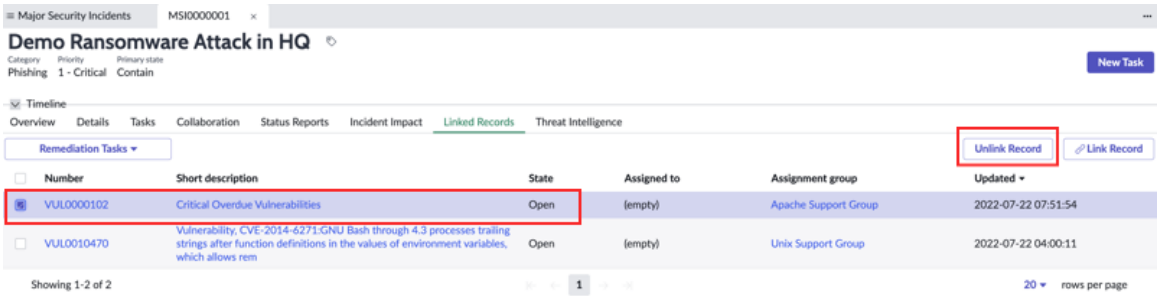
手順

1. 次のように移動する。 **Security Incident Response** > **MSIM** ワークスペース.
2. ワークスペースの左ペインに表示される [リスト] ビューに移動します。
3. [承認済み] をクリックして、昇格された重大なセキュリティインシデントレコードを選択します。
4. [リンクされたレコード] タブをクリックします。
このセクションに、重大なセキュリティインシデントにリンクされたレコードとその関連レコードが表示されます。
5. [セキュリティインシデント]、[修復タスク] (脆弱性一致アイテム)、または [セキュリティケース] など、目的のテーブルビューを選択します。
6. レコードのリストビューから、リンクを解除するレコードを選択します。
7. [レコードのリンクを解除] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

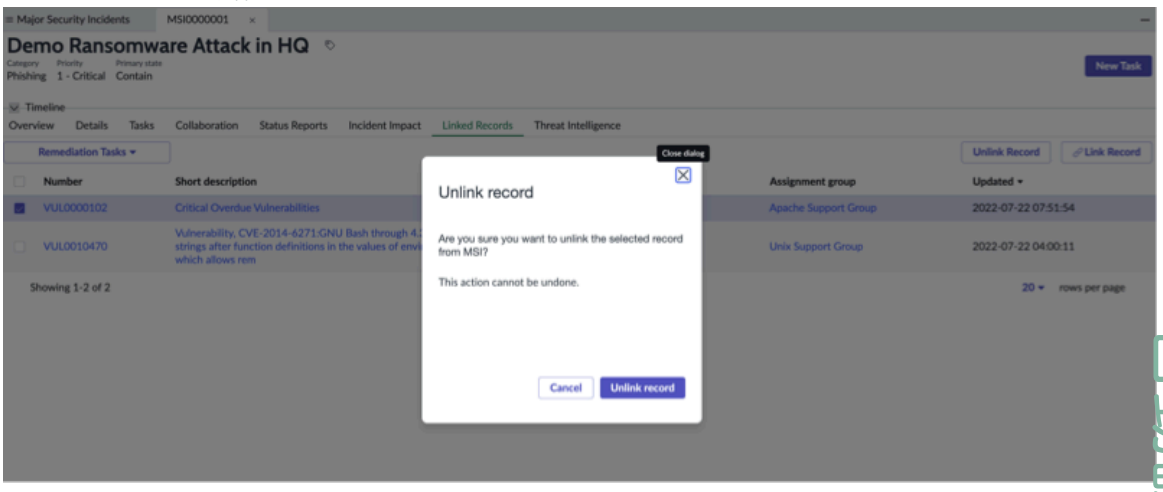
自動翻訳

レコードのリンクを解除



8. 選択したレコードを MSI からリンク解除するかどうかを尋ねる警告メッセージが表示されます。

レコードのリンク解除の警告メッセージ



9. [レコードのリンクを解除] をクリックします。
レコードのリンクが解除されます。一度リンクを解除すると、変更を元に戻すことはできません。リンクを解除した後、[リンクされたレコード] のリストビューが更新されます。

関連情報

重大セキュリティインシデント管理 でのリンクされたレコードの構成

重大セキュリティインシデント管理 でのロールアップレコードの構成

重大セキュリティインシデントでのタスクの管理

[タスク] タブでは、MSIM ワークスペースから重大なセキュリティインシデントに関連するすべてのタスクを追跡および管理できます。デフォルトのビジュアルタスクボード (カンバンビュー) またはリストビューを使用して、さまざまなタスクを表示できます。

sn_msi.workspace_manager は [タスク] タブで次の操作を実行できます。

- タスクの作成
- タスクの変更
- タスクを表示して自分または他のユーザーにアサイン
- タスクの削除

注:
MSIM アプリをインストールした後に、別途 **MSIM VTB Task Card: 1.0.1v** アプリがインストールされていることを確認してください。

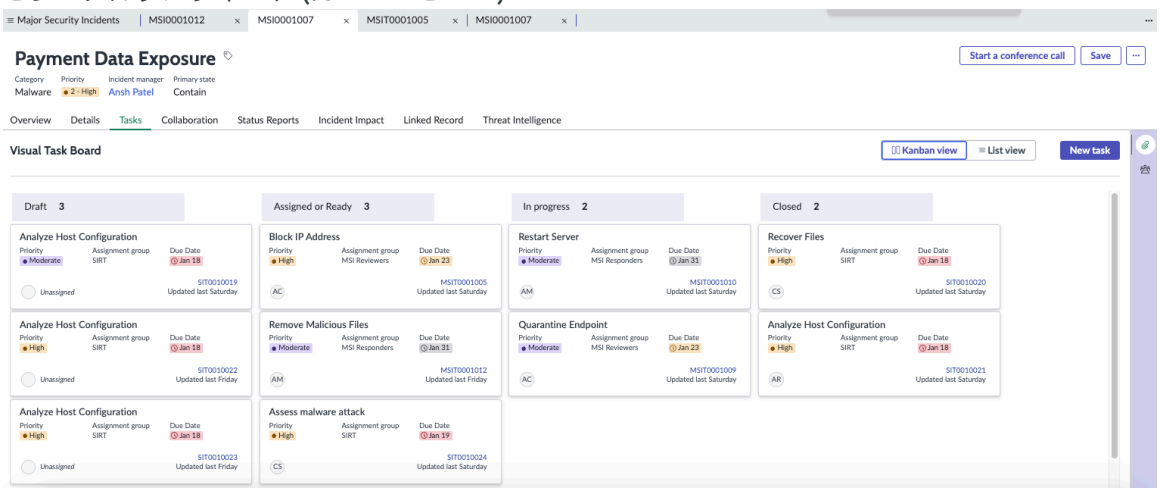
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[タスク] タブには、重大なセキュリティインシデントに関連付けられたすべてのタスクの詳細が表示されます。[タスク] タブでは、次の 2 つのビューがサポートされています。

- ビジュアルタスクボード (カンバンビュー)：

  複数のタスクレコードを表示および更新します。これらのレコードは、重大なセキュリティインシデントのタスクのステータスに基づいてレーン間を移動できるビジュアルタスクボードにカードとして表示されます。

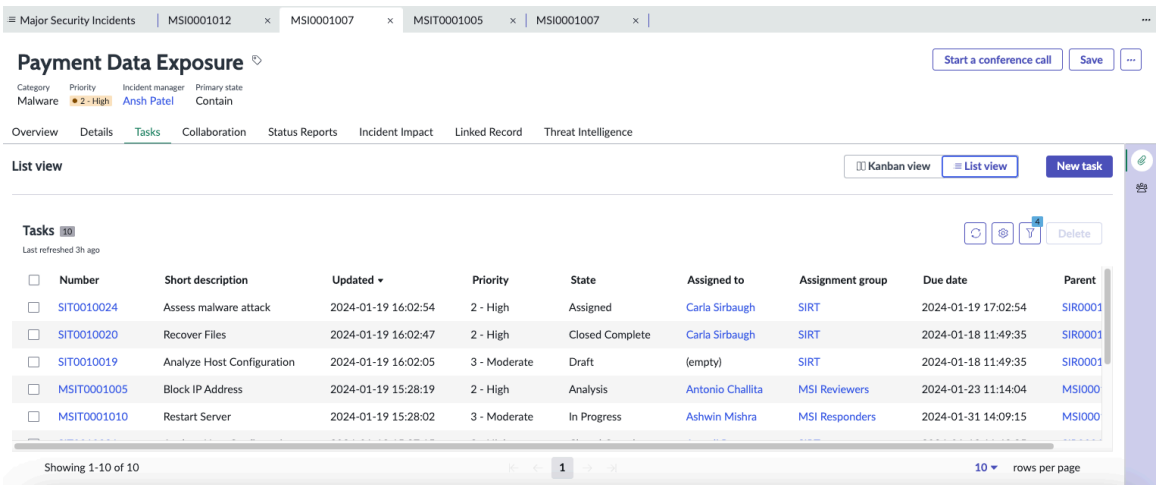
ビジュアルタスクボード (カンバンビュー)



- リストビュー：

  リストのフォームで使用して、複数のタスクレコードを表示および更新します。これらのリストカテゴリとフィルターを使用して、重大なセキュリティインシデントで作業する必要があるタスクをすばやく見つけて追跡することができます。

リストビュー



ラベル付けされたアクティビティは、重大なセキュリティインシデントの [概要] セクションに要約されて表示されます。[概要] セクションで傾向図のグラフを見られるため、統合されたタスクアクティビティのステータスが確認できます。

ビジュアルタスクボードを使用したタスクの管理

ビジュアルタスクボード (カンバンビュー) を使用して、重大なセキュリティインシデントに関連するすべてのタスクを追跡および管理します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ビジュアルタスクボードを使用して、タスクのステータスに応じて、[ドラフト]、[アサイン] または [準備完了]、[処理中]、[クローズ済み] などのレーン間を段階的にカードを移動できます。ボードのアクティビティストリームに最近のアクティビティが表示され、タスクの変更を簡単に追跡できます。タスクを拡張する任意のテーブルからタスクカードを追加して、簡単に更新を追跡してボードから直接重大なセキュリティインシデントを編集できます。

ビジュアルタスクボードを使用したタスクの作成

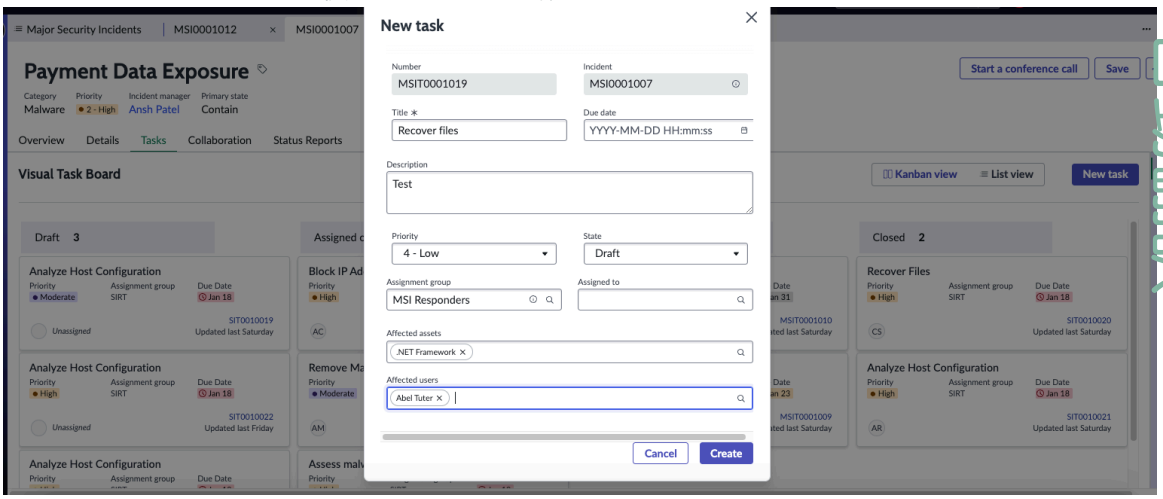
必要なロール：sn_msi.workspace_manager

> **注:**
> MSIM アプリをインストールした後に、別途 **MSIM VTB Task Card: 1.0.1v** アプリがインストールされていることを確認してください。

MSI マネージャーは、次の手順を使用して、ビジュアルタスクボードでタスクを作成できます。

1. 次のように移動する。 ワークスペース > 重大セキュリティインシデント管理 > 重大なセキュリティインシデント.
2. [リスト] ビューを選択します。
3. 必要な重大なセキュリティインシデントレコードを選択します。
4. [タスク] タブを選択します。

ビジュアルタスクボードを使用したタスクの作成



5. [カンバンビュー] を選択し、[新しいタスク] を選択します。
6. フォームのフィールドに入力します。

フィールド	説明
番号	選択したタスクに対して自動的に生成される一意の番号。このフィールドは編集できません。
インシデント	重大なセキュリティインシデントの番号。このフィールドは編集できません。
タイトル	タスクの名前を指定します。
期日	タスクを完了する期限の日時を選択します。[カレンダー] オプションを使用して日付を選択し、[時間の選択] セクションで時間を指定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
説明	タスク固有の説明を入力します。
優先度	タスクをいつ実行するかを決定するタスクの優先度を選択します。優先度は、次のいずれかの値になります。 ○ なし ○ **1-**重大 ○ **2 -** 高 ○ **3 -** 中 ○ **4 -** 低 ○ **5-** 計画中
状況	タスクの現在のステータスを選択します。ステータスは次のいずれかになります。 ○ ドラフト ○ 分析 ○ 処理中 ○ クローズ済み デフォルトのステータスは [ドラフト] です。
アサイン先グループ	検索オプションを使用して、タスクをアサインするユーザーの割り当て先グループを選択します。
アサイン先	検索オプションを使用して、タスクをアサインするユーザーを選択します。
影響を受ける資産	検索オプションを使用してタスクの影響を受ける資産を選択します。
影響を受けるユーザー	検索オプションを使用してタスクの影響を受けるユーザーを選択します。

7. [作成] を選択してタスクを作成します。

ビジュアルタスクボードを使用したタスクの表示と変更

必要なロール：sn_msi.workspace_manager

> **注:**
> MSIM アプリをインストールした後に、別途 **MSIM VTB Task Card: 1.0.1v** アプリがインストールされていることを確認してください。

MSI マネージャーは、MSI レスポンダーからタスクの詳細とアクティビティ情報を表示し、次の手順を使用してビジュアルタスクボードでタスクを変更できます

1. 次のように移動する。 ワークスペース > 重大セキュリティインシデント管理 > 重大なセキュリティインシデント.

2. [リスト] ビューを選択します。

3. 必要な重大なセキュリティインシデントレコードを選択します。

4. [タスク] タブを選択し、[カンバンビュー] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

5. いずれかのレーンで目的のタスクカードを選択して、タスクの詳細を表示します。

   タスクカードは、[ドラフト]、[アサイン] または [準備完了]、[処理中]、または [クローズ済み] のいずれかのレーンに配置できます。

6. [タスク情報] セクションで、次の詳細を変更できます。

フィールド	説明
番号	選択したタスクに対して自動的に生成される一意の番号。このフィールドは編集できません。
インシデント	重大なセキュリティインシデントの番号。このフィールドは編集できません。
タイトル	タスクの名前を指定します。
期日	タスクを完了する期限の日時を選択します。[カレンダー] オプションを使用して日付を選択し、[時間の選択] セクションで時間を指定します。
説明	タスク固有の説明を入力します。
優先度	タスクをいつ実行するかを決定するタスクの優先度を選択します。優先度は、次のいずれかの値になります。 ○ なし ○ **1-**重大 ○ **2 -** 高 ○ **3 -** 中 ○ **4 -** 低 ○ **5-** 計画中
状況	タスクの現在のステータスを選択します。ステータスは次のいずれかになります。 ○ ドラフト ○ 分析 ○ 処理中 ○ クローズ済み デフォルトのステータスは [ドラフト] です。
アサイン先グループ	検索オプションを使用して、タスクをアサインするユーザーの割り当て先グループを選択します。
アサイン先	検索オプションを使用して、タスクをアサインするユーザーを選択します。
影響を受ける資産	検索オプションを使用してタスクの影響を受ける資産を選択します。
影響を受けるユーザー	検索オプションを使用してタスクの影響を受けるユーザーを選択します。

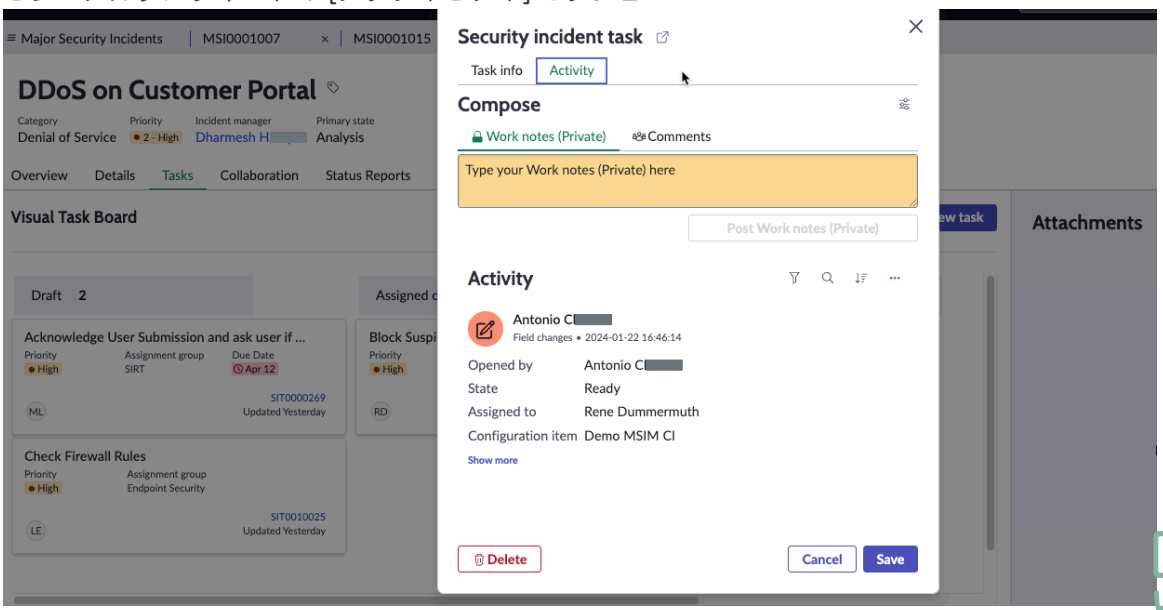
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. [アクティビティ] セクションを選択して、MSI レスポンダーからアクティビティの詳細を表示します。

   [アクティビティ] セクションを使用して、作業メモやコメントを追加したり、アクティビティを非公開で投稿したり、必要に応じて [作成] セクションを使用してコメントを追加したりすることができます。作業メモとコメントを投稿した後にアクティビティを保存すると、追加されたアクティビティや作業メモが [アクティビティ] セクションに表示されます。

   ビジュアルタスクボードの [アクティビティ] セクション



   注:
   [さらに表示] 詳細リンクを選択すると、その重大なセキュリティインシデントに関連付けられている特定のセキュリティインシデントレコードの詳細情報が表示されます。

8. [保存] を選択して、タスク情報を更新します。

   タスク情報はすぐに更新されます。

ビジュアルタスクボードを使用したタスクの削除

必要なロール：sn_msi.workspace_manager

注:
MSIM アプリをインストールした後に、別途 **MSIM VTB Task Card: 1.0.1v** アプリがインストールされていることを確認してください。

MSI マネージャーは、次の手順を使用して、ビジュアルタスクボードでタスクを削除できます。

1. 次のように移動する。 ワークスペース > 重大セキュリティインシデント管理 > 重大なセキュリティインシデント.
2. [リスト] ビューを選択します。
3. 必要な重大なセキュリティインシデントレコードを選択します。
4. [タスク] タブを選択し、[カンバンビュー] を選択します。
5. 削除するタスクカードを選択します。
6. [重大なセキュリティインシデントタスク] ポップアップで、[削除] オプションを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[タスクを削除] ポップアップが表示され、タスクの削除を確認するように求められます。

7. [削除] を選択します。

リストビューを使用したタスクの管理

リストビューを使用して、重大なセキュリティインシデントに関連するすべてのタスクを追跡および管理します。

リストビューには、タスク番号、優先度、現在のステータス、アサイン先、アサイン先グループなど、重大なセキュリティインシデントに関連付けられたすべてのタスクの詳細が表示されます。これらのリストカテゴリとフィルターを使用して、重大なセキュリティインシデントで作業する必要がある必要なタスクをすばやく見つけて追跡することができます。

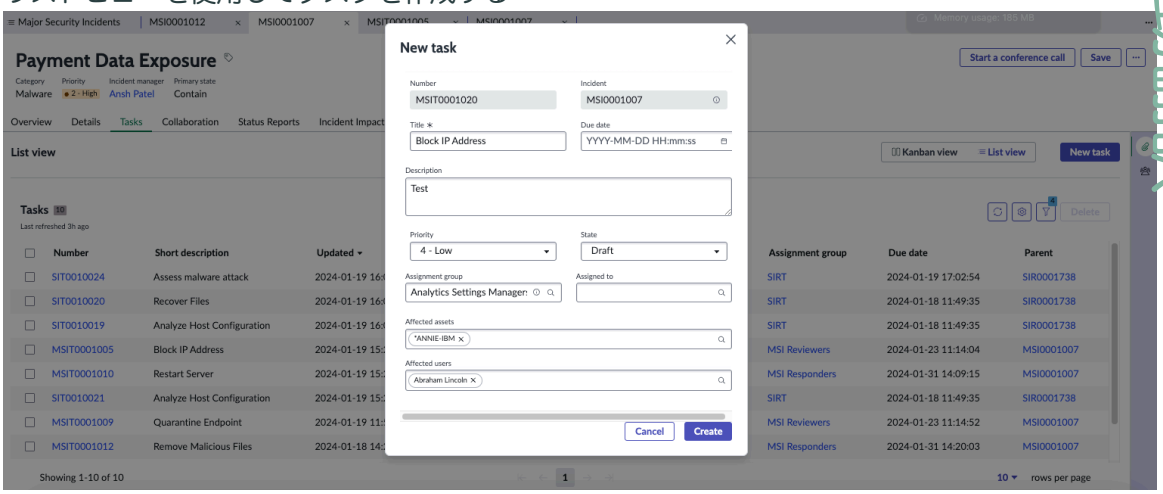
リストビューを使用してタスクを作成する

必要なロール：sn_msi.workspace_manager

MSI マネージャーは、次の手順を使用して、リストビューでタスクを作成できます。

1. 次のように移動する。 ワークスペース > 重大セキュリティインシデント管理 > 重大なセキュリティインシデント.
2. [リスト] ビューを選択します。
3. 必要な重大なセキュリティインシデントレコードを選択します。
4. [タスク] タブを選択します。

リストビューを使用してタスクを作成する



5. [リストビュー] を選択し、[新しいタスク] を選択します。
6. フォームのフィールドに入力します。

フィールド	説明
番号	選択したタスクに対して自動的に生成される一意の番号。このフィールドは編集できません。
インシデント	重大なセキュリティインシデントの番号。このフィールドは編集できません。
タイトル	タスクの名前を指定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
期日	タスクを完了する期限の日時を選択します。[カレンダー] オプションを使用して日付を選択し、[時間の選択] セクションで時間を指定します。
説明	タスク固有の説明を入力します。
優先度	タスクをいつ実行するかを決定するタスクの優先度を選択します。優先度は、次のいずれかの値になります。 ○ なし ○ **1-**重大 ○ **2 -** 高 ○ **3 -** 中 ○ **4 -** 低 ○ **5-** 計画中
状況	タスクの現在のステータスを選択します。ステータスは次のいずれかになります。 ○ ドラフト ○ 分析 ○ 処理中 ○ クローズ済み デフォルトのステータスは [ドラフト] です。
アサイン先グループ	検索オプションを使用して、タスクをアサインするユーザーの割り当て先グループを選択します。
アサイン先	検索オプションを使用して、タスクをアサインするユーザーを選択します。
影響を受ける資産	検索オプションを使用してタスクの影響を受ける資産を選択します。
影響を受けるユーザー	検索オプションを使用してタスクの影響を受けるユーザーを選択します。

7. [作成] を選択してタスクを作成します。

リストビューを使用したタスクの表示と変更

必要なロール：sn_msi.workspace_manager

MSI マネージャーは、MSI レスポンダーからタスクの詳細とアクティビティ情報を表示し、次の手順を使用してリストビューでタスクを変更できます

1. 次のように移動する。 ワークスペース > 重大セキュリティインシデント管理 > 重大なセキュリティインシデント.

2. [リスト] ビューを選択します。

3. 必要な重大なセキュリティインシデントレコードを選択します。

4. [タスク] タブを選択し、[リストビュー] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

5. リストビューで目的のタスクを選択して、タスクの詳細を表示します。
6. [タスク情報] セクションで、次の詳細を変更できます。

フィールド	説明
番号	選択したタスクに対して自動的に生成される一意の番号。このフィールドは編集できません。
インシデント	重大なセキュリティインシデントの番号。このフィールドは編集できません。
タイトル	タスクの名前を指定します。
期日	タスクを完了する期限の日時を選択します。[カレンダー] オプションを使用して日付を選択し、[時間の選択] セクションで時間を指定します。
説明	タスク固有の説明を入力します。
優先度	タスクをいつ実行するかを決定するタスクの優先度を選択します。優先度は、次のいずれかの値になります。 ○ なし ○ **1-**重大 ○ **2 -** 高 ○ **3 -** 中 ○ **4 -** 低 ○ **5-** 計画中
状況	タスクの現在のステータスを選択します。ステータスは次のいずれかになります。 ○ ドラフト ○ 分析 ○ 処理中 ○ クローズ済み デフォルトのステータスは [ドラフト] です。
アサイン先グループ	検索オプションを使用して、タスクをアサインするユーザーの割り当て先グループを選択します。
アサイン先	検索オプションを使用して、タスクをアサインするユーザーを選択します。
影響を受ける資産	検索オプションを使用してタスクの影響を受ける資産を選択します。
影響を受けるユーザー	検索オプションを使用してタスクの影響を受けるユーザーを選択します。

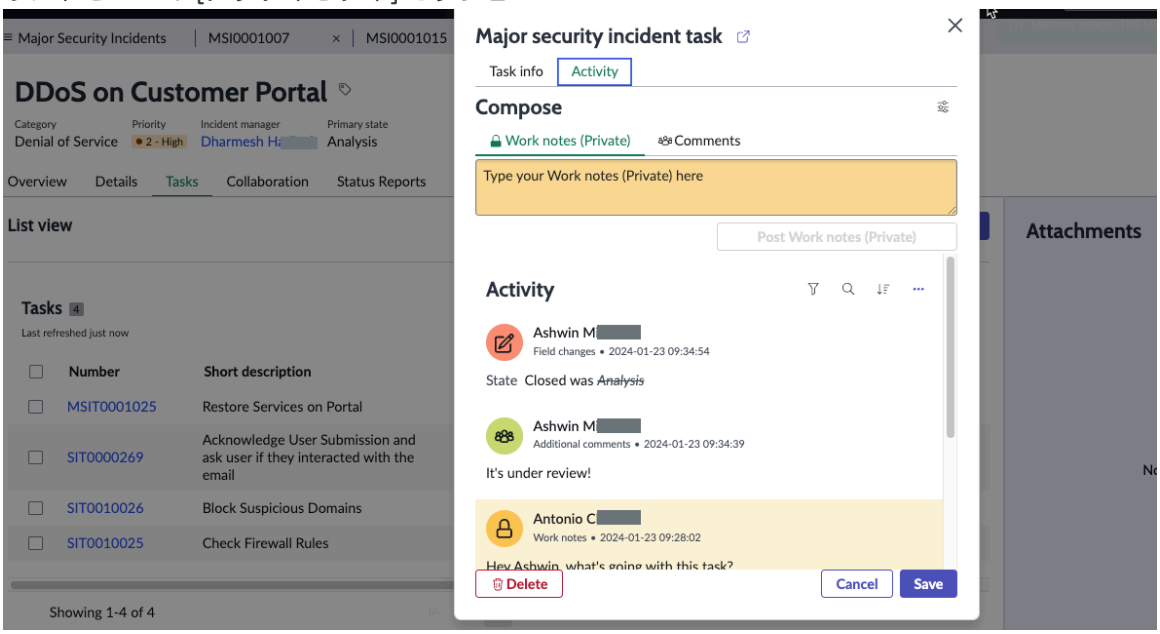
7. [アクティビティ] セクションを選択して、MSI レスポンダーからアクティビティの詳細を表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[アクティビティ] セクションを使用して、作業メモやコメントを追加したり、アクティビティを非公開で投稿したり、必要に応じて [作成] セクションを使用してコメントを追加したりすることができます。作業メモとコメントを投稿した後にアクティビティを保存すると、追加されたアクティビティや作業メモが [アクティビティ] セクションに表示されます。

リストビューの [アクティビティ] セクション



注:
[さらに表示] 詳細リンクを選択すると、その重大なセキュリティインシデントに関連付けられている特定のセキュリティインシデントレコードの詳細情報が表示されます。

8. [保存] を選択して、タスク情報を更新します。

   タスク情報はすぐに更新されます。

9. リストビューでは次のアクションを実行することもできます。
   a. [リフレッシュ] アイコンを選択して、リストビューのタスクのリストを更新します。
   b. [設定] アイコンを選択し、[列の編集] オプションを使用して、リストビューに表示される列の一覧を変更します。[幅をリセット] オプションを使用して、列の幅をリセットします。

リストビューを使用してタスクを削除する

必要なロール：sn_msi.workspace_manager

MSI マネージャーは、次の手順を使用して、リストビューでタスクを削除できます。

1. 次のように移動する。 ワークスペース > 重大セキュリティインシデント管理 > 重大なセキュリティインシデント.
2. [リスト] ビューを選択します。
3. 必要な重大なセキュリティインシデントレコードを選択します。
4. [タスク] タブを選択します。
5. [リストビュー] を選択します。
6. リストから削除するタスクを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. [重大なセキュリティインシデントタスク] ポップアップで、[削除] オプションを選択します。

   [タスクを削除] ポップアップが表示され、タスクの削除を確認するように求められます。

8. [削除] を選択します。

MSIM ワークスペースを介したコラボレーションアクティビティの追跡

MSIM ワークスペースで、重大なセキュリティインシデントの解決に関連するチャットおよびファイルアクティビティを追跡します。

アクティビティは、Microsoft Teams チャットと Microsoft SharePoint ファイルおよびフォルダーを使用してまとめられ、統合を介して 重大セキュリティインシデント に投稿されます。

Microsoft Teams と Microsoft SharePoint が 重大セキュリティインシデント管理 と統合されると、MSIM ワークスペースを使用して、重大なセキュリティインシデントの解決に貢献しているインシデントレスポンスユーザーと他のグループとのコラボレーションを追跡できます。Microsoft SharePoint 内のコラボレーションフォルダーとファイルに対する更新は MSIM ワークスペース File Explorer と同期され、アクティビティストリームコンポーネントにも反映されます。

セキュリティインシデントが重大なセキュリティインシデントに昇格されると、次の動作が起こります。

1. フォルダーテンプレートの構成に基づいて、フォルダー構造が Microsoft SharePoint に作成されます。同じフォルダー構造がワークスペースの File Explorer コンポーネントに反映されます。
2. 複数のチャネルを持つチームが Microsoft Teams アプリケーションの下に作成され、ワークスペースのチャット管理コンポーネントに反映されます。

必要なロール：sn_msi.workspace_manager

ファイルとフォルダーの操作

ファイルエクスプローラーにファイルシステムが表示されるため、インシデントの解決に関連するファイルとフォルダーを確認して操作できます。

特定のセキュリティインシデントについて Microsoft SharePoint でキャプチャされたファイルとフォルダーを表示します。これらのフォルダーは、その重大なセキュリティインシデントを対象として、Microsoft SharePoint に自動的に作成されます。デフォルトで作成されたこのフォルダーを使用して、必要に応じてサポートファイルをアップロードできます。必要に応じて、ファイルやフォルダーの名前を変更、移動、または削除できます。

また、いずれかのフォルダーにファイルをアップロードすると、そのフォルダーに対応するアクティビティが [コラボレーション] タブ内のファイルエクスプローラーフォルダーに自動的に関連付けられて、そのアクティビティが記録されて重大セキュリティインシデント管理ワークスペースの [アクティビティ] セクションに表示されます。

> **注:**
> [コラボレーション] タブでは、Sharepoint の親ファイルに、一意のインシデント番号とインシデントカテゴリが付いたインシデントレコードが追加されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. リポジトリビュー：特定のセキュリティインシデントについて Microsoft SharePoint にリストされているファイルとフォルダーを一覧表示します。それぞれのファイルやフォルダーについて、リポジトリビューに [名前]、 [変更者]、 [最終変更日]、[サイズ] が表示されます。

リポジトリビュー

フィールド	説明
Sharepoint で開く (Open in SharePoint)	重大なセキュリティインシデントの横のこのオプションを選択します。Microsoft SharePoint のフォルダー構造を選択して表示するには、リンクをクリックします。
新しいフォルダー	必要に応じて新しいフォルダーを作成するには、このオプションを選択します。新しいフォルダーを作成すると、同じ新しいフォルダーが作成され、デフォルトで Microsoft SharePoint に関連付けられます。

2. 最近：最近のアクティビティログをすべて表示します。表示されるログには SharePoint とファイルエクスプローラーの両方のアクティビティが含まれます。最近のアクティビティは通常、親フォルダーを含めたサポートファイルです。

   ログファイルを見つける手順は次のとおりです。

   a. それぞれのファイルを選択して詳細情報を表示します。

   b. [ファイルを検索 **(Locate File)]** をクリックします。

   > **注:**
   > 親ファイルと親フォルダーのナビゲーションと詳細情報が [最近] リストビューセクションの下に表示されます。同じファイルは SharePoint で開くことができます。関連するログファイルや任意のアクティビティをアップロードするたびに、アップロードしたすべてのファイルとアクティビティが、SharePoint とファイルエクスプローラーの両方に表示されます。

自動翻訳

Microsoft Teams を使用してチャットチャネルの通信を管理する

チャットチャネルマネージャーは、構成テンプレートのセットアップに基づいて Microsoft Teams アプリケーションで作成された複数のチャネルを、Microsoft Teams に表示します。

ここで構成されたチャネルは、チャネルにアサインされたユーザーおよびユーザーグループとともに、チャット管理コンポーネントに反映されます。チャットチャネルマネージャーでは、次のことを実行できます。

- チャットチャネルを管理する
- チームの名前を変更
- チームメンバーの管理

チームとチャネルは、Microsoft Teams のチャットチャネル構成に基づいて作成されます。

チャットチャネルを管理する

チャットチャネルマネージャーを使用すると、チャットチャネルを作成、編集、または削除できます。Microsoft Teams でチャットチャネルを管理するには、次の手順を実行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. [コラボレーション] タブを選択します。
2. 次のように移動する。 チャットチャネルマネージャー > 新規チャネルを作成.
3. 新しい [チャネル名] と [説明] を追加し、チャネルの [メンバー] を選択します。
4. [作成] を選択します。

   注:
   Microsoft Teams アプリケーションの [Microsoft Teams チャネル] セクションに新しいチャネルレコードが作成され、同じレコードが MSIM に反映されます。

5. チャットチャネルを編集するには、[チャットチャネルマネージャー (Chat Channel Manager)] リストでチャットチャネルを選択します。
6. 要件に基づいて、チャネル名、メンバーリスト、グループメンバーリストを変更できます。
7. [保存] を選択します。
8. チャットチャネルを削除するには、[チャットチャネルマネージャー (Chat Channel Manager)] リストでチャットチャネルを選択します。
9. [チャネルを削除] を選択します。

チームの名前を変更

Microsoft Teams でチームの名前を変更するには、次の手順を実行します。

1. [コラボレーション] タブを選択します。
2. 次のように移動する。 チャットチャネルマネージャー > チームの名前を変更.
3. [チーム名] フィールドで、要件に従ってチームの名前を変更します。
4. [保存] を選択します。

   注:
   チーム名を変更すると、Microsoft Teams のチーム名も変更されます。

チームメンバーの管理

チャットチャネルマネージャーを使用すると、Microsoft Teams でチームメンバーを追加または削除できます。グループからメンバーを追加することもできます。Microsoft Teams でチームメンバーを管理するには、次の手順を実行します。

1. [コラボレーション] タブを選択します。
2. 次のように移動する。 チャットチャネルマネージャー > チームメンバーの管理.
3. [メンバー] フィールドで、要件に従ってチームメンバーを追加または削除します。
4. [グループ経由でメンバーを追加 (Add members via Groups)] フィールドで、Microsoft Teams に追加するグループを選択します。

   注:
   グループメンバーが既にチームに属している場合、それらのメンバーは追加されません。

5. [保存] を選択します。

   チャットチャネルマネージャーには、チームメンバーの総数の詳細と、追加される新しいメンバーの数が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Slack を使用してチャットチャネルの通信を管理する

チャットチャネルマネージャーは、構成テンプレートのセットアップに基づいて Slack アプリケーションで作成された複数のチャネルを、Slack に表示します。

ここで構成されたチャネルは、チャネルにアサインされたユーザーおよびユーザーグループとともに、チャット管理コンポーネントに反映されます。チャットチャネルマネージャーを使用すると、チャットチャネルを管理できます。チームとチャネルは、Slack のチャットチャネル構成に基づいて作成されます。

チャットチャネルを管理する

チャットチャネルマネージャーを使用すると、Slack でチャットチャネルを作成、編集、または削除できます。チャットチャネルを管理するには、次の手順を実行します。

1. [コラボレーション] タブを選択します。
2. 次のように移動する。 チャットチャネルマネージャー > 新規チャネルを作成.
3. 新しい [チャネル名] と [説明] を追加し、チャネルの [メンバー] を選択します。
4. [作成] を選択します。

   注:
   Slack アプリケーションの [Slack チャネル] セクションに新しいチャネルレコードが作成され、同じレコードが MSIM に反映されます。

5. チャットチャネルを編集するには、[チャットチャネルマネージャー (Chat Channel Manager)] リストでチャットチャネルを選択します。
6. 要件に基づいて、チャネル名、メンバーリスト、グループメンバーリストを変更できます。
7. [保存] を選択します。
8. チャットチャネルを削除するには、[チャットチャネルマネージャー (Chat Channel Manager)] リストでチャットチャネルを選択します。
9. [チャネルを削除] を選択します。

アクティビティストリームの会話の管理

Microsoft SharePoint、ファイルエクスプローラー、および Microsoft Teams で実行されたすべてのアクティビティ、ログ、ステータスを表示します。

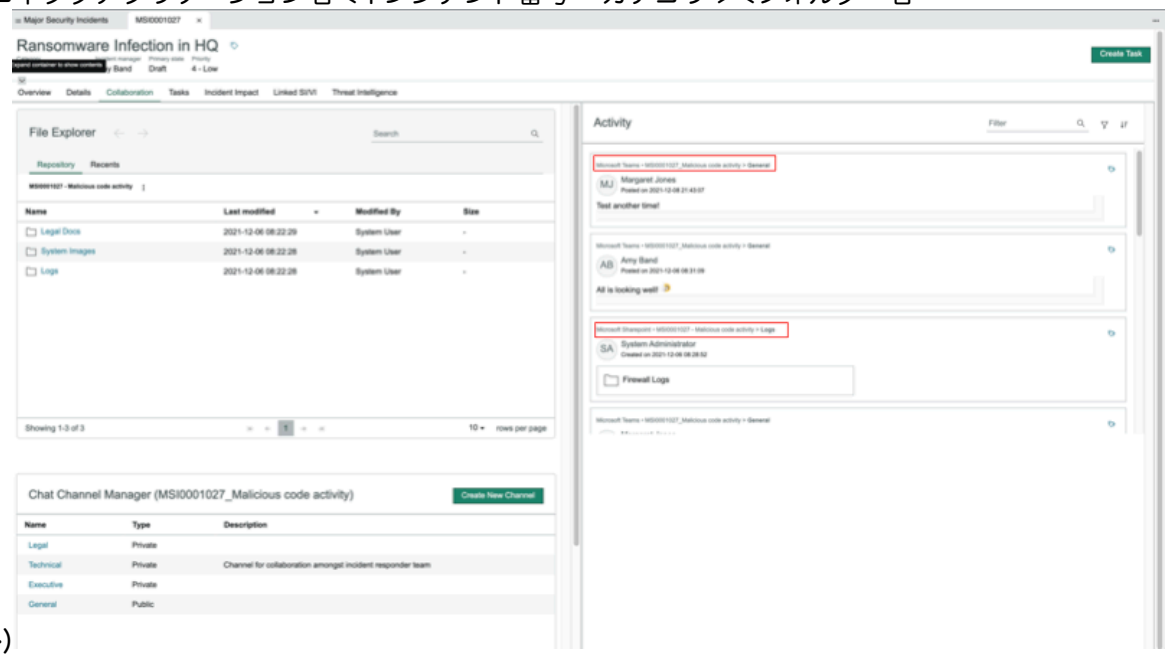
さまざまなファイルやフォルダー間、および Microsoft Teams でやり取りされた特定のアクティビティを表示したり、コラボレーションアクティビティの詳細を検索したりする場合は、[アクティビティストリーム] セクションの右上に表示されるフィルター機能を使用して、目的のアクティビティの詳細情報を探します。

重大セキュリティインシデント管理で共有されるフォルダーとチャットの会話は、次のような構造のブレッドクラムとして反映されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

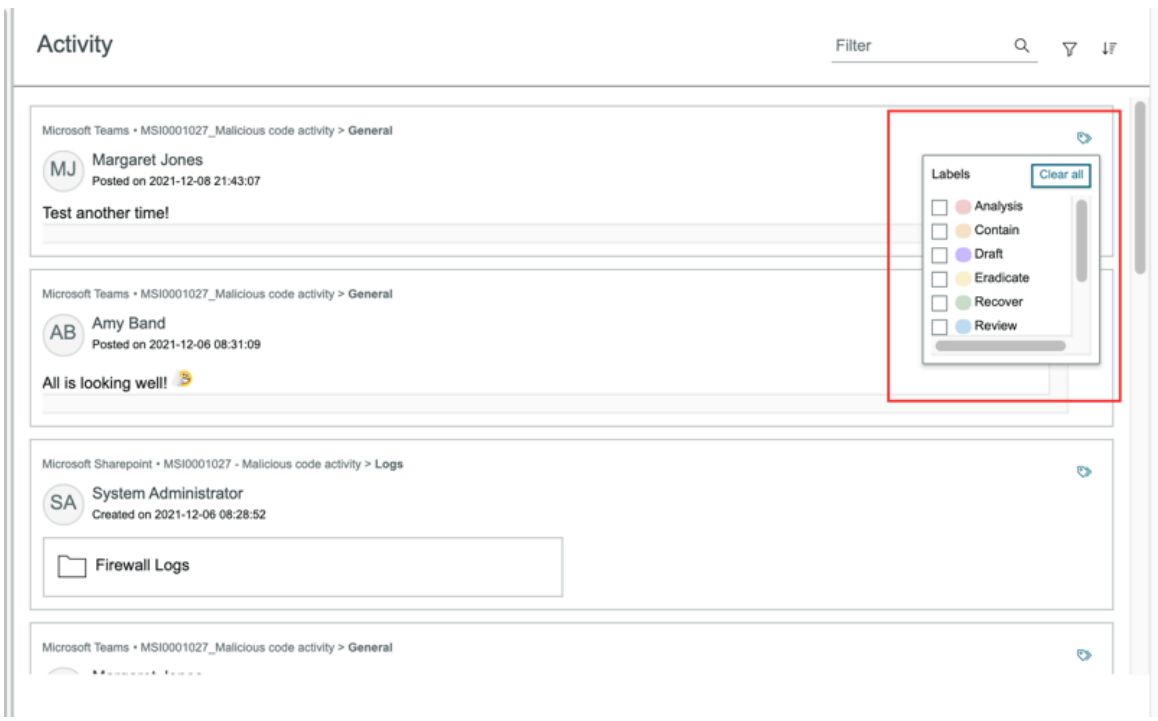
コネクタアプリケーション名 <インシデント番号 – カテゴリ > <フォルダー名



>)

アクティビティへのラベル付け

1. [ラベル] アイコンをクリックします。
2. 次のスクリーンショットで示すとおりに、それぞれのインシデントアクティビティのラベルのチェックボックスをオンにします。



3. ラベルの付いたアクティビティが、ワークスペースの [外部コラボレーション] セクションに色分けされて進捗の傾向グラフとして表示されます。

MSIM ステータスレポートの作成と配布

重大セキュリティインシデント マネージャーは、重大なセキュリティインシデントの解決の過程で、構成済みのレポートテンプレートや以前のステータスレポートを基にさまざまな間隔で各種のステータスレポートを作成し、さまざまなステークホルダーに配布できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：sn_msi.workspace_manager

前に構成したサマリーレポートのデータ要素をプレビューし、テキストやサマリーを追加し、必要に応じて個々のレポートコンポーネントを削除して、レポートの正確性と完全性を検証してから、さまざまなステークホルダーに配布することができます。

[MSI レポートテンプレートのセットアップ (MSI Report Templates Setup)] ページで最初に設定された目的のレポートテンプレートを選択して、ステータスレポートを作成します。

手順

1. 次のように移動する。 ワークスペース > 重大セキュリティインシデント管理 > 重大なセキュリティインシデント.
2. [リスト] ビューを選択します。
3. 昇格された個々の MSI レコードを選択します。
4. [ステータスレポート] タブを選択します。
   [ステータスレポート] タブには、以下のような 3 つのタイプのサブセクションがあります。

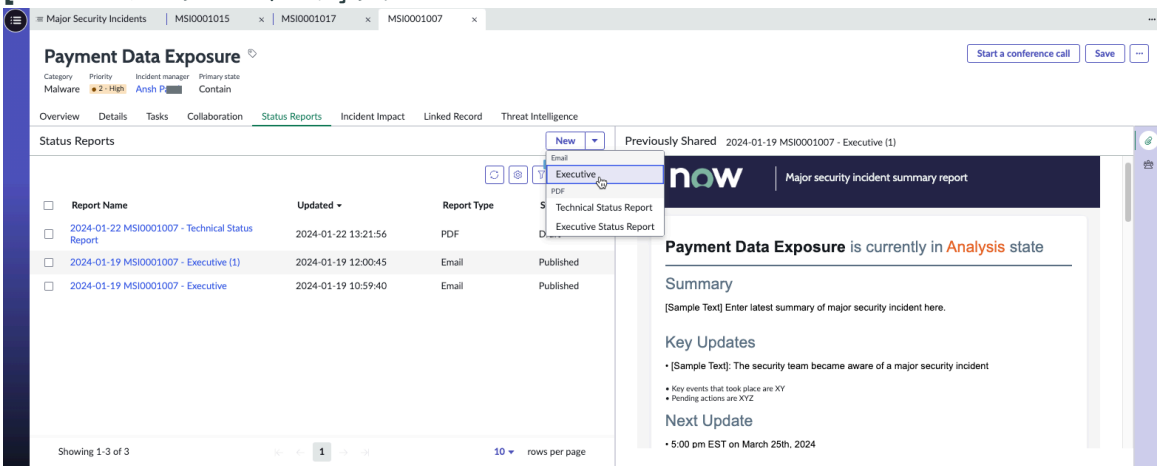
フィールド	説明
レポート名	ステータスレポートテンプレートの名前。 **注:** [ステータスレポート] ビューには、関連するペルソナのベースシステムの一部として利用可能な、既存の事前定義されたレポートテンプレートが一覧表示されます。たとえば、メールによるエグゼクティブステータスレポート (モバイル対応)、技術ステータスレポート、エグゼクティブステータスレポート (PDF 形式) などです。
更新日時	レポートテンプレートが最後に更新された日付。
レポートタイプ	ステータスレポートのタイプ。ステータスレポートは、次のいずれかのタイプになります。 ○ PDF ○ メール
状況	ステータスレポートのステータス。ステータスレポートは、次のいずれかのステータスになります。 ○ ドラフト ○ キューに格納 ○ 公開

5. 表示するステータスレポートのタイプを選択するか、[新規] を選択してステータスレポートを作成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[MSIM ステータスレポート] タブ



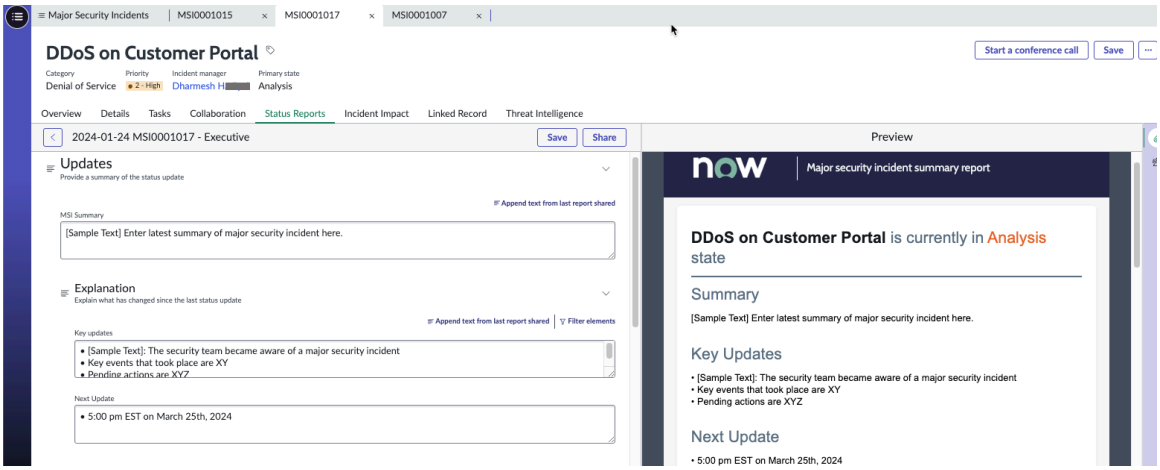
6. リストから次のいずれかのステータスレポートタイプを選択します。
   - エグゼクティブ モバイル対応のメールステータスレポート。
   - 技術ステータスレポート PDF
   - エグゼクティブステータスレポート PDF

   注:
   目的のレポートテンプレートを選択すると、選択したレポートのプレビューがすぐに右ペインに生成されます。MSI の選択したステータスレポートを表示できます。

7. エグゼクティブメールステータスレポートテンプレートで、ステータスレポートの詳細をセクションに入力します。

   注:
   [ステータスレポート] セクションで選択したオプションは、プレビューレポートに表示されるオプションと同じです。

ステータスレポートテンプレート



8. [保存] を選択して、ステータスレポートに加えた更新を保存します。
9. [共有] を選択して、ステータスレポートを社内外のステークホルダーと共有します。
   [共有] ダイアログボックスが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

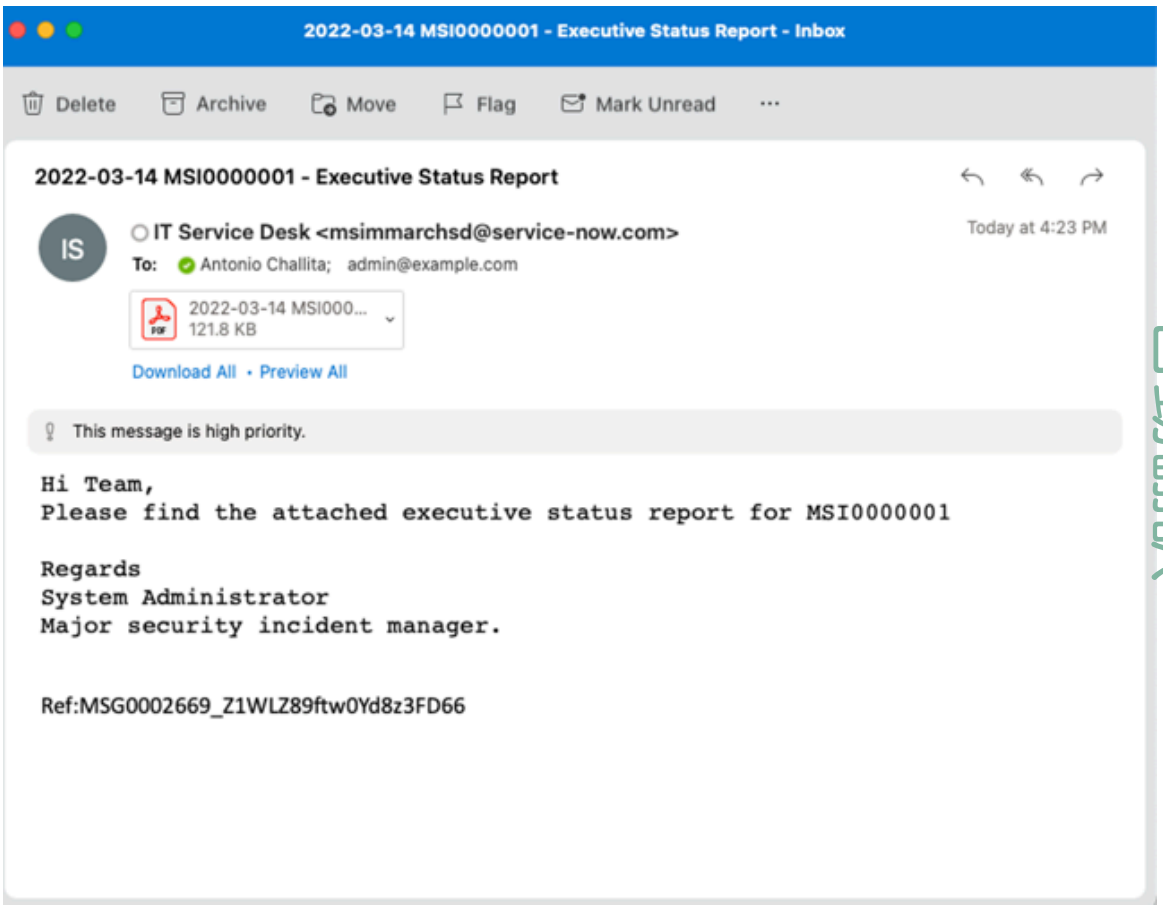
a. [件名] フィールドに、メールレポートの件名を入力します。

b. [内部受信者を追加 (Add internal recipients)] フィールドで、メールレポートの受信者を入力して選択します。

c. [外部受信者の追加 (Add external recipients)] フィールドに、メールレポートの受信者のメールまたは DL を入力します。
カンマまたはセミコロンを使用して、複数のメール ID を追加できます。

10. [レポートをメールで送信] を選択します。
PDF のステータスレポートが添付されたメールが、関係する受信者による確認のため正常に送信されます。

ステータスレポート - メール



11. [ステータスレポート] タブで次のアクションを実行することもできます。

a. [ステータスレポート] ビューの [リフレッシュ] アクションを使用して、ステータスレポートリストを更新する。

b. [ステータスレポート] ビューで [リストアクション] アクションを使用して、列を編集、またはステータスレポートリストの幅をリセットする。

c. [ステータスレポート] ビューの [フィルター] アクションを使用して、特定の条件に基づいてステータスレポートをフィルタリングする。

関連情報

重大セキュリティインシデント ステータスレポートの構成

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

MSIM ステータスレポートの管理

ステータスレポートは、セキュリティ運用プロセスを改善し、解決のタイムラインや期限切れ数、アサインされた各タスクのステータスを測定および分析するための、アクション可能なデータを可視化した事前定義済みの傾向図を示します。

重大セキュリティインシデント ステータスレポートの構成

重大なセキュリティインシデントのレコード修正プロセスのライフサイクル全体を通じてビジネスニーズに応じたレポートをセットアップおよびダウンロードするための、重大なセキュリティインシデントレポートを構成します。

重大セキュリティインシデント管理 ワークスペースのステータスレポート機能を使用して、特定の形式とレイアウトでレポートテンプレートをビルドし、そのレポートを特定の要件に従ってカスタマイズできます。

sn_msi.workspace_manager ロールを持つユーザーは、エグゼクティブステークホルダーや法務部門といった特定のユーザーと共有可能なすべてのステータスレポートの生成に使用できるレポート情報のタイプをまとめたレポートテンプレートを作成および構成したり、そのテンプレートを重大なセキュリティインシデントレコードにマッピングしたりすることができます。

MSI ステータスレポートをカスタマイズするには、まず [レポートテンプレート] を使用してレポートテンプレートを設定する必要があります。[レポートテンプレート] を使用すると、レポートテンプレートのタイプのビルドや、レポートテンプレートのレポートコンポーネントの定義、詳細情報の追加、スコープと進行状況のメトリクスを追跡するためのビジュアル化されたデータの作成、関連リストデータの追加、ステータスレポートの生成などができます。

すべてのレポートテンプレートタイプにあるデフォルトのフィールドを以下に示します。セクションやサブセクション、またその要素を使用して、要件に基づくレポートテンプレートを構成および書式設定できます。

ステータスレポートのコンポーネント

コンポーネントタイプ	説明
レポートタイトル	レポートのタイプのタイトル。たとえば、レポートタイプのデフォルト形式は「{MSI 番号 (MSI Number)} - {エグゼクティブステークホルダーレポート (Executive Stakeholder Report)}」で、「MSI0001001：エグゼクティブステークホルダーレポート (Executive Stakeholder Report)」と表示されます。
名前	重大セキュリティインシデント管理 ワークスペースの [ステータスレポート] セクションを使用してレポートを生成したユーザーの名前を表示します。
サマリー	レポートの簡単なサマリーを表示します。
日付	担当の受信者とレポートが共有される日付を表示します。
進行状況	リンクされた SIR インシデント、対応タスク、補足タスク (Supplementary Tasks)、外部コラボレーション、タイムラインの各コンポーネント、最近のタイムラインイベント (Recent Timeline Events) といった、スコープと進行状況のメトリクスを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ステータスレポートのコンポーネント (続く)

コンポーネントタイプ	説明
課題	このセクションには、重大なセキュリティインシデントの修復プロセス全体に関わる課題についての簡単な説明が表示されます。
次の手順	このセクションには、重大なセキュリティインシデントを解決するための次の手順に関する簡単な説明が表示されます。たとえば、エグゼクティブステークホルダーレポートのアクティブなチームというサブセクションには、重大なセキュリティインシデントレコードの詳細な分析に関与するチームのアサインで次に行う手順が記載されています。
その他のカスタマイズ (Other customizations)	レポートテンプレートでは、ロゴをアップロードしたり、レポートのヘッダーとフッターをカスタマイズしたりすることもできます。

設定および表示できるレポートカテゴリのタイプは次のとおりです。

- エグゼクティブメール
- 技術ステータスレポート PDF
- エグゼクティブステータスレポート PDF

前述のレポートが構成されて、[重大セキュリティインシデント管理] ワークスペースからユーザーがレポートを選択、表示、および生成できるようになります。

モバイル対応エグゼクティブステータスレポート - メール

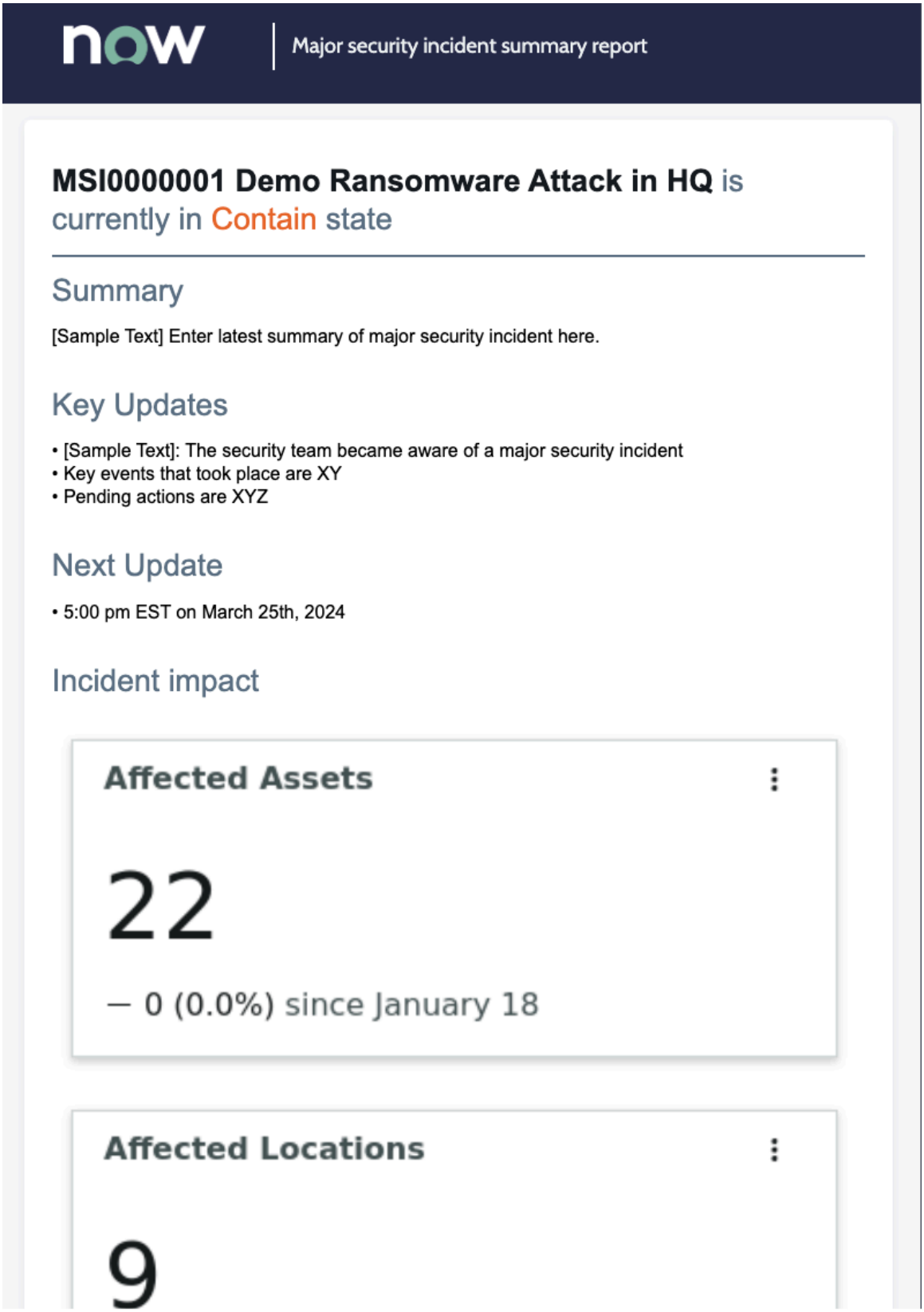
エグゼクティブステータスレポート - メールは、メール形式で生成されたモバイル対応のステータスレポートです。エグゼクティブステータスレポートの場合、レポートセクションには、レポートの簡単な概要、MSI の期間の列、インシデントのスコープや影響、アクティブなチームのメトリクス、進行状況のメトリクス、タイムラインのコンポーネント (特定の重大なセキュリティインシデントレコードの最近のタイムラインイベントなど) が記載されます。

次のレポートテンプレート機能をカスタマイズして設定し、補足情報をレポートに追加します。参考のため、エグゼクティブメールステータスレポートのサンプルを以下に示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エグゼクティブステータスレポートメール



エグゼクティブステータスレポート - PDF

エグゼクティブステータスレポート - PDF は、PDF 形式で生成されたモバイル対応のステータスレポートです。エグゼクティブステータスレポートの場合、レポートセクションには、レポートの簡単な概要、MSI の期間の列、インシデントのスコープや影響、アクティブなチームのメトリクス、

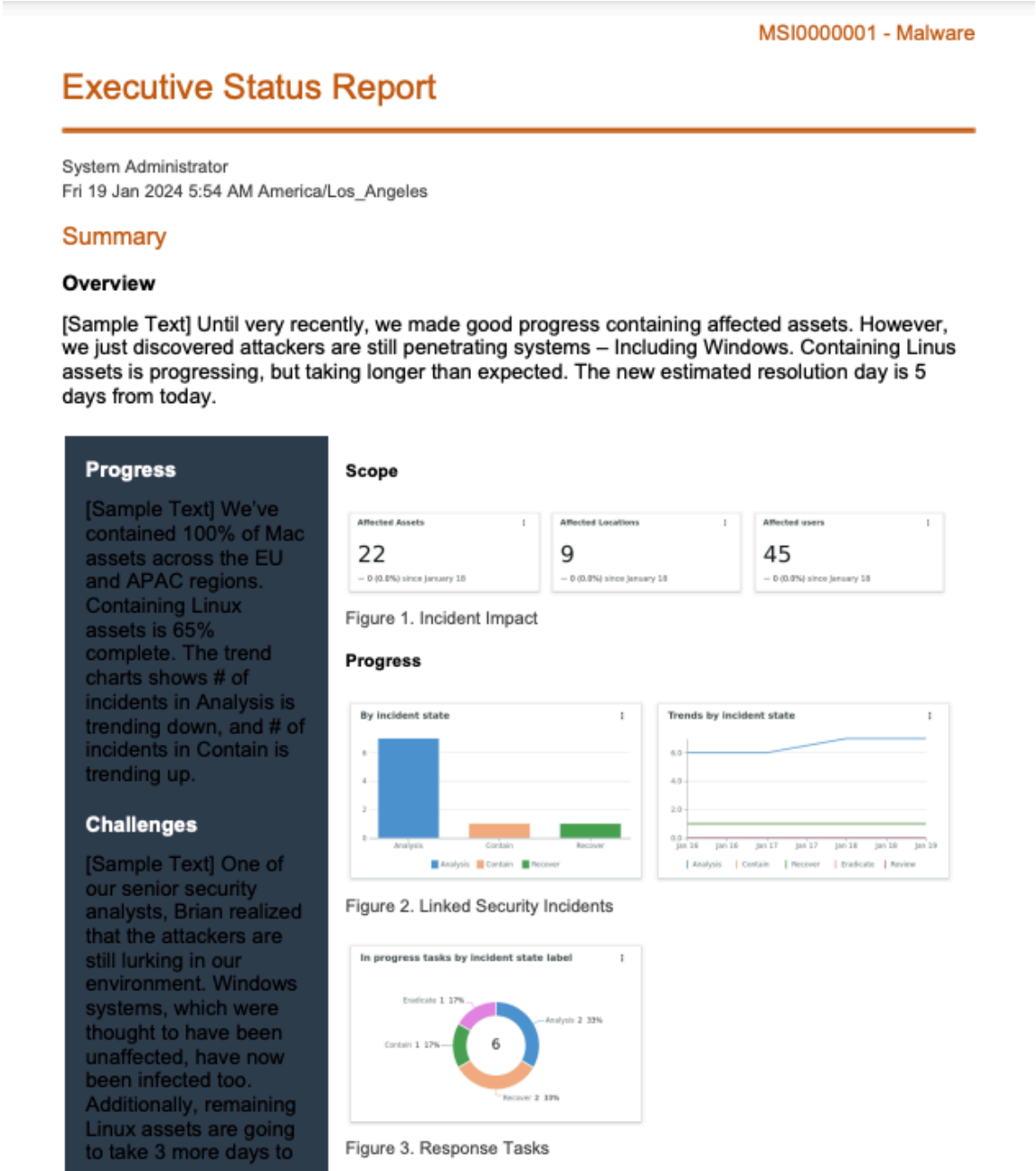
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

進行状況のメトリクス、タイムラインのコンポーネント (特定の重大なセキュリティインシデントレコードの最近のタイムラインイベントなど) が記載されます。

次のレポートテンプレート機能をカスタマイズして設定し、補足情報をレポートに追加します。参考のため、エグゼクティブレポートのサンプルを以下に示します。

エグゼクティブステータスレポート **PDF**



MSI0000001 - Malware

Executive Status Report

System Administrator
Fri 19 Jan 2024 5:54 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets 22
Affected Locations 9
Affected users 45

Figure 1. Incident Impact

Progress

By incident state
Trends by incident state

Figure 2. Linked Security Incidents

In progress tasks by incident state label
6

Figure 3. Response Tasks

技術ステータスレポート - **PDF**

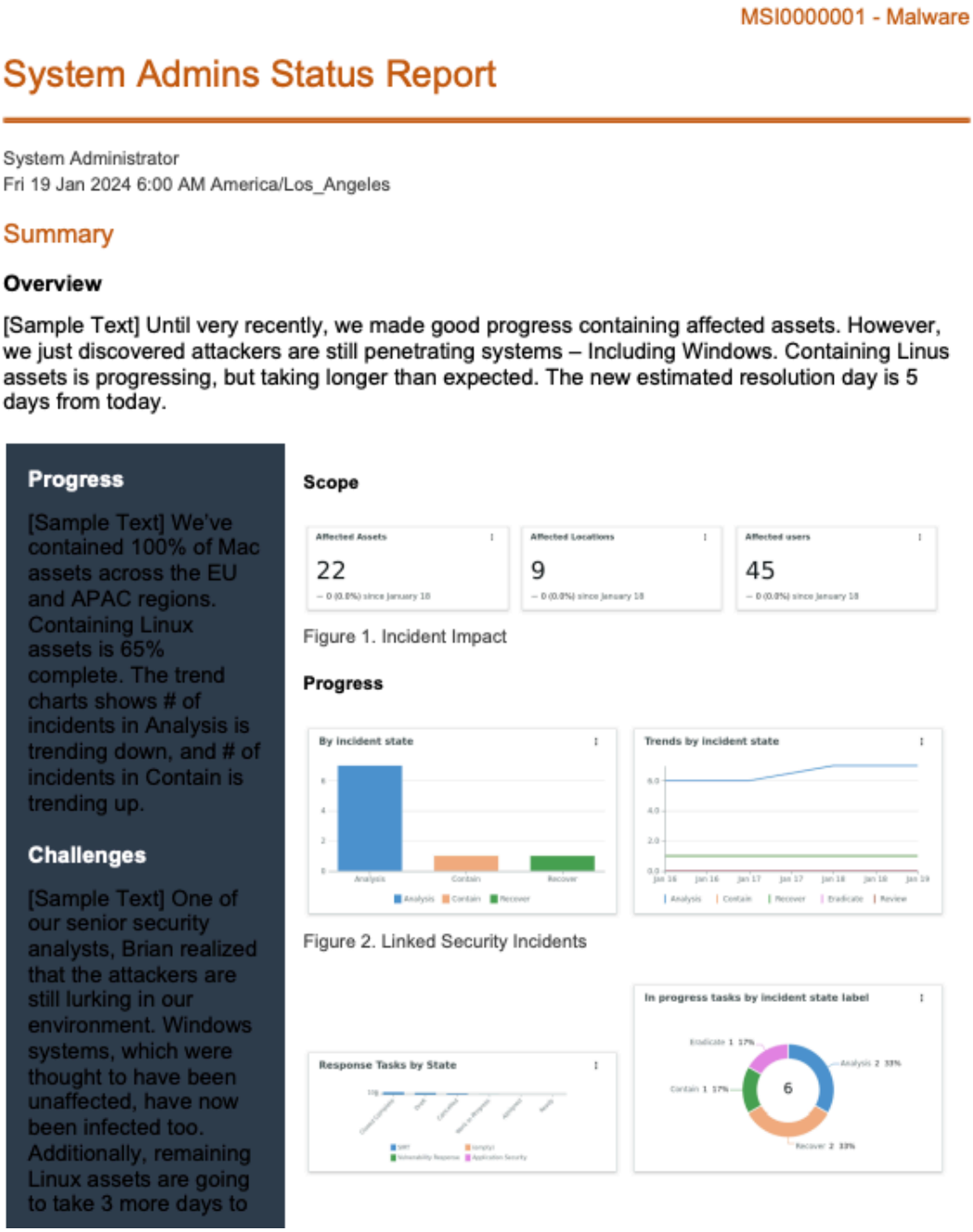
技術ステータスレポート - PDF は、PDF 形式で生成されたモバイル対応のステータスレポートです。レポートセクションには、レポートの概要、MSI の期間の列、インシデントのスコープや影響、アクティブなチームのメトリクス、進行状況のメトリクス、特定の重大なセキュリティインシデントレコードの最近のタイムラインイベントなどのタイムラインコンポーネント、前回のステータスレポートの生成以降にアサイン先グループと選択されたタグラベルに基づいてラベル付けされたタスクの更新とアクティビティ、およびインシデントの影響度やリンクされたインシデントなどの補足情報が記載されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レポートテンプレートをカスタマイズして設定し、補足情報をレポートに追加します。インシデントの影響度などの補足情報を示す技術レポートのサンプルを参考用に図示します。それ以外のレポート情報はエグゼクティブレポートと同様です。

技術ステータスレポート **- PDF**



MSI0000001 - Malware

System Admins Status Report

System Administrator
Fri 19 Jan 2024 6:00 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Figure 1. Incident Impact

Progress

Figure 2. Linked Security Incidents

レポートテンプレートのセクションにはさまざまなサブセクションがあり、そこでレポートのサブセクションおよび次のような要素をビルドできる方法を説明しています。

1. ブランディング：レポートテンプレートへのブランディングの追加
2. テンプレートスクリプト：レポートテンプレートでのテンプレートスクリプトの使用
3. レポートテンプレートでの可視化の使用
4. レポートテンプレートでのレポートリストの使用

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レポートテンプレートの作成

重大なセキュリティインシデントに適用できるさまざまなレポートテンプレートを作成し、ステータスレポートを生成します。ドット連結可能なレポートテンプレートに、[重大なセキュリティインシデントレスポンス] フォームの標準およびカスタムのフィールドを追加できます。また、セクションやサブセクション、またその要素を使用して、要件に基づくレポートを書式設定および構成できます。

始める前に

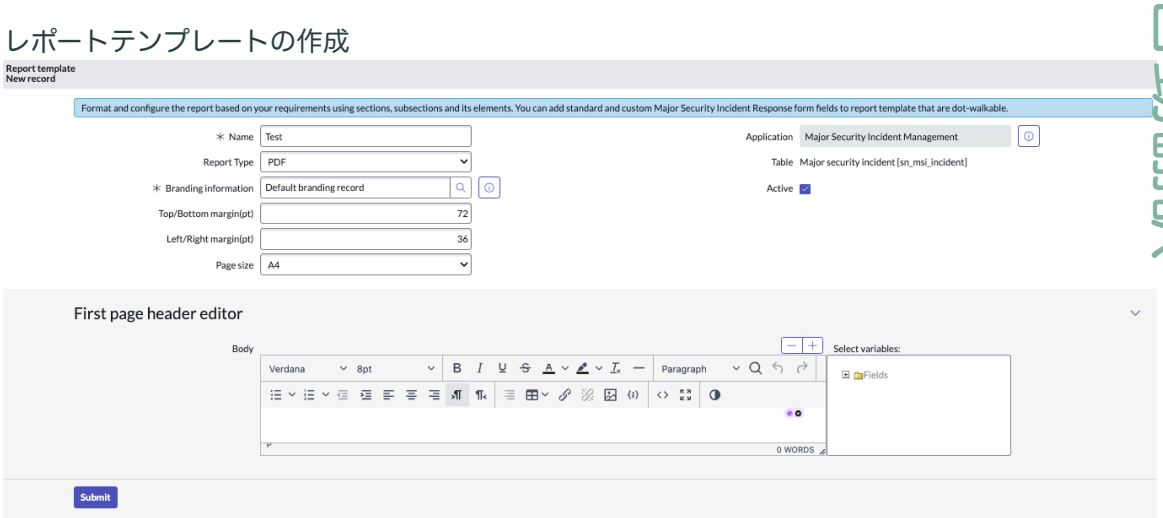
必要なロール：sn_msi.workspace_manager

このタスクについて

レポートテンプレートにレポートコンポーネントを定義し、追加情報を提供することができます。スコープと進行状況のメトリクスを追跡するための可視化されたデータの作成、関連リストデータの追加、ステータスレポートのプレビューと生成または共有ができます。

手順

1. 次のように移動する。 **All** (すべて) > 重大セキュリティインシデント管理 > **MSI** 管理 > ステータスレポート設定.
   [MSI ステータスレポート設定] ページが表示されます。
2. [レポートテンプレート] セクションで、[構成] を選択します。
3. [新規] を選択して、レポートテンプレートを作成します。
4. [レポートテンプレート] フォームのフィールドに入力します。



5. [送信] で新しいレポートテンプレートレコードを送信します。
   [レポートテンプレート] ページの下に新しいレポートテンプレートが作成されます。

関連情報

MSIM ステータスレポートの作成と配布

レポートテンプレートへのブランディングの追加

レポートにブランディングを追加します。ヘッダーとフッターの画像、ヘッダーとフッターのテキストを追加できます。事前定義されている 2 つのレポート以外に、必要に応じて任意のレポートテンプレートのタイプを作成し、そこにこのブランディング情報を入れることができます。

始める前に

必要なロール：sn_msi.workspace_manager

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
レポートテンプレートにブランディングを追加する際の主な考慮事項は次のとおりです。

- ヘッダーとフッターの画像をアップロードし、画像の位置を調整します。
- ヘッダーとフッターの画像の最大サイズ制限は 5 MB です。サイズが指定された制限を超えると、「画像の形式を認識できません (Image format cannot be recognized)」というエラーメッセージが重大なセキュリティインシデントに表示されます。
- ヘッダーとフッターの画像の高さを調整します。
- フッターのテキストの長さは 100 文字に制限されています。

手順

1. 次のように移動する。 **All** (すべて) > 重大セキュリティインシデント管理 > **MSI** 管理 > ステータスレポート設定.
2. ドリルダウン先 レポートテンプレート > 自社用カスタム設定.
3. [**Configure**] を選択します。
4. [新規] を選択して、レポートテンプレートにブランディングを追加します。
5. [ブランディングテンプレート] フォームのフィールドに入力します。
6. [送信] を選択します。
   新しいブランディングテンプレートが [ブランディングテンプレート] ページに作成されます。

レポートテンプレートでの可視化の使用

レポートウィジェットを使用して、データの可視化などのユーザーインターフェイスビルダー (UIB) 要素を定義して MSIM ステータスレポートに含めます。

始める前に
必要なロール：sn_msi.workspace_manager

手順

1. 次のように移動する。 **All** (すべて) > 重大セキュリティインシデント管理 > **MSI** 管理 > ステータスレポート設定.
   [MSI ステータスレポート設定] ページが表示されます。
2. ドリルダウン先 レポートテンプレート > 可視化.
3. [**Configure**] を選択します。
   以下は、ベースシステムの一部として事前定義された UIB の可視化です。これを使用して、ステータスレポートを設定および変更できます。

関連情報

可視化タイプ要素の作成

レポートテンプレートでのレポートリストの使用

レポートリストを使用して、関連リストアーティファクトを定義して含め、設定した MSI リストレコードに基づいて PDF 形式でリストを生成します。

始める前に
必要なロール：sn_msi.workspace_manager

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 重大セキュリティインシデント管理 > **MSI** 管理 > ステータスレポート設定.
   [MSI ステータスレポート設定] ページが表示されます。
2. ドリルダウン先 レポートテンプレート > **Lists** (リスト).
3. [**Configure**] を選択します。
   [MSI ステータスレポートリスト (MSI Status Reports Lists)] の各セクションに、インシデントの作成後に各関連リストが受ける影響が表示されます。以下は、ベースシステムの一部として事前定義された MSI レポートリストです。これを使用して、ステータスレポートを設定および変更できます。

関連情報

リストタイプの要素の作成

レポートテンプレートでのテンプレートスクリプトの使用

関連リストのデータや日付操作、その他の直接ドット連結できないデータを含めるスクリプトを作成します。

始める前に
必要なロール：sn_msi.workspace_manager

このタスクについて
レポートテンプレートを構成してカスタマイズした後、この事前定義されたテンプレートスクリプトを使用して、関連するデータをレポートテンプレートに含めることができます。

レポートテンプレートに関連リストのデータを表示するテンプレートスクリプトをビルドします。テンプレートスクリプトを使用して入力する場合は、タグテンプレートスクリプトのタグを ${template_script:script name} として追加する必要があります。

例：${template_script:msi_collab_cards}

> **注:**
> 事前定義されたテンプレートスクリプトは削除できません。レポートテンプレートがテンプレートスクリプトレコードにマッピングされている場合、そのレコードをアドミンロールを持つユーザーが削除しようとすると、エラーメッセージが表示されます。

手順

1. 次のように移動する。 重大セキュリティインシデント管理 > **MSI** 管理 > ステータスレポート設定.
   [MSI ステータスレポート設定] ページが表示されます。
2. ドリルダウン先 レポートテンプレート > テンプレートスクリプト.
3. [**Configure**] を選択します。
   以下は、ベースシステムの一部として事前定義されたテンプレートスクリプトです。これを使用して、ステータスレポートを設定および変更できます。

   > **注:**
   > リストにあるテンプレートスクリプトに加えて、関連リストのデータや日付操作、その他の直接ドット連結できないデータを含める独自のテンプレートスクリプトを作成することもできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レポートテンプレートのプレビュー

プレビュー機能を使用して設計時レポートテンプレートをプレビューし、実行時に 重大セキュリティインシデント管理 ワークスペースからレポートを生成して他のステークホルダーと共有します。

始める前に
必要なロール：sn_msi.workspace_manager

手順

1. 次のように移動する。 重大セキュリティインシデント管理 > **MSI** 管理 > ステータスレポート設定.
   [MSI ステータスレポート設定] ページが表示されます。
2. [レポートテンプレート] セクションで、[構成] を選択します。
3. 目的のレポートテンプレートを選択します。
4. 要件に基づいて、レポートタイプに [メール] または **[PDF]** を選択します。
5. [レポートの保存とプレビュー] アクションを選択します。

   [レポートをプレビュー] ダイアログボックスが表示されます。
6. 選択したテンプレートでレポートをプレビューするには、検索オプションを使用して重大なセキュリティインシデントを選択します。
7. [レポートをプレビュー] を選択します。
   レポートは、選択したテンプレート構成に従ってプレビューを生成します。レポートタイプに [メール] を選択した場合、プレビューはメールテンプレート形式になります。メール形式のステータスレポートはモバイル対応です。

レポートセクションテンプレートの作成

レポートはさらにさまざまなセクションに分割できます。レポートセクションを使用して、レポートを複数のセクションに分類して、順番に整理し直します。

始める前に
必要なロール：sn_msi.workspace_manager

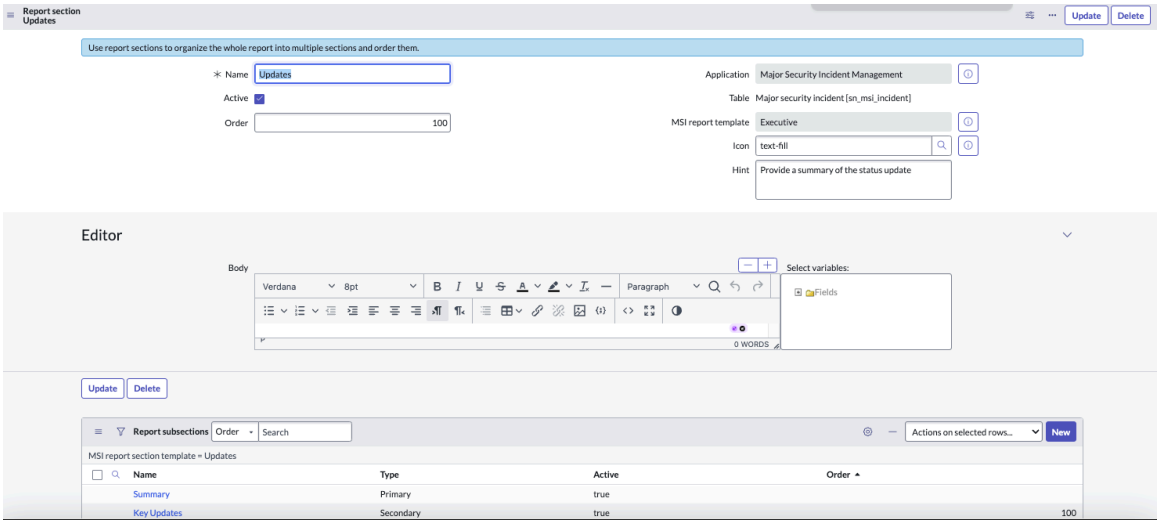
手順

1. 次のように移動する。 重大セキュリティインシデント管理 > **MSI** 管理 > ステータスレポート設定.
   [MSI ステータスレポート設定] ページが表示されます。
2. [レポートテンプレート] セクションで、[構成] を選択します。
3. 既存のレポートテンプレートを開きます。
4. 次のように移動する。 レポートサブセクション > 新規.
   新しいレポートセクションのページが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レポートセクションテンプレートの作成



5. [レポートセクションテンプレート] フォームのフィールドに入力します。

6. 新しいレポートテンプレートセクションを保存して、[送信] で送信します。

レポートサブセクションテンプレートの作成

レポートサブセクションを使用して、セクションをさらに複数のサブセクションに整理し、テキスト サイドパネル、プライマリ、セカンダリといった利用可能なタイプを使用して配置と位置を設定します。

始める前に
必要なロール：sn_msi.workspace_manager

手順

1. 次のように移動する。 重大セキュリティインシデント管理 > **MSI** 管理 > ステータスレポート設定.
[MSI ステータスレポート設定] ページが表示されます。

2. [レポートテンプレート] セクションで、[構成] を選択します。

3. 既存のレポートテンプレートを開き、それぞれの [レポートセクション] リストに移動します。

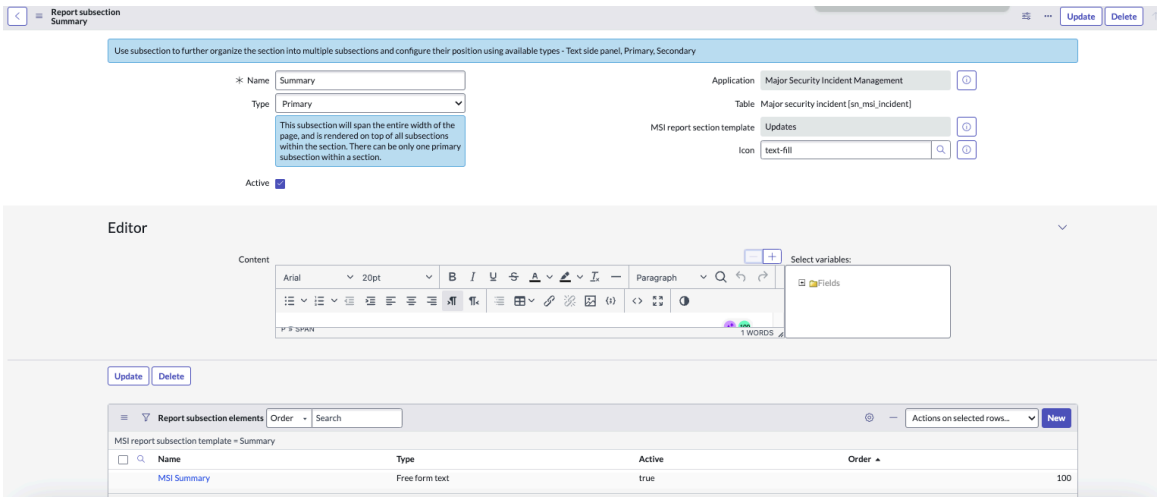
4. [レポートセクション] リストで、既存のレポートセクションテンプレートを開きます。

5. 次のように移動する。 レポートサブセクション > 新規.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レポートサブセクションテンプレートの作成



6. [レポートサブセクション] フォームのフィールドに入力します。

7. 新しいレポートテンプレートセクションを保存して、[送信] で送信します。

レポートサブセクション要素テンプレートの作成

サブセクション要素を使用して、サブセクションをさらに複数の要素に整理します。サブセクション要素によって、アサイン先グループやラベルなどのフィルターオプションで可視化やリスト、自由形式のテキストをより宣言的に定義できます。

始める前に
必要なロール：sn_msi.workspace_manager

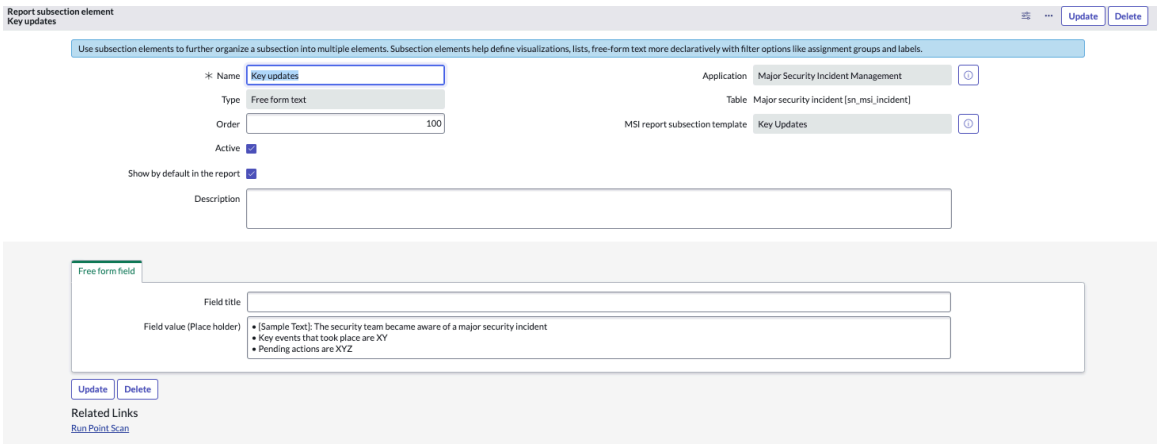
手順

1. 次のように移動する。 重大セキュリティインシデント管理 > **MSI** 管理 > ステータスレポート設定.
   [MSI ステータスレポート設定] ページが表示されます。
2. [レポートテンプレート] セクションで、[構成] を選択します。
3. 既存のレポートテンプレートを開き、それぞれの [レポートセクション] リストに移動します。
4. [レポートセクション] リストで、既存のレポートセクションテンプレートを開きます。
5. [レポートセクションテンプレート] リストで、既存のレポートサブセクションテンプレートを開きます。
6. 次のように移動する。 レポートサブセクション要素 > 新規.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レポートサブセクション要素テンプレートの作成



7. [レポートサブセクション要素] フォームのフィールドに入力します。

8. 新しいレポートテンプレートセクションを保存して、[更新] で更新します。

自由形式タイプの要素の作成

アサイン先グループやラベルなどのフィルターオプションを使用して、自由形式のテキストをより宣言的に定義する自由形式の要素タイプを作成します。

始める前に

必要なロール：sn_msi.workspace_manager

手順

1. 次のように移動する。 重大セキュリティインシデント管理 > **MSI** 管理 > ステータスレポート設定.
   [MSI ステータスレポート設定] ページが表示されます。
2. [レポートテンプレート] セクションで、[構成] を選択します。
3. 既存のレポートテンプレートを開き、それぞれの [レポートセクション] リストに移動します。
4. [レポートセクション] リストで、既存のレポートセクションテンプレートを開きます。
5. [レポートセクションテンプレート] リストで、既存のレポートサブセクションテンプレートを開きます。
6. 次のように移動する。 レポートサブセクション要素 > 新規.
7. レポートサブセクション要素テンプレートの作成 の説明のとおりに、レポートサブセクション要素フォームに必要な詳細情報を入力します。
8. レポートサブセクション要素の [タイプ] フィールドに移動して、[フリーフォームフィールド] オプションを選択します。
   これにより、[フリーフォームフィールド] セクションが表示されます。
9. [フリーフォーム] タブのフィールドに入力します。

可視化タイプ要素の作成

アサイン先グループやラベルなどのフィルターオプションを使用して、可視化要素をより宣言的に定義する可視化要素タイプを作成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

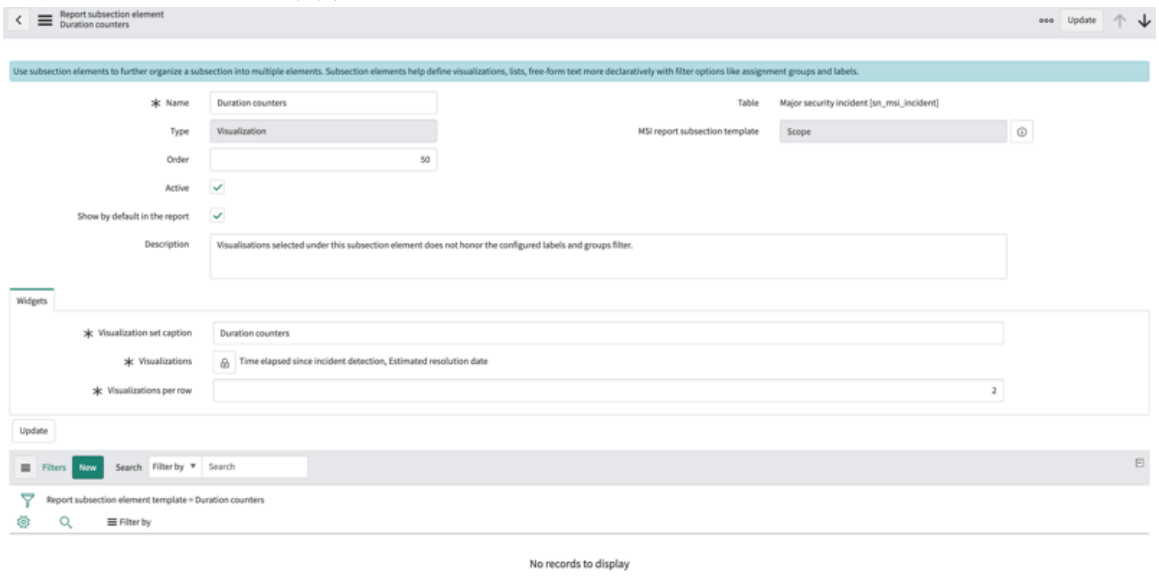
始める前に
必要なロール：sn_msi.workspace_manager

手順

1. 次のように移動する。 重大セキュリティインシデント管理 > **MSI** 管理 > ステータスレポート設定.
   [MSI ステータスレポート設定] ページが表示されます。
2. [レポートテンプレート] セクションで、[構成] を選択します。
3. 既存のレポートテンプレートを開き、それぞれの [レポートセクション] リストに移動します。
4. [レポートセクション] リストで、既存のレポートセクションテンプレートを開きます。
5. [レポートセクションテンプレート] リストで、既存のレポートサブセクションテンプレートを開きます。
6. 次のように移動する。 レポートサブセクション要素 > 新規.
7. レポートサブセクション要素テンプレートの作成 の説明のとおりに、レポートサブセクション要素フォームに必要な詳細情報を入力します。
8. レポートサブセクション要素の [タイプ] フィールドに移動して、[可視化] オプションを選択します。
   これで、[可視化] セクションが表示されます。
9. 可視化フォームのフィールドに入力します。
10. [送信] を選択します。

Example: 技術ステータスレポートのレポートテンプレートサブセクション要素のタイプ

レポートサブセクション要素のタイプ



リストタイプの要素の作成

アサイン先グループやラベルなどのフィルターオプションを使用して、関連リスト要素をより宣言的に定義するリストタイプ要素を作成します。

始める前に
必要なロール：sn_msi.workspace_manager

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 重大セキュリティインシデント管理 > **MSI** 管理 > ステータスレポート設定.
   [MSI ステータスレポート設定] ページが表示されます。
2. [レポートテンプレート] セクションで、[構成] を選択します。
3. 既存のレポートテンプレートを開き、それぞれの [レポートセクション] リストに移動します。
4. [レポートセクション] リストで、既存のレポートセクションテンプレートを開きます。
5. [レポートセクションテンプレート] リストで、既存のレポートサブセクションテンプレートを開きます。
6. 次のように移動する。 レポートサブセクション要素 > 新規.
7. レポートサブセクション要素テンプレートの作成 の説明のとおりに、レポートサブセクション要素フォームに必要な詳細情報を入力します。
8. レポートサブセクション要素の [タイプ] フィールドに移動して、[リスト] オプションを選択します。
   これにより、[リスト] セクションが表示されます。
9. リストフォームのフィールドに入力します。

カスタムタイプの要素の作成

アサイン先グループやラベルなどのフィルターオプションを使用して、関連リスト要素をより宣言的に定義するリストタイプ要素を作成します。

始める前に
必要なロール：sn_msi.workspace_manager

手順

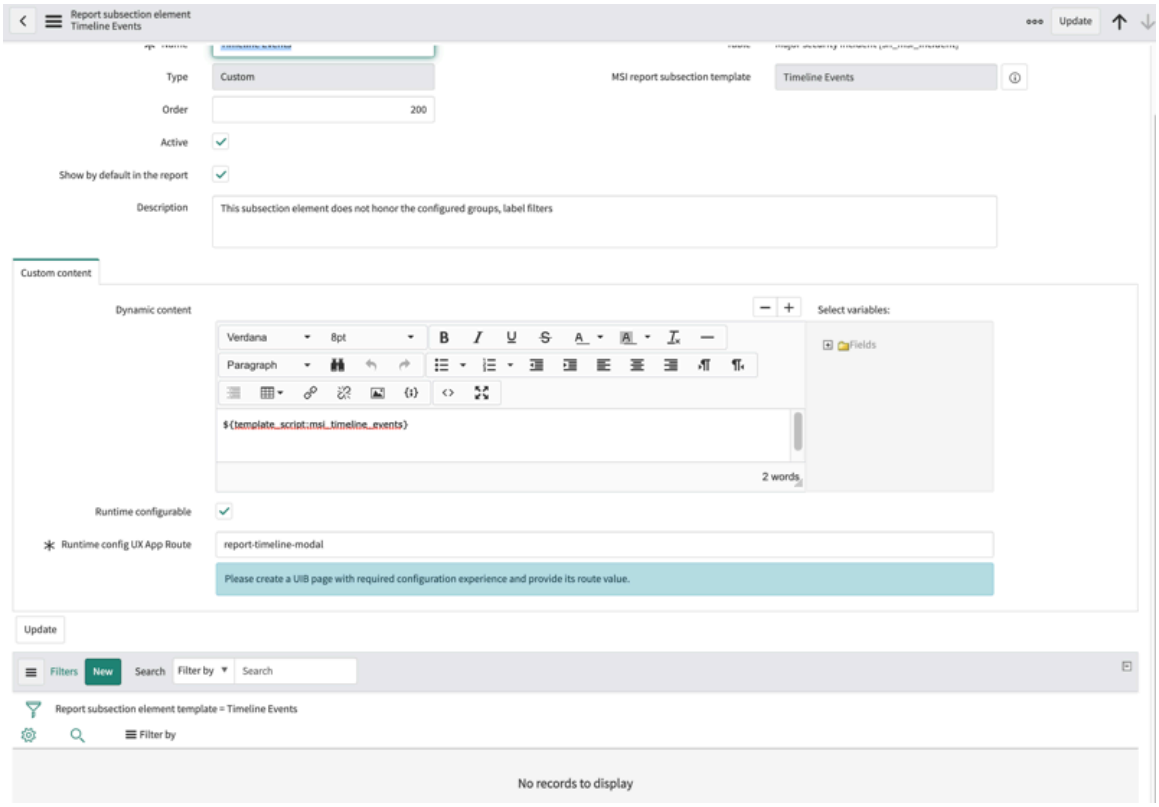
1. 次のように移動する。 重大セキュリティインシデント管理 > **MSI** 管理 > ステータスレポート設定.
   [MSI ステータスレポート設定] ページが表示されます。
2. [レポートテンプレート] セクションで、[構成] を選択します。
3. 既存のレポートテンプレートを開き、それぞれの [レポートセクション] リストに移動します。
4. [レポートセクション] リストで、既存のレポートセクションテンプレートを開きます。
5. [レポートセクションテンプレート] リストで、既存のレポートサブセクションテンプレートを開きます。
6. 次のように移動する。 レポートサブセクション要素 > 新規.
7. レポートサブセクション要素テンプレートの作成 の説明のとおりに、レポートサブセクション要素フォームに必要な詳細情報を入力します。
8. レポートサブセクション要素の [タイプ] フィールドに移動して、[カスタム] オプションを選択します。
   これにより、[カスタムコンテンツ] セクションが表示されます。
9. [カスタムコンテンツ] フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Example: 次は、技術ステータスレポートのレポートテンプレートサブセクション要素のタイプの例です。

レポートサブセクション要素のタイプ



システムのプロパティの追加

MSIM アプリケーションの動作を制御するシステムのプロパティを追加します。重大セキュリティインシデント管理 ステータスレポートの一部として導入されるデフォルトのシステムのプロパティは次のとおりです。

システムプロパティ

プロパティ名	説明
sn_msi.export_img	このプロパティを使用して、画像のエクスポートを制御します。デフォルトではオンに設定されています。
sn_msi.export_img_log	このプロパティを使用して、ブラウザーコンソールへのログインを有効にします。デフォルトではオフに設定されています。
sn_msi.export_img_parallel_threshold	このプロパティを使用して、レポートウィジェット構成から画像を生成する並列要求の最大数を制御します。デフォルト値は 14 に設定されています。
sn_msi.img_export_log	このプロパティを使用して、ブラウザーでのコンソールのログを有効にします。
sn_msi.img_export_poll_interval	このプロパティを使用して、画像が生成されるかどうかをチェックするポーリング間の時間差を制御します。デフォルトのポーリング時間間隔は 3000 ミリ秒に設定されています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システムプロパティ (続く)

プロパティ名	説明
sn_msi.export_poll_request_timeout	このプロパティを使用して、システムがエクスポートされた画像をポーリングできる最大時間を制御します。デフォルト値は 120000 ミリ秒です。
sn_msi.msi_report_uib_element_js_path	このプロパティを使用して、UIB ページ部分から画像をキャプチャするための汎用パスを制御します。
sn_msi.report_default_style_objects	このプロパティを使用して、フォントサイズ、フォントの色、フィールド値など、生成された PDF の CSS を変更します。たとえば、生成された PDF ステータスレポートの左パネルのフォントの色を sn_msi.workspace_manager が変更したいと思った場合、ワークスペースマネージャーはシステムのプロパティのフォントの色を変更して、目的のビューに PDF を表示できます。

重大セキュリティインシデント管理のプレイブック

重大セキュリティインシデント管理のプレイブックフローを自動または手動で呼び出すことができます。

プレイブックは、少なくとも 1 つのプレイブックがセキュリティインシデントに関連付けられている場合にのみ表示されます。プレイブックコンポーネントは、構築されたプロセスオートメーションデザイナー (PAD) でのみサポートされています。重大セキュリティインシデント管理は、法務要求プレイブックをベースシステムとともに提供します。

法務要求のプレイブック

法務要求プレイブックには、重大な違反に必要な 4 日間の期間内に SEC に通知できるように、MSI の最新の概要を法務部門に通知する方法についての詳細なガイダンスが記載されています。

概要

インシデントマネージャーは、法務要求プレイブックを使用して、MSI の最新のサマリーを法務部門に通知し、重大な違反を SEC に通知できるようにすることができます。プロセスオートメーションデザイナー (PAD) テンプレートを使用して、法務要求プレイブックの手順を実行し、法務部門に適宜通知できます。

このプレイブックは、重大なセキュリティインシデントが作成または更新された場合に使用できます。PAD で法務要求プレイブックをアクティブにしてから、分析、封じ込め、除去、レビューなどのすべてのタスクを実行する必要があります。

プロセス定義のレーンは次のとおりです。重大なセキュリティインシデントのステータスに対応しています。

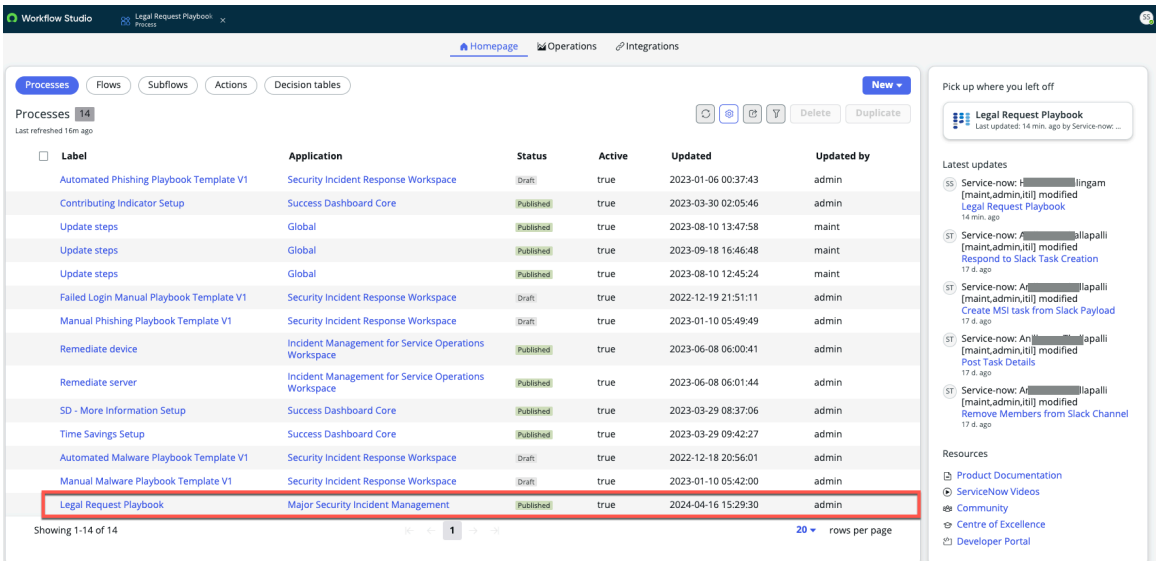
- 分析
- 封じ込め
- 根絶
- レビュー

各レーンには特定のアクティビティがあります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

法務要求のプレイブック



レーン内のタスクを完了としてマークすると、次のタスクに移動できます。タスクはいつでも保存でき、後でプレイブックに戻ることができます。レーン内のすべてのタスクを完了すると、次のレーンに移動できます。タスクとレーンを完了していくに伴い、ステータスが左側のパネルに反映されます。プレイブックの右側にあるアクティビティログには、各タスクに入力したすべてのデータが表示されます。

すべてのタスクを完了すると、すべてのレーンに入力した詳細を確認するように求められます。任意のフィールドを編集するか、[完了] を選択してエンタイトルメントの作成プロセスを完了することができます。

法務要求プレイブックのプロセスの作成

プロセスオートメーションデザイナー (PAD) で法務要求プレイブックのプロセスを作成するには、次の手順に従います。

始める前に
必要なロール：sn_msi.workspace_manager

手順

1. クリックします すべて > **Process Automation Designer** (プロセスオートメーションデザイナー) > > 新しいプロセスを作成する.

   例：法務要求プレイブック。

2. プロセスの名前、説明、およびプロセスを作成するアプリケーションを入力します。
3. [トリガーを選択] をクリックします。
4. [プロセスを実行する独自の条件を定義します] を選択し、プロセスを実行する必要があるタイミングに関するトリガー条件を選択します。
5. [トリガー条件を設定] をクリックします。
6. テーブルを選択して条件を入力することで、プロセスを実行する必要があるタイミングを定義する条件を選択します。
7. [デザイナーに移動] をクリックします。
   [プロセスオートメーションデザイナー] ページが開きます。
8. [新しいレーンを追加] をクリックして、自動プロセスの設計を開始します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レーンのプロパティペインが UI の右側に表示されます。

9. レーンのプロパティペインで、[名前]、[説明]、[実行条件]、および [開始時期を指定 **(Indicate when to start)]** の詳細を入力します。
   [実行条件] および [開始時期を指定 **(Indicate when to start)]** フィールドは、レーンがいつ実行されるかを示します。
10. [保存して閉じる] をクリックします。
11. 別のレーンを追加するには、[別のレーンを追加] をクリックします。
    同様に、必要な数のレーンを作成できます。この例では、それぞれ [分析]、[封じ込め]、[除去]、および [レビュー] のレーンを作成できます。次の例では、[分析] レーンはすぐに開始され、実行条件はありません。[封じ込め] レーンは前のレーンが完了した後に開始され、前のレーンのアクティビティの結果に基づく実行条件を持ちます。
    レーンを追加した後、各レーンのプロセスアクティビティを追加する必要があります。
12. 特定のレーン (分析レーンなど) で [別のプロセスアクティビティを追加] をクリックします。
    [アクティビティを追加] ポップアップが開きます。
    a. [アクティビティを追加] ポップアップで、必要なアクティビティ定義を選択します。
13. [新しいアクティビティを作成] をクリックします。
    アクティビティ定義を追加した後、レーンと同様にさらに構成できます。同様に、各レーンの下に他のプロセスアクティビティを作成できます。
14. [アクティビティのプロパティ] ペインで実行条件を追加し、プロセスアクティビティを開始するタイミングを指定します。
15. 実行条件を追加し、開始するタイミングを指定します。
    このアクティビティに必要なすべての入力 (構成されている自動化プランの入力を含む) が表示されます。値を上書きすることも、事前設定された値を使用することもできます。
16. [すべてのプロパティを表示] をクリックし、[詳細プロパティ] トグルを有効にすると、アクティビティ定義のすべてのアクティビティエクスペリエンスフィールドが表示されます。

法務要求プレイブックの使用

次のステップでは、MSIM ワークスペースでの法務要求プレイブックの使用方法とその機能について説明します。

始める前に

必要なロール：sn_msi.workspace_manager

手順

1. MSIM ワークスペースで、重大なセキュリティインシデントを開きます。
2. [プレイブック] タブを選択します。

   重大セキュリティインシデントに対して有効になっているプレイブックを表示できます。

   > **注:**
   > プレイブックがリストに表示されない場合は、PAD に移動して [プレイブック] タブで表示できるようにする必要があります。

3. [法務要求プレイブック] を選択します。
4. 各レーンをクリックして、このプレイブックによって実行されたタスクを確認します。
5. [分析] をクリックすると、[分析] フェーズで実行されたアクティビティのリストが表示されます。
   要件に応じて変更できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

6. 同様に、[封じ込め]、 [除去]、および [レビュー] をクリックして、それぞれのフェーズで実行されたアクティビティのリストを表示できます。
   要件に応じて変更できます。実行する必要があるアクティビティまたはユーザーアクションが残っている場合は、それぞれのフェーズに表示されます。
7. いずれかのフェーズで必要な残りのアクティビティまたはユーザーアクションがある場合は、それぞれのフェーズをクリックし、アクションを実行してアクティビティを完了します。

MSIM のロールアップフレームワーク

重大セキュリティインシデント管理 のワークスペースからソースレコードをリンクする機能を拡張します。

概要

ロールアップフレームワークでは、ロールアップフローの構成および拡張が可能になります。このフレームワークモデルを使用して、重大なセキュリティインシデントにロールアップできる情報を構成します。

以前は、 sn_msi.workspace_manager を持つユーザーが、MSI として提案または昇格されたセキュリティインシデントと脆弱性一致アイテムをリンクすることができました。セキュリティインシデントまたは脆弱性一致アイテムがリンクされた後、その情報は重大なセキュリティインシデントにロールアップされていました。ロールアップする必要のある情報のタイプは、スクリプトにハードコードされていました。

フレームワークモデルを使用すれば、次の機能をサポートし、アプリケーションの既存の問題にも対処するロールアップフローを構成できます。

ロールアップフレームワークモデルを使用することで、 sn_msi.workspace_manager を持つユーザーには次のようなメリットがあります。

- タスクテーブルを拡張する任意のテーブルでのリンクの追加や削除、MSI レコードの提案や昇格が可能になる。
- インシデントレコードでリンク/提案/昇格などのアクションを実行する際の、MSI にロールアップする情報のタイプの制御。
- クラシック環境と 重大セキュリティインシデント管理 ワークスペースの両方から行われる、セキュリティインシデント、修復タスク、およびすぐに利用可能なセキュリティケース (OOTB) のリンク、提案、または昇格をサポートします。

ロールアップフレームワークには、次の表で説明する構成が表示されます。

ロールアップフレームワークの構成

名前	説明
リンクされたレコード構成	重大セキュリティインシデント へのリンク、昇格、または提案に使用できるタスクテーブルの情報を保存します。
ロールアップレコードの構成	リンク、昇格、または提案のアクションが実行されたときにタスクテーブルからロールアップできる情報をキャプチャします。
レイアウト構成のリスト	重大セキュリティインシデント管理 ワークスペースのタブ ([インシデント影響度]、[リンクされたレコード]、[脅威インテリジェンス] など) に表示されるさまざまなテーブルのラベルとリストレイアウトを制御します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

重大セキュリティインシデント管理 でのリンクされたレコードの構成

[リンクされたレコード構成 (Linked Records Configuration)] を使用して、重大セキュリティインシデント へのリンク、昇格、または提案に使用できるタスクテーブルの情報を保存します。

必要なロール：admin および sn_msi.workspace_admin

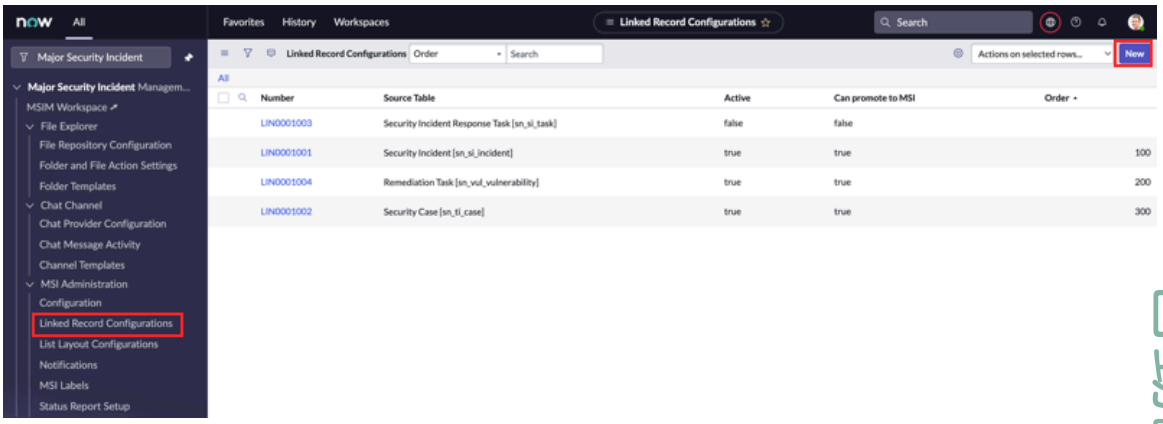
> **注:**
> アドミニストレーターはレコードを作成でき、MSIM ワークスペースアドミニストレーターはそのレコードを更新できます。

手順

1. 次のように移動する。 重大セキュリティインシデント管理 > リンクされたレコード構成.

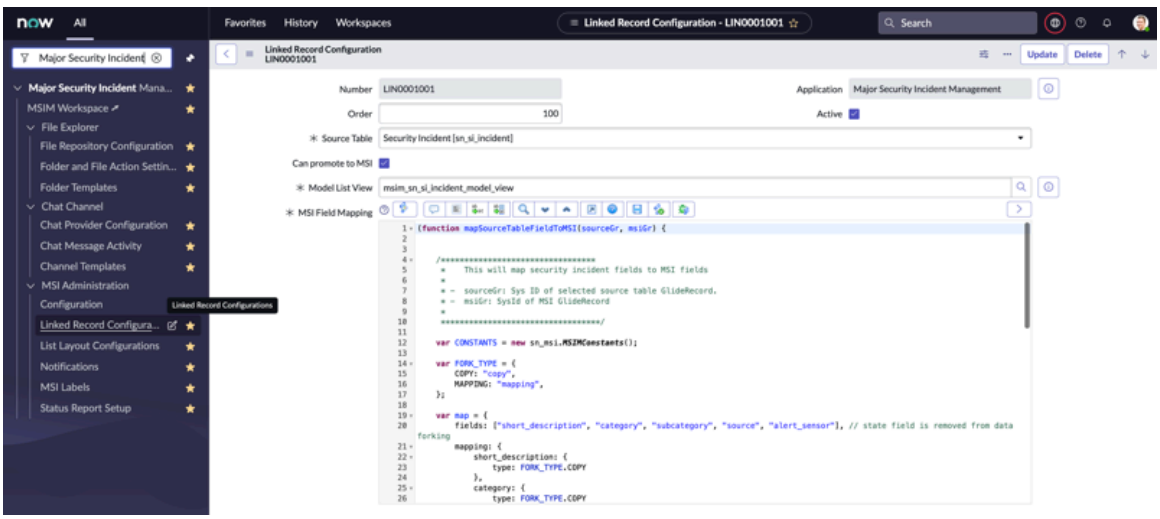
   [リンクされたレコード構成 (Linked Records Configuration)] ページが表示されます。

   リンクされたレコード構成



2. [リンクされたレコード構成 (Linked Record Configuration)] ページで、[新規] をクリックします。

> **注:**
> アプリケーションが 重大セキュリティインシデント管理 スコープになっていることを確認します。



3. レコード構成フォームの各フィールドに記入します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

リンクされたレコードのフィールドの説明

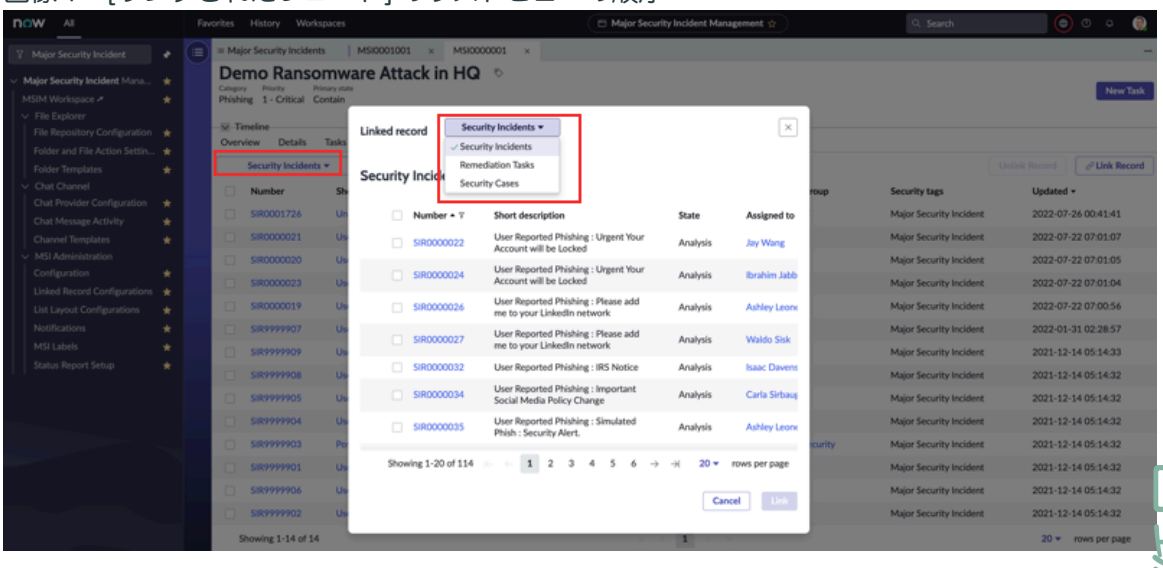
フィールド	説明
ソーステーブル	重大セキュリティインシデントにリンクしてロールアップする必要があるタスクテーブルを示します。
順序	MSIM ワークスペースのドロップダウンで、現在のソーステーブルの順序を制御できます。下に順序の例を示します。 この表の後に記載の画像 1 を参照してください。
モデルリストビュー (Model ListView)	[リンクされたレコードモーダル] リストに表示されるリストレイアウトを制御できるビューを選択します。
MSI に昇格可能	レコードがプライマリレコードかどうかを確認するには、このチェックボックスをオンにします。以下に、**[MSI** に昇格可能] オプションの選択例を示します。 この表の後に記載の画像 2 を参照してください。 このチェックボックスがオンで、値が true の場合は、次のようになります。 ○ 追加の構成でクラシック環境のアクションを使用して、ソースレコードを直接提案して重大セキュリティインシデント に昇格させることができます。 ○ クラシック環境と MSIM ワークスペースの両方から、ソースレコードを重大なセキュリティインシデントにリンクできます。 ○ 重大セキュリティインシデント管理 ワークスペースのリンクされたレコードページに、リンクされたソーステーブルレコードが表示されます。 **注:** レコードを 重大セキュリティインシデント として直接提案または昇格できる場合、そのレコードはプライマリレコードとなります。たとえば、セキュリティ応答タスクテーブル構成では、セキュリティ応答タスクを 重大セキュリティインシデント に直接昇格することはできないため、**[MSI** に昇格可能] の値は false です。したがって、MSIM ワークスペースのリンクされたレコードタブのドロップダウンリストには、そのレコードは表示されません。

自動翻訳

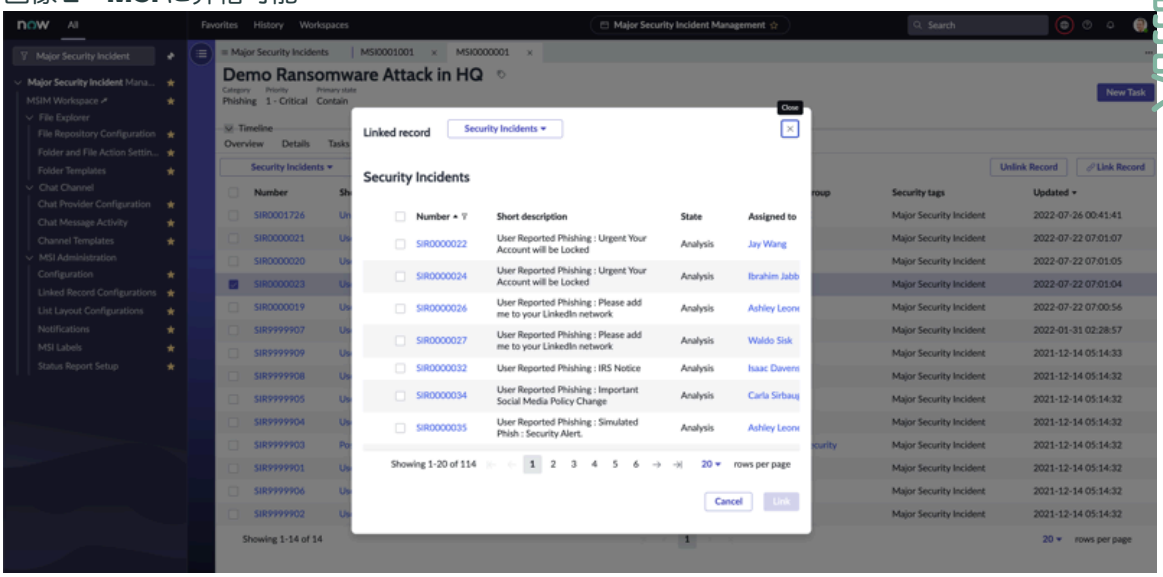
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
MSI フィールドマッピング	ソーステーブルレコードの提案中や昇格中に、ソースレコードのフィールドを新しく作成された重大なセキュリティインシデントにマッピングするスクリプトを作成します。 このスクリプトは、**[MSI** に昇格可能] の値が true の場合にのみ実行されます。

画像 1：[リンクされたレコード] のリストビューの順序



画像 2：**MSI** に昇格可能



重大セキュリティインシデント管理 でのロールアップレコードの構成

重大セキュリティインシデント管理 でロールアップレコードを構成して、ソースレコードが重大なセキュリティインシデントとしてリンク、提案、または昇格されるときにロールアップする情報を制御します。

必要なロール：admin および sn_msi.workspace_admin

自動翻訳

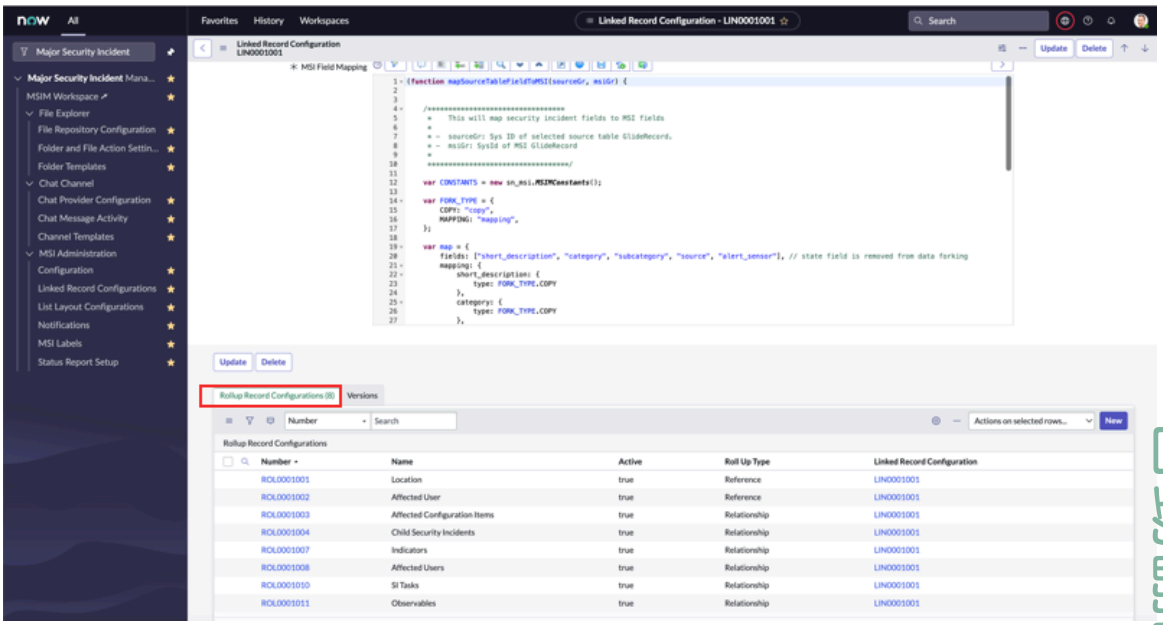
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
システムアドミニストレーターはレコードを作成でき、 MSI ワークスペースアドミニストレーターはレコードを更新できます。

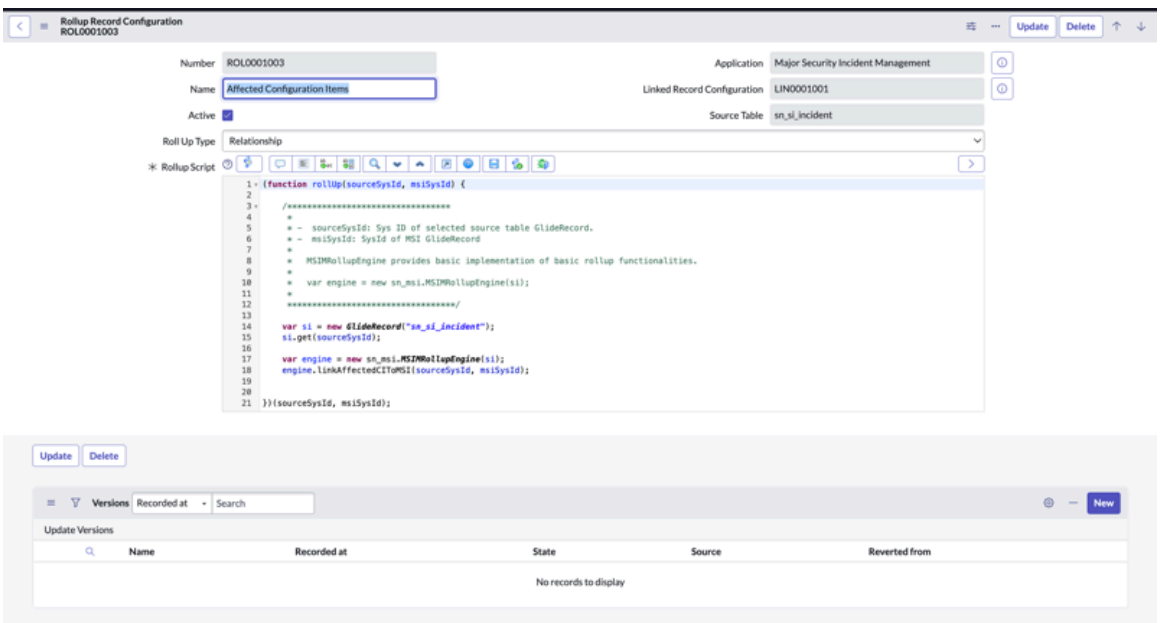
手順

1. 次のように移動する。 **Security Incident Response** > リンクされたレコード構成. [リンクされたレコード構成 (Linked Records Configuration)] ページが表示されます。
2. リンクされたレコードを選択または新規作成し、同じページから [ロールアップレコード構成 **(Roll up Record Configuration)]** セクションに移動します。

[ロールアップレコード構成 **(Roll up Record Configuration)]** セクション



3. [新規] をクリックします。



4. 設定ページで詳細を入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロールアップレコードの構成

フィールド名	フィールドの説明
名前	ロールアップレコードの名前を示します。
アクティブ	ソースレコードのロールアップが発生したときに現在の構成を実装するには、このチェックボックスをオンにします。
リンクされたレコード構成	親のリンクされたレコード構成を指す一意の番号を示します。ここは読み取り専用です。
ソーステーブル	リンクされたレコード構成で使用される読み取り専用のソーステーブル名。
ロールアップタイプ	ロールアップする必要がある情報のタイプを示します。 ○ 関係性：データを関連リストとして存在させる必要がある場合は、このオプションを選択します。 ○ 参照：データがソーステーブルのフォームに参照フィールドとして存在する場合は、このオプションを選択します。
ロールアップスクリプト	ロールアップタイプが [関係性] の場合、[ロールアップスクリプト] フィールドが有効になり、スクリプトを記述してここから情報をロールアップすることができます。 ここで、スクリプトは、ソースレコードと重大なセキュリティインシデントの情報を含む入力情報を受け取ります。関係テーブルから情報を検索してリンクされたレコード (sn_msi_m2m_child) テーブルにロールアップできるようにスクリプトを作成する必要があります。
ソースフィールド	ロールアップタイプが [参照] の場合、[ソースフィールド] が利用可能です。そのため、ロールアップする必要がある情報を含む [ソーステーブル] 参照フィールドが選択可能になります。
ターゲットフィールド	ロールアップタイプが [参照] の場合、[ターゲットフィールド] が利用可能です。そのため、リンクされたレコード (sn_msi_m2m_child) テーブルからフィールドを参照し、選択したソースフィールドとソーステーブルレコードに存在するデータを保存できます。

ロールアップ用のスクリプトの記述

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

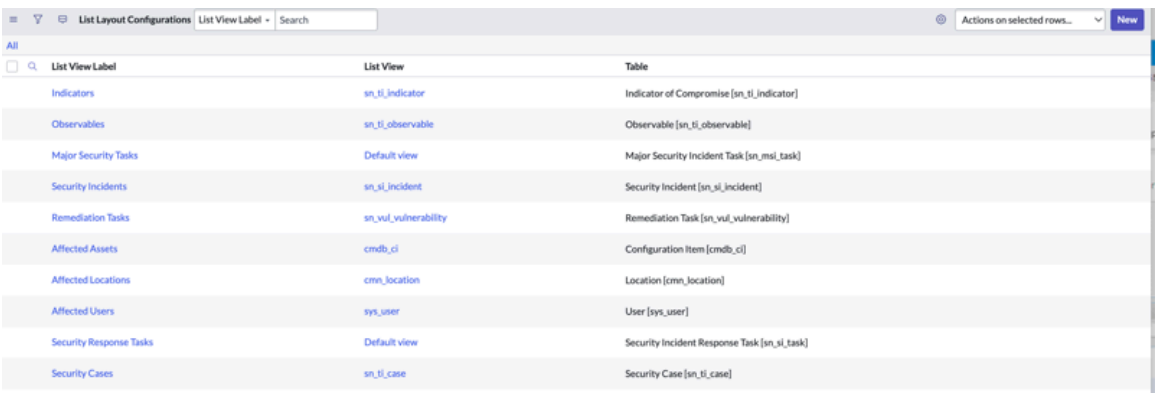
名前	説明
入力	• sourceSysId：リンク、提案、または昇格しようとしているソーステーブルレコードの Sys ID。 • msiSysId：ソースレコードをリンク、提案、または昇格する先の重大なセキュリティインシデントの Sys ID。
出力	出力される戻り値はありません。
責任	スクリプトは、リンクされたレコード (sn_msi_m2m_child) テーブルに情報をロールアップする必要があります。 • sourceSysID を使用して、ServiceNow 関係テーブルからデータを照会します。 • データが取得されたら、データをロールアップする MSIRollupEngine ユーティリティを使用して、リンクされたレコード (sn_msi_m2m_child) にデータをロールアップします。

重大セキュリティインシデント管理 でのリストレイアウトの構成

重大セキュリティインシデント管理 ワークスペースで使用されるレイアウトとラベル ([インシデントの影響度]、[リンクされたレコード]、[脅威インテリジェンス] タブなど) をカスタマイズするには、リストレイアウトを構成します。

必要なロール：admin および sn_msi.workspace_admin

注:
システムアドミニストレーターはレコードを作成でき、 MSI ワークスペースアドミニストレーターはレコードを更新できます。



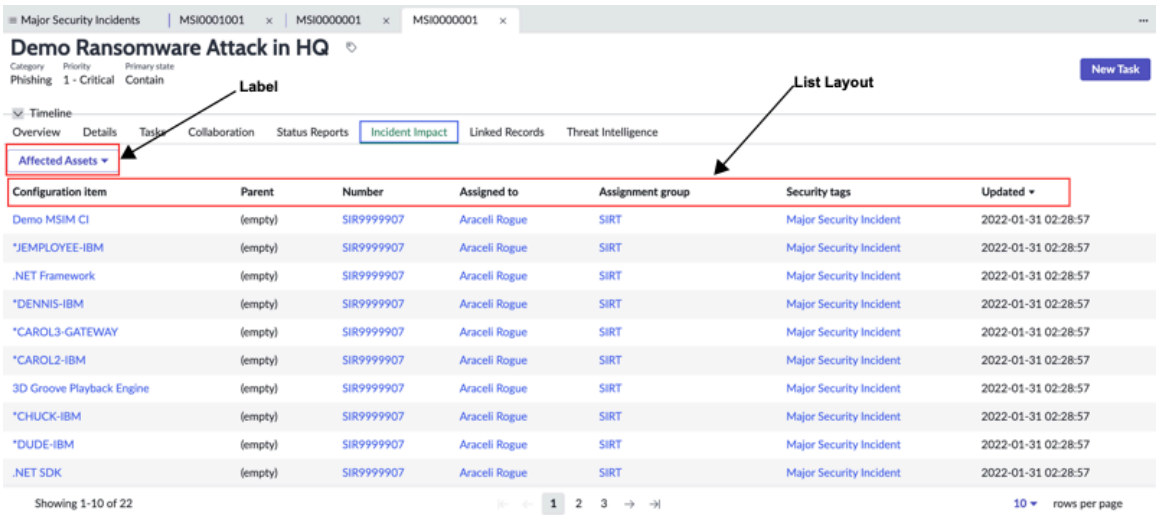
重大セキュリティインシデント管理 ワークスペースに表示される既存のテーブルについては、リストレイアウト構成が既に設定されています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:

- 既存のテーブルのカスタムビューを表示する場合は、リストレイアウト構成内のそれぞれのテーブルレコードをカスタムのリストビューで更新します。
- 新しいタスクテーブルの場合は、新しいリストレイアウト構成を作成して、カスタムのリストビューとラベルを表示します。この手順の詳細については、「ステップ 4：セキュリティケースの新しい [リンクされたレコード] タブのビューを作成する」を参照してください。



自動翻訳

セキュリティケースのユースケース実装のロールアップ例

次の手順で、セキュリティケーステーブルの重大なセキュリティインシデントにリンク、提案、または昇格するためのサポートを追加する方法のユースケースについて、例を挙げて説明します。

- ステップ 1：セキュリティケースのリンクされたレコード構成の作成
- ステップ 2. セキュリティケースのモーダルウィンドウのビューの作成
- ステップ 3：セキュリティケースのソーステーブルの UI アクションの作成
- ステップ 4：セキュリティケースの新しい [リンクされたレコード] タブのビューを作成する
- ステップ 5. 重大セキュリティインシデント管理 ワークスペースユーザーのアクセス制御リスト (ACL) を追加する
- ステップ 6：セキュリティケースのビジネスルールの作成
- ステップ 7. ロールアップレコードの構成の作成

ステップ 1：セキュリティケースのリンクされたレコード構成の作成

セキュリティケースのリンクされたレコード構成を作成します。

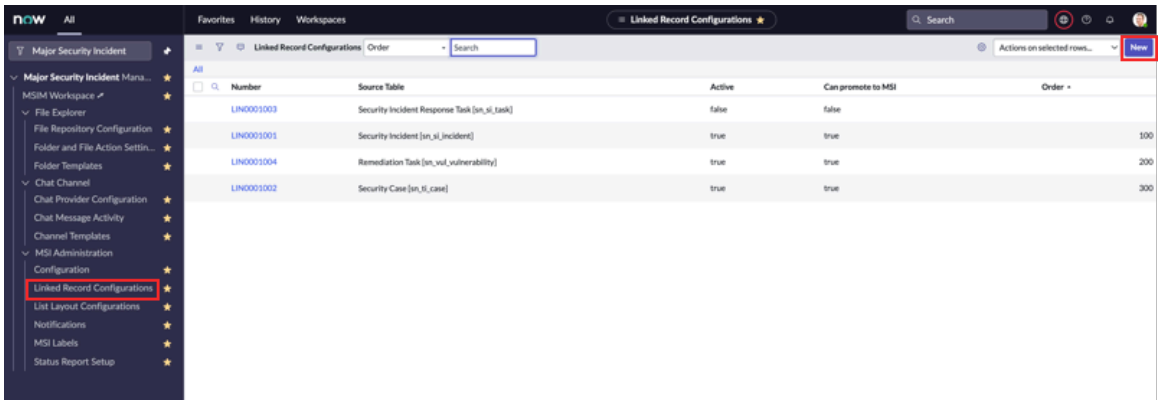
始める前に
必要なロール：admin および sn_msi.workspace_admin

注:
システムアドミニストレーターはレコードを作成でき、 MSI ワークスペースアドミニストレーターはレコードを更新できます。

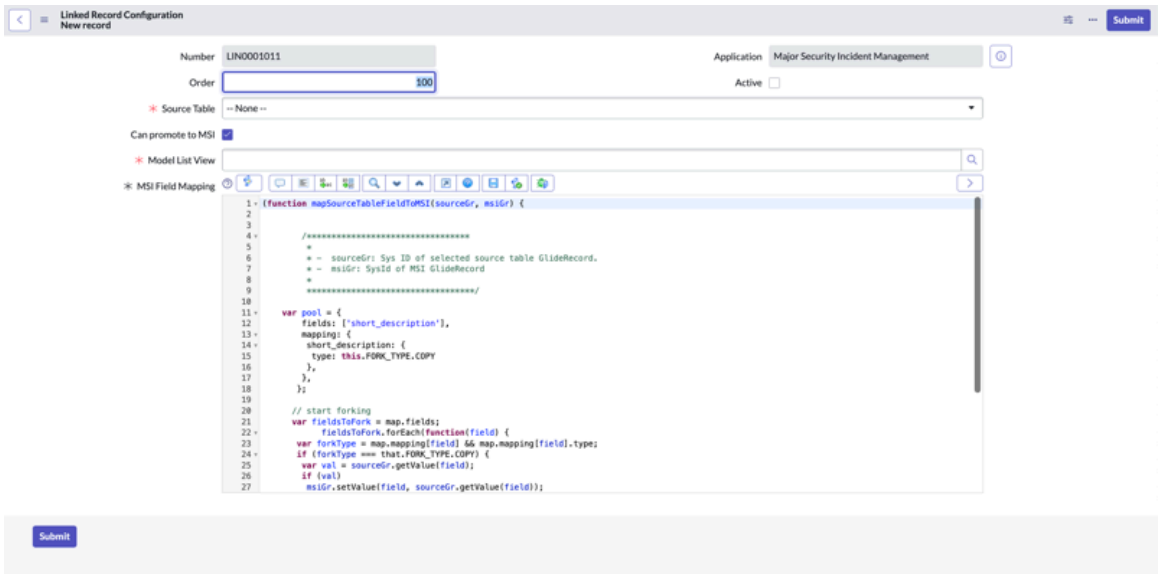
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 左側のナビゲーションから、[リンクされたレコード構成 (Linked Records Configuration)] を検索します。
2. [新規] をクリックします。

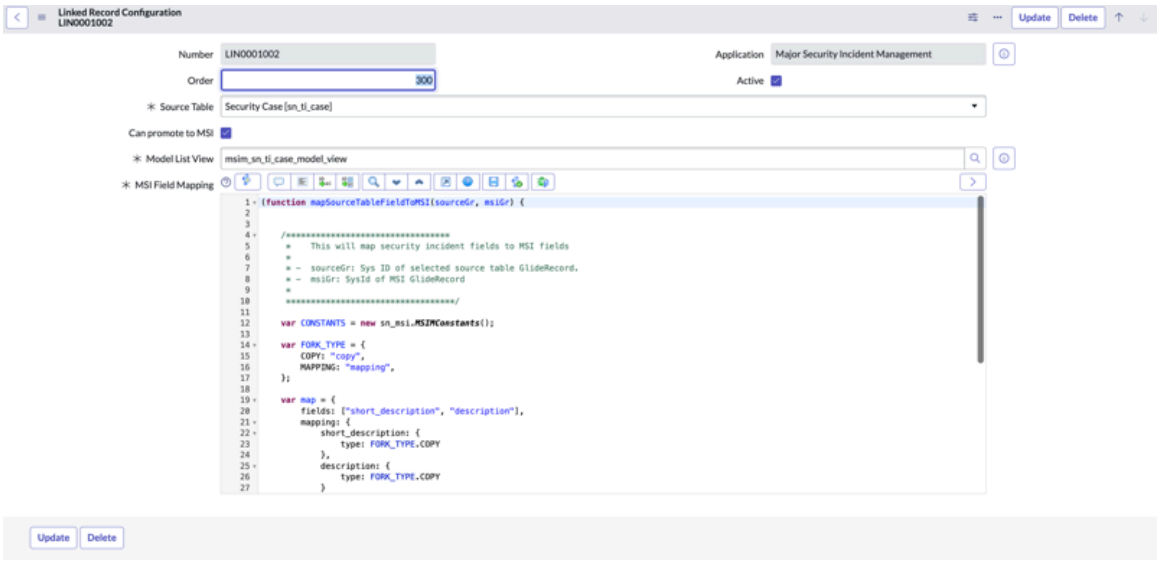


3. 必要な列をフォームに入力し、フィールドマッピングスクリプトを記述します。



4. これで、次の表に示す値を追加して、セキュリティケースのリンクされたレコード構成を作成できました。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



名前	説明
ソーステーブル	セキュリティケース (sn_ti_case)。この例では、セキュリティケースを MSI としてリンク、昇格、または提案します。
順序	入力値：300 **注:** 順序の値が低いものが高いものよりも優先されます。[セキュリティケース] は、[セキュリティインシデント] や [修復タスク] よりも順序が高いため、最後に表示されます。
MSI に昇格可能	セキュリティケースを MSI に昇格させるには、このチェックボックスをオンにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

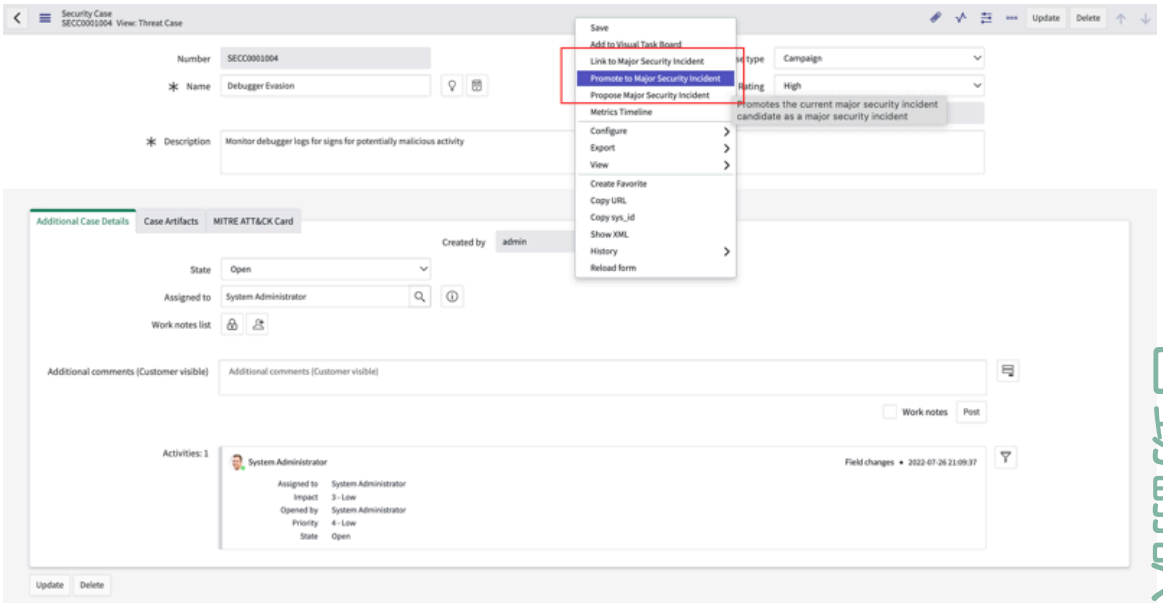
名前	説明
	注: ○ 重大なセキュリティインシデントへのセキュリティケースレコードのリンクおよびリンク解除は、どちらも 重大セキュリティインシデント管理 ワークスペースから行います。また、レコードのリンク解除機能は、リンクされたレコードに対してのみ表示されます。 ▪ これにより、クラシック環境のアクションを使用してセキュリティケースから重大なセキュリティインシデントへリンク、昇格、および提案することが可能になりますが、これらの UI アクションは導入後すぐに使用することはできません。UI アクションはそれぞれ手動で作成する必要があります。詳細については、「ステップ 3：セキュリティケースのソーステーブルの UI アクションの作成」を参照してください。 ▪ セキュリティインシデント、修復タスク、およびセキュリティケースでは、リンク、昇格、および提案の UI アクションをすぐに使用できます。 ○ MSIM ワークスペースのリンクされたレコードページに、リンクされたセキュリティケースレコードが表示されます。 このチェックボックスをオンにした後に利用可能なオプションを確認するには、下の画像 1 を参照してください。
モーダルリストビュー	msim_sn_ti_case_model_view 注: このビューには、MSIM ワークスペースの [リンクレコード] モーダルのリストビューに表示されるフィールドとフィールドの順序が表示されます。詳細については、「ステップ 2. セキュリティケースのモーダルウィンドウのビューの作成」を参照してください。 [リンクされたレコード] ページから確認するには、下の画像 2 を参照してください。
フィールドマッピングスクリプト	このスクリプトは、ソーステーブルレコードの提案中や昇格中に、新しく作成された重大なセキュリティインシデントにソーステーブルレコードのフィールドがマッピングされることを記述したものです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

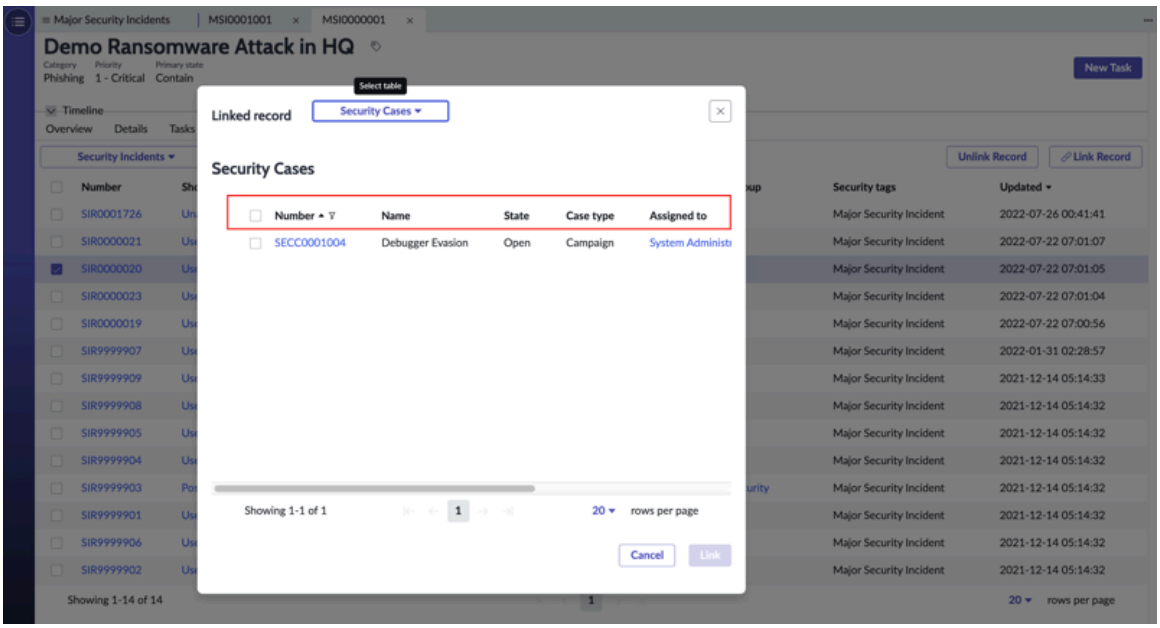
自動翻訳

名前	説明
	受け取る入力は次のとおりです。 ○ sourceGr：セキュリティケースの Glide レコードオブジェクト ○ msiGr：重大なセキュリティインシデントの Glide レコードオブジェクト スクリプトはセキュリティケースの簡単な説明を読み込み、重大なセキュリティインシデントにタイトルとしてコピーします。

画像 1：**MSI** に昇格可能



画像 2：モーダルビュー



ステップ **2.** セキュリティケースのモーダルウィンドウのビューの作成

セキュリティケースのモーダルウィンドウのビューを作成します。

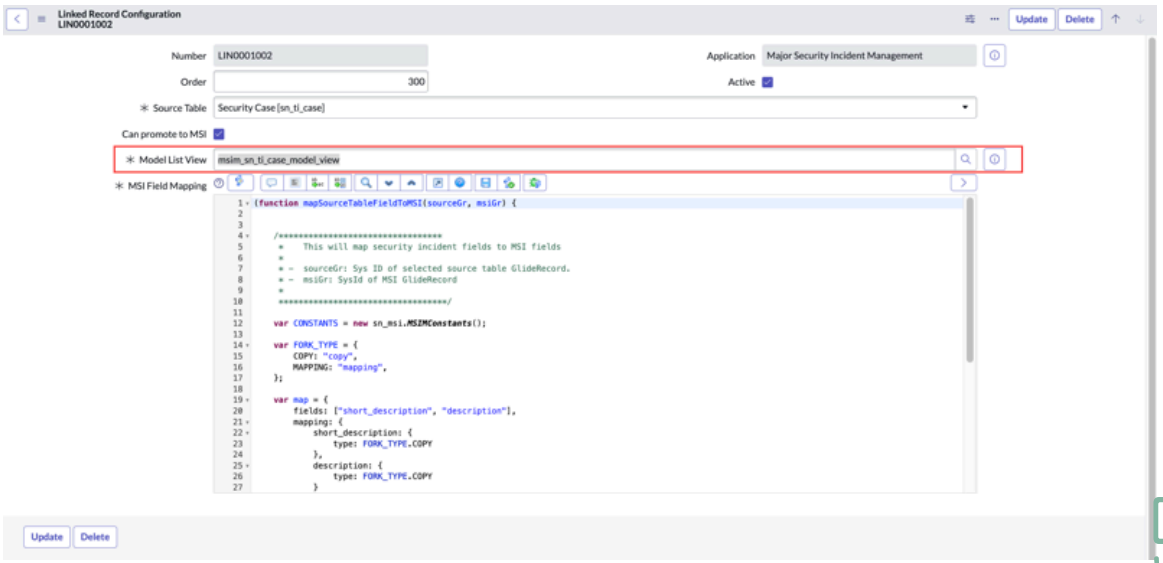
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
主な考慮事項：

- デフォルトでは、リンクされたレコードのモーダルリストにはデフォルトのリストレイアウトのみが表示されます。リストレイアウトをカスタマイズする場合は、ソーステーブルの [カスタムビュー] を使用してカスタマイズできます。
- カスタムビューを表示する場合は、ソーステーブルの [リンクされたレコード構成] でもカスタムビューを選択する必要があります。

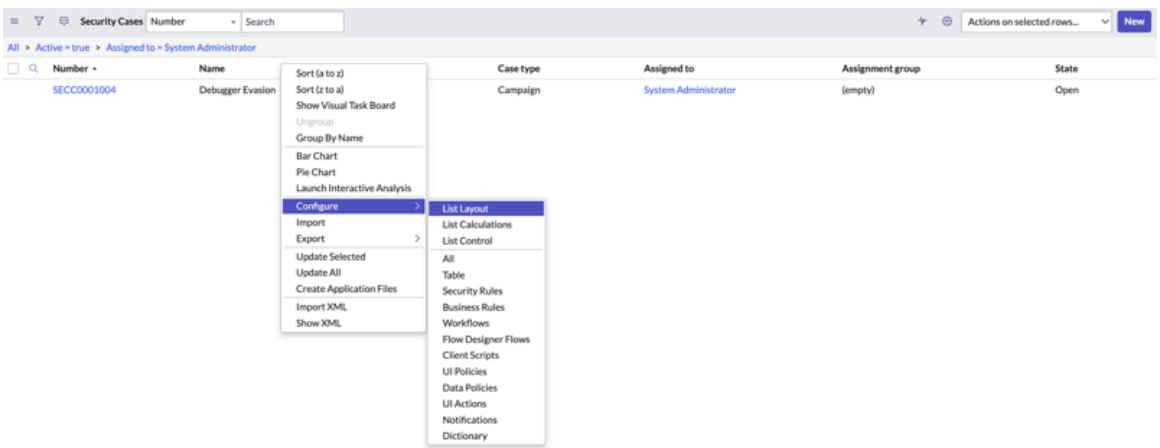
ソーステーブルの [リンクされたレコード構成] モーダルビュー



必要なロール：admin

手順

1. ソーステーブルに移動し、 構成 > リストレイアウト.



2. 検索項目 リストビュー > ビュー名.
3. [ビュー名] ドロップダウンリストで [新規] をクリックし、新しいビュー (msim_sn_ti_case_modal_view など) を作成します。
4. 新しく作成したビューを選択します。
選択すると、使用可能なリストから必要なフィールドを選択できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. **[Save** (保存)] をクリックします。
6. 次のように移動する。 メニュー > ビュー をクリックして、ビューが正しくレンダリングされたかどうかを確認します。

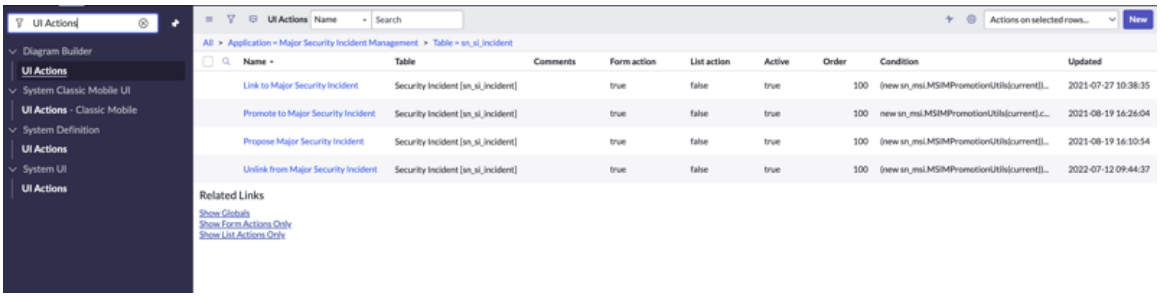
ステップ 3：セキュリティケースのソーステーブルの **UI** アクションの作成

セキュリティケースのソーステーブルの UI アクションを作成します。

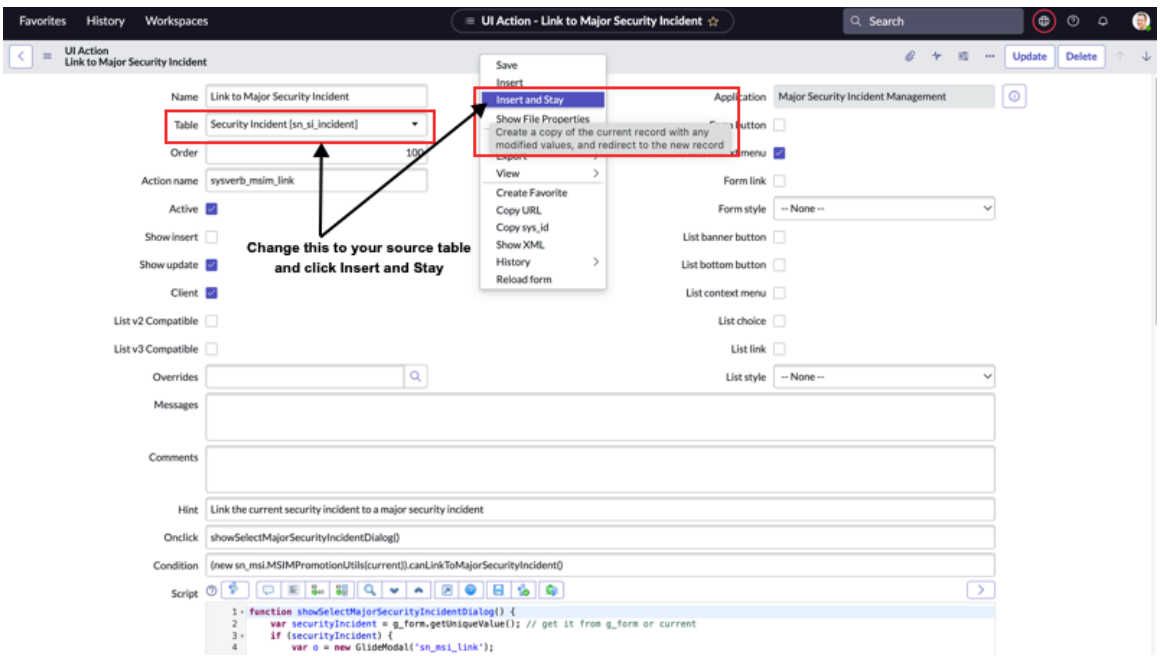
始める前に
必要なロール：admin

手順

1. 次のように移動する。 システム定義 > **UI** アクション.
2. [フィルター] オプションを実行し、[アプリケーション] を「重大セキュリティインシデント管理」、[テーブル] を「sn_si_incident」でリストをフィルタリングします。



3. UI アクションを 1 つずつ選択し、ソーステーブルの詳細を保存します。



4. 次の UI アクションについて、上記と同じ手順を繰り返します。
   - 重大なセキュリティインシデントへのリンク
   - 重大なセキュリティインシデントを提案
   - 重大なセキュリティインシデントからリンク解除
   - 重大なセキュリティインシデントに昇格

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

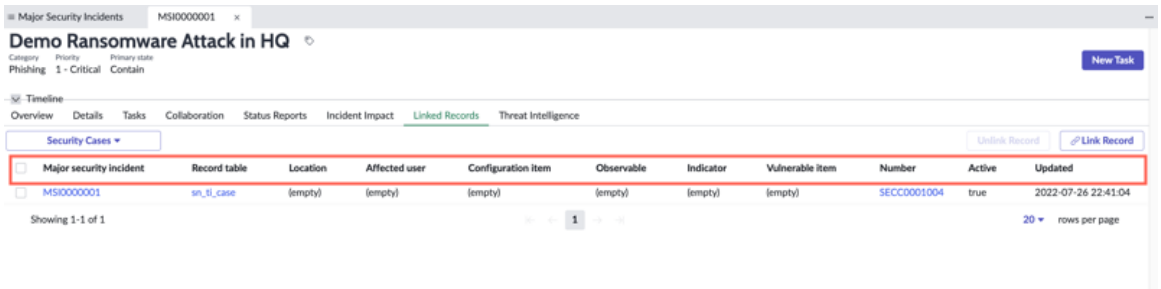
自動翻訳

ステップ 4：セキュリティケースの新しい [リンクされたレコード] タブのビューを作成する

重大セキュリティインシデント管理 ワークスペースで、[リンクされたレコード] ページに表示される [セキュリティケース] テーブルのリストレイアウトをカスタマイズします。

始める前に
必須条件：

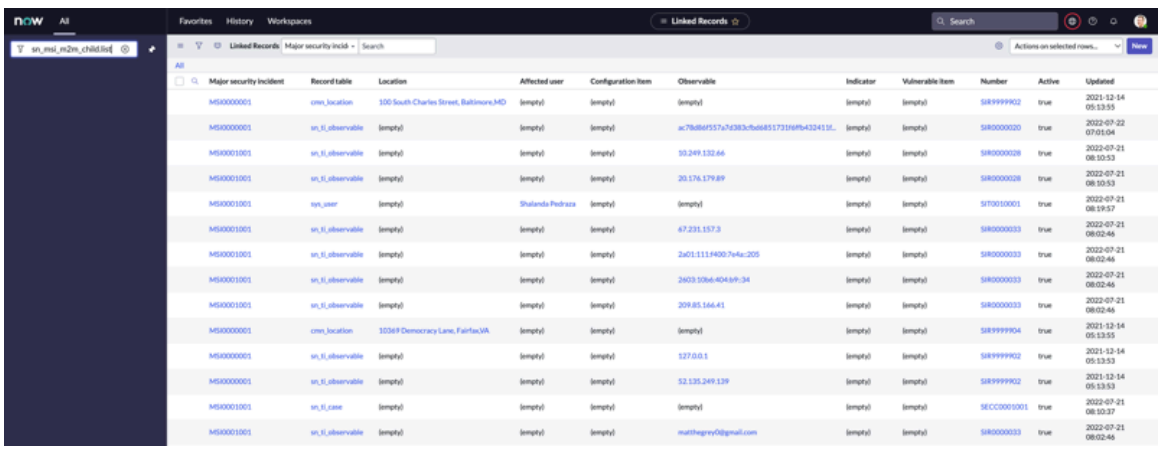
- [セキュリティケース] テーブルのリストの作成時に表示する列を選択します。
- ドロップダウンリストに表示するフィールドの順序を選択します。



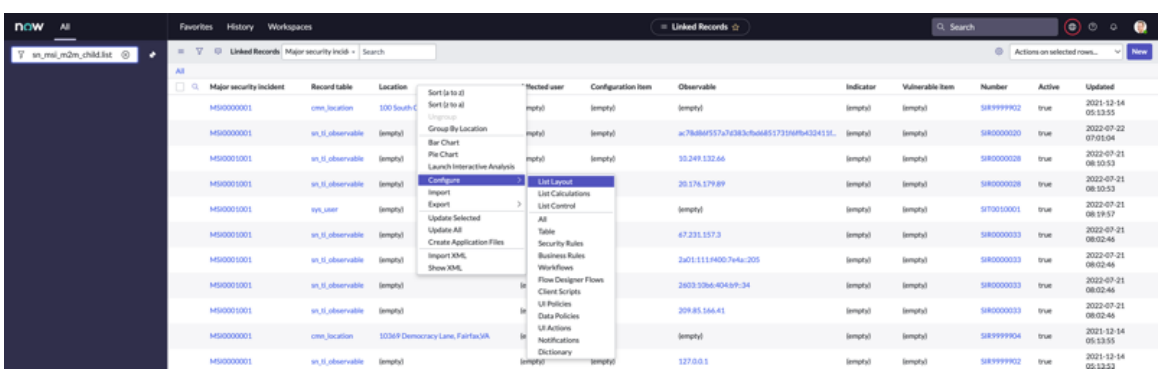
必要なロール：admin

手順

1. 左側のナビゲーションを使用して、**sn_msi_m2m_child** を検索します。
   [リンクされたレコード] テーブルが表示されます。

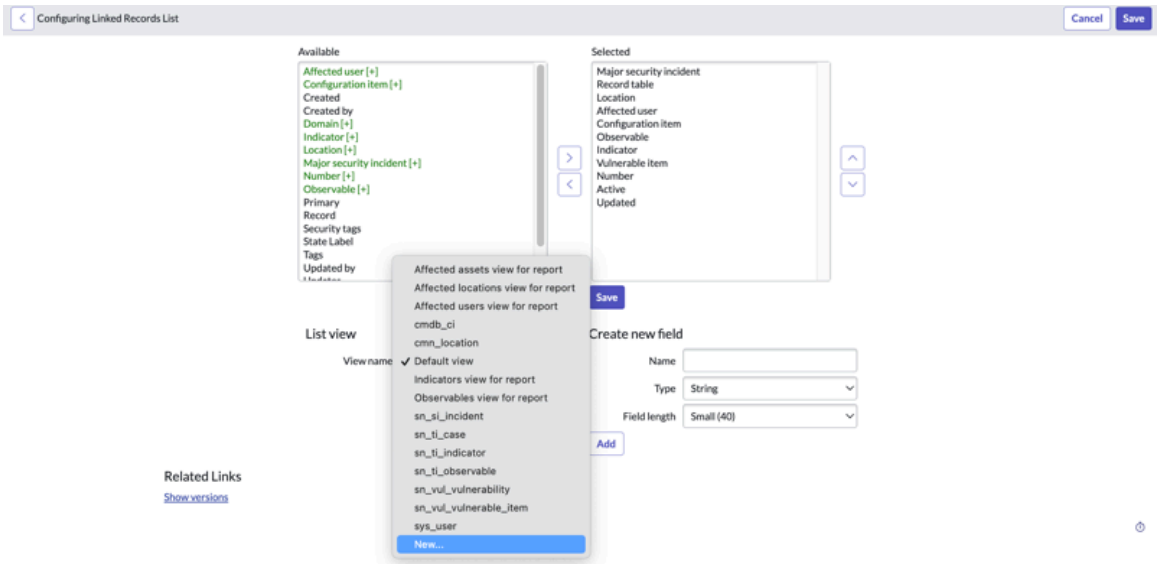


2. ヘッダーを右クリックし、 構成 > リストレイアウト.
   [リンクされたレコードリストの構成 (Configuring Linked Records List)] ページが表示されます。

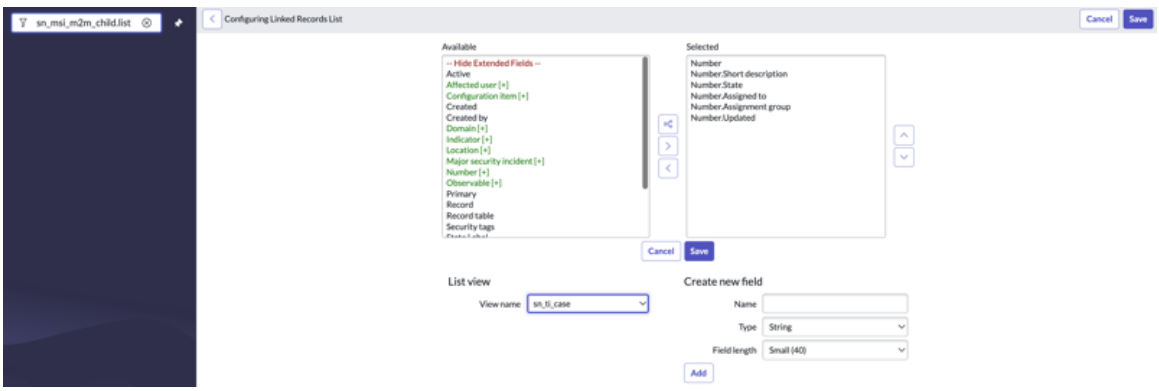


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

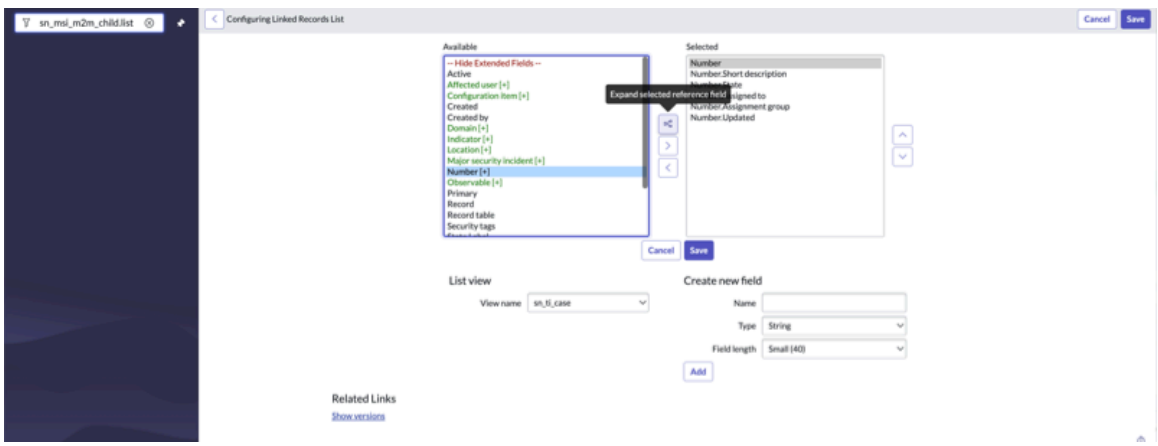
3. 検索項目 リストビュー > ビュー名.
4. [ビュー名] ドロップダウンリストから [新規] を選択します。



5. ワークスペースのリストビューに表示する列を選択します。
   セキュリティケースレコードは [番号] 列に保存されます。セキュリティケースから情報を表示するには、[番号] 列をドット連結する必要があります。



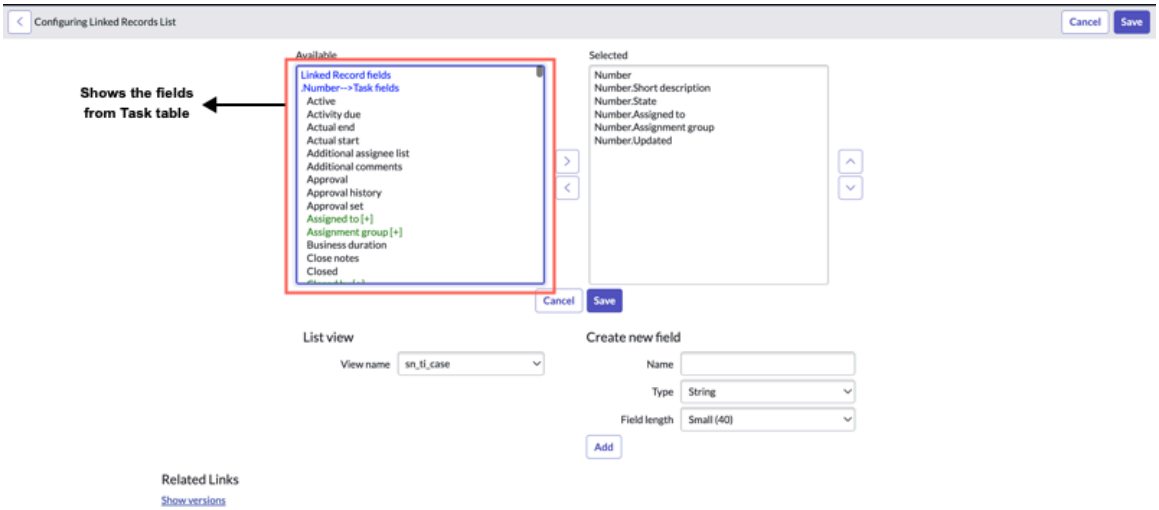
   a. ドット連結を行うには、まず使用可能なリストから [番号] 列を選択し、次に [選択した参照フィールドを展開] をクリックします。



   b. [番号] から列を展開して選択し、[選択済み] リストに移動します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳



c. [保存] をクリックして保存し、ビューを作成します。

6. 次のステップでは、重大セキュリティインシデント管理 ワークスペース内で作成したビューを表示するため、リストレイアウト構成を作成する必要があります。

a. 左側のナビゲーションを使用して、[レイアウト構成のリスト] を検索します。

b. クリックします **MSI** 管理 > レイアウト構成のリスト.

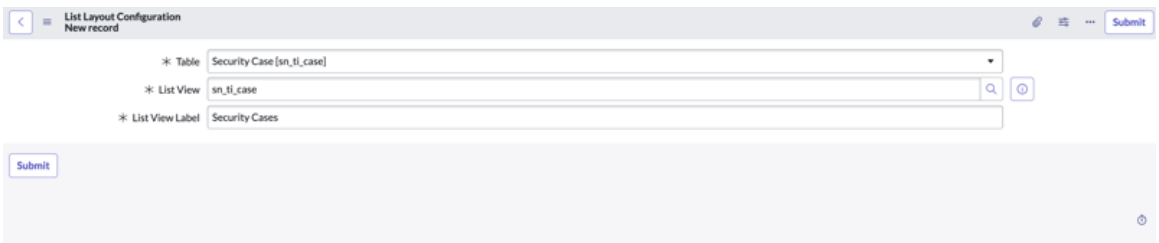
c. [新規] をクリックして、新しい構成を作成します。

d. [テーブル] 列からソーステーブルを選択し、[リストビュー] フィールドから新しく作成されたビューを選択します。

e. [リストビュー] ラベルを使用すると、同じソーステーブルが 重大セキュリティインシデント管理 ワークスペースに表示されるときのラベルを制御できます。

f. [保存] をクリックしてレコードを保存します。

> **注:**
> レコードの保存後、重大セキュリティインシデント管理 ワークスペースに移動すると、作成されたリストビューとラベルがワークスペース内に表示されます。



ステップ **5.** 重大セキュリティインシデント管理 ワークスペースユーザーのアクセス制御リスト **(ACL)** を追加する

重大セキュリティインシデント管理 ワークスペースユーザーのアクセス制御リスト (ACL) を追加します。

始める前に

必要なロール：admin

> **注:**
> 機能のリンクおよびリンク解除に必要な権限は、sn_msi.linkedsivi_read ロールによって制御されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

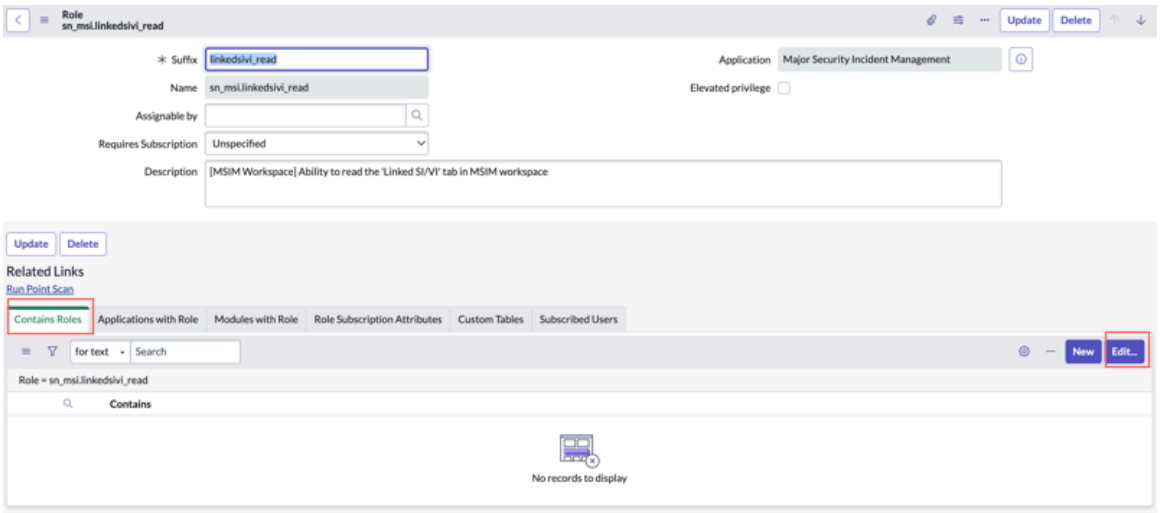
重大セキュリティインシデント管理 ペルソナには sn_msi.linkedsivi_read ロールが含まれています。

1. sn_msi.workspace_admin (MSIM ワークスペースアドミニストレーター)
2. sn_msi.workspace_manager (MSIM ワークスペースマネージャー)
3. sn_msi.workspace_responder (MSIM ワークスペースレスポンダー)

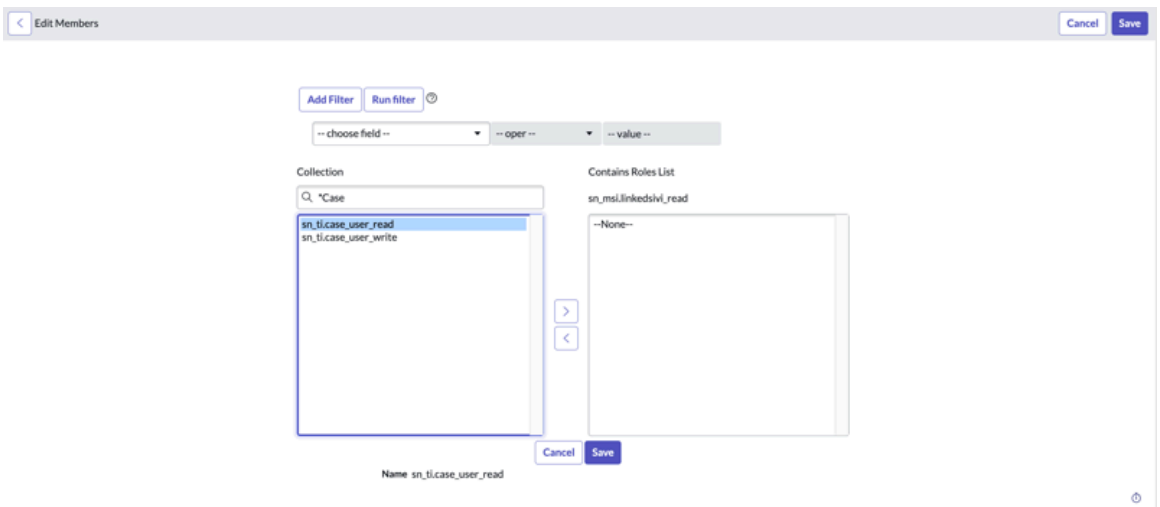
> **注:**
> どのソーステーブルについても、必要なロールが sn_msi.linkedsivi_read ロールに追加されていることを確認する必要があります。

手順

1. 次のように移動する。 ユーザー管理 **(User Administration)** > ロール をクリックし、**sn_msi.linkedsivi_read** ロールを検索します。
2. [ロールを含む] 関連リストセクションで、[編集] をクリックします。



3. [ロールを含む] セクションにソーステーブルのロールが追加されていることを確認します。
セキュリティケースに必要なロールを設定するための [メンバーの編集] ページが表示されます。



4. [コレクション] セクションでソーステーブルのロールを検索します。
セキュリティケースのソーステーブルに対する読み取りおよび書き込みアクセスを許可するために必要なロールを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:

- セキュリティケースには、読み取りと書き込みのための 2 つのロールが別個に必要です。
- 重大セキュリティインシデント管理 ワークスペースにリンクされたレコードモーダルからソースレコードを選択するための、テーブルに対する書き込みアクセス権。

5. [保存] をクリックしてロールを追加します。
6. [含まれるロール] 関連リストセクションにロールが正常に追加されていることを確認します。

ステップ 6：セキュリティケースのビジネスルールの作成

セキュリティケースの必要なビジネスルールを作成します。

始める前に
必要なロール：admin

新しいソーステーブルのセキュリティケース (sn_ti_case) に対して、次の 3 つのビジネスルールを作成します。これらのビジネスルールは、セキュリティインシデント (sn_si_incident) などのすぐに利用可能なソーステーブルで動作の一貫性を維持するために必要です。

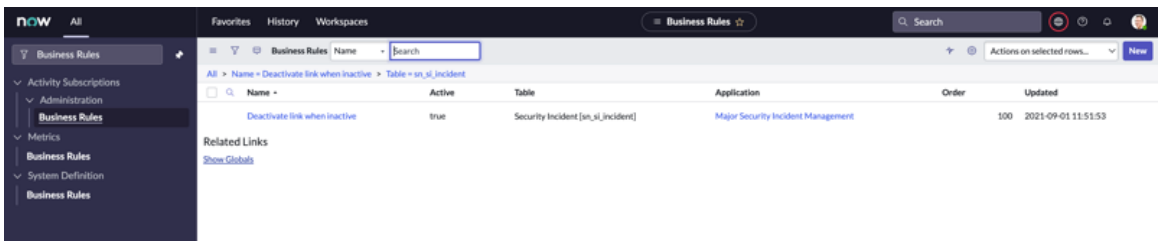
新しいソーステーブルのビジネスルール：

1. 非アクティブ時にリンクを非アクティブ化：セキュリティケースがクローズされると、関連情報が重大セキュリティインシデント管理 ワークスペースページに表示されなくなる。
2. 更新時にチーム情報を同期：[重大なセキュリティインシデントの詳細] タブに、さまざまなタスクで作業中のすべてのアクティブなチームとユーザーに関する情報が表示される。セキュリティケースのアサイン先ユーザーやアサイン先グループが変更されたときに、重大なセキュリティインシデントのアクティブチームセクションでセキュリティケースのチーム情報を更新する必要がある。これらのビジネスルールによって、アクティブチームセクションの新しいアサイン先ユーザーとアサイン先グループが更新される。
3. 削除時にチーム情報を同期：[重大なセキュリティインシデントの詳細 (Major Security Incident details)] タブに、さまざまなタスクで作業中のすべてのアクティブなチームとユーザーに関する情報が表示される。セキュリティケースがクローズされると、重大なセキュリティインシデントのアクティブチームセクションにセキュリティケースのチーム情報を表示する必要がなくなる。これらのビジネスルールによって、アサイン先ユーザーとアサイン先グループがアクティブチームから削除される。

新しいソーステーブルでのビジネスルールの作成：

手順

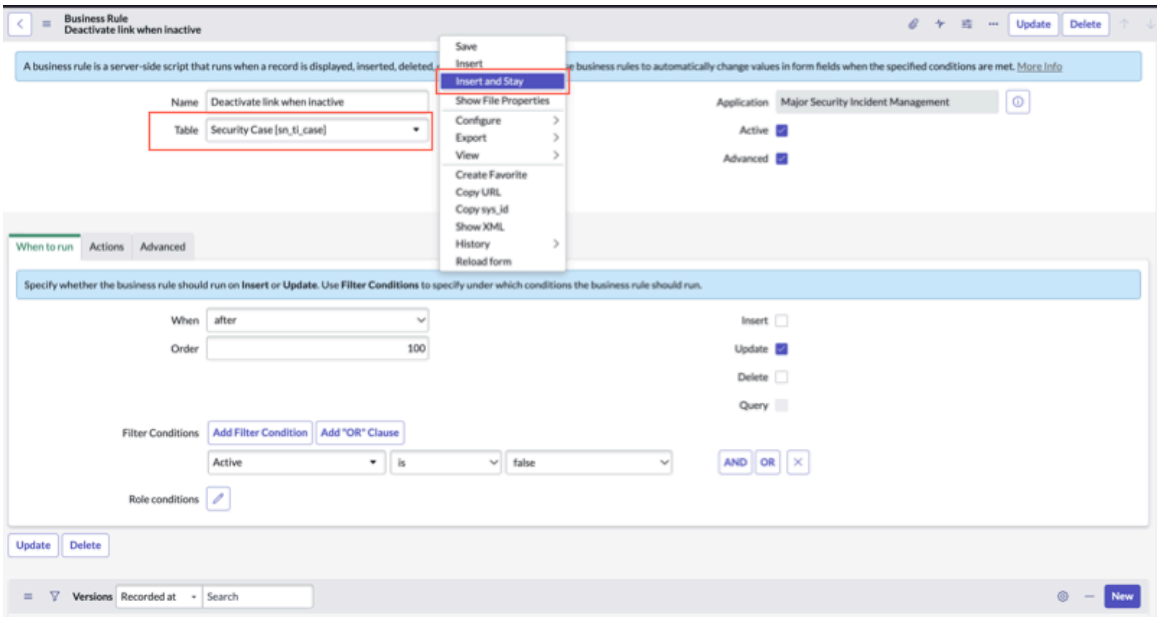
1. 次のように移動する。 システム定義 > ビジネスルール.
2. フィルターオプションを実行し、以下の情報でビジネスルール基準をフィルタリングします。
   - 名前：非アクティブな場合にリンクを非アクティブ化
   - テーブル：sn_si_incident



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. レコードを開き、テーブル名を新しいソーステーブルの sn_ti_case に変更します。
4. ページのメニューを右クリックし、[挿入と維持] をクリックしてレコードを作成します。



5. その他の 2 つのビジネスルールについてこの手順を繰り返します。
   - 削除時にチーム情報を同期
   - 更新時にチーム情報を同期

ステップ 7. ロールアップレコードの構成の作成

追加のレコードを MSI にリンクおよびリンク解除するためのロールアップレコード構成を作成します。

始める前に
必要なロール：admin および sn_msi.workspace_admin

> **注:**
> システムアドミニストレーターはレコードを作成でき、 MSI ワークスペースアドミニストレーターはレコードを更新できます。

セキュリティケースに関連する構成アイテム、観測可能事項、セキュリティ侵害のインジケーターなどの情報をロールアップするには、ロールアップレコード構成を作成します。

手順

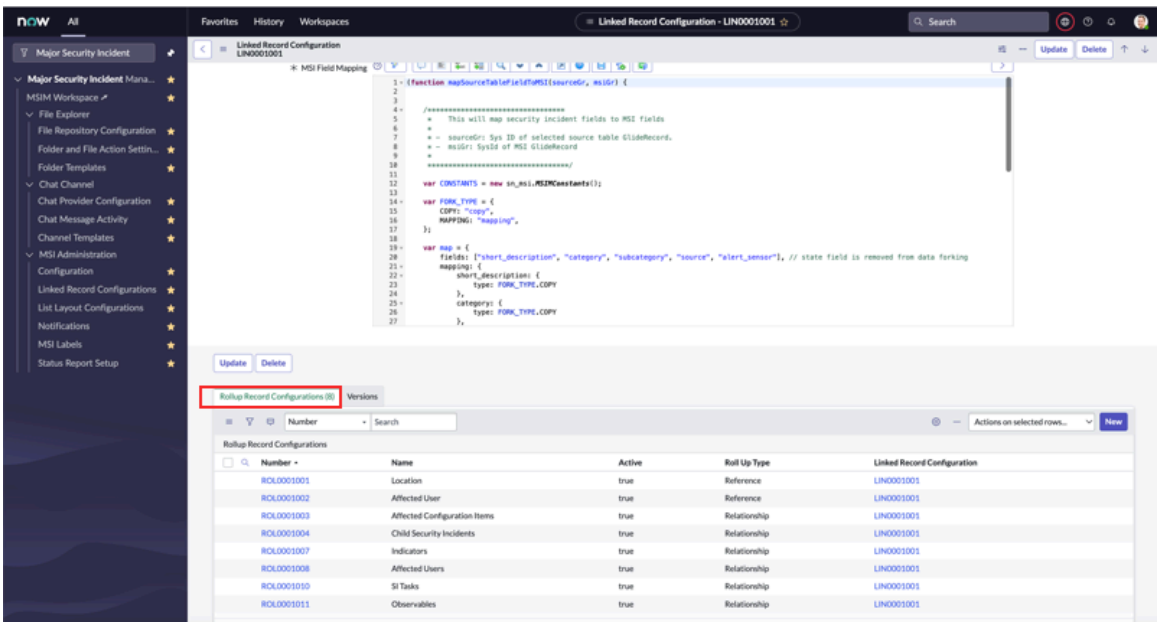
1. 次のように移動する。 **Security Incident Response** > リンクされたレコード構成.
   [リンクされたレコード構成 (Linked Records Configuration)] ページが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. リンクされたレコードを選択または新規作成し、同じページから [ロールアップレコード構成 **(Roll up Record Configuration)]** セクションに移動します。

[ロールアップレコード構成 **(Roll up Record Configuration)]** セクション



次のタスク

- 詳細については、「重大セキュリティインシデント管理 でのロールアップレコードの構成」を参照してください。
- セキュリティケースの例については、「セキュリティケースのスクリプトの記述」を参照してください。

セキュリティケースのスクリプトの記述

レコード構成をロールアップするセキュリティケースのスクリプトを作成します。

始める前に
必要なロール：admin および sn_msi.workspace_admin

注:
システムアドミニストレーターはレコードを作成でき、 MSI ワークスペースアドミニストレーターはレコードを更新できます。

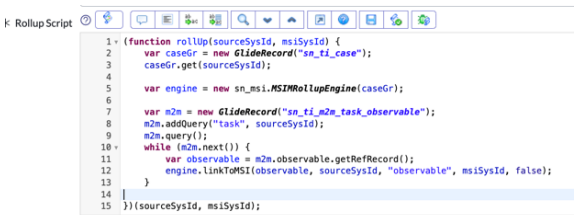
手順

1. 左側のナビゲーションから、[リンクされたレコード構成 (Linked Record configurations)] を検索します。
2. 次のように移動する。 **MSI** 管理 > リンクされたレコード構成.
3. セキュリティケースに対して作成された設定レコードを開きます。
4. ロールアップレコードの構成が [関連リスト] セクションに表示されます。
5. [新規] をクリックして、新しいロールアップレコードの構成を作成します。

   以下のフィールド値を使用してロールアップしようとしているセキュリティケースに関連する観測事象データをロールアップするために作成されたレコードの例を次に示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	説明
ロールアップタイプ	関係 **注:** 観測事象の情報は関連リスト形式で表示されます。
ロールアップスクリプト	sourceSysId の入力にはセキュリティケースの sys id が含まれ、msiSysId には重大なセキュリティインシデントの sys id が含まれます。  ○ Line 2: As a first step, query for Glide Record for sourceSysId from **Security Case(sn_ti_case)** table. ○ Line 7: Next, query **sn_ti_m2m_task_observable** table using security case sys ID to figure out all the linked observables to a security case. ○ Line 10: Next, iterate over all the linked observables and link them to a Major Security Incident using the method: `MSIMRollupEngine.linkToMSI("entityGr", "sourceSysId", "fieldNameInLinkedRecordTable", "msiSysId", "isPrimaryRecord")`

自動翻訳

オンデマンドのアトミックなロールアップを実行する

ロールアップフレームワークは、既存のリンクされたレコードの更新を処理できません。このような場合、リンクされたレコードに対してオンデマンドのアトミックなロールアップが発生する必要があります。この動作はビジネスルールを介して実行できます。

リンクされたレコードの更新をキャプチャするには、ソーステーブルでビジネスルールを作成する必要があります。

作成したビジネスルールは、挿入、更新、および削除の操作の際に機能します。挿入または更新を実行する際は、ロールアップされた情報を MSI に追加または更新する必要があります。削除すると、ロールアップされた情報は MSI から削除されます。

たとえば、セキュリティインシデントが MSI にリンクされると、関連情報が自動的に MSI にロールアップされます 。ただし、後から MSIに新しい観測事象を追加すると、新しく追加された観測事象

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

も MSI にロールアップされます。ここでは、「ロールアップされた観測事象を同期 **(Sync rolled up observable)**」というビジネスルールで更新をキャプチャし、更新されたレコードを MSI にロールアップします。同様に、既存のロールアップされた観測事象がセキュリティインシデントから削除された場合、同じビジネスルールでその削除も処理します。

事前定義されたビジネスルール

事前定義されたビジネスルールをいくつか次に示します。これは、不可分なロールアップの処理方法を理解するのに役立ちます。

ルール	説明
ロールアップされたインジケーターを同期 (Sync rolled up indicator) (sn_ti_m2m_task_indicator)	このビジネスルールを使用して、セキュリティインシデント、セキュリティケース、および修復タスクからの、セキュリティ侵害のインジケーターのロールアップと削除を処理します。
ロールアップされた観測事象を同期 (Sync rolled up observable) (sn_ti_m2m_task_observable)	このビジネスルールを使用して、セキュリティインシデント、セキュリティケース、および修復タスクからの、リンクされた観測事象のロールアップと削除を処理します。
影響を受けるユーザーの同期 (Sync rolled up affected user) (sn_si_m2m_task_affected_user)	このビジネスルールを使用して、セキュリティインシデント、セキュリティケース、および修復タスクからの、影響を受けるリンクされたユーザーのロールアップと削除を処理します。
影響を受けるロールアップされた CI の同期 (Sync rolled up affected CI) (task_ci)	このビジネスルールを使用して、セキュリティインシデント、セキュリティケース、および修復タスクからの、関連する構成アイテムのロールアップと削除を処理します。

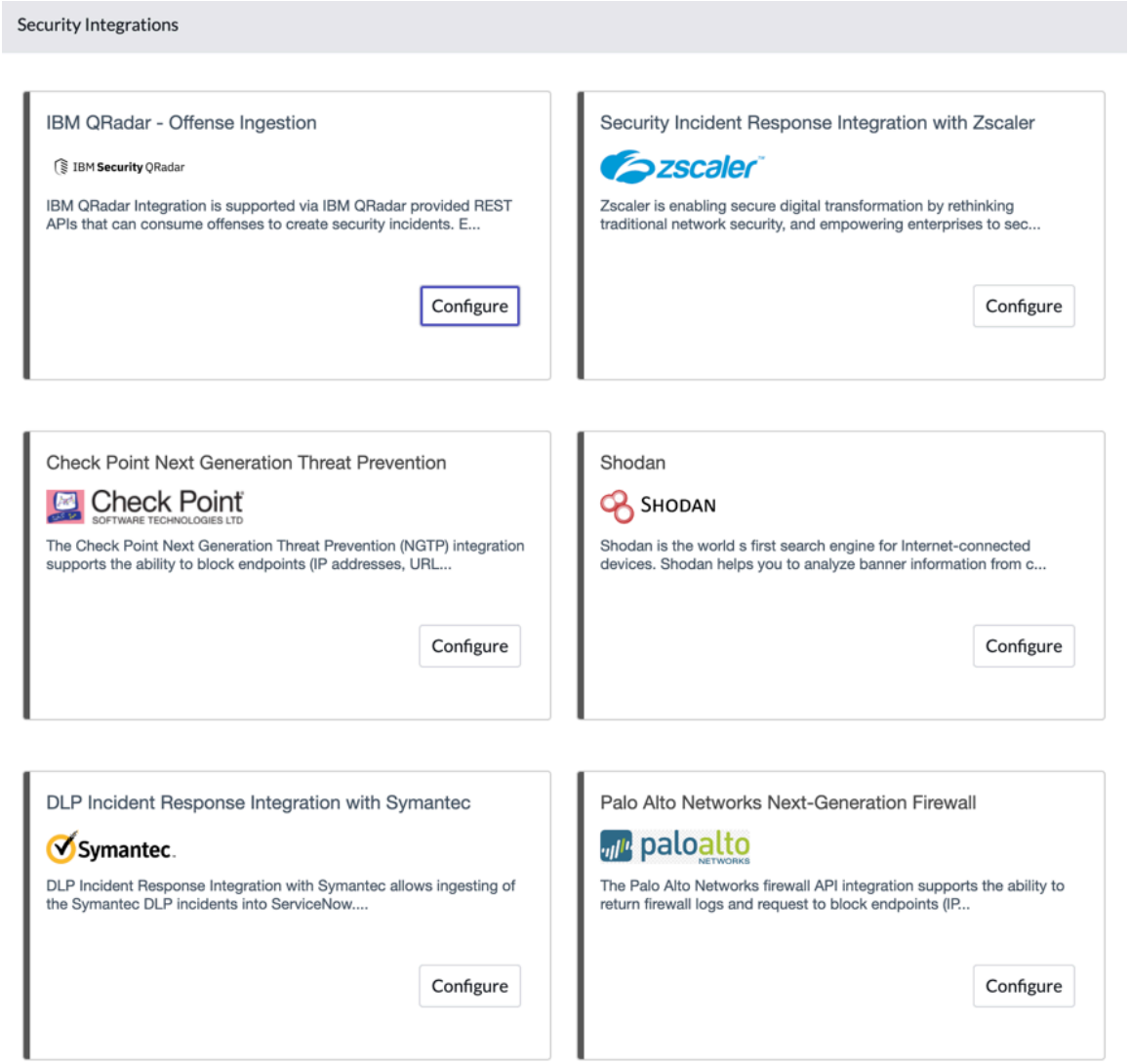
セキュリティインシデントレスポンス の統合

セキュリティオペレーション のすべてのコアアプリケーションとコア以外のサードパーティ統合を ServiceNow Store から入手できます。このセクションでは、統合をアクティブ化し、ServiceNow とサードパーティの両方の統合を構成する手順について説明します。また、独自の統合を開発するための基本的なガイドラインと、ベースシステムに含まれる特定の統合の詳細も含まれています。

統合構成

ベースシステムには、アクティブ化して使用できる各統合実装の一連の「カード」が含まれています。また、セキュリティオペレーション プラグインに依存する ServiceNow Store に投稿された統合についてもカードが表示されます。統合カードを表示するには、次を選択します。 セキュリティオペレーション > 統合設定.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

[カテゴリ] ドロップダウンメニューを使用すると、表示される統合をフィルタリングできます。[設定の表示] ドロップダウンメニューを使用すると、作成できる実装の複数のインスタンスを表示できます。

統合カードのボタン

統合カードには、統合の現在のステータスとカードのソースに応じて異なるボタンが表示されます。

ボタン	説明
プラグインをインストール	このボタンをクリックして該当するプラグインをインストールし、統合をアクティブ化します。プラグインがインストールされると、ボタンが [構成] に変わります。
構成	統合を構成するための情報を入力するには、このボタンをクリックします。一部の統合では、サードパーティ統合の Web サイトから取得した API キーまたは URL を入力する必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ボタン	説明
新規	Carbon Black や IBM QRadar などの特定の統合では、同じ統合の複数の実装を定義できます。これらの統合では、プラグインをアクティブ化した後に [新規] をクリックします。カードを使用すると、プラグインをインストールし (該当する場合)、使用する実装を構成できます。
ページを開く	ベースシステムでは、インスタンスは、ServiceNow Store に対し、セキュリティオペレーション プラグインに依存するアプリケーションについてのクエリを実行します。これらのアプリケーションが見つかり、関連するアプリケーションプラグインが有効になると、それらの統合カードが他のセキュリティ統合カードとともに表示されます。[ページを開く] をクリックしてサードパーティアプリケーションの Web サイトにアクセスし、統合を構成します。構成が完了すると、[ページを開く] ボタンは [構成] に変わります。

セキュリティオペレーション のための **ArcSight ESM** イベントの取り込み統合

セキュリティインシデントレスポンス 製品との ArcSight ESM イベント取り込み統合により、セキュリティインシデントアナリストは ServiceNow プラットフォームで相関イベントを収集し、セキュリティインシデントの作成を自動化できます。データは設定されたポーリングスケジュールに基づいて継続的に取り込まれ、アナリストが潜在的なサイバーセキュリティの脅威を特定して対応するために使用します。

この統合により、セキュリティインシデントの候補である相関イベントを定期的に取り込むことができます。相関イベントのフィールドをセキュリティインシデントフィールドにマップし、イベントの設定をセキュリティインシデントとしてプレビューし、イベントのスケジュール設定された取り込みを設定して、セキュリティインシデントを継続的に自動作成できます。

概要

この統合により、セキュリティオペレーションセンター (SOC) アナリストは ArcSight ESM の相関イベントを表示できます。このデータは、Now Platform セキュリティインシデントレスポンス (SIR) セキュリティインシデントに統合して、さらに調査および修復できます。プロファイルは、Now Platform インスタンスに作成され、ArcSight ESM の相関クエリビューアーを介して作成および利用されるさまざまな相関イベントタイプを処理します。これらのプロファイルは、SIR セキュリティインシデントでのさまざまな ArcSight ESM 相関イベントフィールドの表示方法をカスタマイズします。

主な機能

この統合の主な機能は次のとおりです。

- 複数のイベント取り込みプロファイルを作成して、マルウェア、不正なアクセス試行などの特定のタイプの脅威に対して SIR セキュリティインシデントを作成します。
- 関連付けられている SIR セキュリティインシデントフィールドへの ArcSight ESM 相関イベントフィールド値のドラッグアンドドロップによるマッピング。
- イベントマッピングの詳細を検証するためのサンプル相関イベントに基づく SIR セキュリティインシデントレイアウトのプレビュー。
- 構成可能な間隔で、履歴相関イベントと新しい注目イベントを取り込みます。
- SIR インシデント生成基準を満たさない相関イベント (低優先度イベントなど) を除外します。
- 一致するフィールド値に基づいて既存の SIR セキュリティインシデントにイベントを集計し、重複するセキュリティインシデントを回避します。
- 双方向インターフェイスを介し、SIR インシデントの作成やクローズの条件に基づいて相関イベントを更新します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サポートされている Now Platform のバージョン

この統合は、New York パッチ 6 および Orlando Now Platform リリースをサポートしています。

次の Security Operations アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されている必要があります。スムーズにインストールできるように、アプリケーションを次のリストの順番で、一度に 1 つずつインストールしてアクティブ化します。

1. Security Integration Framework
2. Security Support Common
3. セキュリティインシデントレスポンス
4. Security Operations のイベントとアラートの取り込み
5. Integration Hub プラグイン
   a. ServiceNow Integration Hub ランタイム
   b. ServiceNow Integration Hub アクションステップ - REST

セキュリティオペレーション コアアプリケーションのインストールの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

ArcSight ESM のサポートされているバージョン

この統合は、ArcSight ESM Manager のバージョン 7.0.0.2436 でテストされています。統合では、ArcSight ESM のオンプレミスとクラウド/ホストサービス環境の両方をサポートしています。

MID サーバー

ArcSight® ESM サーバーが企業ネットワーク内に展開されている場合、この統合では、Now Platform インスタンスのインストールされ、構成された MID サーバーを ArcSight ESM サービスに接続する必要があります。ArcSight ESM クラウドサービスを使用している場合、MID サーバーは必要ありません。MID サーバーの詳細については、ServiceNow 製品ドキュメント Web サイト を参照してください。

参照

参照	ドキュメント識別子	ドキュメントタイトル
1	ArcSight ESM 製品ドキュメント	ArcSight 製品ドキュメント 。
2	ServiceNow 製品ドキュメント Web サイト	ServiceNow 製品ドキュメント Web サイト

ArcSight ESM イベントの取り込み統合のために Now Platform® インスタンスを設定

次のセクションでは、ServiceNow Store からアプリケーションをインストールする前に Now Platform インスタンスで完了する必要があるセットアップタスクを示します。

始める前に
必要なロール：admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
スムーズなインストールと構成を行うために、 アプリケーションをダウンロードしてインストールする前に、次のテーブルを参照して、リストされたすべてのタスクを完了していることを確認してください。

セットアップタスク	説明
必要な Now Platform® および セキュリティインシデントレスポンス (SIR) のロールがアサインされていることを確認します。	Now Platform® インスタンスで統合をインストール、セットアップ、および使用するには、次のロールが必要です。 • Now Platform® アドミニストレーターロール (admin) を持つユーザーが ServiceNow Store からアプリケーションをインストールし、セキュリティインシデントアドミニストレーター (sn_si.admin) ロールをアサインします。 • sn_si.admin ロールを持つユーザーは、Now Platform® で次のタスクを監督します。 ○ イベントプロファイルに名前を付け、作成し、編集します。 ○ ArcSight ESM 相関イベントから値を選択し、セキュリティインシデントにマップします。 ○ 構成を確定する前に、正確性を確認するためにセキュリティインシデントの詳細をプレビューします。 ○ 進行中の相関イベント取り込みをスケジュールします。 ○ SIR インシデントが作成されてクローズされたときに、相関イベントの更新を有効にします。 ○ セキュリティインシデントアナリスト (sn_si.analyst) ロールをアサインします。 ○ sn_si.analyst を持つユーザーは、セキュリティインシデントを処理します。 ロールとユーザーへのロールの割り当ての詳細については、Servicenow 製品ドキュメント Web サイト の「ロール」を参照してください。
ArcSight ESM Manager のバージョン 7.0.0.2436 以降を使用していることを確認します。以前のバージョンはサポートされていません。	ArcSight ESM クエリビューアーへのアクセス権がある場合は、この統合に必要な API にアクセスできます。API に必要なその他の特別なセットアップはありません。
ArcSight ESM でクエリビューアーを設定します。	相関イベントを取り込む前に、ArcSight ESM コンソールでクエリビューアーを構成する必要があります。詳細については、「ArcSight ESM クエリビューアーの設定」を参照してください。
Optional ArcSight ESM に相関イベント更新のカスタムステージを作成します。	相関イベントは、クローズされるまでにライフサイクルで多くのステージを通過します。ArcSight ESM は、初期、監視、キューに格納、クローズ済みなどのデフォルトのステージを提供します。これらのステージの中にはユーザー入力が必要なものもありますが、ユーザーの介入なし (ArcSight ESM コンソールで [ユーザーが必要 **(User**

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	Required)] フィールドはオフ) で自動的にイベントに適用されるステージもあります。 ユーザーの介入を必要としないカスタムステージを作成し、Now Platform インスタンスで使用できます。詳細については、「その他のオプション：SIR インシデント状況に基づく相関イベントの更新とクローズの自動化」を参照してください。
MID サーバーアプリケーションがインストールおよび設定されていることを確認します。	設定された MID サーバーアプリケーション ArcSight ESM サーバーが企業ネットワーク内に展開されている場合、 Now Platform インスタンスの MID サーバーを ArcSight ESM サービスに接続する必要があります。MID サーバーアプリケーションの構成方法については、「ArcSight ESM イベント取り込み統合用の ServiceNow アプリケーションのインストールと設定」を参照してください。 MID サーバーについては、「MID サーバー」を参照してください。 ホステッドサービスまたはクラウドサービスを使用している場合、つまりインターネットにアクセスできる場合、MID サーバーは必要ありません。
統合用のアプリケーションをインストールする前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。 **1.** セキュリティインシデントレスポンス **2.** Security Integration Framework **3.** Security Support Common **4.** Security Operations のイベントとアラートの取り込み：このアプリケーションでは次のものが必要です。 ○ com.glide.hub.integration.runtime => ServiceNow 統合ハブランタイム ○ com.glide.hub.action_step.rest => ServiceNow 統合ハブアクションステップ - REST **5.** Threat Core セキュリティオペレーション コアアプリケーションのインストールの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のタスク

統合のために Now Platform ® インスタンスが正常に設定されました。次のステップでは、統合のために ServiceNow Store から ArcSight ESM Security Event Ingestion for Security Operations アプリケーションをインストールします。

ArcSight ESM クエリビューアーの設定

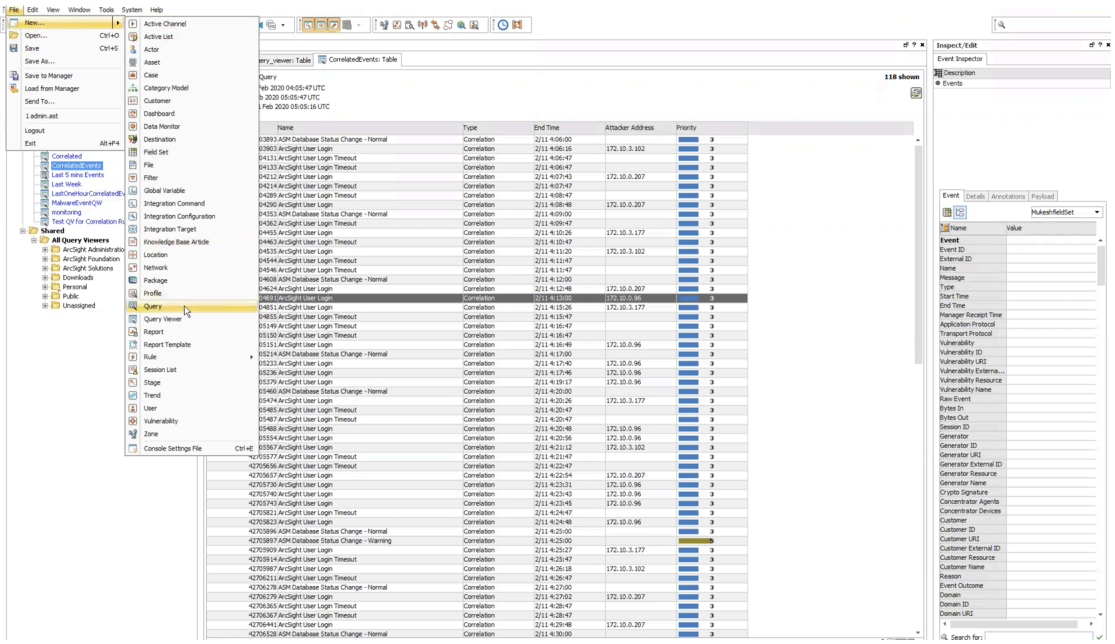
クエリビューアーを作成し、ServiceNow に取り込まれる最近作成された相関イベントを含むフィルターを定義します。

始める前に

必要なロール：ArcSight アドミン

手順

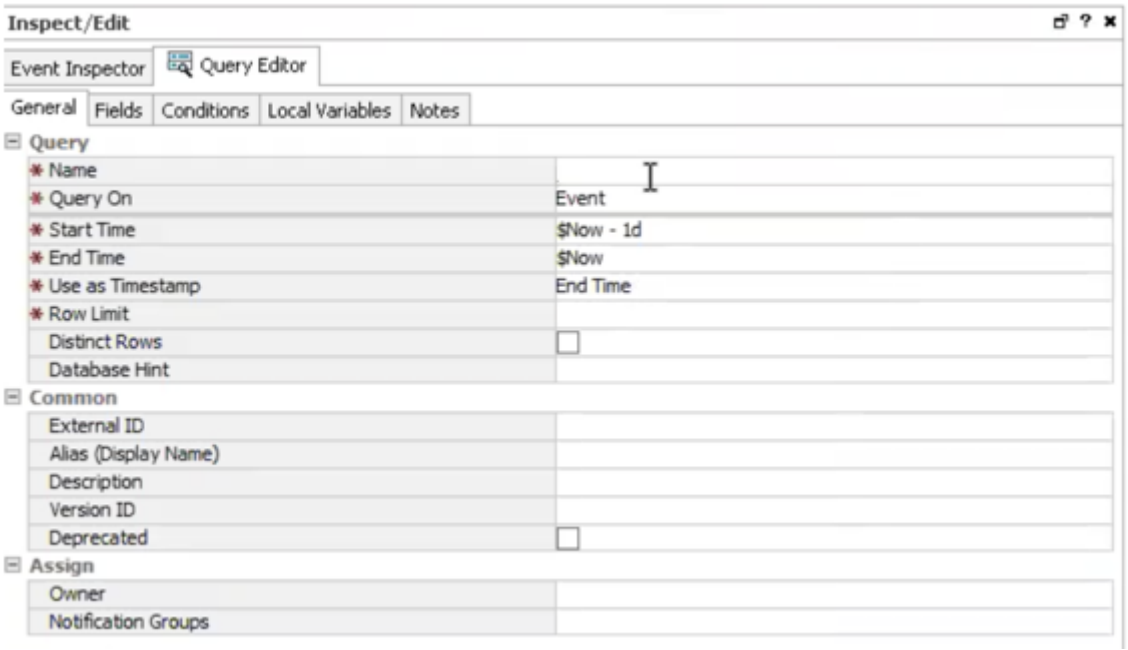
1. ArcSight ESM コンソールにログインして、クエリビューアーを作成します。
2. 新しいクエリを作成するには、次に移動します: ファイル > 新規 > クエリ.



3. [検査/編集 **(Inspect/Edit)]** パネルでクエリビューアーの条件を定義します。

自動翻訳

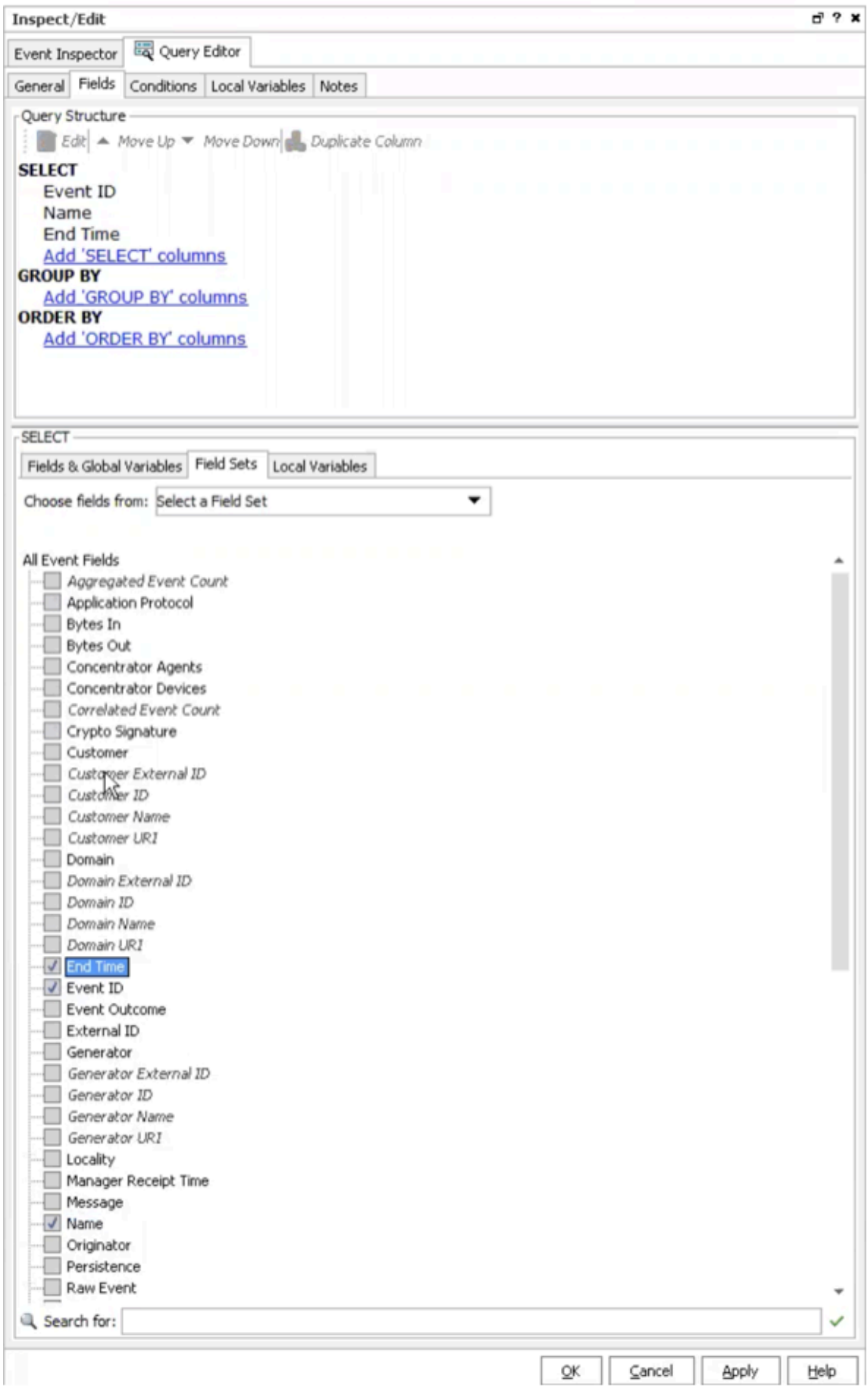
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [フィールド] タブをクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

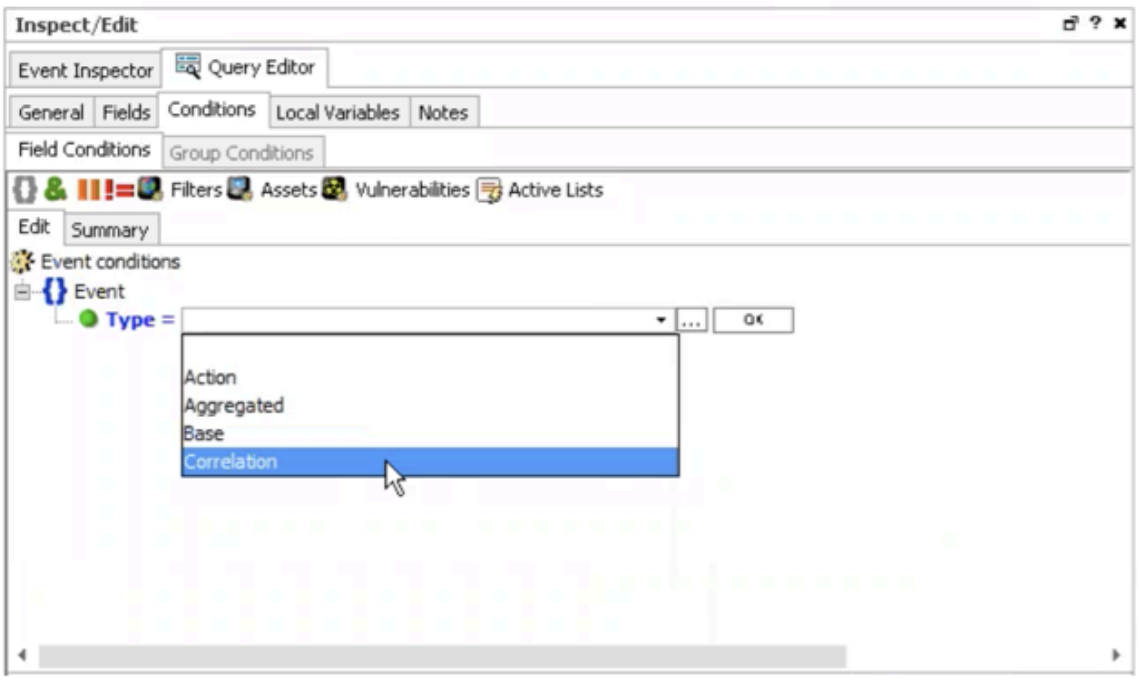


自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. 取り込み時に含める必要があるフィールドを選択します。
   取り込みを成功させるには、[イベント *ID*]、[名前]、および [終了時刻] フィールドを選択する必要があります。
6. **[[ORDER BY]** 列を追加 **(Add 'ORDER BY' columns)]** リンクをクリックして [イベント **ID]** フィールドを選択し、ソート順を [降順] に指定して、最新のイベントが取り込まれるようにします。
7. [条件] タブをクリックします。
8. [サマリー] セクションの [イベント条件] で [イベント] を右クリックします。
9. クリックします 新しい条件 > ルート > タイプ をクリックし、[イベントタイプ] で [相関] を選択します。

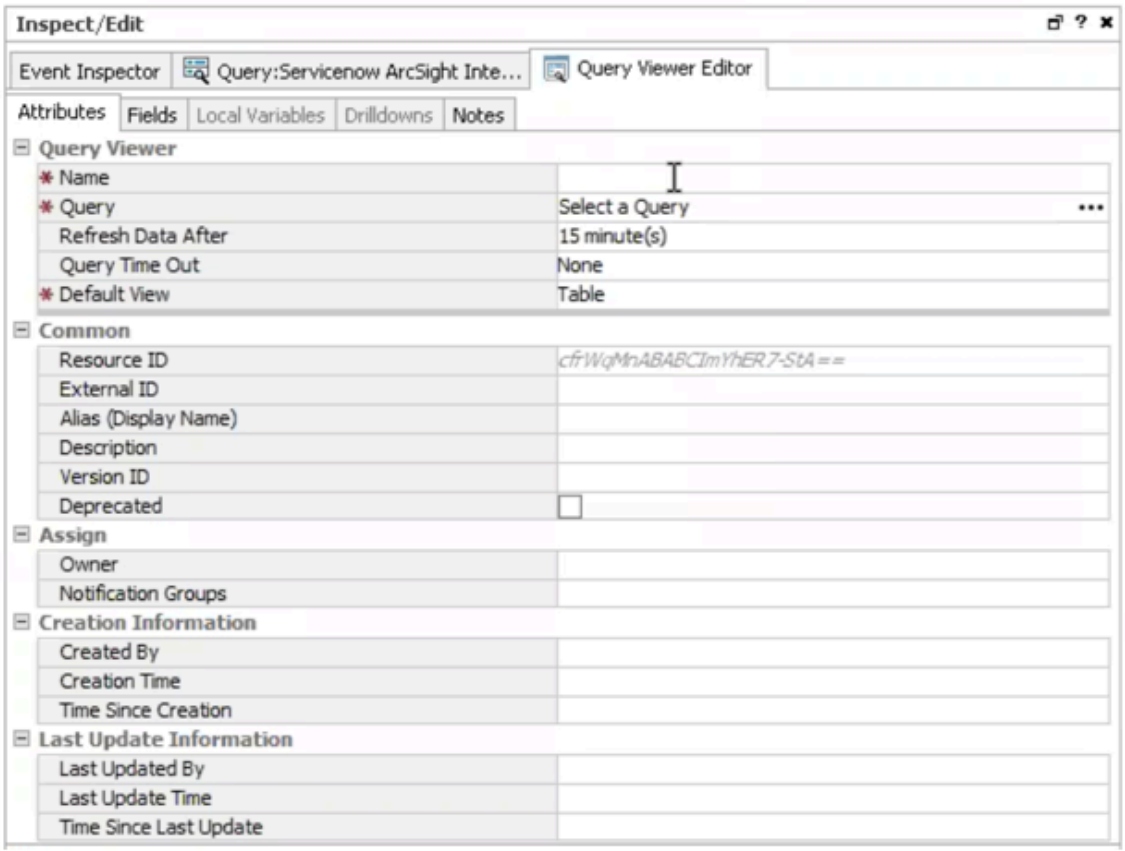
> **重要:**
> 相関イベントのみが取得されます。相関のベースイベントは取得されません。



10. **[OK]** をクリックしてクエリを保存します。
    次のステップでは、このクエリのクエリビューアーを作成します。
11. 次のように移動する。 ファイル > 新規 > クエリビューアー.

自動翻訳

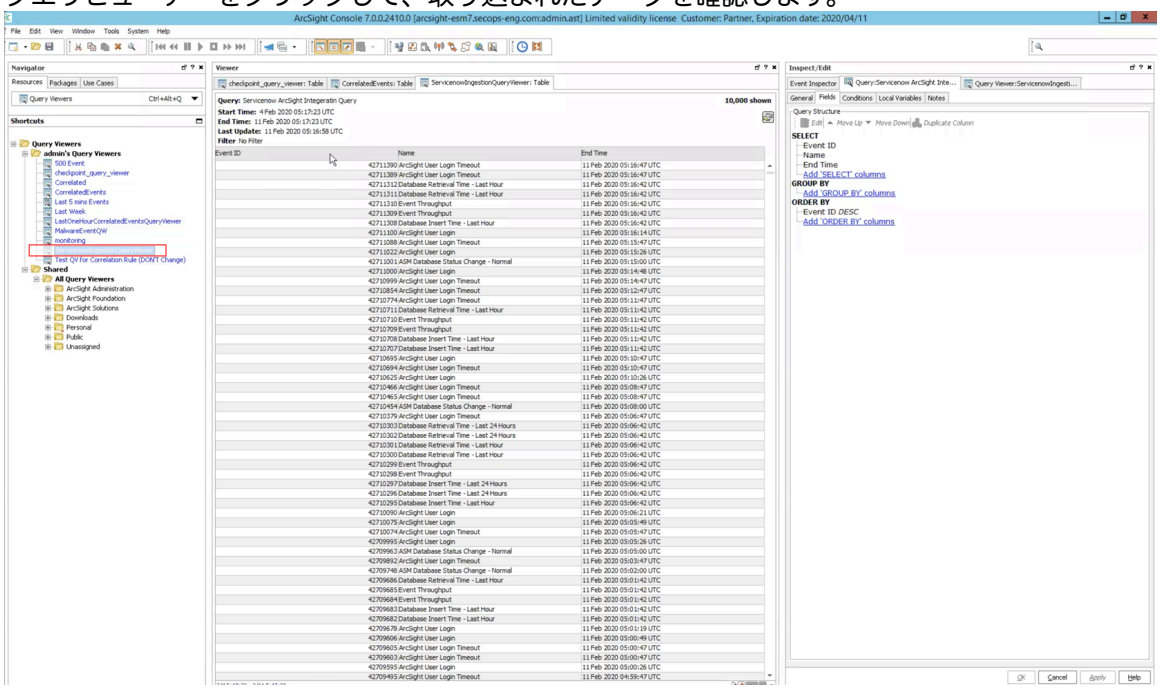
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



12. [フィールド] タブをクリックし、クエリで指定した必須フィールド ([イベント ID]、[名前]、[終了時刻]) が選択されていることを確認します。

13. [適用] をクリックしてクエリビューアーを保存します。
作成した新しいクエリビューアーが [クエリビューアー] セクションに表示されます。

14. クエリビューアーをクリックして、取り込まれたデータを確認します。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ArcSight ESM® イベント取り込み統合用の ServiceNow アプリケーションのインストールと設定

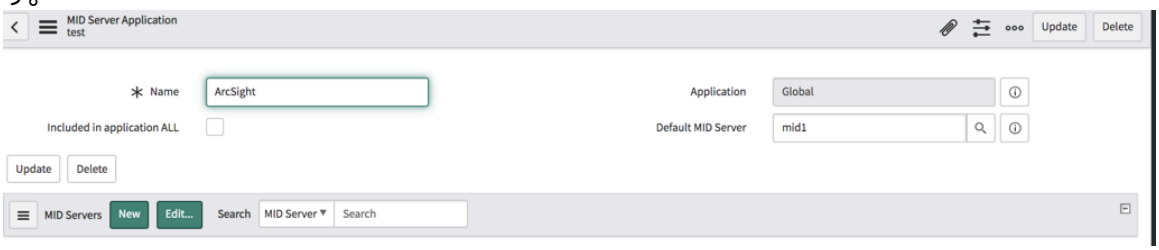
Now Platform インスタンスで統合を実行する前に、これらのインストールと構成のステップを完了して、Now Platform インスタンスでアプリケーションが セキュリティインシデントレスポンス と セキュリティオペレーション 製品と適切に統合されるようにします。

始める前に

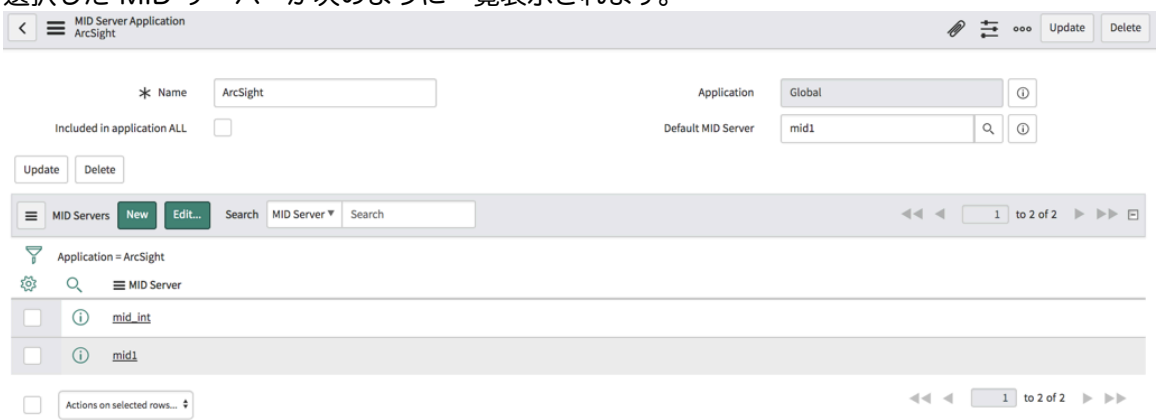
必要なロール：sn_si.admin

手順

1. ServiceNow Store から統合用の ArcSight ESM アプリケーションをインストールしていない場合は、「セキュリティオペレーション 統合のインストール」を参照し、ステップに従ってインストールしてください。
2. アプリケーションのインストールが完了したら、 統合 > 統合構成 をクリックし、 ArcSight ESM タイルを見つけます。
3. アプリケーションを設定するには、[新規] をクリックします。
4. または、[構成] ボタンがタイルに表示されている場合は、そのボタンをクリックして既存の構成を編集します。
5. フォームのフィールドに入力します。
   新しい MID サーバーアプリケーションを作成するには、次の手順を実行します。
   a. 次のように移動する。 **MID** サーバー > アプリケーション をクリックし、[新規] をクリックします。
   b. MID サーバーアプリケーションの名前を入力し、デフォルトとして使用する MID サーバーを選択します。
   c. [すべてのアプリケーションに含める] チェックボックスをオフにして、[保存] をクリックします。



   d. [編集] をクリックします。[メンバーの編集] ページで、利用可能なすべての MID サーバーを選択し、[MID サーバー] リストに移動して、[保存] をクリックします。
   e. 選択した MID サーバーが次のように一覧表示されます。

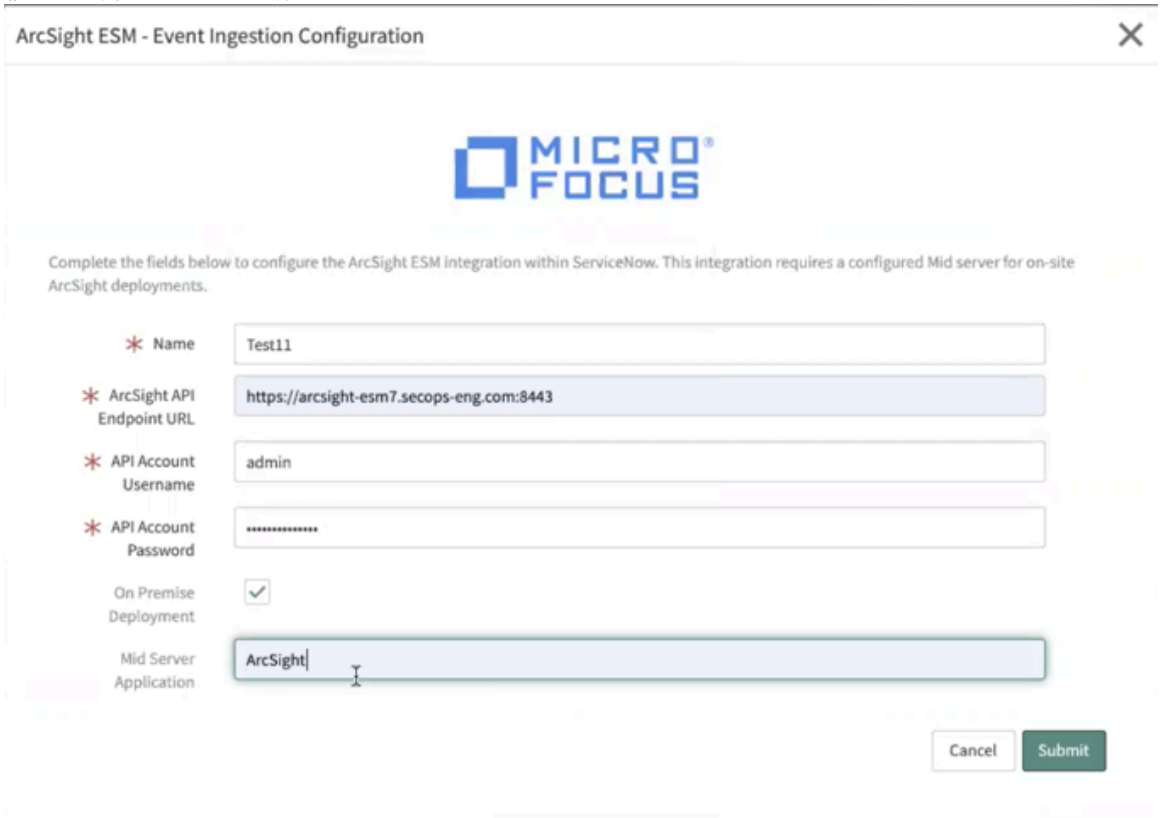


自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

可用性に応じて、MID サーバーアプリケーションで構成された MID サーバーの 1 つが使用されます。

6. 構成の詳細を入力し、作成した MID サーバーアプリケーションを指定します。



ArcSight ESM Manager コンソールから取り込む各相関イベントには、インスタンス内に一意のイベントプロファイルが必要です。ただし、[イベントの取り込み構成] フォームで構成した ArcSight ESM ソースは、各プロファイルが一意の相関イベントタイプを取り込む限り、複数のプロファイルで再利用できます。

7. **[Submit]** をクリックします。
検証と送信が正常に完了すると、各 ArcSight ESM サーバー構成は [セキュリティ統合] ページにタイルとして保存されます。保存された構成タイルが右上隅にある [セキュリティ統合] ページに表示されていない場合、[構成を表示] 選択リストから [はい] をクリックします。

次のタスク

アプリケーションのインストールと設定が正常に完了しました。次のステップは、イベントプロファイルの作成です。

ArcSight ESM 相関イベントの取り込み統合のためのプロファイルの作成

sn_si.admin ロールを持つユーザーは、Now Platform インスタンスにプロファイルを作成し、どの相関イベントでセキュリティインシデントが作成されるかを決定します。Now Platform セキュリティインシデントレスポンス (SIR) セキュリティインシデントが相関イベントから作成される前に、イベントのフィールド値が Now Platform セキュリティインシデントのレイアウトに表示されるため、実際のセキュリティインシデントがどのように作成されるかをプレビューできます。

始める前に

必要なロール：sn_si.admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
定義されたプロファイルタイプに応じて、相関イベントが Now Platform インスタンスの セキュリティオペレーション 環境に自動的に取り込まれます。プロファイルは、不正なアクセス試行やマルウェアといった 1 つのタイプの相関イベントをカプセル化したものです。

相関イベントが取り込まれた後、個々の相関イベントフィールドをセキュリティインシデントの対応するフィールドにマップできます。相関イベントをフィルタリングして、セキュリティインシデントを作成するイベントを指定できます。たとえば、高リスクとして識別された相関イベントに対してのみセキュリティインシデントを作成するフィルターを使用できます。追加のイベント集計条件を定義して、受信する重複相関イベントをオープンセキュリティインシデント別に集計することもできます。最後に、取り込みスケジュールを定義し、プロファイルをアクティブ化することができます。

Now Platform インスタンス内のイベントプロファイルの名前は一意である必要があり、常に 1 つのアクティブなイベントプロファイルにのみマッピングできます。

ArcSight ESM イベントの取り込み統合のためのプロファイルの作成と名前設定

相関イベントを取り込むようにプロファイルを設定できます。

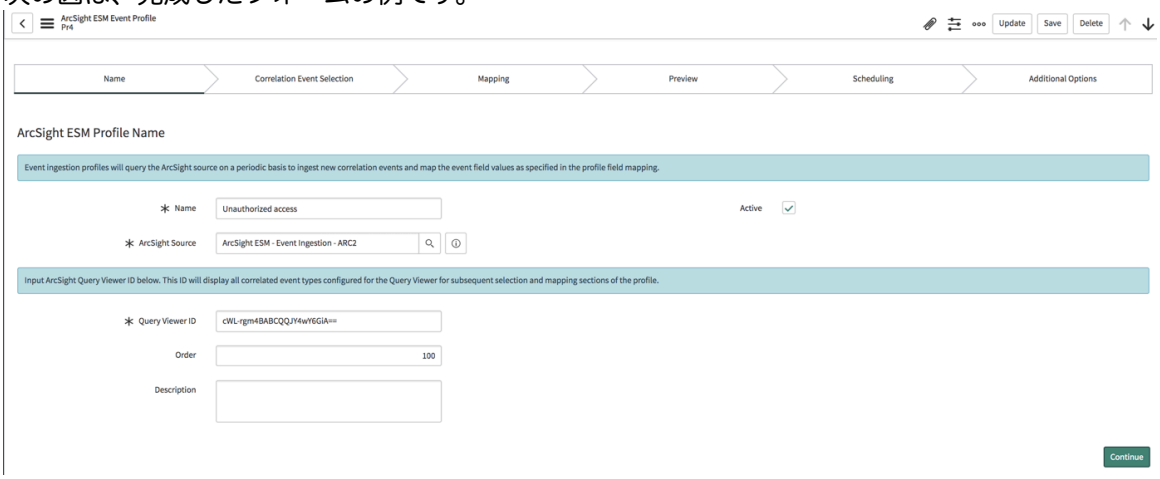
始める前に
必要なロール：sn_si.admin

手順

1. Now Platformインスタンスで相関イベントのイベントプロファイルを作成するには、 **ArcSight ESM** 統合 > **ArcSight ESM** イベントプロファイル.
2. [**New**] をクリックします。
3. フィールドに入力します。

   完成したフォームの例が表の後に表示されます。

   次の図は、完成したフォームの例です。

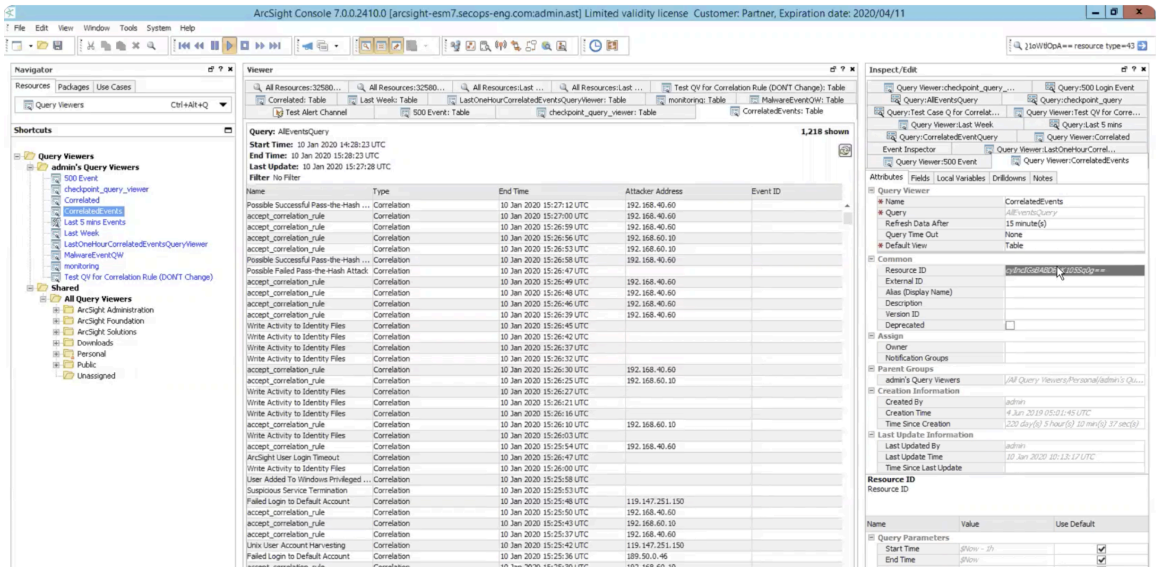


   プロファイルの詳細を入力したら、[続行] をクリックします。クエリビューアー ID が検証され、対応するリソース ID が ArcSight ESM クエリビューアーに存在する場合、クエリビューアーの名前が次のように返されます。検証に失敗した場合は、ArcSight ESM コンソールにリソース ID が

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

存在するかどうかを確認します。リソース ID が見つからない場合は、正しいリソース ID を見つけてプロファイルに入力します。



次のタスク
次のステップでは、前のステップで選択したクエリビューアーから取り込む相関イベントタイプを選択します。

ArcSight ESM イベントの取り込み統合のための相関イベントの選択

ArcSight ESM ソースと構成されたクエリビューアーに基づいて、プロファイルの相関イベントルールを選択します。

始める前に
必要なロール：sn_si.admin

このタスクについて
Now Platform インスタンスの [相関イベントの選択] にリストされる利用可能な相関イベントを表示して、どの相関イベントを取り込んでセキュリティインシデントを作成するかを決定できます。各プロファイルのリストから選択できる相関ルールタイプは 1 つだけです。
[クエリビューアー] フォームで指定されたクエリビューアー ID とクエリビューアー名が表示されます。リストから、取り込まれた相関イベントの構成マッピングを作成するために使用できる相関イベントを選択します。

[相関イベントリスト] フィールドのドロップダウンリストをクリックします。ArcSight ESM クエリビューアーコンソールに存在する相関イベントのリストが表示されます。

[続行] をクリックして、ウィザードの次のステップに進みます。

ArcSight ESM イベントの取り込み統合の相関イベントフィールドをマッピングする

リストから特定の相関イベントルールを特定したら、次のステップでは、相関イベントフィールドをセキュリティインシデントフォームのフィールドにマップします。

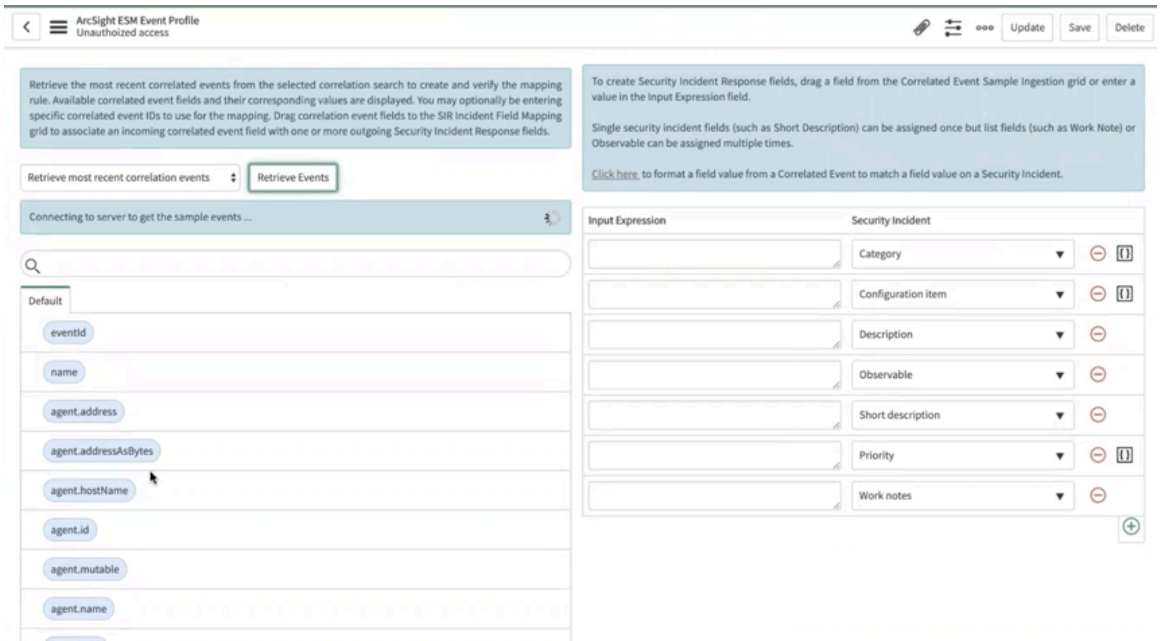
概要

マッピングステップでは、選択した相関ルールのサンプル相関イベントを取り込むことができます。このマッピングフェーズで、関連するすべての相関イベントフィールドデータが、SIR インシデントフォームの適切な場所にマッピングされていることを確認して、SIR インシデントをプレビューセクションで可視化できます。

次の図は、相関イベントプロファイルを作成するために提供されるデフォルトのマッピング構成を示しています。セキュリティインシデントを入力するフィールドをカスタマイズできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[イベントを取得] をクリックすると、相関イベントフィールドの名前と対応する値がフォームの左側に入力されます。これらは、セキュリティインシデントフィールドにマップ可能な ArcSight ESM 相関イベントフィールドです。

コンソールでいくつかのサンプル相関イベントを確認して、フィールドマッピング構成ステップに取り込むこともできます。このステップは、進捗状況バーで [マッピング] とラベル付けされます。このページが表示されない場合は、進捗状況バーの [マッピング] をクリックします。選択した相関ルールについて ArcSight ESM Manager から最大 5 つのサンプル相関イベントを取り込んで、フィールドマッピングプロセスを支援できます。選択した相関イベントの最新の 5 つの相関イベントを取り込むか、イベント ID に基づいて最大 5 つの特定の相関イベントを取り込むかのオプションがあります。

相関イベントをマップするために必要なステップの概要を以下に示します。

- フィールドマッピング：左側から相関イベントフィールドをドラッグして、右側の SIR インシデントマッピングセクションにドロップし、マッピング構成を編集します。右側のマッピングで、受信する相関イベントフィールドを送信セキュリティインシデントフィールドに関連付けることができます
- マッピングエクスペリエンス：[SIR インシデントフィールドマッピング] セクションの下部にある [+] アイコンを使用してフィールドを追加または削除し、マッピンググリッドをカスタマイズします。提供されている色分け (マップされたフィールドはグレー表示され、ブルーのフィールドはマップされていません) を使用して、見落とされているフィールドや以前マップされたフィールドを追跡します。
- インシデント生成条件：マッピングセクションが完了すると、フィルター条件を定義して、どの相関イベントがセキュリティインシデントを作成し、どの相関イベントがフィルタリングで除外されるか (低優先度の相関イベントなど) をフィルターできるようになります。これは、[相関イベントサンプルの取り込み] セクションの下にある [インシデント生成条件] セクションで行います。
- イベント集計基準：類似の重複する可能性があるインシデントを作成するのではなく、既存の SIR セキュリティインシデントに受信相関イベントを集計する追加のイベント集計基準を定義します。この追加の集計機能では、各プロファイルのフィールド一致値基準を使用して、関連するすべてのセキュリティ注目イベントデータを単一のセキュリティインシデントに配置することで、アクティブな重複するセキュリティインシデントの数を減らすことができます。
- フォーマットフィールド変換：場合によっては、 ArcSight ESM 相関イベントのイベントフィールド値が SIR セキュリティインシデントのフィールドに直接変換されないことがあります。これらの値については、マッピングステップでスクリプトエディターを使用してセキュリティインシデン

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

トのフィールド値をフォーマットできます。類似しているが同一ではない値をフォーマットする場合は、スクリプトエディターを使用します。

たとえば、スクリプトエディターを使用すると、 [マルウェアアラート] と [ウイルス感染]のカテゴリ値でソースカテゴリのフィールド値が異なる可能性がありますが、フォーマットフィールド変換機能を使用して、SIR セキュリティインシデントの [カテゴリ] フィールドで両方の値を一般的な悪意のあるコードアクティビティに変換することができます。

次のステップでは、サンプル相関イベントを取り込み、値を SIR セキュリティインシデントフィールドにマップします。

ArcSight ESM イベントの取り込み統合のマッピングの作成

このステップでは、サンプル相関イベントを取り込み、値を SIR セキュリティインシデントフィールドにマップします。

始める前に

必要なロール：admin、sn_si.admin

このタスクについて

sn_si.admin ロールを持つユーザーは、フォームの左側にある [相関イベントサンプルの取り込み] 列で最大 5 つのサンプル相関イベントを確認して、イベントフィールド値を右側の [SIR インシデントフィールドマッピング] 列のセキュリティインシデントフィールドにマッピングして変換することができます。
フォームの右側にあるマッピンググリッドのフィールドを追加または削除して、カスタムマッピングを作成します。デフォルトで表示されるフィールドは、通常、セキュリティインシデント応答フォームに入力する重要なフィールドです。ただし、[+] および [-] ボタンを使用して、これらのフィールドを削除し、追加のフィールドを表示することができます。フォームの右側にあるマッピンググリッドのフィールドを追加または削除して、カスタムマッピングを作成します。フィールドをカスタマイズすると、セキュリティインシデントのデフォルトのマッピンググリッドに表示されていない ArcSight ESM フィールドをマッピングできます。

手順

1. このマッピングフォームが表示されない場合は、進捗状況バーの [マッピング] をクリックします。
2. 選択した相関ルールの最新のサンプル相関イベントをプルするか、相関イベントマッピングエクスペリエンスに使用する特定の相関イベントの一意の相関イベント ID を指定できます。
3. ドロップダウンリストから、次のいずれかを選択します。
   - 最新の相関イベントを取得
   - イベント ID に基づいて相関イベントを選択します

   [イベントを取得] をクリックして、選択した相関検索ルールについて ArcSight ESM コンソールから最新のサンプル相関イベントをプルします。

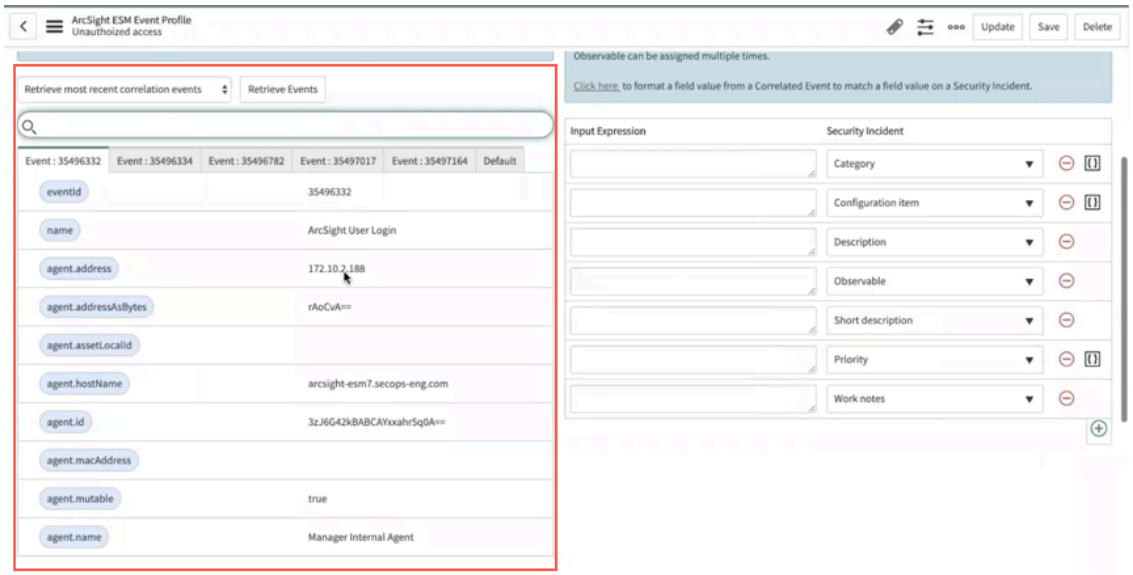
   相関イベントのフィールドと値の結果は、個別のタブとして表示されます。

   サンプル相関イベントのプルには少し時間がかかる場合があります。トランザクションが機能していることを示すメッセージが画面の上部に表示されます。

   次の図では、取り込みプルの完了後に、取り込まれた相関イベントまたはインポートされたサンプルイベントのフィールド名値のペアがこのフォームの左側に表示されます。これらの値は、フォームの [SIR インシデントフィールドマッピング] 側のセキュリティインシデントフィールドにマッピングする値です。

自動翻訳

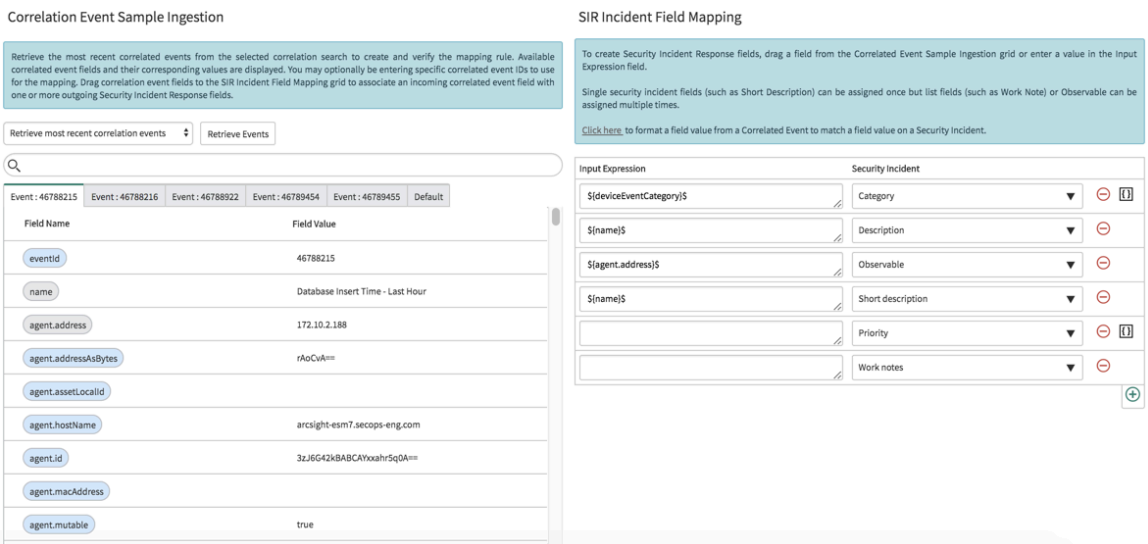
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. フォームの左側からフォームの右側のセキュリティインシデントのフィールドにフィールド値をマッピングするには、フォームの左側で青色のフィールド名をクリックしたままにします。
5. フィールド名 (agent.hostname など) をドラッグして、[セキュリティインシデント] 列のフィールド名の横にある [入力式] 列のフィールドにドロップします。

   マッピングプロセスでイベントフィールドが見落とされたり重複したりしないように、フィールドは色分けされています。左側のライトブルーのフィールドは、相関イベントフィールドがまだ未選択で、セキュリティインシデントにマップされていないことを示します。受信相関フィールドをセキュリティインシデントの 1 つ以上のフィールドに関連付けることができます。

   灰色のフィールドは、フィールドが選択され、セキュリティインシデントのフィールドにマッピングされていることを示します。この色分けは、今後のセキュリティインシデントフィールドマッピングでどのイベントフィールドが既に使用されているかを追跡するのに役立ちます。



6. フォームの右側のセキュリティインシデントに表示されるデフォルトのフィールドにフィールドを追加するには、次のステップを実行します。

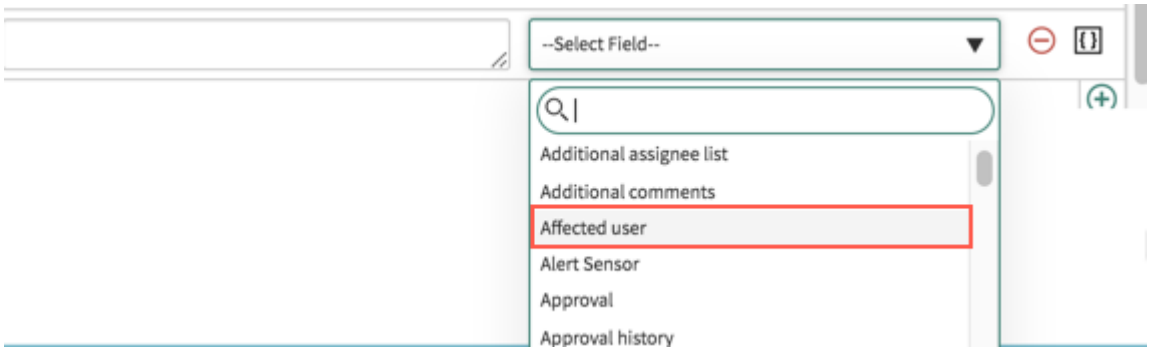
   a. フォームの右側の [SIR インシデントフィールドマッピング] セクションで、グリッドの下部にあるプラスアイコンをクリックします。
   新しいフィールドが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

b. [セキュリティインシデント] 列で表示されている選択リストを展開し、フィールドを選択します。

新しいフィールドの展開された選択リストでは、一部のフィールドが網掛けされています。セキュリティインシデントにマップされたため、次の図では、[影響を受けるユーザー] のバックグラウンドはグレーになっています。フォームの左側の相関イベントフィールドの色分け同様、セキュリティインシデントフィールドのこの色分けも、すでにマップされた SIR インシデントフィールドを追跡するのに役立ちます。



注:
同じセキュリティインシデントに複数の観測事象を表示できるため、[観測事象] フィールドを異なる値で複数回マップできます。同様に、[構成アイテム] フィールドと [作業メモ] フィールドは複数の値をサポートします。複数の値をサポートできないフィールドに 2 つの値をマッピングしようとすると、インシデントをプレビューするときに、フィールドに値がないことを示すエラーメッセージが表示されます。同様に、セキュリティインシデントのフィールドに複数のオプションを選択できる選択リストがあり、選択リストに表示されていないフィールドにオプションをマップしようとすると、そのフィールドはセキュリティインシデントに入力されません。

c. または、新しい行の [検索] フィールドに値を入力します。

d. フォームの左側の [入力式] フィールドで[イベント **ID]** を左クリックして選択します。
ドラッグアンドドロップ機能を使用して、新しいフィールドの横にマッピングします。

7. オプション: スクリプトエディターを開き、編集を続行します。

(Optional) スクリプトエディターの詳細については、「スクリプトエディターを使用して ArcSight ESM 統合のために相関イベント値をフォーマットする」を参照してください。インシデント生成フィルタリング条件

8. オプション: 先行するフィールドマッピングステップを完了したら、インシデント生成条件ビルダーで同じフィールド値を使用して、SIR セキュリティインシデントを作成するために、受信相関イベントが満たす必要がある追加の条件を定義することができます。
インシデント生成条件を設定するには、次のステップを実行します。

a. フォームの [インシデント生成条件] セクションまでスクロールし、[条件に基づいてフィルター] チェックボックスをオンにして、オプションを有効にします。

(Optional) フィルター条件ビルダーが表示されます。これらのフィルターを使用して、フィールドで説明されている特定の条件に一致するセキュリティインシデントを作成します。

フィルター条件ビルダーの最初のフィールドの選択リストにあるオプションは、取り込んだイベントの [相関イベントサンプルの取り込み] セクションに表示されるフィールドと一致します。これらのフィールドは動的であり、取り込む相関イベントに応じて変化します。入力する条件は

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

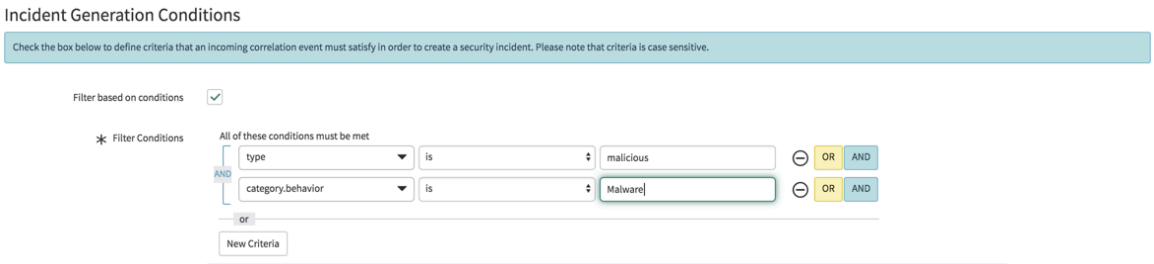
大文字と小文字が区別され、ArcSight ESM 相関イベントの値と正確に一致する必要があります。

条件ビルダーの選択リストとフィールドを使用して、最初の行のフィルターを設定します。

b. 条件を追加するには、フィールドの右側にある **[AND]** または **[OR]** をクリックします。
[**AND**] を選択した場合は、すべての条件に一致する必要があります。**[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。

c. オプション: 2 行目で、2 番目のフィルター条件を設定します。

(Optional) 次の画像は、セキュリティインシデントが作成される前に一致する必要がある 2 つの条件を含む例です。



(Optional) 入力した両方のフィルタリング条件に一致した場合にのみセキュリティインシデントが作成されるように、インシデント生成条件を設定しました。

この種のインシデント生成条件フィルタリングでセキュリティイベントを絞り込むことができ、基になる相関検索を変更することなく作成する不要なセキュリティインシデントの数を制限したり、ArcSight ESM でイベントをフィルターで除外したりすることができます。追加のフィルタリング条件を設定する場合、すべての条件に一致する相関イベントのみがインシデントにマップされます。

> **注:**
> イベントフィールド名に引用符 ("")、ハイフン ('')、アンダースコア (-)、またはアンパサンド (@) などの特殊文字が含まれている場合、これらの文字はマッピング変換のために置き換える必要があり、重複イベント名が作成される可能性があります。マッピングは適切に実行できますが、重複するイベント名を持つフィールドを区別するために数値のサフィックスが追加されます。たとえば、最初のイベントフィールドが events.event で、2 番目のイベントフィールドが events.event の場合、残りの標準的なテキスト文字は同じであるため、これらのフィールドは一意に識別されません。この場合、サフィックスが 2 番目のイベントフィールドに追加され、フィールド名が「events.event(1)」に変更されます。

類似の相関イベントを処理して重複インシデントを防止するイベント集計基準

9. オプション: 重複セキュリティイベントが作成されないように、追加のイベント集計条件を定義して、受信する相関イベントをオープンセキュリティインシデント別に集計します。
基準を設定するには、以下のステップを実行します。

a. フォームで [イベント集計基準] セクションにスクロールして、[集計条件] チェックボックスをオンにして、このオプションを有効にします。

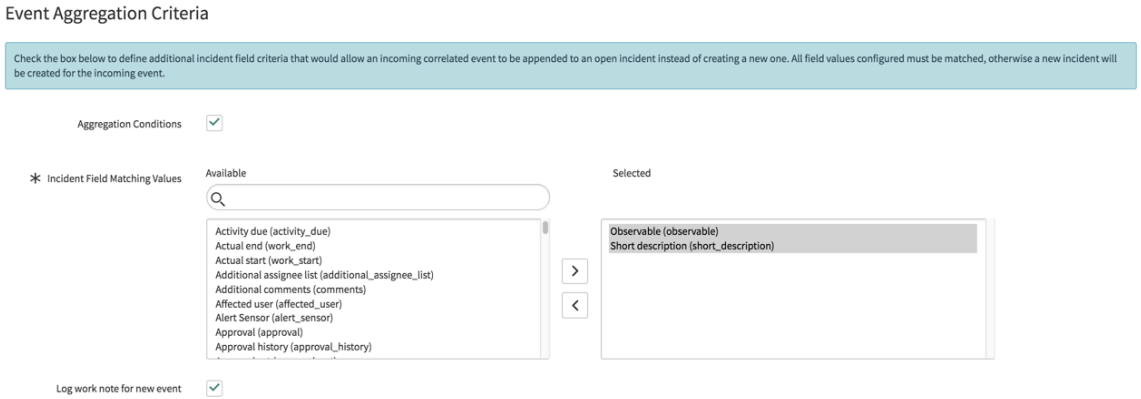
(Optional) [値が一致するインシデントフィールド] 列が表示されます。これらのフィールド名は、SIR セキュリティインシデントで構成されたカスタムフィールドを含むセキュリティインシデントのフィールドです。

b. [利用可能] リストから、Now Platform の既存のセキュリティインシデントで照合するフィールド値を選択し、[選択済み] リストに移動させます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

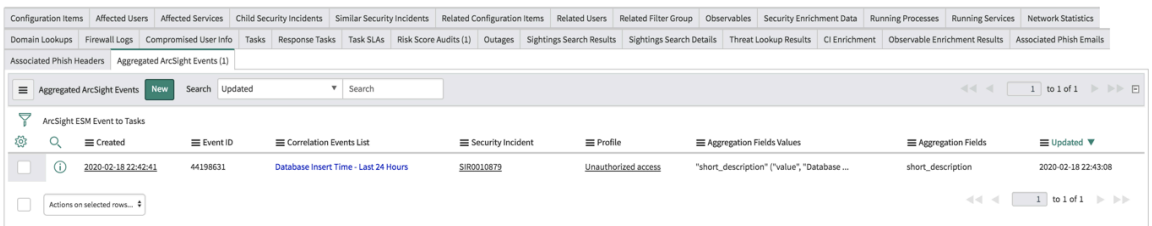
(Optional) この受信相関イベントを既存のセキュリティインシデントに追加するには、選択するすべてのフィールド値が一致する必要があります。これには、複数の相関イベントフィールド値がマッピングされている可能性がある [観測事象] や [構成アイテム] などのフィールドが含まれます。すべての値が一致している必要があります。値のサブセットのみが一致した場合、イベント集計条件は満たされず、新しいセキュリティインシデントが作成されます。複数値フィールドのマッピングについては、以下のスクリーンショットを参照してください。



新しい相関イベントが、マッピングステップの集計フィールド条件で選択されたすべての値と一致する場合、新しい相関イベントは、同じフィールド値を持つ最新のオープンセキュリティインシデントに自動的に追加されます。セキュリティインシデントを扱う SOC アナリストは、セキュリティインシデントの関連リストで、追加されたすべての集計相関イベントを表示できます。セキュリティインシデントの集計された相関イベントはすべて、[集計された **ArcSight** イベント] 関連リストに表示されます。このリストには、関連するタイムスタンプと集計されたフィールド値の詳細が表示されます。この情報は、これらの相関イベントが既存のセキュリティインシデントに集計される理由を理解するのに役立ちます。このタブが表示されない場合は、[関連リンク] の下のレコードの左側にスクロールし、[すべての関連リストを表示] リンクをクリックします。

注:
この関連リストが表示されない場合は、次のステップを実行します。

- [セキュリティインシデント] フォームヘッダーを右クリックし、 構成 > 関連リスト.
- [利用可能] リストで [集計された **ArcSight** イベント] を選択し、[選択済み] リストに移動して [保存] をクリックします。
- [関連リストを表示] をクリックします。[関連リスト] セクションに [集計された **ArcSight** イベント] タブが表示されます。



c. オプション: セキュリティインシデントでイベントが集計されるたびに作業メモを記録するには、このチェックボックスをオンにしてこのオプションを有効にします。
作業メモには、新しい相関イベントが追加されたことが、相関イベントの詳細へのリンクとともに記録されます。

相関イベントから SIR セキュリティインシデントのフィールドに値を正常にマッピングしました。また、インシデント生成フィルタリング基準を使用してセキュリティインシデントの作成を制

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

限する追加条件も構成しました。また、イベントフィールド値が設定された集計基準に一致する場合は、相関イベントを既存の SIR セキュリティインシデントに集計しました。

10. いずれかを選択して、プロファイル構成を続行します。

ArcSight ESM イベントの取り込み統合のセキュリティインシデントをプレビューする

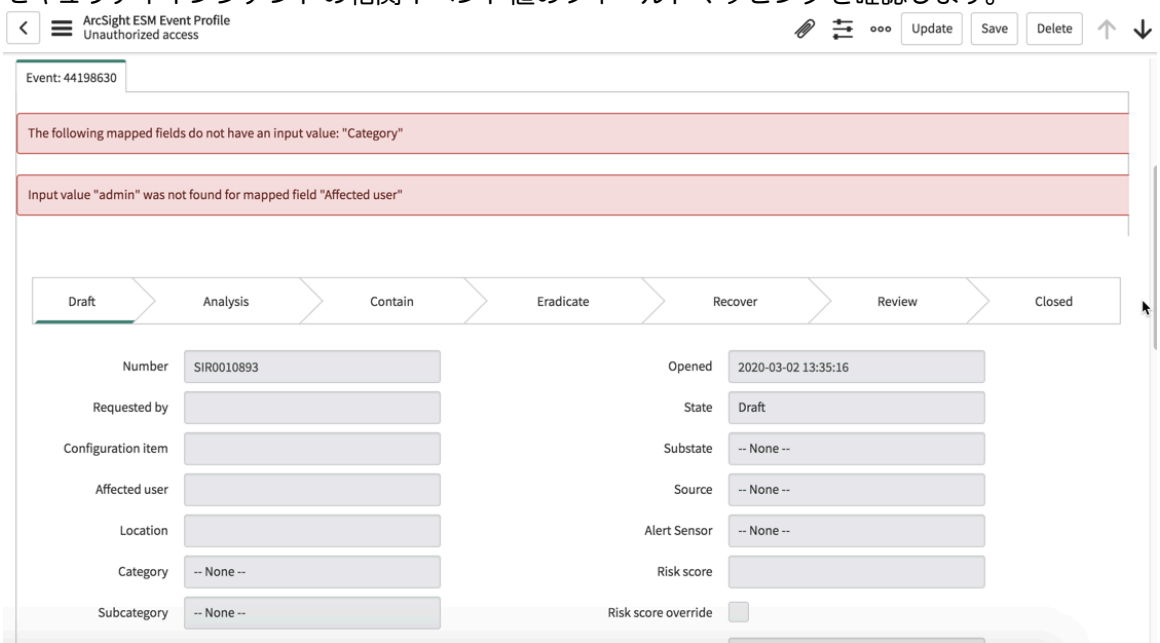
マッピングステップを完了したら、Now Platform セキュリティインシデントレスポンス (SIR) セキュリティインシデントでマッピングした値をプレビューします。このプレビューステップでは、セキュリティインシデントに表示するすべての相関フィールドがマッピングされていることを確認できます。

始める前に
必要なロール：sn_si.admin

このタスクについて
sn_si.admin ロールを持つユーザーは、セキュリティインシデントをプレビューし、必要に応じてマッピングを再編集して、エラーのあるフィールドを修正するか、欠落しているデータを入力します。プレビューが正常に完了しない場合、スケジュール設定ステップに進むことはできません。セキュリティインシデントのプレビューは、セキュリティインシデントレスポンス 製品の実際のインシデントとして保存されません。

手順

1. セキュリティインシデントのプレビューが表示されない場合は、進捗状況バーの [プレビュー] をクリックします。
2. [サンプルイベント ID] 選択リストから、アイテムを選択します。
   セキュリティインシデントが表示されます。フィールドの情報は変更しないでください。このビューは読み取り専用であり、このセキュリティインシデントのレコードは保存されません。
3. セキュリティインシデントの相関イベント値のフィールドマッピングを確認します。



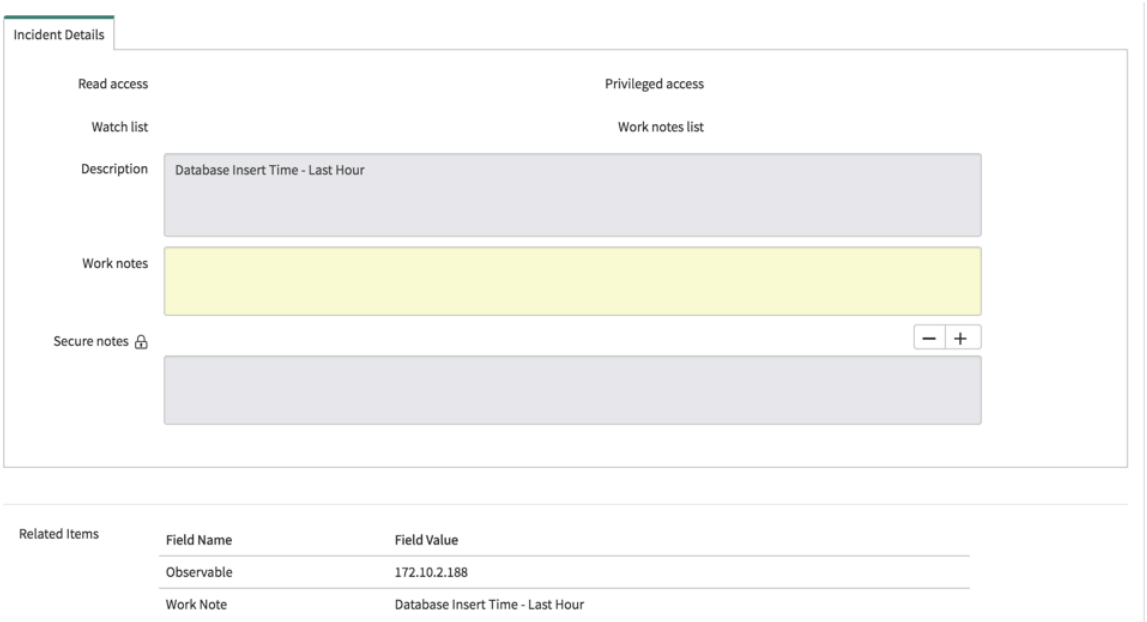
前の画像は、マッピングエラーのあるプレビューの例です。この例では、相関イベントのフィールド値に、SIR インシデントフォームの参照フィールドの許容値がありません。特定の値セットを持つ参照フィールドである［カテゴリ］フィールドの入力値が見つからなかったことを示すエラーメッセージが表示されます。その結果、このマップされたフィールド値は、さらに変更しないと SIR セキュリティインシデントフォームに表示されません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. このエラーを解決するには、進捗状況バーの [マッピング] をクリックします。
5. マッピングを編集して誤った値を修正するか、欠落しているデータを入力します。
6. マッピングを再度プレビューし、エラーメッセージに記載されているエラーの修正を続行します。

次の図は、すべてのエラーメッセージが解決された後のセキュリティインシデントの下半分にある [インシデントの詳細] タブの例です。この例では、 [説明] および [作業メモ] フィールドがマッピングされ、これらのフィールドには ArcSight ESM 相関イベントサンプルからプルされた値のペアの値が入力されます。



自動翻訳

次のタスク
エラーメッセージが表示されず、セキュリティインシデントのフィールドマッピングに問題がない場合は、次のステップでスケジュールを定義します。

ArcSight ESM イベントの取り込み統合のスケジュール作成

新しい相関イベントのポーリングまたはプルのスケジュールを定義できます。このステップでは、必要に応じて、相関イベント取得の既存設定を確認したり、スケジュールを変更したりすることができます。このステップでは、日付範囲を使用して履歴相関イベントを取得することもできます。

始める前に
必要なロール：sn_si.admin

このタスクについて
[スケジュール] ステップで履歴相関イベントを取り込むかどうかを選択できます。また、プロファイル構成に一致する将来の新しい相関イベントをポーリングする頻度も選択します。

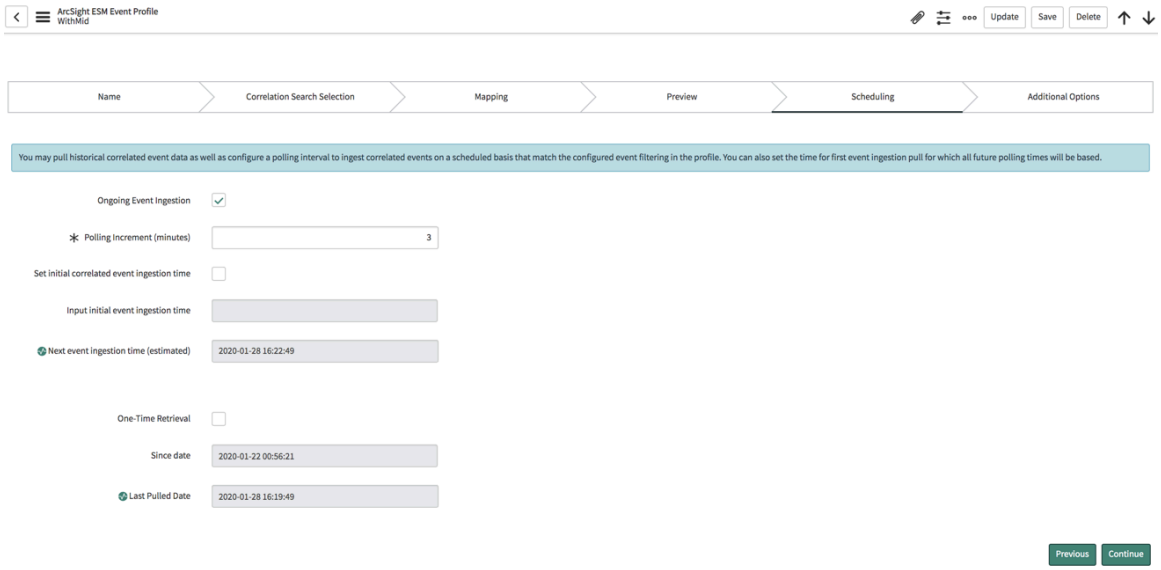
sn_si.admin ロールを持つユーザーは、これらのポーリング間隔をプロファイルごとに設定します。ArcSight ESM 相関イベントの取り込み統合のパフォーマンスは、ポーリング間隔が異なると影響を受けます。スケジューリングでは、ArcSight ESM サーバーのポーリングのオーバーヘッドを減らすことと、イベントが作成または更新されたときにできるだけ早く通知することのバランスを取ることをお勧めします。どのプロファイルにも 5 分のデフォルト値が設定されていますが、必要に応じてこの設定を 1 分に変更することもできます。

新規および更新された相関イベントのプル

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 進捗状況バーに [スケジュール] ページが表示されない場合は、[スケジュール] を選択します。
2. <ArcSight> コンソールから相関イベントをプルする方法とタイミングをスケジュールするものを選択します。



初期相関イベントの取り込み時刻をスケジュールする例として、現地時間の午前 4 時に 1 日 1 回実行される日次 ArcSight ESM セキュリティチェックがある場合、Now Platform インスタンスで対応する相関イベントプロファイルを現地時間午前 4 時 5 分に実行するように設定して、セキュリティ障害イベントをすぐにキャプチャし、セキュリティインシデントを作成できます。[初期イベントの取り込み] フィールドに「04 05 00」と入力します。[インクリメント (分)] フィールドに「1440 (24 時間)」と入力して、最初のイベントの取り込みから 24 時間後に次のイベントの取り込みをスケジュールします。初期イベントの取り込み時刻と次のイベントの取り込み時刻の両方がフィールドに表示されます。

3. この例の設定を構成するには、次のステップを実行します。

   a. [スケジュール] ページを表示した状態で、[進行中のイベントの取り込み] チェックボックスをオンにしてこのオプションを有効にします。

   b. [インクリメント (分)] フィールドに「1440 (24 時間)」と入力します。

   c. [最初の相関イベントの取り込み時刻を設定] チェックボックスをオンにして [初期イベントの取り込み (Initial event ingestion)] と [次のイベントの取り込み (Next event ingestion)] フィールドの編集を有効にします。

   d. [初期イベントの取り込み時刻] フィールドに「04 05 00」と入力します。
   [次のイベントの取り込み時刻 (推定)] フィールドに、次のイベントの取り込み時刻が表示されます。

4. [続行] をクリックして、[他のオプション] ページに移動します。

> **注:**
> 1 日に作成および集計できるセキュリティインシデントのデフォルト数とフロー期間は、[ArcSight ESM 統合の設定] で定義されます。必要に応じて、これらの設定を変更できます。詳細については、「イベントの取り込み統合のための ArcSight ESM 統合設定」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

その他のオプション：**SIR** インシデント状況に基づく相関イベントの更新とクローズの自動化

ArcSight ESM 統合には、セキュリティインシデントを作成する相関イベント、およびセキュリティインシデント番号、アサイン先グループ、SIR インシデント URL などの関連するインシデントの詳細を使用して、セキュリティインシデントが作成/クローズされると相関イベントを更新する機能を許可する双方向インターフェイスがあります。

始める前に

必要なロール：sn_si.admin

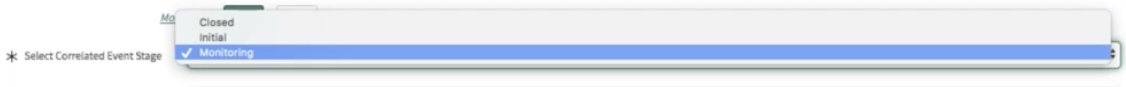
手順

1. 進捗状況バーに [その他のオプション] ページが表示されない場合は、[その他のオプション] を選択します。
2. 以下の手順に従って、セキュリティインシデントが作成されたときに相関イベントを更新するための構成を完了します。

   相関イベントステージが構成されていない場合：Now Platform インスタンスで相関イベントステージを構成していない場合、[相関イベントステージの更新] 選択リストには [ステージのアサイン：初期設定] のみが表示されます。ステージを構成するには、次の手順を実行します。

   - [ステージリソース ID を入力 (Enter Stage Resource ID)] フィールドにリソース ID を入力し、[送信] をクリックします。リソース ID が ArcSight ESM コンソールで検証され、次の画面が表示されます。

   - [保存] をクリックして新しいステージ ([監視]) を保存します。
   - [相関イベントステージを選択] ドロップダウンリストをクリックします。



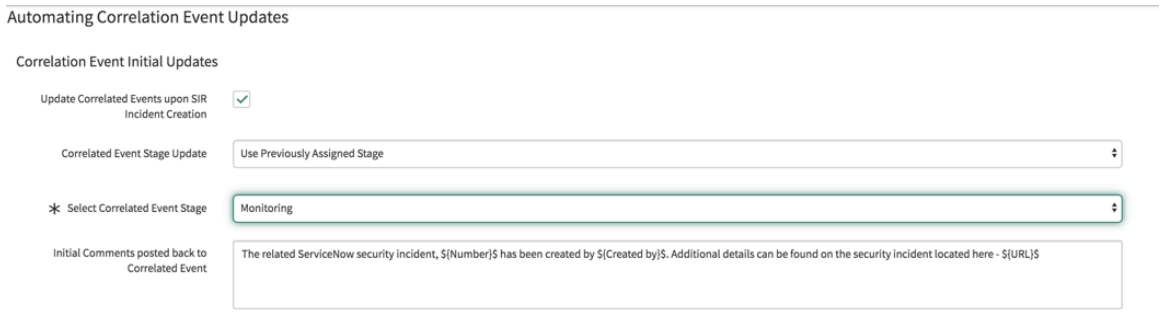
   - 新しく作成されたステージをリストから選択できます。

   相関イベントステージが既に構成されている場合：相関イベントステージを既に構成している場合は、次の手順を実行します。

   - [相関イベントステージの更新] 選択リストで [以前にアサインされたステージを使用] を選択します。
   - 次に示すように、 [相関イベントステージを選択] 選択リストから既存のステージを選択します。

自動翻訳

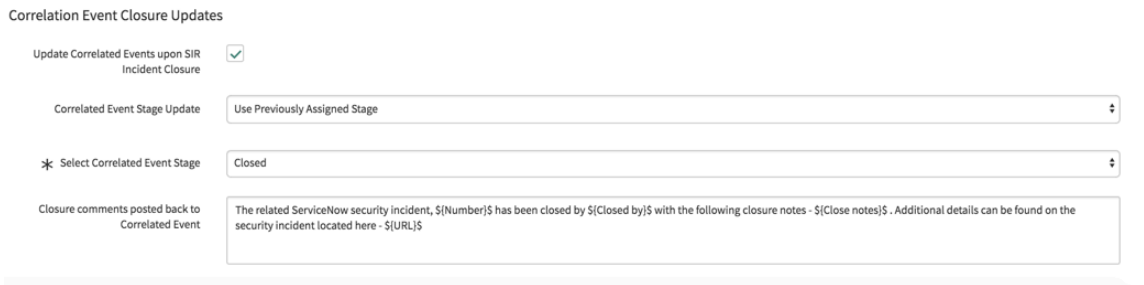
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



- 相関イベントに投稿される最初のコメント：相関イベントステージ値の更新に加えて、相関ステージ注釈にコメントを投稿することもできます。説明したとおり、セキュリティインシデントレスポンスインシデントフォームの任意のフィールドでのフォーマット ${field name}$ を使用した置換変数の追加または変更など、[コメント] セクションに表示されるデフォルトテキストの編集を行うことができます。

> **注:**
> ArcSight ESM コンソールで定義されたデフォルトのステージを使用することも、独自のカスタムステージを作成することもできます。新規ステージを作成するには、次のステップに従います。
>
> - ArcSight ESMコンソールで、 ファイル > 新規 > ステージ. [検査/編集 (Inspect/Edit)] タブが表示されます。
> - 新しいステージを定義します。[ユーザーが必要 **(User Required)]** チェックボックスをオンにしないでください。ステージが正しく定義され、イベントライフサイクル内の正しい位置にあることを確認します。

3. [相関イベントのクローズの自動化 (Automating Correlated Event Closure)] セクションでは、セキュリティインシデントがクローズされたときに更新する方法を定義できます。
4. フォームのフィールドに入力します。



5. [完了] をクリックして、構成を完了します。
   確認ダイアログが表示されます。これで統合のセットアップと構成が正常に完了しました。このプロファイルをアクティブ化して、スケジューリングに基づいて ArcSight ESM コンソールから相関イベントをプルします。

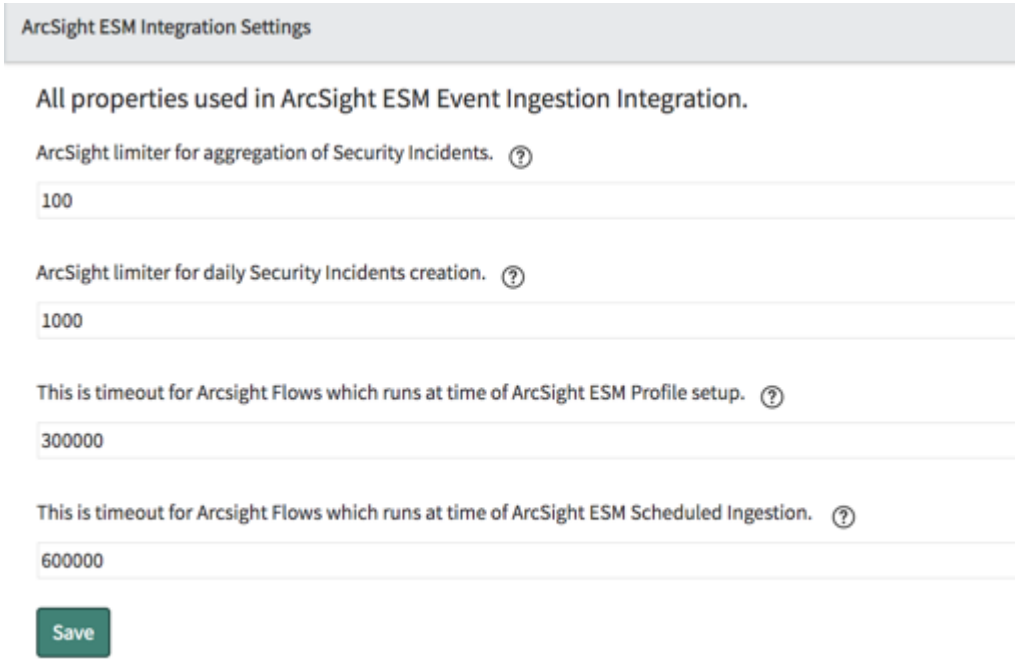
イベントの取り込み統合のための **ArcSight ESM** 統合設定

ArcSight ESM のデフォルトの取り込み設定を変更するには、このオプションを使用します。

システムプロパティを変更するには、 *`sn_si.admin`* ロールを持つユーザーとしてログインし、次の場所に移動します。 **ArcSight ESM** 統合 > **ArcSight ESM** 統合設定.

デフォルトの構成設定が表示されます。必要に応じて、これらの設定を変更できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

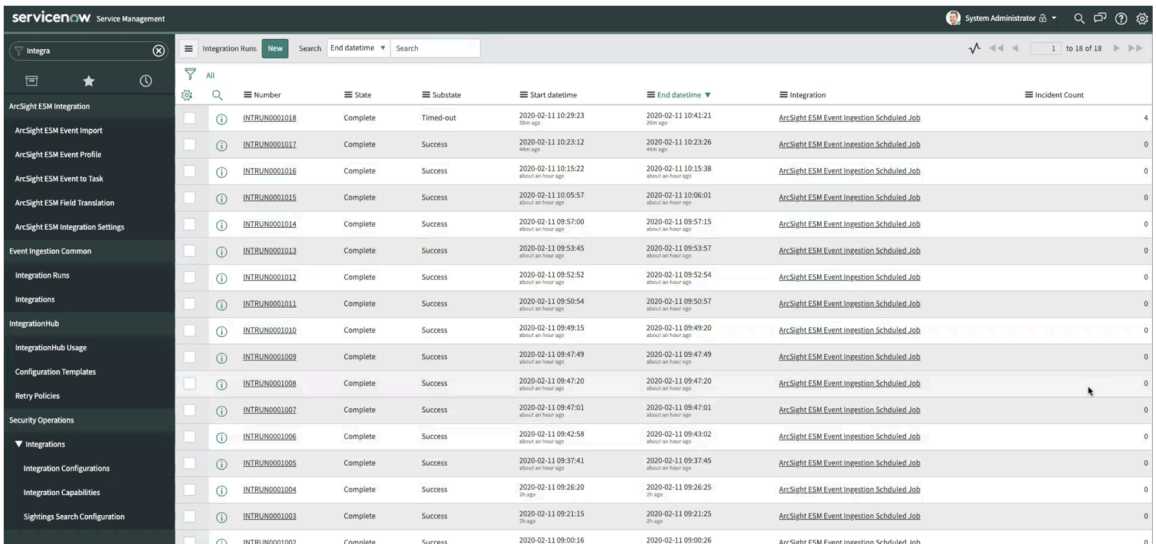


ArcSight ESM イベントの取り込み統合のトラブルシューティング

このセクションでは、イベントの取り込み中に発生する可能性のあるエラーのトラブルシューティング方法について説明します。

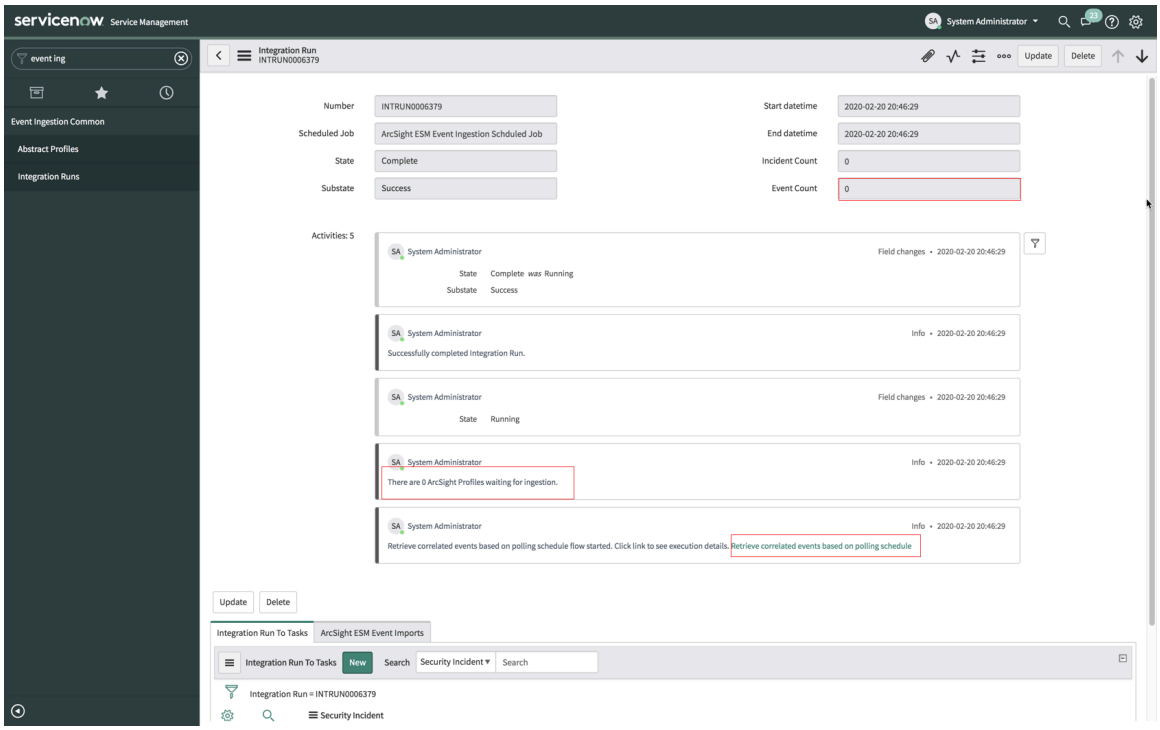
統合実行

次のように移動する。 イベントの取り込み共通 > 統合実行. 統合実行は毎分行われ、スケジュール済みジョブ中に取り込まれたイベントに関する詳細がキャプチャされます。



統合実行のリストと各実行のステータス ([成功]、[タイムアウト]、[待機中])、および作成されたセキュリティインシデントの数を確認できます。[番号] リンクをクリックして、詳細な [統合実行] ページにドリルダウンします。

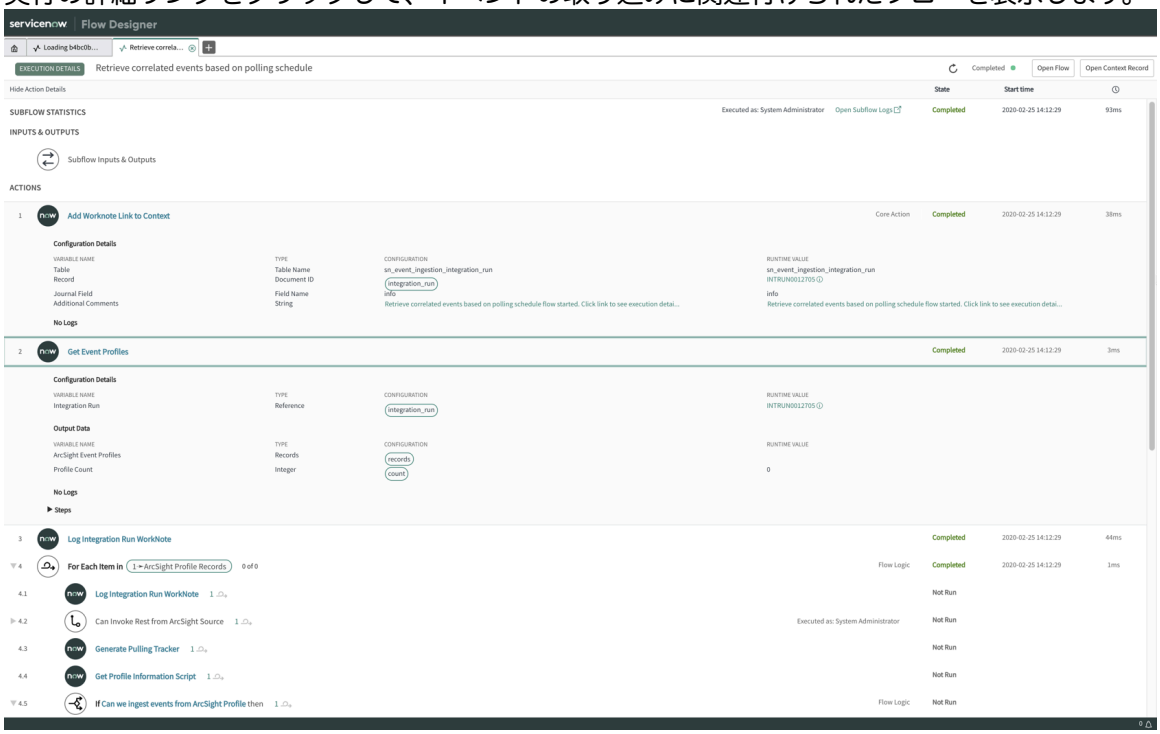
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



取り込まれたイベントの数、ステータス、セキュリティインシデントに変換されたイベント、取り込み中に実行されたさまざまなタスクなどの詳細を表示できます。さらに、リンクをクリックしてフロー実行の詳細を表示できます。

フロー実行の詳細

実行の詳細リンクをクリックして、イベントの取り込みに関連付けられたフローを表示します。



フローの一部として実行されたさまざまなアクションとサブフローを詳細に示す、フローのステップごとの実行を表示できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

イベントの取り込み統合のための **ArcSight ESM** プロファイルのコピー

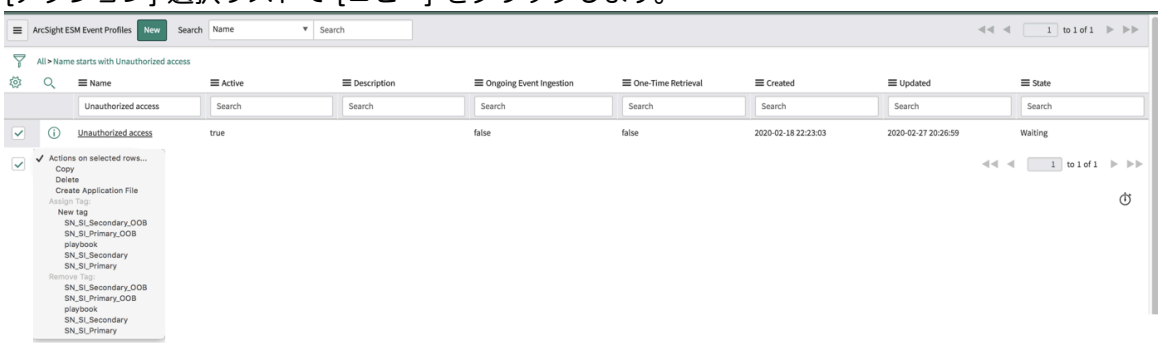
新しいプロファイルを作成する代わりに、既存のプロファイルとその関連設定をコピーします。複数のプロファイルを作成していて、既存のプロファイルの設定を再利用する場合は、時間を節約するためにプロファイルをコピーすることをお勧めします。

始める前に
必要なロール：sn_si.admin

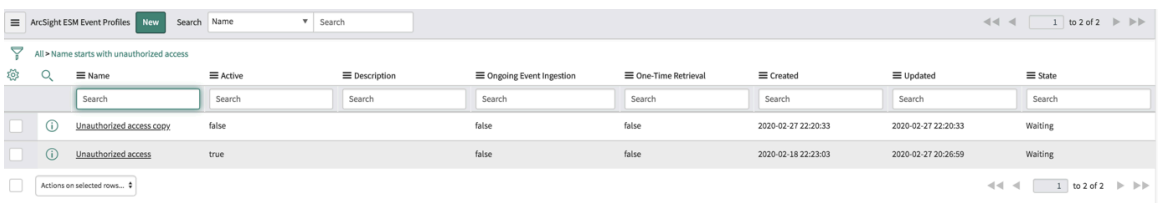
このタスクについて
sn_si.admin ロールを持つユーザーがプロファイルをコピーすると、プロファイルの重複を避けるためにプロファイル名が最初に変更されます。また、コピーされたプロファイルは無効 (false) であるため、構成が完了する前に誤って有効になることはありません。既にプレビューおよび検証したセキュリティインシデントのプロファイルをコピーし、既存のマップを使用します。

手順

1. 次のように移動する。 **All** (すべて) > **ArcSight ESM** 統合 > **ArcSight ESM** イベントプロファイル.
2. 表示される [ArcSight プロファイル] リストでコピーするプロファイルを選択し、選択した行の [アクション] 選択リストで [コピー] をクリックします。



プロファイルがコピーされ、リストに表示されます。コピーには、マッピングとスケジュール設定を含む元のプロファイルのすべての設定が含まれます。プロファイルの名前に「copy」が含まれています。元のプロファイルは有効ですが (true)、この時点でコピーは無効になります (false)。必要に応じて、コピーしたプロファイルの値を編集して名前を変更し、構成設定を新しいプロファイルに適用することもできます。



既存のプロファイルから新しいプロファイルに設定が正常にコピーされました。プロファイルをアクティブ化する必要があるため、[アクティブ] 列のステータスが false に設定されていることに注意してください。

スクリプトエディターを使用して **ArcSight ESM** 統合のために相関イベント値をフォーマットする

取り込まれた相関イベント値から直接マッピングされたフィールドに加えて、マッピングステップでスクリプトエディターを使用してセキュリティインシデントのフィールド値をフォーマットします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_si.admin

このタスクについて
スクリプトエディターは、ArcSight ESM 相関イベントフィールドの値を変更して、Now Platform SIR セキュリティインシデントでサポートされている値が [カテゴリ]、 [構成アイテム (CI)]、[観測事象]、およびその他のセキュリティインシデントフィールドにマッピングされるように変更します。

場合によっては、ArcSight ESM 相関イベント値は、セキュリティインシデントの [カテゴリ]、[構成アイテム (CI)]、および [観測事象] フィールドなどの参照フィールドにマップされます。sn_si.admin ロールを持つユーザーは、マッピングされたイベントフィールドの値を編集して、予想されるインシデントフィールドのフォーマットと値に合わせてフォーマットまたはデータ値を変換することができます。ArcSight ESM 相関イベントの値を SIR セキュリティインシデントのこれらのフィールドでサポートされている値に変換する場合は、スクリプトエディターを使用します。

手順

1. [マッピング] フォームを表示した状態で、リンクをクリックしてスクリプトエディターを開きます。
2. 選択リストから、編集する値の宛先フィールドを選択します。
3. または、[SIR インシデントフィールドマッピング] セクションで、フィールドの横にある角かっこアイコン [{}] をクリックして、そのフィールドのスクリプトエディターを開きます。

   場合によっては、 [構成アイテム] フィールドにスクリプトインクルードが適している場合があります。たとえば、相関イベントの場合、構成アイテムの値が一致しない可能性があります。

   次の図に示すように、[構成アイテム] フィールドの Now Platform CMDB で一致するホスト名が見つからない場合は、IP アドレスが見つかった場合に [構成アイテム] フィールドに入力されるようにルールを編集できます。

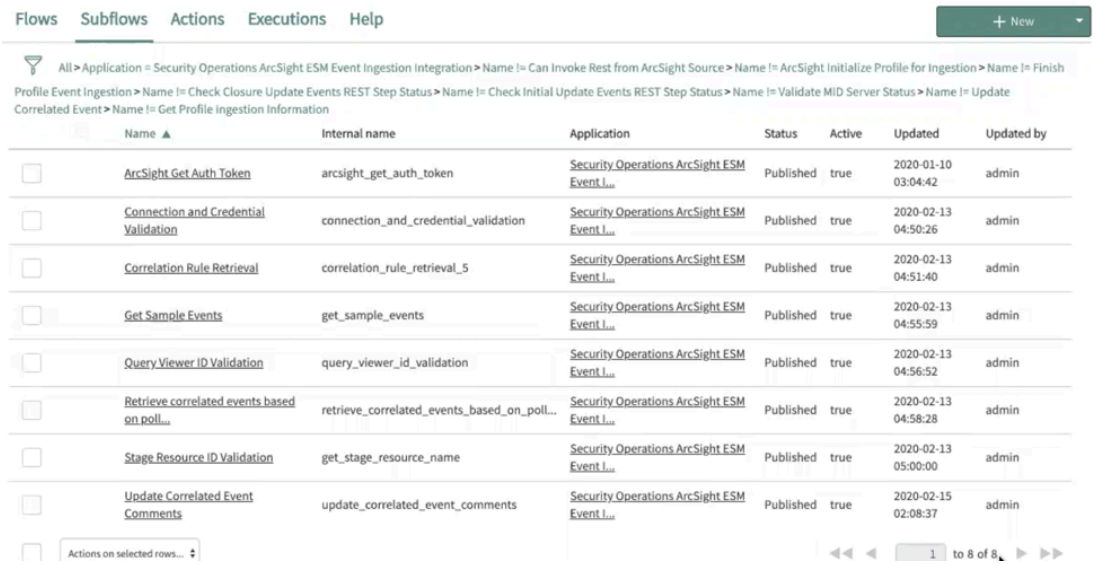
   エディターが開き、[宛先フィールド] にフィールドが表示されます。
4. スクリプトに変更を入力し、[更新] をクリックして変更を保存します。
   [ArcSight ESM フィールド変換] テーブルが表示されます。
5. テーブルを閉じて [マッピング] フォームに戻ります。

ArcSight ESM イベントの取り込み統合でのフローデザイナーの使用

統合ハブとフローデザイナーを使用すると、いくつものフロー、サブフロー、およびアクションを ArcSight ESM 統合で使用できます。

これらのサブフローを表示するには、次の場所に移動します **Flow Designer** > デザイナー をクリックし、[サブフロー] タブをクリックします。次の図は、プロファイルの作成時に使用される重要なサブフローと、スケジュール設定済みの取り込みジョブを示しています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



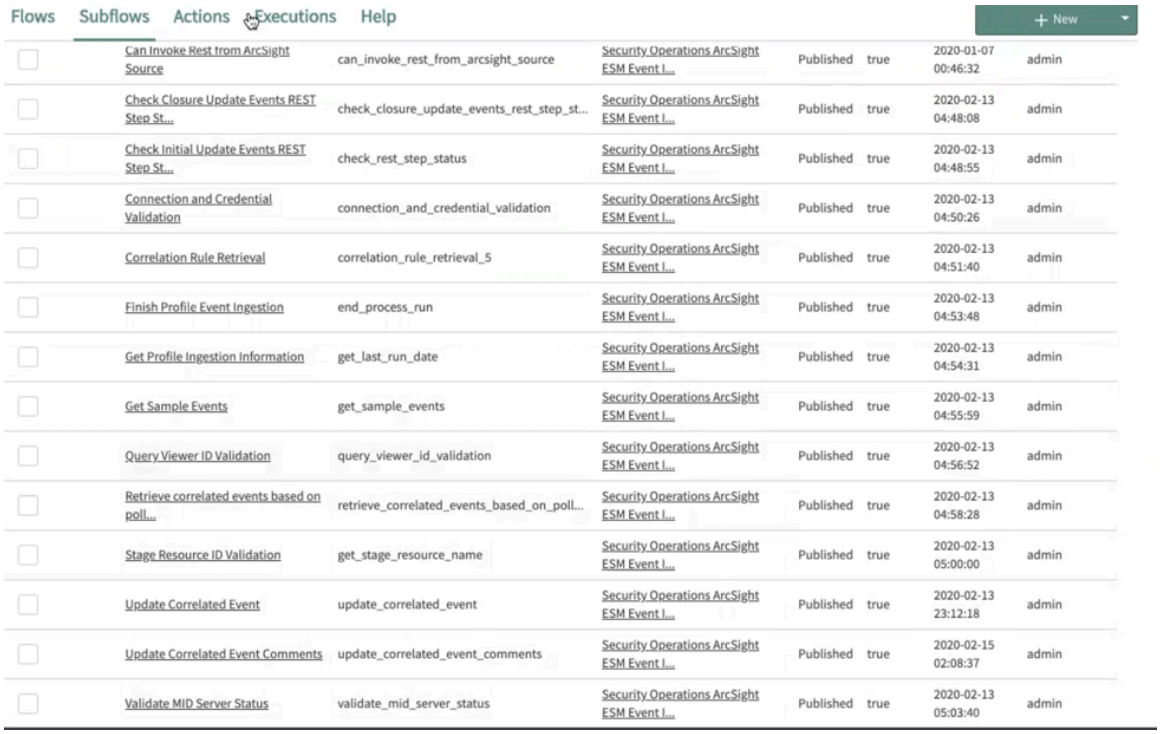
これらのサブフローを実行される順序で以下にリストします。

- [接続と資格情報の検証]：このサブフローは、ArcSight ESM サーバーとの ServiceNow 接続性と指定された認証情報を検証します。このサブフローは、次の **[ArcSight ESM -** イベントの取り込み]タイルで [構成] ボタンをクリックすると使用されます。 セキュリティオペレーション > 統合 > 連携の設定 ページ
- **[ArcSight** 認証トークン取得]：このサブフローは、ArcSight ESM Login Service を使用して、ユーザー名とパスワードから ArcSight ESM 認証トークンを生成します。Login Service は、他の ArcSight ESM エンドポイントを呼び出すために使用できる認証トークンを提供します。このサブフローは他のすべてのサブフローで使用されます。
- [クエリビューアー **ID** の検証]：このサブフローは、プロファイルの作成時に指定されたクエリビューアー ID が ArcSight ESM サーバーに存在するかどうかを確認します。
- [相関ルールの取得]：このサブフローは、クエリビューアー ID に基づいて相関ルールを取得します。
- [サンプルイベントを取得]：このサブフローは、ArcSight ESM サーバーからサンプル相関イベントをフェッチします。これらのサンプルイベントは、プロファイルの [マッピング] セクションのセキュリティインシデントフィールドにマッピングされます。
- [ステージリソース **ID** 検証]：このサブフローは、ArcSight ESM コンソールで指定されたステージリソース ID を検証し、リソース名をフェッチします。
- [相関イベントコメントを更新]：このサブフローは、プロファイルの [他のオプション] ページで [インシデント] の [初期] セクションと [クローズ] セクションで相関イベントのコメントを更新します。
- [ポーリングスケジュールに基づいて相関イベントを取得]：このサブフローは、ポーリング間隔に基づいて相関イベントをフェッチするスケジュール済みジョブを実行します。

実行中、上記のサブフローは、次に示すように他のいくつかのサブフローやアクションも直接的または間接的にトリガーします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



Can Invoke Rest from ArcSight Source	can_invoke_rest_from_arcsight_source	Security Operations ArcSight ESM Event I...	Published	true	2020-01-07 00:46:32	admin
Check Closure Update Events REST Step St...	check_closure_update_events_rest_step_st...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:08	admin
Check Initial Update Events REST Step St...	check_rest_step_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:55	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:50:26	admin
Correlation Rule Retrieval	correlation_rule_retrieval_5	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:51:40	admin
Finish Profile Event Ingestion	end_process_run	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:53:48	admin
Get Profile Ingestion Information	get_last_run_date	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:54:31	admin
Get Sample Events	get_sample_events	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:55:59	admin
Query Viewer ID Validation	query_viewer_id_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:56:52	admin
Retrieve correlated events based on poll...	retrieve_correlated_events_based_on_poll...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:58:28	admin
Stage Resource ID Validation	get_stage_resource_name	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:00:00	admin
Update Correlated Event	update_correlated_event	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 23:12:18	admin
Update Correlated Event Comments	update_correlated_event_comments	Security Operations ArcSight ESM Event I...	Published	true	2020-02-15 02:08:37	admin
Validate MID Server Status	validate_mid_server_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:03:40	admin

Amazon Web サービス (AWS) Security Hub 統合

AWS Security Hub は、AWS リソースに対する自動化された継続的なセキュリティチェックとベストプラクティスチェックを提供するクラウドセキュリティポスチャ管理 (CSPM) サービスです。

AWS Security Hub 統合の概要

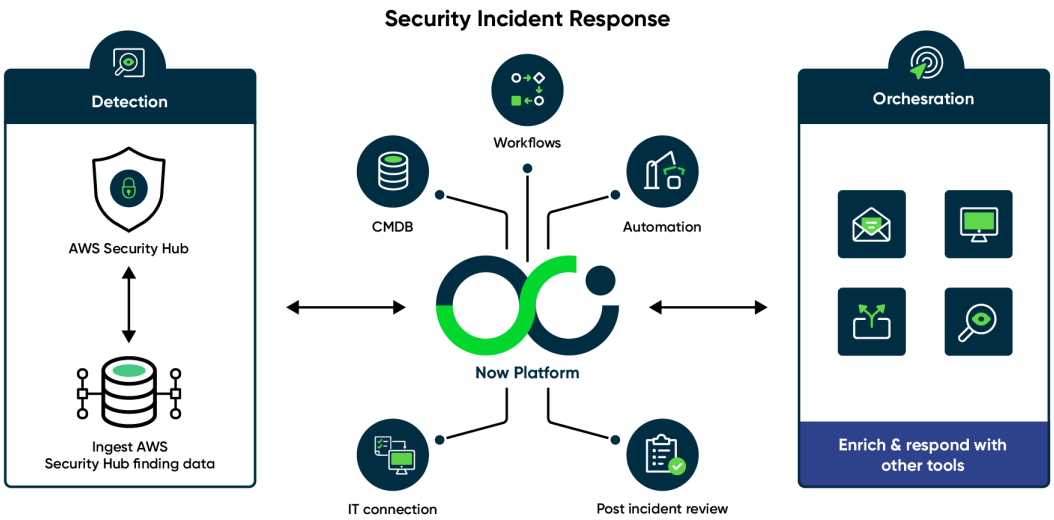
AWS Security Hub 構成の問題を特定できます。Security Hub は、検索結果と呼ばれるセキュリティアラートを集約します。 AWS Security Hub は、これらの検出結果を標準化された形式で生成し、より簡単に拡張、調査、および修復できるように優先順位を付けます。AWS Security Hub 統合を使用して Security Hub の検索結果を取り込み、セキュリティインシデントレスポンス でセキュリティインシデントを自動的に作成できます。

AWS Security HubSIR での統合は、双方向アーキテクチャに従います。SIRは、Security Hub検出結果データを取り込み、セキュリティインシデントを作成すると同時に、対応するセキュリティインシデントの更新でSecurity Hub結果を更新します。

AWS Security Hub と Now Platform セキュリティオペレーション アプリケーションとの統合方法については、次の図を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

主要な機能

この統合の主な機能を使用して、次のアクションを実行します。

- セキュリティインシデントの候補である AWS Security Hub の結果を検出し、これらのセキュリティインシデントの作成を自動化します。
- AWS Security Hub の検索結果とエンティティフィールドを SIR セキュリティインシデントフィールドにマッピングします。
- AWS Security Hub の検索結果をフィルタリングします。
- 検索結果を既存のオープンセキュリティインシデントに集計して、重複するセキュリティインシデントを作成する必要がないようにします。
- セキュリティインシデントレスポンスの AWS Security Hub 検索結果ステータスの更新を自動化して、セキュリティインシデントを作成してクローズできるようにします。

  注:
  ServiceNow はまた、セキュリティインシデントの作成、進捗状況、またはクローズに基づいて、AWS Security Hub 検索結果のステータスを更新します。この更新には、集計された調査結果と新しい調査結果のコメントも含まれています。

- 検索結果の取り込みをスケジュールして、セキュリティインシデントを定期的に作成します。
- AWS Security Hub 検索結果コメントを SIR 作業メモと同期します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

この統合の詳細

ドキュメント識別子	ドキュメントタイトル
AWS Security Hub 製品ドキュメントウェブサイト	AWS Security Hub ドキュメントウェブサイト
ServiceNow 製品ドキュメント Web サイト	ServiceNow 製品ドキュメント Web サイト

AWS Security Hub 統合を開始する

Security Operations プラグインの AWS Security Hub 検出結果統合をアクティブ化して設定し、ServiceNow® インスタンスおよび セキュリティインシデントレスポンス 製品と連動させます。

始める前に

必要なロール：sn_si.admin

AWS Security Hub 統合を使用する前に、ServiceNow Store からダウンロードする必要があります。

このタスクについて

次のセットアップチェックリストを確認し、スムーズな統合のためのすべてのタスクを完了したことを確認します。

チェックリスト

必要な ServiceNow® プラットフォームと セキュリティインシデントレスポンス ロールをアサインして確認します。	期待される結果を構成および検証するには、次のロールが必要です。 • admin ロールは、ServiceNow Store から統合をインストールし、sn_si.admin ロールをアサインします。 • 次のタスクを実行するには、sn_si.admin ロールが必要です。 ○ 統合を構成します。 ○ インシデントプロファイルを作成します。 ○ AWS Security Hub検索結果データフィールドをセキュリティインシデントフィールドにマッピングします。 ○ 進行中のインシデントの取り込みをスケジュールします。 ○ セキュリティインシデントレスポンス インシデントが作成されてクローズされたときに、インシデントの更新を有効にします。
AWS Security Hub に必要なロールをアサインします。	アプリケーションを登録して構成するには、AWS Security Hub で次のロールが必要です。 • SecurityHubReadOnlyアクセス • SecurityHubフルアクセス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト (続く)

AWS Security Hub 統合設定を確認する	次のように移動する。 **All** (すべて) > **AWS Security Hub** 検索結果の統合 > **AWS Security Hub** 検索結果の統合設定. 要件に応じてプロパティ設定を確認または変更します。
AWSポータルでアプリケーションを構成します。	AWS ポータルにアプリケーションを登録し、アプリケーションへの読み取りおよび書き込みアクセス権をユーザーに付与します。 詳細は、以下のトピックを参照してください。 • コンソールを使用した AWS Config の設定 • Security Hub の統合.

AWS Security Hub ポータルの登録と構成

AWS Security Hub ポータルにアプリケーションを登録し、アプリケーションへの読み取りおよび書き込みアクセス権をユーザーに付与します。

AWSポータルへの**ServiceNow®**ユーザープロファイルの登録

始める前に
必要なロール:AWSSecurityHubFullAccess

手順

1. AWS ポータルにログインします。
2. 次のように移動する。 **ID** とアクセス管理 **(IAM)** > ユーザー > 新規ユーザーを作成.
3. 次の表では、ユーザープロファイルを作成するために構成する必要があるフィールドについて説明します。

ユーザープロファイルの作成

フィールド	説明
ユーザーの詳細を指定 > ユーザー名	ユーザープロファイルの名前。
権限の設定 > グループにユーザーを追加	事前定義された権限ポリシーを使用して、ユーザープロファイルをグループに追加します。 好みに応じてグループを作成し、そのグループに権限ポリシーを割り当てることができます。後でユーザープロファイルをグループに追加すると、グループに割り当てられた権限ポリシーがユーザープロファイルに自動的に割り当てられます。
権限をコピー	ユーザープロファイルから権限をコピーし、それを新しいユーザープロファイルに割り当てます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ポリシーを直接添付	ユーザープロファイルの権限ポリシーとして AWSSecurityHubFullAccess を追加します。 必要に応じて、ユーザープロファイルに新しい権限ポリシーを割り当てます。
レビューおよび作成	ユーザープロファイルに追加したすべての詳細を確認します。

4. [ユーザーの作成] を選択します。
5. 表示されたポップアップウィンドウから [ユーザーを表示] を選択します。
6. ユーザープロファイルのアクセスキーと秘密アクセスキーを作成します。
これらのキーは、ServiceNow インスタンスから AWS Security Hub 統合にアクセスするために必要です。
7. 次のように移動する。 **AWS** サービス > 検索 > **AWS Security Hub** > **.**
8. [移動] *Security Hub*を選択します。
9. [AWS Security Hub を有効にする] ページで、[ダウンロード] を選択して AWS 構成を有効にします。
ファイルをダウンロードして、アカウントで実行します。これにより、さまざまな AWS レポートサービスからすべての情報を収集し、 AWS Security Hubに集約するアクセス許可が付与されます。
10. ページの下部にある [有効化 *AWS Security Hub*] を選択します。
*AWS Security Hub*ダッシュボードにすべての詳細が表示されるまで少し時間がかかります。
11. [リージョン] を [グローバル] から [米国東部 (オハイオ)] に変更します。
米国東部 (オハイオ) のコードは **us-east-2** です。すべての ServiceNow リソースがこのリージョンコードに割り当てられます。

AWS Security Hub 統合のインストールと構成

Now Platform インスタンスのServiceNow Storeから AWS Security Hub 統合をインストールして構成し、AWS Security Hub検索結果の取り込みを開始します。

始める前に
必要なロール：sn_si.admin

手順

1. AWS Security Hub 統合を ServiceNow Store からダウンロードしてインストールします。
2. 次のように移動する。 セキュリティオペレーション > 統合 > 統合設定.
3. AWS Security Hub タイルを検索し、[構成] をクリックします。
4. フォームのフィールドに入力します。

AWS Security Hub 構成フォーム

フィールド	説明
名前	AWS Security Hub インスタンス構成の名前。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
リージョン名	AWS Security Hubポータル のServiceNow ユーザープロファイルで割り当てた地域。
秘密キー	AWS Security Hubポータル のServiceNow ユーザープロファイル用に作成した秘密キー。
アクセス キー	ポータルのServiceNow ユーザープロファイル用に作成したアクセスキーAWS Security Hub

5. [**Submit** (送信)] を選択します。

タスクの結果
構成の検証と送信が正常に完了すると、各 Security Hub 検索結果取り込みサーバー構成が [セキュリティ統合] ページにタイルとして保存されます。

AWS Security Hub検索統合のためのプロファイルの作成

AWS Security Hub からデータを取り込み、対応するセキュリティインシデントを セキュリティインシデントレスポンスワークスペース で作成するために使用する Now Platform インスタンスにAWS Security Hubプロファイルを作成します。

始める前に
必要なロール：admin

このタスクについて
統合により、不正なアクセス試行やマルウェアなど、 AWS Security Hub プラットフォーム上のさまざまなタイプの検索結果のセキュリティインシデントを作成できます。これらのインシデントは、Now Platform インスタンスで構成したプロファイルに基づいて作成されます。すべてのインシデントは、最初にプロファイル内の設定された検索結果タイプに対して作成されます。作成した検索結果をさらにフィルタリングして、セキュリティインシデントを作成する検索結果を指定できます。

AWS Security Hubテナントの選択基準を満たし、AWS Security Hub API を介して利用可能なすべての検出結果は、最初に Now Platform インスタンスに取り込まれます。

手順

1. 次のように移動する。 **All** (すべて) > **AWS Security Hub** 検索結果の統合 > **AWS Security Hub** プロファイルの検索.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

AWS Security Hub - [検索結果取り込み構成] フォーム

フィールド	説明
名前	プロファイルの名前。 この名前は、プロファイルタイプを識別するのに役立ち、このプロファイルに関連付けられているセキュリティタグのデフォルト名でもあります。
アクティブ	プロファイルを有効にする場合に選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	プロファイルがアクティブな場合、 Now Platform が検索結果データをアクティブに取り込み AWS Security Hub フィルタリング条件に一致したときに、対応するセキュリティインシデントが SIR で作成されることを意味します。
ソース	検索結果を取り込むように構成した AWS Security Hub 統合テナント。複数のテナントが構成されている場合は、プロファイルに取り込む予定の検出タイプに適したテナントを選択します。
順序	2 つ以上のプロファイルがトリガー条件を共有する場合にフローが実行される順序を示す、このフィールドの値を入力します。 番号が最も小さいフローの優先度が最も高くなります。 操作の順序を設定するには、値を入力します。例：100、200、300、400。 デフォルトは 100 です。
説明	このプロファイルを他のプロファイルと区別するための追加テキスト。

AWS Security Hub検索結果フィールドのマッピング

個々の AWS Security Hub 検索結果フィールドを SIR セキュリティインシデントのフィールドにマッピングし、マッピングされたデータでインシデントを作成できるようにします。

始める前に
必要なロール：sn_si.admin

手順

1. マッピングページの [マッピング AWS Security Hub] セクションで、いずれかのサンプル取り込み方法を選択します。

サンプルの取り込み方法

フィールド	説明
すべてのデフォルトの検索フィールド	この取り込み方法を使用して、すべての検出結果フィールドの静的リストを表示します。この方法には、値のないデフォルトのフィールド名のみが含まれます。 この情報を使用して SIR フィールドとマッピングできます。
最近の AWS Security Hub 結果を取得	この取り込み方法を使用して、最新の検出結果データをインポートします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	デフォルトでは、5 つのサンプル結果を取り込むことができ、最大 20 個のサンプル結果を取り込むことができます。 サンプル検出結果フィールドの値は、プロファイルがサンプル検出結果を取り込むときに入力されます。これらの検索結果を **SIR** インシデントターゲットフィールドにマッピングできます。検出結果フィールドと値は個別のタブとして表示されます。
サンプルデータをインポート (Import Sample Data)	[**Import Sample Data**] を選択して、 AWS Security Hub からサンプル検出結果をインポートします。 このボタンは、[最近の AWS Security Hub 検索結果を取得] 取り込み方法を選択すると表示されます。 サーバーからサンプル結果を取得する AWS Security Hub 少し時間がかかります。 これらの結果を **SIR** インシデントターゲットフィールドにマッピングします。検出結果フィールドと値は個別のタブとして表示されます。

2. セキュリティインシデントに表示されるデフォルトのフィールドにフィールドを追加するには、次のアクションを実行します。

[SIR インシデントターゲットフィールド] セクションで、[⊕ Map another field ボタン。SIRフィールドのリストが表示され、そこから新しいフィールドを表示できます。

a. [セキュリティインシデント] 列で表示されているリストを展開し、フィールドを選択します。

> **注:**
> 同じセキュリティインシデントに複数の観測事象を表示できます。たとえば、[観測事象] フィールドは異なる値で複数回マッピングできます。同様に、[構成アイテム] フィールドと [作業メモ] フィールドは複数の値をサポートします。複数の値をサポートできないフィールドに 2 つの値をマッピングしようとすると、このフィールドは複数の値をサポートしていないというエラーメッセージが表示されます。同様に、セキュリティインシデントのフィールドに複数のオプションを選択できるリストがあり、リストに表示されていないフィールドにオプションをマップしようとすると、そのフィールドはセキュリティインシデントに入力されません。

b. [ソースフィールド AWS Security Hub] セクションからフィールドをドラッグして新しいフィールドにマッピングします。

c. フィールドに対応するチェックボックスをオンにすると、 AWS Security Hub に加えられた新規または更新された変更が、新しいインシデントデータでそれぞれの SIR で自動的に更新されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
ベースシステムでは、SIR にリンクされている新しいアラートに関連する AWS Security Hub 更新を受信するために、システムプロパティ sn_sec_security.finding_updates はデフォルトで True に設定されています。

- デフォルトでは、[影響を受けるユーザー]、[構成アイテム]、および [観測可能] フィールドはオンになっています。つまり、新しい観測事象、関連する構成アイテム、または影響を受けるユーザーがインシデントに追加されるたびに、その情報が自動的に抽出され、そのポーリング間隔中にセキュリティインシデントレスポンス (SIR) のそれぞれの関連リストに入力されます。
- その他のフィールドについては、 AWS Security Hubの結果に加えられた新規または更新された変更のフィールドに対応するチェックボックスをオンにする必要があります。これにより、それぞれの SIR インシデントデータが新しいインシデントデータで自動的に更新されます。

重要:
既存のデータを上書きすると、アナリストのデータが不安定になり、セキュリティインシデントのフィールド値によっても設定されている他の自動化も影響を受ける可能性があるため、この機能を選択する前にデューデリジェンスを行う必要があります。そのため、上書き機能を選択する前にデューデリジェンスを行うことが重要です。

3. フィールドを削除するには、[SIR インシデントターゲットフィールド (SIR Incident Target Fields)] セクションの入力式フィールドの横にある (アイテムを削除) ボタンを使用します。
4. [AWS Security Hub ソースフィールド] セクションのフィールド値を [SIR インシデントターゲットフィールド] セクションのフィールドにマップするには、次のいずれかのアクションを使用します。

   a. フィールド名 ([ID] など) をドラッグし、[SIR インシデントターゲットフィールド (SIR Incident Target Fields)] 列のフィールド名の横にドロップします。

   [AWS Security Hub ソースフィールド] セクションの任意の値を [SIR インシデントターゲットフィールド] セクションのフィールドと照合できます。マッピングプロセスで結果フィールドを見落としたり重複したりしないように、フィールドは色分けされています。ライトブルーのフィールドは、検出結果フィールドがまだ選択されておらず、セキュリティインシデントにマッピングされていないことを示します。受信検出結果フィールドをセキュリティインシデントの 1 つ以上のフィールドに関連付けることができます。灰色のフィールドは、検出結果フィールドが選択され、セキュリティインシデントのフィールドにマッピングされていることを示します。これにより、セキュリティインシデントに追加されたフィールド値と、マップされていない残りの重要な結果情報を視覚化できます。ただし、[AWS Security Hub ソースフィールド] セクションには、[SIR インシデントターゲットフィールド] セクションのフィールドと互換性のないフィールドがいくつかあります。このような値をマッピングすると、SIR の作成時には表示されません。

   b. テキストとフィールドの組み合わせを追加できます。
   たとえば、 名前の検索は ${name}$ です。ここでは、 検索名は 手動で入力でき、 ${name}$ は AWS Security Hub ソースフィールドセクションからマッピングされます。

   c. ソース検索フィールドを手動で入力して、ターゲットフィールドにマッピングできます。
   ソース検索フィールドを手動でマッピングするには、${field name}$ 形式を使用します。たとえば、結果フィールド [重大度] をマッピングする場合、形式は ${properties(severity)}$ です。

この統合は、特定の観測事象サブタイプを分類します。AWS Security Hub結果フィールドを SIR 観測事象フィールドにマッピングすると、Now Platformによって観測事象が自動分類され

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ます。受信 AWS Security Hub 観測事象を SIRの観測事象タイプに汎用的にマッピングする場合は、[観測事象] フィールドに [AWS Security Hub] フィールドをドラッグアンドドロップします。ただし、SIR で受信AWS Security Hub観測事象の観測事象タイプを把握している場合は、SIR [観測事象タイプ] フィールドに具体的にマッピングします。SIR の具体的な観測事象タイプの例には、[観測事象 (ドメイン名) (Observable(Domain name))]、[観測事象 (メールアドレス) (Observable(Email address))]、[観測事象 (IP アドレス (V4)) (Observable(IP address (V4)))]、および [観測事象 (ホスト名) (Observable(Host name))] が含まれます。

AWS Security Hub でフィールド値を検索しても、SIR セキュリティインシデントのフィールドに直接変換されないことがあります。これらの値については、マッピングステップでスクリプトエディターを使用してセキュリティインシデントのフィールド値をフォーマットできます。類似しているが同一ではない値をフォーマットする場合は、スクリプトエディターを使用します。

5. セキュリティインシデントのフィールド値と一致するように、AWS Security Hub検出結果からの新しいフィールドのフィールド変換をフォーマットするには、[**SIR** インシデントターゲットフィールド] ヘッダーの [ここをクリック] リンクをクリックします。

6. フィールド変換をサポートするフィールドを変更するには、 スクリプトフォーマットフィールド変換アイコンをクリックします。
フィールドの翻訳をサポートしているフィールドは、[カテゴリ]、[構成アイテム]、および [優先度]です。たとえば、[カテゴリ] の横にある アイコンをクリックします。AWS Security Hub結果フィールド翻訳スクリプトエディターが開きます。

7. スクリプトへの変更を入力し、[更新] をクリックして変更を保存し、 [マッピング] ページに戻ります。
たとえば、カテゴリの場合はスクリプトエディターで次のように定義します。

```
"<Incoming Security Hub finding Field Value>" : "<Category to assign to the Security Incident>".
```

このマッピングにより、プロファイルが構成済みのカテゴリのみを使用するようになります。

8. フィールド値を追加または削除して、マッピングを続行します。
インシデント生成条件ビルダーで同じフィールド値を使用して、セキュリティインシデントを作成するために受信検出が満たす必要がある追加の条件を定義できます。

9. [フィルタリングと集計] セクションに移動するには、[続行] をクリックします。

次のタスク

フィルター条件を定義して設定すると、セキュリティインシデントを作成する検索結果を指定できます。インシデント生成条件ビルダー ([フィルタリングと集計] セクション) で同じフィールド値 ([マッピング] セクションで定義) を使用して、セキュリティインシデントを作成するために受信検出が満たす必要がある追加の条件を定義できます。

AWS Security Hub検索結果の取り込みのためのフィルターとアグリゲーション基準の定義

フィルター条件を定義して設定することで、セキュリティインシデントを作成する受信検出結果を指定できます。同じ検出結果に対して別のセキュリティインシデントを作成する代わりに、受信検出結果をオープンセキュリティインシデントに追加できるように、追加のインシデントフィールド基準を定義することもできます。

検索結果 **AWS Security Hub** フィルタリング条件を設定してセキュリティインシデントを作成する

フィルタリング条件が一致した場合にのみセキュリティインシデントが作成されるように、フィルタリング条件を設定します。

始める前に

必要なロール：sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタスクについて
このタイプのフィルタリングは、セキュリティインシデントを分離し、作成するセキュリティインシデントの数を制限するのに役立ちます。追加のフィルタリング基準を設定すると、クエリまたはトリガーされたインシデント構成を変更することなく、必要な結果のみが取り込まれます。

セキュリティインシデントを作成するために、受信 AWS Security Hub 結果が満たす必要がある基準を定義するには、次の手順を実行します。

手順

1. [事前フィルタリング] セクションで [事前フィルターの適用] を選択します。

   このオプションを使用すると、特定の検索結果をフィルタリングし、検索結果の取り込みの負荷を軽減できます。

   [**API** フィルター] フィールドに、要件に従って JSON 条件を入力し、条件に基づいて特定の検出結果を除外します。たとえば、次の値を入力して、Security Hub でワークフローステータスが解決済みである検索結果を除外します。

   ```
   {"Filters"{
     "WorkflowStatus":[{
     "Comparison":"NOT_EQUALS",
     "Value": "RESOLVED"}]
    }
   }
   ```

   指定された条件に基づいて、 AWS Security Hub 検出結果が取り込まれ、 AWS Security Hub 検出結果の生テーブルに表示されます。

   次のように移動する。 **All** (すべて) > **AWS Security Hub** 検索結果の統合 > **AWS Security Hub** 生の検索 をクリックして生の検出結果データを表示します。

2. [フィルター条件の検索結果フィールドを選択] セクションで、[利用可能な検索結果フィールドを表示] を選択して、 AWS Security Hub 検索結果で利用可能なすべてのフィールドのリストを表示します。
   [すべての検索結果フィールド] リストから、[セキュリティインシデント生成条件] セクションに表示する検索結果フィールドを選択します。

   > **注:**
   > AWS Security Hub の結果に複数のフィールドと値が含まれています。[すべての検索フィールド] リストで、要件に従って検索フィールドを検索して選択できます。

3. [セキュリティインシデント生成条件] セクションで、[条件に基づいてフィルター] を選択し、セキュリティインシデントを作成するために受信 AWS Security Hub 結果が満たす必要がある基準を定義します。

   [フィルター条件] の最初のフィールドには、 AWS Security Hub 検索で使用可能な 200 フィールドのデフォルトリストと、[フィルター条件の検索フィールドを選択] セクションで選択した検索結果フィールドが含まれています。

   フィルター条件の 2 番目のフィールドには、条件演算子が含まれています。選択したオプションによって、結果を取り込むために満たす必要のある条件が決まります。

   フィルター条件の 3 番目のフィールドには、利用可能な検索フィールドでサポートされる値が含まれています。入力した検出結果フィールドが検出結果の値と一致していることを確認します。

   たとえば、複数の値を持つ次のフィールドに は 、フィルター条件 contains を使用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ワークフロー (ステータス)
- WorkflowState

4. 条件ビルダーのリストとフィールドを使用して、最初の行のフィルターを設定します。
5. 条件を追加するには、**[AND]** または **[OR]** をクリックします。
   - [**AND**] を選択した場合は、すべての条件に一致する必要があります。
   - **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。
6. 2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。

タスクの結果
フィルタリング条件に基づいて、 AWS Security Hub 検出結果が SIR にインポートされます。次のように移動する。 **All** (すべて) > **AWS Security Hub** 検索結果の統合 > **AWS Security Hub** インポートの検索 をクリックして、インポートされた結果を表示します。

AWS Security Hub検索結果をセキュリティインシデントにアグリゲートする条件を定義します

類似の重複する可能性があるインシデントを作成するのではなく、既存の SIR セキュリティインシデントに受信 AWS Security Hub 結果を集計する追加のインシデント集計基準を定義します。この追加の集計では、各プロファイルのフィールド一致値基準を使用して、関連するすべてのインシデントデータを単一のセキュリティインシデントに配置することで、アクティブな重複するセキュリティインシデントの数を減らすことができます。

始める前に
必要なロール：sn_si.admin

このタスクについて
新しいインシデントが、マッピングステップの集計フィールド条件で選択されたすべての値と一致する場合、新しいインシデントは、同じフィールド値を持つ最新のオープンセキュリティインシデントに自動的に追加されます。セキュリティインシデントを扱う sn_si.analyst ロールを持つユーザーは、セキュリティインシデントの関連リストで、追加されたすべての集計インシデントを表示できます。
セキュリティインシデントのすべての集計 AWS Security Hub 結果は、[AWS Security Hub] 関連リストに表示されます。このリストには、関連するタイムスタンプと集計されたフィールド値の詳細が表示されます。この情報は、 AWS Security Hub 検出結果が既存のセキュリティインシデントに追加される理由を理解するのに役立ちます。

手順

1. 新しいインシデントを作成する代わりに、受信した AWS Security Hub 結果をオープンセキュリティインシデントに追加できるようにする追加のインシデントフィールド基準を定義するには、[集計条件] オプションを選択します。
2. [値が一致するインシデントフィールド **(Incident fields with matching values)]** フィールドに、Now Platform インスタンスの既存のセキュリティインシデントで照合するフィールド値を入力します。
   集計基準が満たされ、この受信インシデントを既存のセキュリティインシデントに追加できるように、複数選択入力フィールドで選択したすべてのフィールド値が一致する必要があります。この選択は、複数のフィールド値を持つ可能性がある [観測事象] や [構成アイテム] などのフィールドがマッピングされる *AND* 条件を意味します。値のサブセットのみが一致した場合、 AWS Security Hub 検索結果の集計条件は満たされず、新しいセキュリティインシデントが作成されます。
3. 複数のフィールド一致条件を追加するには、[新しい基準を追加] をクリックします。
   定義した複数選択フィールド条件のいずれかが満たされると、集計が行われます。この選択は *OR* 条件を意味します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. 新しい検出結果がセキュリティインシデントに追加されたときにその検出結果の作業メモを更新するには、[新しい検出結果の作業メモをログ記録] を選択します。

   作業メモには、新しい検出結果が追加されたことが記録され、検出結果の詳細へのリンクが含まれています。作業メモの記録では、マッピングセクションの作業メモフィールドに追加した詳細も更新されます。

5. スケジュールを設定するには、[続行] をクリックします。

タスクの結果
集計条件に基づいて、 AWS Security Hub 結果が集計されて作成され、 SIR インシデントが作成されます。次のように移動する。 **All** (すべて) > **AWS Security Hub** 検索結果の統合 > **AWS Security Hub** タスクに対する検索結果 作成済みのセキュリティインシデントのリストを表示します。

次のタスク
プロファイルの基準に一致する検索データと検索インシデントを取得するスケジュールを設定します。

AWS Security Hub検索の取得をスケジュール

検出結果データを取得し、プロファイルの基準に一致する AWS Security Hub 検出結果を取り込むスケジュールを設定します。

始める前に
必要なロール：sn_sni.admin

このタスクについて
AWS Security Hub 検出プロファイル構成に一致する将来のAWS Security Hub検出結果をポーリングする頻度を計画できます。

ポーリング間隔は、各プロファイルで個別に設定されます。ポーリング間隔が異なると、 AWS Security Hub 所見統合のパフォーマンスに影響する可能性があります。スケジュールを設定するときは、インシデントの緊急度とシステム負荷のバランスを取るように計画してください。すべてのプロファイルに 1 分のデフォルト値が設定されています。この設定は、インシデントの緊急度とシステムの予想される負荷に基づいて変更できます。

特定のポーリング間隔でインシデントに追加されたアラートは処理されてから、 AWS Security Hub アラート関連リストとコメントに追加されます。

手順

1. スケジュールフォームで、フィールドに入力します。

   スケジュールを構成して、 AWS Security Hub テナントから結果をプルする方法とタイミングを定義します。

   スケジュールフォーム

フィールド	説明
継続的な検索結果の取り込み	Now Platformインスタンスが新しいインシデントの AWS Security Hub テナントからプルする進行中の検索結果の取り込み。トリガーされた検出結果が検出され、セキュリティインシデント生成のフィルタリング基準が一致すると、セキュリティインシデントが作成されます。
クローズ済み結果のポーリング	解決済みのポーリング結果。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	これらの検出結果は、進行中のインシデントの取り込み中に取り込まれます。
ポーリングインクリメント (分)	定義されたポーリング頻度 (分単位)。
初期検索の取り込み時刻を設定	設定された日時に基づく検索結果の取り込み。 このオプションを使用して、最初の取り込みに対する特定の日時を定義できます。それ以降の取り込みはポーリング間隔の時間に基づいて決まります。
入力 初期検索の取り込み時刻	インシデントの取り込みに指定した日時。
1 回限りの取得	履歴 AWS Security Hub 所見を 1 回だけ取得し、データの調整を行うには、このチェックボックスをオンにします。このチェックボックスをオンにすると、約 90 日間までのオープンおよびクローズ済みの AWS Security Hub 結果がすべてプルされます。 データを処理するときは、進行中の検出結果と履歴データの両方がプルされますが、進行中の検出結果の処理は履歴プルよりも優先されます。そうしないと、期間と取り込まれる結果の数に基づいて、履歴プルに時間がかかる場合があります。 **注:** 取得された履歴 AWS Security Hub 所見は、 セキュリティインシデントレスポンス アプリケーション内での重複を防ぐために重複排除チェックを受けます。
開始日	履歴検出結果が AWS Security Hubから取り込まれてからの日付。 **注:** 検出結果データは、およそ過去 90 日間から取得されたものです。

[スケジュール] ページでは、 AWS Security Hub テナントから検索結果をプルする方法とタイミングを定義できます。

2. [他のオプション] ページに移動するには、[続行] をクリックします。

SIRインシデントステータス別にAWS Security Hub検索の更新とクローズを自動化する

SIRインシデントのステータスに従って、AWS Security Hub結果の更新とクローズを自動化します。AWS Security Hub統合には双方向インターフェイスがあり、検索結果の取り込みでセキュリティインシデントを作成し、SIRインシデントの変更に応じて検索結果のステータスを更新できます。

始める前に
必要なロール：sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. フォームで、詳細を入力します。
   指示に従って、SIR でセキュリティインシデントを作成またはクローズするときに、AWS Security Hub結果を更新するための構成を完了します。

   [インシデントの更新の自動化] フォーム

カテゴリ	フィールド	説明
ステータスの更新	SIR インシデントステータス	SIRインシデント状況のリストを表示します。このリストからオプションを選択して、 Security Hub 検索ステータスにマッピングします。
	Security Hub ステータスの検索	Security Hubワークフローステータスのリストを表示します。 検出結果のワークフローステータスは、対応する SIR ステータスのインシデントステータスが変更されると、AWS Security Hub に更新されます。
優先度を更新	SIR インシデント優先度	SIRインシデントの優先度レベルのリストを表示します。このリストからオプションを選択して、 Security Hub 検索の優先度レベルにマッピングします。
	Security Hub 検索の優先度	Security Hub重大度レベルのリストからオプションを選択します。 検出結果の重大度は、対応するセキュリティインシデントの優先度が変更されると、 AWS Security Hub に更新されます。
作業メモを更新	対応するインシデントの作業メモが更新されたときにSecurity HubSIRのメモセクションを更新するには、このオプションを選択します。 SIRの作業メモセクションには、Security Hub検出結果のメモセクションでサポートされているため、512 文字の制限があります。	
追加コメントを更新	選択すると、[AWS Security Hub 結果コメント] セクションがインシデント SIR 入力した追加のコメントで更新されます。	
解決メモを更新	SIRインシデントの解決時に入力した解決メモで [AWS Security Hub終結コメント] セクションを更新する場合に選択します。	

   注:
   作業メモの各更新は、 Security Hub 検出結果のメモセクションの最後の更新を上書きします。SIRインシデントに関連する作業メモを追加することをお勧めします。

2. [完了] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のタスク
プロファイルは [待機中] ステータスに移行します。セットアップと構成が完了したことを示す確認メッセージが表示されたら、プロファイルを有効にできます。

SIRAWS Security Hub結果取り込み後のフォーム

Now PlatformがAWS Security Hub結果を取り込むと、セキュリティインシデントが作成され、そのセキュリティインシデントレコードが更新されます。

作業メモ

インシデントが集計され、AWS Security Hub検索結果の取り込みのためのフィルターとアグリゲーション基準の定義で [新しい検索の作業メモを記録] オプションを構成した場合、作業メモが投稿されます。

生のインシデントデータを含む内部結果インポートレコードを表示することもできます。

[ここをクリック] リンクをクリックすると、AWS Security Hub 環境でレコードを表示できます。次の例は、AWS Security Hub 環境でのレコードを示しています。

集計された **AWS Security Hub** 結果

集計された AWS Security Hub 結果の表示: セキュリティインシデントに集計されたインシデントを表示します。次のように移動する。 すべての関連リストを表示 > 集計された **AWS Security Hub** 検索結果.

セキュリティインシデントの作成：リストからインシデントを選択し、[アクション] メニューをクリックして、[セキュリティインシデントの作成] をクリックします。このオプションで、インシデントの新しいセキュリティインシデントを作成できます。このインシデントは親セキュリティインシデントからは集計されません。

Carbon Black - インシデント拡張統合

Carbon Black 統合を使用して、API を使用してセキュリティインシデントに関連付けられているエンドポイントに対するクエリや操作を行うことで、セキュリティインシデントを調査および対処します。

Carbon Black - インシデント拡張統合のリソースを見つける

- Carbon Black - インシデント拡張統合を開始する
- Security Operations Carbon Black 統合 - 実行中のプロセスを取得フロー
- [Security Operations Carbon Black 統合 - ホストを隔離] フロー
- Security Operations Carbon Black 統合 - ホスト隔離削除フロー

統合の概念を理解する

- 提供される ServiceNow 統合のタイプ
- セキュリティオペレーション ワークフロートリガー

ServiceNowのリソースからサポートを受ける

- Security Operations Community で質問や回答をする
- Known Error Portal で既知のエラー記事を検索

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 連絡先 カスタマーサービス & サポート
- Madrid にアップグレード

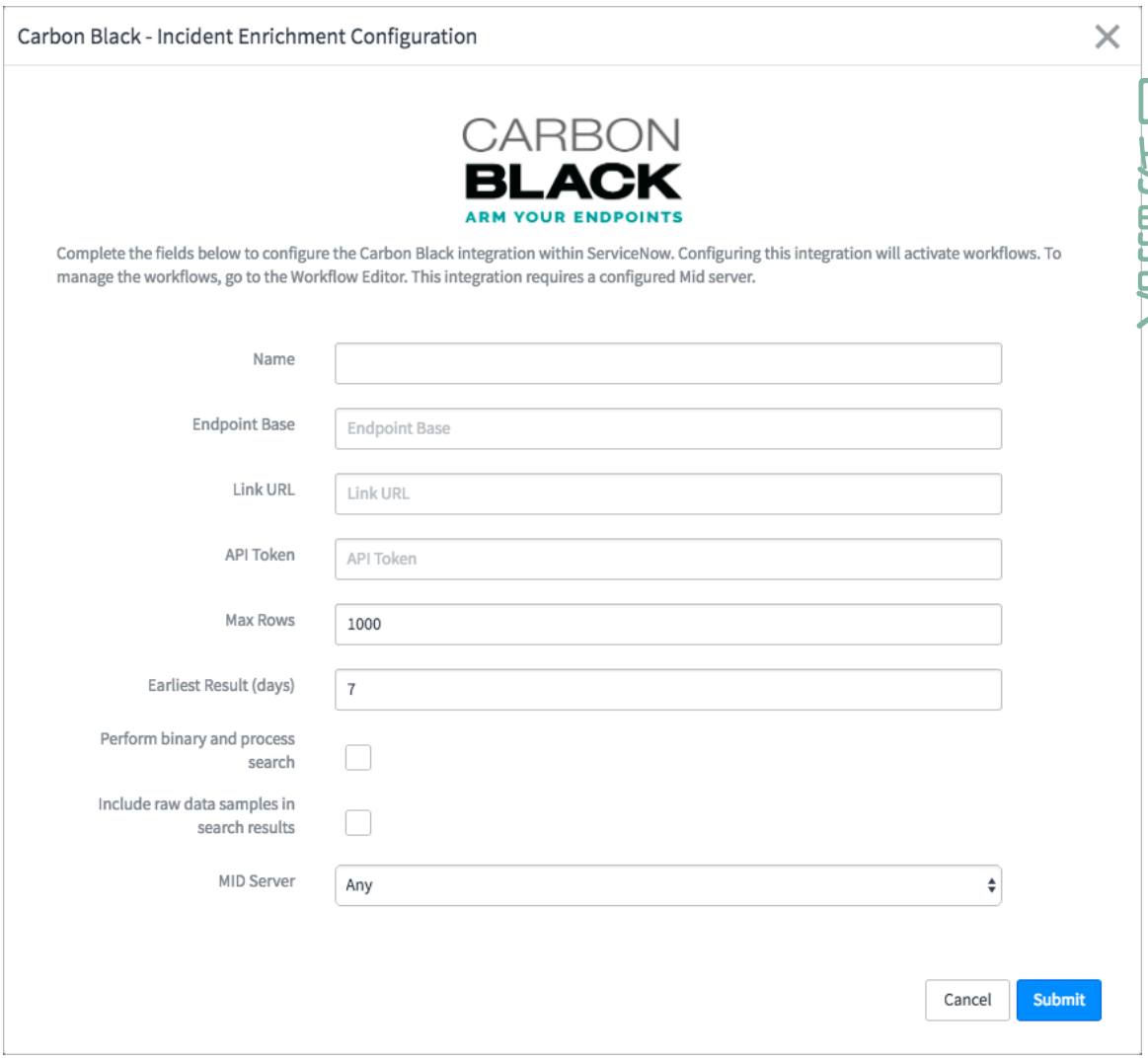
Carbon Black - インシデント拡張統合を開始する

Carbon Black インシデント拡張は、悪意のある可能性があるインジケーターをログでクエリすることで、セキュリティインシデントの調査を容易にします。Carbon Black - インシデント拡張統合を使用する前に、ServiceNow Store から統合をダウンロードし、適切なエンドポイントベース URL と MID サーバーを追加する必要があります。

始める前に
必要なロール：sn_si_admin

手順

1. から統合をダウンロードします ServiceNow Store.
2. ダウンロードが完了したら、Carbon Black Web サイトにアクセスし、プロファイルの下のエンドポイントベース URL と API トークンを取得します。
3. インスタンスで、 セキュリティオペレーション > 統合 > 統合設定.
4. Carbon Black - インシデント拡張カードで、[構成] をクリックします。



5. 必要に応じて、フィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
名前	この構成の名前。
エンドポイントベース	Carbon Black サイトから取得したエンドポイント URL。
リンク URL	Carbon Black インスタンスにリンクするリンク URL (利用可能な場合)。
API トークン	Carbon Black サイトから取得した API トークン。
最大行数	検索する行の最大行数。デフォルトは 1,000 行です。
最も早い結果 (日数)	表示する最も早い結果 (日数単位)。
バイナリとプロセスの検索を実行	これを選択すると、バイナリ検索を実行してファイルハッシュなどのバイナリファイルを検索し、実行済みの .exe プロセスの検索を処理します。
検索結果に生データサンプルを含める	サイティング検索結果に生データのサンプルを含めるには、これを選択します。返されるデータの量は、[セキュリティインシデントレスポンス] プロパティの [生データの行数] プロパティの設定によって異なります。
MID サーバー	[任意] を選択して、 任意のアクティブな MID サーバーを使用するか、特定の MID サーバー名を選択します。

注:
この統合を設定すると、ワークフローが有効になります。ワークフローを管理するには、[ワークフローエディター] に移動します。

6. **[Submit]** をクリックします。
   統合構成カードが表示されます。
7. 統合構成カードの元のリストに戻るには、[構成を表示] ドロップダウンから [いいえ] を選択します。

Carbon Black 統合

Carbon Black 統合を使用すると、API を使用してセキュリティインシデントに関連付けられているエンドポイントに対するクエリや操作を行うことで、セキュリティインシデントを調査および対処できます。

探索

- セキュリティインシデントレスポンス の統合
- Carbon Black - インシデント拡張統合

セットアップ

Carbon Black 統合を開始する

使用

開発

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

- セキュリティオペレーション ワークフロートリガー
- セキュリティインシデントの影響を受けるアイテムの表示
- Security Operations - 実行中のプロセスを取得フロー
- Security Operations Carbon Black 統合 - 実行中のプロセスを取得フロー
- セキュリティインシデントの影響を受けるアイテムの表示
- ブロック要求の実行
- Security Operations Integration - ブロック要求フロー
- ホスト隔離の実行
- [Security Operations Carbon Black 統合 - ホストを隔離] フロー
- Security Operations Carbon Black 統合 - ホスト隔離削除フロー
- ServiceNow セキュリティオペレーション 統合開発のガイドライン
- 統合を作成するためのヒント
- 開発者トレーニング
- 開発者ドキュメント
- アプリケーションとともにインストールされているコンポーネントの検索

トラブルシューティングとヘルプ

- 統合のトラブルシューティング
- Security Operations Community で質問や回答をする
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

自動翻訳

Carbon Black 統合を開始する

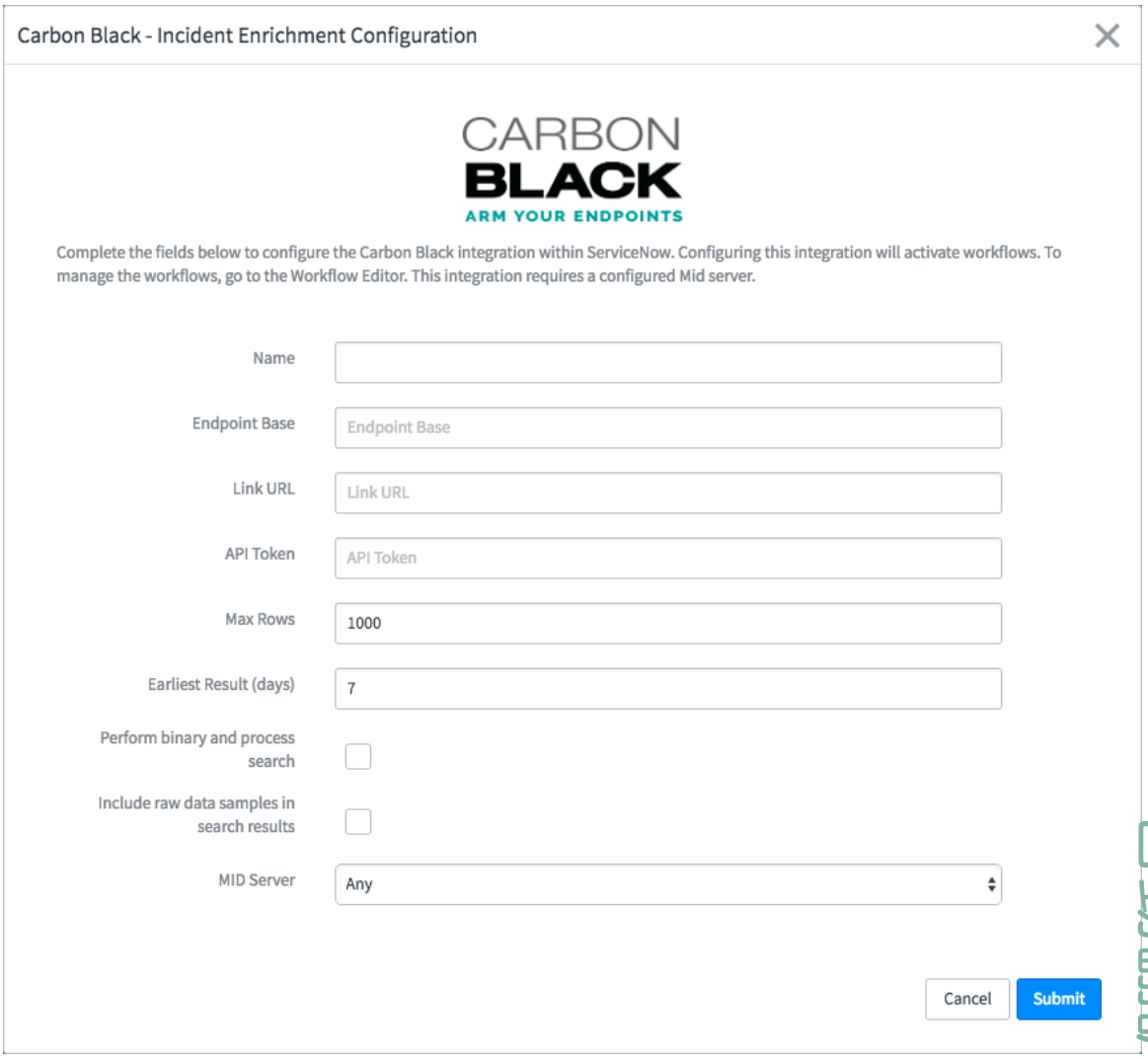
Carbon Blackは、 セキュリティオペレーションと簡単に統合できる高度なセキュリティシステムです。Carbon Black 統合を使用する前に、ServiceNow Store から統合をダウンロードし、適切なエンドポイントベースと API トークンを追加する必要があります。

始める前に
必要なロール：sn_si_admin

手順

1. から統合をダウンロードします ServiceNow Store.
2. インストールが完了したら、Carbon Black Web サイトにアクセスし、プロファイルの下のエンドポイントベース URL と API トークンを取得します。
3. インスタンスで、 セキュリティオペレーション > 統合 > 統合設定.
   利用可能なセキュリティ統合が一連のカードとして表示されます。
4. Carbon Black カードで、[新規] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

5. 必要に応じて、フィールドに入力します。

フィールド	説明
名前	この構成の名前。
エンドポイントベース	Carbon Black サイトから取得したエンドポイントベース。
API トークン	Carbon Black サイトから取得した API トークン。
MID サーバーを使用	まだオンになっていない場合は、このチェックボックスをオンにします。
MID サーバー	[任意] を選択して、 任意のアクティブな MID サーバーを使用するか、特定の MID サーバー名を選択します。
ホストの隔離を有効化	選択した構成アイテムをセキュリティインシデントの [構成アイテム] 関連リストから分離できるようにするには、このチェックボックスをオンにします。

注:
この統合を設定すると、ワークフローが有効になります。ワークフローを管理するには、[ワークフローエディター] に移動します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. **[Submit]** をクリックします。
   統合構成カードが表示されます。
7. 統合構成カードの元のリストに戻るには、[構成を表示] ドロップダウンから [いいえ] を選択します。

チェックポイントアンチボット - メールパーサー統合

チェックポイントアンチボット - メールパーサー統合は、セキュリティインシデントを作成し、拡張ワークフローと応答ワークフローを推進するために、チェックポイントアンチボットからのメール通知を消費するメールパーサーを使用してサポートされています。

チェックポイントアンチボット - メールパーサー統合の構成

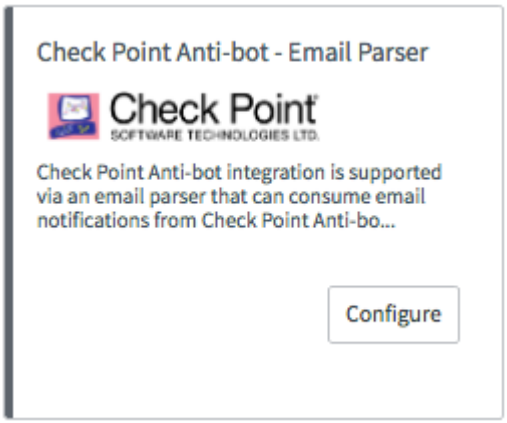
チェックポイントアンチボット - メールパーサー統合では、メール通知を使用して拡張および応答ワークフローを推進します。

始める前に
必要なロール：sn_si_admin

このタスクについて
統合に使用するチェックポイントアンチボットメールパーサーテンプレートが提供されています。統合が行われる前に、構成してアクティブ化する必要があります。パーサーを更新すると有効になります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > 統合 > 統合設定.
   利用可能なセキュリティ統合が一連のカードとして表示されます。



2. チェックポイントアンチボット - メールパーサーカードで、[構成] をクリックします。
3. [チェックポイントアンチボット - メールパーサー構成 **(Check Point Anti-bot - Email Parser Configuration)]** ダイアログボックスで、[メールパーサーの設定] リンクをクリックします。
4. [チェックポイントアンチボット **(Check Point Anti-bot)]** リンクをクリックして、提供されたテンプレートメールパーサーの設定を編集します。
   少なくとも、[メールの送信元] フィールドに入力します。メールパーサーを作成するには、「Security Operations でのメールパーサーの作成」を参照してください。
5. [アクティブ] ボックスをオンにします。
6. [メールパーサー] フォームで [更新] をクリックします。
   メールパーサーは有効です。[統合構成] に戻る必要はありません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Check Point Next Generation Threat Prevention の統合

このドキュメントでは、チェックポイント次世代の脅威防止 (NGTP) 機能を ServiceNow® セキュリティインシデントレスポンス (SIR) と統合して、アプリケーションが適切に連携するようにするために必要な手順について説明します。

インストールと設定が完了すると、セキュリティインシデントアナリストは ServiceNow セキュリティインシデントレスポンス (SIR) 製品のブロック要求リスト機能を使用して、悪意のある IP アドレス、URL、およびドメインをブロックします。このブロック要求リストは、チェックポイントゲートウェイでカスタムインテリジェンスフィードとして設定されます。カスタムインテリジェンスフィード機能には、カスタムサイバーインテリジェンスフィードを次世代の脅威防止エンジンに追加する機能があります。これにより、サードパーティサーバー (この場合は ServiceNow セキュリティインシデントレスポンス アプリケーション) から、アンチウイルスおよびアンチボットブレードによって強制されたチェックポイント次世代ゲートウェイに直接フィードを取得できます。セキュリティインシデントレスポンスアナリストは、ServiceNow SIR セキュリティインシデントで悪意があると判断された観測事象からチェックポイントブロックリストのエントリを作成します。

ほとんどの実装では、ブロック要求リストは外部 Web サーバーでホストされている csv ファイルです。この統合では、この Web サーバーは Now Platform インスタンスです。ブロックする IP アドレス、URL、およびドメインのリストをチェックポイント次世代の脅威防止エンジンがフェッチできるようにします。

チェックポイントゲートウェイで観測事象のブロックを強制するには、アンチボットブレードおよびアンチウイルスブレードを有効にして脅威防止ポリシーを設定してください。ブロックリストのエントリが変更されると、脅威防止エンジンは設定された間隔でリストを動的にインポートし、設定の変更やファイアウォールへのコミットを行うことなくポリシーを適用します。この統合では、設定された取得間隔で認定されたチェックポイント次世代ゲートウェイによって取得されるブロックリストエントリを含むテーブルを Now Platform に作成しました。

この統合には次の機能が含まれています。

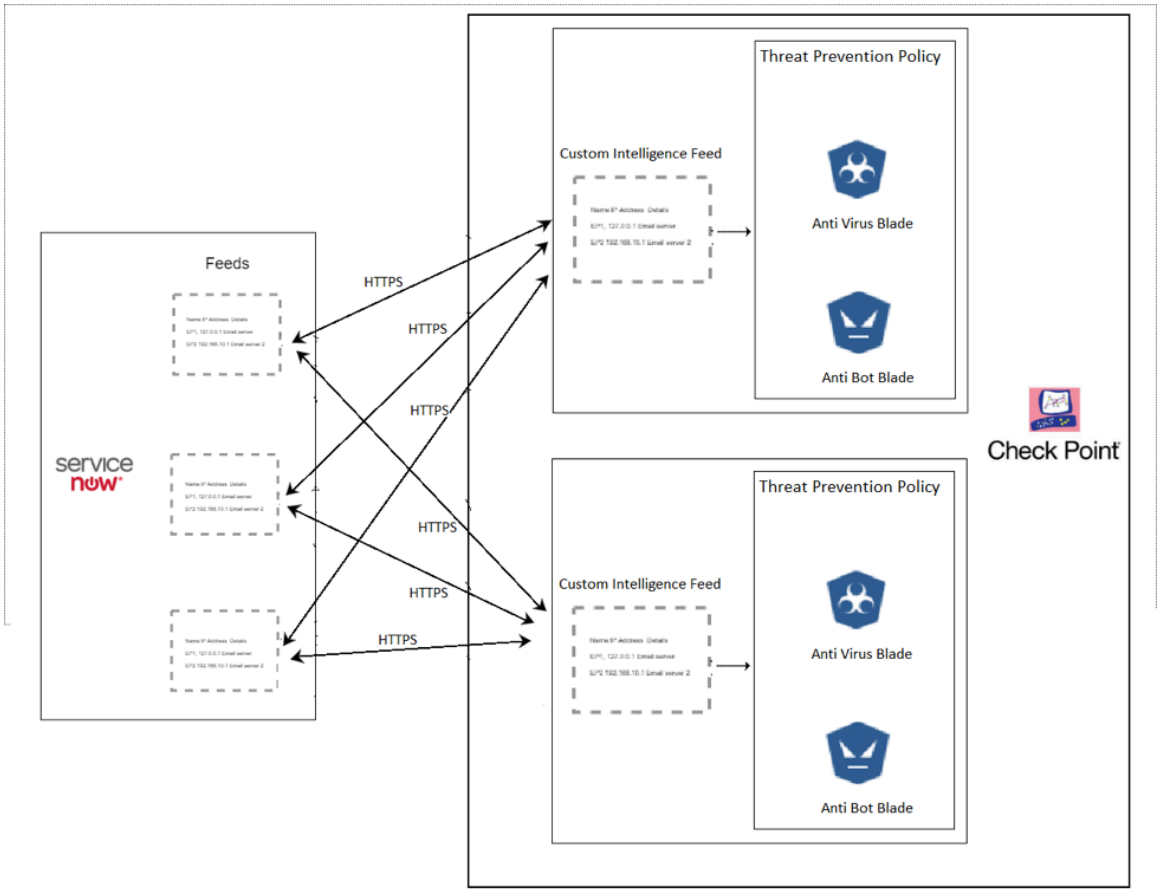
- 複数のチェックポイントゲートウェイに適用される複数のブロックリストを作成できる柔軟性
- ブロックされているサイトのタイプ (フィッシング、マルウェア、許可リスト) に関する詳細なレポート
- 観測可能タイプ (URL、ドメイン、IP アドレス) によるブロックリストエントリによる Now Platform セキュリティインシデントのタグ付け
- 古いエントリを自動的に期限切れにするか削除することでブロックリストのサイズを維持するためのブロックリストの有効期間の設定
- 異なるブロックリスト間のブロックリストエントリの検索
- 脅威インテリジェンスの結果とエントリがブロックされた理由の詳細を含む、観測事象レコードとセキュリティインシデントへのブロックリストエントリのリンク

統合アーキテクチャ図

以下は、関連するコンポーネントおよび Now Platform と Check Point Systems 間の統合ポイントを示すアーキテクチャの全体図です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
Check Point Systems のロゴ、アンチウイルスブレード画像、およびアンチボットブレード画像は、Check Point Systems © のものです。これらは Check Point Systems に帰属します。

プラグイン

統合する際は、セキュリティインシデントレスポンス (com.snc.security_incident) プラグインを有効にする必要があります。

セキュリティインシデントレスポンス プラグインをインストールするには：

1. HI 認証情報を使用してインスタンスにログインします。
2. アドミン (admin) ロールがあることを確認します。
3. インスタンスで [システム定義] > [プラグイン] に移動します。
4. セキュリティインシデントレスポンスを選択してクリックします。

これらのプラグインをインストールすると、ServiceNow Store から新しい Check Point Integration プラグインをアップロードできるようになります。次の構成手順に従ってください。

サポートされている **Check Point OS** バージョン

この統合には、Check Point のカスタムインテリジェンスフィードとアンチボットブレードおよびアンチウイルスブレードが必要です。これらは R80.20 以降でサポートされています。Check Point R80.10 Jumbo HF Take 121 以降と呼ばれるカスタムインテリジェンス機能のホットフィックスをインストールします。製品互換性マトリクスの詳細については、チェックポイントカスタムインテ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リジェンスフィードのドキュメントの「Installation (インストール)」セクションを参照してください。

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

ホットフィックスをインストールした後、チェックポイントゲートウェイで以下のコマンドにアクセスできることを確認してください。ゲートウェイに SSH で接続し、エキスパートモードでログインします。

```
gw-93440b> expert
Enter expert password:


Warning! All configurations should be done through clish
You are in expert mode now.

[Expert@gw-93440b:0]# ioc_feeds --help
External indicators configuration

positional arguments:
  show, add, delete, modify
                        Select an action for the external indicators configurations

optional arguments:
  -h, --help            show this help message and exit
  --feed_name           Set feed name
  --transport           Set feed transport protocol: http, https, local_file, local_directory
  --resource            Set feed resource URL
  --state               Set feed enforcement Active / Inactive
  --feed_action         Set feed action: Prevent, Detect, Ask
  --proxy               Set feed proxy
  --proxy_user_name     Set feed proxy user name
  --user_name           Set user name for remote feed
  --test                Set test as true if feed is for testing purposes only
  --format [ [ ...]]    Enter format in order to fetch custom csv file
  --delimiter           Enter delimiter in order to fetch custom csv file
  --comment [ [ ...]]   Enter comment char in order to fetch custom csv file
Missing a few arguments.
[Expert@gw-93440b:0]#
```

サポートされている **ServiceNow** バージョン

San Diego リリースバージョン以降がサポートされています。

参照

前提条件の設定に役立つ Check Point の参考文献の一部を以下に示します。

1. カスタムインテリジェンスフィード機能 - https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193
2. アンチボットブレードおよびアンチウイルスブレードを設定するには、『Check Point User Guide (Check Point ユーザーガイド)』(http://downloads.checkpoint.com/dc/download.htm?ID=46534) を参照してください。
3. Check Point で HTTPS インスペクションを設定するには、https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202 のリンク先を参照してください。

権限とロール

次の ServiceNow ロールが必要です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 統合アプリケーションプラグインをインストールするためのアドミンロール (admin)
- ServiceNow でブロックリストを作成し、ブロックリストエントリを追加および非アクティブ化するための要求を承認するSecurity Incident Management者ロール (sn_si.admin)
- ブロックリストエントリレコードを作成および管理するセキュリティアナリスト (ここでは SOC アナリストとも呼ばれます) ロール (sn_si.analyst)

セキュリティアナリストロールのアサインの詳細については、ServiceNow ドキュメント Web サイト で、[Security Operations] > [セキュリティインシデントレスポンス] > [セキュリティアナリストのアサイン (Assigning security analysts)] に移動してください。

Check Point NGTP のセットアップ

Check Point NGTP 統合を使用するには、API アカウントを作成し、ポリシーを設定し、統合をアクティブにする必要があります。

Check Point NGTP 統合用の API アカウントの作成

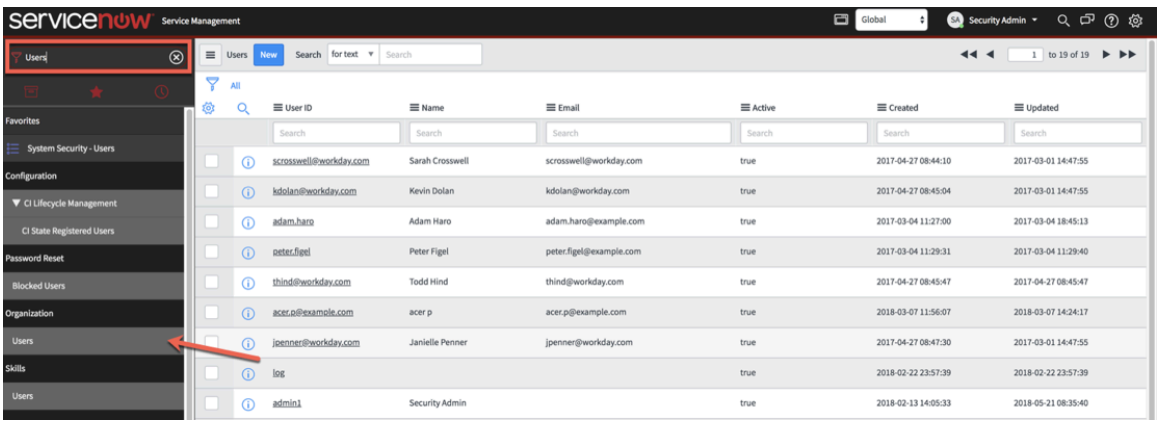
この統合を行うには、Now Platform インスタンスに API アカウントロールが必要です。このアカウントに関連付けられたユーザー名とパスワードは Now Platform で作成されチェックポイントに入力されるため、チェックポイントはブロックリストエントリを取得するときに Now Platform で認証します。

始める前に
必要なロール：admin

このタスクについて
Now Platform アドミニストレーターが API アカウントロール (sn_sec_checkpoint.api_account_access) を作成します。このアカウントは、ゲートウェイが Now Platform からブロックリストを取得できるよう、チェックポイントでの認証に必要な認証情報を入力するためにのみ使用されます。このアカウントは Now Platform インスタンス内の独立した一意の API ユーザーアカウントであり、チェックポイントアドミニストレーターにアサインされます。

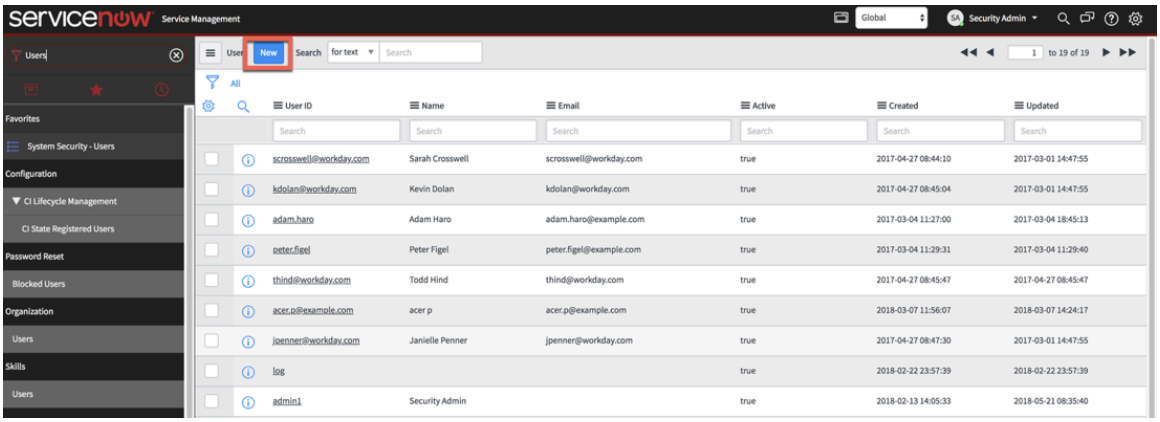
手順

1. 次のように移動する。 **All** (すべて) > 組織 > ユーザー.
2. [ユーザー] モジュールをクリックします。

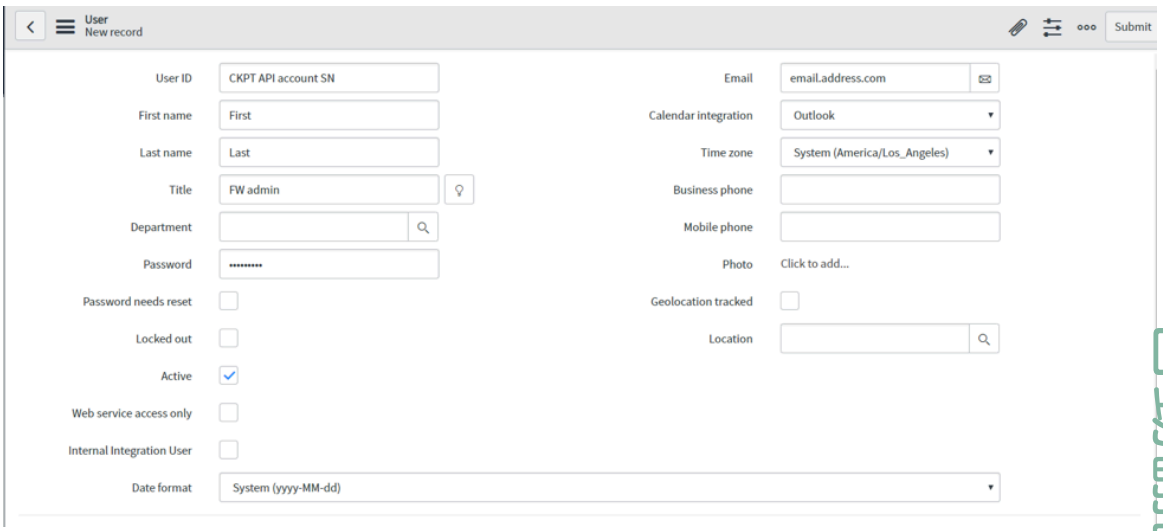


3. [ユーザー] リストが表示されます。[新規] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



新しいフォームが表示されます。



4. 必要に応じてフォームに入力します。

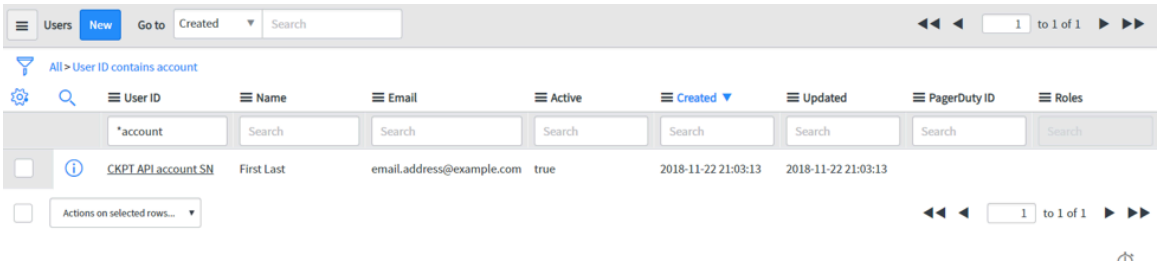
> **注:**
> 以下のテーブルと図に示す [ユーザー ID]、[タイトル]、[メールアドレス] の値は一例です。

フィールド	説明
ユーザー ID	Now Platform インスタンスのロールの一意のユーザー ID。このユーザー ID は、ブロックリスト構成チェックポイントゲートウェイの [クライアント認証 **(Client Authentication)]** セクションの [ユーザー名 **(Username)]** フィールドに入力されます。例：CKPT API account SN
名	アサインするユーザー
姓	アサインするユーザー
役職	ジョブタイトル (例：FW admin)
パスワード	このロール用に作成された一意のパスワードです。このパスワードは、チェックポイントゲートウェイのブロックリスト構成の [クライアント認証 **(Client Authentication)]** セクションの [パスワード] フィールドに入力されます。
メール	一意のメールアドレス

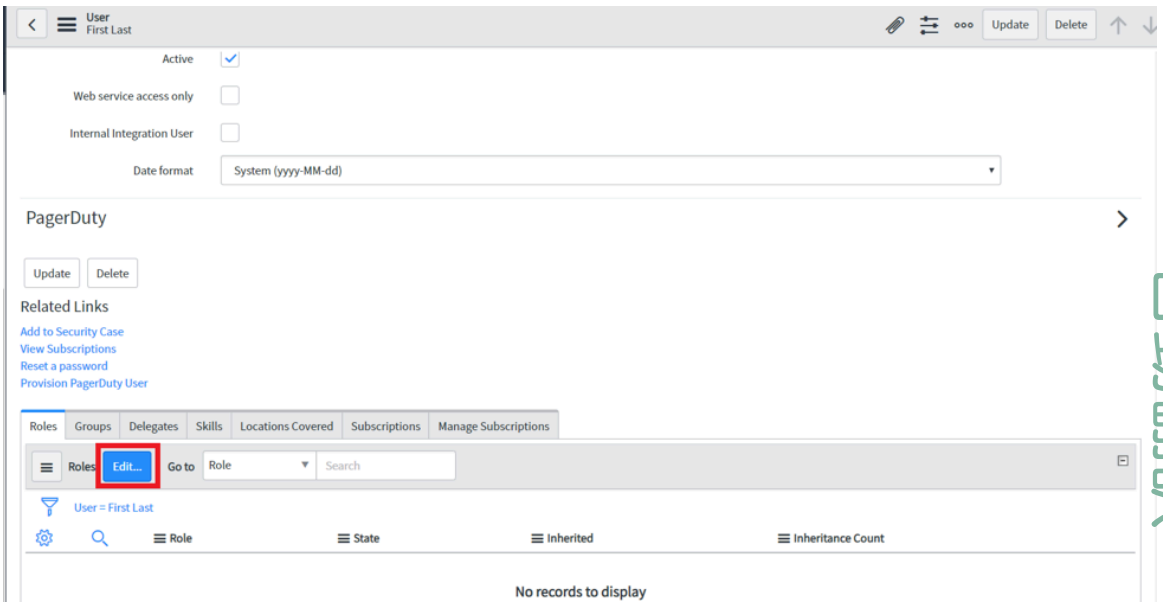
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. [送信] をクリックします。
   送信すると、ロールをアサインすることができるようになります。
6. [ユーザー ID] 列の [ユーザー] リストで、入力したユーザー ID の名前 (例：CKPTAPI account SN) をクリックします。



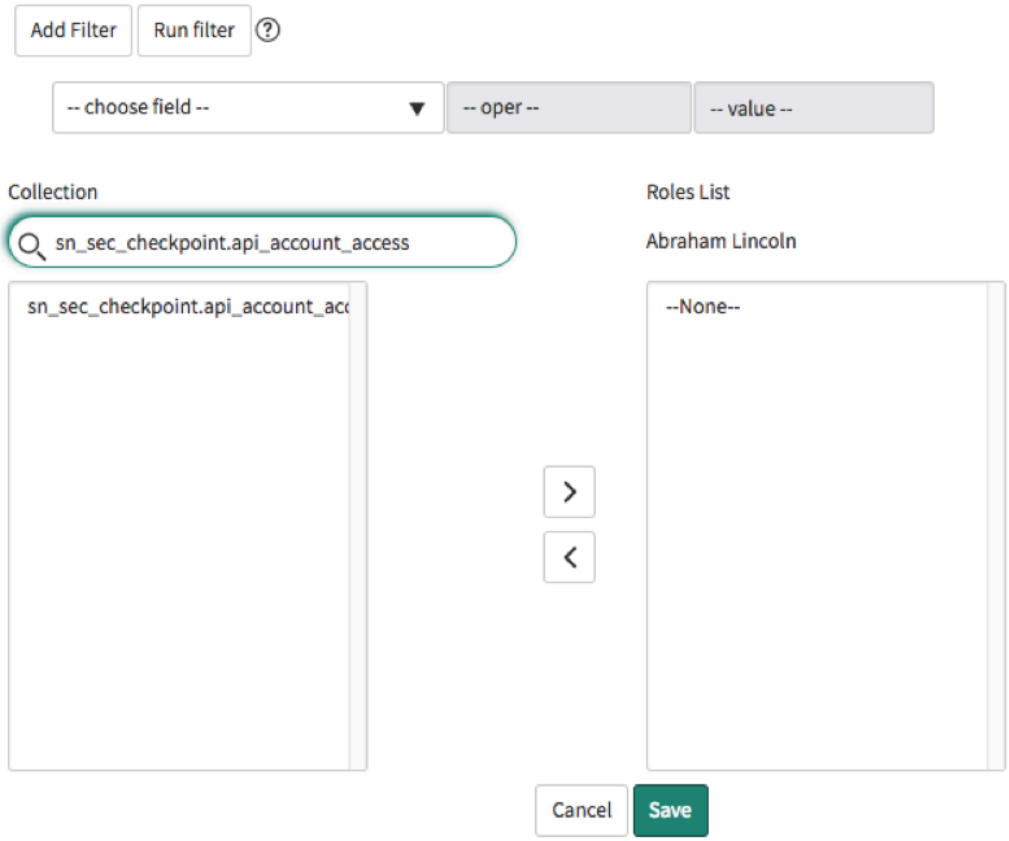
7. [ロール] セクションのオープンレコードで、[編集] をクリックします。



8. 表示される [エレメントの編集] フォームで、[コレクション] フィールドに「sn_sec_checkpoint.api_account_access」と入力します。

自動翻訳

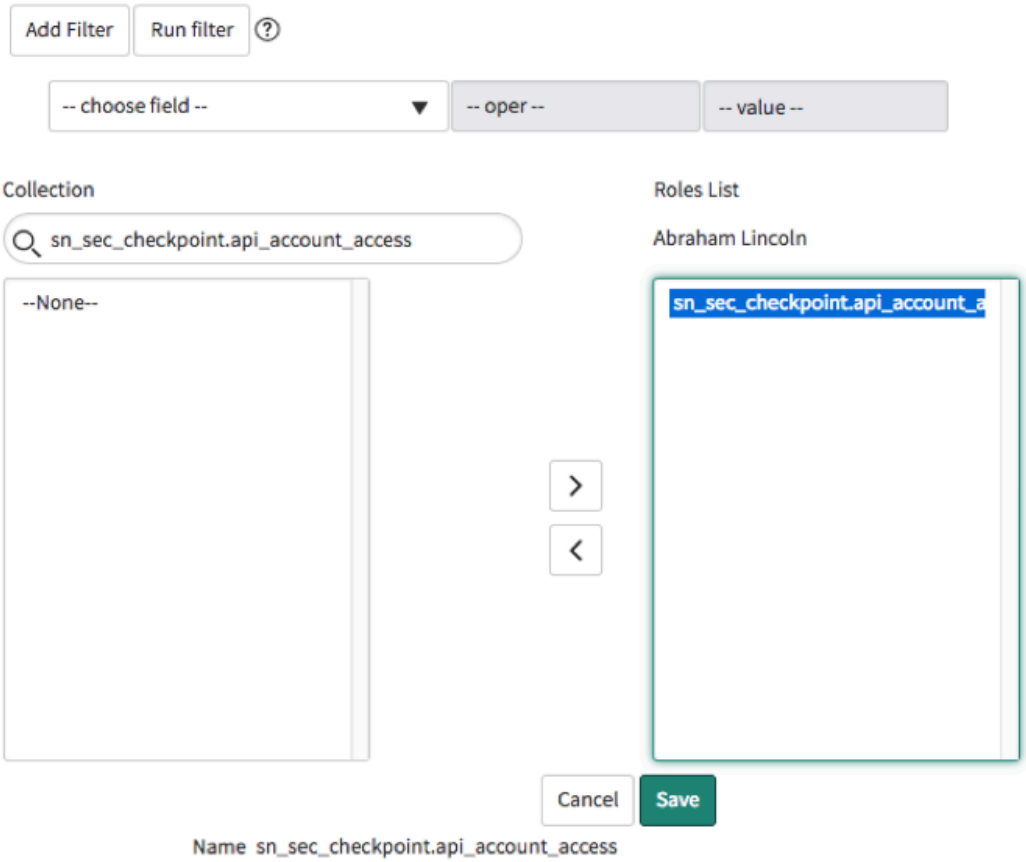
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



9. [コレクション] 列で、[sn_sec_checkpoint.api_account_access] を選択して [ロールリスト **(Roles List)]** に移動します。
10. [保存] をクリックします。
11. [ユーザー] に移動し、リストの [ユーザー] 列で、ロール (CKPT API account SN) に対して作成した ID 名をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



12. ユーザーレコードが表示されます。このレコードで、ユーザーアカウントがアサインされていることを確認します。

Check Point NGTP 統合の設定

Check Point Next Generation Threat Prevention 統合を設定するには、次の手順を実行します。これにより、統合が機能するための前提条件が満たされます。

始める前に
必要なロール：admin

手順

1. 脅威防止ポリシーが設定されており、アンチボットブレードとアンチウイルスブレードが有効になっていることを確認します。
   アンチボットブレードとアンチウイルスブレードの設定の詳細については、『Check Point User Guide (Check Point ユーザーガイド)』の「Reference (参照)」セクションを参照してください。

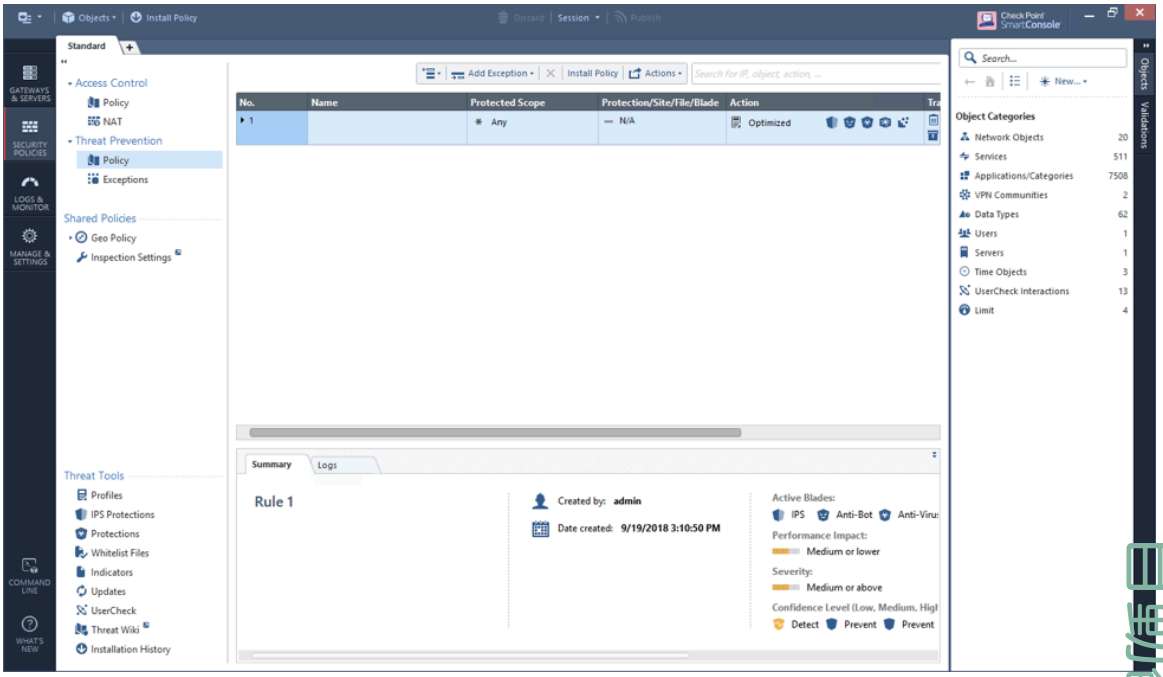
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

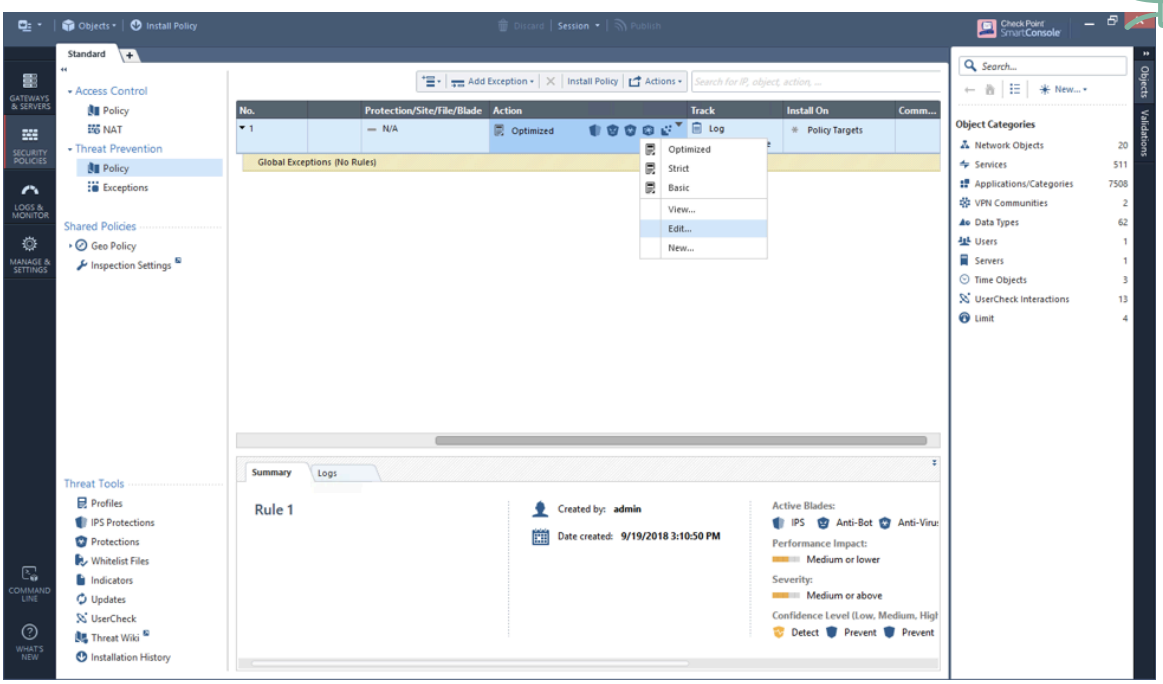
注:
このトピックの画像は特権が付与された専有コンテンツであり、Check Point Software Technology, Ltd. の許可を得て使用しています。

a. [スマートコンソール **(Smart Console)]** にログインします。

b. 次のように移動する。 セキュリティポリシー > 脅威の防止 > ポリシー.



c. [脅威防止ポリシー (Threat Prevention Policy)] を編集モードで開きます。

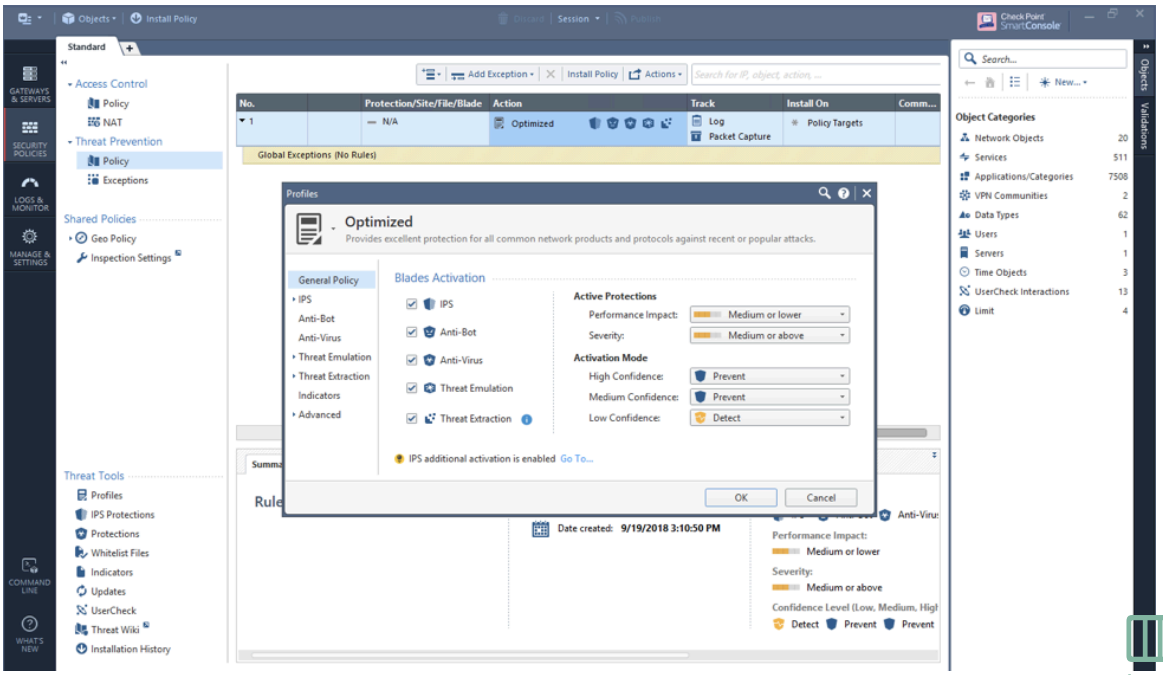


d. アクティブな保護 (Active Protections) → [重大度] は [中程度以上 (Medium or above)] である必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

e. アクティベーションモード (Activation Mode) → [高信頼性 (High Confidence)] は [防止 (Prevent)] である必要があります。

f. [ブレードのアクティブ化 (Blades Activation)] → [アンチウイルス] および [アンチボット] を選択する必要があります。



g. 変更があれば公開し、ポリシーをインストールします。

2. まだ構成していない場合は、アンチボットブレードおよびアンチウイルスブレードを有効にした後にカスタムインテリジェンスフィードを追加する必要があります。
チェックポイントカスタムインテリジェンスフィード機能に関するドキュメント (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193) の「Installation (インストール)」セクションを参照してください。

3. まだ設定していない場合は、HTTP プロキシを介してすべてのインターネットトラフィックをルーティングするようにチェックポイントゲートウェイを設定します (HTTPS インスペクションを設定している場合)。

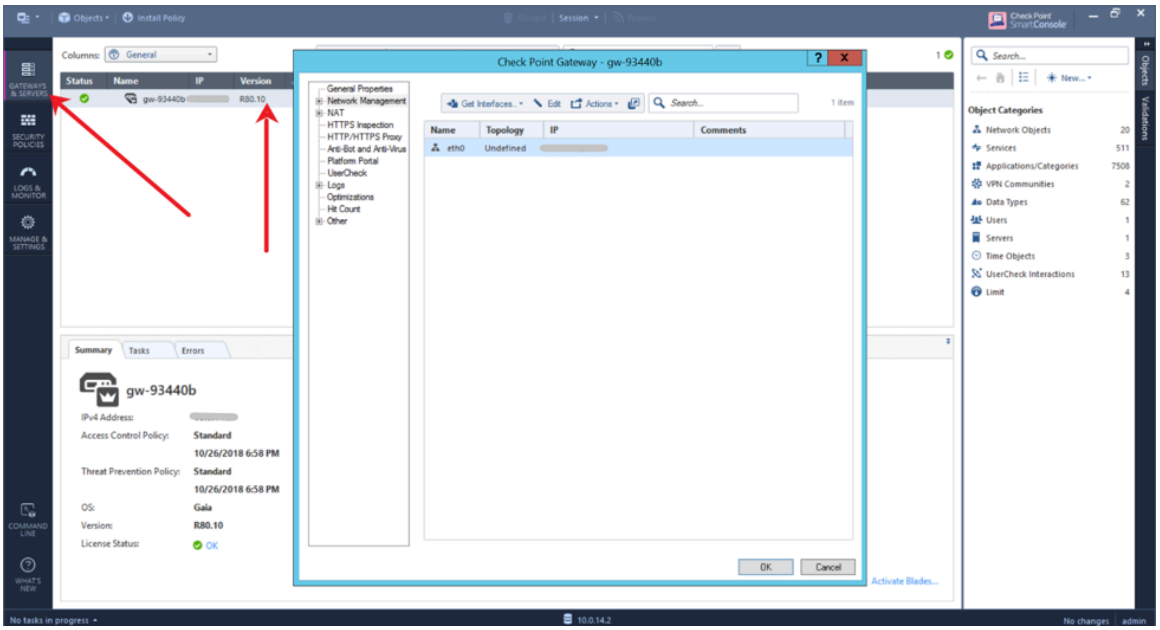
> **注:**
> チェックポイント NGTP の URL ブロックには、確認する必要がある特定の設定があります。HTTPS インターネットトラフィックは SSL (Secure Sockets Layer) プロトコルを使用し、データのプライバシーを保護するように暗号化されます。ただし、HTTPS は本来ブロックされるべき悪意のあるトラフィックを非表示にする可能性があります。チェックポイントゲートウェイで HTTPS トラフィックを可視化するには、HTTP プロキシを介してトラフィックをルーティングするか、HTTPS インスペクションをセットアップします (推奨)。このセクションでは、チェックポイントゲートウェイで HTTP プロキシをセットアップする手順について詳しく説明します。

a. [スマートコンソール **(Smart Console)]** にログインします。

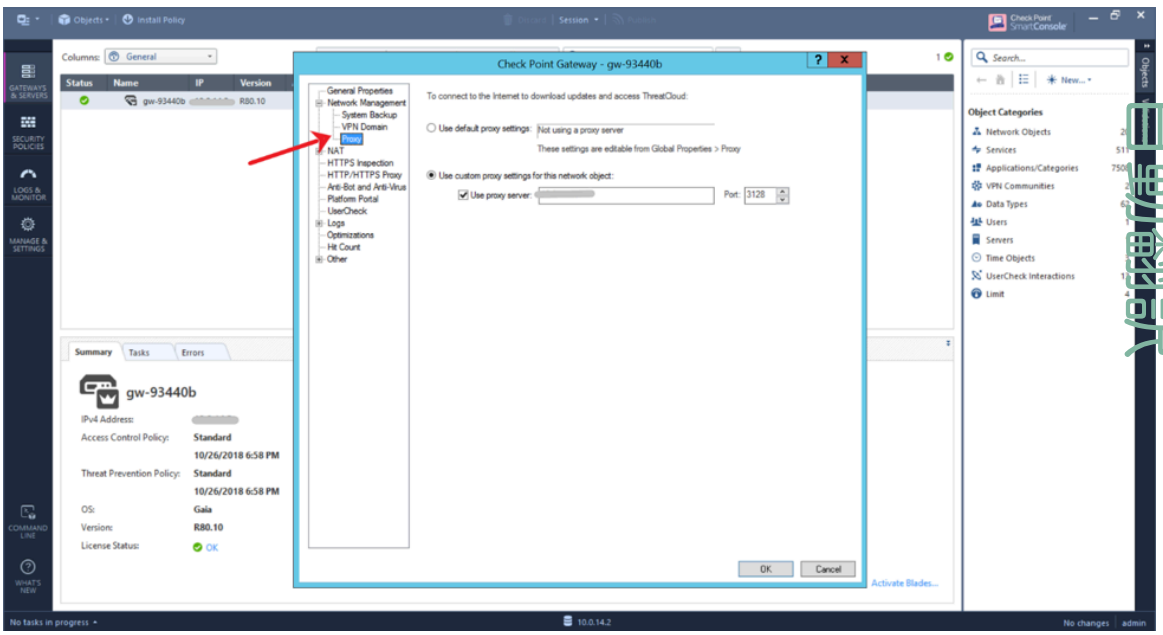
b. [サーバーとゲートウェイ **(Servers and Gateways)]** に移動し、該当するサーバーをダブルクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



c. 次のように移動する。 ネットワーク管理 > プロキシ.



d. HTTP トラフィックのルーティングに使用するプロキシの詳細を入力します。

e. クライアントエンドポイントからの HTTP 要求が HTTP プロキシ経由であることを確認します。

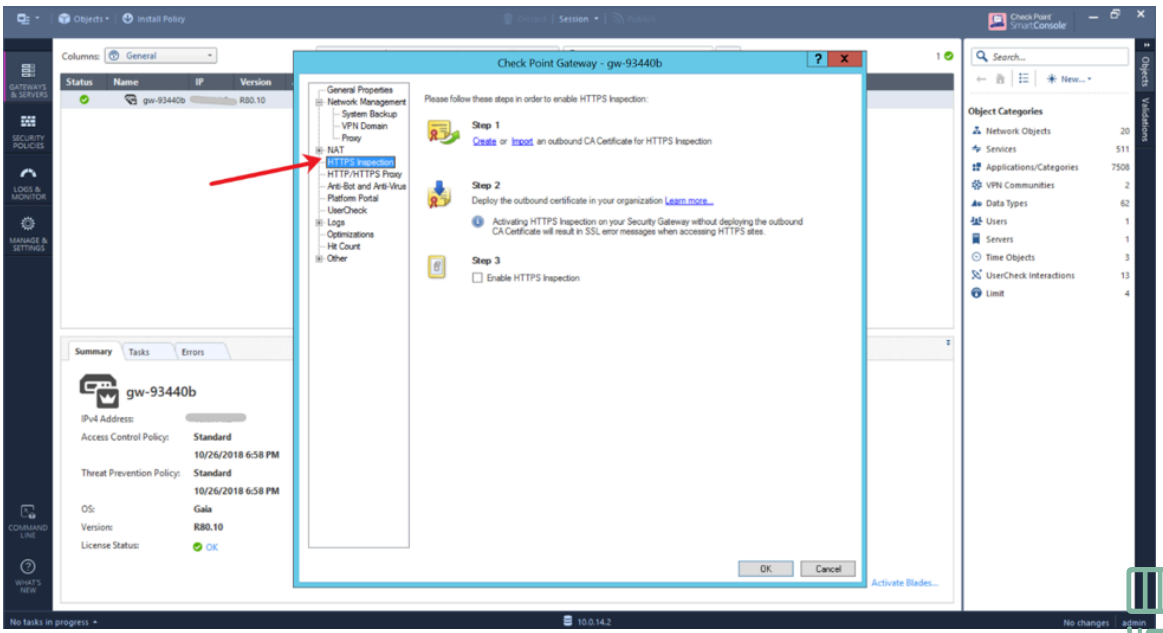
4. まだ設定されていない場合は、HTTPS インスペクションを有効にします (HTTP プロキシが設定されている場合)。
ほとんどのトラフィックが SSL を介している場合は、HTTPS インスペクションブレードを使用することをお勧めします。これにより、トラフィックは GW に対して透過的になります。次のように、チェックポイントゲートウェイで HTTPS インスペクションを有効にします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. [スマートコンソール **(Smart Console)**] にログインします。

b. [サーバーとゲートウェイ **(Servers and Gateways)**] に移動し、該当するサーバーをダブルクリックします。

c. **[HTTPS** インスペクション **(HTTPS Inspection)]** に移動します。



d. 『Check Point User Guide (Check Point ユーザーガイド)』の手順に従って HTTPS インスペクションを設定 します。

Check Point NGTP 統合の有効化

アプリケーションをインストールしていない場合は、指示に従ってインストールしてください。

始める前に
必要なロール：admin

手順

1. アプリケーションをインストールするインスタンスにログインします。
2. 次のように移動する。 システムアプリケーション > アプリケーション.
3. [ダウンロード] タブをクリックします。
   インストール可能なアプリケーションのリストが表示されます。
4. Check Point Next Generation Threat Prevention アプリケーションを見つけて選択し、[インストール] をクリックします。
   アプリケーションがインスタンスに自動的にインストールされます。

ブロックリストの操作

ServiceNow Check Point Next Generation Threat Prevention 統合は、IP、URL、およびドメインの観測事象を受け入れるブロックリストをサポートしています。

ServiceNow により構成されたブロックリストは、外部 Web サーバーでホストされている csv ファイルです。この統合では Now Platform インスタンスです。カスタムインテリジェンスフィー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドは、事前設定された間隔で Now Platform から IP アドレス、URL、およびドメインをプルするチェックポイントゲートウェイで設定されます。

この統合は、次の 3 つのタイプのブロックリストをサポートしています。

- IP アドレス (これには、ブロックリストの個々の IP アドレス (IPv4 のみ) と、許可リストのアドレスの CIDR ブロック (範囲) が含まれます)
- URL
- ドメイン

Check Point NGTP 統合によってサポートされる観測事象

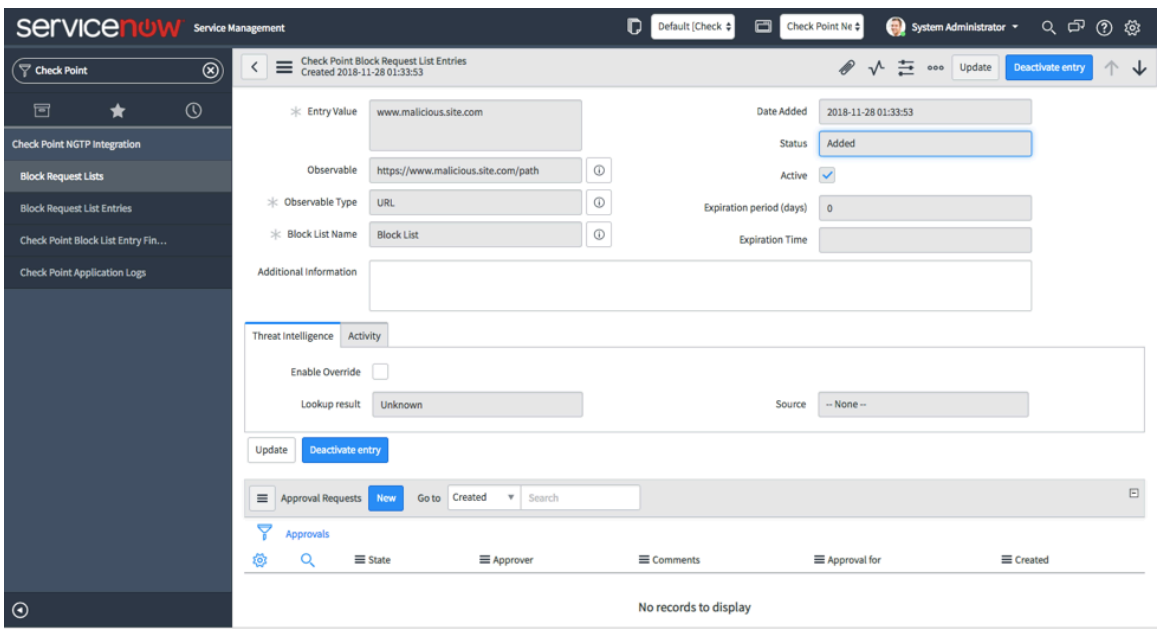
このセクションでは、この統合でサポートされている観測事象の説明と、各タイプの形式の例を示します。

観測事象タイプ	例	説明
ドメイン	• example.com • mail.example.com	ワイルドカードはサポートされていません。
IP アドレス	95.153.103.54 (IPv4)	単一の個別のインターフェイスアドレスを表します。この統合は IPv4 および CIDR 形式のみをサポートしています (CIDR 形式は許可リストを使用する目的でのみサポートされています)。 許可リストを使用する目的で、統合は CIDR (クラスレスドメイン間ルーティング) 範囲 (95.153.100.0/22 など) を含む IP アドレスの観測事象をサポートしています。 **注:** CIDR 範囲の一部として既に許可されているブロックリストに単一の IP アドレスを添付しようとすると、エラーメッセージが表示されます。たとえば、単一のアドレス 95.153.103.54 は、95.153.100.0/22 (95.153.100.0 ～ 95.153.103.255) で表される CIDR 範囲の一部です。
URL	• https://www.example.com • http://www.example.com	説明：HTTPS URL は、URL からパスをトリミングしてドメイン名のみを保持するよう

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

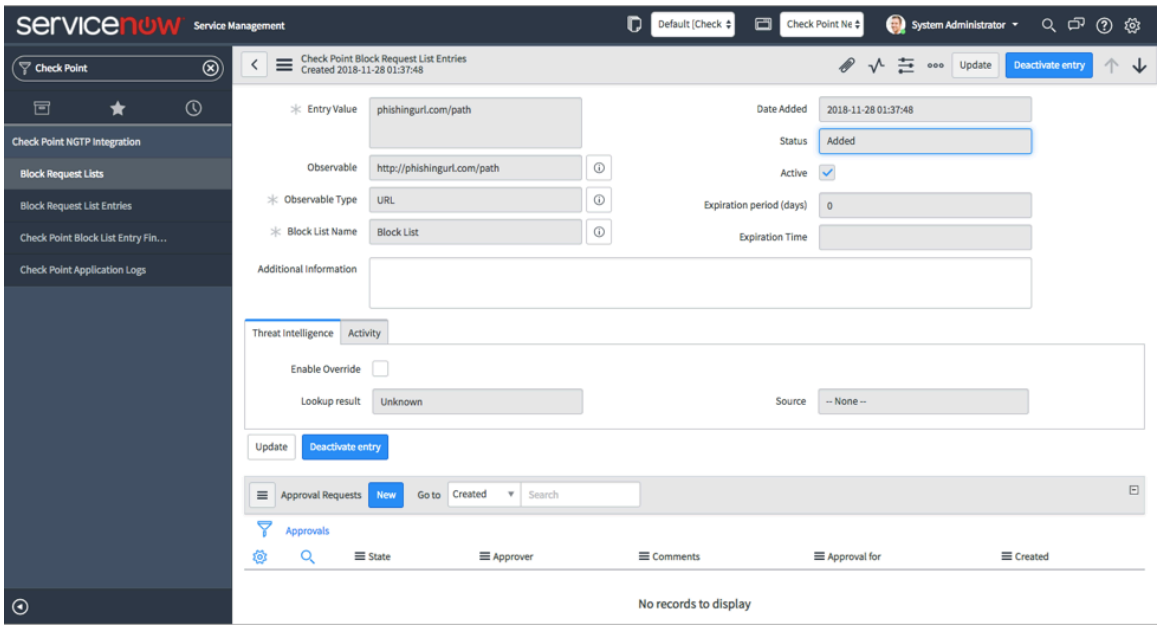
観測事象タイプ	例	説明
		に、アプリケーションによってフォーマットされます。 チェックポイント NGTP は、HTTP CONNECT 要求に依存して Web トラフィックを評価し、ブロックを強制します。HTTPS CONNECT 要求の場合、URL 全体は要求に表示されず、ドメイン名のみが表示されます。ユーザーが特定のパス (例：https://www.example.com/path) を持つ HTTPS URL をブロックすると、アプリケーションによってパスが自動的にトリミングされます (www.example.com)。アプリケーションは、元の観測事象とフォーマットされた URL の関係を維持します。以下は、フォーマットされた URL と元の観測事象を示すブロックリストエントリのスクリーンショットです。



特定のパス (例：http://www.example.com/path) を持つ HTTP URL の場合、URL 全体が CONNECT 要求で表示されるため、チェックポイントは指定された URL をブロックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳



Check Point NGTP 統合のブロックリストの作成

Now Platform インスタンスでブロックリストを作成します。承認されてアクティブ化されると、Now Platform セキュリティインシデントレスポンス (SIR) インシデントで悪意のあると判断された観測事象からこれらのブロックリストのエントリを作成し、それらをブロックするための承認を要求できます。

始める前に

必要なロール：セキュリティインシデントアドミニストレーター (sn_si_admin)

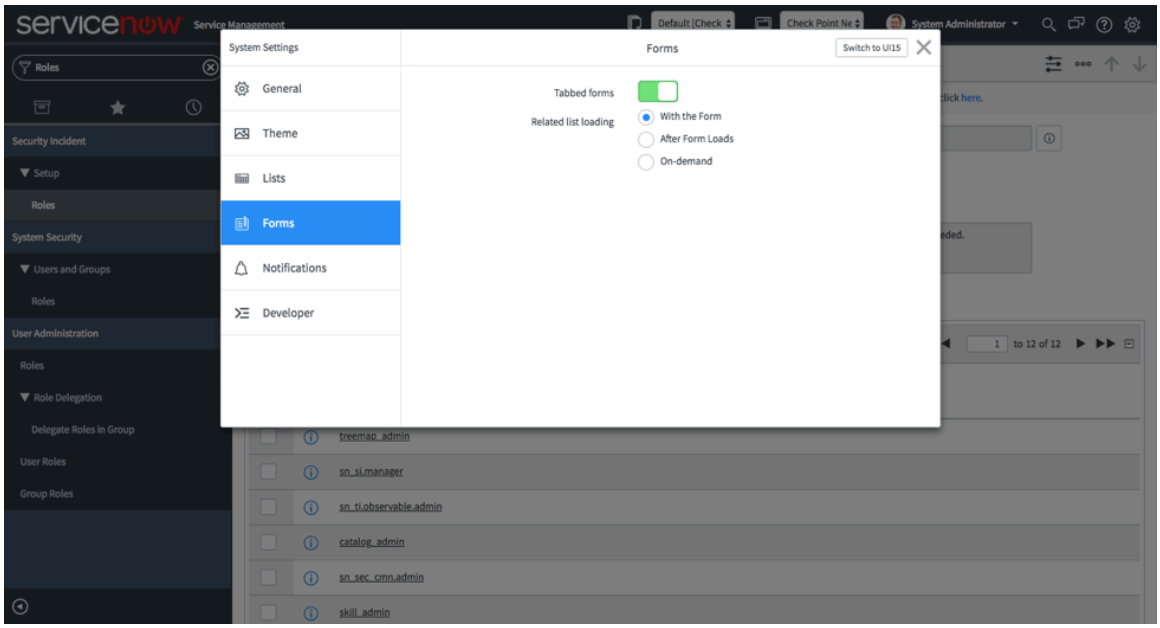
このタスクについて

チェックポイントがリストに含まれているオブジェクト (IP アドレス、URL、ドメイン) をインポートできるように、Now Platform インスタンスでブロックリストを作成します。カスタムインテリジェンスフィードは、事前設定された間隔で Now Platform から IP アドレス、URL、およびドメインをプルするチェックポイントゲートウェイで設定されます。観測事象を確実にブロックするには、アンチボットブレードおよびアンチウイルスブレードを有効にして脅威防止ポリシーを設定してください。

注:
このトピックの図は、[システムの設定] で [タブ付きフォーム] をクリアした状態で表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



手順

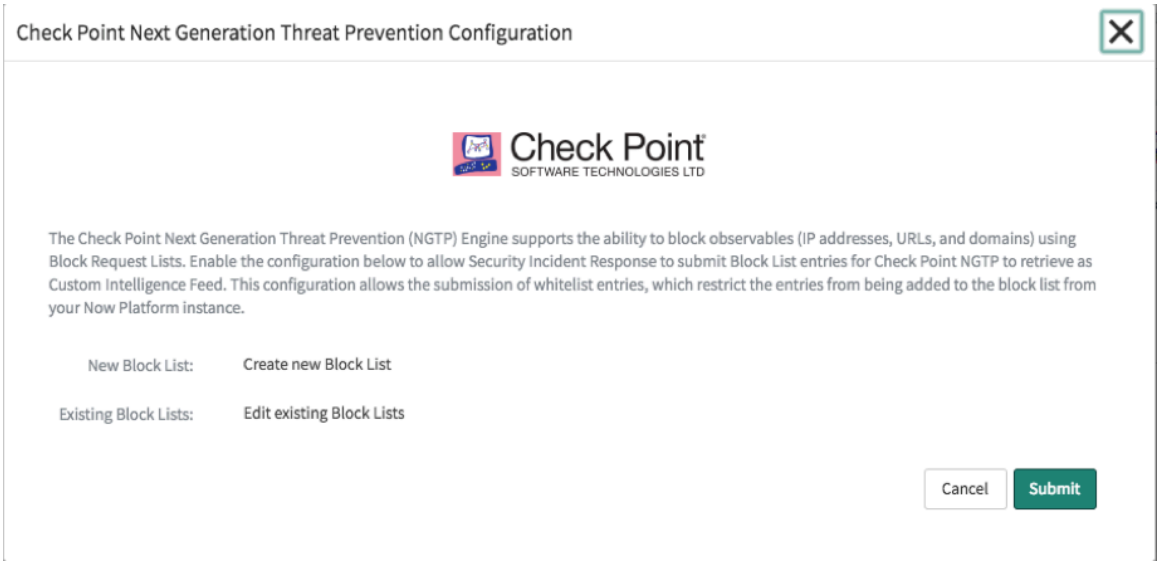
1. アプリケーションのインストールが完了したら、次に移動します: 統合 > 統合設定.
2. [チェックポイント次世代の脅威防止] カードを探し、[構成] をクリックします。

自動翻訳

注:
特権が付与された専有コンテンツは、Check Point Software Technology, Ltd. の許可を得て使用しています。

3. [新しいブロックリストを作成 **(Create new Block List)]** をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. フォームのフィールドに入力します。

フィールド	説明
名前	チェックポイントブロック要求リストの名前。 セキュリティアナリストが名前でブロックリストの意図を簡単に認識できるように、このフィールドに観測事象タイプ (URL、IP、ドメイン) を含めます。また、これらのブロックリストオブジェクトがマッピングされているファイアウォールポリシーを明確に示す名前である必要があります。ブロックリスト名の例としては、「Outbound Malware IP」、「Outbound Phishing URL」などが挙げられます。
アクティブ	デフォルトではこのチェックボックスはオフになっており、ブロックリストが非アクティブであることを示します。 非アクティブの場合、ブロックリストは追加のエントリを受け取ることができません。 チェックボックスがオンになっている場合 (変更要求がクローズされている場合、または変更要求が生成されていない場合)、ブロックリストはアクティブになり、ブロックリストエントリで使用できます。
タグを表示	このチェックボックスはデフォルトでオンになっており、観測事象がブロックリストでブロックされた場合に、観測事象と関連するセキュリティインシデントレコードに自動的にタグが付きます。オンにした場合、フォームで [観測事象のタグ] フィールドを使用できます。 **注:** デフォルトでは、[名前] フィールドに入力した値にプリフィックス「Check Point」を付けて作成されます (例：Check Point-Malware OutBound IP)。タグ名と色は変更できます。ブロックリストが保存されると、[観測事象のタグ] フィールドにタグ名が表示されます。 チェックボックスをオフにすると、タグは作成されず、[観測事象のタグ] フィールドはフォームで使用できません。
観測事象	リストからこのブロックリストが受け入れる観測事象タイプ (IP アドレス (許可リストの CIDR を含む)、URL、またはドメイン) を選択します。

自動翻訳

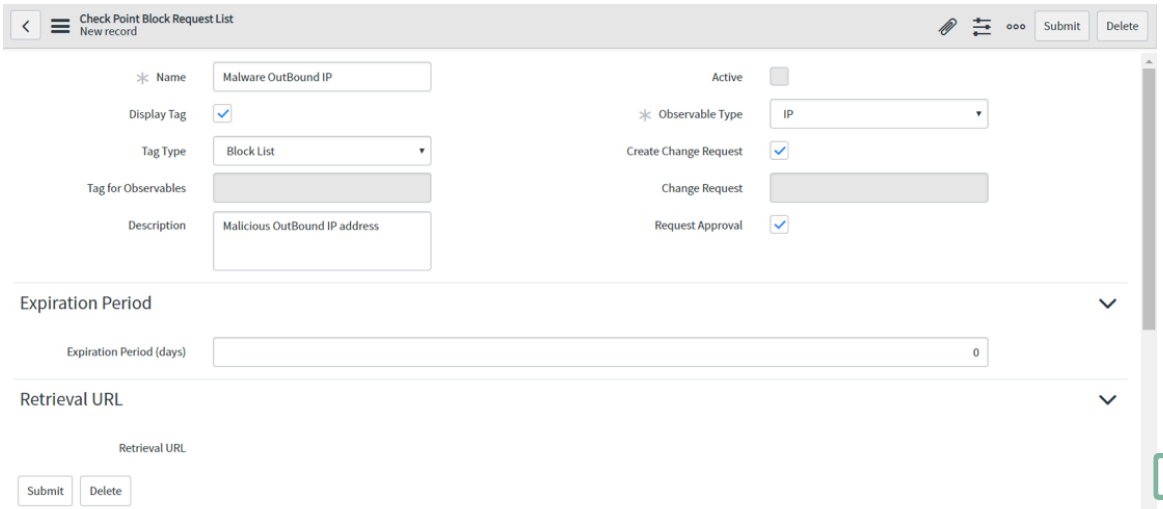
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
タイプ	
タグタイプ	リストから利用可能なタグ。 ブロックリストは、チェックポイント次世代の脅威防止でブロックする観測事象のリストです。 許可リストは、いかなる場合もチェックポイント次世代の脅威防止でブロックしない観測事象のリストです。 デフォルトでは、ブロックリストのタグの色は黒で、許可リストのタグの色は灰色です。色は変更できます。
変更要求の作成	このチェックボックスはデフォルトでオンになっており、Now Platform インスタンスで変更要求と変更タスクを自動的に作成し、ブロックリストレコードに添付します。 変更要求は、チェックポイント次世代ファイアウォールゲートウェイでブロックリスト取得 URL を設定するために使用されます。 ファイアウォールアドミニストレーターがファイアウォールポリシーまたはルールの変更に Now Platform も使用している場合は、このオプションをお勧めします。要求を作成した場合、ブロックリストは要求がクローズされると自動的にアクティブになります。 すべてのチェックポイントゲートウェイでカスタムインテリジェンスフィードが設定されたというメール通知をファイアウォールアドミンから受信した後、チェックボックスをオフにしてブロックリストを手動で有効にします。 [変更要求を作成] チェックボックスをオフにすると、[変更要求] フィールドは使用できません。
承認リクエスト	このチェックボックスは、ブロックリストのブロックリストエントリをアクティブ化/削除するための承認を要求するために、デフォルトでオンになっています。承認は、Security Incident Management者 (sn_si.admin) ロールを持つユーザーから要求されます。承認リクエストはメールで承認者に送信されます。 承認されると、そのブロックリストでエントリがアクティブになります。 チェックボックスがオンになっていない場合、そのブロックリストのエントリは承認ワークフローに従わず、ブロックリストで直接アクティブ化されます。
観測事象のタグ	このフィールドは、[タグを表示] チェックボックスがオンになっている場合にのみ表示されます。ブロックリストが保存されると、このフィールドに [名前] フィールドのデフォルト値が自動的に入力されます。ブロックリストが「Malware URL」という名前で作成されている場合、派生するタグ名は「Block List – Malware URL」となります。
変更要求	[変更要求を作成] チェックボックスをオンにした場合、ブロックリストが保存されると、変更の要求番号が Now Platform インスタンスに表示されます。 [変更要求を作成] チェックボックスをオフにすると、このフィールドは表示されません。
説明	チェックポイントブロックリストの説明。名前には通常、このブロックリストにあると予想されるサイトと観測事象のタイプが含まれており、このフィールドを使用して詳細を確認できます。
有効期間	ブロックリストの有効期間。 0 (デフォルト) は、ブロックリストエントリが無期限であることを示します。

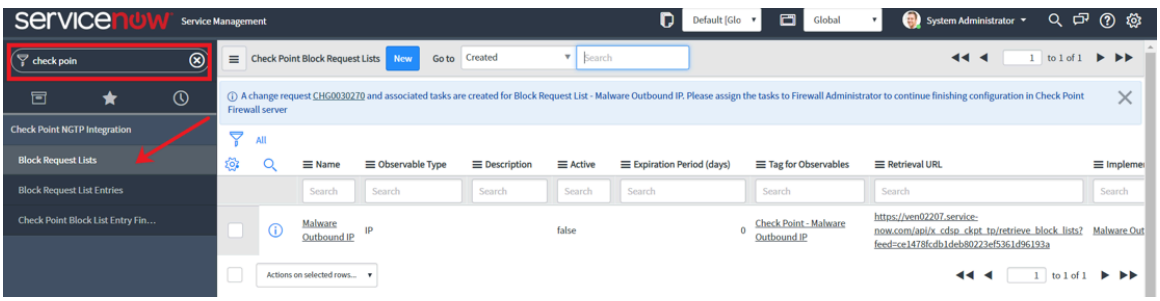
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

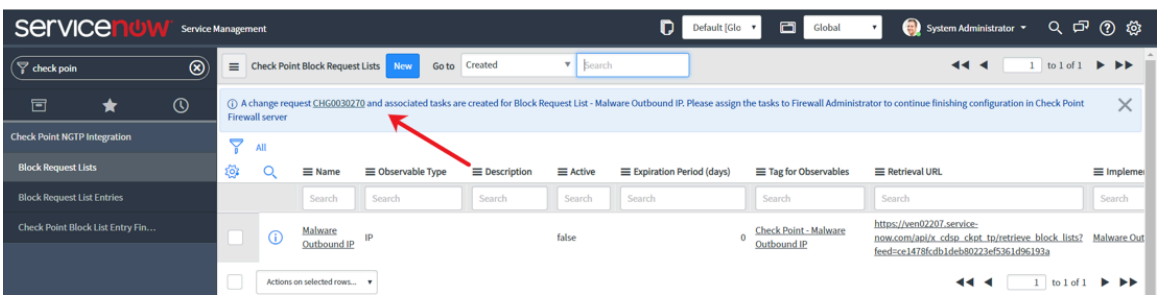
フィールド	説明
(日数)	この値を変更すると、このエントリは入力した日数の間有効になります。入力できる最小値は 1 (24 時間) で、最大値はありません。
取得 URL	ブロックリストが保存されると、取得 URL が自動的に生成されます。チェックポイントゲートウェイでこのブロックリストを設定するには、この URL を使用する必要があります。この URL を設定すると、チェックポイントは csv 形式でブロックする観測事象をフェッチします。



5. [**Submit** (送信)] を選択します。
6. [チェックポイントブロック要求リスト] が表示されない場合は、次に移動します: チェックポイント **NGTP** 統合 > ブロック要求リスト.



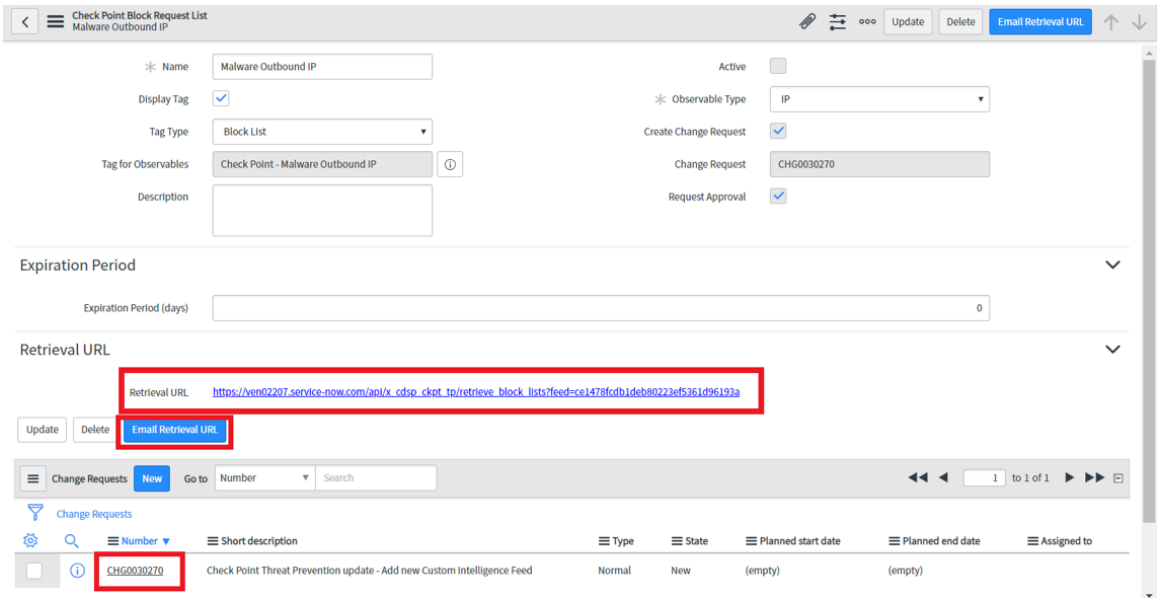
新しいブロックリストが表示されます。[ブロックリスト] ステータスがまだ非アクティブ (false) です。これは、ブロックリストがエントリを受け入れることができないことを意味します。[変更要求を作成] が設定されている場合は、Now Platform インスタンスに変更要求とタスクが作成されたことを示すメッセージが表示されます。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. [名前] 列でアイテムをクリックしてレコードを開きます。
   ブロックリストレコードが表示されます。この例は「Malware Outbound IP」ブロックリストを示しています。次のフィールド、オプション、リンクが送信後に新しいレコードに表示されます。詳細は次の表を参照してください。



フィールド	説明
メール取得 URL (Email Retrieval URL)	チェックポイントのファイアウォールアドミニストレーターに、ブロックリンクが設定可能であることを通知するメールを送信します。
取得 URL	この URL は、チェックポイントゲートウェイでカスタムインテリジェンスフィードを設定するのに使用されます。 **注:** [システムの設定] を [タブ付きフォーム] に設定している場合、このリンクがレコードの下部にある [ブロックリスト取得情報 (Block List Retrieval Info)] タブに表示されます。
Now Platform 変更要求	設定時に変更要求レコードへのリンクが [変更要求] セクションに表示され、要求番号が [変更要求] フィールドに表示されます。
更新	データを変更し、編集可能なフィールドを更新します。
削除	レコードを削除します。

8. 必要に応じてブロックリストを作成して追加します。
   ブロックリストが [チェックポイントブロック要求リスト] ページに表示されます。

次のタスク
手動で、または Now Platform 変更要求を使用して、ブロック要求リストをアクティブにします。

Check Point NGTP 統合のブロックリストのアクティブ化

Now Platform でブロックリストが作成され、URL が利用可能になると、チェックポイントアドミニストレーターは、すべてのチェックポイント次世代ゲートウェイでブロックリストをカスタムインテリジェンスフィードとして設定します。ブロックリストエントリを受け入れるようにするには、ブロックリストをチェックポイントで設定し、Now Platform で有効にする必要があります。

自動翻訳

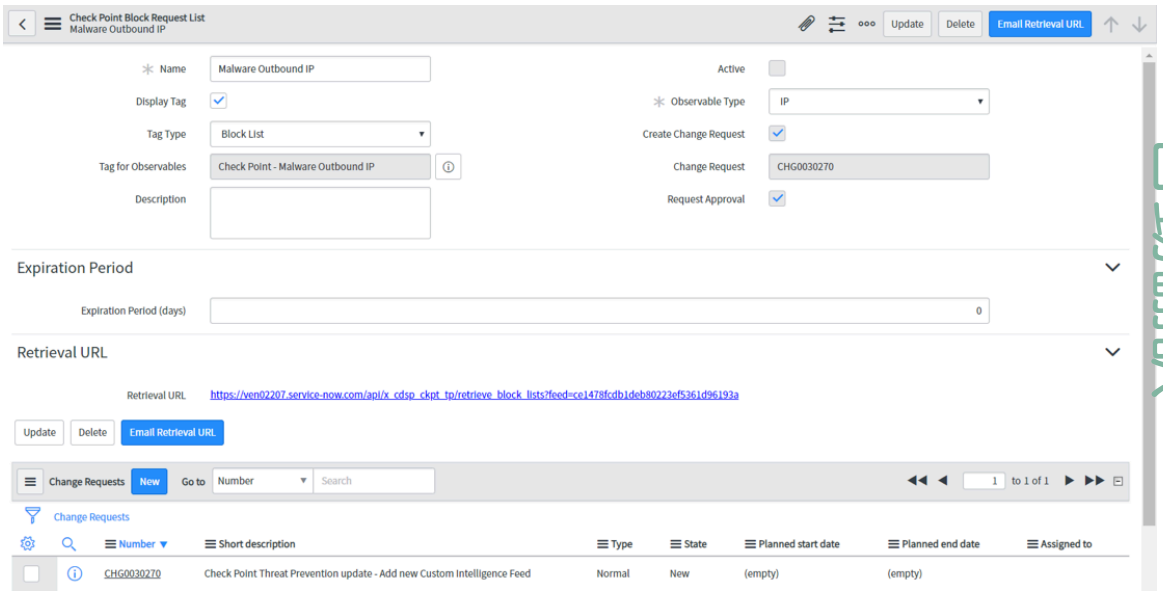
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：セキュリティインシデントアドミニストレーター (sn_si_admin)

このタスクについて
ブロックリストを設定した後、セキュリティインシデントアドミニストレーターとして手動でブロックリストをアクティブにするか、Now Platform 変更要求の完了時にブロックリストを自動的にアクティブにすることができます。ブロックリストのエントリを受け入れるには、変更要求を承認し、非アクティブ状況からアクティブ状況に移行する必要があります。

手順

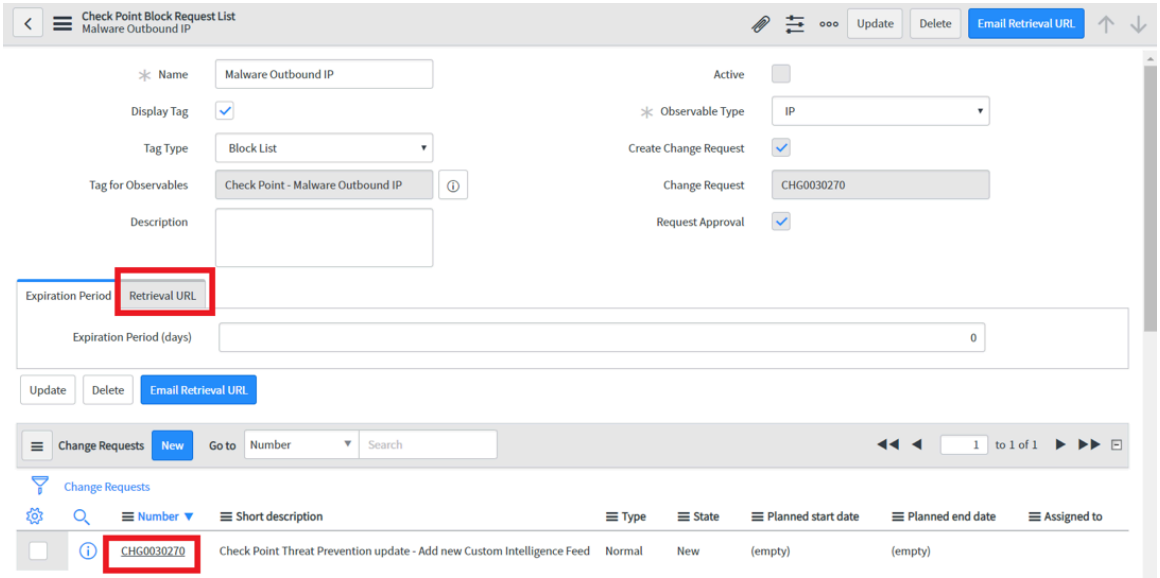
1. 次のように移動する。 **All** (すべて) > チェックポイント **NGTP** 統合 > ブロック要求リストをクリックし、[ブロック要求リスト] モジュールを選択します。
2. 表示される [チェックポイントブロック要求リスト] リストで、[名前] 列で新しいブロックリストを選択します。
3. 表示されるレコードで、[メール取得 **URL (Email Retrieval URL)]** ボタン、アクティブなブロックリストの取得 URL リンク、および [変更要求] セクションの Now Platform の変更要求をメモします。
   [アクティブ] チェックボックスがオフになっていることも確認してください。



> **注:**
> システムの設定で [タブ付きフォーム] をクリアすると、ブロックリストの取得 URL が [取得 URL] セクションに表示されます。

4. [ブロックリスト取得 **URL (Block List Retrieval URL)]** タブをクリックして、取得 URL を表示します。
   次の図では、システムの設定で [タブ付きフォーム] がオンになっているため、[ブロックリスト取得 URL (Block List Retrieval URL)] が表示されています。変更要求 (CH0030270) へのリンクも表示されています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. 設定を完了してブロックリストを非アクティブからアクティブにするには、次のいずれかのオプションを選択して、取得 URL が利用可能であることをファイアウォールアドミニストレーターに通知する必要があります。

オプション	説明
[メール取得 URL (Email Retrieval URL)] をクリックする。	ブロックリスト取得 URL をファイアウォールアドミニストレーターに直接メールで送信します。このオプションを使用すると、ファイアウォールアドミニストレーターはチェックポイントプラットフォームでの設定を完了できます。ファイアウォールアドミニストレーターが Now Platform を使用していない場合は、このオプションを選択します。
Now Platform 変更要求を完了し、構成タスクをファイアウォールアドミニストレーターにアサインする。	このオプションは、チェックポイントのファイアウォールアドミニストレーターが Now Platform も使用しており、Now Platform の変更の管理および承認プロセスが設定されている場合にのみ使用できます。 **注:** セキュリティインシデントアドミニストレーター (sn_si.admin) ロールを持つユーザーは、Now Platform 変更要求を承認できます。構成タスクが完了し、変更要求がクローズされると、ブロックリストは自動的にアクティブになります。

次のタスク
取得 URL が利用可能であることをファイアウォールアドミニストレーターに通知し、セキュリティインシデントアドミニストレーターとしてブロックリストがチェックポイントで設定されていることを確認したら、ブロックリストをアクティブにします。ブロックリストは手動でアクティブにするか、設定されている場合は、Now Platform の変更要求フォームを使用してブロックリストをアクティブにします。ブロックリストは、変更要求がクローズされると自動的にアクティブになります。

Check Point NGTP 統合でのカスタムインテリジェンスフィードとしてのブロックリストの設定

ファイアウォールアドミニストレーターは、Now Platform で作成されたブロックリストに対応するカスタムインテリジェンスフィードを設定する必要があります。

始める前に
必要なロール：admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
このタスクは、各チェックポイント NGTP ゲートウェイで実行する必要があります。ファイアウォールアドミニストレーターには、ゲートウェイサーバーの SSH アクセス権が必要になる場合があります。組織に Now Platform の変更管理および承認プロセスがある場合は、メールの送受信機能が有効になっていることを確認します。
ファイアウォールアドミニストレーターには、ブロックリストの取得 URL と、チェックポイント API アカウントアクセスロール (sn_sec_checkpoint.api_account_access) を持つ ServiceNow ユーザー認証情報が必要です。

ファイアウォールアドミニストレーターが Now Platform を使用していない場合には、NOW Security Incident Management者はメールで必要な情報を提供できます。または、ファイアウォールアドミニストレーターが Now Platform を使用している場合には、ブロックリストに関連付けられた変更要求をファイアウォールアドミニストレーターにアサインすることができます。この変更要求には、カスタムインテリジェンスフィードを設定するために必要な情報が含まれています。

チェックポイントゲートウェイでのカスタムインテリジェンスフィードの設定の詳細については、以下を参照してください。https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

手順

1. 次の場所に移動して、Now Platform インスタンスでメールの送受信機能が有効になっていることを確認します。 メールプロパティ > アドミニストレーション > メールプロパティ.
2. [送信メール設定] で、[メール送信] と [メール受信] が選択されていることを確認します。
3. SSH をエキスパートモードでチェックポイントゲートウェイに変更します。
4. カスタムインテリジェンスフィードを追加するコマンドを実行します。
   コマンドはインタラクティブに実行され、フィード形式とパスワードの入力を求められます。
   - フィード形式の入力を求めるプロンプトが表示されたら、「cp_csv」と入力します。
   - API アクセス権を持つ Now Platform ユーザーパスワードの入力を求められた場合。

   コマンドを実行すると、サーバー証明書 (Now Platform) がマシンによって信頼されていないと警告され、サーバーセキュリティ証明書をマシンの信頼できるストアに追加するように求められる場合があります。「**Y**」と入力します。

   「Status:Succeed」というメッセージが表示され、フィードが正常に追加されたことが確認できます。

```
[Expert@gw-93440b:0]# ioc_feeds add --feed_name phishing_url --transport https --resource https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/retrieve_block_lists?feed=<feed_id> --user_name <now_ckpt_api_user> --feed_action Prevent
Enter feed format. Should be cp_csv/stix_1.x: cp_csv
Only Check Point's csv format files will be loaded
Enter Password
Password: <now_ckpt_api_password>

Default value for active is: true

Feed Name: phishing_url
Feed is Active
File will be fetched via HTTPS
Resource: https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/retrieve_block_lists?feed=<feed_id>
Action: Prevent
User Name: admin

[============================================================] 100.0% ...Getting file from the server
The server security certificate is not trusted by your machine.
SHA256 Fingerprint=SHA256 fingerprint of the NOW instance.

Do you want to trust it for this specific feed?  [y/n]: y
Fetching active feeds

Update summary
##############
feed: phishing_url. Status: Succeed
##############
Activating Scheduler

[Expert@gw-93440b:0]#
```

Check Point NGTP 統合のセキュリティインシデントからのブロックリストエントリの送信

セキュリティインシデントレコードに添付された観測事象は、さまざまなブロックリストへのブロックリストエントリとして承認のために送信されます。ブロックリストエントリのオプションの承認プ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ロセスは、事前設定されたワークフローの一部です。ゲートウェイは、ブロックリストに含まれているブロックリストエントリ (IP アドレス、URL、ドメイン) をインポートします。

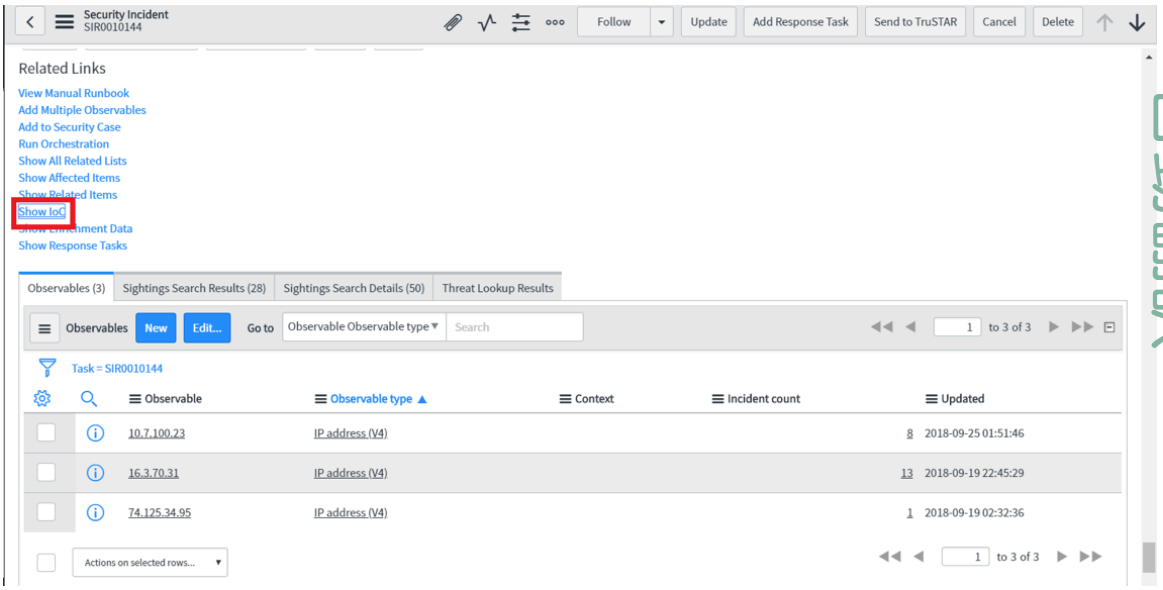
始める前に
必要なロール：

- ブロックリストエントリを送信するセキュリティインシデントアナリスト (sn_si.analyst)。
- ブロックリストエントリを承認するSecurity Incident Management者 (sn_si.admin)。この権限は、組織の必要に応じてアサインすることができます。

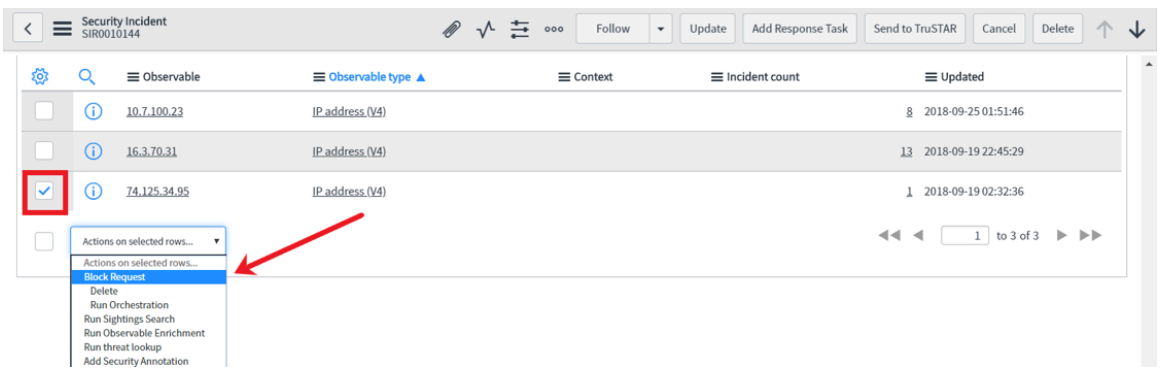
このタスクについて
sn_si.analyst ロールを持つユーザーが、セキュリティインシデントレコードに添付された観測事象のブロックを要求して、ブロックエントリを送信します。送信されると、ステータスが [処理待ち] のブロックリストエントリが生成され、承認のために送信されます。次の例は、URL 観測事象のブロック要求を示しています。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示をクリックし、セキュリティインシデントレコードをクリックして開きます。
2. **[IoC** を表示] 関連リンクをクリックします。



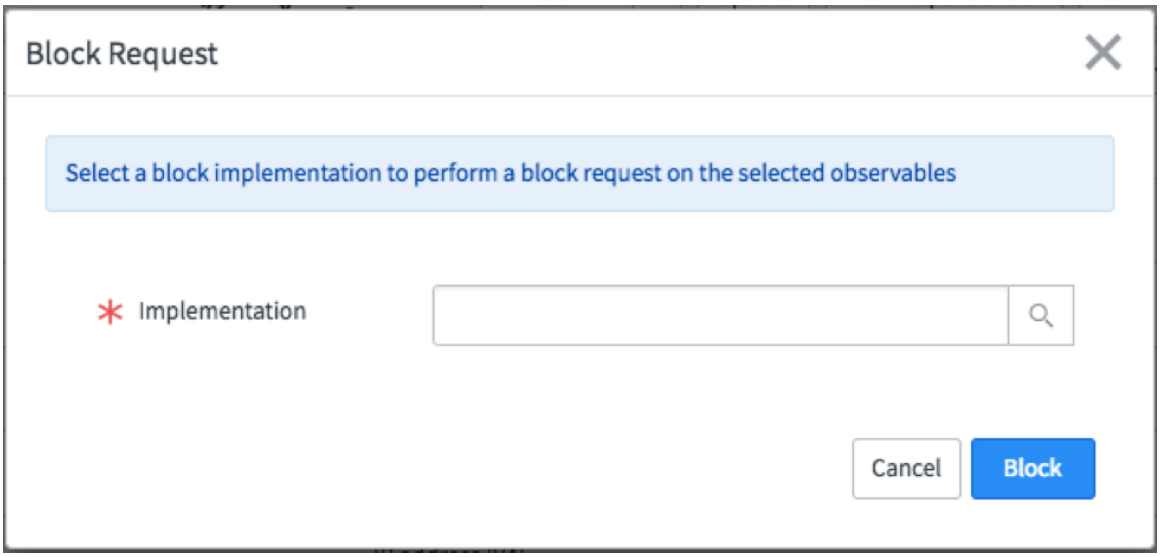
3. [観測事象] 関連リストでブロックする観測事象を選択し、[選択した行のアクション] リストから [ブロック要求] を選択します。



自動翻訳

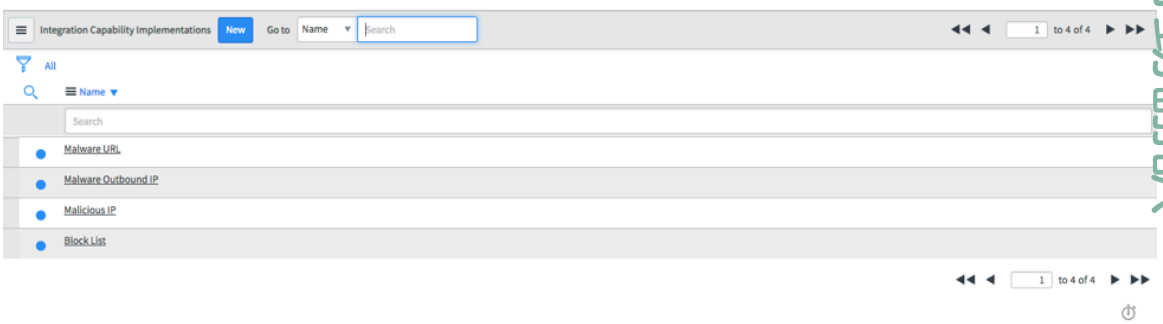
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. 表示されるダイアログボックスで、検索アイコン ( ) をクリックします。

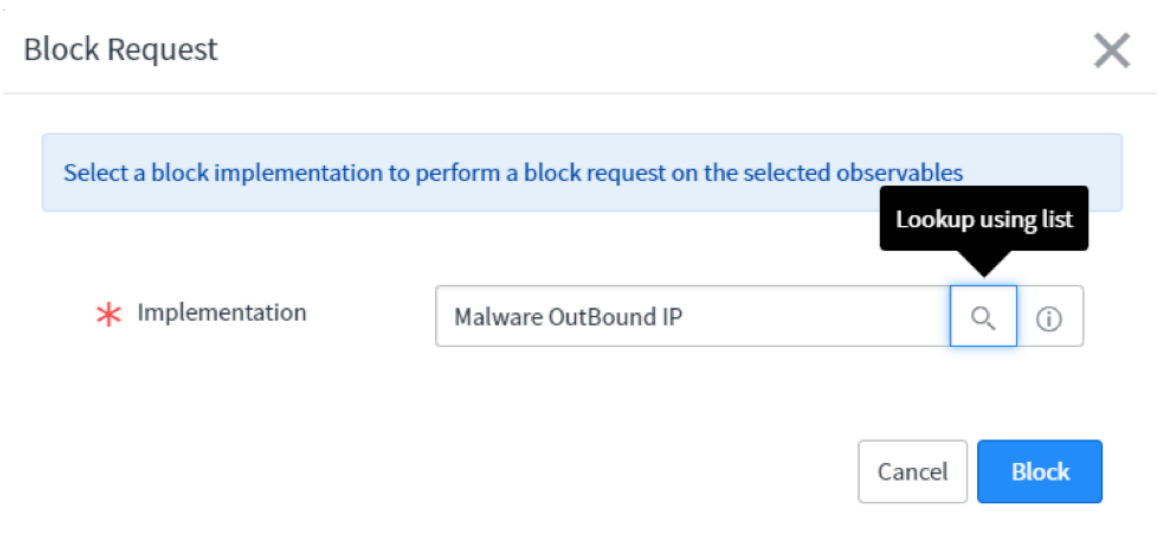


5. リストから、このエントリを添付するブロックリストを選択します。

注:
この例では、エントリの観測事象タイプ (IP) が [ブロックリスト] の観測事象タイプ (IP) と一致している必要があります。



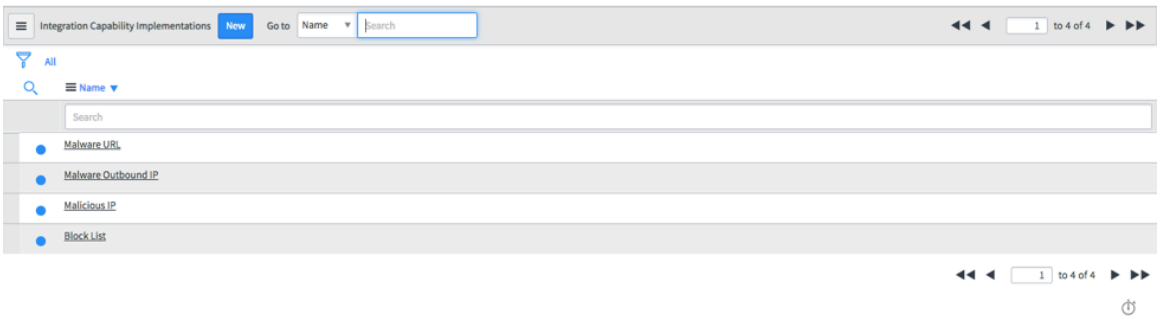
6. [ブロック要求] ダイアログボックスでブロックリスト名が [実装] フィールドに表示されたら、[ブロック] をクリックします。



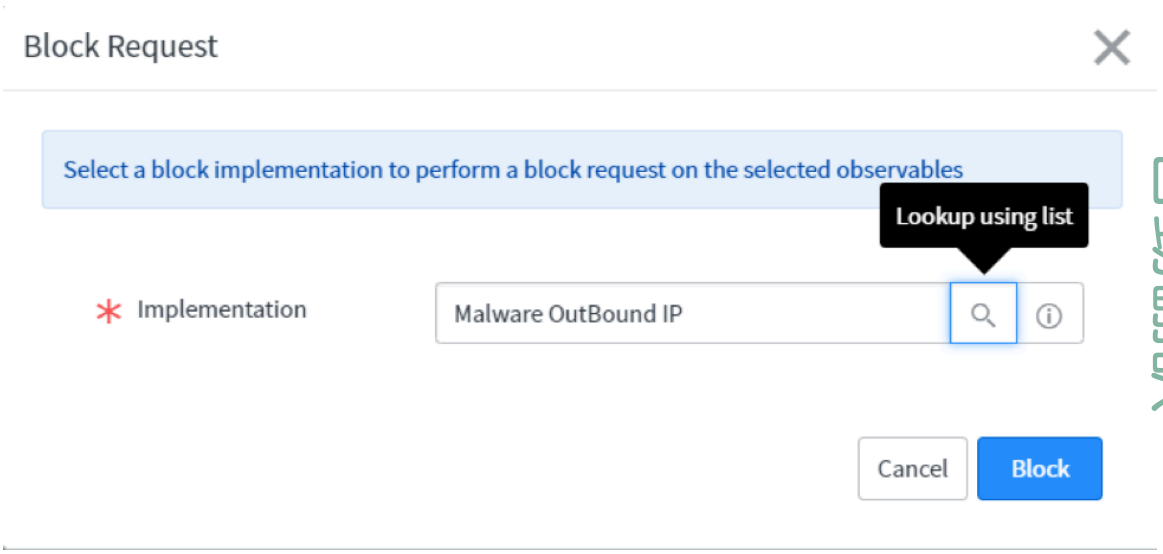
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. 表示されたリストからこのエントリに添付するブロックリストを選択します。

   注:
   この例では、エントリの観測事象タイプ (IP) が [ブロックリスト] の観測事象タイプ (IP) と一致している必要があります。



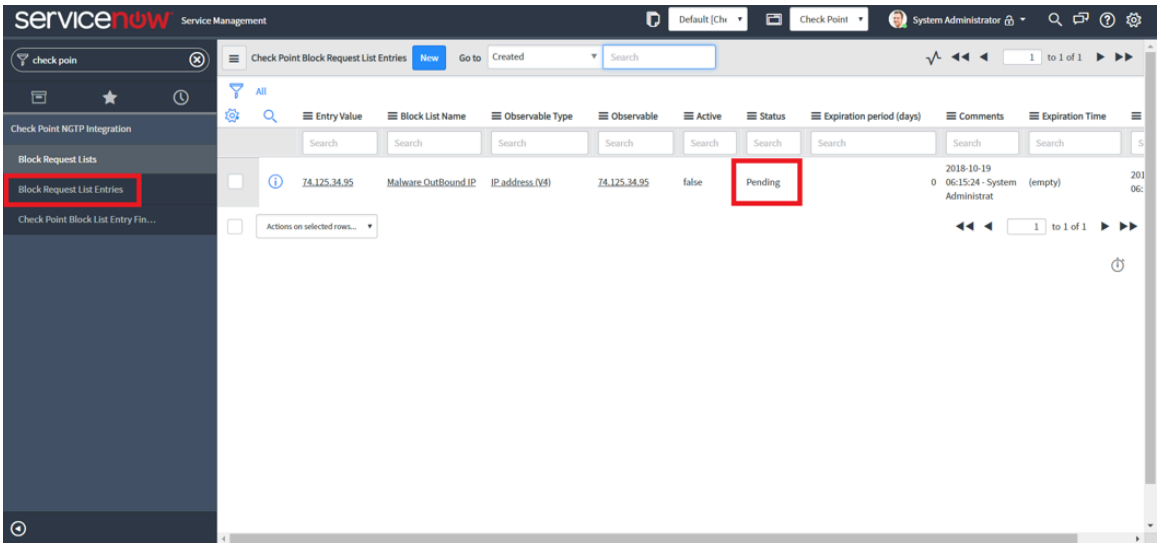
8. [ブロック要求] ダイアログボックスでブロックリスト名が [実装] フィールドに表示されたら、[ブロック] をクリックします。



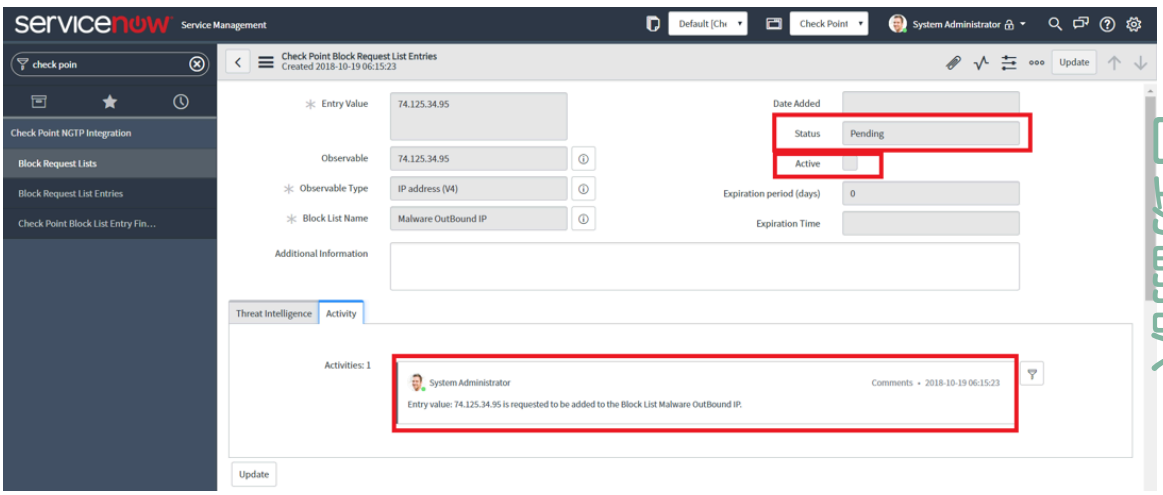
9. 次のように移動する。 チェックポイント **NGTP** 統合 > ブロック要求リストエントリをクリックし、[要求リストエントリのブロック**(Block Request List Entries)**] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



10. [チェックポイントブロック要求リストエントリー] リストで、[エントリー値] 列の観測事象をクリックしてレコードを開きます。
この例では、「**74.125.34.95**」のレコードが表示されます。



ステータスが [処理待ち] で、 [アクティブ] チェックボックスがオフになり、作業メモに観測事象を追加する要求があることが示されます。このブロックリストエントリ要求は承認の準備ができています。

[観測事象] フィールドの横にあるアイコンは、Now Platform の [観測事象] テーブルへのリンクです。

[観測事象] フィールドの値 (74.125.34.95) が [観測事象] テーブルにリンクされ、セキュリティインシデントレスポンスインシデントトリガーイベントから引き継がれた形式と照合されます。

ブロックリストエントリテーブルからのブロックリストエントリの直接送信

悪意があると判断され、特定の Now Platform セキュリティインシデントに関連付けられていない観測事象の場合は、ブロックリストからブロックリストエントリを送信します。

始める前に

必要なロール：Security Incident Management者 (sn_si.analyst)

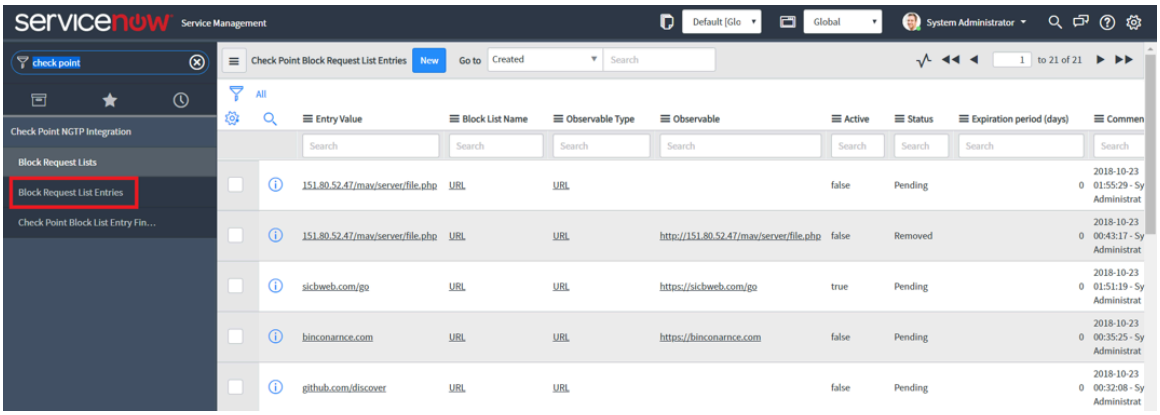
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
悪意があると判断した観測事象をブロックするか、または悪意がないと判断した観測事象を許可する必要があり、その観測事象が特定の Now Platform セキュリティインシデントレコードに関連付けられていない場合は、ブロックリストからブロックリストエントリを直接送信します。これらのタイプのブロックリストエントリの例として、特定のサイトの URL やドメインが挙げられます。

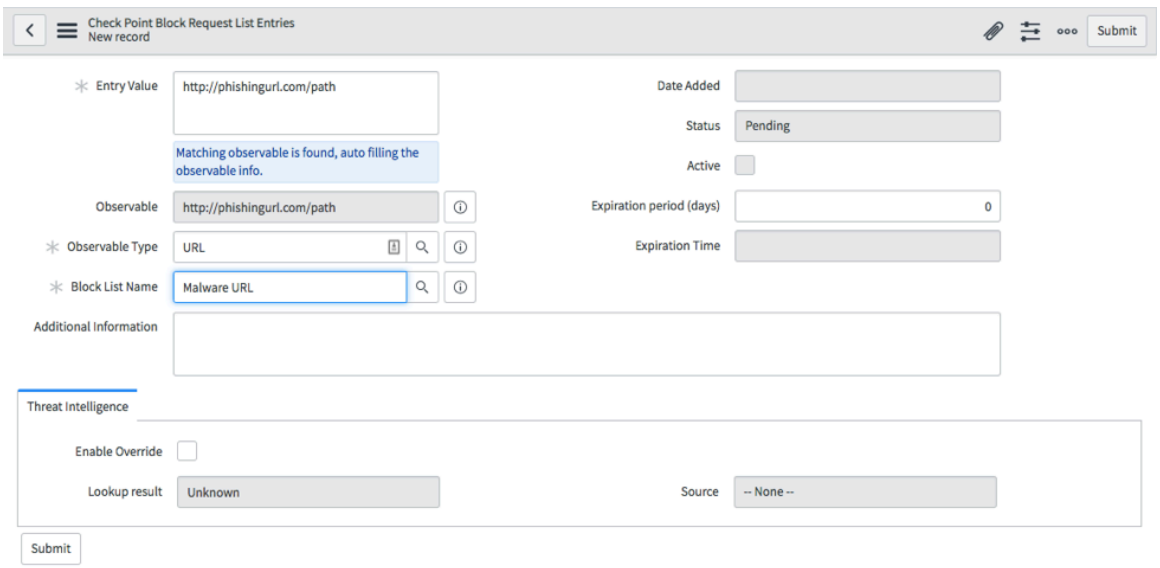
手順

1. 次のように移動する。 **All** (すべて) > チェックポイント **NGTP** 統合 > ブロック要求エントリー.



2. [ブロック要求リスト] モジュールをクリックします。
3. [チェックポイントブロック要求リストエントリー] リストで [新規] をクリックします。
4. [エントリー値] フィールドに観測事象の値を入力します。
   このエントリで考えられる結果 2 パターン：
   - フォームの残りのフィールドがすべて自動入力されます。
   - 一致する観測事象が見つかり、一致する観測事象が存在することを示すメッセージが表示されます。このエントリを添付するブロックリストを選択し、[送信] をクリックします。有効期間を設定する前に、このエントリを添付するブロックリストを選択します。

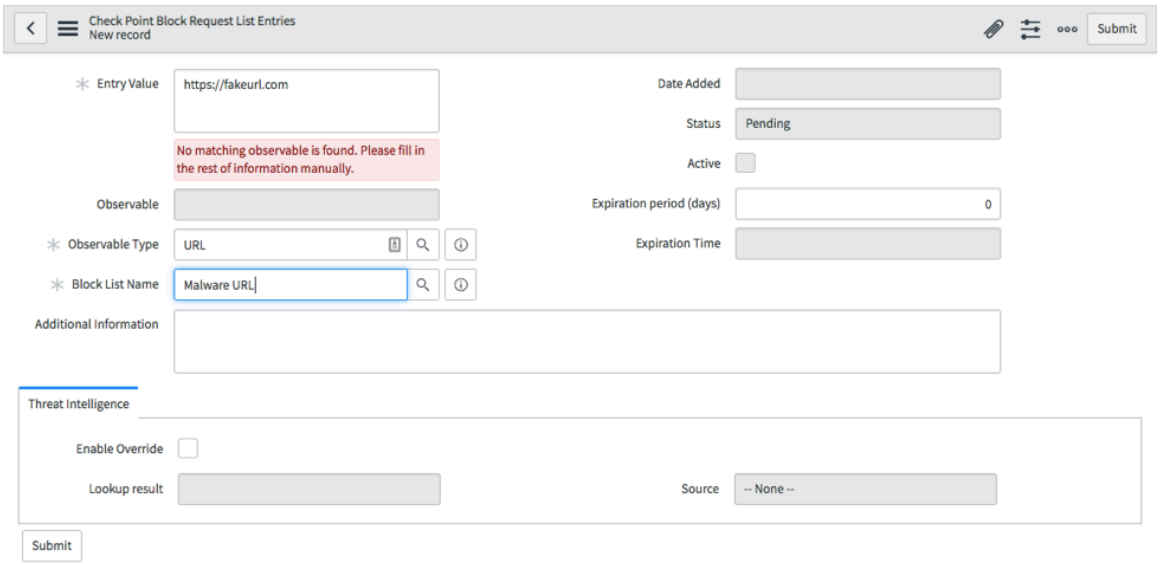
   フォームに入力するよう指示するメッセージが表示されます。一致する観測事象が見つかりません。フォームに入力する必要があります。完了したら、観測事象を添付するブロックリストを選択し、[送信] をクリックします。観測事象レコードが作成されます。次の図は、既存のドメイン観測事象の例と、フィールドがどのように自動入力されるかを示しています。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. 検索アイコンをクリックして、エントリを添付するブロックリストを選択します。
6. [送信] をクリックします。
7. ワークフローでメール承認が設定されている場合は、承認メール要求が送信されます。
   残りの情報を手動で入力するように要求するメッセージが表示された場合は、フィールドに入力します。



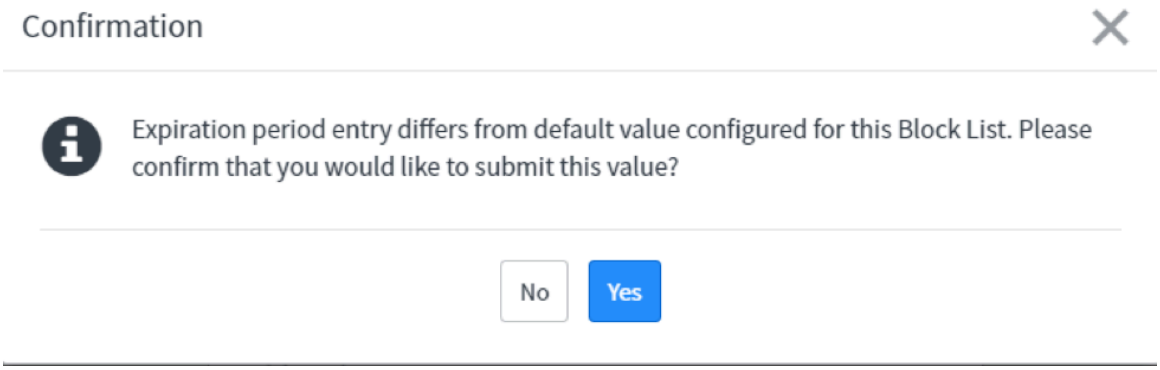
フィールド	説明
観測事象タイプ	ダイアログからサポートされている観測事象タイプ。
ブロックリスト名	エントリに対するブロックリスト。 **注:** 有効期間を設定する前に、エントリを添付するブロックリストを選択します。
上書きを有効化 (デフォルトではオン)	ルックアップ結果またはソース。設定すると、ルックアップ結果とその結果の検索に使用したソースを入力できます。通常、これらのフィールドはセキュリティインシデントレコードの作成時に入力されます。この場合、ルックアップ結果やソースはなく、これらのフィールドは手動で入力します。
ルックアップ結果	[不明] または [悪意がある] を選択します。
ソース	ブロックリストエントリで脅威のルックアップを実行するソース (ThreatCrowd など)
有効期間	デフォルトでブロックリストから継承された有効期間。この値はエントリの作成中にのみ上書きできます。 0 は、ブロックリストエントリが無期限であることを示します。 この値を変更すると、このエントリは入力した日数の間有効になります。入力できる最小値は 1 で、最大値はありません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

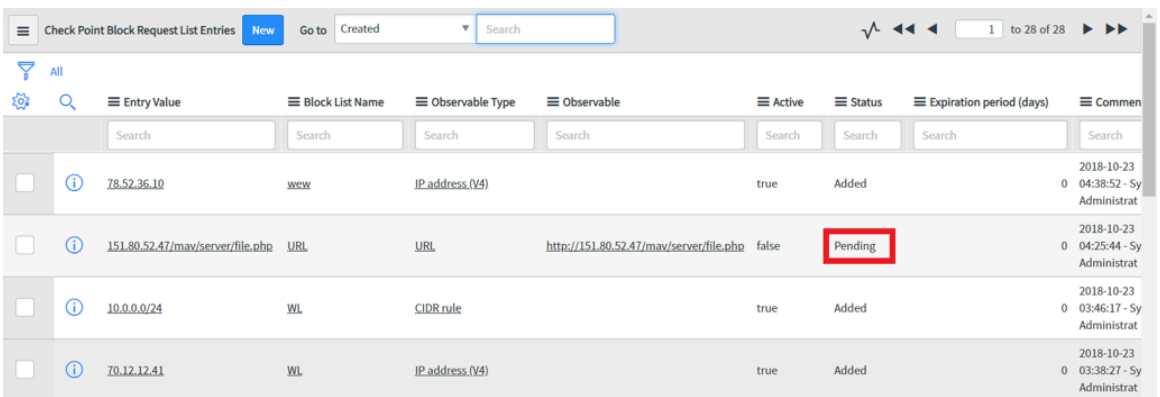
フィールド	説明
	たとえば、5 月 1 日の午後 2 時 1 分に 30 日と入力すると、ブロックリストのエントリは 5 月 31 日の午後 2 時 1 分に有効期限切れになります。ただし、スケジューラは毎日 00:00 に期限切れのエントリをチェックし、6 月 1 日 00:00 にエントリのステータスを [期限超過] に変更します。

8. [送信] をクリックします。
ブロックリストエントリのデフォルトの有効期間を変更した場合は、期間が選択したブロックリストと異なることを示す警告確認ダイアログボックスが表示されます。



オプション	説明
あり	有効期限の上書きを確認し、レコードを保存して、チェックポイントブロックリストエントリに戻ります。ワークフローでメール承認が設定されている場合は、承認メール要求が送信されます。
いいえ	上書きをキャンセルします。この時、[有効期間] の値を変更できます。 値を変更したら、[送信] をクリックしてチェックポイントブロックエントリのリストに戻ります。

9. 表示されない場合は、[チェックポイントブロック要求リストエントリー] に移動し、エントリのステータスが [処理待ち **(Pending)]** であることを確認します。



これで、エントリを承認する準備ができました。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Check Point NGTP 統合のブロックリストエントリの承認

ブロックリストエントリの承認プロセスは、事前設定されたワークフローの一部です。ブロックリストでエントリがアクティブになる前にブロックリストエントリを承認します。ブロックリストエントリを承認すると、ゲートウェイがそのエントリを取得し、それ以降は観測事象がブロックされます。

始める前に

- ブロックリストエントリの承認は、デフォルトでSecurity Incident Management者 (sn_si.admin) にアサインされますが、この権限は組織の必要に応じてアサインすることができます。次の例では、Now Platform アドミニストレーターが承認権限を持っています。

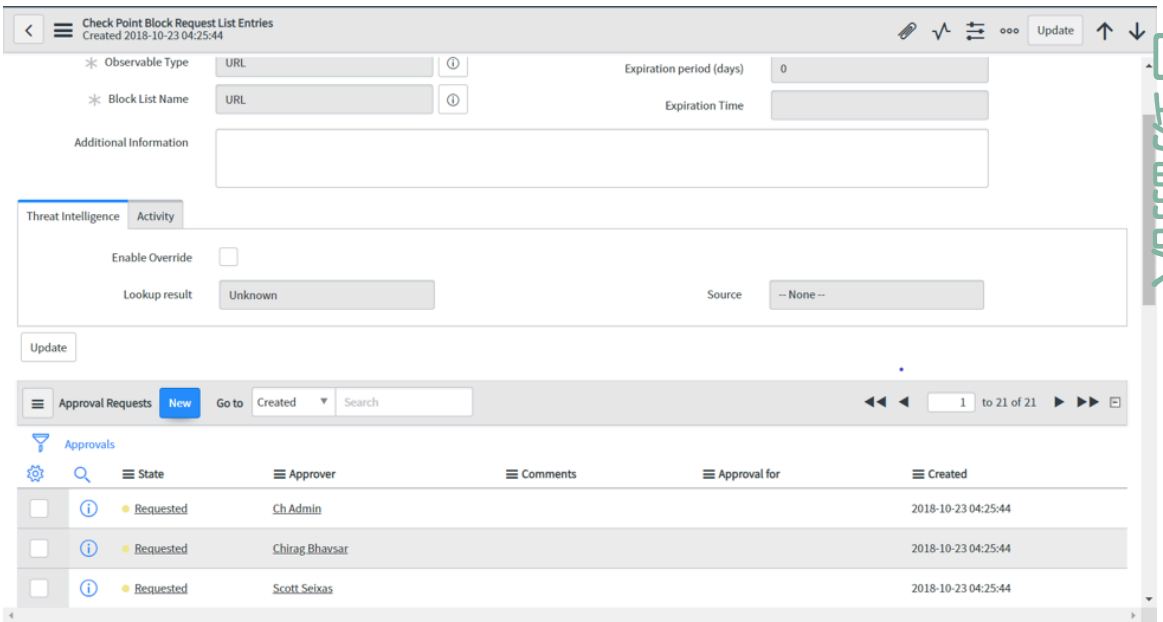
必要なロール：sn_si.admin

このタスクについて

承認プロセスが有効になっている場合、ブロックリストエントリは承認されるまでブロックリストでアクティブ化も非アクティブ化もされません。

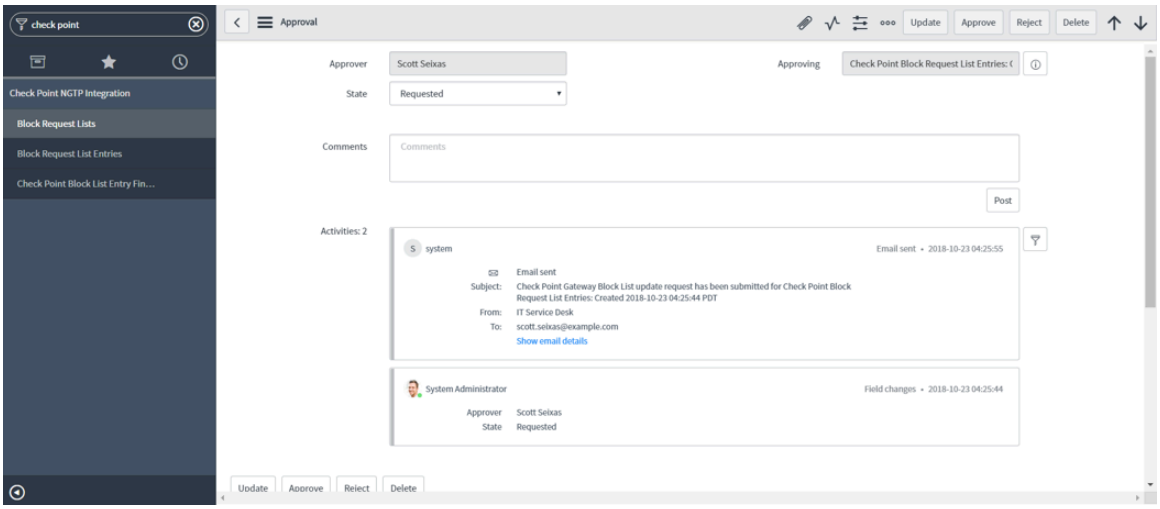
手順

1. 次のように移動する。 **All** (すべて) > チェックポイント **NGTP** 統合 > ブロック要求リストエントリをクリックし、ブロックリストエントリレコードを開きます。
2. [ブロックリストエントリ (Block List Entry)] レコードで、[承認要求] セクションまでスクロールします。



3. [承認要求] で、[ステータス] 列のアイテムをクリックして開きます。
承認レコードが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



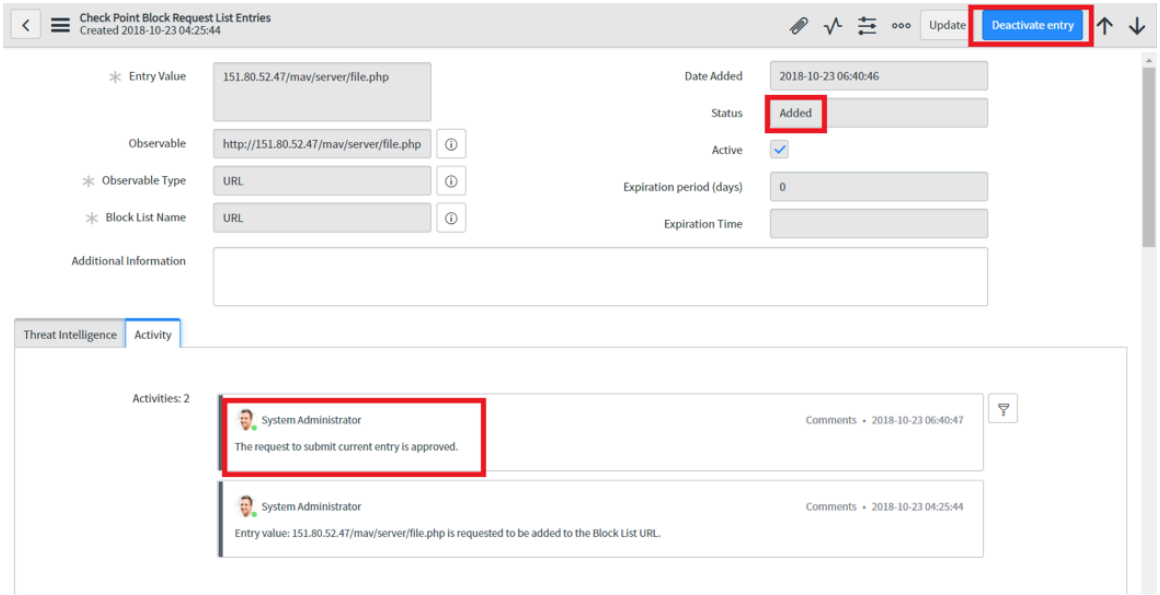
4. ブロックリストエントリを承認するためのオプションを 1 つ選択してください。

オプション	説明
承認	エントリレコードで [ステータス] フィールドが [追加済み] に変わり、[アクティブ] チェックボックスがオンになります。 [非アクティブ化] ボタンが表示され、アクティブになります。 作業メモは、ブロックリストエントリの要求が承認されたことを示しています。
却下	エントリレコードで [ステータス] フィールドが [却下] に変わり、[アクティブ] チェックボックスがオフになり、エントリがゲートウェイでブロックされていないことが示されます。 作業メモは、ブロックリストエントリの要求が却下されたことを示しています。

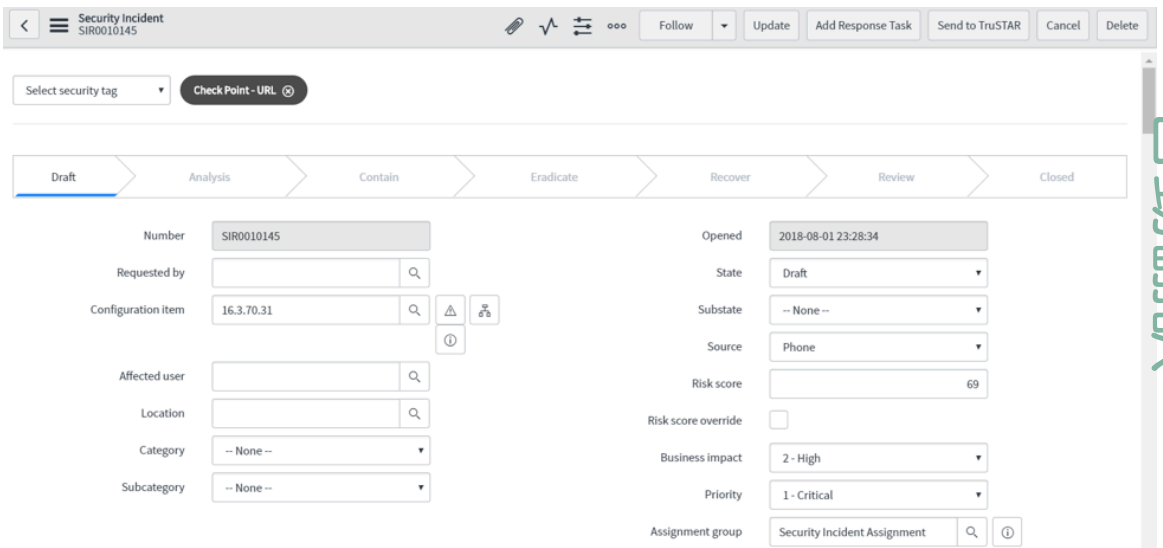
ブロックリストエントリを承認してアクティブにすると、チェックポイント次世代ファイアウォールは、次の取得間隔の後にブロックリストエントリを取得します。エントリが取得されると、その時点から観測事象がブロックされます。次の図では、[アクティブ] チェックボックスがオンで、ステータスが [追加] になっており、作業メモに要求が承認されたことが示されています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

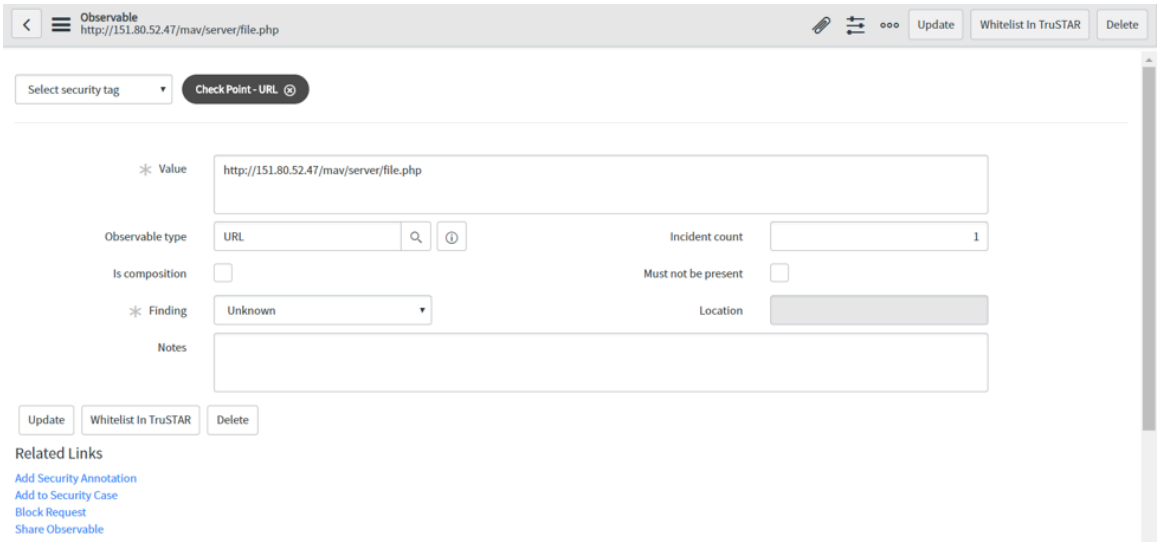


ブロックリストのエントリが承認されてアクティブ化されると、セキュリティインシデントレコードがセキュリティタグでマークされます。タグはレコードの上部に表示されます。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティタグは観測事象レコードにも表示されます。



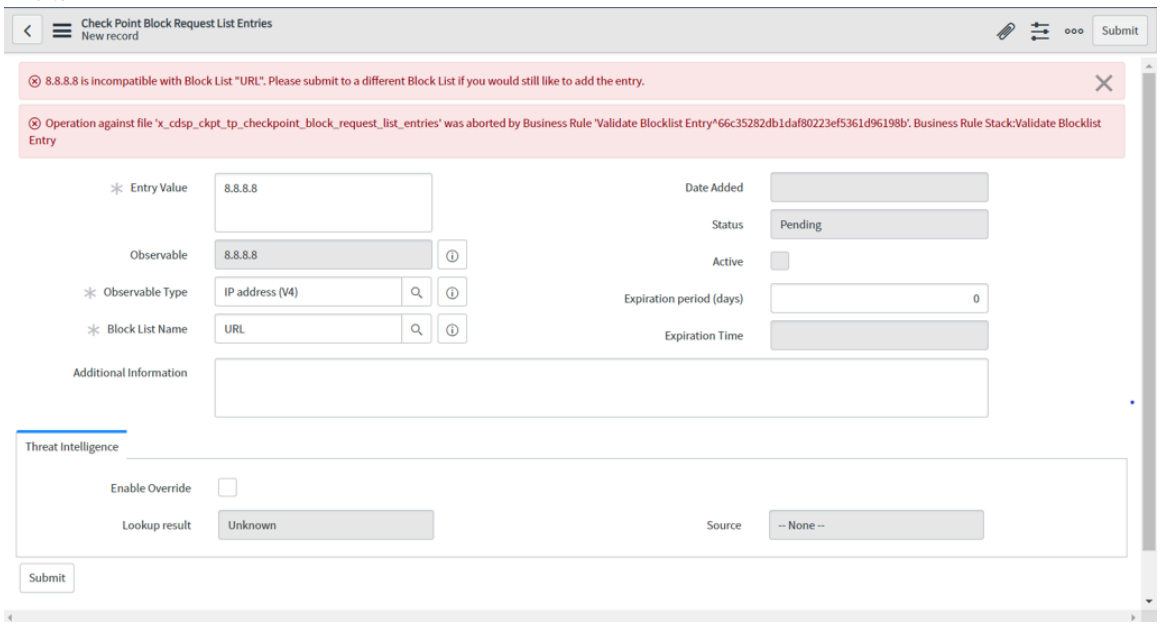
Check Point NGTP 統合のブロックリストエントリの例外

ブロックリストエントリをブロックリストに追加する場合には制限があります。ブロックリストエントリをブロックリストに追加しようとしたときに、重複、互換性、または CIDR (クラスレスドメイン間ルーティング) の競合が存在する場合は、これらのエラーの解決に役立つエラーメッセージが表示されます。

互換性の例外

各ブロックリストは、その観測事象タイプと互換性のあるエントリのみを受け入れます。ドメインブロックリストを作成し、それに IP アドレスの観測事象を添付しようとすると、非互換性エラーメッセージが表示されます。たとえば、次の図に示すように、ドメインブロックリストはドメイン観測事象のみを受け入れます。

互換性エラーのあるブロックリストフォーム

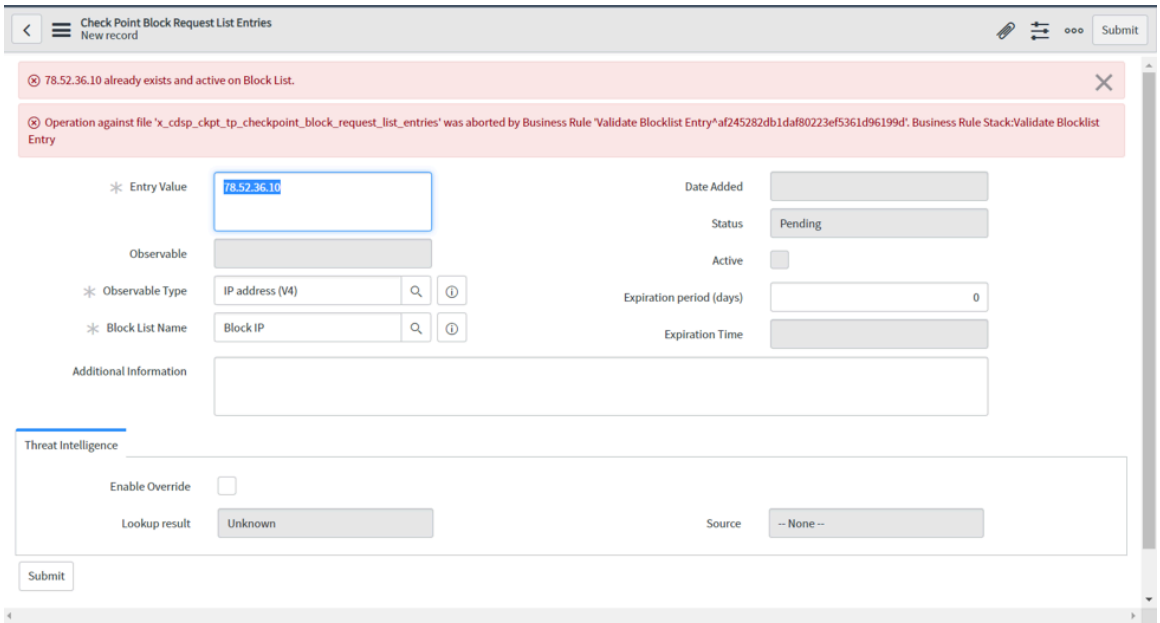


自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

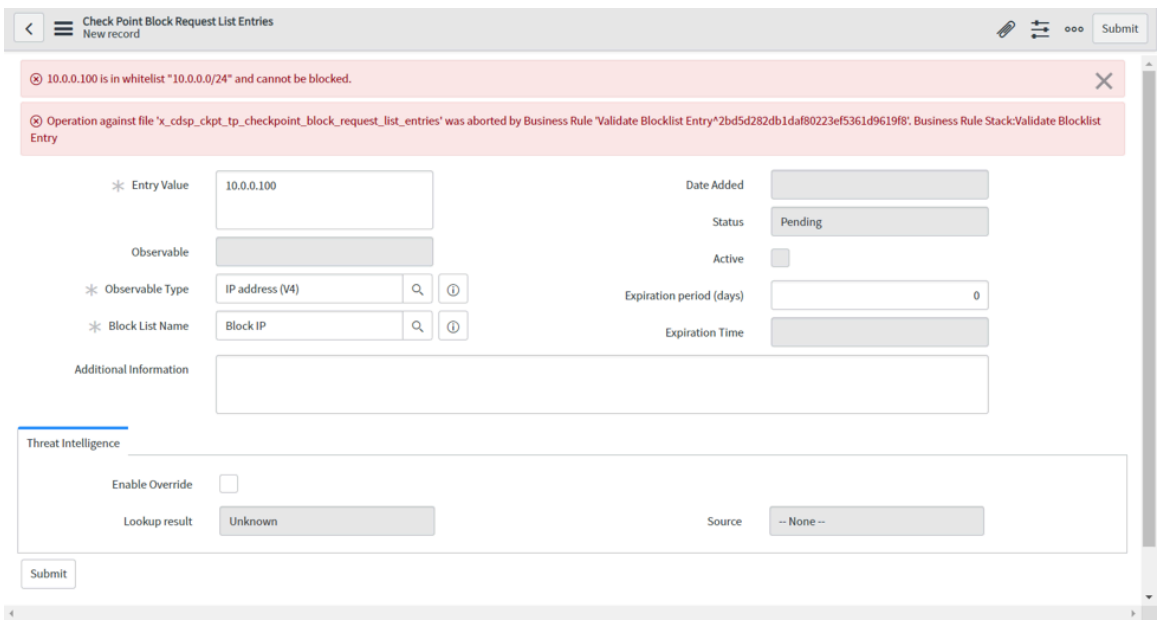
重複の例外

1 つの観測事象を観測事象タイプが同じ複数のブロックリストでアクティブにすることはできません。ある URL ブロックリストで既にアクティブになっている URL 観測事象をフィッシング URL ブロックリストでアクティブにしようとすると、重複エラーメッセージが表示されます。



CIDR (クラスレスドメイン間ルーティング) の例外

単一の IP アドレスを許可リストに添付しようとしたときに、この IP アドレスが既にブロックリスト/許可リストにある CIDR 観測事象の一部であった場合、CIDR 競合エラーが表示されます。このエラーは、単一の IP アドレスが CIDR 観測事象の一部としてブロックリストまたは許可リストに既に含まれていることを示します。たとえば、192.168.24.25 は CIDR ブロック 192.168.0.0/22 の一部です。



Check Point NGTP 統合のセキュリティタグ名の編集

ブロックリストレコードの作成時に [タグを表示] チェックボックスをオンにすると、セキュリティタグの名前と色を編集できます。セキュリティタグは、既にブロックされている観測事象を追跡するのに役立ちます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

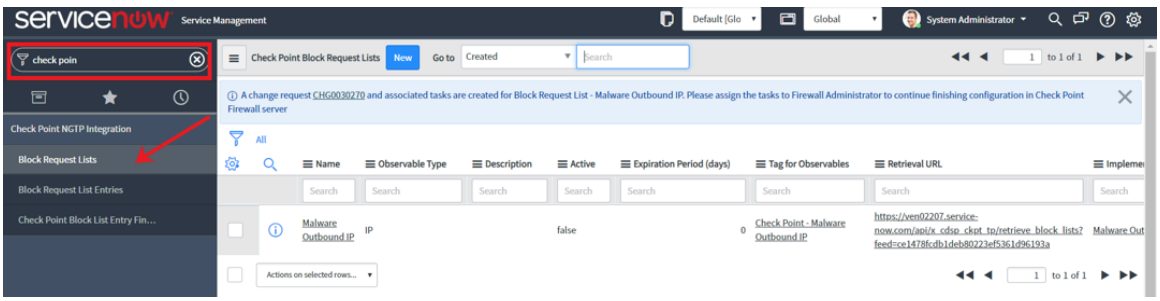
自動翻訳

始める前に
必要なロール：sn_si.admin

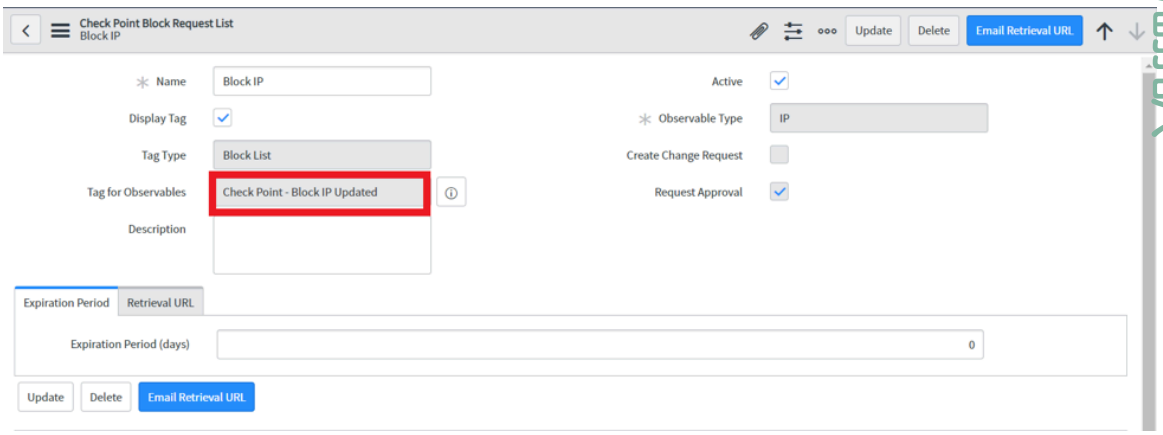
このタスクについて
セキュリティタグは、どのセキュリティインシデントのブロックリストに観測事象があるのかをすばやく識別するのに役立ちます。タグは、観測事象が既にブロックされているかどうか、またはブロックリストから削除されているかどうかを識別するのにも役立ちます。デフォルトでは、セキュリティタグの色は、ブロックリストエントリの場合は黒、許可リストエントリの場合はグレーです。特定のタグをより簡単に認識できるように、タグの名前と色を変更できます。

手順

1. 次のように移動する。 **All** (すべて) > チェックポイント **NGTP** 統合 > ブロック要求リストの構成.

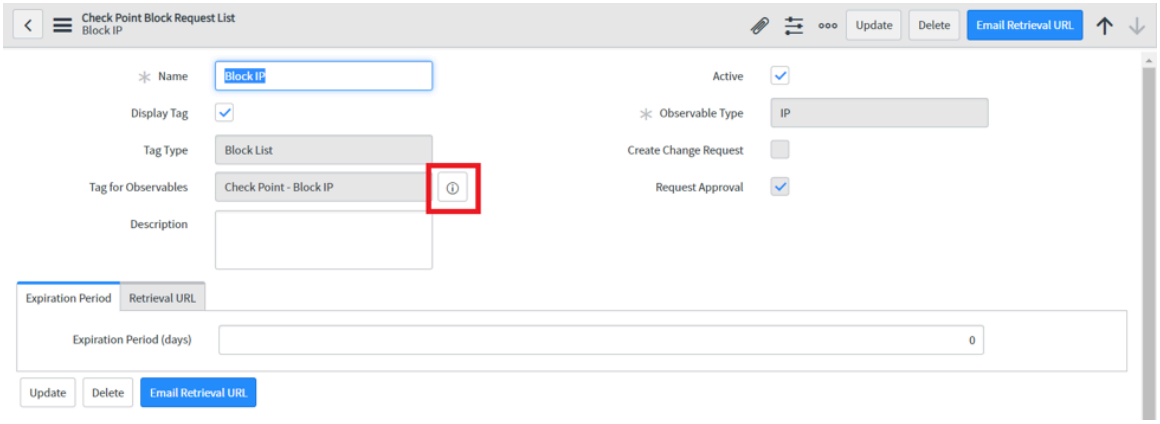


2. [名前] 列でアイテムをクリックしてレコードを開きます。
ブロックリストレコードが表示されます。デフォルトでは、セキュリティタグ名は、ブロックリストの作成時に [名前] フィールドに入力した値と同じです。デフォルトでは、名前には「Block List」プリフィックスも含まれます (例：Block List – Malware Malicious URLs)。

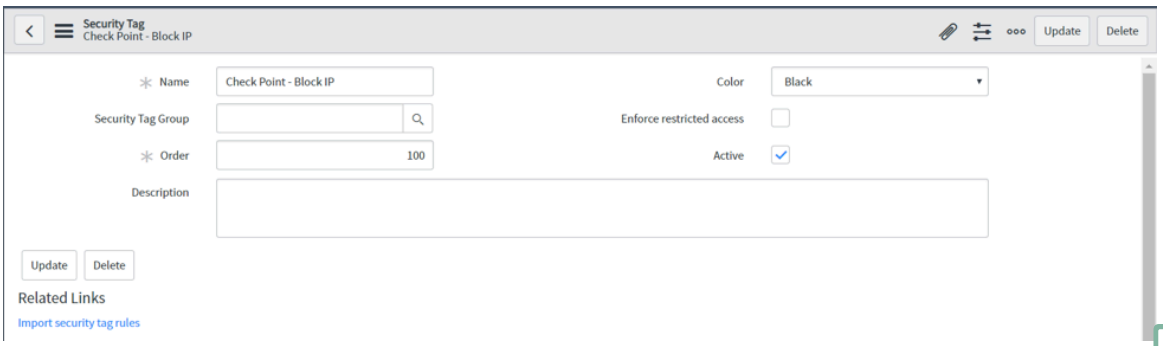


3. 観測事象のタグの横にある情報アイコンをクリックし、レコードを開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

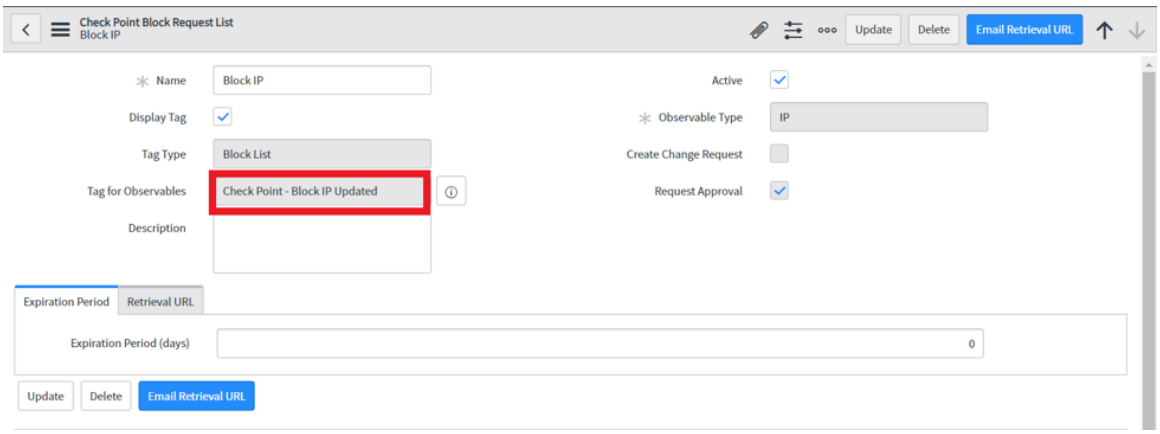


[セキュリティタグ] フォームが表示されます。



4. [名前] フィールドでセキュリティタグ名を変更します。
5. [更新] をクリックします。
   更新されたブロックリストレコードが、変更されたタグ名とともに表示されます。

   注:
   次の例では、タグ名に Outbound (送信) が追加されています。チェックポイント次世代ファイアウォールの統合に関連付けられていることを識別できるように、新しいタグ名にプリフィックス「Check Point」を付けておきます。

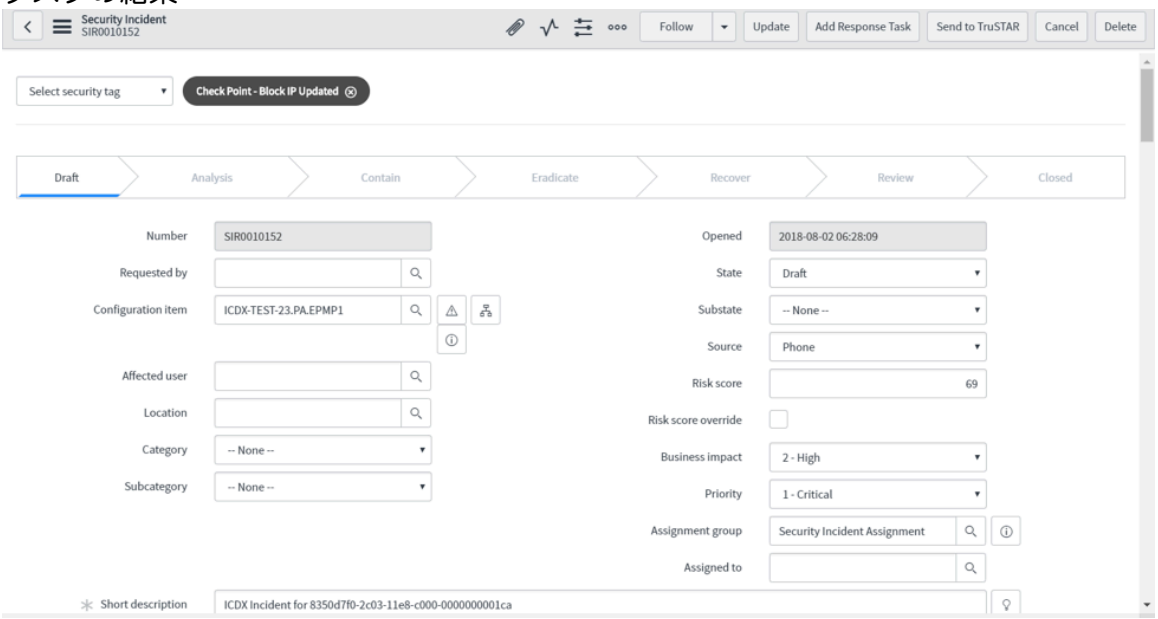


ブロックリストに観測事象が追加されるたびに、セキュリティインシデントレコードと観測事象レコードに、各観測事象タイプ (IP、URL、ドメイン) のセキュリティタグが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスクの結果



観測事象が既にブロックリストに追加されており、この観測事象のセキュリティインシデントにセキュリティタグが表示されている場合は、以降に作成されるセキュリティインシデントレコードにもブロックリストのセキュリティタグが自動的に表示されます。この重複は、観測事象がすでにブロックリストにあることを示しています。この観測事象を追加して再度ブロックする必要はありません。

観測事象のブロックが解除されると、セキュリティインシデントレコードまたは観測事象レコードにセキュリティタグが表示されなくなります。この場合、セキュリティタグがないことは、観測事象の有効期限を過ぎているか、観測事象がブロックリストから非アクティブ化されていることを示しています。

Check Point NGTP の統合のアンインストール

Now Platform インスタンスから Check Point NGTP 統合をアンインストールし、統合から残りをすべて削除する場合は、アプリケーションのアンインストールの手順について、ServiceNow ドキュメントサイトを参照してください。

必要なロール：admin

CrowdStrike Falcon Host 統合

CrowdStrike Falcon Host 統合により、セキュリティインシデント内の観測事象をウォッチリストにプッシュし、追加のアラートを生成できるようにします。この統合は、[CrowdStrike Falcon Host - ウォッチリストに公開 (CrowdStrike Falcon Host - Publish to Watchlist)] ワークフローの実装です。

詳細

セキュリティインシデントレスポンス の統合

セットアップ

CrowdStrike Falcon Host 統合を開始する

使用

観測事象のルックアップを実行する

開発

- ServiceNow セキュリティオペレーション 統合開発のガイドライン
- 統合を作成するためのヒント

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

- 開発者トレーニング
- 開発者ドキュメント
- アプリケーションとともにインストールされているコンポーネントの検索

トラブルシューティングとヘルプ

- 統合のトラブルシューティング
- Security Operations Community で質問や回答をする
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

CrowdStrike Falcon Host 統合を開始する

統合構成機能を使用すると、CrowdStrike Falcon Host 統合を含むサードパーティのセキュリティ統合をすばやくアクティブ化して設定できます。CrowdStrike Falcon Host 統合を使用する前に、ServiceNow Store からダウンロードし、ユーザー名とパスワードを追加する必要があります。

始める前に

- CrowdStrike Falcon Host 統合を以前のバージョンからアップグレードする場合は、既存の構成を削除して新しい構成を設定する必要があります。新しい統合は OAUTH2 認証をサポートしています。この更新では、**[API** クライアント **ID]** と **[API** クライアントシークレット] を入力して認証し、構成を完了する必要があります。
- CrowdStrike Falcon Host ポータルの **[API** スコープ **(API Scopes)]** で、**[IOC** (セキュリティ侵害のインジケーター) **(IoC (Indicators of Compromise))]** の [読み取り] および [書き込み] 設定を有効にします。

必要なロール：sn_si_admin

手順

1. から統合をダウンロードします ServiceNow Store.
2. インストールが完了したら、次に移動します: セキュリティオペレーション > 統合 > 統合設定. 利用可能なセキュリティ統合が一連のカードとして表示されます。
3. CrowdStrike Falcon Host カードで、[構成] をクリックします。
4. フォームのフィールドに入力して構成を完了します。

CrowdStrike Falcon Host 構成

フィールド	説明
名前	統合の名前 (例：demo-1)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
API クライアント **ID**	CrowdStrike Falcon Host ポータルのアカウントプロファイルの設定セクションから取得するクライアント ID。
API クライアントシークレット	CrowdStrike Falcon Host ポータルのアカウントプロファイルの設定セクションから取得するクライアント秘密キー。

5. **[Submit]** をクリックします。

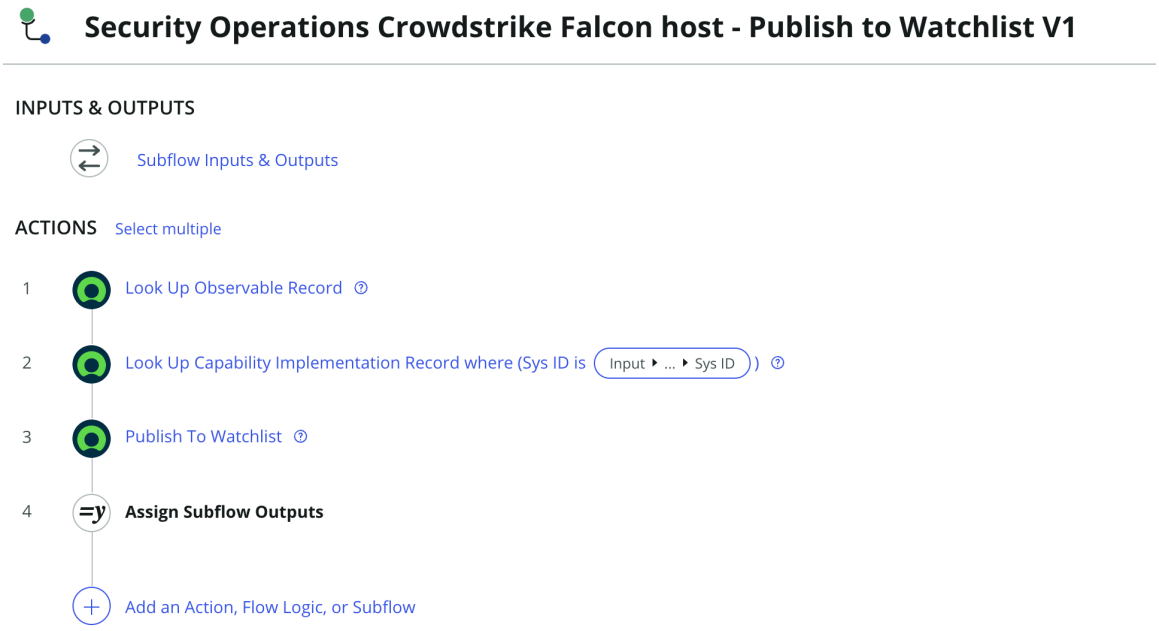
タスクの結果
構成後、セキュリティインシデントレスポンス のウォッチリストに観測事象を公開するために CrowdStrike Falcon Host 統合を選択できます。

Security Operations CrowdStrike Falcon Host - ウォッチリストに公開フロー

[Security Operations CrowdStrike Falcon Host - ウォッチリストに公開] フローデザイナーを使用して、アラートまたはイベントを生成するためのウォッチリストを指定します。アラートとイベントは、構成方法に基づいて CrowdStrike Falcon Host システムに表示されます。

ウォッチリストに公開フロー

このフローデザイナーは、セキュリティインシデントに関連付けられた 1 つ以上の観測事象を選択し、[ウォッチリストに公開] UI アクションを使用して観測事象をウォッチリストにプッシュすると、 Security Operations Integration - [ウォッチリストに公開] 機能 によってトリガーされます。その後、観測事象を使用して追加のアラートを生成できます。詳細については、「サードパーティのウォッチリストへの観測事象の公開」を参照してくださ



い。

CrowdStrike Falcon Insight for セキュリティオペレーション 統合

CrowdStrike Falcon Insight for セキュリティオペレーション 統合を使用すると、Now Platform セキュリティインシデントレスポンス 製品を使用して、エンドポイントに対してリアルタイムで修

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

復アクションを実行し、プロファイルを使用してホストに関する詳細情報を収集し、エンドポイントに対して特定のクエリまたはアクションを実行できます。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

CrowdStrike Falcon Insight for セキュリティオペレーション 統合は Now Platform と連携するため、インシデントのスコープに関する追加のインサイトを得ることができます。CrowdStrike Falcon Insight は関連するすべてのエンドポイントイベントアクティビティをキャプチャします。Now Platform を使用して調査と修復アクションに集中できます。

この統合の詳細

ドキュメント識別子	ドキュメントタイトル
ServiceNow 製品ドキュメント Web サイト	ServiceNow 製品ドキュメント Web サイト
CrowdStrike Falcon Insight for セキュリティオペレーション	CrowdStrike Falcon Insight 統合を開始する

CrowdStrike Falcon Insight 統合を開始する

CrowdStrike Falcon Insight をアクティブ化して、Now Platform インスタンスおよび セキュリティインシデントレスポンス 製品と連動するように設定できます。

始める前に

必要なロール：admin

セキュリティオペレーション 統合用に CrowdStrike Falcon Insight を使用する前に、ServiceNow Store からダウンロードする必要があります。

このタスクについて

チェックリスト

セットアップタスク	説明
必要な Now Platform および セキュリティインシデントレスポンス ロールをアサインして確認します。	予想される結果の構成と検証には、次のロールが必要です。 • admin ロールは、ServiceNow Store から統合をインストールし、sn_si.admin ロールをアサインします。 • sn_si.admin ロールは、統合を構成し、プロファイルを作成してアクティブ化し、sn_si.analyst ロールをアサインします。 • sn_si.analyst ロールは、セキュリティインシデントに対応し、プロファイルを手動で起動

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト (続く)

セットアップタスク	説明
	し、ホストの隔離や、承認されたグループのホスト隔離の削除などのアクションの要求を送信できます。
この統合を構成する前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	ServiceNow 統合ハブ Enterprise Pack Installer [com.glide.hub.integrations.enterprise] プラグインが必要です。このプラグインは、IntegrationHub アクションとフローの実行を有効にします。 セキュリティインシデントレスポンス プラグイン (com.snc.security_incident) が必要です。このプラグインは、セキュリティインシデントレスポンス 製品をサポートするために必要なすべての依存関係を自動的にインストールします。統合に必要な他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。 次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化する必要があります。 **1.** セキュリティインシデントレスポンス 依存関係 (com.snc.si_dep) **2.** Security Integration Framework **3.** Security Support Common **4.** セキュリティサポートオーケストレーション **5.** 脅威インテリジェンス Support Common **6.** トラステッドセキュリティサークル **7.** セキュリティオペレーション セットアップアシスタント **8.** セキュリティインシデントレスポンス
承認グループを設定します。	ホストマシンの隔離、ネットワークの復元、サイティング検索の開始に使用できるオプションの承認機能があります。 このオプションを有効にするには、ホストマシンを隔離してネットワークに復元する前、またはサイティング検索を実行するとき

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト (続く)

セットアップタスク	説明
	に、sn_si.admin ロールからの事前承認が必要です。これらのアクションをより詳細に制御する必要がある場合は、プロファイルの構成で [承認が必要] オプションを有効にします。承認権限は、sn_si.admin ロールを持つユーザーに割り当てられます。承認権限を承認グループに再割り当てすることもできます。
CrowdStrike Falcon プラットフォームのロールをアサインして確認します。	統合構成用の CrowdStrike Falcon プラットフォームには、次のロールが必要です。 • API クライアントまたはキーを表示、作成、または変更するには、Falcon アドミンロールが必要です。 • カスタムスクリプトを作成して実行するには、リアルタイムレスポンダー - アドミンロールが必要です。 • カスタムスクリプトを作成して実行するには、リアルタイムレスポンダー - アクティブレスポンダーロールが必要です。
CrowdStrike Falcon プラットフォームでカスタムスクリプトのロールと権限が有効になっていることを確認します。	この統合では、いくつかの拡張機能に CrowdStrike のカスタムスクリプトが使用されます。 • リアルタイムレスポンダー - アドミンおよびリアルタイムレスポンダー - アクティブレスポンダーのロールが利用可能であることを確認します。 • CrowdStrike Falcon UI の [構成] > [応答ポリシー (Response Policies)] で [デフォルト **(Windows)** ポリシー **(Default(Windows) policy)]** オプションが有効になっていることを確認します。 • CrowdStrike Falcon UI で、[リアルタイム機能 (Real Time Functionality)] の [リアルタイム応答 **(Real Time Response)]** と [カスタムスクリプト **(Custom Scripts)]** が有効になっていることを確認します。
CrowdStrike Falcon プラットフォームで、API クライアントとキーを生成します。	Now Platform 統合構成で使用する CrowdStrike Falcon プラットフォームで CrowdStrike API クライアントまたはキーを作成します。

CrowdStrike API クライアントの作成とキーの生成

CrowdStrike API クライアントを作成し、CrowdStrike Falcon Insight 統合を構成するために使用するクライアント ID とキーを生成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：CrowdStrike Falcon アドミン

手順

1. CrowdStrike Falcon プラットフォームで、**[API** クライアントとキー **(API Clients and Keys)]** に移動します。
2. [OAuth2 API クライアント (OAuth2 API Clients)] テーブルで、[新しい **API** クライアントを追加 **(Add new API client)]** をクリックします。
3. 次の詳細を入力して API クライアントを定義します。

フィールド	説明
クライアント名	クライアント名を入力します。このフィールドは必須です。
説明	クライアント名の説明を入力します。
API スコープ (API Scopes)	スコープの定義が必要です。 **重要:** API アカウントを有効にし、API アカウントに対して次のスコープが有効になっていることを確認します。 ○ ホスト API の読み取りおよび書き込みスコープの有効化 ○ インジケーター API の読み取りスコープの有効化

4. [追加] をクリックして API クライアントを保存し、クライアント ID と秘密キーを生成します。

CrowdStrike Falcon Insight のインストールと構成

Now Platform インスタンスで ServiceNow Store から CrowdStrike Falcon Insight for セキュリティオペレーション アプリケーションをインストールして設定します。

始める前に
必要なロール：admin

注:
機能は 1 つのプロファイルにのみ関連付けることができます。1 つの機能を複数のプロファイルに関連付けることはできません。CrowdStrike サーバーを構成する場合、CrowdStrike サーバーを共有する複数のプロファイルで CrowdStrike 機能を再利用することはできません。プロファイルには同じ CrowdStrike 機能を持たせることができます。各プロファイルは独自の CrowdStrike サーバーを使用する必要があります。

手順

1. ServiceNow Store から CrowdStrike Falcon Insight for Security Operations Integrations をダウンロードしてインストールします。
2. 次のように移動する。 セキュリティオペレーション > 統合 > 統合設定.
3. CrowdStrike Falcon Insight for セキュリティオペレーション 統合タイルを検索し、[構成] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. フォームのフィールドに入力して構成を完了します。

CrowdStrike Falcon Insight 構成

フィールド	説明
名前	統合の名前 (例：demo-1)。
CrowdStrike Falcon Insight API URL	CrowdStrike API をホストするベース URL。HTTPS プロトコルの URL を入力します。例：https://api.crowdstrike.com。
クライアント ID	CrowdStrike Falcon Insight ポータルのアカウントプロファイルの設定セクションから取得するクライアント ID。
クライアントシークレット	CrowdStrike Falcon Insight ポータルのアカウントプロファイルの設定セクションから取得するクライアント秘密キー。

5. [Submit] をクリックします。

タスクの結果
統合の検証と送信が正常に完了すると、[セキュリティ統合] ページにタイルとして保存されます。アプリケーションナビゲーターで CrowdStrike Falcon Insight モジュールを表示できます。

承認グループの作成

ホストマシンの隔離、ネットワークへの復元、およびサイティング検索の開始の要求を承認できる CrowdStrike Falcon Insight for セキュリティオペレーション 統合の承認グループを作成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
インスタンスの承認グループを使用できる場合を除き、グループに承認権限を再アサインできません。

> **注:**
> プロファイル構成の承認オプションは、[ホストを隔離] および [ホスト隔離削除] 機能に対してのみ表示されます。

必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > ユーザー管理 **(User Administration)** > グループ.
2. [グループ] リストで、[新規] をクリックします。
3. フォームのフィールドに入力します。

[承認グループ] フォーム

フィールド	説明
名前	承認要求を送信するときに表示されるグループの名前。
グループ メール	グループのメール配布リストまたは連絡先メールアドレス (グループマネージャーなど)
マネージャー	グループマネージャーの名前。検索アイコンをクリックしてリストを表示します。
親	親グループの名前 (親に関連付けられている場合)。
タイプ	グループのカテゴリ。
ベンダー	組織のベンダー管理プロセスでユーザーに割り当てる vendor_manager ロール。
説明	グループに関する補足情報。

4. **[Submit]** をクリックします。
   新しいグループが [グループ] リストに表示されます。

   このプロファイルの構成で [承認が必要] オプションが有効になっている場合、このグループは要求を処理できます。

   承認グループの各メンバーは、sn_si.analyst ロールを持つユーザーが送信した要求を監視および処理するには、Now Platform で [自分の承認] タブに移動します。

次のタスク
次のステップでは、ServiceNow Store から CrowdStrike Falcon Insight アプリケーションをインストールして構成します。

CrowdStrike Falcon Insight 統合の機能プロファイルの作成

プロファイルを作成し、そのプロファイルで実行する CrowdStrike Falcon Insight 機能を選択します。

始める前に
必要なロール：sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタスクについて
CrowdStrike Falcon Insight 機能を追加する前に、プロファイルを作成する理由を検討してください。次の表は、プロファイルで特定のクエリまたはアクションを実行する場合にプロファイルに追加する必要がある機能を示しています。

システムの詳細に関するクエリの実行、ログインしているユーザーのリスト、実行中のサービスのフェッチ、実行中のプロセスのフェッチ、ネットワーク統計情報のフェッチ、ホストの隔離、隔離されたホストの削除を行う単一のプロファイルを作成できます。または、それぞれが単一の機能を持つプロファイルを複数作成することもできます。

注:
プロファイルの作成中に、ホストの隔離、隔離の削除、およびファイルの取得の機能を他の機能と結合することはできません。

プロファイルタイプと必要な **CrowdStrike Falcon Insight** 機能

プロファイルの目的	**CrowdStrike** 機能
ホストの詳細とログインユーザーの収集	• ホストの詳細を取得 • ログオンユーザーを取得
ホストに対して実行中のネットワーク統計、プロセス、およびサービスをフェッチ	• ネットワーク統計の取得 • 実行中のプロセスの取得 • 実行中のサービスを取得
ホストを隔離	ホストの隔離
ホストの隔離を削除	隔離を削除
ホストエンドポイントからファイルを取得	ファイルを取得

自動翻訳

手順

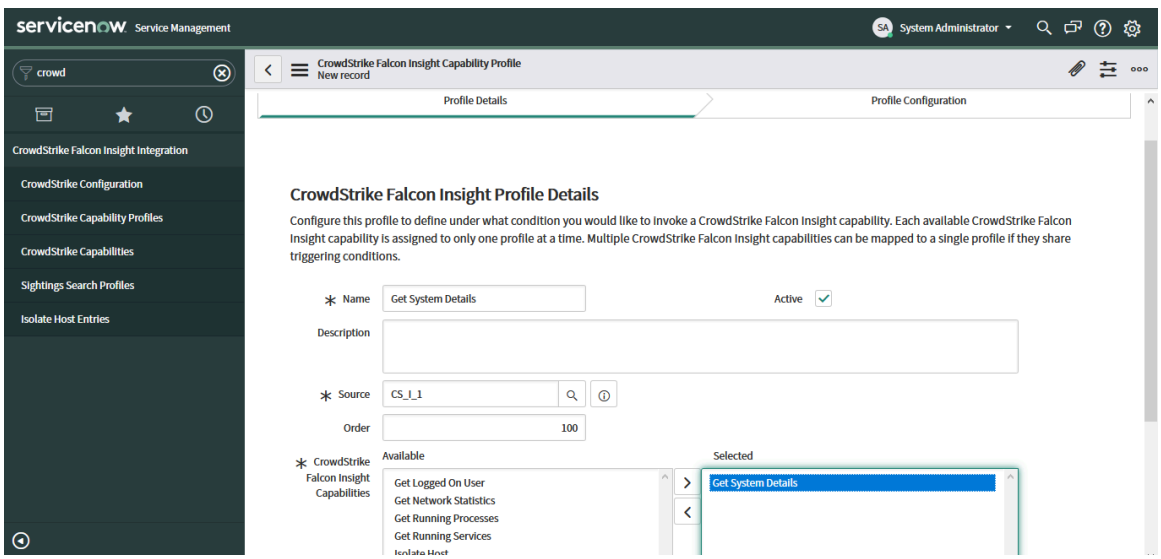
1. 次のように移動する。 **All** (すべて) > **CrowdStrike Falcon Insight** 統合 > **CrowdStrike** 機能プロファイル.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

フィールド	説明
名前	新しい機能プロファイルの名前。 この名前は、プロファイルタイプを識別するのに役立ち、このプロファイルに関連付けられているセキュリティタグのデフォルト名でもあります。
アクティブ	プロファイルがアクティブかどうかを示します。 プロファイルがアクティブになると、構成で指定したフィルター条件に一致するセキュリティ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	インシデントが作成されたときに、自動的にトリガーされます。
説明	機能プロファイルの固有の説明。
ソース	サーバーの名前。リストからは、以前に構成されたサーバーのみを表示できます。
順序	フロー優先度。このフィールドの値は、2 つ以上のプロファイルがトリガー条件を共有する場合にフローが実行される順序を示します。 番号が最も小さいフローの優先度が最も高くなります。操作の順序を設定するには、値を入力します。例：100、200、300、400。 デフォルト：100
CrowdStrike Falcon Insight 機能	CrowdStrike Falcon Insight プロファイルの機能。 このプロファイルの機能を [利用可能 **(Available)]** 列から選択し、それを [選択済み] 列に移動します。

次の例は、[システムの詳細の取得] 機能を備えたプロファイルの完成したフォームです。



4. [次へ] をクリックします。

次のタスク
これで、プロファイルを構成できます。プロファイルを構成する前に、プロファイルとトリガー条件の構成の概念を確認してください。

CrowdStrike Falcon Insight統合のためのプロファイルとセキュリティインシデントの構成

設定した条件でのみプロファイルがトリガーされるように、プロファイル設定を構成します。

始める前に
必要なロール：sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタスクについて
プロファイルに対して選択した CrowdStrike Falcon Insight 機能を自動的にトリガーする条件を定義します。[構成アイテム] (CI) フィールドの代替入力フィールドを選択することもできます。この代替フィールドでは、トリガーイベントに関連するセキュリティインシデントのみが自動的にプロファイルをトリガーするように、フィルタリング条件を設定できます。

注:
プロファイルの詳細を入力した後にのみ、[プロファイル設定] ページに移動します。詳細については、「CrowdStrike Falcon Insight 統合の機能プロファイルの作成」を参照してください。

手順

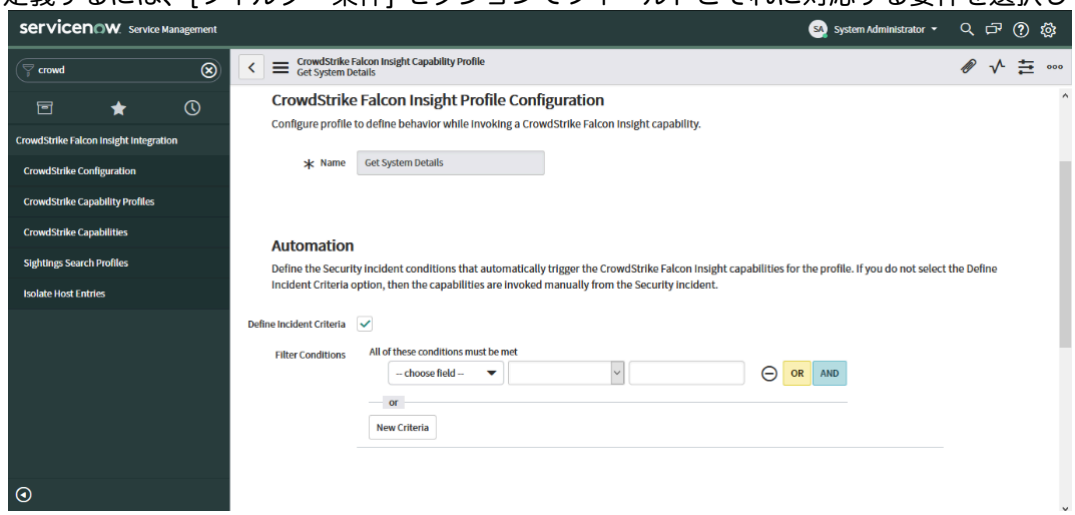
1. [プロファイル設定] ページで、次のセクションを確認して構成します。

   [インシデント基準の定義] ([自動化] 内)

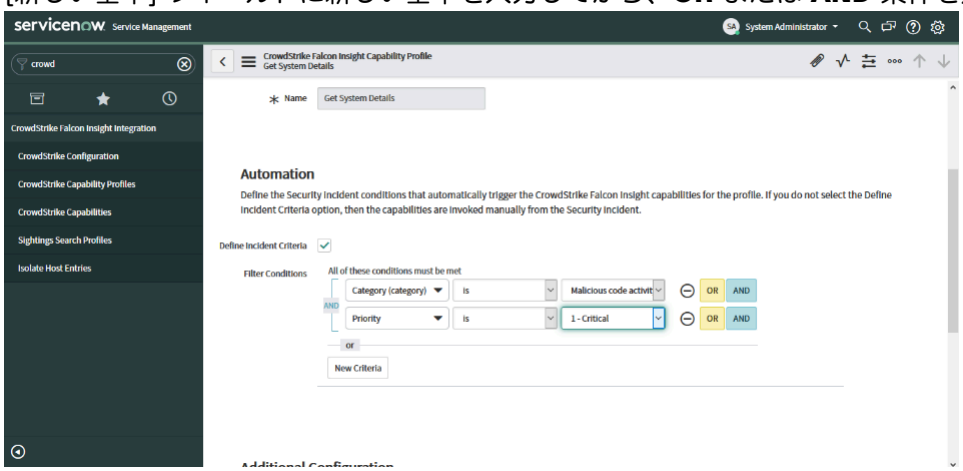
   プロファイルに対して CrowdStrike Falcon Insight 機能を自動的にトリガーするセキュリティインシデント条件を定義します。[インシデント基準の定義] オプションを選択しない場合、機能はセキュリティインシデントから手動で呼び出されます。

   a. [インシデント基準の定義] オプションを選択します。

   b. 条件を定義するには、[フィルター条件] セクションでフィールドとそれに対応する要件を選択します。



   c. [新しい基準] フィールドに新しい基準を入力してから、**OR** または **AND** 条件を定義します。



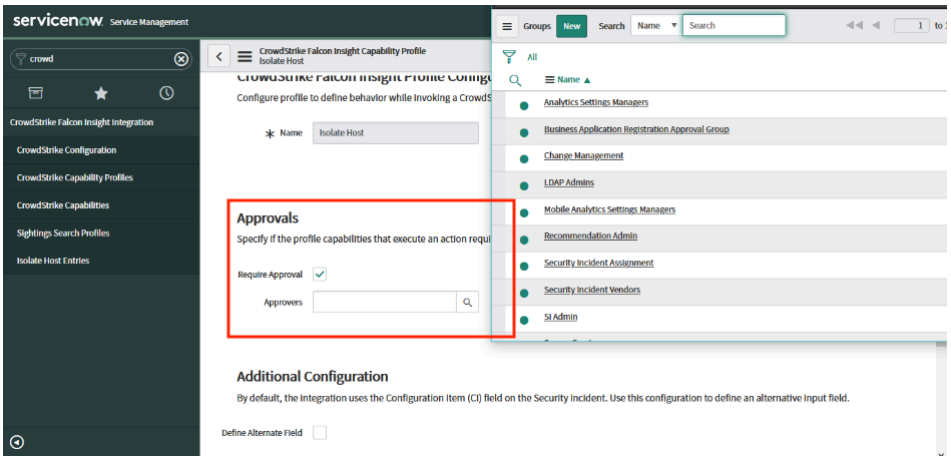
   承認

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CrowdStrike Falcon Insight 機能を使用するときの制御を強化するには、[承認が必要] オプションを選択します。プロファイル構成の承認オプションは、[ホストを隔離] および [ホスト隔離削除] 機能に対してのみ表示されます。

注:
承認権限は、sn_si.admin ロールを持つユーザーに割り当てられます。承認権限を承認グループに再割り当てすることもできます。詳細については、「set up an approval group (承認グループの設定)」を参照してください。



追加設定

セキュリティインシデントの代替フィールドを選択して、資産のスキャン中に見つかった一致する CI データを表示します。デフォルトでは、統合はセキュリティインシデントの構成アイテム (CI) フィールドを使用します。

a. [代替フィールドを定義 **(Define Alternative Field)]** オプションを選択します。

b. [代替 **CI** トリガーフィールド] で、入力フィールドを選択します。

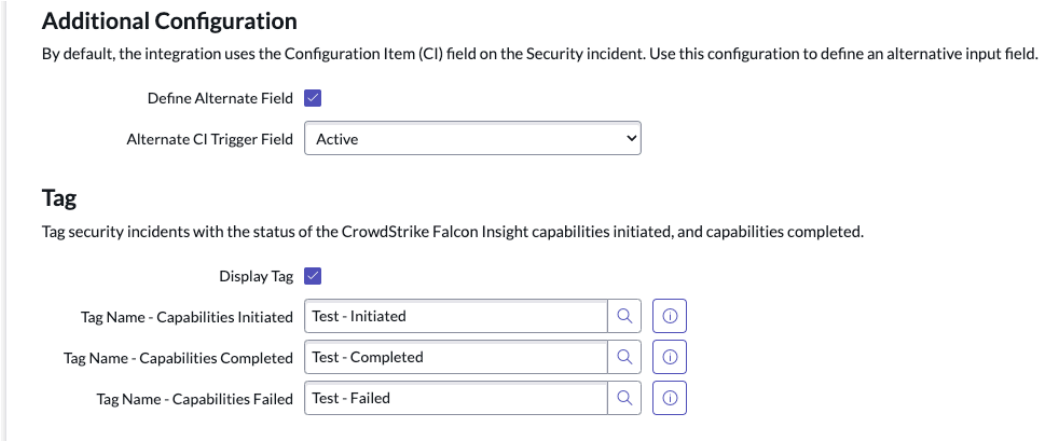
注:
詳細については、「Understand how trigger conditions work with a configuration item for a profile (プロファイルの構成アイテムに対するトリガー条件の作用の理解)」を参照してください。

タグ

「CrowdStrike Falcon Insight 機能 - 開始済み」、「機能 - 完了」、および「機能 - 失敗」タグでセキュリティインシデントにタグ付けするには、[タグを表示] オプションを選択します。デフォルトでは、このオプションはすべてのプロファイルで無効になっています。

注:
以下のタグは、ベースシステムに付属しています。必要に応じて独自のタグを作成できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



2. [完了] をクリックします。

プロファイルの構成アイテムに対するトリガー条件の作用

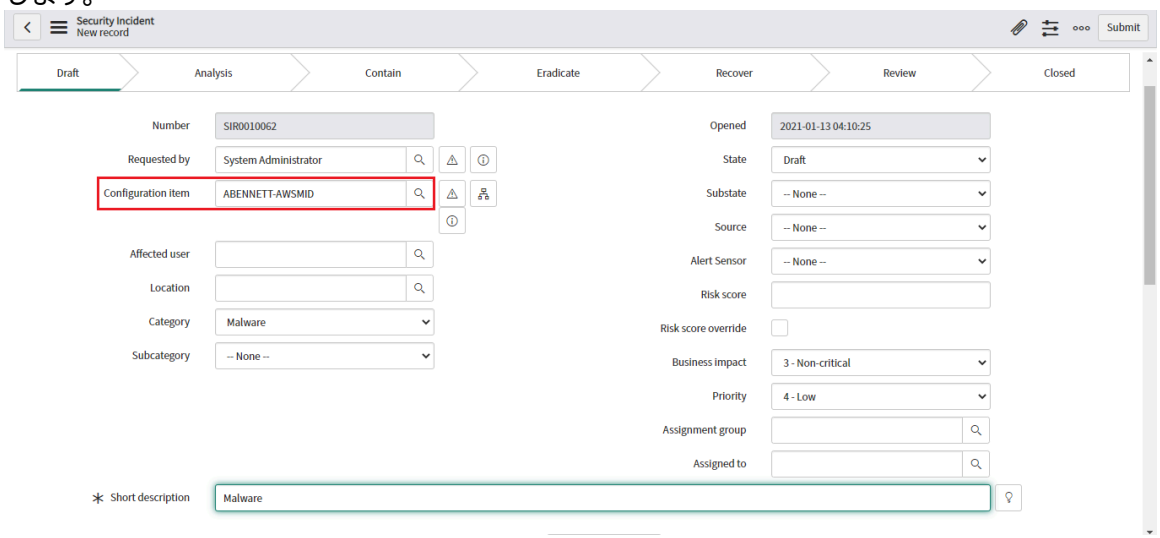
一連の特定の条件が満たされた場合にのみプロファイルが実行されるようにプロファイル設定を構成したり、セキュリティインシデントの特定のフィールド値を検索するようにプロファイルを設定したりできます。

プロファイルを作成し、プロファイルを実行する CrowdStrike Falcon Insight 機能を選択したら、デフォルトのフィールド値が Now Platform セキュリティインシデントに一致したときにプロファイルが自動的に実行されるように、トリガー条件を設定できます。

デフォルトでは、統合はセキュリティインシデントの [構成アイテム **(CI)**] フィールドを使用します。このフィールドは、資産 ID を Now Platform データベースに格納されている情報と照合するために使用されます。SIR セキュリティインシデントがセキュリティイベントによって作成され、プロファイルがアクティブ化されたときに、ホスト名または IP アドレスの値が一致するかどうか、資産がスキャンされます。

一致する値がデータベース内で見つかると、そのデータが CrowdStrike Falcon Insight コンソールから収集され、Now Platform インスタンスにプルされて、セキュリティインシデントの関連リストに表示されます。

次に、SIR セキュリティインシデントのホスト名が入力された [構成アイテム] フィールドの例を示します。

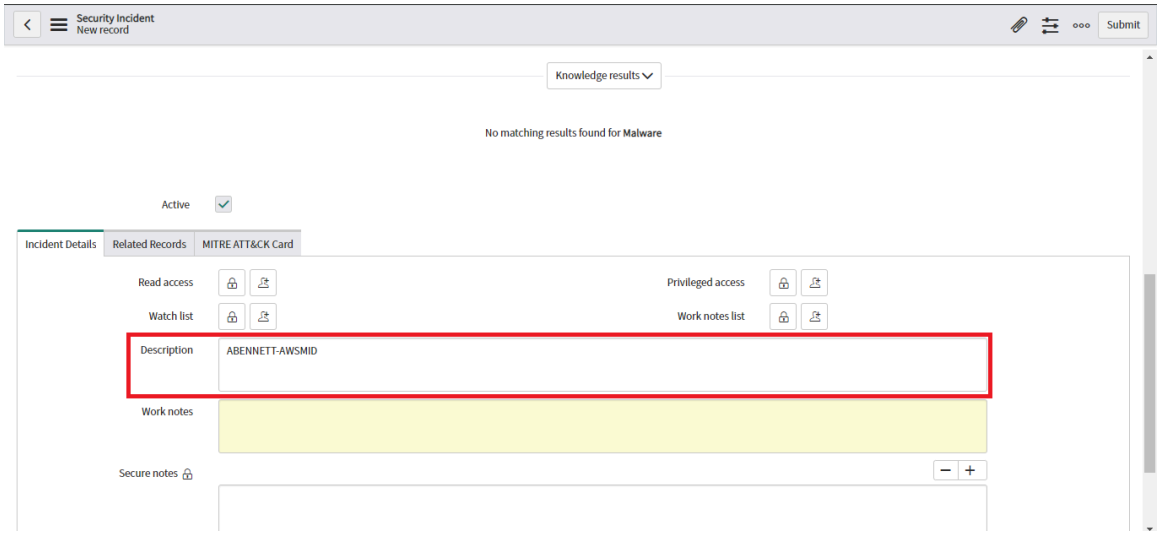


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[構成アイテム **(CI)**] フィールドにデータベースと一致するホスト名または IP アドレスが入力されていない場合は、セキュリティインシデントのその他のフィールドを選択して、資産のスキャン中に見つかった一致する CI データを表示できます。

プロファイルセットアップの構成では、エンドポイント識別用の代替 **CI** トリガーフィールドを選択して、CrowdStrike Falcon Insight ルックアップからの CI データが関連するセキュリティインシデントに入力されるようにすることができます。作成したカスタムフィールドを含む、セキュリティインシデントの任意のフィールドを代替 CI トリガーフィールドとして選択できます。インシデントの作成時に関連するセキュリティインシデントで CI フィールドが入力されていない場合は、この代替 CI フィールドを選択して、プロファイルがトリガーされるようにします。

次に、SIR セキュリティインシデントのホスト名が入力された代替
フィールドの例を示します。代替フィールドは [説明] フィールドです。



CrowdStrike Falcon Insight プロファイルのトリガー条件の確認

プロファイルをテストし、構成したトリガー条件フィルターが想定どおりに機能することを確認します。

始める前に

必要なロール：sn_si.admin

このタスクについて

指定した構成済みトリガー条件に基づいてプロファイルをアクティブ化し、Now Platform セキュリティインシデントのクエリ結果を表示できるようにします。

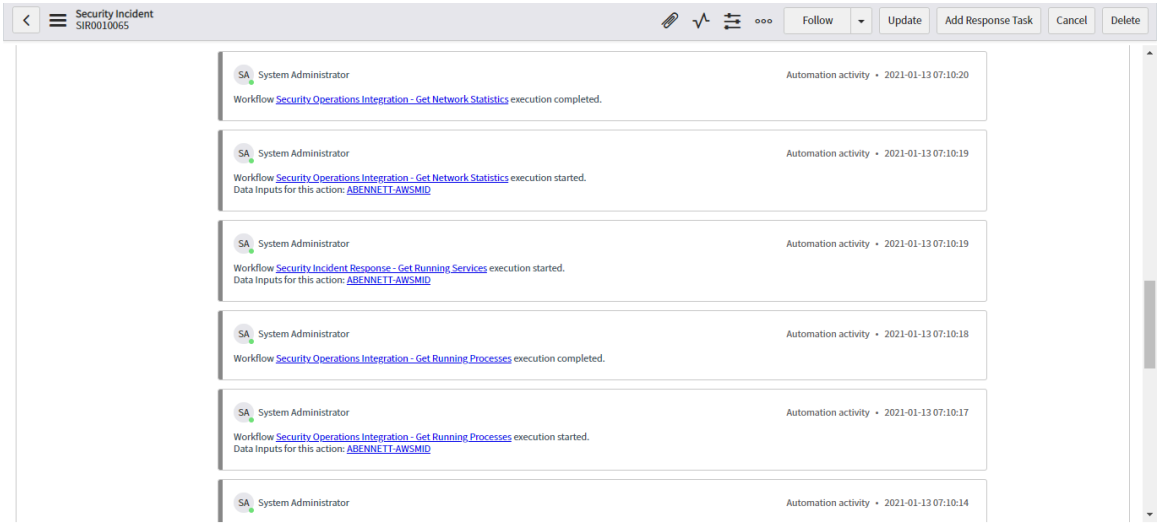
手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. [新規] を選択して、セキュリティインシデントを作成します。
3. セキュリティインシデントを作成するには、必要な情報を入力し、[保存] をクリックします。

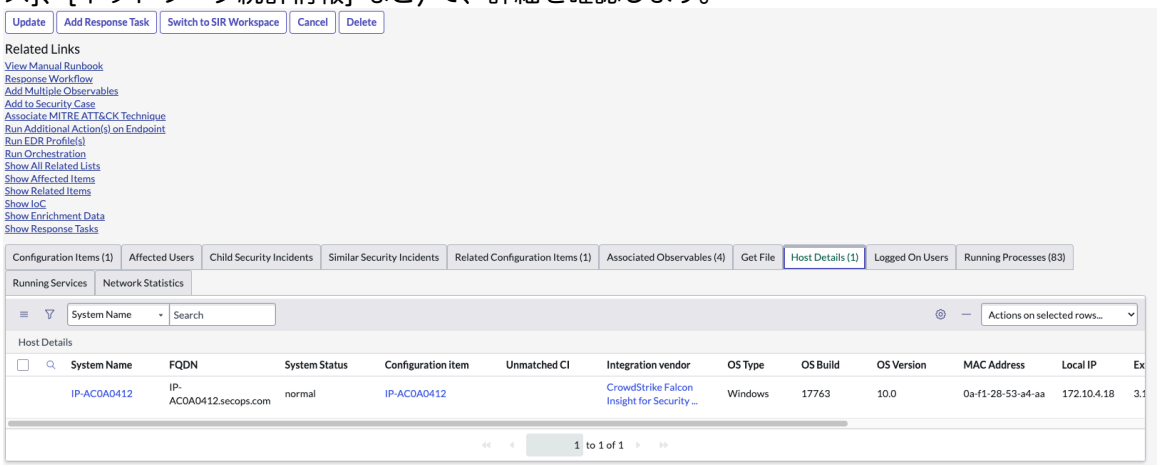
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [作業メモとアクティビティ] セクションを表示し、プロファイル開始済みタグとプロファイル完了済みタグを表示できます。



5. [CrowdStrike Falcon Insight の詳細 (CrowdStrike Falcon Insight Details)] の関連リスト ([ファイルを取得]、[ホストの詳細]、[ログオンユーザー]、[実行中のプロセス]、[実行中のサービス]、[ネットワーク統計情報] など) で、詳細を確認します。



セキュリティインシデントからの **CrowdStrike Falcon Insight** プロファイルの手動トリガー

セキュリティインシデントを確認した後は、プロファイルを手動でトリガーします。

始める前に

必要なロール：admin

このタスクについて

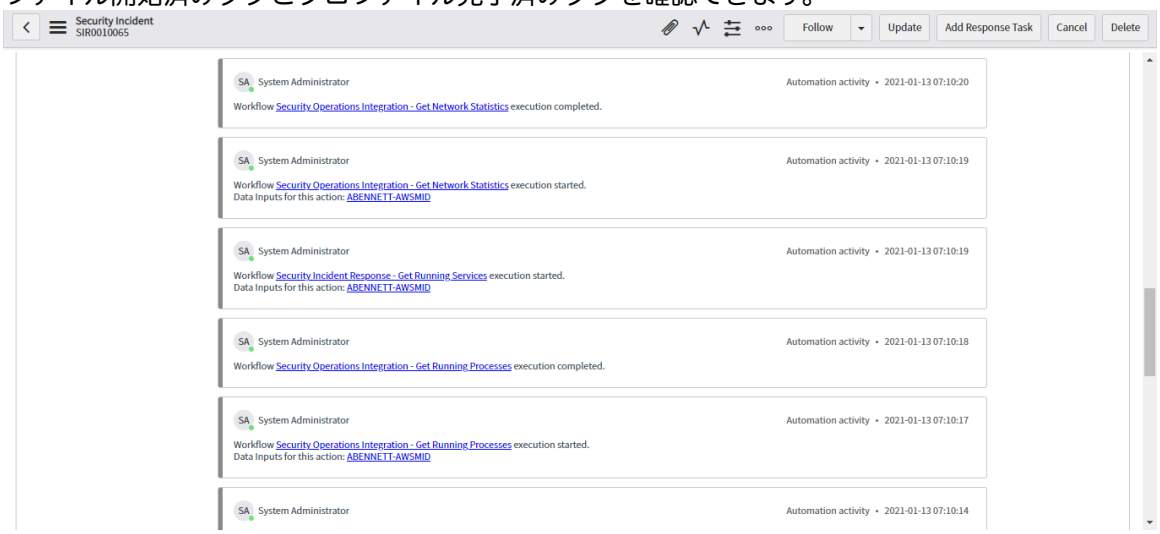
構成されたトリガー条件に基づいてプロファイルをアクティブ化すると、Now Platform セキュリティインシデントのクエリ結果を表示できます。CrowdStrike Falcon Insight により、プロファイルを使用せずに構成アイテム (CI) に対して個々の機能を実行することもできます。

手順

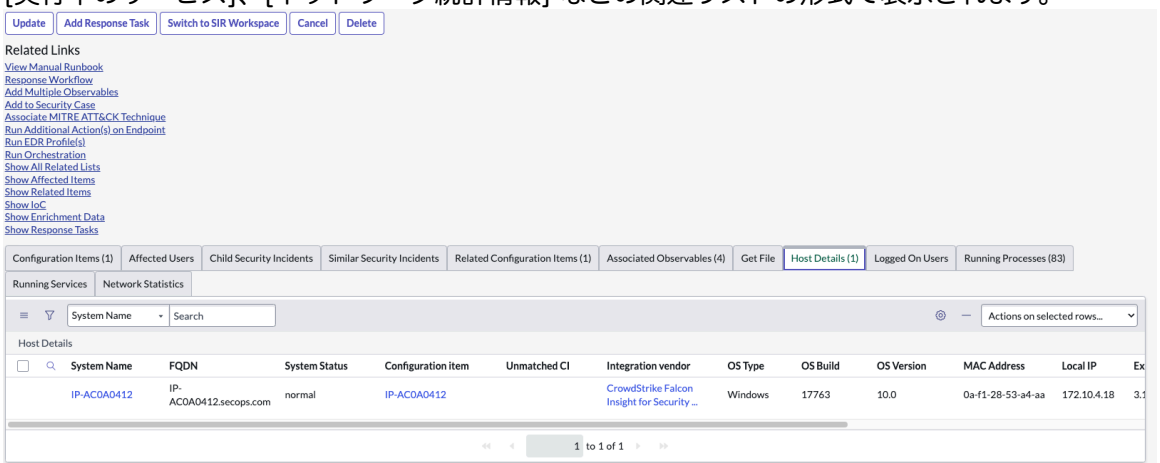
1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. CrowdStrike Falcon Insight 情報で確認するセキュリティインシデントを選択します。
3. 関連リストのセクションで、**[EDR** プロファイルを実行] をクリックします。
4. 利用可能なプロファイルのリストを参照してプロファイルを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. プロファイルのすべての関連 CI に対してこのプロファイルを実行するには、[関連 **CI** を含める **(Include Related CI)]** を選択します。
   たとえば、セキュリティインシデントに 5 つの CI が関連付けられている場合、選択したプロファイルは 5 つの CI すべてに対して実行されます。
6. **[Submit]** をクリックします。
   選択したプロファイルは手動でトリガーされます。[作業メモとアクティビティ] セクションを表示し、[作業メモ] セクションのプロファイル開始済みタグとプロファイル完了済みタグを確認できます。



7. 結果は、[ファイルを取得]、[ホストの詳細]、[ログオンユーザー]、[実行中のプロセス]、[実行中のサービス]、[ネットワーク統計情報] などの関連リストの形式で表示されます。



8. CI に対して個々の機能を実行するには、次の手順を実行します。

   a. [構成アイテム] 関連リストで、必要な CI を選択します。

   b. [選択した行のアクション...] ドロップダウンリストをクリックし、選択した CI に対して実行する必要な機能を選択します。
   たとえば [ホストを隔離] などです。

   c. 検索オプションを使用して CI に必要な機能実装を検索し、**[CrowdStrike Falcon Insight** ホストを隔離 **(CrowdStrike Falcon Insight Isolate Host)]** を選択します。

   d. [ホストを隔離] をクリックして、選択した CI に対して実行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

サイティング検索のプロファイルの作成と構成

CrowdStrike Falcon Insight のサイティング検索を使用して、組織のネットワーク全体で感染したマシンを特定し、セキュリティインシデント応答ケースに対処します。

始める前に

必要なロール：sn_si.analyst

このタスクについて

個々のまたは複数の観測事象を選択し、CrowdStrike Falcon Insight で手動サイティング検索を実行することで、脅威のまん延を時系列で見極めることができます。

手順

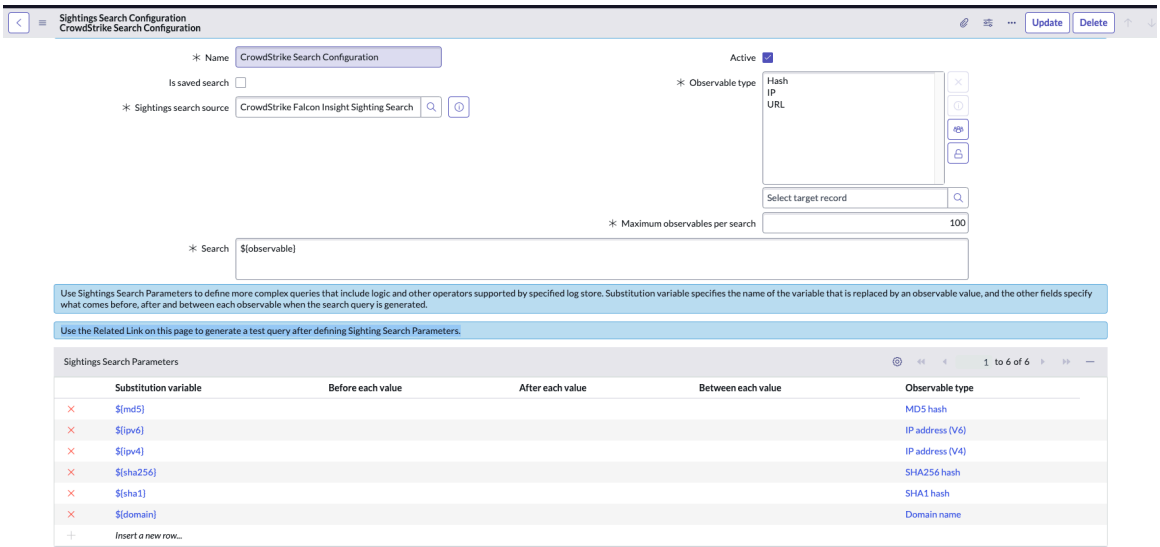
1. 次のように移動する。 **All** (すべて) > **CrowdStrike Falcon Insight** 統合 > サイティング検索プロファイル.
2. [**New**] をクリックします。
3. このプロファイルを構成して、特定の CrowdStrike Falcon Insight 検索機能を検索するサーバーを決定します。
4. フォームの各フィールドに入力します。

フィールド	説明
名前	サイティング検索プロファイルの名前。
保存された検索	このオプションを選択すると、保存された検索構成が作成されます。
サイティング検索ソース	サイティング検索のソース。ソースとして **[CrowdStrike Falcon Insight** サイティング検索] を選択します。
アクティブ	追加アクションがアクティブかどうかを示すオプション。
観測可能タイプ	CrowdStrike Falcon Insight 統合では、次の観測可能タイプがサポートされています。 ○ ハッシュ ○ IP ○ URL サイティング検索は、次の観測可能タイプでサポートされています。 ○ ドメイン名 ○ IP アドレス (V4) ○ IP アドレス (V6) ○ MD5 ハッシュ ○ SHA1 ハッシュ ○ SHA256 ハッシュ
検索あたりの最大観測事象の数	検索クエリから表示できる観測事象の最大数。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
検索	デフォルトの検索文字列は $(observable) ですが、CrowdStrike Falcon Insight 統合でサポートされているパラメーターを指定して、独自の検索クエリを定義できます。
サイティング検索パラメーター	指定されたログストアでサポートされているロジックやその他の演算子を含むより複雑なクエリを定義するパラメーター サイティング検索パラメーターを定義した後、このページの下部にある [関連リンク] を使用してテストクエリを生成できます。



5. **[Submit]** をクリックします。
   構成が完了し、Now Platform セキュリティインシデントからサイティング検索を呼び出すことができます。
6. 構成を確認し、サイティング検索を実行するには、次の手順を実行します。

   a. セキュリティインシデントを開き、セキュリティインシデントの下部までスクロールして、[すべての関連リストを表示] をクリックします。

   b. [実行中のプロセス] 関連リストから 1 つ以上の構成アイテム (CI) を選択した場合。

   > **注:**
   > [実行中のプロセス] 関連リストから CI のサイティング検索を実行する場合。プロセスハッシュのサイティング検索のみになります。

   c. [選択した行のアクション...] ドロップダウンリストから、**[CrowdStrike** サイティング検索を実行 **(Run CrowdStrike Sightings Search)]** を選択します。

   d. 検索オプションを使用して、必要なサイティング検索プロファイルを検索します。

   e. 必要なサイティング検索プロファイルを選択し、[送信] をクリックします。

自動翻訳

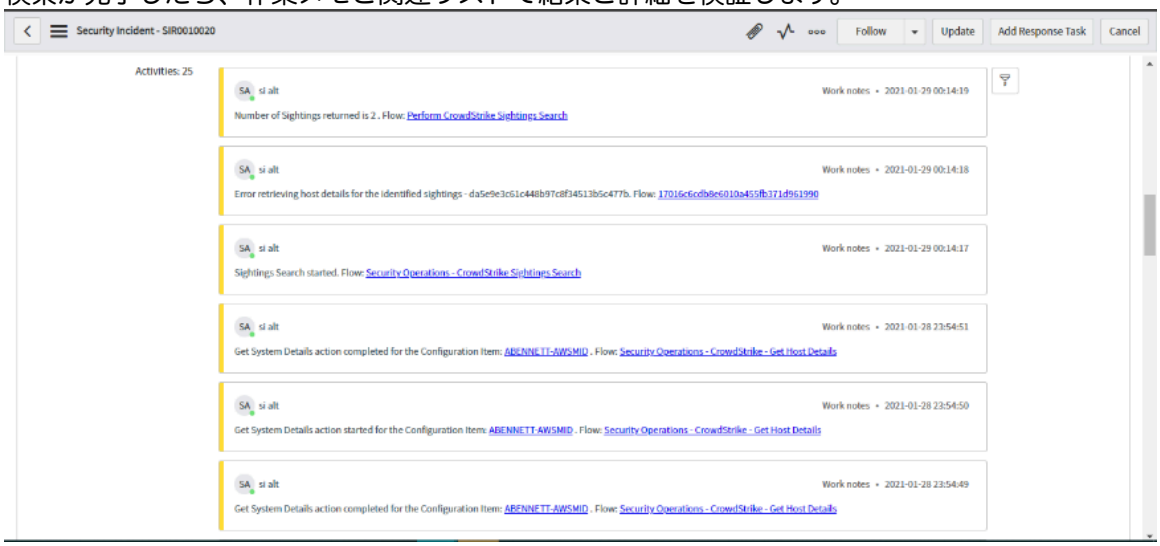
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

f. [関連する観測事象 **(Associated Observables)]** 関連リストから 1 つ以上の観測事象を選択した場合。

g. [選択した行のアクション...] ドロップダウンリストから、[サイティング検索を実行] を選択します。

h. 期間ポップアップで、任意のランダム値を選択して [検索] をクリックします。

i. 検索が完了したら、作業メモと関連リストで結果と詳細を検証します。



j. [サイティング] タブを選択して、サイティングの詳細を表示します。

k. CI の横にある [プレビュー] アイコンをクリックして、CrowdStrike サイティングの詳細に関する追加情報を表示します。

l. [サイティング検索の詳細] タブをクリックしてサイティング検索の詳細を確認し、[サイティング検索結果] タブをクリックして検索結果を確認します。

CrowdStrike Falcon Insight での追加アクションの構成とトリガー

CrowdStrike Falcon Insight 統合では、正規表現 (regex) などの追加アクションの実行がサポートされています。CrowdStrike Falcon Insight 統合には、ベースシステム向けの 40 の追加アクションが用意されています。

始める前に

必要なロール：sn_si.analyst

手順

1. 次のように移動する。 **All** (すべて) > **CrowdStrike Falcon Insight** 統合 > **CrowdStrike** の追加アクション.
2. [新規] をクリックして独自の追加アクションを作成するか、ベースシステムに付属する既存のアクションを選択します。
   たとえば、新しい追加アクションを作成するとします。
3. フォームの各フィールドに入力します。

自動翻訳

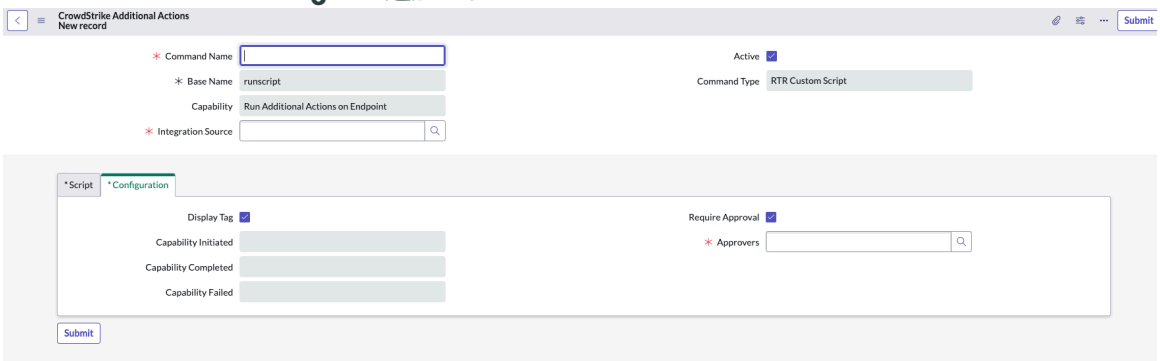
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
コマンド名	追加アクションのコマンド名。たとえば reg set です。
ベース名	追加アクションのベース名。このフィールドはデフォルトで設定されています。たとえば reg です。
機能	追加アクションの機能名。このフィールドはデフォルトで設定されています。たとえば、[エンドポイントで他のアクションを実行 (Run Additional Actions on Endpoint)] です。
統合ソース	追加アクションのソース。たとえば、CrowdStrike Falcon Insight 統合です。
アクティブ	追加アクションがアクティブかどうかを示すオプション。
コマンドタイプ	追加アクションのコマンドタイプ。このフィールドはデフォルトで設定されています。たとえば、[RTR カスタムスクリプト] です。
スクリプト	○ **OS** タイプ：スクリプトの OS タイプを選択するオプション。次のいずれかを選択します。 ▪ **Windows** ▪ **MAC OS X** ▪ **Linux** ▪ なし ○ スクリプト：[なし (None)] オプションを除く次のいずれかの OS を選択した場合に、スクリプトを入力するオプション。
構成	○ タグを表示：構成のタグを表示するオプション。次のフィールドのタグを選択できます。 ▪ 機能 - 開始済み。たとえば、「reg set - 開始済み」です。 ▪ 機能 - 完了。たとえば、「reg set - 完了」です。 ▪ 機能 - 失敗。たとえば、「reg set - 失敗」です。 ○ 承認が必要：構成を承認する必要がある承認者またはグループを選択するオプション。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

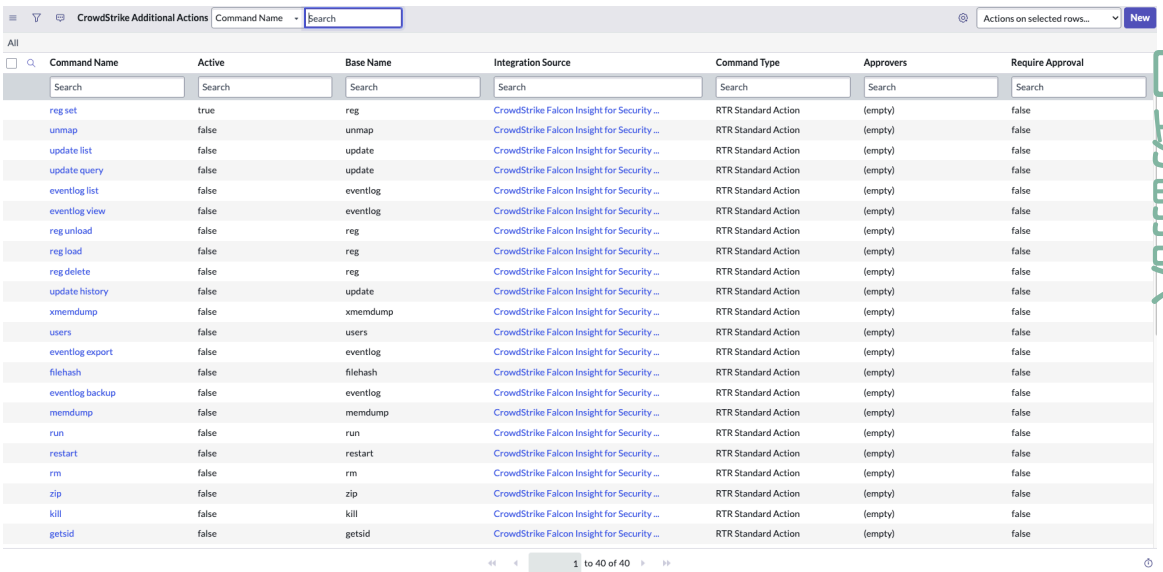
CrowdStrike Falcon Insight の追加アクション



4. **[Submit]** をクリックします。
5. 次の既存の追加アクションから選択することもできます。
   ベースシステムに付属する 40 個の追加アクション。これらのアクションを使用して、追加の構成を実行すできます。

   注:
   [CrowdStrike の追加アクション] リストを開き、必要な追加アクションを **[true]**に設定してください。このように設定しないと、追加アクションはワークスペースで使用できません。

   ベースシステムに付属する追加アクションのリスト



6. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
7. [エンドポイントで他のアクションを実行 (Run Additional Actions on Endpoint)] を使用してレビューするセキュリティインシデントを選択します。

   a. 関連リンクセクションで、 エンドポイントで他のアクションを実行.

   b. 必要な機能を参照して選択します。
   たとえば、**[reg set]** 機能をクリックします。

   c. エンドポイントのすべての関連 CI に対して追加アクションを実行するには、[関連 **CI** を含める **(Include Related CI)]** を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

d. エンドポイントで追加アクションを実行するためのサブキーを定義できます。
このサブキーは、HKLM/ソフトウェア/新規キーにすることができます。

8. エンドポイントで追加アクションの実行を開始するには、[他のアクションを実行] をクリックします。
9. 実行の自動化アクティビティを表示し、検証します。
10. [エンドポイントでの追加アクション] 関連リストでアクションのステータスを検証します。

アナリストワークスペースでの **CrowdStrike Falcon Insight** 統合の使用

CrowdStrike Falcon Insight 統合を使用して、SIR アナリストワークスペースで CrowdStrike Falcon Insight 機能を活用します。

始める前に
必要なロール：sn_si.admin

セキュリティインシデントレスポンスワークスペースで CrowdStrike Falcon Insight 統合を使用する前に、ServiceNow Store からこの統合をダウンロードして構成する必要があります。詳細については、「CrowdStrike Falcon Insight 統合を開始する」を参照してください。

このタスクについて
CrowdStrike Falcon Insight 統合を使用すると、セキュリティインシデントレスポンス ワークスペースを使用して、エンドポイントに対してリアルタイムで修復アクションを実行し、プロファイルを使用してホストに関する詳細情報を収集し、エンドポイントに対して特定のクエリまたはアクションを実行できます。

CrowdStrike Falcon Insight 統合により、アナリストは セキュリティインシデントレスポンス アナリストワークスペースで次の CrowdStrike Falcon Insight 機能を使用できます。

- ホストの詳細を取得
- ログオンユーザーを取得
- ネットワーク統計の取得
- 実行中のプロセスの取得
- 実行中のサービスを取得
- ホストの隔離
- 隔離を削除
- ファイルを取得

手順

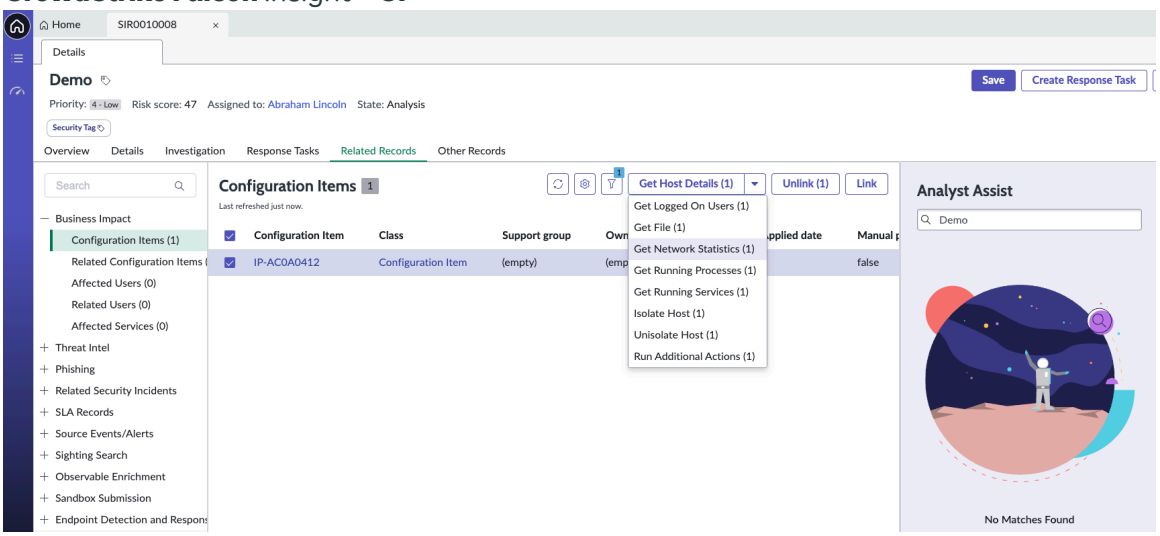
1. SIR ワークスペースで必要なセキュリティインシデントを開き、[関連レコード] タブを選択します。
2. 分析のために、[ビジネスインパクト] 関連リストで CrowdStrike Falcon Insight 機能を使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. 構成アイテムを選択し、ドロップダウンリストから機能を選択します。

CrowdStrike Falcon Insight：**CI**



b. **CrowdStrike Falcon Insight** 実装を選択し、[送信] をクリックします。
[ネットワーク統計情報を取得] 機能が CI に対して呼び出されます。作業メモで結果と検出結果を確認できます。

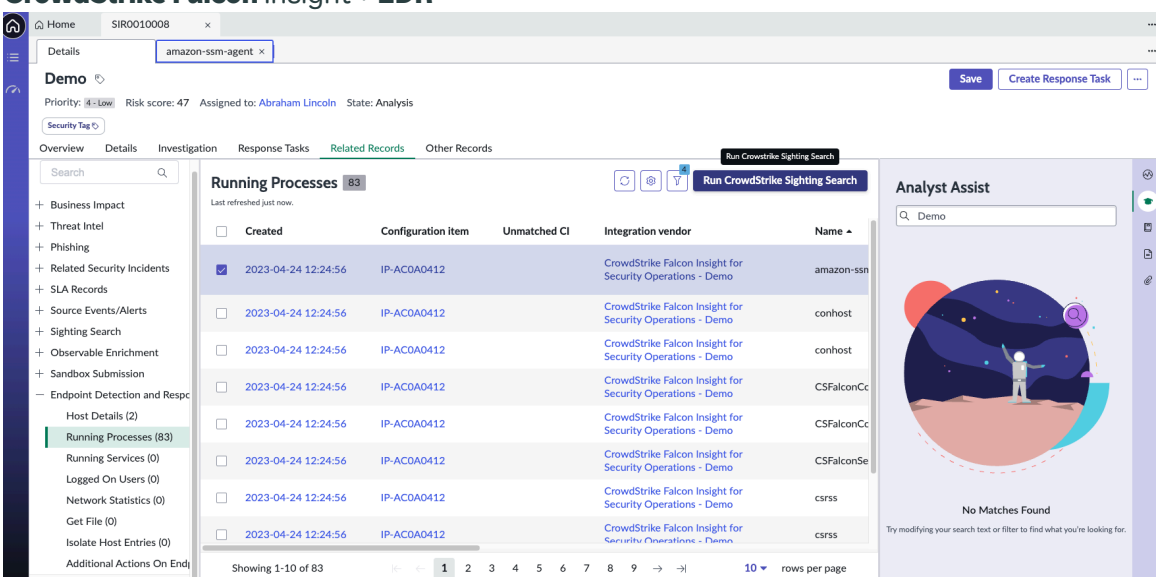
3. 分析のために、**[Endpoint Detection and Response (EDR)]** 関連リストで CrowdStrike Falcon 機能を使用できます。

a. [Endpoint Detection and Response (EDR)] 関連リストから EDR を選択します。

b. 特定の実行中のプロセスをクリックすると、CrowdStrike Falcon Insight の実行中のプロセスの詳細が表示されます。

c. 特定の実行中のプロセスで CrowdStrike Falcon サイティング検索を実行するには、実行中のプロセスを選択して **[CrowdStrike** サイティングを実行 **(Run CrowdStrike Sighting)]** をクリックします。

CrowdStrike Falcon Insight：**EDR**



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

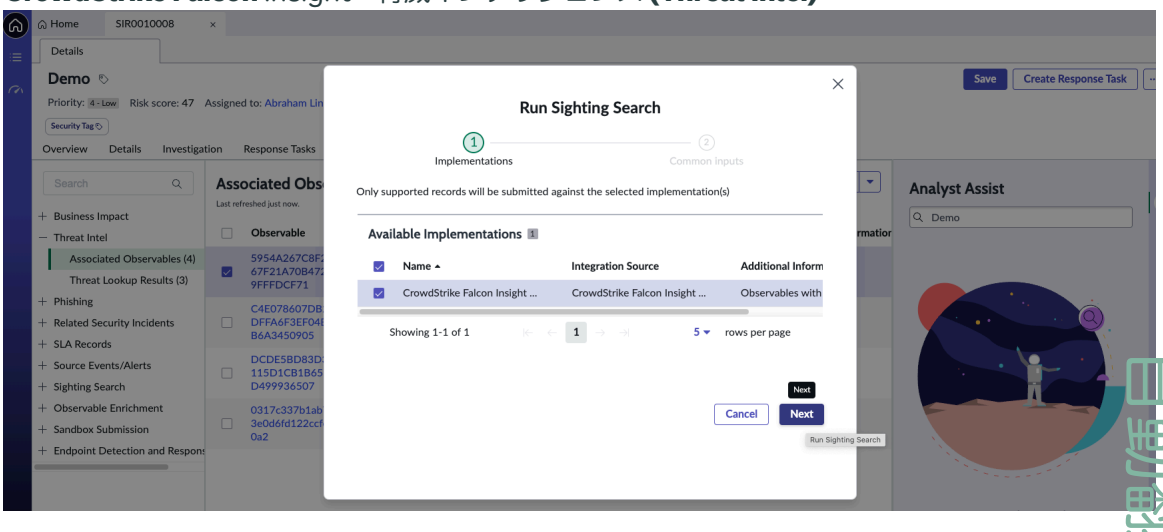
d. CrowdStrike Falcon Insight 実装を選択し、[検索を実行] をクリックします。
これで、選択した実行中のプロセスに対してハッシュサイティング検索が実行されます。作業メモで結果と検出結果を確認できます。

4. 分析のために、[脅威インテリジェンス **(Threat Intel)]** で CrowdStrike Falcon Insight 機能を使用できます。

a. [脅威インテリジェンス (Threat Intel)] グループで観測事象を選択し、ドロップダウンリストから CrowdStrike Falcon Insight 機能を選択します。

b. CrowdStrike Falcon Insight 実装を選択し、[次へ] をクリックします。

CrowdStrike Falcon Insight：脅威インテリジェンス **(Threat Intel)**



c. [日付/時刻を選択 (Select Date/Time)] ポップアップで、任意のランダム値を選択して [送信] をクリックします。
これで、選択した観測事象に対してサイティング検索が実行されます。作業メモで結果と検出結果を確認できます。

CrowdStrike Falcon X Sandbox for Security Operations Integrations

CrowdStrike Falcon X Sandbox for セキュリティオペレーション 統合を使用すると、セキュリティインシデント応答プロセスの一部としてファイルと URL を CrowdStrike Falcon X Sandbox に送信して、詳細なマルウェアと脅威の分析を実行できます。

CrowdStrike Falcon X Sandbox 統合は、マルウェア分析を実行できるオンデマンドの隔離された仮想環境を提供し、統合を通じて ServiceNow セキュリティインシデントに結果を提供できます。

マルウェアインシデントを送信すると、セキュリティインシデントレコードの一部として保持されます。さらなるインシデント解決のためにこれらのレコードを使用し、ファイルと URL の送信を自動化できます。

統合では、フィッシングおよびマルウェアの両方の対応 Playbook の自動化をサポートします。これにより、セキュリティオペレーション センター担当者は、セキュリティインシデント応答の生産性と効率性を高めることができます。

主な特長

この統合を使用すると、次のことができます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ユーザーから報告されたフィッシング (URP)、メールメッセージ、添付ファイル、およびその他のセキュリティインシデントからのファイルと URL の送信を自動化します。
- 分析を更新するために、以前に分析したファイルと URL を手動で送信または再送信します。
- オペレーティングシステム、スキャンタイプ、ランタイムオプションなどの CrowdStrike Falcon X Sandbox 送信パラメーターを自動的に適用する複数の送信構成を作成します。
- SIR インシデント内の HTML 形式のレポートでマルウェアと脅威の結果を分析します。脅威のルックアップ結果と、複数回分析されたファイルと URL に関するインジケーター履歴を表示できます。
- ServiceNow インシデントに送信処理ステータスと脅威の検出結果をタグ付けします。

関連項目

ドキュメント識別子	ドキュメントタイトル
CrowdStrike Falcon X Sandbox	CrowdStrike Falcon Sandbox FAQ
ServiceNow 製品ドキュメント Web サイト	ServiceNow 製品ドキュメント Web サイト

CrowdStrike Falcon X Sandbox 統合を開始する

CrowdStrike Falcon X Sandbox をアクティブ化して、ServiceNow インスタンスおよび セキュリティインシデントレスポンス 製品と連動するように設定できます。

始める前に

- CrowdStrike Falcon X Sandbox for Security Operations integrations を使用する前に、ServiceNow Store からダウンロードする必要があります。
- 次のセットアップチェックリストを確認し、スムーズな CrowdStrike Falcon X Sandbox 統合のためのすべてのタスクを完了したことを確認します。

必要なロール：admin、sn_si.admin

チェックリスト

セットアップタスク	説明
必要な Now Platform ロールと セキュリティインシデントレスポンス ロールがアサインされていることを確認します。	期待される結果を構成および検証するには、次のロールが必要です。 • アドミニストレーター (admin) は、ServiceNow アプリストアからサンドボックス統合をインストールしてセキュリティインシデントアドミニストレーター (sn_si.admin) ロールをアサインします。 • sn_si.admin は、構成およびグローバル設定を作成および編集し、セキュリティインシデントアナリスト (sn_si.analyst) ロールをアサインします。 • セキュリティインシデントアナリスト (sn_si.analyst) は、ファイルと URL をサ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト (続く)

セットアップタスク	説明
	ンドボックスに送信して送信結果を分析するなど、セキュリティインシデントに対応します。
この統合を構成する前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	この統合は Paris および Orlando リリースをサポートしています。 これらの依存プラグインがインストールされていることを確認します。これらのプラグインは、統合ハブ アクションとフローの実行を有効にします。 • ServiceNowIntegrationHub アクションステップ - REST (com.glide.hub.action_step.rest) • ServiceNow 統合ハブランタイム (com.glide.hub.integration.runtime) **注:** プラグインが見つからない場合は、ServiceNow 担当者から要求することが必要な場合があります。プラグインを要求するには、「プラグインの要求」の手順に従います。 セキュリティインシデントレスポンス プラグイン (com.snc.security_incident) が必要です。このプラグインは、セキュリティインシデントレスポンス 製品をサポートするために必要なすべての依存関係を自動的にインストールします。統合に必要な他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。 次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。 **1.** セキュリティインシデントレスポンス 依存関係 (com.snc.si_dep) **2.** Security Integration Framework **3.** Security Support Common **4.** セキュリティサポートオーケストレーション

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト (続く)

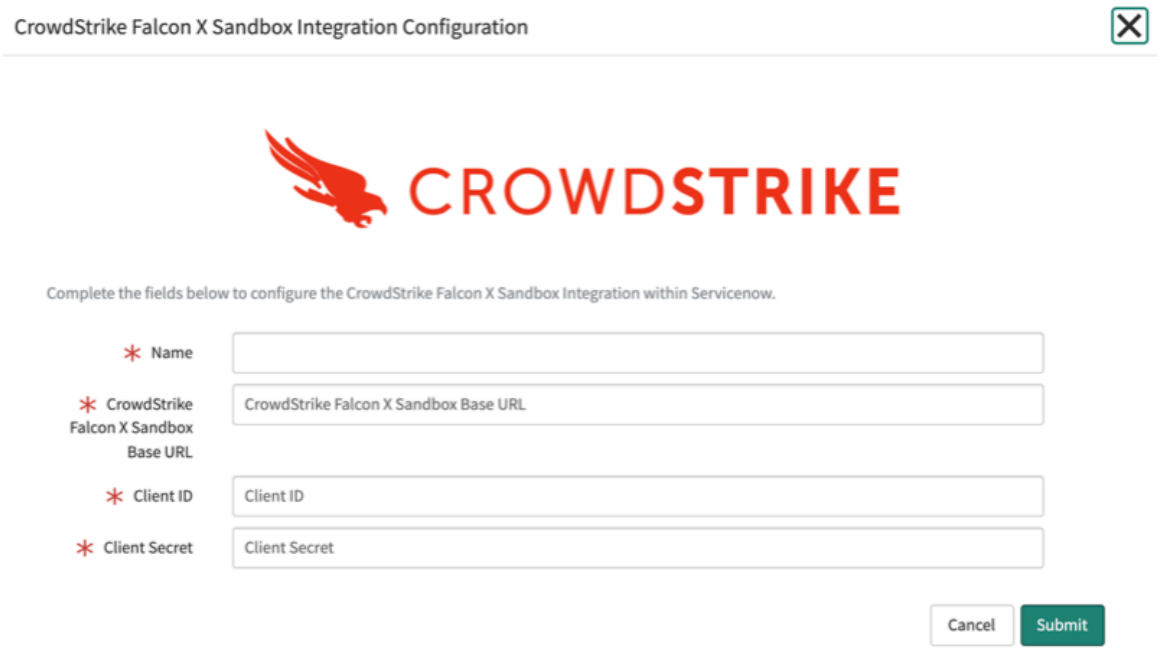
セットアップタスク	説明
	5. 脅威インテリジェンス Support Common (サンドボックス統合機能を使用するために必要) **6.** トラステッドセキュリティサークル **7.** セキュリティオペレーション セットアップアシスタント **8.** セキュリティインシデントレスポンス 統合のための Now Platform インスタンスの設定の詳細については、「Security Operations 製品またはアプリケーションのエンタイトルメントの取得 (Get entitlement for a Security Operations product or application)」および「ServiceNow Store アプリケーションの有効化 (Activate a ServiceNow Store application)」を参照してください。
Falcon Sandbox プライベート API キーのライセンスが付与され、CrowdStrike Falcon X Sandbox の完全な API キーを取得していることを確認します。	この統合は、Falcon Sandbox プライベートクラウドのみをサポートしています。 **注:** このリリースでは、Falcon X 統合をサポートしていません。 CrowdStrike Falcon X Sandbox は、自己署名された制限付き API キーとアップグレードされた完全な API キーを提供します。この統合では自動送信の無制限アクセスを有効にするため、完全な API キーを使用します。 詳細については、CrowdStrike Falcon Sandbox のナレッジベース を参照してください。

手順

1. ServiceNow Store から CrowdStrike Falcon Sandbox for Security Operations Integrations をダウンロードします。
2. インスタンスが完了したら、**[Security Operations]** > [統合] > [統合構成] へ移動します。
3. CrowdStrike Falcon X Sandbox 統合タイルを検索し、[構成] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. 次の詳細を入力して構成を完了します。

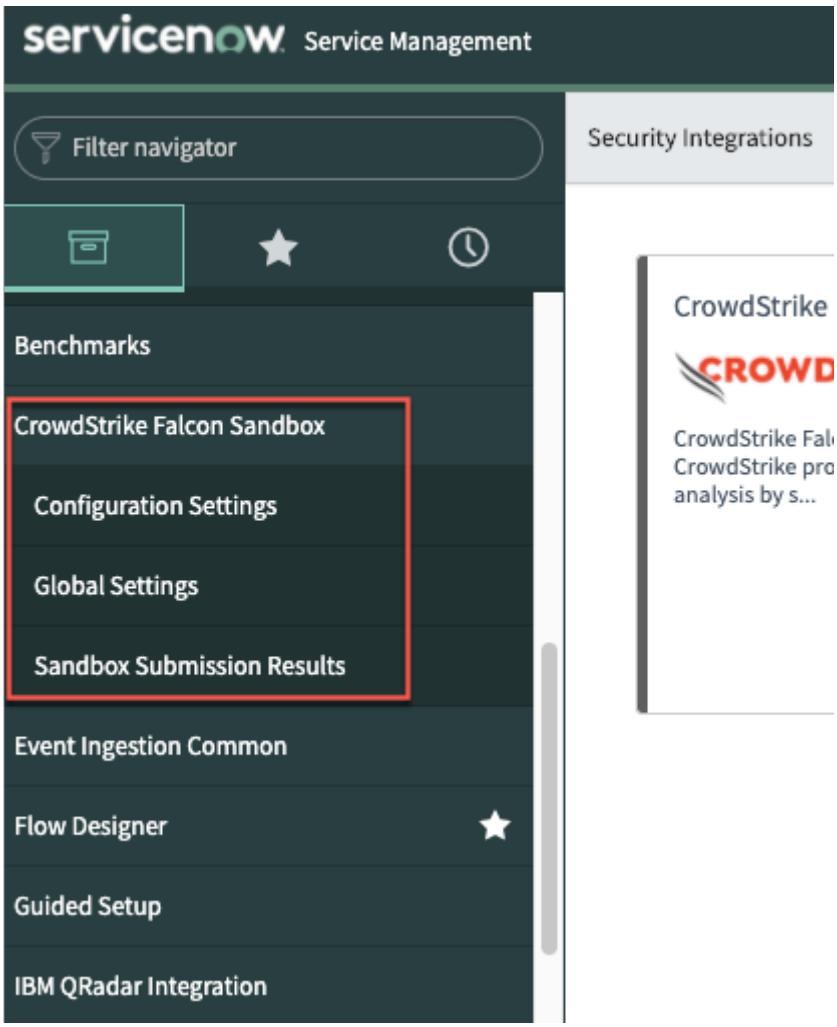
フィールド	説明
名前	この統合の名前 (例：demo-1)。これはサンドボックス構成を識別するための一意の名前ですが、構成できるのは ServiceNow インスタンスごとに 1 つの統合のみです。
CrowdStrike Falcon Sandbox ベース **URL**	サンドボックスのベース URL。この URL は、サンドボックスを構成した後に使用できます。たとえば、https://servicenow.falcon-sandbox.com がベース URL です。
クライアント **ID**	OAuth2 API クライアント ID。詳細については、「API Clients and Keys (API クライアントとキー)」を参照してください。
クライアントシークレット	OAuth2 API クライアントシークレットキー。詳細については、「API Clients and Keys (API クライアントとキー)」を参照してください。

5. [Submit] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サンドボックスの検証と送信が正常に完了すると、[セキュリティ統合] ページにタイルとして保存されます。アプリケーションナビゲーターでサンドボックスモジュールを表示できます。



次のタスク

統合が正常に完了したら、次のステップはサンドボックスの送信構成を設定することです。

サンドボックスの送信構成の設定

サンドボックス構成を設定して、マルウェア分析のためのセキュリティインシデントレコード送信の分析環境とランタイムオプションを定義します。

始める前に

必要なロール：sn_si.admin

このタスクについて

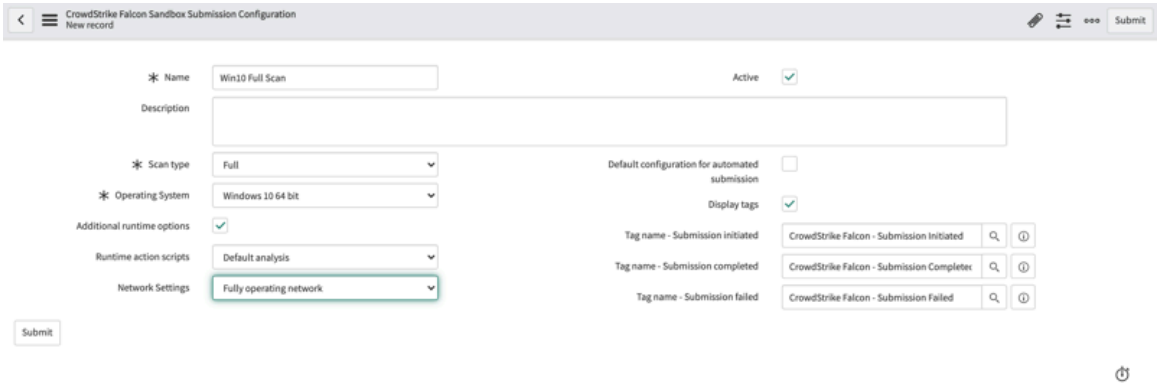
統合を使用して CrowdStrike Falcon X Sandbox にファイルまたは URL を送信する前に、少なくとも 1 つの送信構成を構成する必要があります。送信構成では、サンドボックスのオペレーティングシステム、スキャンタイプ、ランタイムオプション、およびその他のインシデント処理特性を定義します。CrowdStrike Falcon X Sandbox 環境で利用可能なさまざまなオプションを使用するために、複数の構成を作成することができます。

手順

1. 次のように移動する。 **All** (すべて) > **CrowdStrike Falcon X** サンドボックス > 構成設定.
2. [**New**] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳



3. [スキャンタイプ] が完全の構成を作成するには、次のフィールドに入力します。

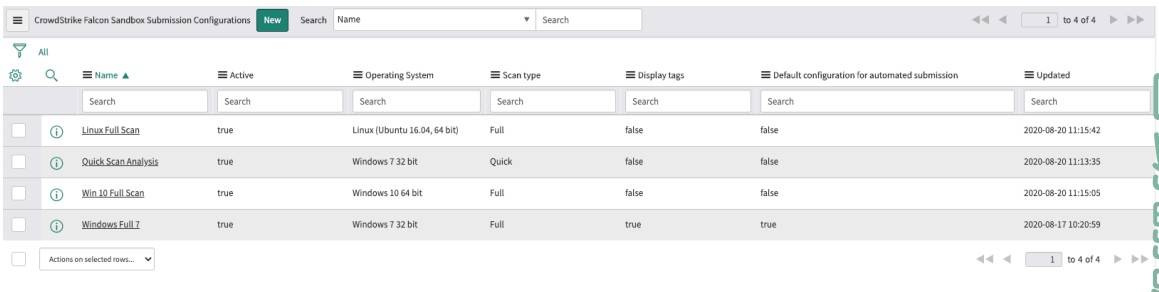
フィールド	説明
名前	送信構成の一意の名前。この名前は、アナリストがファイルを送信するときに表示されます。名前は、わかりやすいもので、他の構成と簡単に区別できるものにすることが重要です (例：Win 10 Full Scan)。名前が一意でない場合は、エラーが表示され、重複する設定レコード名は保存されません。
スキャンタイプ	スキャンタイプは [完全] にします。[クイック] スキャンタイプでは、限定的な脅威分析が提供されます。
オペレーティングシステム	サンドボックスがファイルまたは URL をスキャンする分析 VM 環境。
アクティブ	ファイルまたは URL を手動で送信する場合に選択するオプション。
自動送信のデフォルト設定	デフォルトでクリアされているオプション。このオプションを選択すると、この構成をマルウェア分析の送信の自動化に使用できるようになります。 **注:** 自動送信のデフォルト構成として使用できるアクティブな送信構成は 1 つだけです。
タグを表示	デフォルトでクリアされているオプション。このオプションを選択すると、ファイルまたは URL の送信ステータスを示すタグが表示されます。分析の処理には数分かかることがあります。表示タグは送信開始、送信完了、または送信失敗です。
他のランタイムオプション	デフォルトでクリアされているオプション。このオプションを選択すると、サンドボックスがサポートする追加のランタイムパラメーターが使用可能になります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ランタイムアクションスクリプト	分析中に人間の行動をシミュレートしてファイルまたは URL を操作するアクションスクリプトを使用できるようにするオプション 。 https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/ 詳細については、CrowdStrike Falcon X Sandbox ドキュメントを参照してください。
ネットワーク設定	URL またはファイルをサンドボックスに送信するときに使用するネットワーク設定のタイプを選択できるオプション。

4. **[Submit]** をクリックします。
   構成を送信すると、[構成設定] ページにレコードとして保存されます。構成をサンドボックスの送信で使用するには、[アクティブ] である必要があります。



自動翻訳

次のタスク
サンドボックス送信を構成した後、次のステップは 手動でファイルまたは ULR をサンドボックスに送信することです

。

サンドボックスへのファイルまたは **URL** の手動送信

カテゴリーがフィッシングであるなどの特定のインシデント基準が満たされた場合に、ファイルまたは URL をサンドボックスに手動で送信できます。

始める前に
必要なロール：sn_si.analyst

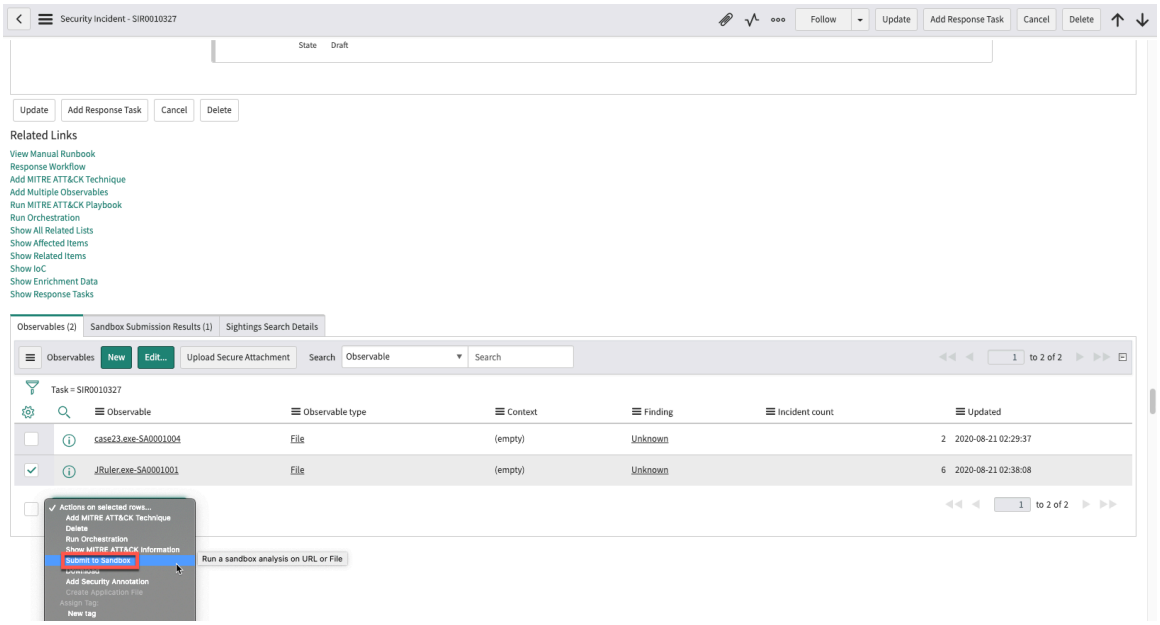
このタスクについて
セキュリティインシデントとファイルまたは URL を確認した後、[サンドボックスに送信] オプションを選択して、マルウェア分析を実行できます。

手順

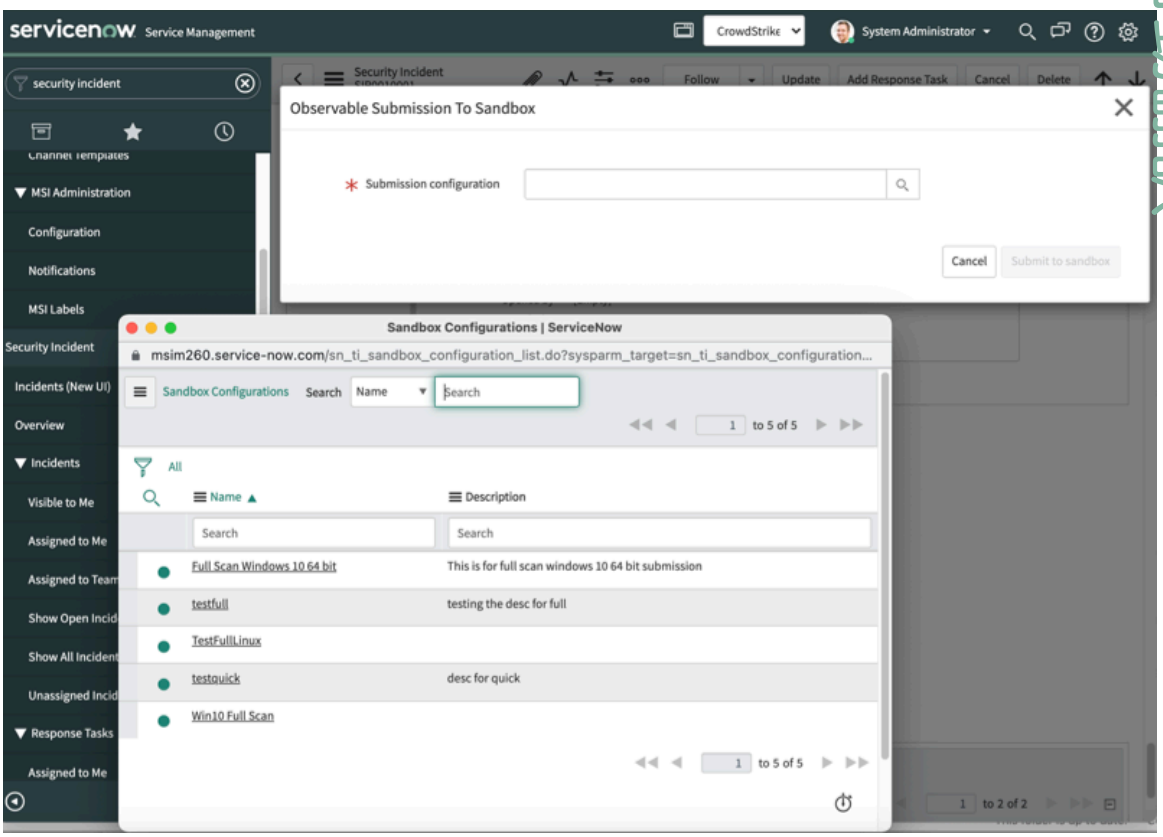
1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデント > すべてのインシデントを表示 をクリックし、ファイルまたは URL 観測可能タイプレコードの送信先にするセキュリティインシデントを開きます。
2. **[IoC** を表示] 関連リンクをクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [観測事象] タブで、マルウェア分析または脅威分析を実行する 1 つまたは複数のレコードを選択し、[サンドボックスに送信] をクリックします。

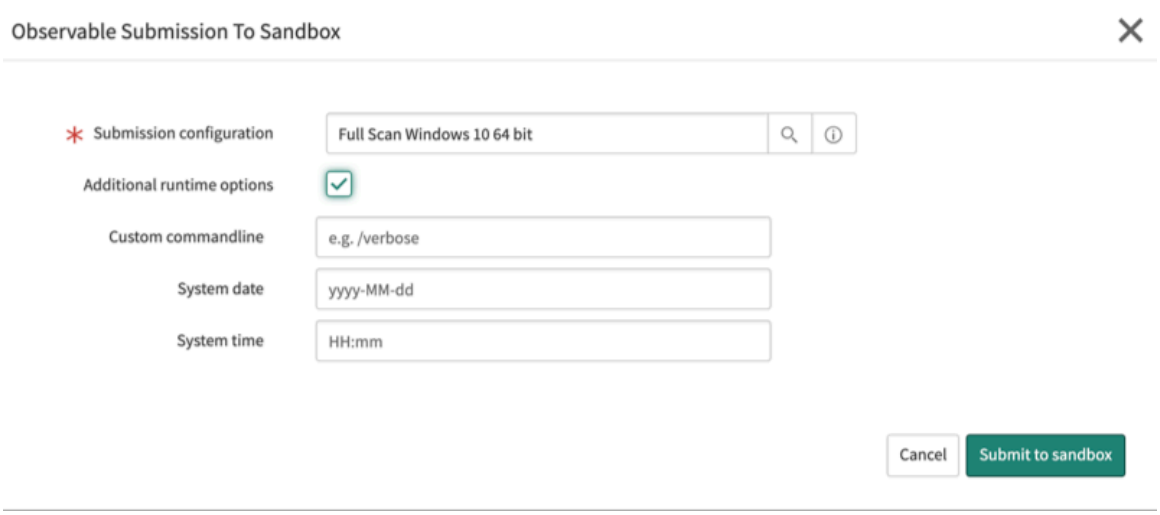


4. [ファイル送信] フィルターが表示されたら、[送信構成] で希望するサンドボックスの構成を選択し、[サンドボックスに送信] をクリックします。



5. オプション: さらにカスタムオプションを指定する場合は、[他のランタイムオプション] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



フィールド	説明
カスタムコマンドライン	通常のアプリケーションコマンドラインまたは特別な操作。
システム日付	yyyy-MM-dd 形式のシステム日付。
システム時間	HH:mm 形式のシステム時間。

送信を開始した後、 作業メモを表示して送信のステータスを確認できます。 送信のステータスの詳細について、または結果を分析するには、[サンドボックスの送信結果] を表示します。

注:
CrowdStrike Falcon X Sandbox では、URL のクイックスキャンはサポートされていません。作業メモの情報が多すぎる場合は、[フィルター] オプションを使用して、関連性のある必要な作業メモにドリルダウンできます。

次のタスク
マルウェア分析のために観測事象をサンドボックスに送信する場合は、サンドボックスの送信結果を表示して、潜在的な脅威に対する次のステップを実行します。

フローデザイナーを使用した **CrowdStrike Falcon Sandbox** 送信の自動化

CrowdStrike Falcon X Sandbox 統合には、ワークフロースタジオ を使用して作成された、セキュリティインシデントレコードを処理するフローテンプレートが含まれています。

始める前に

- サンドボックスの送信構成を作成し、[自動送信のデフォルト設定] として 1 つの構成が有効になっていることを確認します。このフローがトリガーされると、デフォルト構成でサンドボックス送信が発生します。

必要なロール：sn_si.admin

このタスクについて
これらのフローは、主にインシデント応答ワークフローの一部としてファイルまたは URL の送信を自動化する際の開始点として設計されています。
サンプルフローでフィッシングとしてセキュリティインシデントを定義すると、サンプルフローをアクティブ化したときに、フィッシングファイル添付ファイルが自動的に送信されます。または、.exe ファイルタイプが観測事象レコードにアタッチされている場合は、このファイルタイプすべてを送信できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

これらのサンプルフローを変更して、さまざまな条件、カテゴリ、複合条件などで自動送信をトリガーできます。

サンドボックス統合は、デフォルトでは無効になっている 2 つのベースシステムフローで構成されています。

- [カテゴリがフィッシングの場合にファイルを送信]：このフローは、セキュリティインシデントカテゴリがフィッシングとして定義されている場合に、マルウェア分析のためにファイルをサンドボックスに送信します。セキュリティインシデントの観測事象レコードにファイルをアタッチする必要があります。ユーザーから報告されたフィッシング (URP) 機能を使用している場合、メールの添付ファイルは自動的に解析され、観測事象レコードとして SIR インシデントレコードに追加されます。送信を自動化するための追加のアクションは必要ありません。
- [観測事象のファイルタイプが **exe** の場合に送信]：このフローは、セキュリティインシデント観測事象が exe の場合に、マルウェア分析のためにファイルをサンドボックスに送信します。フィッシングカテゴリフローと同様に、セキュリティインシデントの観測事象レコードにファイルをアタッチする必要があります。これは、ファイルをアップロードして手動で行うことも、フィッシングメールの添付ファイル、またはインシデントを作成するその他のメカニズムが観測事象レコードに関連付けられている場合は自動的に行うこともできます。

フローが構成され、インシデント条件がパラメーターを満たすと、セキュリティインシデントをレビューするときにサンドボックスの送信が自動的にトリガーされます。送信が開始されたことを示す作業メモを確認します。構成で有効になっている場合はタグが表示されます。送信処理待ちの結果レコードを確認します。

サンドボックス統合には、複数のサブフローも含まれています。サブフローは、統合送信機能全体の内部コンポーネントです。セキュリティ基準に合わせてサブフローをカスタマイズおよび編集できます。

サブフローを参照して、サンドボックス送信に関する問題のトラブルシューティングを行うことができます。サブフローを呼び出すたびに実行レコードが作成されます。このレコードは、フロー内で特定のエラーが発生した場所を示すため、問題を修正できます。

サンドボックス統合 - 複数のワークフロー

Flows | Subflows | Executions | Help | + New

All > Application Name contains Sandbox

Name ▲	Internal name	Application	Status	Active	Updated	Updated by
Search	Search	*Sandbox	Search	Search	Search	Search
Add submission status tag on SIR	add_submission_status_tag_on_sir	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 12:33:57	admin
Aggregate Additional Runtime Options	aggregate_additional_runtime_options	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 08:47:54	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-18 02:52:33	admin
CrowdStrike Falcon Sandbox Poll Submission	crowdstrike_falcon_sandbox_polling	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-02 05:11:53	admin
CrowdStrike Falcon Sandbox Submission	submit_file_to_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:17:57	admin
CrowdStrike Falcon Submission Results	crowdstrike_falcon_submission_results	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:30:16	admin
CrowdStrike Polling Quick/Full Scan	crowdstrike_polling_quickfull_scan	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 20:23:07	admin
Fetch Environment Ids from Sandbox	fetch_environment_ids_from_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-25 07:45:54	admin
Submit File or URL to CrowdStrike Quick ...	submit_fileurl_to_crowdstrike	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 19:04:42	admin
Submit File/URL to Sandbox	submit_fileurl_to_sandbox	Security Operations CrowdStrike Falcon S...	Draft	true	2020-05-25 07:50:18	admin
Submit Observable for Automated submission	submit_observable_for_automated_submission	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-06 06:15:35	admin

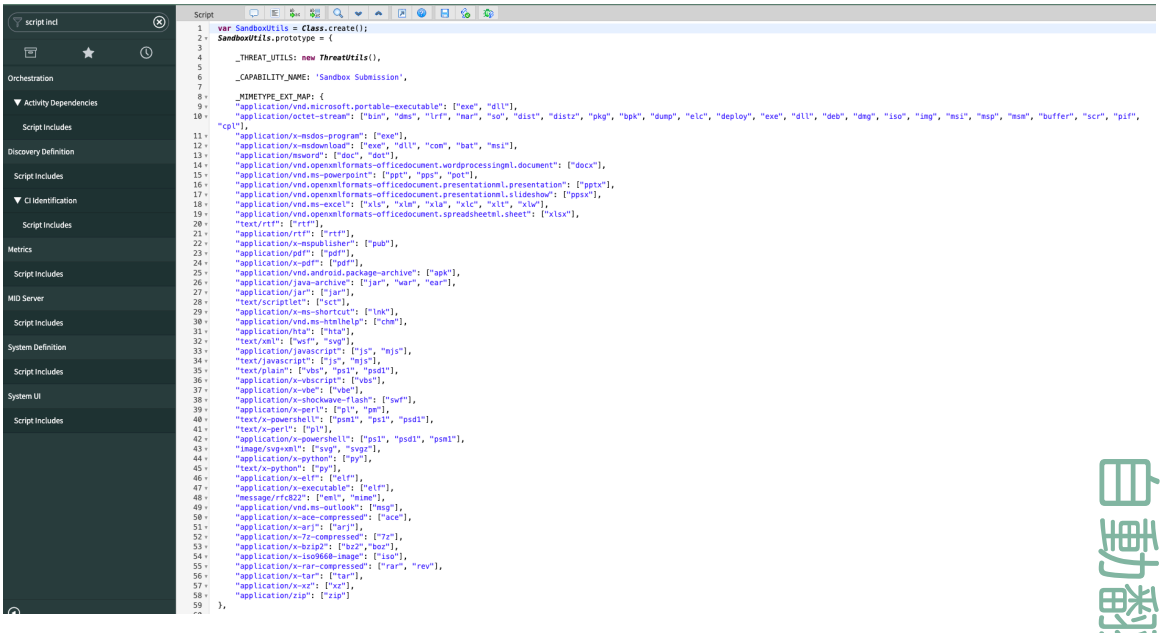
Actions on selected rows... | 1 to 11 of 11

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

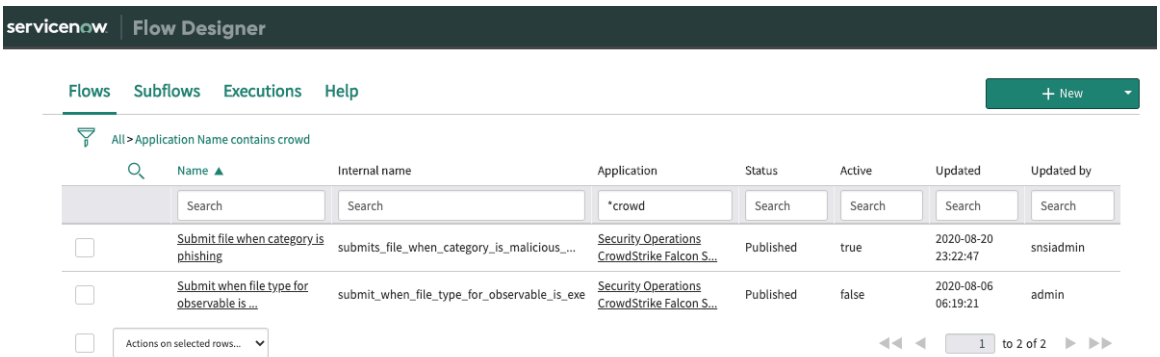
- デフォルトのフローをカスタマイズする場合は、自動送信をトリガーするために [自動送信の観測事象を送信] サブフローがフローに含まれていることを確認する必要があります。
- exe に代わるファイル拡張子をカスタマイズして定義できます。[観測事象のファイルタイプが **.exe** の場合に送信] フローのコピーを作成し、そのコピーを変更します。コンテンツタイプとファイル拡張子は SandboxUtils スクリプトでマッピングされます。スクリプトインクルードにアクセスするには、[システム定義] > [スクリプトインクルード] に移動し、SandboxUtils を検索します。

SandboxUtils スクリプト



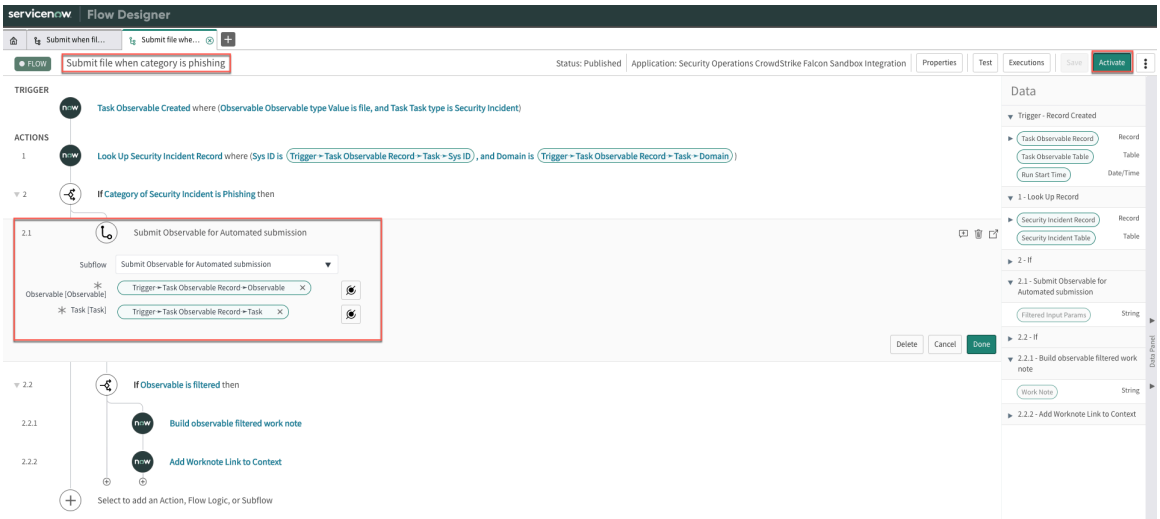
手順

1. 次のように移動する。 **All** (すべて) > **Flow Designer** > デザイナー > フロー.
2. [アプリケーション] タイプでフローをフィルタリングします。
   たとえば、*crowd は 2 つの CrowdStrike Falcon X Sandbox フローをフィルタリングします。



3. 詳細を表示するフローを選択します。
   次の例は、[カテゴリがフィッシングの場合にファイルを送信] フローを示しています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [アクティブ化] をクリックし、確認メッセージが表示されたら **[OK]** をクリックします。

次のタスク
自動送信フローを構成した後は、サンドボックスの送信結果を表示して脅威を分析できます。

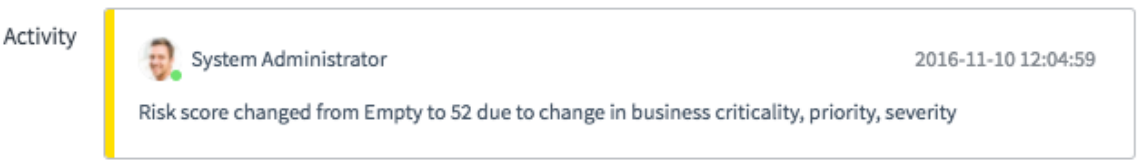
サンドボックスの送信結果の監視

すべてのサンドボックスの送信結果は、セキュリティインシデントごとの [サンドボックスの送信結果] タブに表示されます。

始める前に
必要なロール：sn_si.analyst

手順

1. 作業しているセキュリティインシデントを開き、サンドボックスの送信が成功したことを確認します。

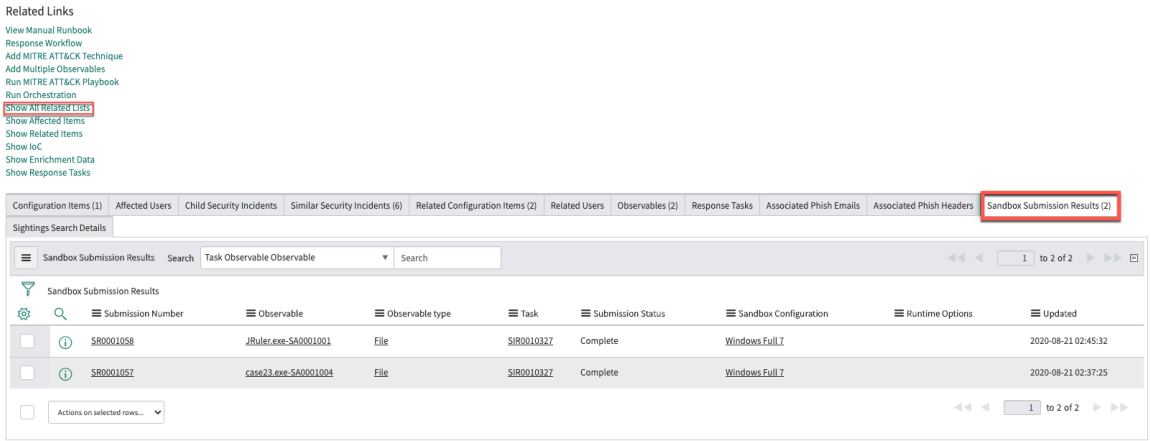


2. スキャンが成功したことを確認できない場合は、作業メモで詳細と対処方法を確認してください。

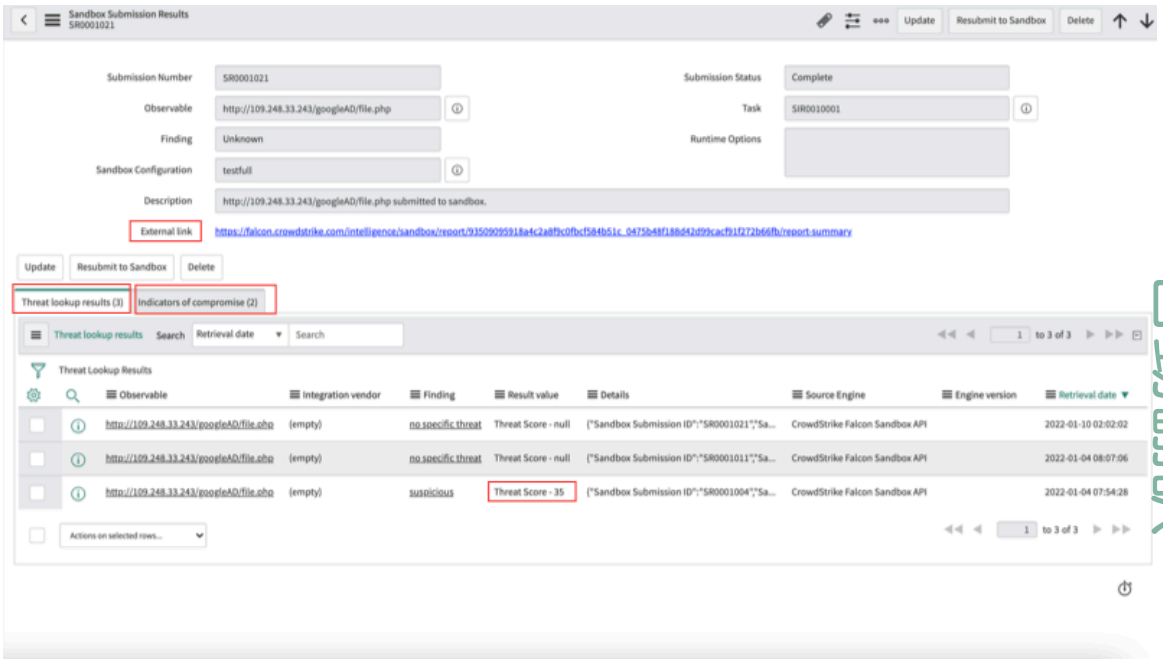
3. 作業メモある完全な結果リンクをクリックするか、または、セキュリティインシデントの下部で [すべての関連リストを表示] > [サンドボックスの送信結果] に移動します。
結果は [サンドボックスの送信結果] タブに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. 任意のレコードをクリックして開くと、完全なサンドボックス分析が表示されます。



5. オプション:　[サンドボックスに再送信] をクリックして、観測事象を再処理します。

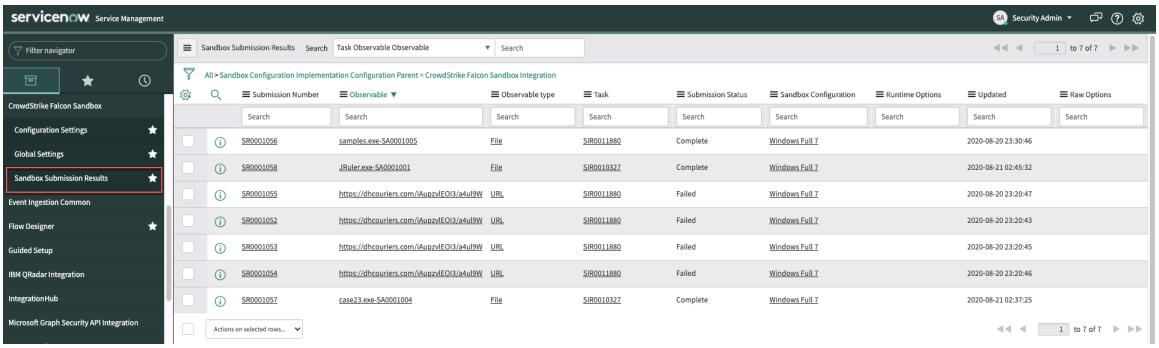
タスクの結果

- [脅威のルックアップの結果] タブには、悪意の検出結果、脅威スコア、その他の詳細などの脅威アセスメントが表示されます。これらの詳細は、すべての ServiceNow 脅威ルックアップ統合の標準的な脅威ルックアップ形式構造で提供されます。
- [セキュリティ侵害のインジケーター] タブは、信頼スコアとともに悪意のあるまたは不審なサンドボックスの結果を提供します。 信頼スコアは、ServiceNow プラットフォームに格納されている他のインジケーター情報と類似しています。情報として分類されているインジケーターは、このタブには含まれていません。
- CrowdStrike Falcon X Sandbox ポータルでサンドボックスの結果を表示するには、[外部リンク] をクリックします。

> **注:**
> このオプションを使用するには、結果を表示できる CrowdStrike Falcon X Sandbox ロールが必要です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

に移動すると、すべてのセキュリティインシデントのandboxの送信結果を監視 できます **CrowdStrike Falcon Sandbox** > サンドボックスの送信結果.



Sandbox 送信ステータスによるセキュリティインシデントのタグ付け

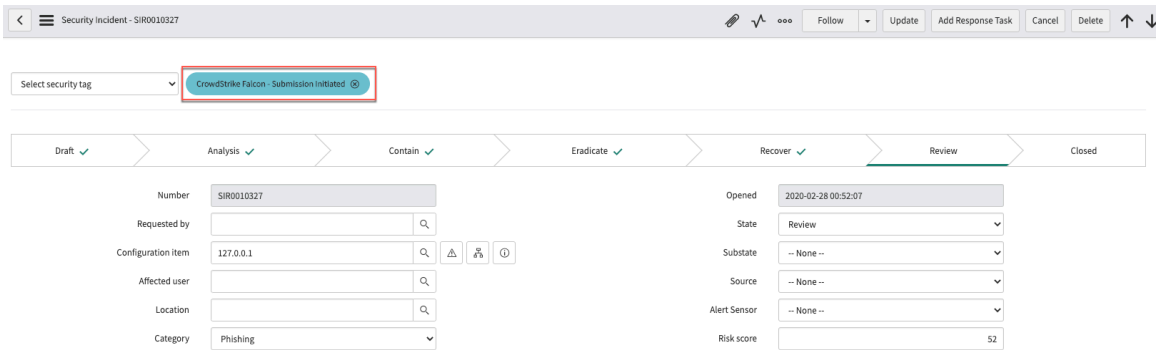
オプションで、送信開始タグおよび送信完了タグを使用してセキュリティインシデントにタグを付けることができます。

[サンドボックスの送信構成] で [タグを表示] オプションを選択すると、ファイルまたは URL の送信ステータスを示すタグが表示されます。サンドボックス分析は処理に数分かかる場合があるため、この方法でステータスを確認すると便利です。

表示タグは送信開始、送信完了、および送信失敗です。

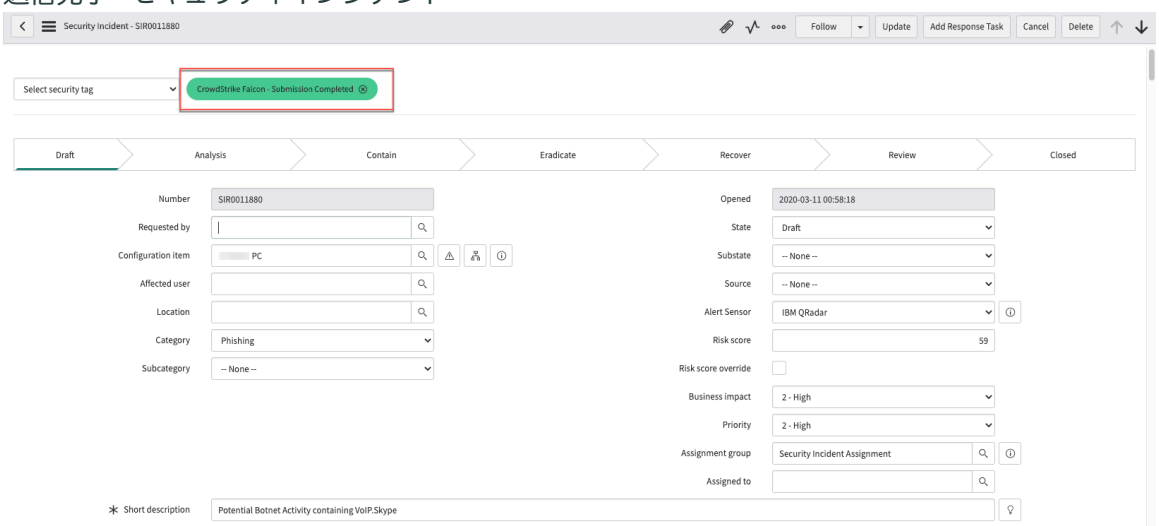
次の例は、送信が開始されたセキュリティインシデントを示しています。

送信開始 - セキュリティインシデント



次の例は、送信が完了したセキュリティインシデントを示しています。

送信完了 - セキュリティインシデント



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サンドボックスのグローバル設定の確認

ファイルまたは URL の送信結果で問題が発生した場合は、グローバルサンドボックスの設定を確認して変更します。

始める前に
必要なロール：sn_si.admin

手順

1. 次のように移動する。 **All** (すべて) > **CrowdStrike Falcon** サンドボックス > グローバル設定.
2. 設定を確認し、必要に応じて変更します。

フィールド	説明
ファイルサイズ制限 (MB)	サンドボックスのアップロードファイルサイズ制限 (メガバイト単位)。 **注:** デフォルトでは 256 MB のファイルサイズ制限が構成されています。256 MB を超えて値を増やさないでください。ただし、大きなファイルを送信しないように、最大ファイルサイズ制限を小さくすることをお勧めします。
送信結果の最大タイムアウト (分)	サンドボックスからの送信結果の最大タイムアウト。 **注:** デフォルトのタイムアウトは 30 分です。結果が 30 分以上かかる場合は、時間を増やすことができます。また、サンドボックスポータルで結果を表示することもできます。

3. [保存] をクリックします。

Elasticsearch インシデント拡張統合

Elasticsearch - インシデント拡張統合はログを検索し、関連するサイティング情報をセキュリティインシデントに追加します。

探索

セキュリティインシデントレスポンス の統合

セットアップ

- Elasticsearch の開始 - インシデント拡張統合
- サイティング検索設定レコードの作成

使用

開発

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

- サイティング検索の実行
- Security Operations Integration - サイティング検索フロー
- Security Operations - Elasticsearch サイティング検索フロー
- ServiceNow セキュリティオペレーション 統合開発のガイドライン
- 統合を作成するためのヒント
- 開発者トレーニング
- 開発者ドキュメント
- アプリケーションとともにインストールされているコンポーネントの検索

トラブルシューティングとヘルプ

- 統合のトラブルシューティング
- Security Operations Community で質問や回答をする
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

自動翻訳

Elasticsearch の開始 - インシデント拡張統合

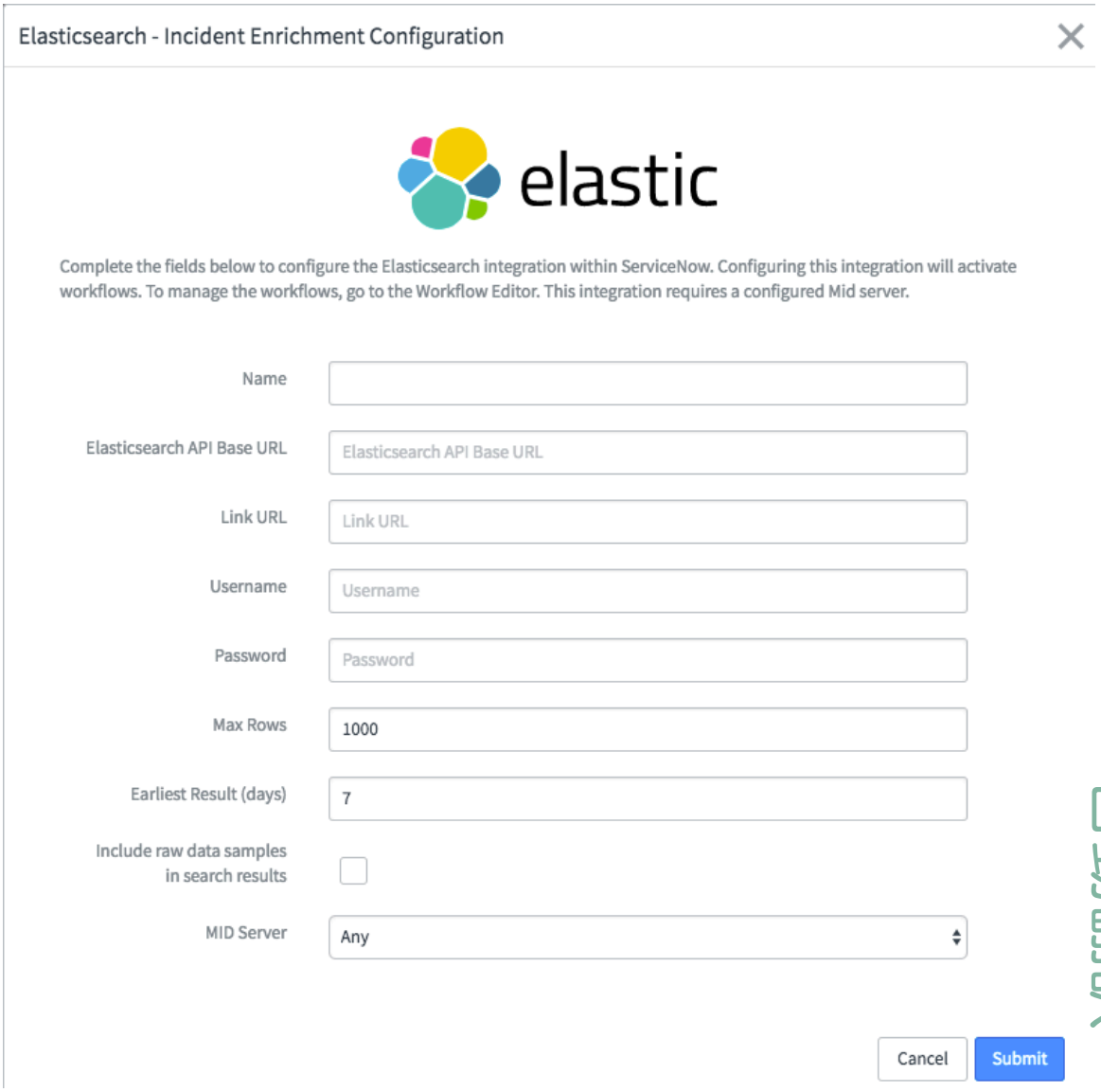
Elasticsearch は、セキュリティオペレーション と簡単に統合できる分散型の RESTful 検索および分析エンジンです。Elasticsearch - インシデント拡張統合を使用する前に、ServiceNow Store から統合をダウンロードし、適切な API Base URL とログイン認証情報を追加する必要があります。

始める前に
必要なロール：sn_si.admin

手順

1. から統合をダウンロードします ServiceNow Store.
2. インストールが完了したら、Elasticsearch にアクセスし、Elasticsearch プロファイルの下の API Base URL を取得します。
3. インスタンスで、 セキュリティオペレーション > 統合 > 統合設定.
   利用可能なセキュリティ統合が一連のカードとして表示されます。
4. Elasticsearch - インシデント拡張カードで、[新規] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

5. 必要に応じて、フィールドに入力します。

フィールド	説明
名前	この構成の名前。
Elasticsearch API のベース URL	Elasticsearch サイトから取得したベース URL。
リンク URL	[オプション] 利用可能な場合、Kibana インスタンスへのリンク
ユーザー名	Intel Elasticsearch ユーザー名。
パスワード	Intel Elasticsearch パスワード。
最大行数	検索する行の最大行数。
最も早い結果 (日数)	表示する最も早い結果 (日数単位)。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
検索結果に生データサンプルを含める	サイティング検索結果に生データのサンプルを含めるには、これを選択します。返されるデータの量は、[セキュリティインシデントレスポンス] プロパティの [生データの行数] プロパティの設定によって異なります。
MID サーバー	[任意] を選択して、 任意のアクティブな MID サーバーを使用するか、特定の MID サーバー名を選択します。

注:
この統合を設定すると、ワークフローが有効になります。ワークフローを管理するには、[ワークフローエディター] に移動します。

6. **[Submit]** をクリックします。
   統合構成カードが表示されます。
7. 新しい構成カードを表示すると、[構成] または [削除] をクリックして、構成を変更または削除できます。
8. 統合構成カードの元のリストに戻るには、[構成を表示] ドロップダウンから [いいえ] を選択します。

タスクの結果
構成後、セキュリティインシデントレスポンスのウォッチリストに観測事象を公開するために Elasticsearch - インシデント拡張統合を選択できます。

FireEye Endpoint Security 統合

FireEye Endpoint Security (HX シリーズ) は、エンドポイント上の既知の脅威と不明な脅威を検査および分析するのに役立ちます。

今日の熟練した攻撃者は、ほとんどのセキュリティチームがエンドポイントを保護するために何年も依存してきた従来の防御を回避します。従来の防御では、既知の脅威を阻止しても、その脅威の意図を特定することはできません。FireEye HX Endpoint Security は、セキュリティチームがエンドポイントに対する既知および不明の高度な脅威を追跡して阻止するのに役立ちます。

セキュリティインシデントレスポンスと FireEye HX のゴールドスタンダードな統合により、セキュリティアナリストはツール間を移動することなく、簡単かつ効率的にセキュリティインシデントを即座に調査および修正できます。ネットワーク封じ込めを使用して、エンドポイントで修復アクションを実行し、プロファイルを実装してホストに関する特定の詳細を収集し、エンドポイントで特定のクエリまたはアクションを実行できます。

主な機能

- ホスト拡張アクションを実行して、ホストの詳細、ネットワーク統計情報、ユーザーの詳細、ファイルの詳細、プロセスの詳細、サービスの詳細といったエンドポイントに関する詳細を収集する機能。
- エンタープライズセキュリティ検索を実行して、エンドポイント間で潜在的な悪意のある可能性のある観測事象を検出し、是正措置を実行する機能。
- エンドポイントの詳細な検査と分析のためにトリアージ取得とデータ取得を収集する機能。

制限事項

この統合の既知の制限は次のとおりです。

1. MID アプリケーションフィールド値は手動で入力する必要があります。
2. [ホストを隔離] および [実行中のサービスを取得] は Linux エージェントでは実行できません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. [隔離を削除] は Linux エージェントをサポートしていません。
4. [トリアージ取得] は Linux エージェントをサポートしていません。
5. ユーザーは [拡張データを表示] 関連リンクを構成する必要があります。初期設定では利用できません。
6. サイティング検索では、一度に 5 つのアクティブな検索のみが存在できます。残りはキューに入れられ、進行中のサイティングのいずれかが完了すると開始されます。
7. サイティングはすぐに利用できますが、デフォルトでは active false に設定されています。
8. [実行中のプロセスを取得] ではハッシュはサポートされていません。

FireEye 統合のための NowPlatform インスタンスの設定

FireEye 統合用に NowPlatform インスタンスを設定するには、次の構成手順を確認してください。

始める前に
必要なロール：Now Platform アドミン (sn_si_admin)

次のセクションでは、FireEye 統合用にアプリケーションをインストールする前に NowPlatform インスタンスで完了する必要があるセットアップタスクを示します。

ServiceNow Store からアプリケーションをインストールする前に、次のタスクを完了していることを確認してください。

タスク	説明
必要な NowPlatform および セキュリティインシデントレスポンス (SIR) のロールがアサインされていることを確認します。	以下のロールが必要です。 1. 統合用にアプリケーションをインストールするには、システムアドミニストレーター (admin) ロールを持つユーザーが必要です。 2. 統合を構成し、プロファイルを作成、アクティブ化、および削除するには、セキュリティインシデントアドミニストレーター (sn_si.admin) ロールを持つユーザーが必要です。 3. セキュリティインシデントを操作するには、セキュリティインシデントアナリスト (sn_si.analyst) ロールを持つユーザーが必要です。このロールを持つユーザーは、統合で利用可能なすべての機能を開始できます。
MID サーバーがインストールおよび設定されていることを確認します。	MID サーバーを構成します。ファイルを管理し、組織のネットワーク内に展開された FireEye サービスに接続するには、NowPlatform インスタンスに MID サーバーが必要です。MID サーバーの詳細については「https://servicenow.com/docs」を参照してください。
アプリケーションをインストールする前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	このアプリケーションをインストールする前に、次のアプリケーションを ServiceNow Store からインストールしてアクティブ化する必要があります。スムーズにインストールできるように、アプリケーションを次のリストの順

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスク	説明
	番で、一度に 1 つずつインストールしてアクティブ化します。 **1.** セキュリティインシデントレスポンスサポート **2.** Security Support Core **3.** Security Support Common **4.** セキュリティインシデントレスポンス **5.** 脅威インテリジェンス Support Common **6.** ServiceNow Integration Hub Enterprise Pack Installer
プロファイルの承認オプションを有効にする前に、承認グループが作成されていることを確認します。	オプションの承認ワークフローは、ホストマシンの隔離、ネットワークへの復元、ファイルの取得、エンドポイントでの追加アクションの実行に使用できます。 組織でこれらのアクションをより詳細に制御する必要がある場合は、プロファイルの構成時に [承認が必要] オプションを有効にします。 プロファイルがない場合は、関連リストから直接機能が呼び出されると、FireEye のデフォルト設定モジュールから承認を処理できます。 セキュリティアドミニストレーターは、プロファイルとデフォルト設定を構成するときに承認を設定できます。承認グループは、インスタンスの [グループ] リストで使用できる必要があります。

自動翻訳

手順

1. 次のように移動する。 ユーザー管理 **(User Administration)** > グループ.

2. クリックします 新規 [グループ] リストにあります。

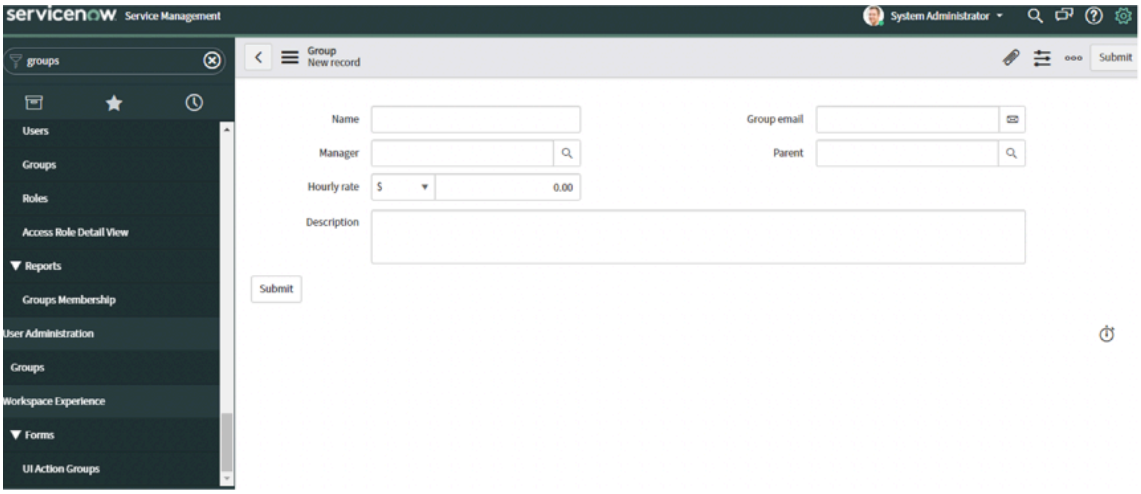
3. 以下の詳細をフォームに入力します。

フィールド	説明
名前	承認要求が送信されたときに表示されるグループの名前。
グループ メール	(オプション) グループのメール配布リストまたは連絡先メールアドレス (グループマネージャーなど)。
マネージャー	(オプション) グループマネージャーの名前。検索アイコンをクリックしてリストを表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
親	(オプション) 親グループの名前 (親に関連付けられている場合)。
時間単価	(オプション) 作業時間ごとに支払われる金額。
説明	(オプション) グループに関する補足情報。

4. クリックします 送信.



新しいグループが [グループ] リストに表示されます。承認グループが正常に作成されました。必要に応じて、セキュリティアナリストによって送信された要求を承認できるユーザーをこの新規グループに追加します。ユーザーは、ユーザーが属するすべてのグループからロールを継承します。ロールをユーザーに直接アサインすることもできます。

sn_si.analyst ロールを持つユーザーによって送信された要求を監視および処理するには、承認グループの各メンバーは、Now Platform で [自分の承認] に移動する必要があります。または、承認者は FireEye Approvals で FireEye 統合用に送信された要求を見つけることができます。

次のタスク
次のステップでは、ServiceNow Store からアプリケーションをインストールして構成します。

トリアージ取得のタイムスタンプ設定

インストール手順の前に、タイムスタンプ設定を構成して確認します。

始める前に
必要なロール：NowPlatform セキュリティインシデントアドミニストレーター (sn_si_admin)

FireEye アプリケーションをインストールする前に、FireEye で実行する必要がある前提条件がいくつかあります。

トリアージ取得は、[タイムスタンプ前後 (Around Timestamp)] フィールドまたは [標準] フィールドの入力を使用して要求できます。[タイムスタンプ前後 (Around Timestamp)] は、タイムスタンプ前の指定された時刻から、タイムスタンプ後の指定された時刻までに収集された情報を要求します。タイムスタンプとは、アラートを生成したイベントの発生時刻です。[標準] を選択すると、Endpoint Security アプライアンスは、イベント前後のすべてのデータについてホストからの情報を要求します。

Endpoint Security ユーザーが特定の日時に基づいてトリアージ収集を要求すると、エージェントはアラート前後の指定された期間の情報を返します。タイムスタンプ設定は、トリアージ収集期間の長

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

さを制御します。タイムスタンプ設定は、エージェント URL イベント (URL 監視イベント) およびレジストリキーイベント (レジストリキーイベント) にのみ適用されます。

[タイムスタンプ設定 (Timestamp Settings)] タブを使用して、情報が収集されるタイムスタンプ前後の時間の長さを指定できます。[タイムスタンプ設定 (Timestamp Settings)] の範囲は 0 ～ 86400 秒です。両方の設定のデフォルトは 600 秒です。

[自動トリアージ設定 (Automatic Triage Settings)] ページの [タイムスタンプ設定 (Timestamp Settings)] タブを使用して、情報が収集されるタイムスタンプ前後の時間の長さを指定できます。タイムスタンプとは、アラートをトリガーしたイベントの発生時刻です。

手順

1. 次のように移動する。 エンドポイントセキュリティ **Web UI**.
2. 選択 アドミン > トリアージ設定.
3. クリックします タイムスタンプ設定 のタブ 自動トリアージ設定 ページ
4. 情報が必要なタイムスタンプ前後の時間の長さを指定します。
5. 指定されたタイムスタンプより前の情報が必要な秒数を入力します。
6. タイムスタンプより後の情報が必要な秒数を入力します。
7. クリックします **Save** (保存).

> **注:**
> クリックすると、ページ上のすべての値をデフォルト設定に戻すことができます デフォルト値にリセットをクリックし、[保存] をクリックします。

- 取得スペースエリア:取得ページには、取得用に残っているディスク容量が表示されます。
- 取得のディスク使用制限の設定:
  - トリアージ、ファイル取得、およびデータ取得は時間の経過とともに累積し、使用するディスクスペースが増加します。これを制御するために、一定量のディスクスペースを割り当てることができます。指定したディスクスペースの 10% が自動トリアージ取得用に予約されます。割り当てられた取得スペースの合計を超えると、最も古い自動トリアージが削除されます。
  - 完了した取得の合計ディスクサイズが指定された制限を超えると、Endpoint Security アプライアンスは、合計が指定された制限を下回るように十分なディスクスペースがクリアされるまで、完了した取得を最も古いものから削除します。まだ完了していない取得は影響を受けません。
  - アドミン、アナリスト、または調査担当者が Endpoint Security Web UI を使用して関連付けられたエージェントを手動で削除すると、Endpoint Security アプライアンスは取得を自動的に削除します。

  Web UI を使用して完全な取得のディスク使用制限を設定するには：
- **Endpoint Security Web UI** に移動します。
- 選択 ディスク使用率の制限 から アドミン 関連付けます
- 関連エントリフォームで、 取得スペース制限 エリアで、トリアージ、ファイル、およびデータの取得を保存するために使用できるディスクスペースの最大量 (GB 単位) を指定します。有効な

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

値とデフォルトは、Endpoint Security アプライアンスモデルによって異なります。モデルに適した値が [ディスク使用制限 (Disk Utilization Limits)] ページに表示されます。

- クリックします **Save** (保存).

> **注:**
> 上記のすべての設定が優先されるため、失敗またはエラーが発生した場合、Now Platform はそれらのエラーを返すだけです。

統合用のアプリケーションのインストールとソースの構成

Now Platform インスタンスで ServiceNow Store からアプリケーションをインストールして設定します。

始める前に
必要なロール：NowPlatform アドミン (admin)

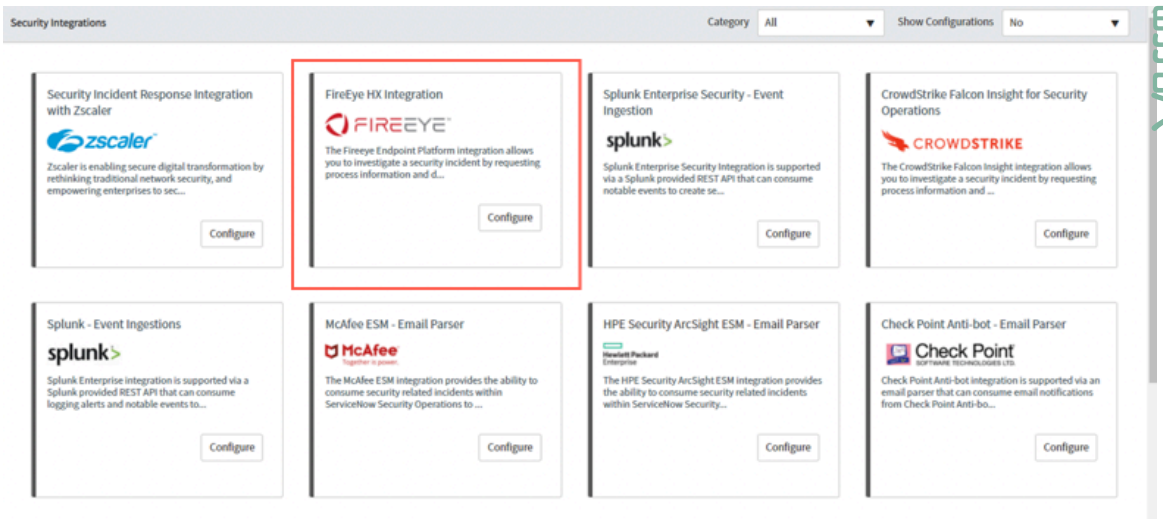
> **注:**
> ソースを構成するには、アクティブな MID サーバーが必要です。

ServiceNow Store から FireEye HX アプリケーションとのセキュリティインシデントレスポンス統合をダウンロードしてインストールします。

アプリケーションを正常にインストールしたら、以下の手順に従って構成します。

手順

1. 次のように移動する。 統合 > 統合設定.
2. [統合設定 モジュールを使用して利用可能な統合を表示し、 **FireEye** 選択します。

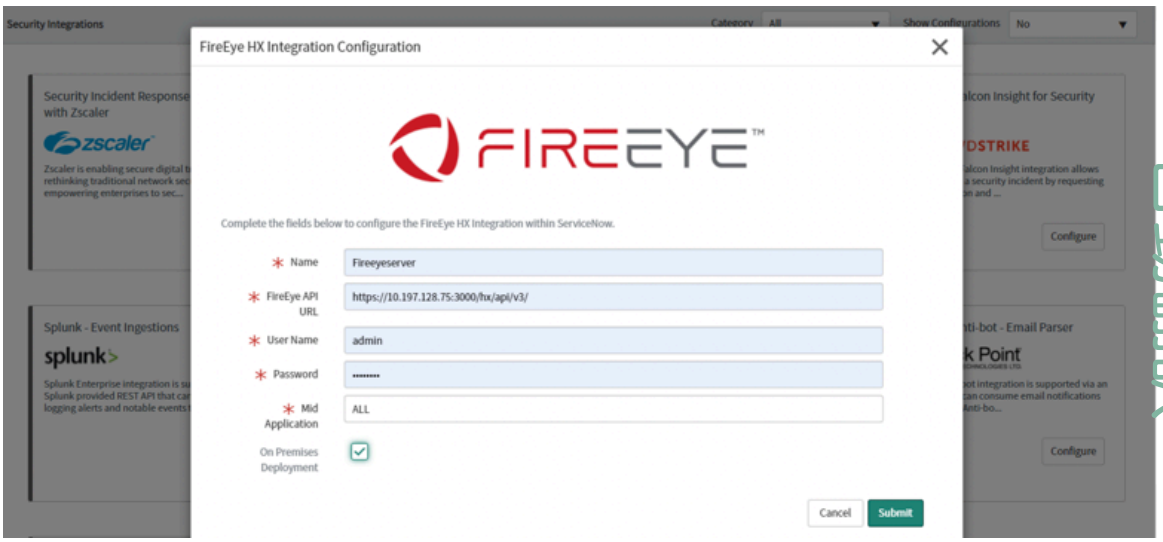


3. クリックします 構成 FireEyeタイル上。
4. FireEye 統合を設定するには、次の詳細を入力します。

フィールド	説明
名前	FireEye 構成の名前。この名前は、ソースと関連する認証情報および構成を識別するために使用されます。この名前は、認証情報とアカウントを区別して各ソースを識別し、プロファイルとの競合を回避するのに役立ちます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
API URL	FireEye API をホストするベース URL。
ユーザー名	FireEye アカウントのユーザー名を入力します。
パスワード	FireEye アカウントのパスワードを入力します。
MID アプリケーション	環境に設定されている MID アプリケーション。一部の拡張機能の zip ファイルを処理するには、MID サーバーが必要です。デフォルトでは [すべて] になります。ユーザーは有効なアプリケーション名を手動で入力する必要があります。
オンプレミス展開	デフォルトでは無効になっています。クラウドベースバージョンの FireEye を使用している場合は、チェックボックスがオフになっていることを確認します。

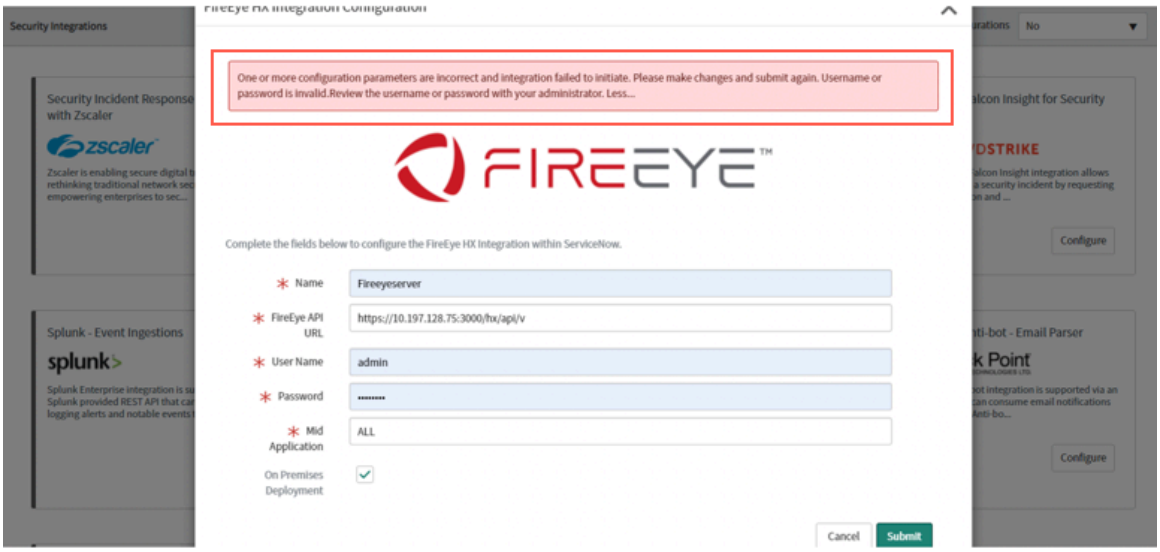


自動翻訳

5. クリックします 送信.
   新しい設定レコードを含む FireEye 構成リストが表示されます。これで FireEye サーバーの構成が完了しました。FireEye に接続できない場合、または認証情報が間違っている場合は、次の図に

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

示すように検証エラーメッセージが表示されます。認証情報が正しいことを確認して、再試行してください。



FireEye のデフォルト設定

インストール完了後の追加の構成設定は次のとおりです。

インストールが完了すると、左側のナビゲーションに [FireEye のデフォルト設定] モジュールが表示されます。これには、さまざまな FireEye 機能のデフォルト設定が含まれています。

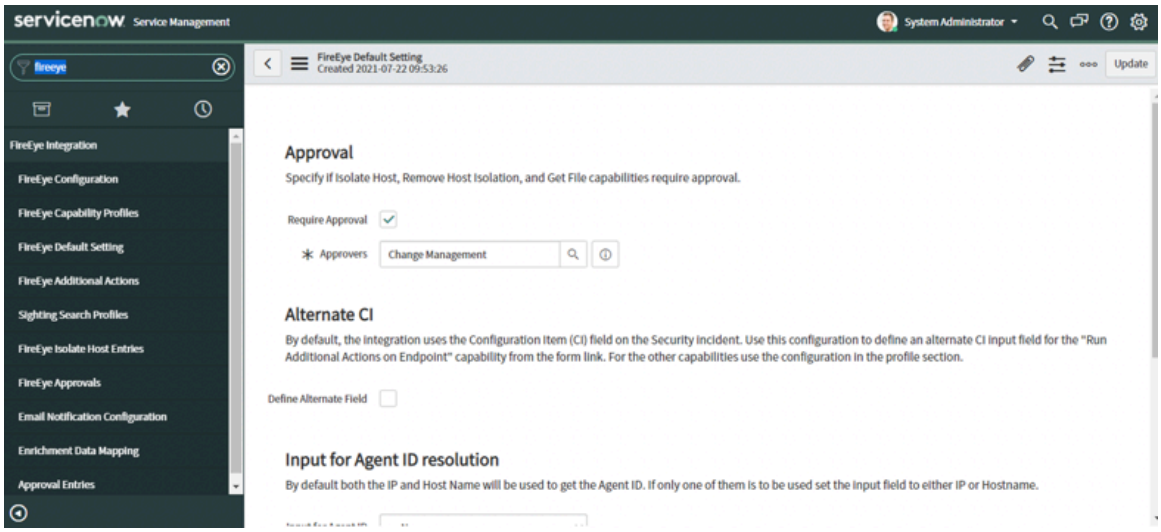
追加の構成

追加の構成設定は次のとおりです。

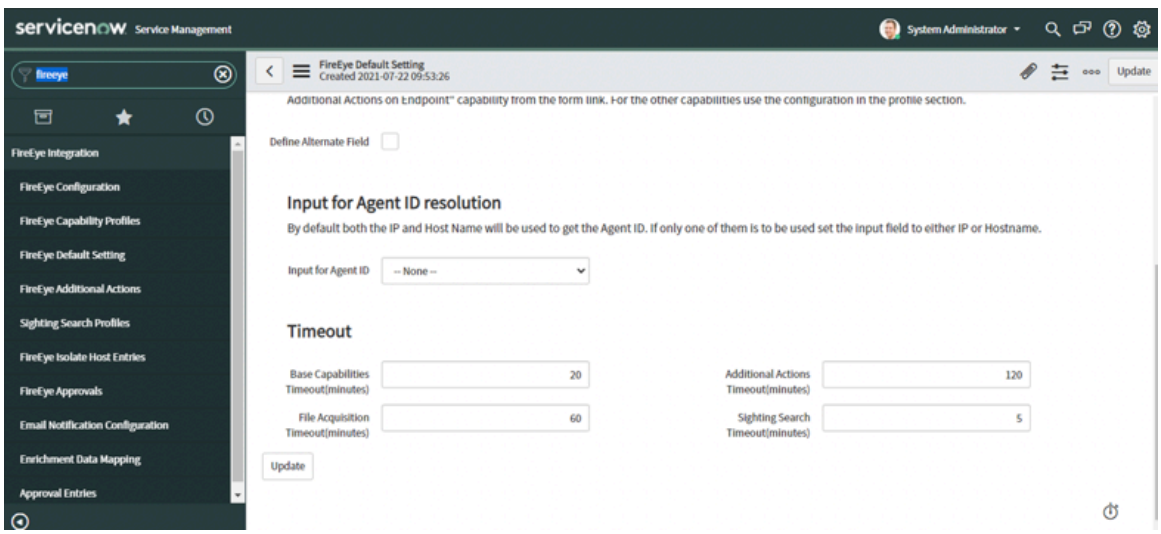
1. 承認:この承認は、特に [ホストを隔離]、[ホスト隔離削除]、および [ファイルを取得] 機能が関連リストから直接トリガーされ、それらのプロファイルがない場合に適用されます。これらの機能の既存のプロファイルがある場合、プロファイルの承認構成が優先されます。
   - 承認が必要: [承認が必要] を有効にすると、フォームで [承認者] フィールドが使用可能になります。
   - 承認者:承認者グループのリスト。要求が送信された後、要求を完了するにはグループからの承認が必要です。
2. 代替 **CI**:このチェックボックスを有効にすると、代替 CI を機能に渡すために使用できるフィールドのリストが表示されます。デフォルトでは、統合はセキュリティインシデントの構成アイテム (CI) フィールドを使用します。この構成は、[エンドポイントで他のアクションを実行] 機能にのみ適用されます。したがって、この構成は、[エンドポイントで他のアクションを実行] 機能の代替 CI 入力フィールドを定義するためにのみ使用します。その他の機能については、プロファイルセクションの設定を使用します。プロファイルで代替 CI が定義されていない場合、機能は [セキュリティインシデント] フォームの [CI] フィールドを選択します。
3. エージェント **ID** 解決の入力:デフォルトでは、IP とホスト名を使用してエージェント ID を取得します。いずれか一方のみを使用する場合は、入力フィールドを [IP] または [ホスト名] に設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. タイムアウトには以下も含まれています。
   - 基本機能のタイムアウト (分): 設定された時間内に応答がない場合、拡張、ホストの隔離、およびホスト隔離削除の機能は失敗します。
   - 追加アクションタイムアウト (分): 設定された時間内に応答がない場合、エンドポイント機能での追加アクションの実行機能は失敗します。
   - ファイル取得タイムアウト (分): 設定された時間内に応答がない場合、ファイル取得機能は失敗します。
   - サイティング検索タイムアウト (分): 設定された時間が経過すると検索が停止されます。



FireEye Endpoint 統合の新規機能プロファイルの作成

プロファイルを作成し、そのプロファイルで実行する FireEye HX 機能を選択します。

始める前に

必要なロール：NowPlatform セキュリティインシデントアドミニストレーター (sn_si_admin)

このタスクについて

プロファイルは機能に合わせて作成され、アナリストが簡単に調査/修復を行うのに役立ちます。

プロファイルに追加できる機能のリストは次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. ホストの詳細を取得
2. ログオンユーザーを取得
3. ネットワーク統計情報を取得
4. 実行中プロセスを取得
5. 実行中のサービスを取得
6. ファイルを取得
7. ホストを隔離
8. 隔離を削除

プロファイルの作成中に、[ファイルの取得]、[ホストの隔離]、[ホスト隔離削除] の機能を他の機能と結合することはできません。これらのプロファイルは個別に作成する必要があります。一方、[システムの詳細を取得]、[ログオンしているユーザーを取得]、[ネットワークステータスを取得]、[実行中のプロセスを取得]、および [実行中のサービスを取得] は一緒に使用できます。プロファイルは個別に作成することも、必要に応じてすべてまたは一部を組み合わせて作成することもできます。一度プロファイルに含まれた機能は、別のプロファイルに含めることはできません。

新規機能プロファイルを作成するには、次のステップに従います。

手順

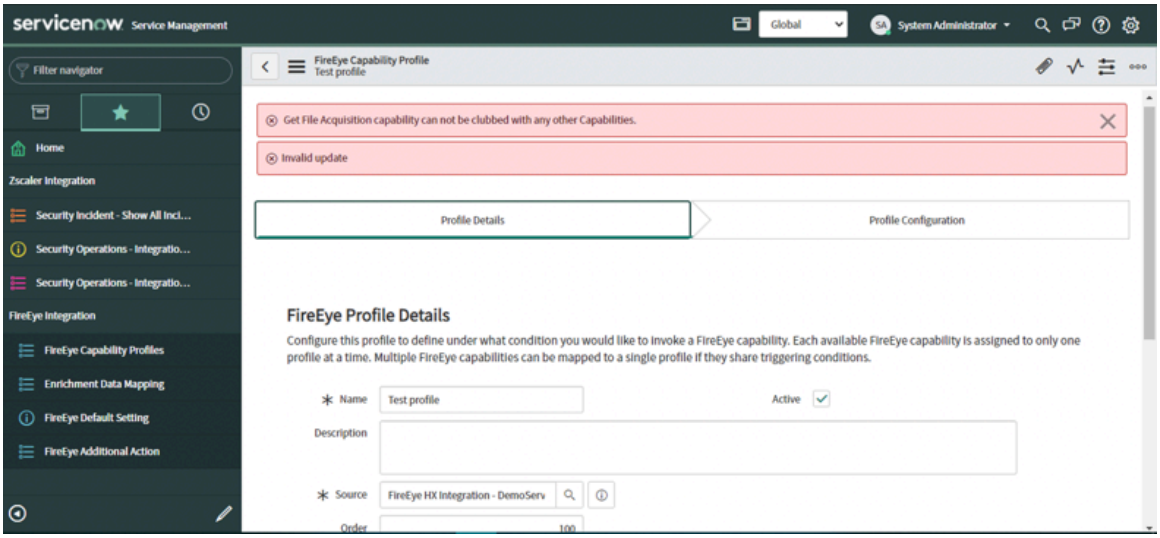
1. 次のように移動する。 **FireEye** 統合 > **FireEye** 機能プロファイル.
   機能プロファイルのリストが表示されます。
2. クリックします 新規.
3. フォームの各フィールドに入力します。

名前	FireEye HX 機能プロファイルの名前。この名前は、プロファイルタイプを識別して説明するのに役立ちます。
説明	プロファイルをさらに説明する、プロファイルに関する追加情報。
ソース	FireEye HX ソースの名前。選択リストからは、設定されたソースのみを使用できます。
FireEye HX の機能	FireEye HX プロファイルの機能。このプロファイルの機能を [利用可能] 列から選択し、それを [選択済み] 列に移動します。
順序	フロー優先度。デフォルトは 100 です。このフィールドの値は、2 つ以上のプロファイルがトリガー条件を共有する場合にフローが実行される順序を示します。 番号が最も小さいフローの優先度が最も高くなります。 操作の順序を設定するには、値を入力します。例：100、200、300、400。
アクティブ	これは、プロファイルがアクティブであることを示しています。プロファイルがアクティブに

自動翻訳

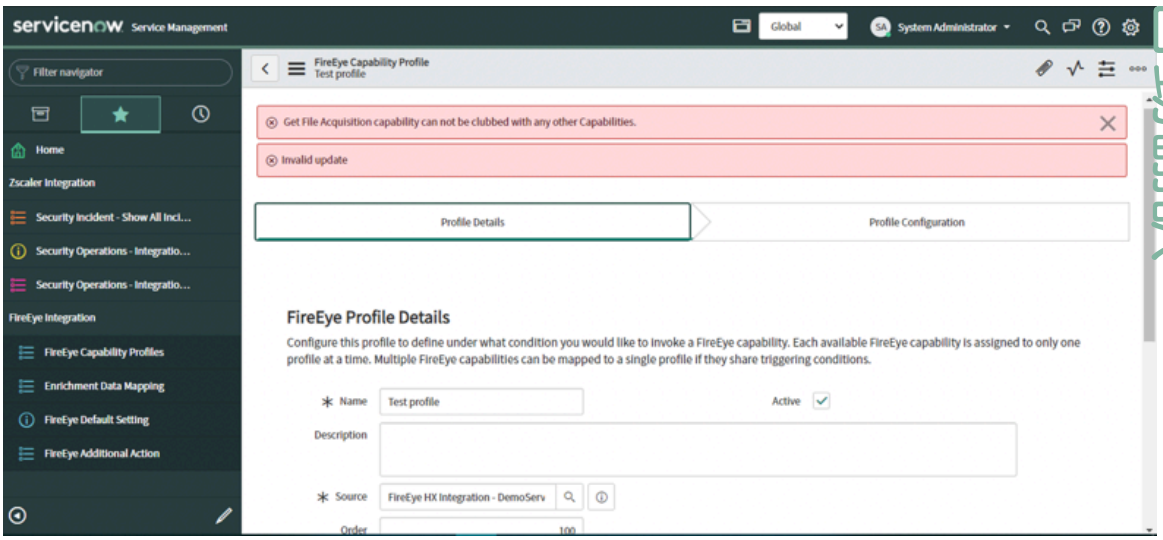
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

	なると、構成で指定したフィルター条件に一致するセキュリティインシデントが作成されたときに、自動的にトリガーされます。



次の図は、[ホストの詳細を取得] 機能を備えたプロファイルの詳細の完成したフォームの例です。

4. クリックします 次 プロファイル設定に進みます。



自動翻訳

注:
[ホストの隔離]、[ホスト隔離削除]、[ファイルの取得] の機能を他の機能と結合することはできません。

次のタスク

次のステップは、プロファイルを設定することです。プロファイルの設定を構成する前に、プロファイルとトリガー条件の構成の概念を確認することをお勧めします。詳細については、「Understand how trigger conditions work with a configuration item for a profile (プロファイルの構成アイテムに対するトリガー条件の作用の理解)」を参照してください。

構成アイテムに対するトリガー条件の作用の理解

プロファイルを作成し、そのプロファイルで実行する FireEye 機能を選択したら、一連の特定の条件が満たされた場合にのみ実行されるようにプロファイル設定を構成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

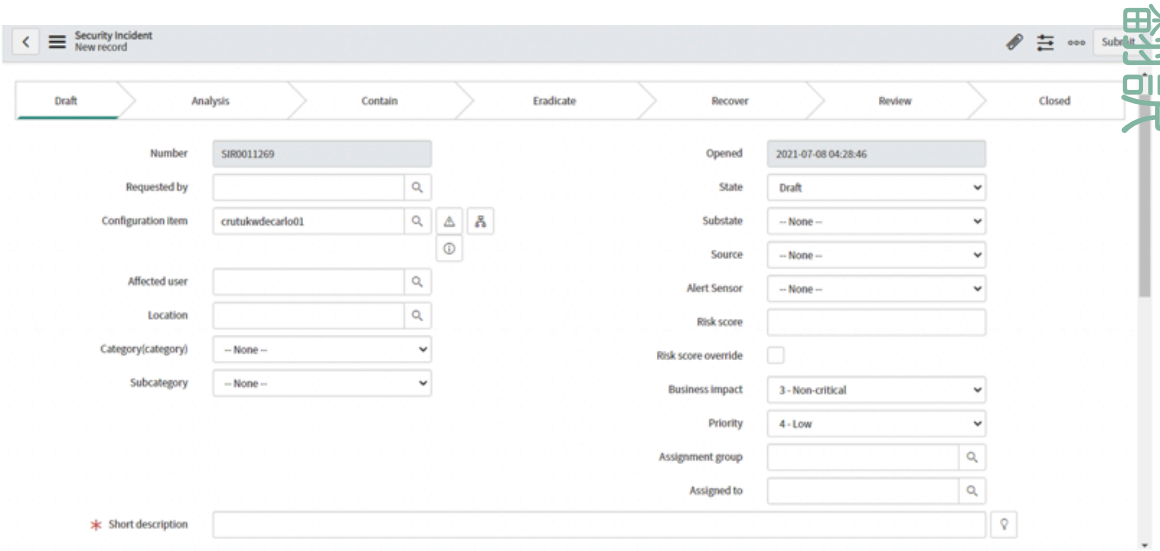
トリガー条件を設定して、トリガー条件に一致するセキュリティインシデントが作成されるたびにプロファイルが自動的に実行されるようにすることができます。トリガー条件が設定されていない場合は、セキュリティインシデントの [EDR プロファイルを実行] フォームをクリックしてプロファイルを選択することで、これらのプロファイルを手動で実行できます。

デフォルトでは、統合はセキュリティインシデントの構成アイテム (CI) フィールドを使用します。この値は、資産の ID を Now Platform CMDB に格納されている情報と照合するために使用されます。セキュリティインシデントが作成され、プロファイルが自動または手動で実行されると、CI フィールドの値に基づいて CMDB が検索され、ホスト名や IP アドレスが取得されます。ホスト名や IP は、FireEye HX でエージェント ID を解決してエンドポイントを識別するために使用されます。

理想的には、一致する値がデータベースで見つかり、一致する資産に関して FireEye HX コンソールからデータが収集されます。さまざまな機能のデータが Now Platform インスタンスにプルされ、セキュリティインシデントの関連リストに表示されます。セキュリティインシデントの構成アイテム (CI) フィールドにホスト名、またはデータベースと一致する IP アドレスが入力されていない場合は、セキュリティインシデントでホスト名または IP のいずれかを含む代替フィールドを選択して、エージェント ID の解決を実行できます。

プロファイルセットアップの構成手順では、エンドポイント識別用の代替 CI フィールドを選択して、FireEye HX でエンドポイントを識別できるようにすることができます。作成したカスタムフィールドを含む、セキュリティインシデントの任意のフィールドを代替 CI トリガーフィールドとして選択できます。この代替 CI フィールドをバックアップとして選択することで、インシデントの作成時に、関連するセキュリティインシデントに CI フィールドが設定されていない場合でもプロファイルが実行されるようにします。

注:
代替 CI フィールドは、プロファイルに追加できる機能に対してのみ考慮されます。すべての追加アクションでは、デフォルト設定ページから代替 CI が選択されます。



FireEye HX統合のためのプロファイルとセキュリティインシデントの構成

プロファイルを作成し、そのプロファイルで実行する FireEye HX 機能を選択したら、デフォルト条件でのみプロファイルを呼び出せるように設定を構成します。

始める前に
必要なロール：sn_si.admin

指定した条件が満たされた場合にのみ実行されるように機能プロファイルを構成します。必要に応じて構成アイテム (CI) フィールドの代替入力フィールドを選択し、トリガー条件を満たすセキュリ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ティインシデントが作成されたときにプロファイルが自動的にトリガーされるようにフィルタリング条件を設定します。

> **注:**
> 以下に移動できます プロファイル設定 入力後にのみページを表示 プロファイルの詳細.

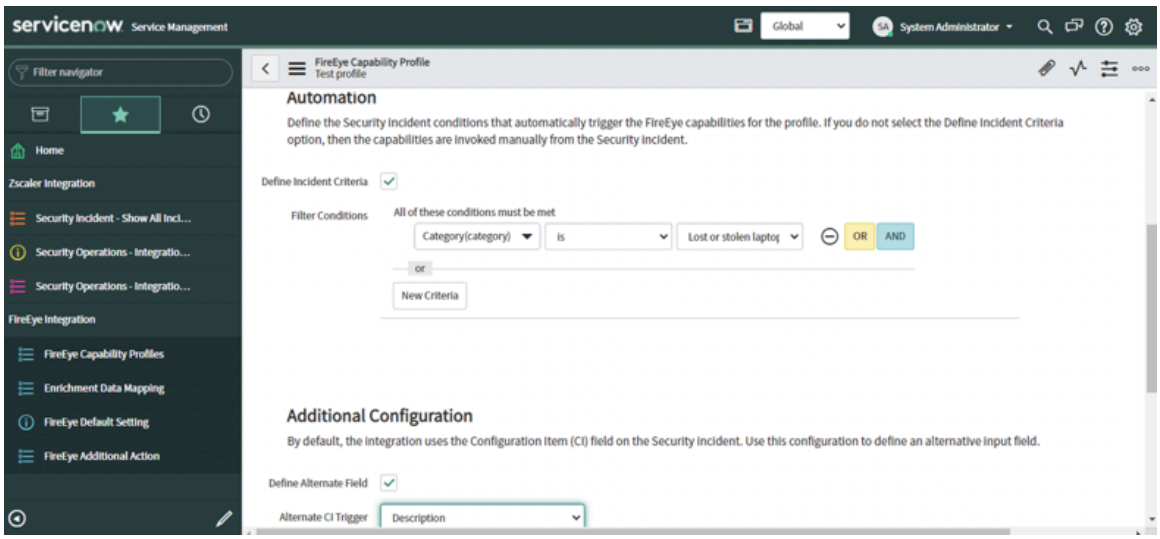
手順

1. 次のように移動する。 **FireEye** 統合 > **FireEye** 機能プロファイル.
2. クリックします 次 上の プロファイルの詳細 ページ ([プロファイルの詳細] セクションを完了した後)。
3. 次のセクションを確認して構成します。
   - [インシデント基準の定義] ([自動化] 内):プロファイルの FireEye HX 機能を自動的にトリガーするセキュリティインシデント条件を定義します。選択しない場合 インシデントクライテリアの定義 オプションを選択した場合、プロファイルと基本的な機能をセキュリティインシデントから手動で呼び出すことができます。
     - 選択 インシデントクライテリアの定義 プロファイルの FireEye HX 機能を自動的にトリガーするオプション。
     - 関連エントリフォームで、 フィルター条件で、必要なフィールドを選択します。
     - 次を追加できます: 新しいクライテリア また、ORまたはAND条件も定義します。

       > **注:**
       > [ホストを隔離]、[ホスト隔離削除]、[ファイルを取得] は自動的にトリガーされません。

   - 追加設定:セキュリティインシデントの構成アイテム (CI) フィールドにホスト名、またはデータベースと一致する IP アドレスが入力されていない場合は、セキュリティインシデントの代替フィールドを選択して、 FireEye HX API をクエリできます。
     - [代替フィールドを定義 代替入力フィールドを定義するオプション。
     - から入力フィールドを選択 代替 **CI** トリガーフィールド.

       > **注:**
       > 詳細については、「構成アイテムに対するトリガー条件の作用の理解」を参照してください。

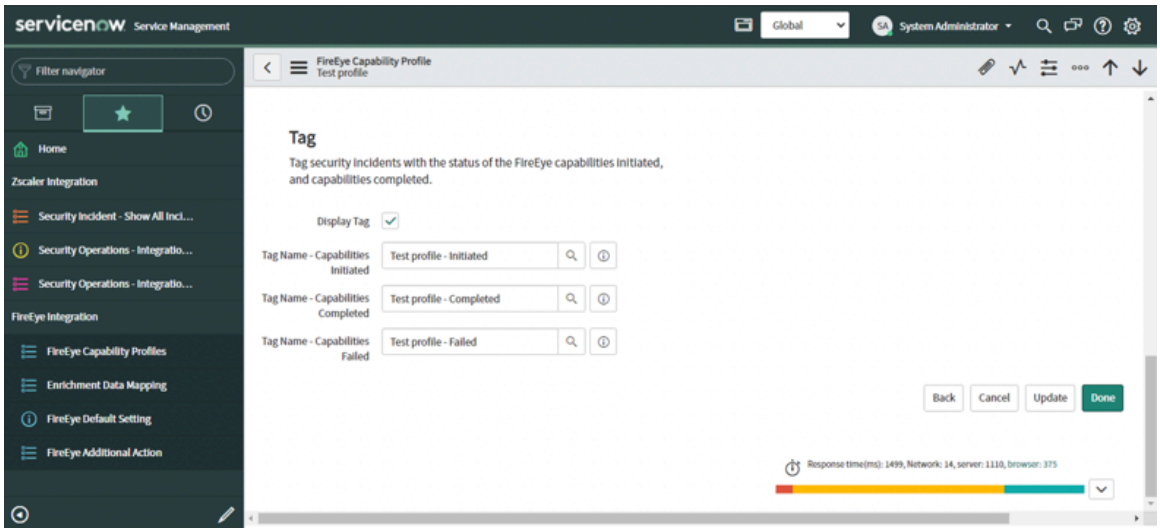


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

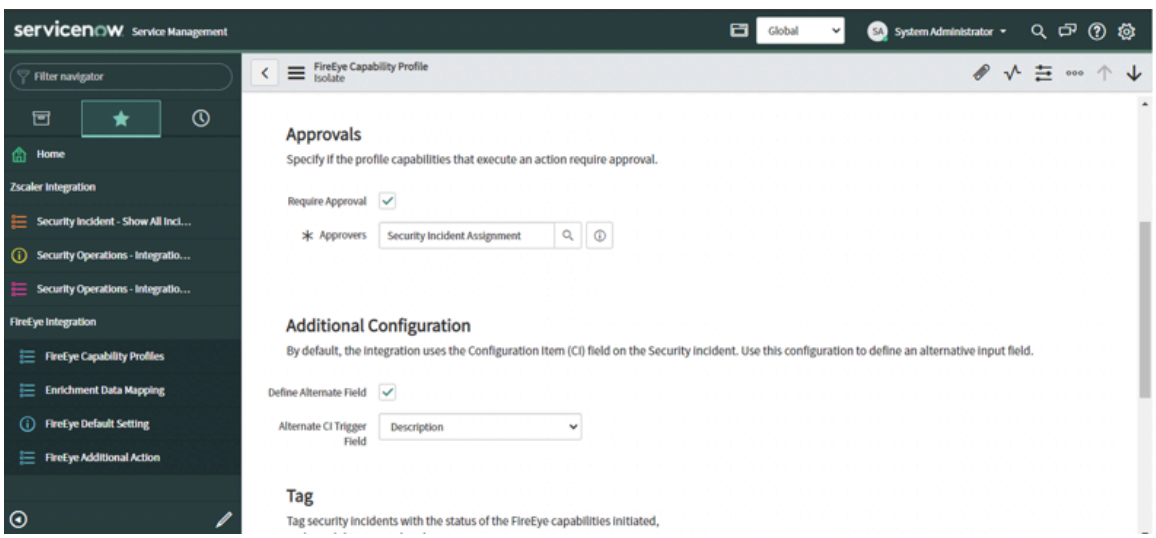
- タグ:オプションで、 FireEye HX プロファイル開始、プロファイル完了、およびプロファイル失敗のタグをセキュリティインシデントにタグ付けできます。

  [タグを表示 セキュリティインシデントのタグ付けを有効にするには、チェックボックスをオンにすると、タグが有効になるとプロファイル名がプリフィックスとして付きます。デフォルトでは、このオプションはすべてのプロファイルで無効になっています。



- 承認:次を選択します。 承認が必要 ホストマシンの隔離、ネットワークへの復元、ファイルの取得に FireEye HX 機能を使用するときに、追加レベルの制御を提供するチェックボックス。

  プロファイル構成の承認オプションは、[ホストを隔離]、[ホスト隔離削除]、[ファイルを取得] 機能に対してのみ表示されます。



4. [完了] をクリックします。
5. FireEye HX トリガー条件を確認します。

トリガー条件フィルターの確認

プロファイルをテストし、構成したトリガー条件フィルターが想定どおりに機能することを確認します。

始める前に
必要なロール：sn_si.admin または sn_si.analyst

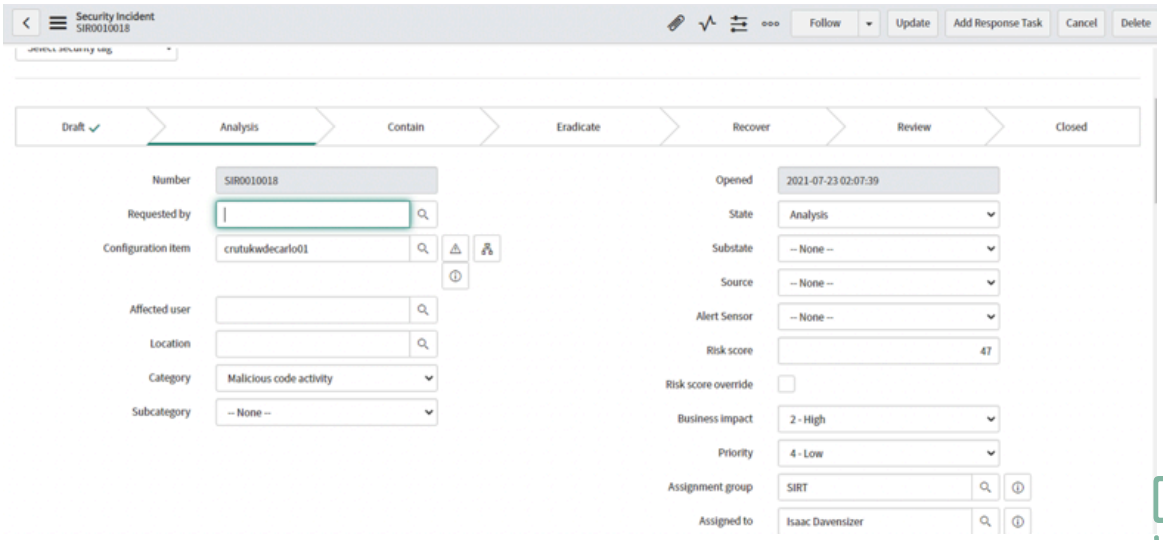
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

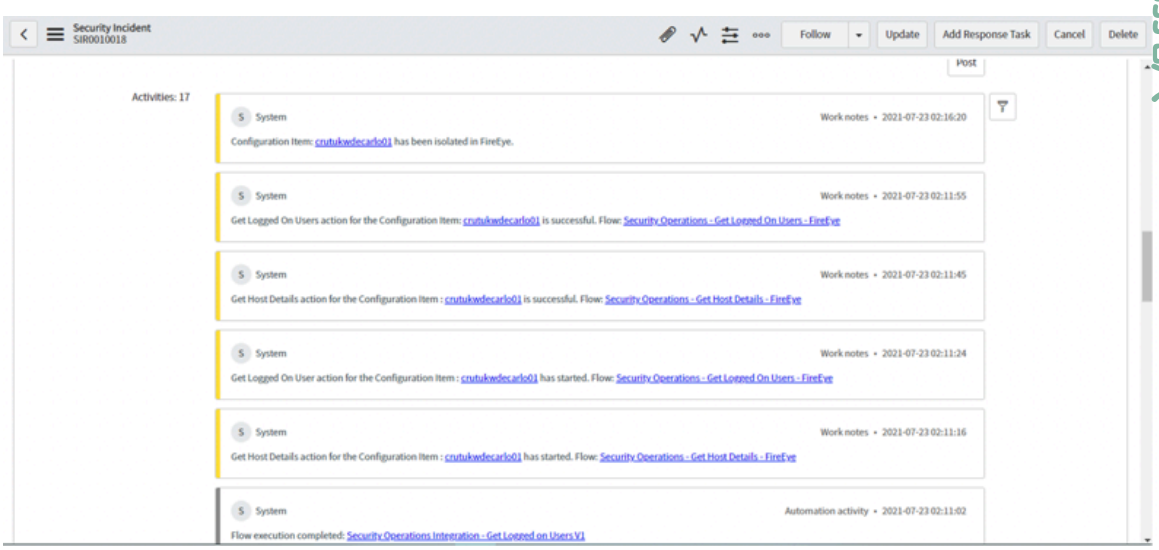
構成されたトリガー条件に基づいてプロファイルをアクティブ化すると、Now Platform セキュリティインシデントのクエリ結果を表示できます。

手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. 選択 新規 をクリックして、新しいセキュリティインシデントを作成します。
3. 機能プロファイルで指定されたフィルター条件を指定して、それぞれのプロファイルをトリガーします。



4. クリックします **Save** (保存).

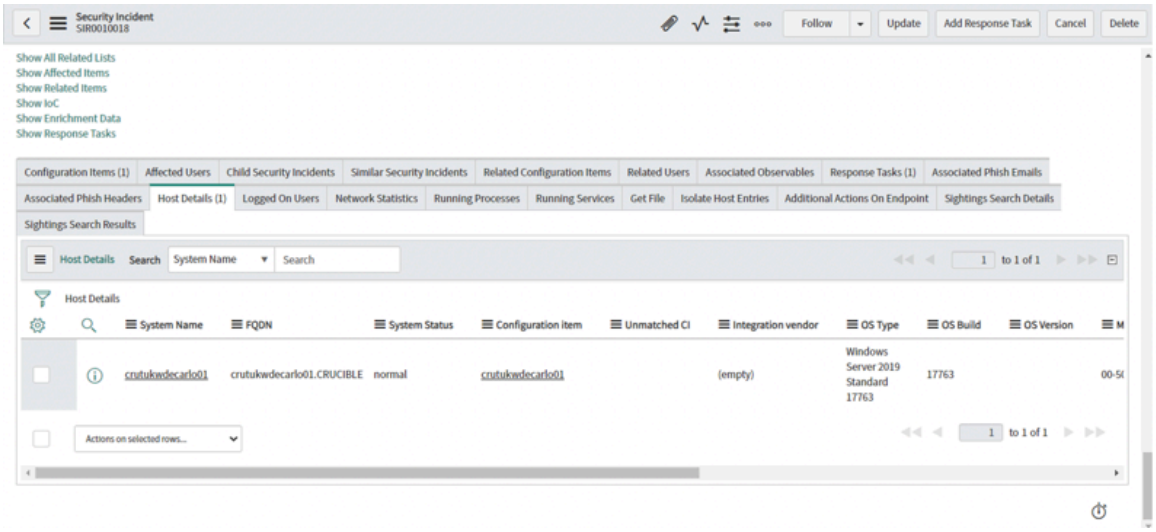


5. 作業メモセクションとアクティビティセクションを確認します。
6. プロファイル開始、プロファイル完了、またはプロファイル失敗のタグを表示します。
7. クリックします すべての関連リストを表示.
8. 任意の関連リスト (タブ) をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

たとえば、[ホストの詳細] です。



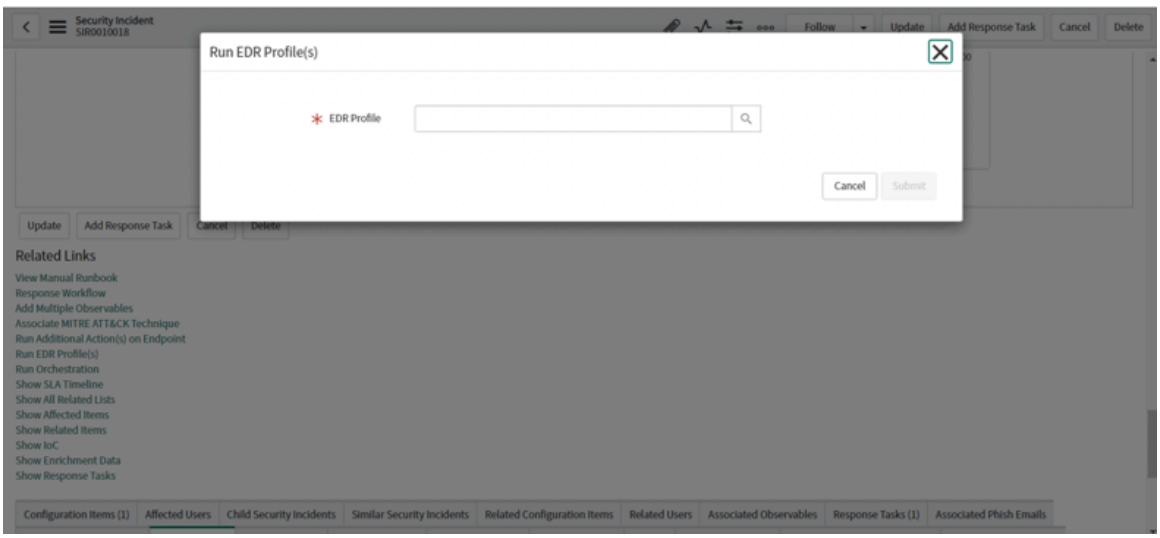
関連リンクから **FireEye** 機能プロファイルのトリガー

関連リンクからセキュリティインシデントを確認した後、機能プロファイルを手動でトリガーします。

始める前に
必要なロール：sn_si.admin または sn_si.analyst

手順

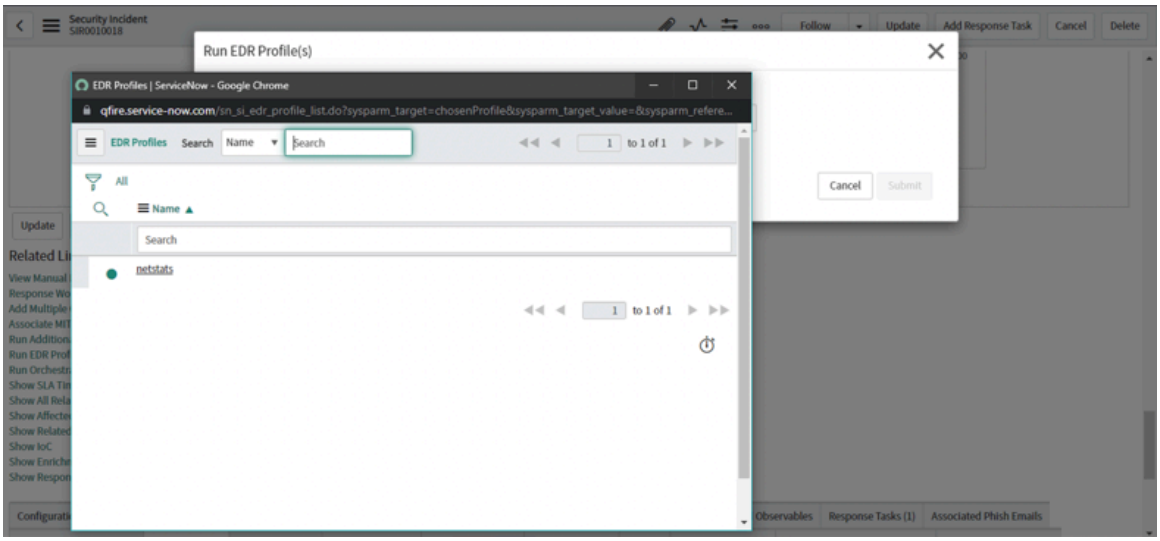
1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. 確認するセキュリティインシデントを選択します。
3. クリックします **EDR** プロファイルを実行[関連リンク] セクション。

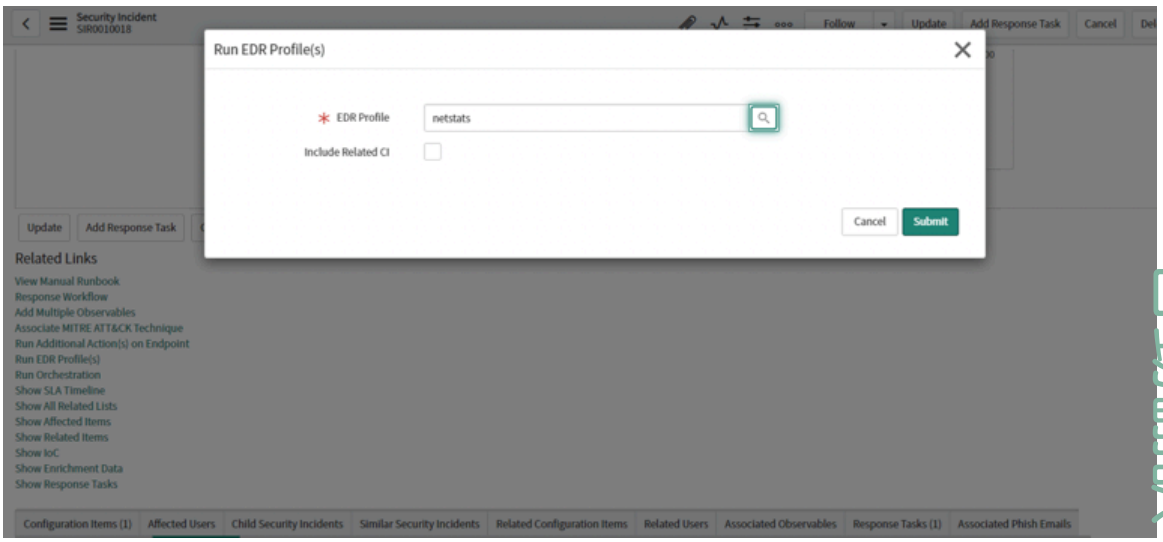


4. 利用可能なプロファイルのリストからプロファイルを参照して選択し、 送信.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。





5. 選択したプロファイルは手動でトリガーされます。
6. 作業メモセクションとアクティビティセクションを確認します。
7. タグを表示し、関連リストでデータを確認します。

> **注:**
> セキュリティインシデントの CI または代替 CI のプロファイルを実行することに加えて、ダイアログボックスの [関連 CI を含める (Include Related CI)] をオンにして、構成アイテム関連リストに存在する CI 値のプロファイルを実行することもできます。これにより、関連リストに存在する CI 値のデータもフェッチされます。または、関連リストに存在する CI 値に対してのみプロファイルを実行することもできます。

構成アイテム関連リストから **FireEye** 機能プロファイルのトリガー

構成アイテム関連リストから機能プロファイルを手動でトリガーします。

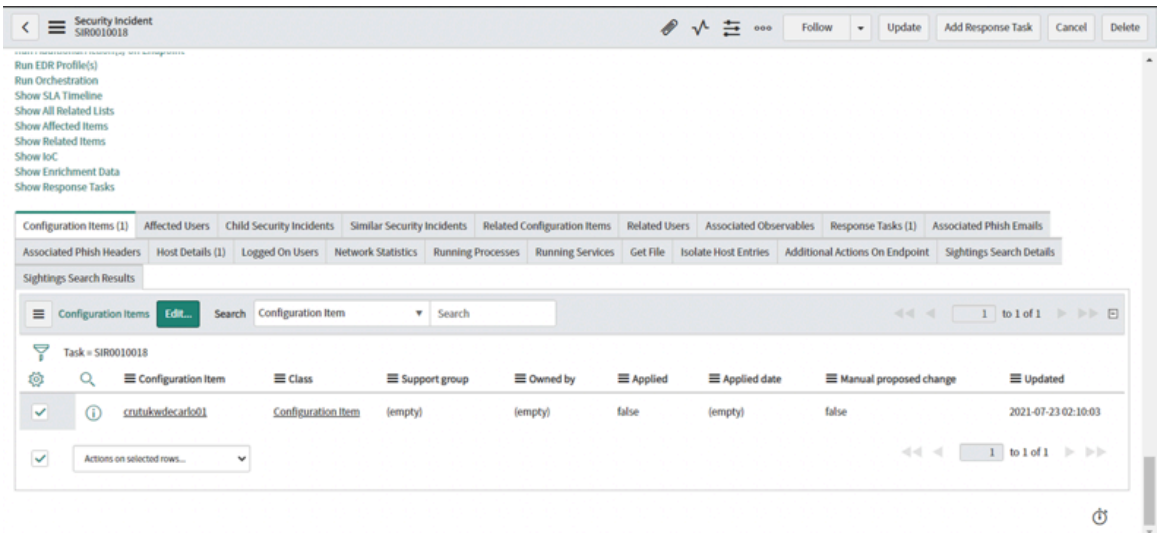
始める前に

必要なロール：sn_si.admin、sn_si.analyst

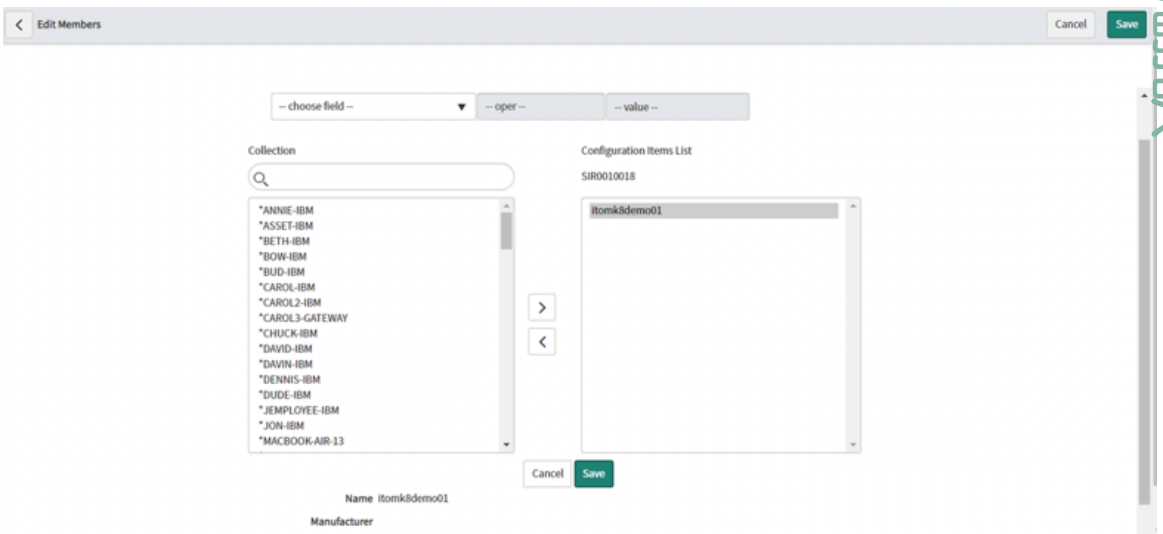
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. FireEye HX 情報で確認するセキュリティインシデントを選択します。
3. クリックします すべての関連リストを表示 [関連リスト] セクション。
4. バナーの 構成アイテム 関連付けられます



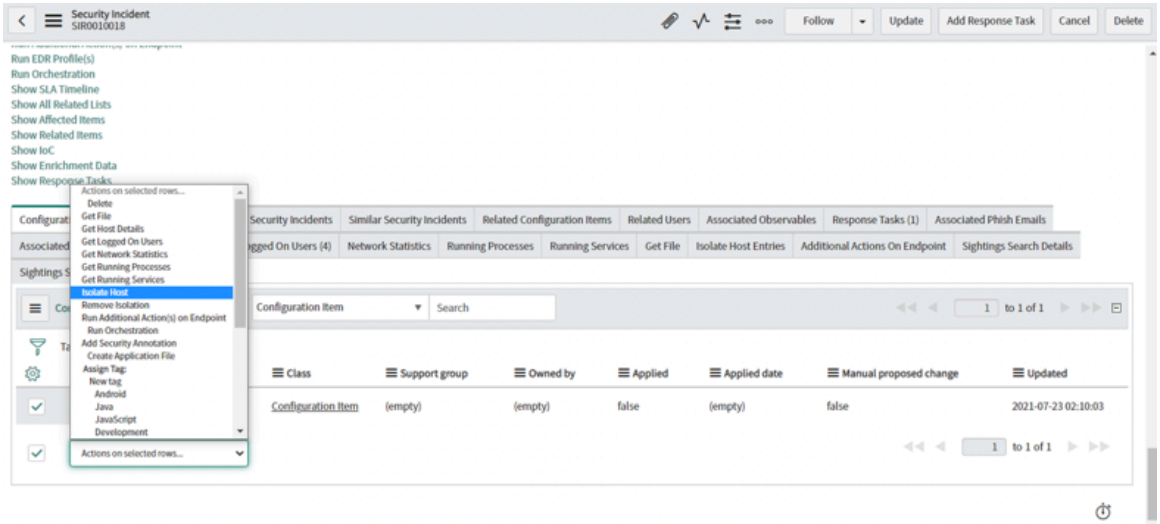
5. クリックします 編集 値がまだ存在しない場合に使用可能な構成アイテムを追加するには、 **Save** (保存).



6. 追加された構成アイテムを選択し、[選択した行のアクション] から機能を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



7. 選択した機能は手動でトリガーされます。
8. 作業メモセクションとアクティビティセクションを確認します。
9. タグを表示し、関連リストでデータを確認します。

FireEye の [ファイルを取得] 機能

ファイル取得要求は、ホストエンドポイントからファイルを取得するように Endpoint Security エージェントに指示します。ファイル取得は、潜在的な侵害または確認済みの侵害の静的または動的な分析、および内部の脅威調査中に証拠保持のために使用されます。[ファイルを取得] 機能は個別のプロファイルとして作成する必要があります。

始める前に
必要なロール：admin

[ファイルプロファイルを取得] をトリガーし、 FireEye HX 機能プロファイルを作成する ファイルを取得 要約機能を持たせたい場合も

手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. 確認するセキュリティインシデントを選択します。
3. クリックします **EDR** プロファイルを実行[関連リンク] セクション。
4. 利用可能なプロファイルのリストから [ファイルを取得] プロファイルを参照して選択します。
5. 次を指定します: ファイル名 AND ファイルパス.

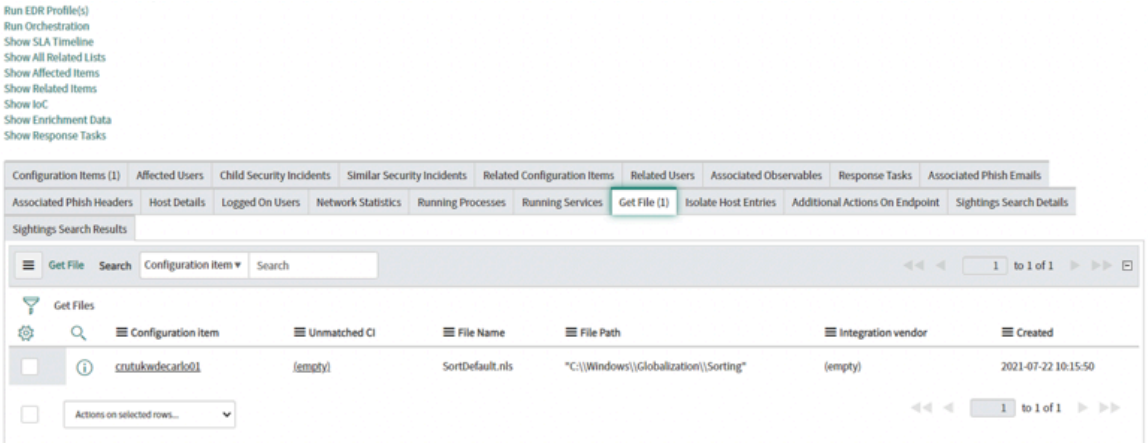
> **注:**
> 取得するファイルの名前を入力します。正確なパス名、または別の適切なパスベースの Windows 環境変数を指定します。ドライブ文字またはパス名を指定する必要があります。エンドポイントが異なると、ドライブマッピングが異なる場合があります。フォルダー名を明示的に指定する場合は、パスをバックスラッシュで終了できます。ただし、最後のバックスラッシュは必須ではありません。

6. クリックします 送信.
7. 作業メモセクションとアクティビティセクションを確認します。
8. タグを表示し、次で結果を確認します ファイルを取得 関連付けられます

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[ファイルを取得] プロファイルが手動でトリガーされるようになりました。



ダウンロードしたファイルの取得を確認するには:

- ファイル取得の .zip ファイルを開きます。
- ファイルを開くために必要なパスワードを入力します。パスワードは、FireEye HX コンソールのダウンロードリンクにカーソルを合わせると表示できます。パスワードを表示するには、以下の手順に従います。
  - FireEye HX コンソールにログインします。
  - 次のように移動する。 取得 取得タイプ - ファイルでフィルタリングします。
  - 目的のレコードを選択します。

    注:
    取得したファイルの詳細が右側のタブに表示されます。

  - [ダウンロード パスワードを取得するための上部にあるリンク。

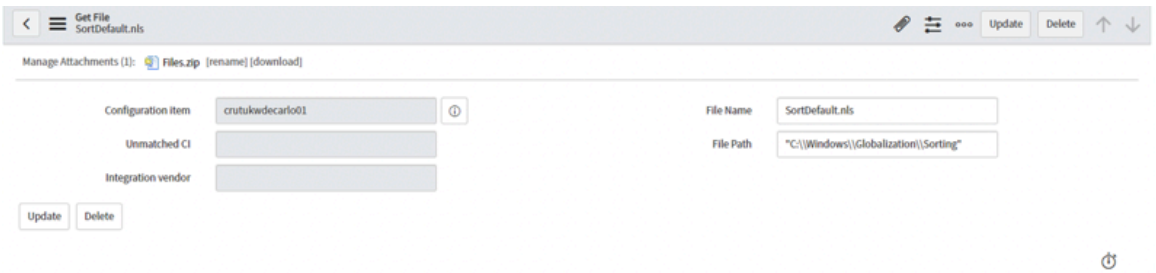
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

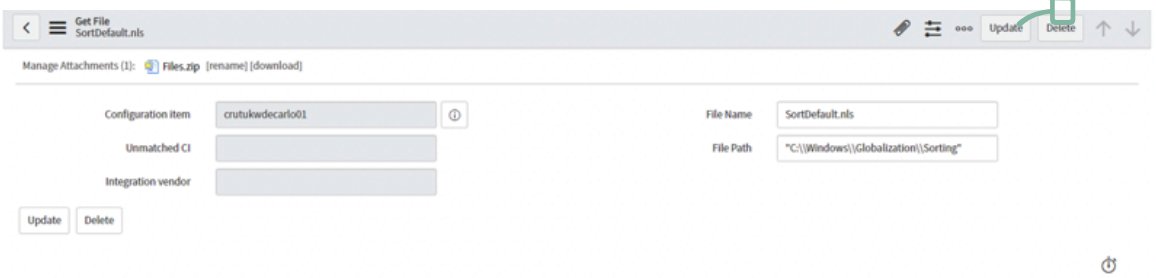
- テキストエディターまたは XML エディターを使用して、.zip ファイル内のファイルを開いて確認します。

  注:

  - 取得されたファイルは、セキュリティインシデントに対する証拠として追跡できるように、観測事象として手動で追加することをお勧めします。これは、将来、パスワードを忘れたときや変更したときにファイルを表示するのにも役立ちます。
  - [ファイルを取得] アクションでサポートされている最大ファイルサイズは 1024 MB で、この値は変更することで構成できます **com.glide.attachment.max_size**デフォルトのタイムアウトは 60 分で、[FireEye HX デフォルト設定] ページで設定できます。



  - [ファイルを取得] は、構成アイテム関連リストからトリガーすることもできます。



自動翻訳

FireEye のエンドポイントでの追加アクション

FireEye 統合は、ゴールドスタンダードのアクション以外に追加アクションの実行をサポートしています。

これらのアクションは、トリアージ取得とデータ取得で構成されます。デフォルト設定では、次の 2 つのデータ取得がサポートされています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 包括的調査の詳細スクリプト (Comprehensive Investigative Details Script)
- 標準調査の詳細スクリプト (Standard Investigative Details Script)

さらに、トリアージ取得も初期設定でサポートされています。これら 3 つはすべて、デフォルトでソースとともに作成されます。お客様は、FireEye の追加アクションモジュールからのデータ取得など、独自のアクションを作成することもできます。[1] FireEye の追加アクションでサポートされている最大ファイル サイズは 1024 であり、この値は変更することで構成できます **com.glide.attachment.max_size**デフォルトのタイムアウトは 120 分で、[FireEye のデフォルト設定] ページから設定できます。

包括的調査の詳細スクリプト **(Comprehensive Investigative Details Script)**

エンドポイントからすべてのフォレンジックアーティファクトおよび調査アーティファクトを収集できるようにしますが、これは非常にコストがかかるオプションです。この構成は、問題のエンドポイントからデータを収集するためのウィンドウが 1 つしかなく、後でより多くのデータを取得できることが保証されていない状況に最適です。したがって、このアクションは注意して使用してください。

標準調査の詳細スクリプト **(Standard Investigative Details Script)**

エンドポイントからフォレンジックアーティファクトおよび調査アーティファクトを収集するための最も一般的なオプションを有効にします。エンドポイントが侵害されている可能性があり、そのエンドポイントの詳細分析を実行する必要がある場合のプライマリ応答ツールとして使用されます。最も関連性が高く価値のあるデータを収集することと、さらに調査して必要なことが判明した場合は後で収集する可能性があるというコストのかかるオプションを回避することとのバランスを取ることを目的としています。

トリアージ取得

トリアージ収集には、ルックバックキャッシュ内の情報と、URL ダウンロード履歴、ファイルダウンロード履歴、プロセスとポートのリスト、標準システム情報などの追加のフォレンジック監査情報が含まれています。異常なネットワークトラフィックが検出され、エンドポイントアクションの可視化を高める必要がある場合に、このような情報を調べる場合があります。

FireEye でのデータ取得スクリプトの管理

データ取得要求 (ライブ応答要求とも呼ばれます) を使用すると、実行中の単一エンドポイントから必要なデータを取得できます。FireEye の [データ取得スクリプト (Data Acquisition Scripts)] ページを使用すると、データ取得要求に使用するデータ取得スクリプトを作成、編集、コピー、削除できます。

FireEye の [データ取得スクリプト **(Data Acquisition Scripts)]** ページへのアクセス

[データ取得スクリプト (Data Acquisition Scripts)] ページにアクセスするには：

1. [エンドポイントセキュリティ] Web ユーザーインターフェイスに移動します。
2. [管理] メニューの [データ取得スクリプト (Data Acquisition Scripts)] を選択します。

FireEye でのスクリプトの作成

データ取得スクリプトを作成するには：

1. 選択 データ取得スクリプト > アドミン エンドポイントセキュリティ Web ユーザーインターフェイスのメニュー。
2. クリックします スクリプトを作成.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. に新しいスクリプトの名前を入力します。 スクリプト名 示されます。
4. 必要に応じて、スクリプトの説明を入力します。
5. スクリプトを適用するオペレーティングシステムを選択します。[スクリプトを作成 (Create Script)] ダイアログで選択できるオペレーティングシステムは 1 つだけです。
6. クリックします 作成/挿入 をクリックして、スクリプト定義を開始します。
7. で取得データタイプを選択 取得タイプを追加ドロップダウンボックスをクリックし、 追加. 要求した取得タイプのオプションがスクリプトリストの右側に表示されます。
8. 取得タイプオプションの値を指定するか、既に選択されているデフォルト値を使用します。Web UI は、指定内のタブ、スペース、または不要な文字 (\n など) を警告したり削除したりしません。
9. 前の 2 つのステップを繰り返して、データ取得スクリプトの追加データを要求します。取得データタイプには、スクリプトで 1 回のみ使用できるものもあれば、複数回指定できるものもあります。スクリプトに取得タイプを追加した後、 取得タイプを追加ドロップダウンボックスは適切に調整されます。
10. スクリプトから取得データタイプを削除するには、ページの左側にある [取得] タブで [x] アイコン ( ) をクリックします。

> **注:**
> この統合ではサポートされていません 取得する前に編集を許可 スクリプト作成時のオプション。したがって、チェックボックスがオフになっていることを確認してください。

FireEye からのスクリプトのエクスポート

データ取得スクリプトを JSON ファイルにエクスポートできます。データ取得スクリプトをエクスポートするには：

1. 選択 データ取得スクリプト > アドミン エンドポイントセキュリティの Web ユーザーインターフェイスの
2. [管理] メニューの [データ取得スクリプト (Data Acquisition Scripts)] を選択します。
3. ページの左側で、エクスポートするスクリプトを選択します。
4. 選択 **Actions** (アクション) > スクリプトをエクスポート.
5. JSON ファイルがコンピューターにダウンロードされます。JSON ファイル名にはオペレーティングシステムが含まれているため、どのスクリプトがどのオペレーティングシステム用かを簡単に判断できます。

Now Platform での新しいデータ取得アクションの作成

新規アクションを作成するには、次のステップに従います。

1. 次のように移動する。 **FireEye** 統合 > **FireEye** の追加アクション. [FireEye の他のアクション] リストが表示されます。
2. クリックします 新規. 新しいアクションのフォームが表示されます。
3. フォームに記入します。

アクション名	実行される FireEye アクションの名前。この名前は、アクションタイプを識別して説明するのに役立ちます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

取得	取得では、分析するデータを取得します。これは読み取り専用フィールドで、デフォルトは [データ取得] です。
ソース	FireEye ソースの名前。選択リストからは、設定されたソースのみを使用できます。
機能	これは読み取り専用フィールドであり、[他のアクションを実行] 機能が設定されています。
取得タイプ	取得して分析する必要がある取得アクションのタイプ。
アクティブ	これは、アクションがアクティブであることを示します。
承認が必要	[承認が必要] オプションを有効にすると、フォームで [承認者] フィールドが使用可能になります。要求が送信された後、要求を完了するにはグループからの承認が必要です。
タグを表示	スクリプトを追加するための Windows、Mac、Linux などのオペレーティングシステムのタイプ。 **注:** 1 つのタイプの OS のみが現在サポートされています。オペレーティングシステムごとに 1 つのアクションを作成できます。他のオペレーティングシステムの場合は、必要に応じて新しいアクションを作成します。
スクリプト	選択した OS タイプに対して、FireEye からインポートされたスクリプトを指定する必要があります。各 OS タイプに追加できるスクリプトは 1 つだけです。

4. クリックします 送信.

セキュリティインシデントからのデータ取得のトリガー

作成された追加アクションは、 エンドポイントで他のアクションを実行 セキュリティインシデントで

注:
取得する前に編集を許可 FireEye 機能は、エンドポイントの追加アクションではサポートされていません。

FireEye 統合によるサイティング検索のプロファイルの作成と構成

次の手順を使用して、サイティング検索プロファイルを構成します。

始める前に

必要なロール：NowPlatform セキュリティインシデントアドミニストレーター (sn_si_admin)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソースが作成されるたびに、5 つのタイプ (ファイル、IP (v4)、MD5、SHA1、および SHA256) の個々のサイティング検索構成が作成され、デフォルトでは無効になります。サイティング検索を使用する前にアクティブにする必要があります。観測事象タイプごとに、サイティングを取得するための検索クエリが異なります。観測事象タイプごとに異なる検索を開始します。観測事象に対して AND 演算が実行され、結果が不正確になる可能性があるため、FireEye ではサイティング検索で複数の観測事象を検索できません。

注:
サイティング検索では、一度に 5 つのアクティブな検索のみが存在できます。残りはキューに入れられ、進行中のサイティングのいずれかが完了すると開始されます。

新しいサイティング検索プロファイルを作成する場合は、以下の手順に従います。

手順

1. 次のように移動する。 統合 > サイティング検索構成.
2. クリックします 新規.
3. フォームの各フィールドに入力します。

フィールド	説明
名前	機能プロファイルの名前。
保存された検索	保存された検索を実行します。つまり、[名前] フィールドは保存された検索の名前と一致している必要があります。
サイティング検索ソース	統合用に構成されたソースを定義します。
検索	クエリを形成するネイティブ検索文字列を追加します。
アクティブ	クエリは、アクティブになっている場合のみ実行されます。
観測可能タイプ	観測事象カテゴリのタイプを定義します。
検索あたりの最大観測事象の数	検索クエリが複数のクエリに分割される前の観測事象の数。この統合では、この値を 1 に設定します。
サイティング検索パラメーター	サイティング検索パラメーターを使用して、指定されたログストアでサポートされているロジックやその他の演算子を含むより複雑なクエリを定義します。

4. クリックします 送信 をクリックして構成を完了します。

セキュリティインシデントからのサイティング検索の呼び出し

以下の手順に従って、SIR セキュリティインシデントからサイティング検索を呼び出します。

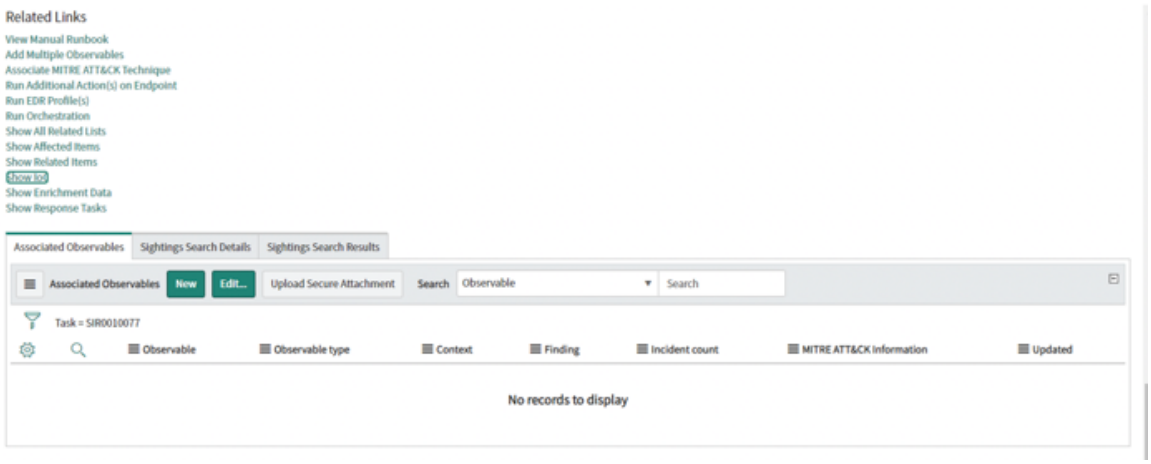
始める前に
必要なロール：Now Platform アドミン (sn_si_admin)

自動翻訳

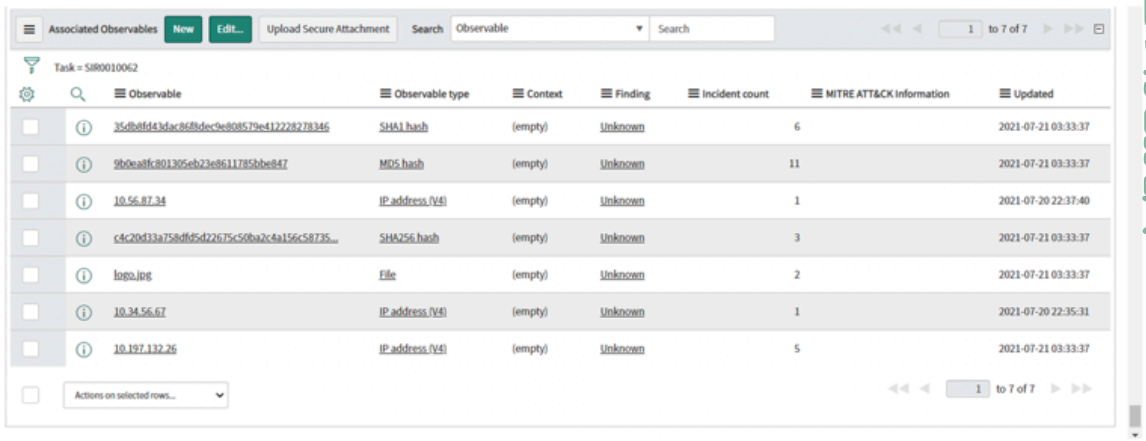
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

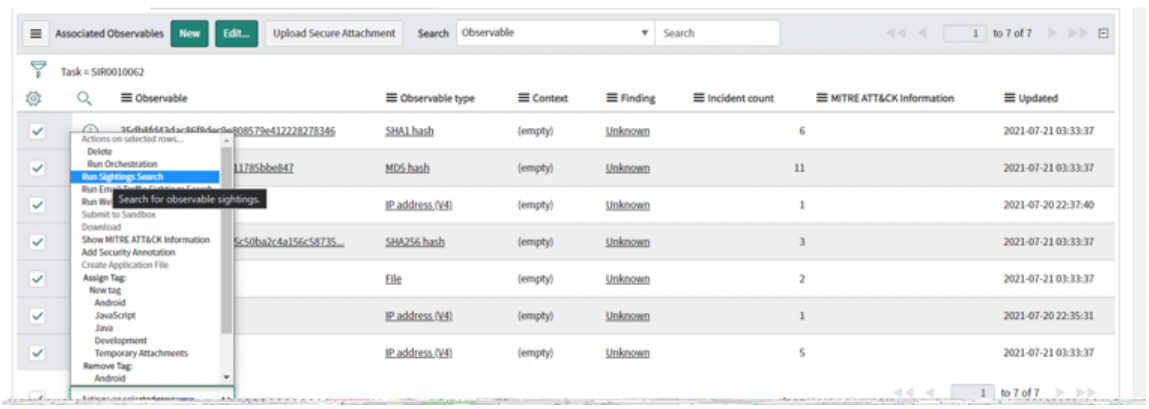
1. [セキュリティインシデント] に移動します。
2. 既存の SIR を開くか、新しい SIR を作成します。
3. [関連リンク] で [IoC を表示] をクリックします。
4. クリックします 関連する観測項目 関連リスト。



5. 既存の観測事象を追加するか、新しい観測事象を作成します。



6. 観測事象を選択し、[選択した行のアクション] から サイティング検索を実行.

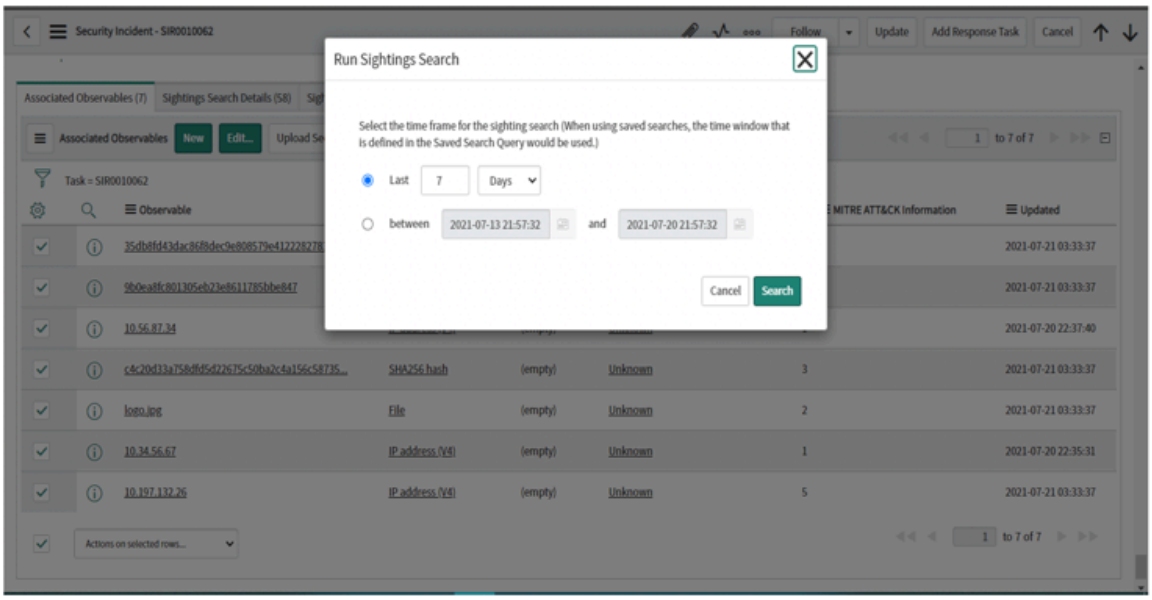


7. 時間データを要求する次のダイアログボックスの入力を無視します。

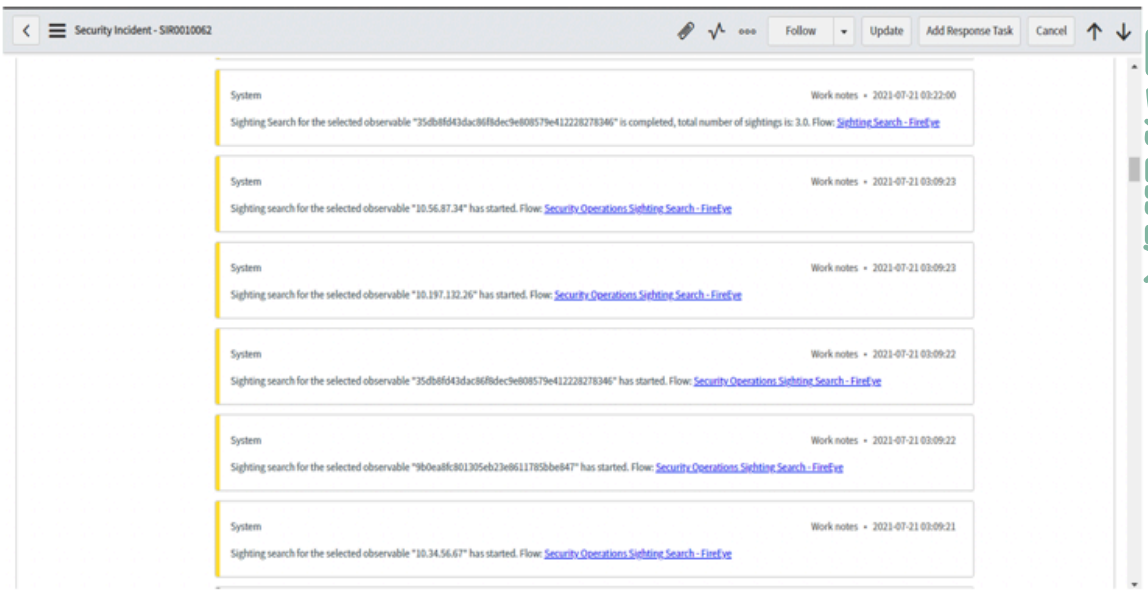
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

デフォルト値が設定されています。ただし、検索はリアルタイムで実行され、この統合では時間の値は無視されます。



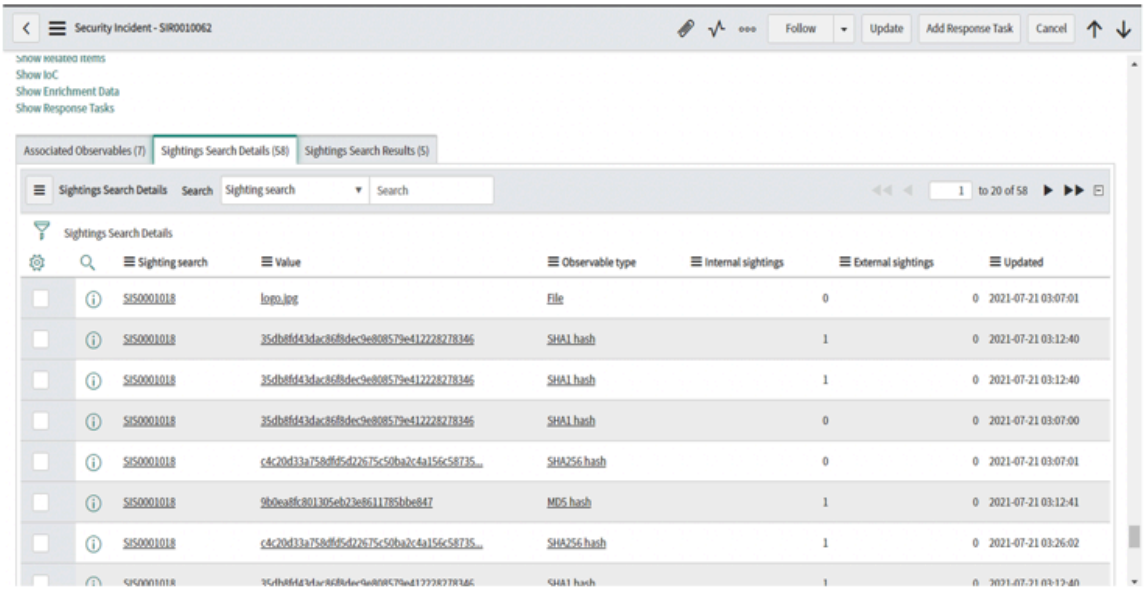
8. 作業メモでステータスを確認します。

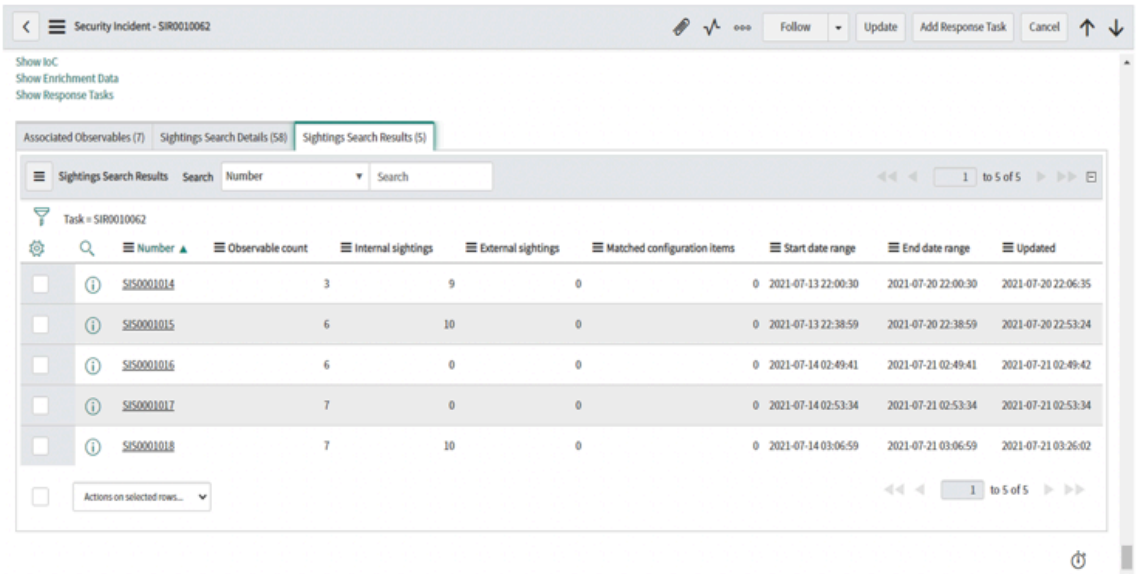


9. 検索が完了したら、関連リストで結果と詳細を確認します。

10. [サイティング検索の詳細 詳細のタブと サイティング検索結果 検索結果のタブ。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。





自動翻訳

Have I been pwned? の統合

セキュリティオペレーション Have I been pwned? 統合を使用すると、ドメイン名とメールアドレスのルックアップを送信して、データ漏洩によってユーザーの個人データが侵害されているかどうかを判断できます。

探索

セキュリティインシデントレスポンス の統合

セットアップ

- Security Operations Have I been pwned? 統合セットアップ
- Security Operations Have I been pwned? 統合のアクティブ化

使用

開発

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

観測事象のルックアップを実行する 脅威のルックアップ - Have I been pwned? フロー

- ServiceNow セキュリティオペレーション 統合開発のガイドライン
- 統合を作成するためのヒント
- 開発者トレーニング
- 開発者ドキュメント
- アプリケーションとともにインストールされているコンポーネントの検索

トラブルシューティングとヘルプ

- 統合のトラブルシューティング
- Security Operations Community で質問や回答をする
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

自動翻訳

Security Operations Have I been pwned? 統合セットアップ

Have I been pwned? は、データ漏洩によるオンラインアカウントの侵害または「pwned」(打ち負かされた) が原因でリスクにさらされている人がいるかどうかを評価するために使用される無料のリソースです。セキュリティオペレーション と簡単に統合できます。

Have I been pwned? 統合を使用する前に、プラグインをアクティブ化する必要があります。必要に応じて、X509 SSL 証明書を更新することもできます。

セキュリティオペレーション Have I been pwned? 統合を実装するには セキュリティインシデントレスポンス、脅威インテリジェンス、および セキュリティオペレーション Have I been pwned? プラグインが必要です。

脅威のルックアップ **- Have I been pwned?** フロー

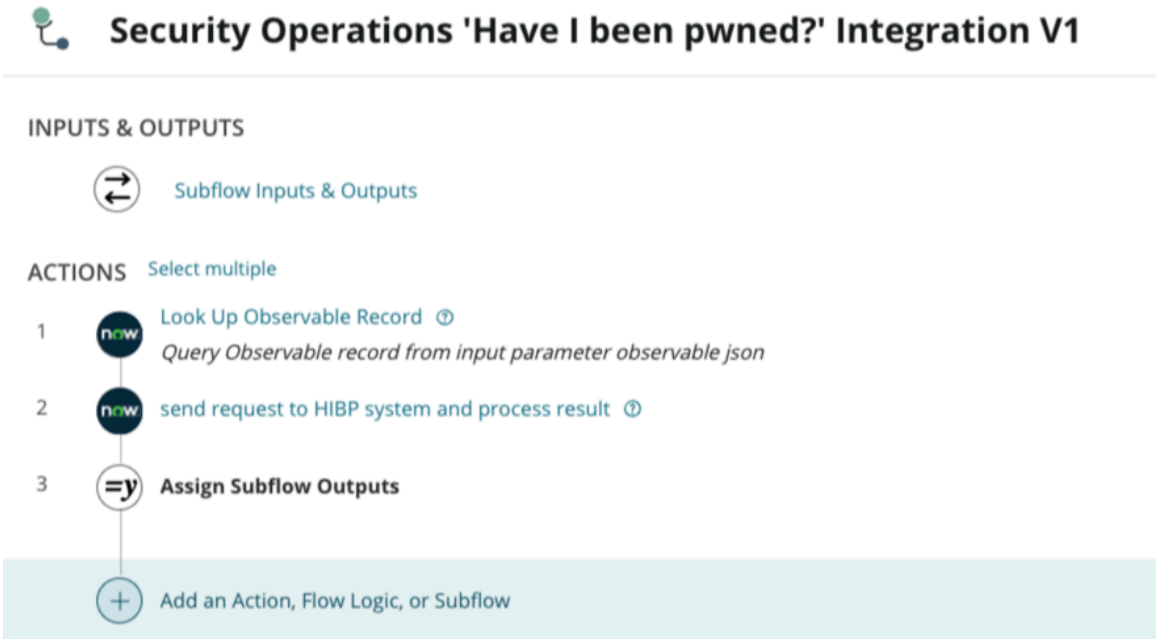
脅威のルックアップ - Have I been pwned? フローでは、選択された観測事象に対してルックアップが実行されます。観測事象が Have I been pwned? によって認識されるタイプである場合、観測事象でマルウェアがスキャンされ、結果が返されます。

必要なロール：sn_si_admin

このフローは、1 つ以上の観測事象で脅威のルックアップを実行し、Have I been pwned? の実装が選択されている場合に [Security Operations Integration - 脅威のルックアップ] 機能 でトリガーされます。詳細については、「観測事象のルックアップを実行する」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

「Have **I been** pwned」フロー



このフローで実行されるアクティビティについて、詳細は「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

Security Operations Have I been pwned? 統合のアクティブ化

統合構成機能を使用すると、セキュリティオペレーション Have I been pwned? 統合を含むサードパーティのセキュリティ統合をすばやくアクティブ化して設定できます。Have I been pwned? 統合を使用する前に、ServiceNow Store からダウンロードする必要があります。

始める前に

- セキュリティオペレーション Have I been pwned? 統合を使用する前に、脅威インテリジェンスプラグインをインストールしてアクティブ化する必要があります。

必要なロール：sn_si_admin

手順

から統合をダウンロードします ServiceNow Store.
この統合はオープン API をサポートしており、追加の構成は必要ありません。脅威インテリジェンス の観測事象およびセキュリティインシデントの観測事象でルックアップを実行するために、Have I been pwned? を選択できるようになりました。

関連情報

観測事象のルックアップを実行する

X.509 証明書の更新

統合に SSL 接続が必要な場合は、サードパーティベンダーによって提供された証明書が ServiceNow でまだ信頼されていないか、有効期限が切れていることがあります。このタスクはオプションです。

始める前に
必要なロール：admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. サードパーティベンダーから SSL 証明書を取得します。
   たとえば、次のように、Firefox ブラウザーの SSL エンドポイントから X.509 証明書 (PEM) をインポートできます。

   a. ブラウザーのアドレスバーにエンドポイント URL を入力します。
      例： https://<3rdparty>/。

   b. 住所のロックアイコンをクリックします。

   c. [詳細情報] をクリックし、[セキュリティ] タブをクリックします。

   d. [証明書を表示 **(View Certificate)]** をクリックし、[詳細] タブをクリックします。

   e. [エクスポート] をクリックして、PEM をローカルファイルシステムに保存します。

   f. 保存したファイルをテキストエディターで開き、内容をクリップボードにコピーします。
      -----BEGIN CERTIFICATE----- で始まり、-----END CERTIFICATE----- で終わる必要があります。

2. 次のように移動する。 システム定義 > 証明書.
3. [新規] をクリックし、統合の新規レコードを作成 します。
4. ダウンロードしてクリップボードにコピーした証明書を **[PEM** 証明書] に貼り付けます。
5. 証明書を ID プロバイダーレコードに追加します。
   a. 次のように移動する。 マルチプロバイダー **SSO** > **ID** プロバイダー.
   b. 新しい証明書を作成したアクティブなデフォルトの ID プロバイダーを選択します。
   c. **[X.509** 証明書] 関連リストまで下にスクロールし、[編集] をクリックします。
   d. 新しく作成した証明書を [選択済み] 列に移動します。
6. [保存] をクリックします。
   レコード内の他のフィールドは自動的に生成されます。

   注:
   有効期限が切れた証明書がある場合は、それを削除する必要があります。期限切れの証明書を削除する方法については、「KB0691439 Replacing an expiring SAML certificate (期限切れ間近の SAML 証明書の置き換え)」を参照してください。

HPE Security ArcSight ESM - メールパーサー統合

HPE Security ArcSight ESM - メールパーサー統合は、セキュリティインシデントを作成するために ESM からのメール通知を消費するメールパーサーを使用してサポートされています。

HPE Security ArcSight ESM - メールパーサー統合の構成

HPE Security ArcSight ESM - メールパーサー統合では、ESM からのメール通知を使用して拡張および応答ワークフローを推進します。

始める前に
必要なロール：sn_si_admin

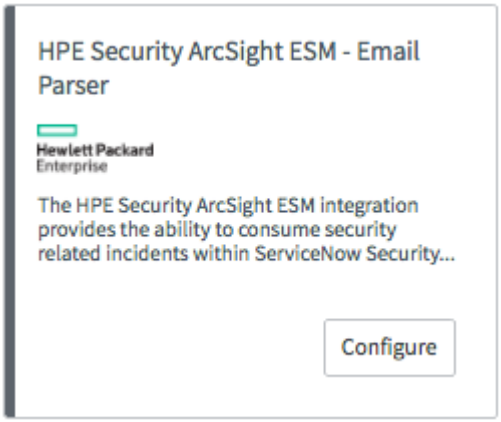
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
統合に使用する HPE Security ArcSight ESM - メールパーサーテンプレートが提供されています。統合が行われる前に、構成してアクティブ化する必要があります。パーサーを更新すると有効になります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > 統合 > 統合設定.
   利用可能なセキュリティ統合が一連のカードとして表示されます。



2. HPE Security Arcsight ESM - メールパーサーカードで、[構成] をクリックします。
3. **[HPE Security ArcSight ESM -** メールパーサー構成 **(HPE Security ArcSight ESM - Email Parser Configuration)]** ダイアログボックスで、[メールパーサーの設定] リンクをクリックします。
4. **[ArcSight ESM]** リンクをクリックして、提供されたテンプレートメールパーサーの設定を編集します。
   少なくとも、[メールの送信元] フィールドに入力します。独自のメールパーサーを作成するには、「Security Operations でのメールパーサーの作成」を参照してください。
5. [アクティブ] ボックスをオンにします。
6. [メールパーサー] フォームで [更新] をクリックします。
   メールパーサーは有効です。[統合構成] に戻る必要はありません。

HPE ArcSight Logger - インシデント拡張統合

HPE ArcSight Logger - インシデント拡張統合はログを検索し、関連するサイティング情報をセキュリティインシデントに追加します。

探索	設定
セキュリティインシデントレスポンス の統合	• HPE ArcSight Logger の開始 - インシデント拡張統合 • サイティング検索設定レコードの作成
使用	開発

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

- サイティング検索の実行
- Security Operations Integration - サイティング検索フロー
- Security Operations - Arcsight Logger サイティング検索フロー
- サイティング検索の詳細の表示
- サイティング検索結果の表示
- ServiceNow セキュリティオペレーション 統合開発のガイドライン
- 統合を作成するためのヒント
- 開発者トレーニング
- 開発者ドキュメント
- アプリケーションとともにインストールされているコンポーネントの検索

トラブルシューティングとヘルプ

- 統合のトラブルシューティング
- Security Operations Community で質問や回答をする
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

自動翻訳

HPE ArcSight Logger の開始 - インシデント拡張統合

HPE ArcSight Logger はリアルタイムデータをストリーミングして特定のログに分類し、セキュリティオペレーション と簡単に統合します。HPE ArcSight Logger - インシデント拡張統合を使用する前に、ServiceNow Store から統合をダウンロードし、API URL とログイン認証情報を追加する必要があります。

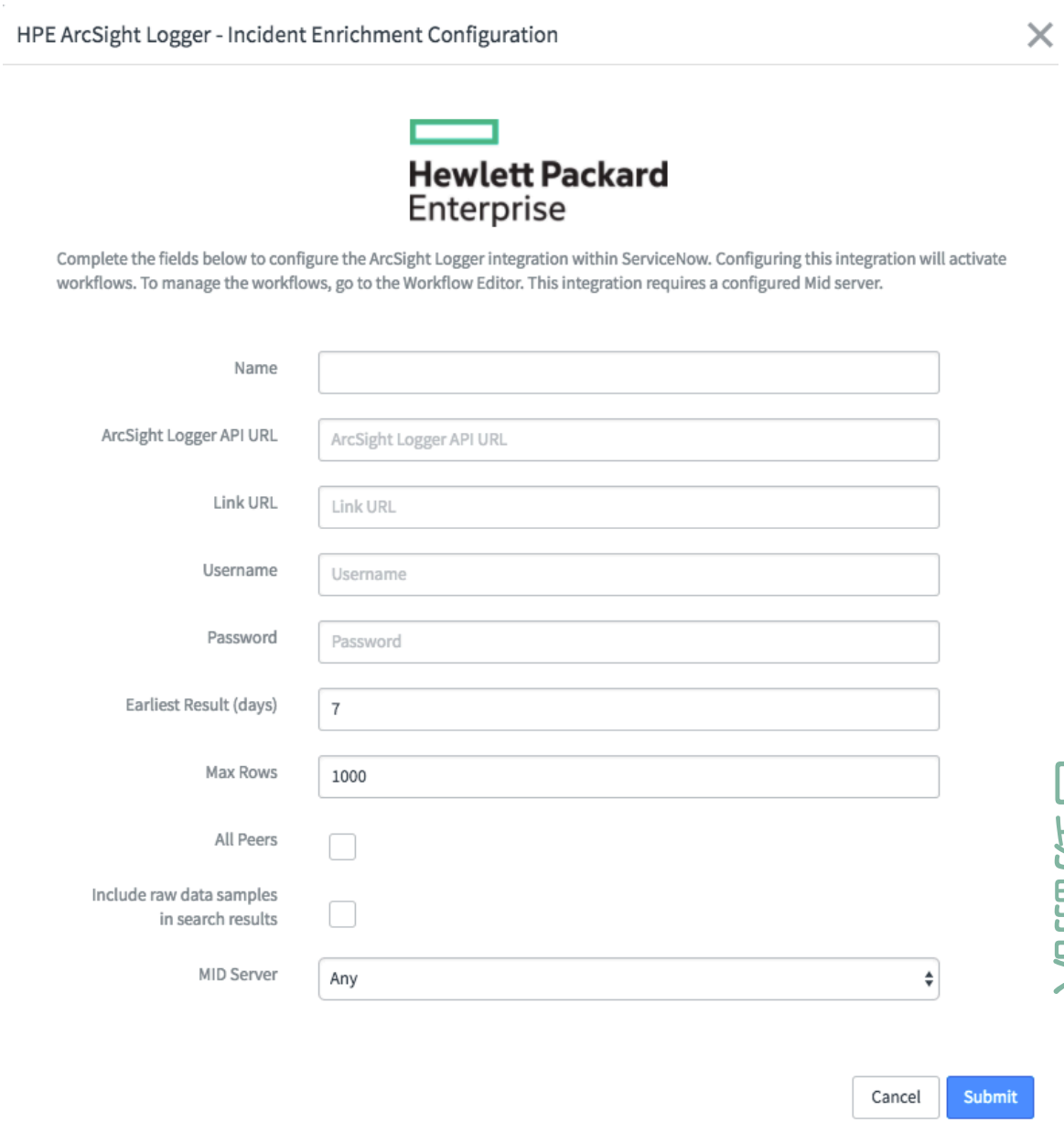
始める前に

必要なロール：sn_si_admin

手順

1. から統合をダウンロードします ServiceNow Store.
2. インストールが完了したら、次に移動します: セキュリティオペレーション > 統合 > 統合設定. 利用可能なセキュリティ統合が一連のカードとして表示されます。
3. HPE ArcSight Logger - インシデント拡張カードで、[新規] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

4. 必要に応じて、フィールドに入力します。

フィールド	説明
名前	この構成の名前。
ArcSight Logger API Base URL	HPE Security ArcSight Logger サイトから取得したベース URL。
リンク URL	[オプション] HPE Security ArcSight Logger インスタンスに接続するリンク URL (利用可能な場合)。
ユーザー名	Intel HPE ArcSight Logger ユーザー名。
パスワード	Intel HPE ArcSight Logger パスワード。
最も早い結果 (日数)	表示する最も早い結果 (日数単位)。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
最大行数	検索する行の最大行数。
すべてのピア	デフォルトはオフで、接続しているローカルロガーのみを検索します。オンにすると、相互に接続されているすべてのロガーが検索されます。
検索結果に生データサンプルを含める	サイティング検索結果に生データのサンプルを含めるには、これを選択します。返されるデータの量は、[セキュリティインシデントレスポンス] プロパティの [生データの行数] プロパティの設定によって異なります。
MID サーバー	[任意] を選択して、 任意のアクティブな MID サーバーを使用するか、特定の MID サーバー名を選択します。

注:
この統合を設定すると、ワークフローが有効になります。ワークフローを管理するには、[ワークフローエディター] に移動します。

5. **[Submit]** をクリックします。
   統合構成カードが表示されます。
6. 新しい構成カードを表示すると、[構成] または [削除] をクリックして、構成を変更または削除できます。
7. 統合構成カードの元のリストに戻るには、[構成を表示] ドロップダウンから [いいえ] を選択します。

ハイブリッド分析 の統合

ハイブリッド分析 アプリケーションは、ユーザーが脅威に関してファイルと URL を分析するオープンなオンラインコミュニティの一部です。結果を共有し、コミュニティからの調査を利用することで、インシデントにより効果的に対応することができます。共有された脅威情報を Now Platform セキュリティオペレーション 製品と統合することで、特定の観測事象の重大度に関するさらなるインサイトが得られます。

ハイブリッド分析 統合は、次の観測事象で脅威のルックアップを実行します。

- ファイルハッシュ
- IP アドレス
- URL

フローは、新しい観測事象がセキュリティインシデントに入るとチェックします。観測事象が API 統合によって認識されるタイプである場合、観測事象が評価されます。悪意があると判定された観測事象にタグ付けされます。

ハイブリッド分析 のインストールと構成

インスタンスで統合を実行する前に、インストールと構成の手順を完了して、ハイブリッド分析 アプリケーションが Now Platform セキュリティオペレーション と適切に統合されるようにします。

始める前に

インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

セットアップタスク	説明
必要な Now Platform ロールと セキュリティインシデントレスポンス ロールがアサインされていることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	• システムアドミニストレーター (admin) は、アプリをインストールしてセキュリティインシデントアドミン (sn_si.admin) ロールをアサインします。 • セキュリティインシデントアドミン (sn_si.admin) は構成を監視し、期待する結果を確認します。このロールでは セキュリティオペレーション モジュールにもアクセスでき、sn_si.analyst ロールをアサインします。
API キーを取得します。	API キーの詳細とアカウントの作成方法については、ハイブリッド分析 の Web サイト (ハイブリッド分析の Web サイト) を参照してください。設定するには、API キーを入力する必要があります。
統合用のアプリケーションをインストールする前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	Madrid リリース以降のファミリーリリースでは、com.snc.si_dep プラグインが必要です。このプラグインは、セキュリティインシデントレスポンス 製品をサポートするために必要なすべての依存関係を自動的にインストールします。他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。 次の セキュリティオペレーション アプリケーションを、ServiceNow Store からインストールしてアクティブ化する必要があります。スムーズにインストールできるように、アプリケーションを次のリストの順番で、一度に 1 つずつインストールしてアクティブ化します。 **1.** Security Integration Framework **2.** Security Support Common **3.** セキュリティサポートオーケストレーション **4.** セキュリティインシデントレスポンス 統合のための Now Platform インスタンスのセットアップの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

必要なロール：admin

このタスクについて
システムのプロパティを更新し、統合をインストールして設定するには、次の手順を実行します。

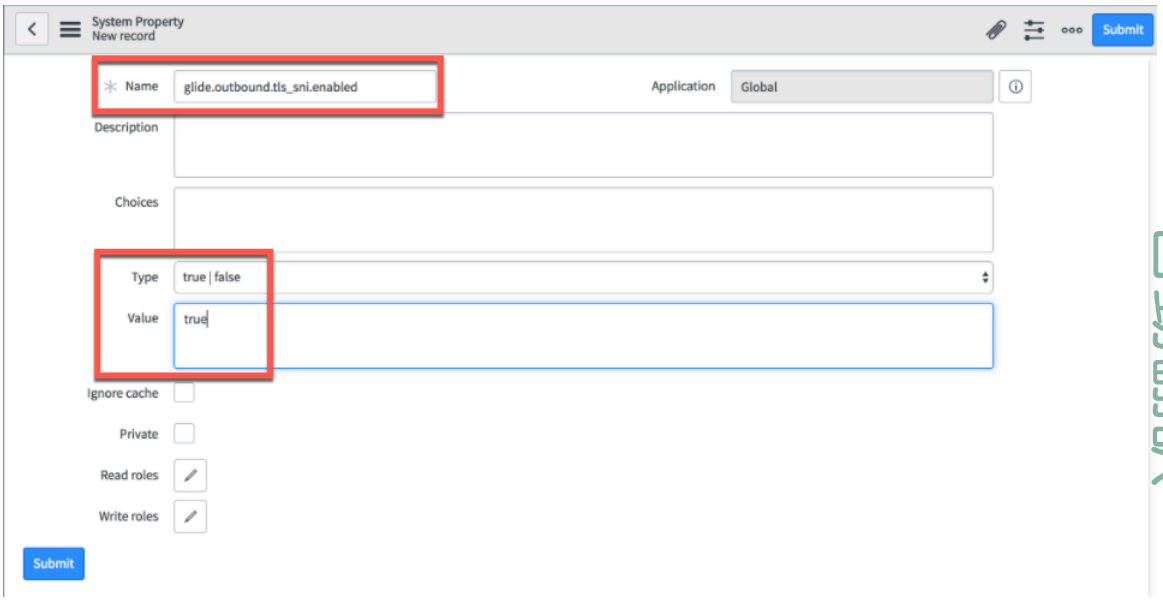
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. ナビゲーションフィルターで「sys_properties.list」と入力し、**Enter** キーを押します。
   [システムのプロパティ] リストが表示されます。
2. [新規] をクリックします。
   新しいレコードが表示されます。
3. フィールドに入力するか、次のテーブルに記載されている値を選択して [送信] をクリックします。

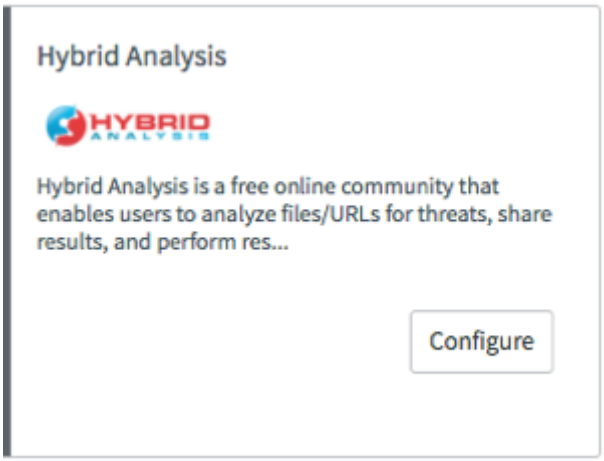
フィールド名	値
名前	glide.outbound.tls_sni.enabled
タイプ	**[True | False]** を選択します。
値	true



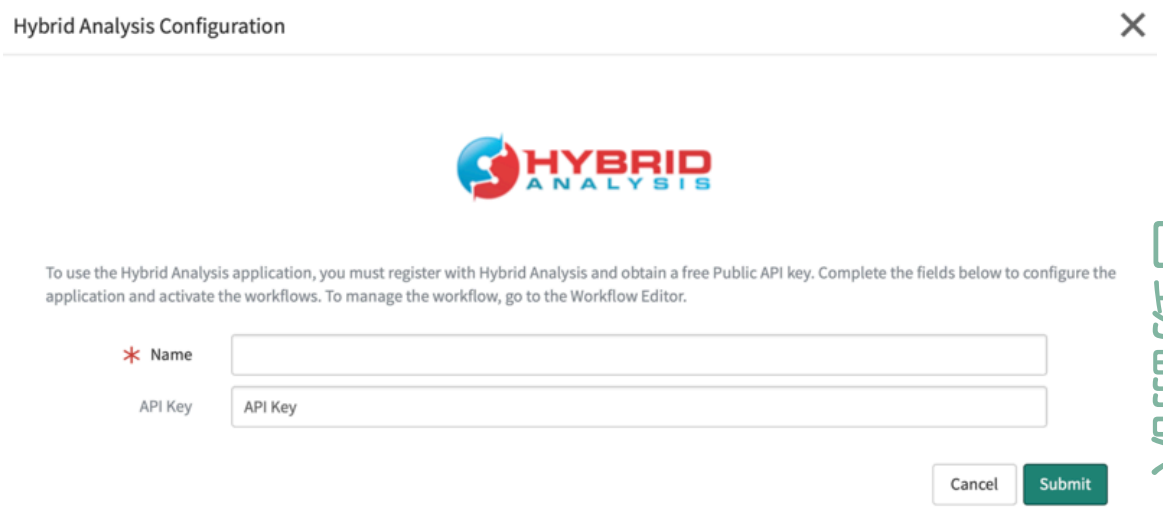
4. 統合用のアプリケーションをインストールしていない場合は、「セキュリティオペレーション 統合のインストール」を参照し、手順に従ってインストールしてください。
5. インストールが完了したら、次に移動します: 統合 > 統合構成 をクリックし、 ハイブリッド分析 タイルを見つけます。
6. [構成] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



7. [ハイブリッド分析構成 **(Hybrid Analysis Configuration)**] ダイアログボックスで、ハイブリッド分析 Web サイトから取得した API キーを入力し、[送信] をクリックします。



8. 正常に構成されていることを確認します。
エラーメッセージが表示されない限り、構成は正常に完了しています。

Trouble?

構成中にエラーメッセージが表示された場合は、 ハイブリッド分析 API キーが無効である可能性があります。

ハイブリッド分析 の期待される結果の確認

観測事象は、セキュリティインシデントによって自動的に生成され、アプリケーションによってスキャンされます。セキュリティインシデントのルックアップ結果を探し、脅威のルックアップが正常に実行されたことを確認します。また、生データを表示し、子観測事象に対して脅威のルックアップを実行します。

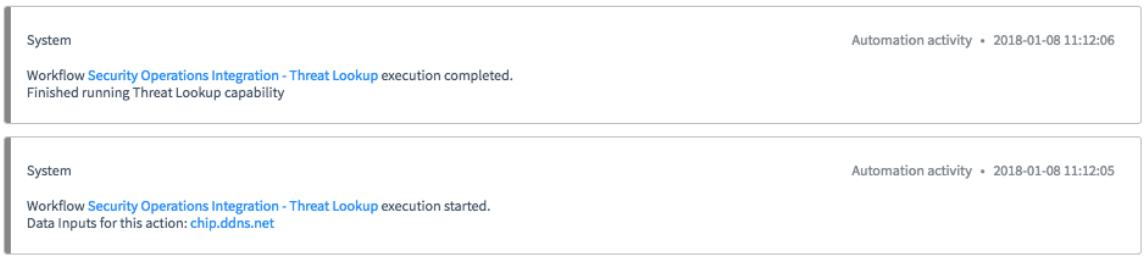
始める前に
必要なロール：sn_si.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

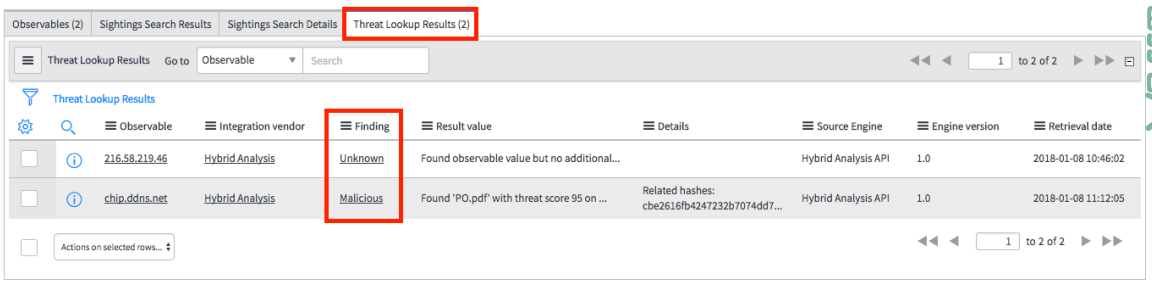
1. 作業しているセキュリティインシデントレコードを開き、ルックアップが正常に実行されたことを確認します。



アプリケーションを設定すると、インシデントの作成時にフローが自動的に起動します。続いてルックアップの実行および完了ステータスがセキュリティインシデントの作業メモに表示されます。

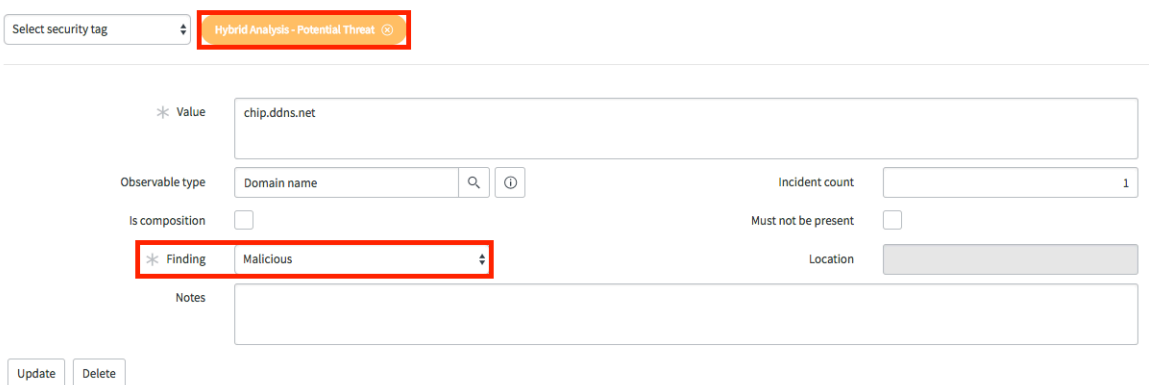
2. ルックアップが正常に実行されたことを確認できない場合は、作業メモで対処方法を確認してください。
3. セキュリティインシデントレコードの下部に移動し、[すべての関連リストを表示] 関連リンクをクリックして結果を表示します。

> **注:**
> 次の手順の図は、[システムの設定] で [タブ付きフォーム] 設定をアクティブにした状態で示されています。バナーフレームの右上隅にある [設定] 歯車アイコンをクリックします。表示される [システムの設定] ダイアログボックスで [フォーム] をクリックし、[タブ付きフォーム] と [フォームと同時] が選択されていることを確認します。



[脅威のルックアップの結果] タブでは、セキュリティインシデントレコードの下部にルックアップ結果が表示されます。悪意があると判断されていないレコードについては、[結果] 列に [不明] と表示されます。結果で悪意があると判断された場合は、[結果] 列に [悪意がある] と表示されます。

4. [観測事象] 列で観測事象をクリックし、レコードを開きます。



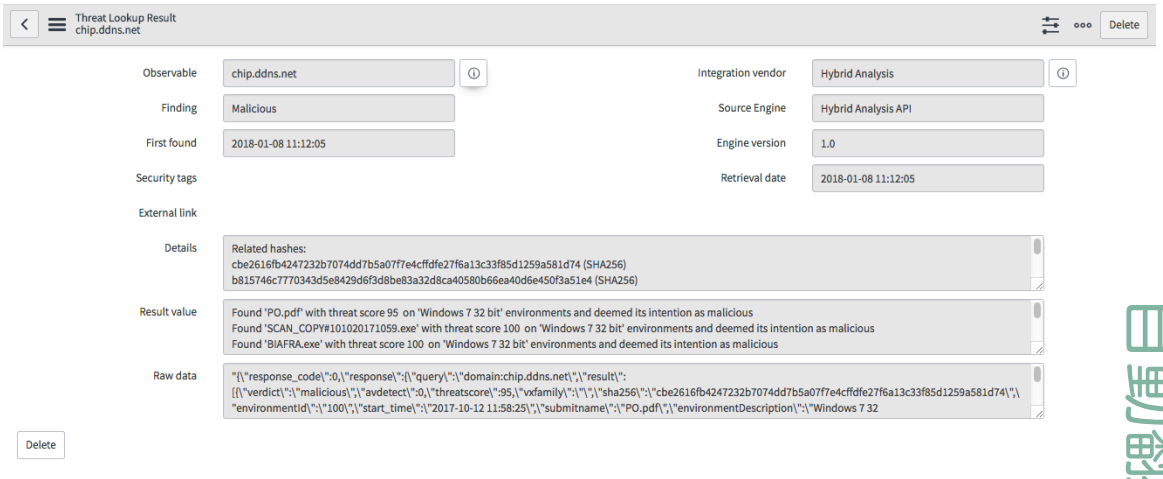
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ルックアップで悪意があると判断された場合は、[結果] フィールドに「Malicious」と表示され、悪意があると判断された 脅威インテリジェンス ソースで観測事象がタグ付けされます。この場合は ハイブリッド分析 統合です。

5. オプション: 手順に従って生データを表示し、子観測事象のリストを表示したら、選択した子観測事象で脅威のルックアップを実行します。

   a. セキュリティインシデントに戻り、[脅威のルックアップの結果] タブで、観測事象の横にある青色の情報アイコンをクリックします。

   b. 表示されるウィンドウで [レコードを開く] をクリックし、データを表示します。
   ハイブリッド分析 統合により、ルックアップから表示される生データ内の観測事象から子観測事象または関連する観測事象も作成されます。



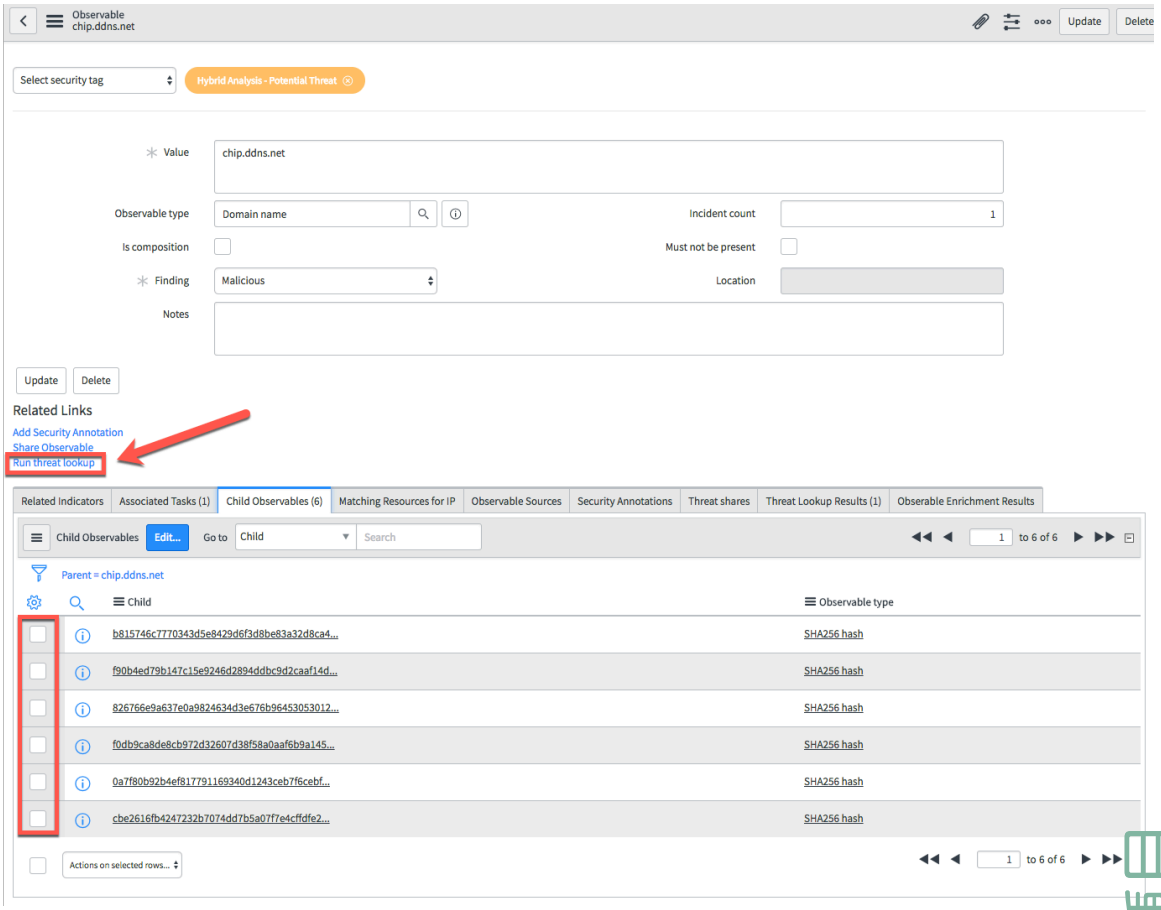
   API によって作成されたリンク、生データ、およびその他の情報が表示されます。

   c. セキュリティインシデントに戻り、**[IoC** を表示] 関連リンクをクリックします。
   子観測事象は、セキュリティインシデントの [子観測事象] タブに表示されます。これは、ルックアップでこれらの関連する観測事象と最初に送信された観測事象との間に既存の関連性が見つかったためです。

   d. [子] 列の観測事象の横にあるフィールドをクリックして選択し、[脅威のルックアップを実行] 関連リンクをクリックしてルックアップを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



e. 表示されるダイアログボックスで ハイブリッド分析 統合が選択されていることを確認し、[送信] をクリックします。

f. 作業メモで、ルックアップが正常に実行されたことを確認し、セキュリティインシデントの [脅威のルックアップの結果] タブで子観測事象のルックアップ結果を探します。

Trouble?
[脅威のルックアップの結果] タブに結果が表示されない場合は、観測事象が統合によるルックアップでサポートされているタイプであることを確認します。

(オプション) ハイブリッド分析 の観測事象を手動で添付する

最初のイベントトリガーでセキュリティインシデントに添付されていない観測事象に対して脅威のルックアップを実行する場合は、観測事象を手動で添付できます。また、関連する観測事象に関する詳細情報が必要な場合にも、このタスクを実行します。

始める前に

観測事象が統合でサポートされているタイプであることを確認します。統合は、次のタイプの観測事象でルックアップを実行します。

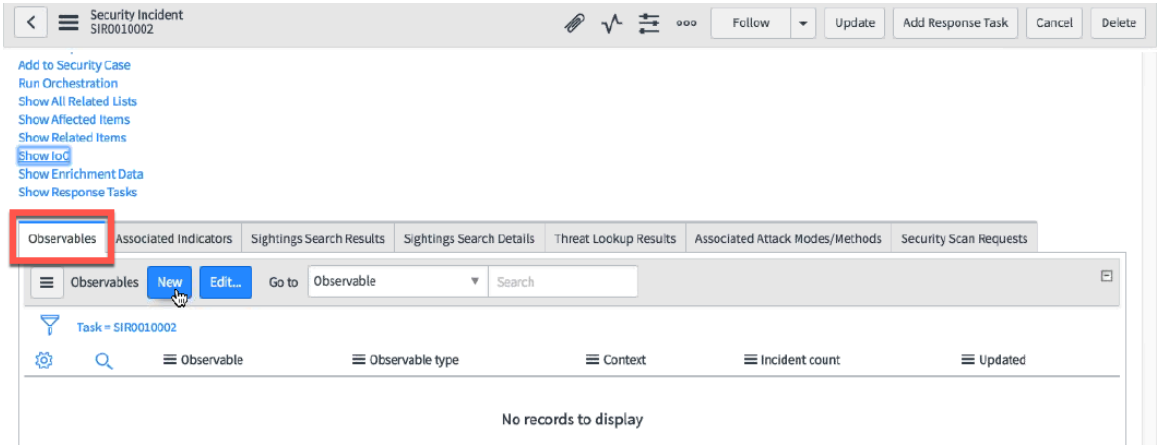
- ファイルハッシュ
- IP アドレス
- URL

必要なロール：sn_si.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

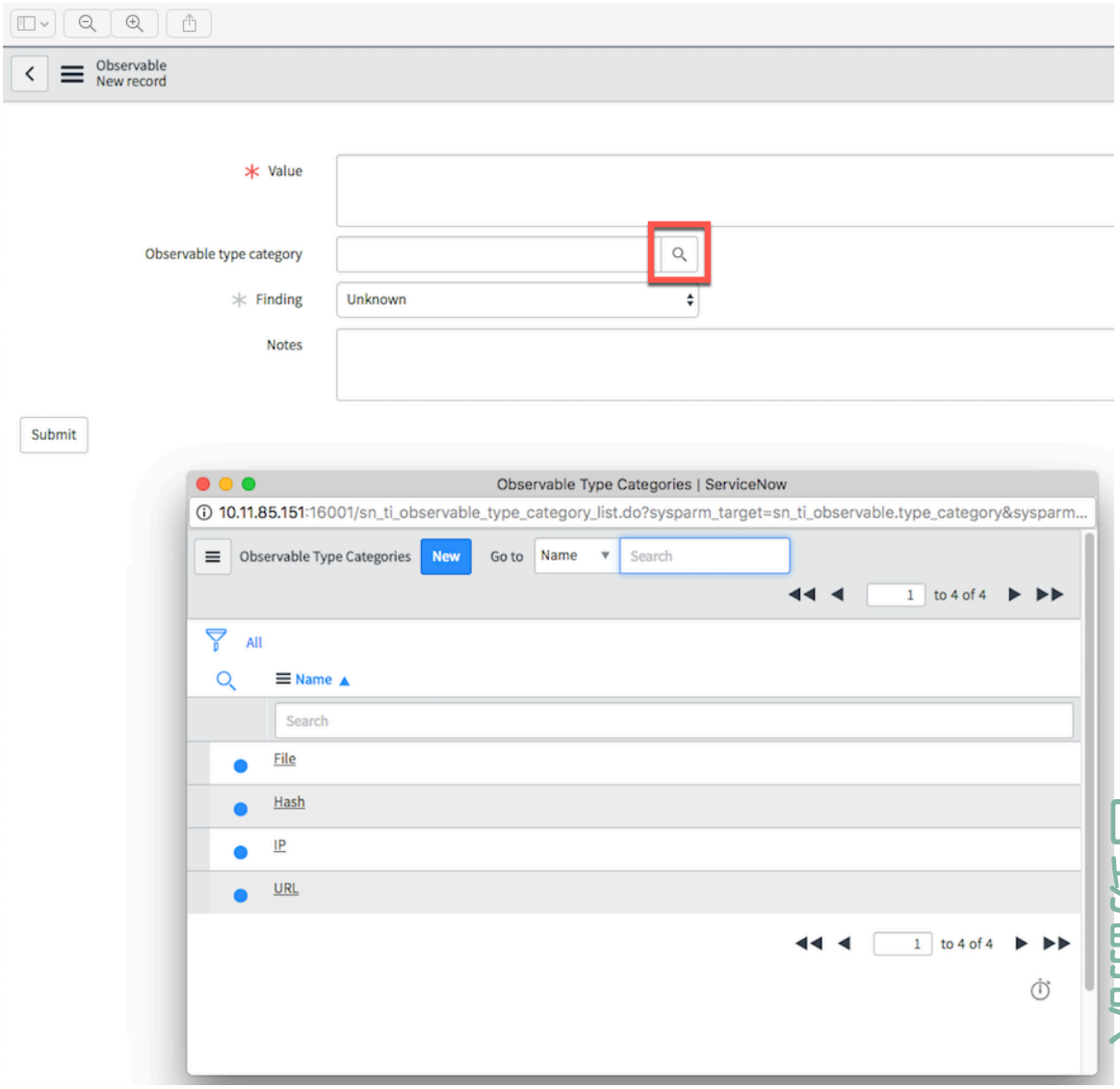
1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデント > すべてのインシデントを表示 をクリックし、観測事象を添付するセキュリティインシデントを開きます。
2. オープンセキュリティインシデントで、[関連リンク] の **[IoC** を表示] リンクをクリックします。



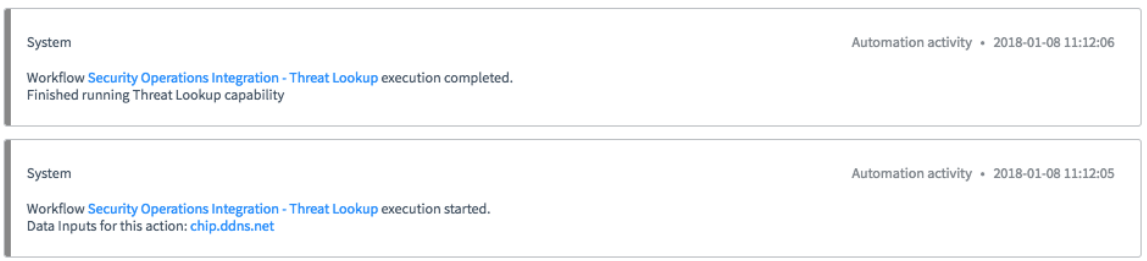
3. [観測事象] タブで、[新規] をクリックします。
   観測事象フォームが表示されます。
4. [値] フィールドに観測事象 (ファイルハッシュ、IP アドレス、または URL) を入力します。
5. 検索アイコンをクリックし、[観測事象タイプカテゴリ] ダイアログボックスからリストで目的の観測事象タイプをクリックしてフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



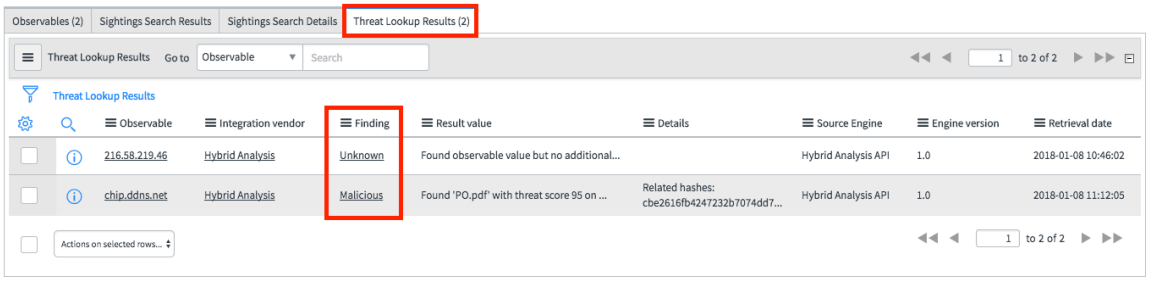
6. [送信] をクリックします。
   フローが起動し、新しい観測事象がチェックされます。実行および完了ステータスは、[セキュリティインシデント] レコードの作業メモセクションに表示されます。
7. セキュリティインシデントに移動し、作業メモを確認します。



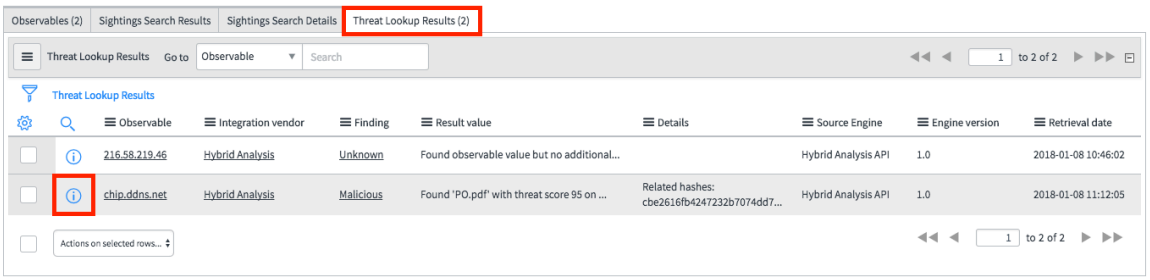
8. レコードの下部で、[すべての関連リストを表示] 関連リンクをクリックします。
9. [脅威のルックアップの結果] タブをクリックして結果を表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



10. [観測事象] 列で、特定の観測事象の横にある青色の情報アイコンをクリックして、詳細情報と生データを表示します。



11. 表示されるダイアログボックスで、[レコードを開く] をクリックして生データと詳細を表示します。
    または、既存の観測事象をセキュリティインシデントレコードに添付することもできます。
12. オプション: [観測事象] タブを選択した状態で [編集] をクリックします。
13. オプション: 表示される [エレメントの編集] フォームで、既存の観測事象を [コレクション] から [観測事象リスト] に移動し、[保存] をクリックします。
    セキュリティインシデントに戻ります。
14. 左端の列でルックアップを実行する観測事象を選択し、[選択した行のアクション...] 選択リストから [脅威のルックアップを実行] を選択します。
    要求が処理されていることを示すメッセージがレコードの上部に表示されます。ルックアップが正常に実行されたことを確認します。

Trouble?
ルックアップが正常に実行されたことを確認できない場合は、作業メモで詳細と対処方法を確認してください。

IBM QRadar Offense Ingestion の統合

IBM QRadar Offense Ingestion の統合により、IBM QRadar 違反を自動的にフェッチしてセキュリティインシデントに変換し、自動応答アクションを有効にすることができます。

この統合は以下をサポートしています。

- セキュリティインシデントの候補である IBM QRadar 違反のディスカバリー。
- 違反に関連付けられている最新のイベントまたはフローの取得。
- 違反の重要な更新を定期的に追跡。
- 違反、イベント、およびフローフィールドのセキュリティインシデントフィールドへのマッピング。
- マップされたフィールドの予備ビュー。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 違反の取り込みをスケジュールして、セキュリティインシデントを定期的に作成。
- セキュリティインシデントがクローズされた場合に違反をクローズ。

IBM QRadar® 違反の取り込み統合用の ServiceNow アプリケーションのインストールと設定

Now Platform インスタンスで統合を実行する前に、これらのインストールと構成のステップを完了して、Now Platform インスタンスでアプリケーションが セキュリティインシデントレスポンス と セキュリティオペレーション 製品と適切に統合されるようにします。

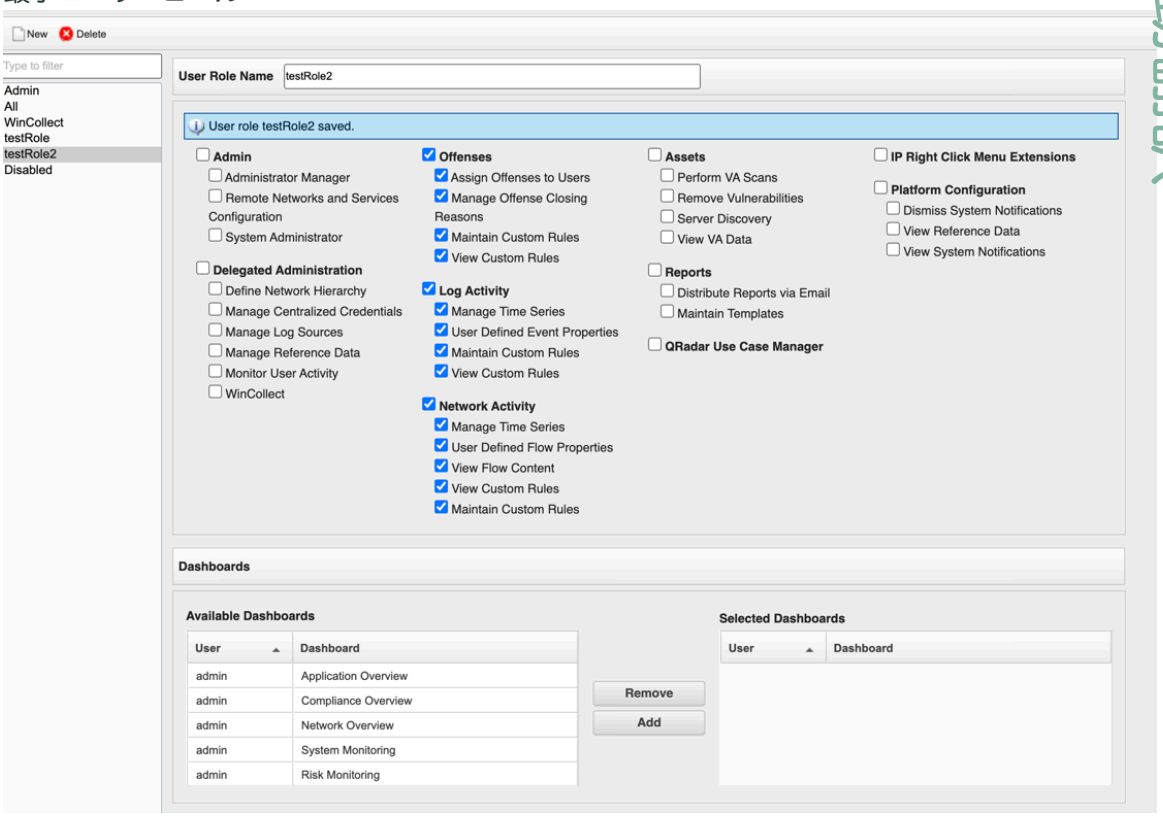
始める前に

必要なロール：sn_si.admin

手順

1. ServiceNow Store から統合用の IBM QRadar アプリケーションをインストールしていない場合は、「セキュリティオペレーション 統合のインストール」を参照し、ステップに従ってインストールしてください。
2. アプリケーションのインストールが完了したら、 統合 > 統合構成 をクリックし、 IBM QRadar タイルを見つけます。
3. アプリケーションを設定するには、[新規] をクリックします。
4. または、[構成] ボタンがタイルに表示されている場合は、そのボタンをクリックして既存の構成を編集します。
5. 表示される [違反の取り込み構成] ダイアログで、フィールドに入力します。

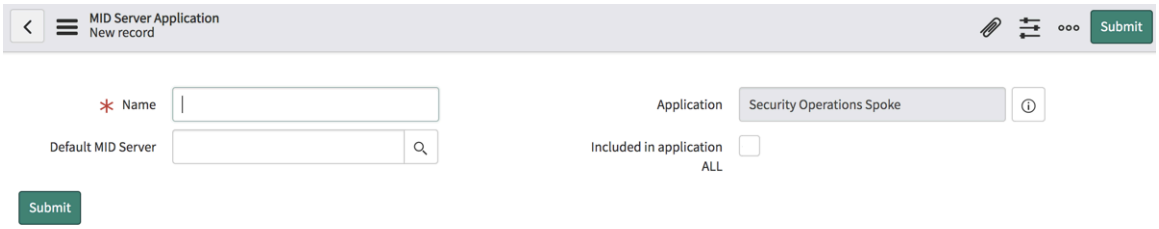
最小ユーザーロール



新しい MID サーバーアプリケーションを作成するには、次の手順を実行します。

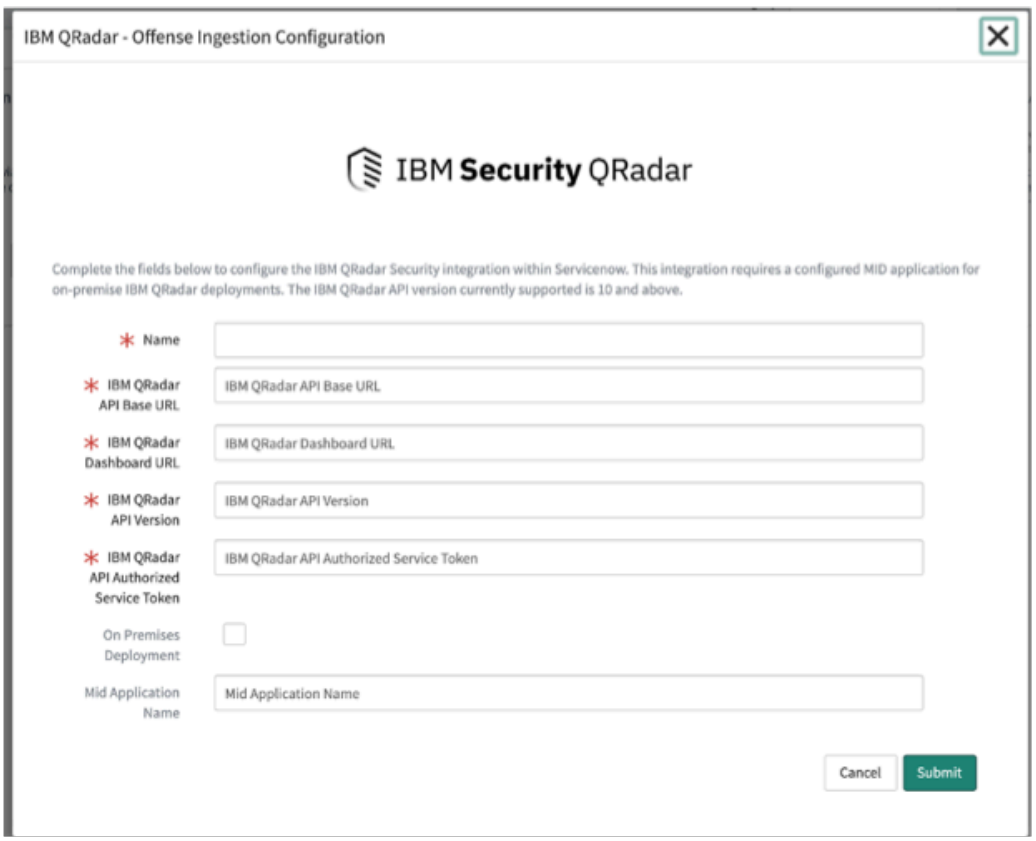
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 次のように移動する。 **MID Server** > アプリケーション をクリックし、[新規] をクリックします。
- MID サーバーアプリケーションの名前を入力し、デフォルトとして使用する MID サーバーを選択します。
- [すべてのアプリケーションに含める] チェックボックスをオフにして、[保存] をクリックします。



- [編集] をクリックします。[メンバーの編集] ページで、利用可能なすべての MID サーバーを選択し、[MID サーバー] リストに移動して、[保存] をクリックします。可用性に応じて、MID サーバーアプリケーションで構成された MID サーバーの 1 つが使用されます。

6. 構成の詳細を入力し、作成した MID サーバーアプリケーションを指定します。



[IBM QRadar 違反の取り込み構成] フォームで構成したソースは、各プロファイルが違反を取り込む限り、複数の Now Platform プロファイルで再利用できます。

7. **[Submit]** をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

検証と送信が正常に完了すると、各 IBM QRadar サーバー構成は [セキュリティ統合] ページにタイルとして保存されます。保存された構成タイルが右上隅にある [セキュリティ統合] ページに表示されていない場合、[構成を表示] 選択リストから [はい] をクリックします。

注:
IBM QRadar ドメインセグメンテーション機能で問題が発生した場合は、 IBM QRadar カスタマーサポートにお問い合わせください。

次のタスク
アプリケーションのインストールと設定が正常に完了しました。次のステップは、プロファイルの作成です。

IBM QRadar 違反の取り込み統合での Now Platform® インスタンスの設定

次のセクションでは、ServiceNow Store からアプリケーションをインストールする前に Now Platform® インスタンスで完了する必要があるセットアップタスクを示します。

始める前に
必要なロール：sn_si.admin

このタスクについて
スムーズなインストールと構成を行うために、 アプリケーションをダウンロードしてインストールする前に、次のテーブルを参照して、リストされたすべてのタスクを完了していることを確認してください。

セットアップタスク	説明
必要な Now Platform® および セキュリティインシデントレスポンス (SIR) のロールがアサインされていることを確認します。	Now Platform® インスタンスで統合をインストール、セットアップ、および使用するには、次のロールが必要です。 • Now Platform® アドミニストレーターロール (admin) を持つユーザーが ServiceNow Store からアプリケーションをインストールし、セキュリティインシデントアドミニストレーター (sn_si.admin) ロールをアサインします。 • sn_si.admin ロールを持つユーザーは、Now Platform® で次のタスクを監督します。 ○ 違反プロファイルに名前を付け、作成し、編集します。 ○ IBM QRadar 違反データフィールドを選択して、セキュリティインシデントフィールドにマッピングします。 ○ 構成を確定する前に、正確性を確認するためにセキュリティインシデントの詳細をプレビューします。 ○ 進行中の違反の取り込みをスケジュールします。 ○ SIR インシデントが作成されてクローズされたときに、違反の更新を有効にします。 ○ セキュリティインシデントアナリスト (sn_si.analyst) ロールをアサインします。 ○ sn_si.analyst を持つユーザーは、セキュリティインシデントを処理します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	ロールとユーザーへのロールの割り当ての詳細については、Servicenow 製品ドキュメント Web サイト の「 ロール」を参照してください。
次のバージョンを使用していることを確認します。 • IBM QRadar バージョン 7.3.2 以降。 • IBM QRadar API バージョン 10 以降。 以前のバージョンはサポートされていません。	IBM QRadar コンソールへのアクセス権がある場合は、この統合に必要な API にアクセスできます。API に必要なその他の特別なセットアップはありません。
MID サーバーアプリケーションがインストールおよび設定されていることを確認します。	設定された MID サーバーアプリケーション。 IBM QRadar サーバーが企業ネットワーク内に展開されている場合、Now Platform インスタンスの MID サーバーを IBM QRadar サービスに接続する必要があります。MID サーバーの詳細については、ServiceNow 製品ドキュメント Web サイト を参照してください。 IBM QRadar クラウドサービスを使用している場合、MID サーバーは必要ありません。
統合用のアプリケーションをインストールする前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。 **1.** セキュリティインシデントレスポンス **2.** Security Operations のイベントとアラートの取り込み：このアプリケーションでは次のものが必要です。 ○ com.glide.hub.integration.runtime => ServiceNow 統合ハブランタイム ○ com.glide.hub.action_step.rest => ServiceNow 統合ハブアクションステップ - REST **注:** Integration Hub コンポーネントは、イベントおよびアラートの取り込みプラグインとともにインストールされます。これらがインストールされていない場合は、 カスタマーサポートに連絡してください。 セキュリティオペレーション コアアプリケーションのインストールの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のタスク

統合のために Now Platform® インスタンスが正常に設定されました。次のステップでは、統合のために ServiceNow Store から IBM QRadar アプリケーションをインストールします。

IBM QRadar 違反の取り込み統合のプロファイル作成

sn_si.admin ロールを持つユーザーは、 Now Platform インスタンスに違反プロファイルを作成し、セキュリティインシデントを作成する違反を指定します。Now Platform セキュリティインシデントレスポンス (SIR) セキュリティインシデントが違反から作成される前に、違反のフィールド値が Now Platform セキュリティインシデントのレイアウトに表示されるため、実際のセキュリティインシデントがどのように作成されるかをプレビューできます。

始める前に

必要なロール：sn_si.admin

このタスクについて

利用可能な API を使用した統合の観点から、IBM QRadar 違反は、定義されたプロファイルタイプに応じて、Now Platform インスタンスの セキュリティオペレーション 環境に自動的に取り込まれます。統合ワークフローでは、不正なアクセス試行やマルウェアなどのさまざまなタイプの違反を取り込めます。これらの違反は、インスタンスの セキュリティオペレーション 環境で設定したプロファイルに基づいて取り込まれます。すべての違反は、最初にプロファイル内の設定された違反タイプに対して取り込まれます。取り込まれた違反をさらにフィルタリングして、セキュリティインシデントを作成する違反を指定できます。たとえば、高リスクとして識別された違反に対してのみセキュリティインシデントを作成するフィルターを使用できます。プロファイルがアクティブになり、取り込まれた違反からセキュリティインシデントが作成される前に、個々のフィールド値が、プレビュー用のセキュリティインシデントのレイアウトの対応するフィールドにマッピングされます。

Now Platform インスタンスの違反プロファイル名は一意である必要があります。複数のソースに対して複数の構成を作成できます。また、1 つのソースに対して複数のプロファイルを作成することもできます。

IBM QRadar 違反を取り込むためのプロファイルの作成

違反を取り込むようにプロファイルを設定できます。

始める前に

必要なロール：sn_si.admin

手順

1. Now Platformインスタンスで違反のプロファイルを作成するには、次に移動します: **IBM QRadar** 統合 > **IBM QRadar** プロファイル.
2. [**New**] をクリックします。
3. フィールドに入力します。

   完成したフォームの例が表の後に表示されます。

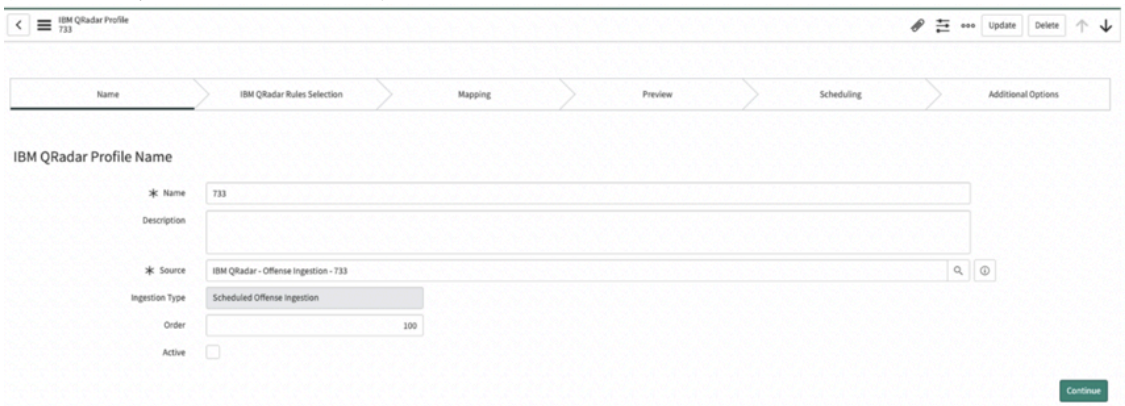
フィールド	説明
名前	プロファイルの一意の名前。名前が一意でない場合、エラーが表示され、重複するプロファイル名は保存されません。 Now Platform インスタンスのプロファイル名は一意である必要があります。
アクティブ	デフォルトでは、このチェックボックスはクリアされます。このオプションを無効にすると、

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	プロファイルは非アクティブになり、取り込みは行われません。 **注:** アクティブにする前に、プロファイルのすべてのセクションを完了する必要があります。
ソース	違反を取り込むように設定した IBM QRadar サーバー。複数の IBM QRadar サーバーが設定されている場合は、プロファイルに取り込まれる違反タイプに適したサーバーを選択します。値を入力する必要があります。
順序	デフォルトは 100 です。 複数のプロファイルを作成した場合、この値は、2 つ以上のプロファイルが同じトリガー条件を共有する場合の実行時の優先度を示します。プロファイル内の番号が最も小さいワークフローの優先度が最も高くなります。
(オプション) 説明	このプロファイルを他のプロファイルと区別するための追加テキスト。

次の図は、完成したフォームの例です。



次のタスク
次のステップでは、取り込み対象の違反を選択します。

IBM QRadar ルールの選択

IBM QRadar ソースに基づいて、プロファイルに 1 つ以上の IBM QRadar ルールを選択します。

始める前に
必要なロール：sn_si.admin

このタスクについて
Now Platform インスタンスで利用可能な IBM QRadar ルールを表示して、セキュリティインシデントを取り込んで作成するアクティブな IBM QRadar ルールを把握します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

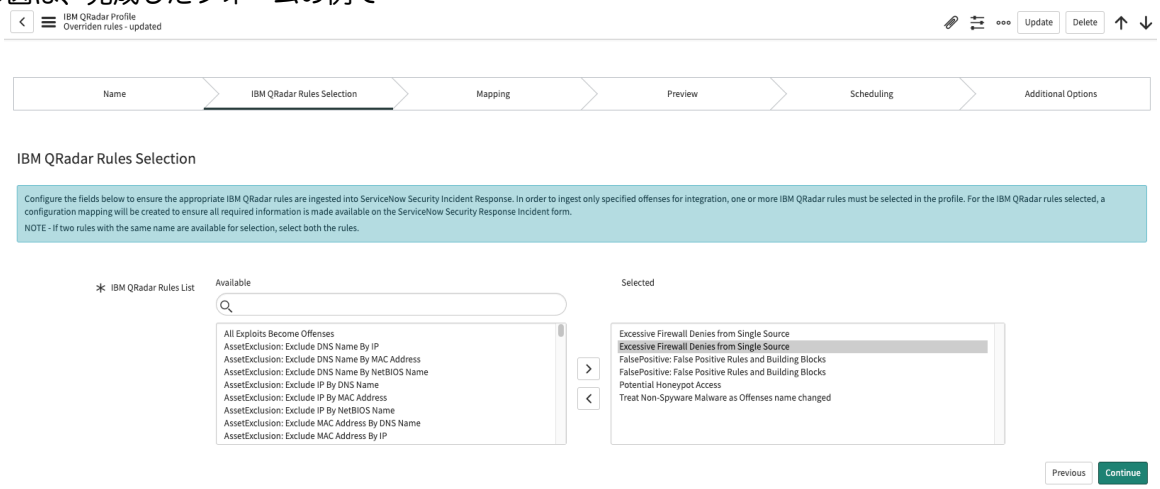
自動翻訳

IBM QRadar では、システム、上書き、およびユーザールールの作成元からルールを識別できます。デフォルトでは、ルールの作成元はシステムルールにリンクされています。IBM QRadar でシステムルールを変更すると、その作成元が [上書き] に設定されます。

[IBM QRadar ルールリスト] フィールドのリストをクリックします。IBM QRadar コンソールに存在するアクティブな IBM QRadar ルールのリストが表示されます。リストから 1 つ以上のルールを選択し、[選択済み] 列に移動します。選択した 1 つ以上の IBM QRadar ルールによってトリガーされた違反がこのプロファイルに取り込まれます。

同じ名前のルール：Now Platform インスタンスに、アクティブなルールまたは有効なルールのリストが表示されます。IBM QRadar でアクティブまたは有効なシステムルールを変更すると、新しい上書きルールが作成されます。これにより、2 つのルールが Now Platform に同じ名前で表示されます。このシナリオが発生した場合は、セキュリティインシデントの取り込みと作成の両方のルールを選択します。

次の図は、完成したフォームの例で



す。

[続行] をクリックして、ウィザードの次のステップに進みます。

IBM QRadar 統合の違反フィールドのマッピング

ルールを選択した後の次のステップでは、違反、イベント、またはフローフィールドをセキュリティインシデントフォームのフィールドにマップします。

概要

マッピングステップでは、最初に 1 つ以上の選択された IBM QRadar ルールのサンプル違反を取り込む必要があります。関連するすべての違反フィールドデータが SIR インシデントフォームの適切な場所にマッピングされていることを確認する必要があります。そうすることで、SIR インシデントをプレビューセクションでビジュアル化できます。

サンプル違反フィールドのマッピングには、次のものが含まれます。

- サンプルデータの取得と入力：「サンプル IBM QRadar 違反の取り込み」を参照してください。
- セキュリティインシデントへの違反フィールドのマッピング：「IBM QRadar 違反フィールドのセキュリティインシデントレスポンスフィールドへのマッピング」を参照してください。

サンプル IBM QRadar 違反の取り込み

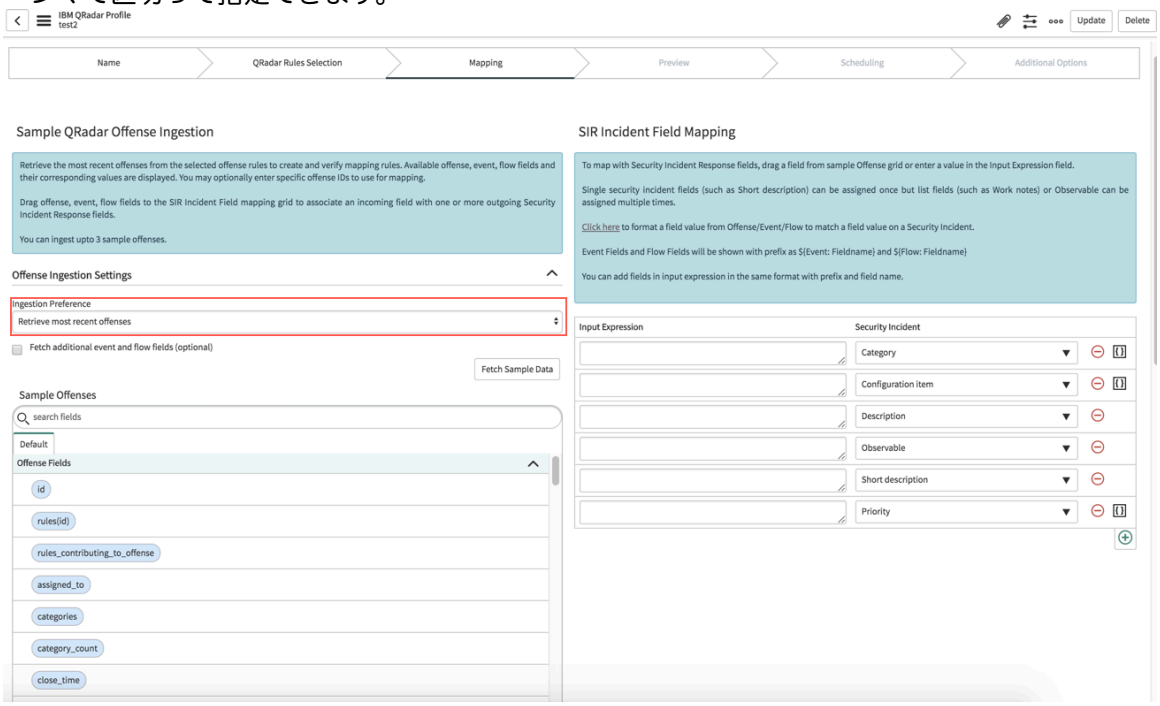
1 つ以上の選択された IBM QRadar ルールのサンプル違反を取り込むことができます。

始める前に
必要なロール：sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. このマッピングフォームが表示されない場合は、進捗状況バーの [マッピング] をクリックします。
2. 最新の 3 つのサンプル違反をプルするか、マッピングエクスペリエンスに使用する特定の違反の一意の違反 ID を指定できます。
   [取り込み設定] 選択リストから、次のいずれかを選択します。
   - 最新の違反を取得：選択したルールの最新の 3 つの違反が取得されます。
   - 違反 ID に基づく違反の選択：取得する違反の違反 ID を指定します。最大 3 つの違反 ID をカンマで区切って指定できます。



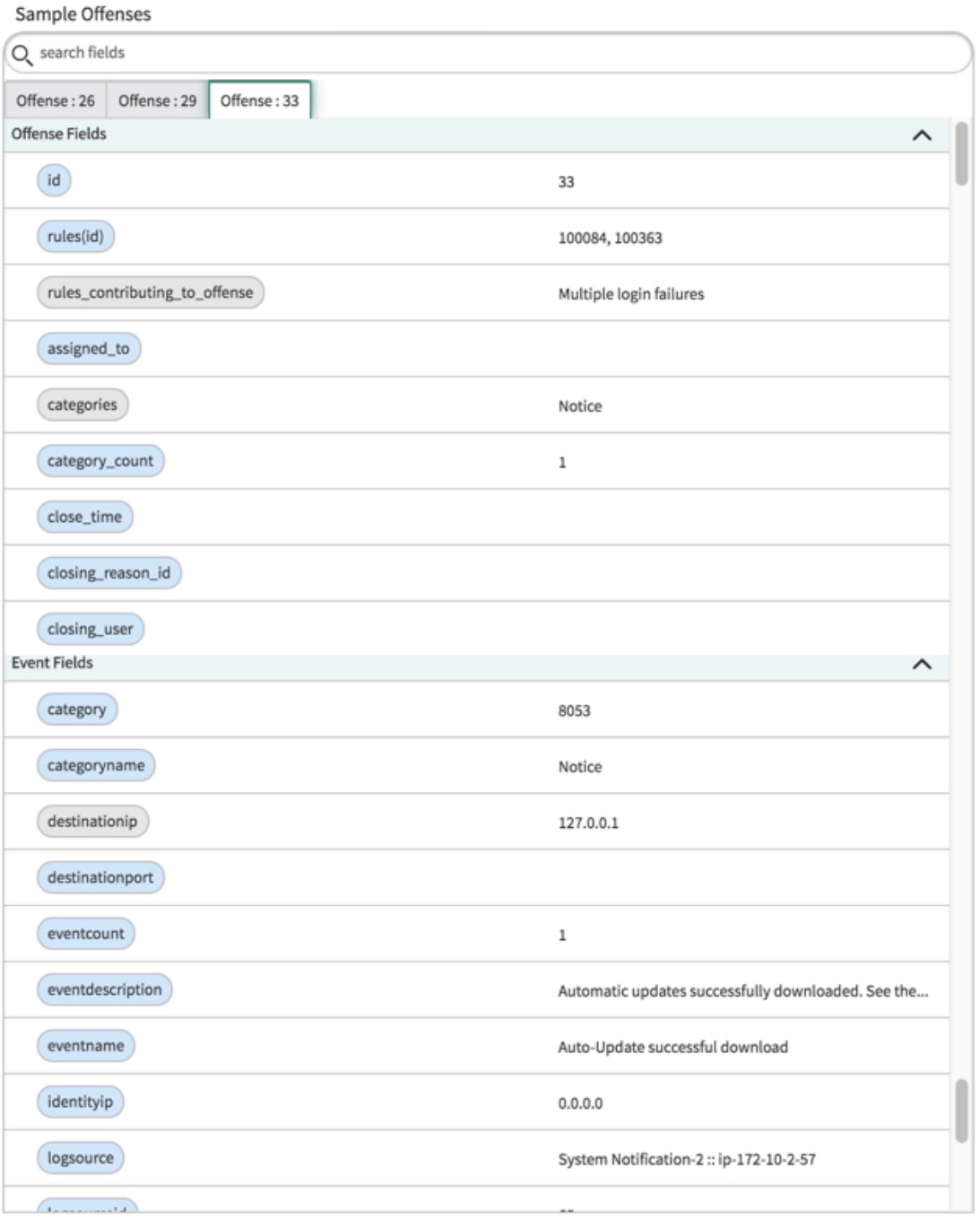
3. [サンプルデータのフェッチ] をクリックして、IBM QRadar コンソールから選択した違反ルールに対する最新のサンプル違反データをプルします。

   違反のフィールドと値の結果は、個別のタブとして表示されます。違反は、次の 3 つのタイプのルールに基づいてトリガーされます。
   - イベント：このルールでは、イベントログがチェックされ、指定された条件が満たされると違反が作成されます。
   - フロー：ネットワークデータとトラフィックがチェックされ、特定の条件が満たされると違反が作成されます。
   - 一般：この場合、イベントまたはフローの条件を指定でき、いずれかまたは両方の条件が満たされると違反が作成されます。

   サンプル違反のプルには少し時間がかかる場合があります。トランザクションが機能していることを示すメッセージが画面の上部に表示されます。違反をトリガーしたルールに応じて、次の「

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



」図に示すように、違反フィールドと一緒に、イベントまたはフローフィールドに入力されます。

注:
表示されるイベントまたはフローフィールドは、対応するイベントまたはフロールールに基づいて違反をトリガーした最初のイベントまたはフローフィールドに属します。

4. この統合用に作成されたカスタム違反フィールドは次のとおりです。
これらのカスタムフィールドに加えて、標準違反フィールドをマッピングに使用できます。
   - rules_contributing_to_offense：ルール ID に基づいて違反に貢献した IBM QRadar ルール。
   - users：違反のユーザー名

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- remote_destination_ip：違反のリモート宛先 IP

  違反のローカル宛先 ID に基づいて、次のカスタムローカル宛先アドレスフィールドを使用できます。

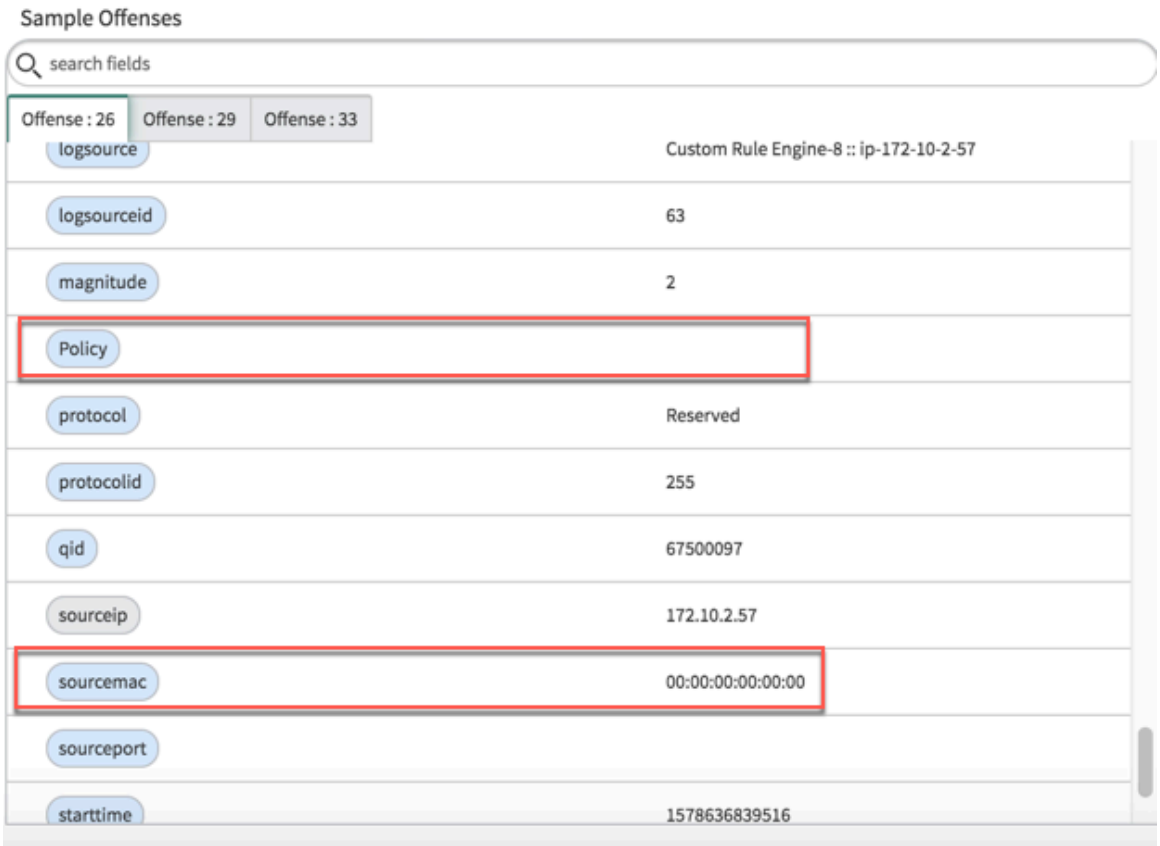
  - local_destination_address (domain_id)
  - local_destination_address (event_flow_count)
  - local_destination_address (first_event_flow_seen)
  - local_destination_address (id)
  - local_destination_address (last_event_flow_seen)
  - local_destination_address (local_destination_address_ids)
  - local_destination_address (magnitude)
  - local_destination_address (network)
  - local_destination_address (offense_ids)
  - local_destination_address (local_destination_ip)

- 違反のソース ID に基づいて、次のソースアドレスを使用できます。
  - source_addresses (domain_id)
  - source_addresses (event_flow_count)
  - source_addresses (first_event_flow_seen)
  - source_addresses (id)
  - source_addresses (last_event_flow_seen)
  - source_addresses (source_address_ids)
  - source_addresses (magnitude)
  - source_addresses (network)
  - source_addresses (offense_ids)
  - source_addresses (source_ip)

[追加のイベントおよびフローフィールドをフェッチ (オプション)] チェックボックスをオンにします。任意のアクティブで有効なカスタムイベントおよびフローフィールドからサンプルイベントとフローデータをフェッチできます。次に示すように、カスタムフィールドをカンマで区切って指定します。

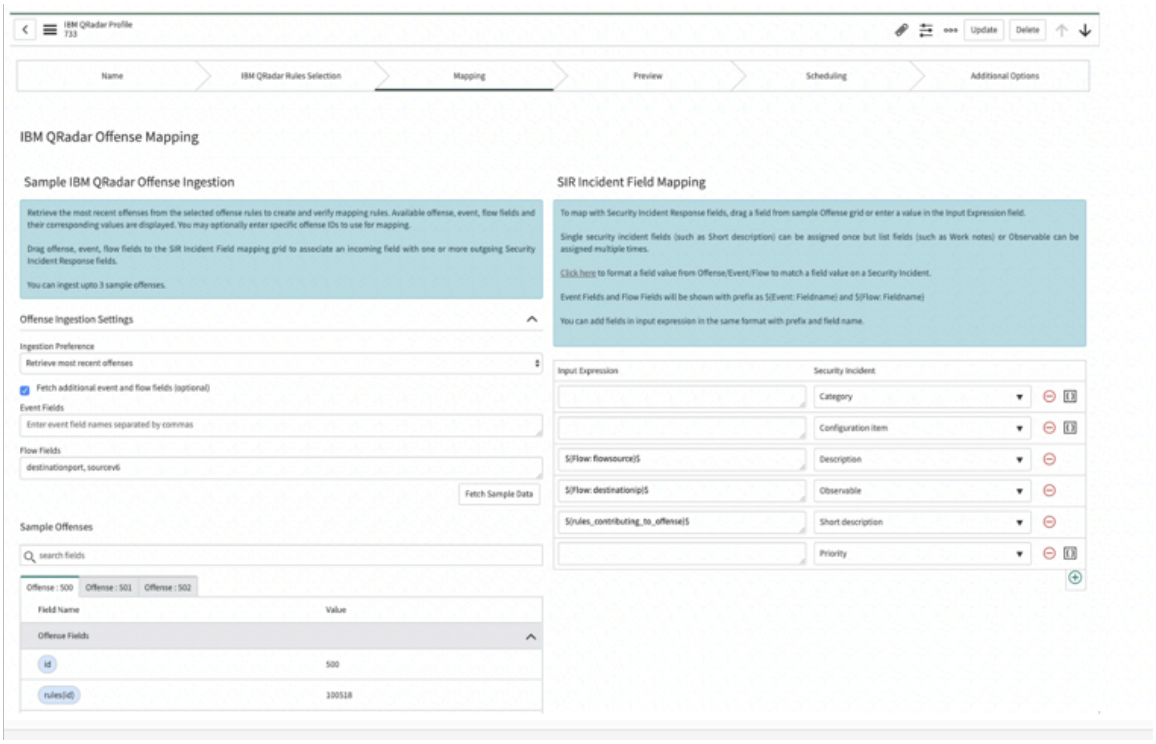
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[サンプルデータをフェッチ] をクリックします。指定されたイベントまたはフローフィールドとその値 (利用可能な場合) は、「



」に示すように [イベント] または [フロー] セクションに追加されます 。

サンプルデータをフェッチすると、これらのフィールドに対応する値がフォームの左側に入力されます。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のタスク
サンプルデータをフェッチした後の次のステップで、違反フィールドをセキュリティインシデントにマップします。

IBM QRadar 違反フィールドのセキュリティインシデントレスポンスフィールドへのマッピング

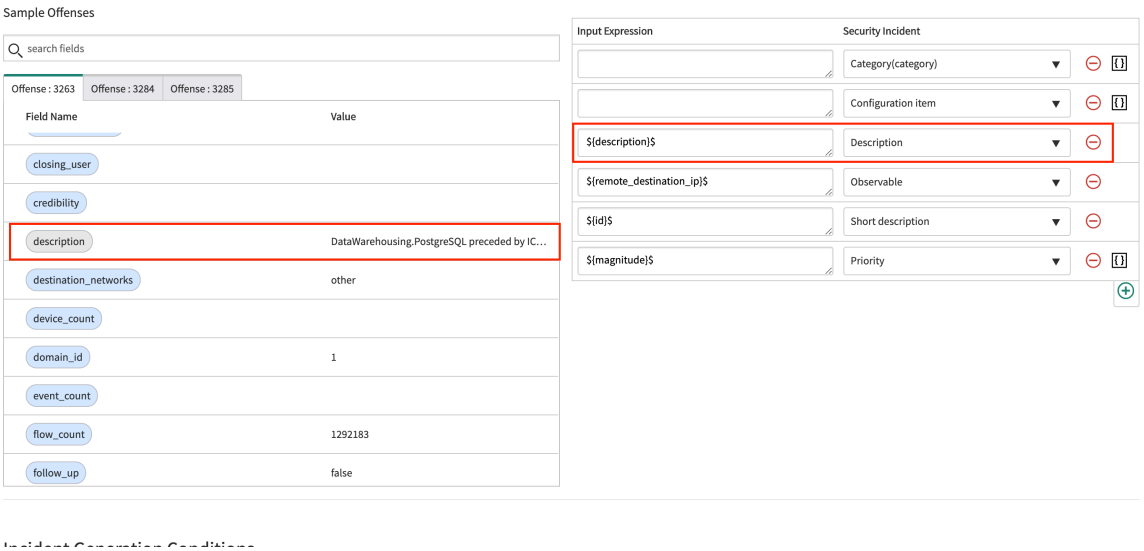
個々の違反、イベント、およびフローフィールドを Now Platform SIR セキュリティインシデントのフィールドにマッピングします。

違反フィールドのマッピング

sn_si.admin ロールを持つユーザーとして、左側の [サンプル違反] セクションのフィールドを使用し、[SIR インシデントフィールドマッピング] 列の [セキュリティインシデント] フィールドにマップします。左側から違反、イベント、またはフローフィールドをドラッグし、右側の [ServiceNow SIR インシデントマッピング] セクションにドロップして、マッピング構成を編集します。右側のマッピングで、受信違反フィールドを送信セキュリティインシデントフィールドに関連付けることができます

1. サンプルデータをフェッチした後の次のステップで、違反、イベント、またはフローフィールドをセキュリティインシデントにマップします。フォームの左側からフォームの右側のセキュリティインシデントのフィールドにフィールド値をマッピングするには、フォームの左側で青色のフィールド名をクリックしたままにします。
2. フィールド名 (descriptionなど) をドラッグして、[セキュリティインシデント] 列のフィールド名の横にある [入力式] 列のフィールドにドロップします。

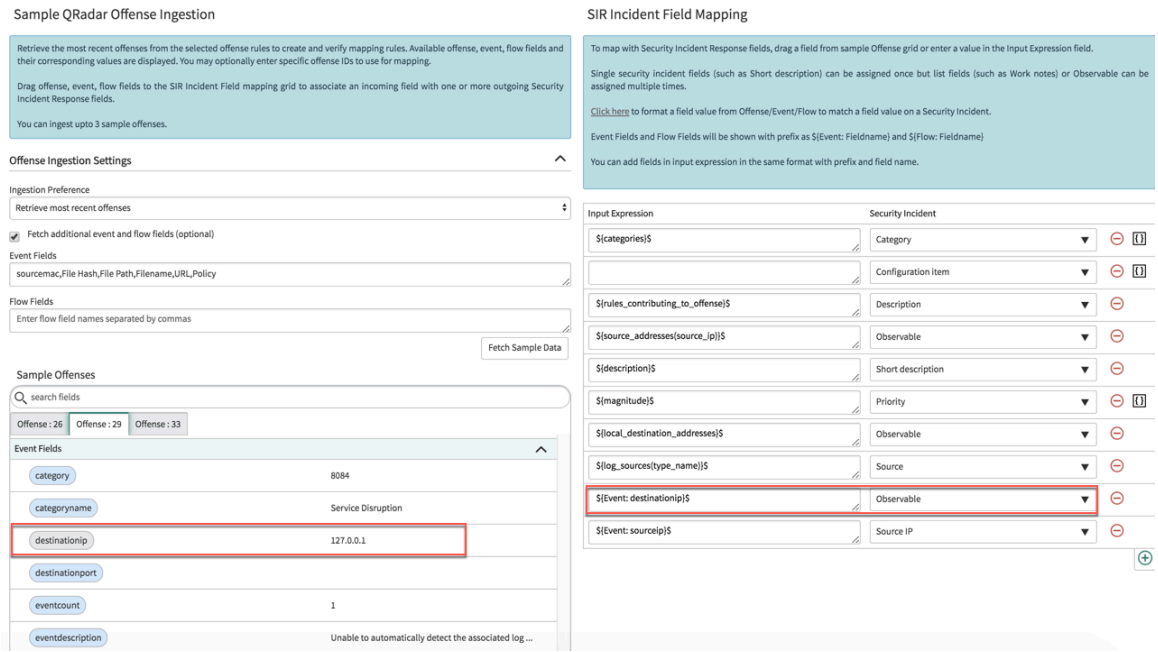
   フィールド値が [入力式] 列に表示されます。次の画像で、descriptionをセキュリティインシデントの [説明] フィールドにマップします。



注:
[入力式] セクションに手動でイベントまたはフローフィールド名を入力する場合は、マップされるフィールドの名前の前に *${Event:eventfield}$* または *${Flow:flowfield}$* というプリフィックスを追加する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



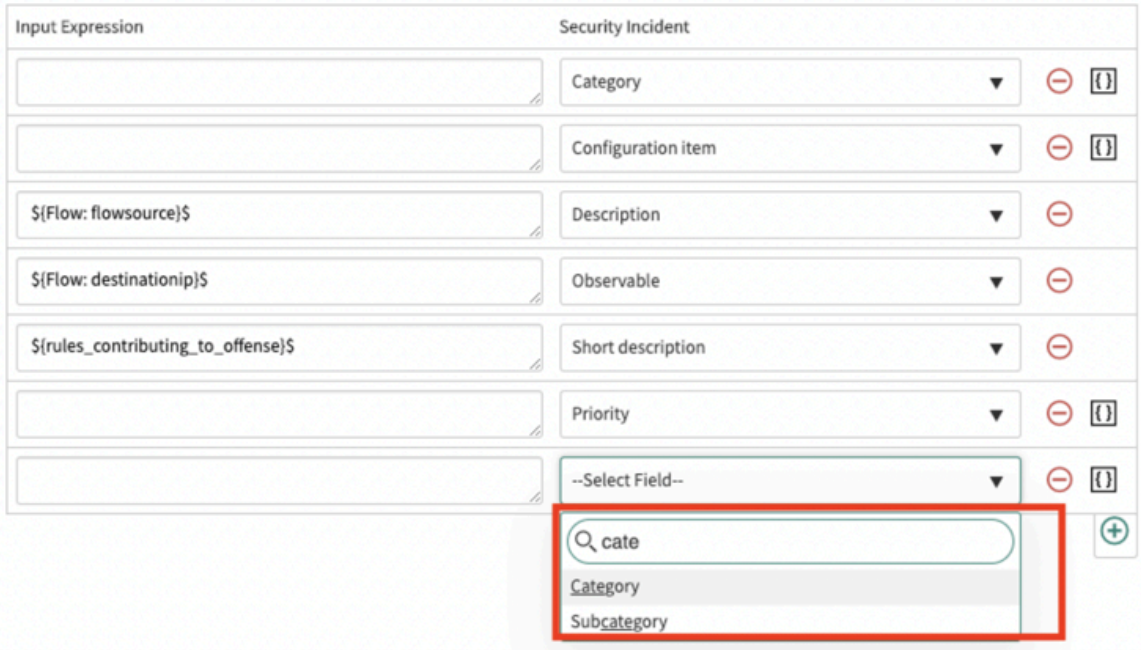
マッピングプロセスで違反、イベント、またはフローフィールドが見落とされたり、重複したりしないようにするために、フィールドは色分けされています。マップされていない残りのすべてのフィールドは青で表示されるのに対し、違反フィールドはグレー表示されるため、違反フィールドの色分けは、すでにマップされた違反値の追跡に役立ちます。色分けすることで、セキュリティインシデントに追加されたフィールド値、およびマップされていない残りの重要な違反情報を視覚的に把握できます。

左側のライトブルーのフィールドは、違反フィールドがまだ未選択で、セキュリティインシデントにマップされていないことを示します。受信違反、受信イベント、または受信フローフィールドをセキュリティインシデントの 2 つ以上のフィールドに関連付けることがあります。灰色のフィールドは、フィールドが選択され、セキュリティインシデントのフィールドにマッピングされていることを示します。この色分けは、マッピングを追跡するのに役立ちます。

3. フォームの右側のセキュリティインシデントで表示されるデフォルトフィールドにフィールドを追加するには、次のステップを実行します。
   a. グリッドの下部にある [SIR インシデントフィールドマッピング] セクションのフォームの右側で、プラス (+) アイコンをクリックします。新しいフィールドが表示されます。
   b. [セキュリティインシデント] 列で表示されている選択リストを展開し、フィールドを選択します。

      新しいフィールドの展開された選択リストでは、一部のフィールドが網掛けされています。次の図では、セキュリティインシデントにマッピングされているため、カテゴリのバックグランドがグレーになっています。フォームの左側の違反フィールドの色分け同様、右側にあるセキュリティインシデントフィールドのこの色分けも、すでにマップされた SIR インシデントフィールドを追跡するのに役立ちます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



> **注:**
> 同じセキュリティインシデントに複数の観測事象を表示できるため、[観測事象] フィールドを異なる値で複数回マップできます。同様に、[構成アイテム] フィールドと [作業メモ] フィールドは複数の値をサポートします。複数の値をサポートできないフィールドに 2 つの値をマッピングしようとすると、インシデントをプレビューするときに、フィールドに値がないことを示すエラーメッセージが表示されます。同様に、セキュリティインシデントのフィールドに複数のオプションを選択できる選択リストがあり、選択リストに表示されていないフィールドにオプションをマップしようとすると、そのフィールドはセキュリティインシデントに入力されません。

c. または、新しい行の [検索] フィールドに値を入力します。

d. フォームの左側で違反フィールドを選択し、右側の適切なセキュリティインシデントフィールドにドラッグアンドドロップします。

4. [SIR インシデントフィールドマッピング] セクションのフィールド名の横にある - アイコンを使用してフィールドを削除します。
5. フィールドの値をマッピングに追加するか、削除して、マッピングを続行します。

複数の値を持つ違反フィールド

- ベース製品で利用可能な [カテゴリ] や [ユーザー] フィールド (影響を受けるユーザー、担当者など) などのセキュリティインシデントフィールドは、複数の値をサポートしていません。
- 次の IBM QRadar フィールドは複数の値をサポートしています。
  - `categories`
  - `destination_networks`
  - `source_address_ids`
  - `local_destination_address_ids`
  - `remote_destination_ips`
  - `rules_contributing_to_offense`
  - `users`

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

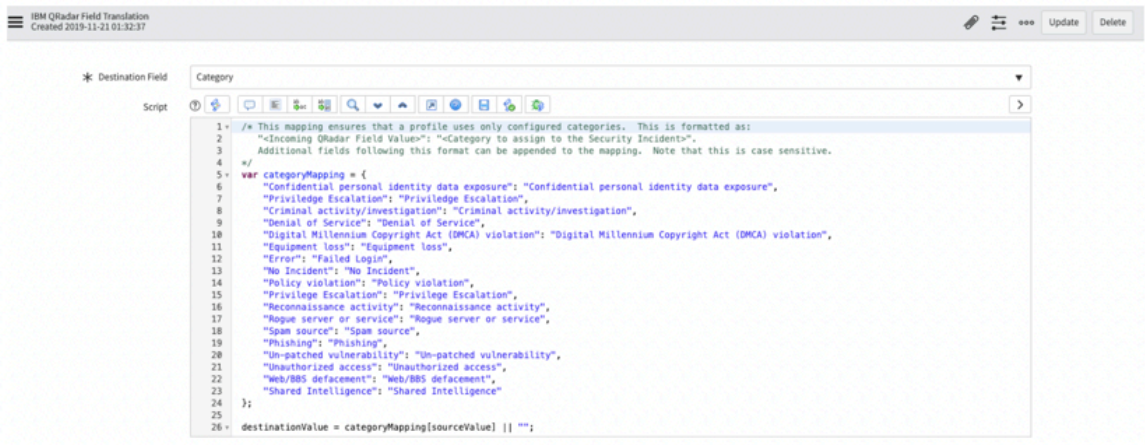
上記のフィールドを CI および観測事象タイプフィールド以外の セキュリティインシデントレスポンス フィールドにマッピングする必要がある場合は、リストタイプの新しい セキュリティインシデントレスポンス フィールドを作成して、上記のフィールドをマッピングに使用する必要があります。

注:
デフォルトでは、非参照リストタイプフィールドのみがサポートされています。

フォーマットフィールド変換

特定の場合、IBM QRadar の違反フィールド値は SIR セキュリティインシデントのフィールドに直接変換されないことがあります。これらの値については、マッピングステップでスクリプトエディターを使用してセキュリティインシデントのフィールド値をフォーマットできます。類似しているが同一ではない値をフォーマットする場合は、スクリプトエディターを使用します。たとえば、スクリプトエディターで、マルウェアアラートとウィルス感染のカテゴリ値がソースカテゴリでは異なるフィールド値であっても、フォーマットフィールド変換機能を使用して、両方の値が SIR セキュリティインシデントで [カテゴリ] フィールドの一般的な悪意のあるコードアクティビティに変換される場合があります。

スクリプトエディターを使用するには、 をクリックします。スクリプトエディターが表示されます。



スクリプトへの変更を入力し、[更新] をクリックして変更を保存し、 [マッピング] ページに戻ります。

インシデント生成条件

マッピングセクションが完了すると、フィルター条件を設定して、どの違反でセキュリティインシデントが作成され、どの違反がフィルタリングで除外されるか (低優先度の違反など) を指定できるようになります。インシデント生成条件ビルダーで同じフィールド値を使用して、セキュリティインシデントを作成する際に受信違反が満たす必要がある追加の条件を定義することができます。インシデント生成条件を設定するには、次のステップを実行します。

1. フォームの [インシデント生成条件] セクションまでスクロールし、[条件に基づいてフィルター] チェックボックスをオンにして、オプションを有効にします。

   フィルター条件ビルダーが表示されます。これらのフィルターを使用して、フィールドで説明されている特定の条件に一致するセキュリティインシデントを作成します。

   フィルター条件ビルダーの最初のフィールドの選択リストオプションは、取り込まれた違反の [サンプル QRadar 違反の取り込み] セクションに表示されるフィールドと一致します。これらのフィールドは動的で、取り込む違反に応じて変更されます。入力する条件は大文字と小文字が区別され、IBM QRadar 違反の値と正確に一致する必要があります。フィルターフィールドに入力す

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

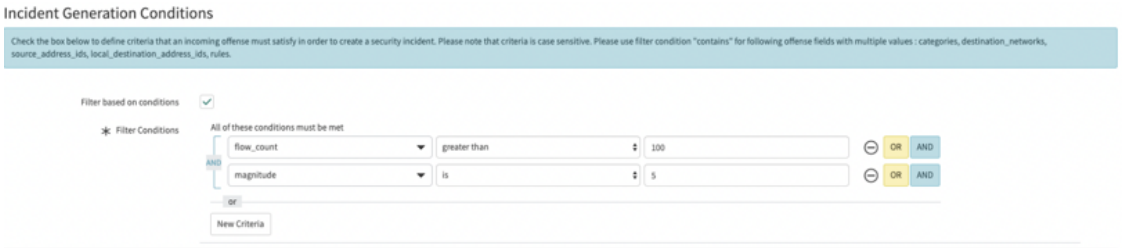
自動翻訳

る値が不明な場合、IBM QRadar コンソールに戻り、違反をレビューしてキーワードを確認することができます。

> **注:**
> *categories*、*destination_networks*、*source_address_ids*、*local_destination_address_ids*、の各違反フィールドには複数の値を設定できます (値はアレイに格納されます)。フィルター条件は文字列のみ取得できるため、これらのフィールドに包含フィルター条件を使用して、データが正確にフィルタリングされるようにする必要があります。

2. 条件ビルダーの選択リストとフィールドを使用して、最初の行のフィルターを設定します。
3. 条件を追加するには、フィールドの右側にある [**AND**] または [**OR**] をクリックします。
   - [**AND**] を選択した場合は、すべての条件に一致する必要があります。
   - **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。
4. (オプション) 2 番目の行で、2 番目のフィルター条件を設定します。

次の画像は、セキュリティインシデントが作成される前に一致する必要がある 2 つの条件を含む例です。



入力した両方のフィルタリング条件に一致した場合にのみセキュリティインシデントが作成されるように、インシデント生成条件を設定しました。

この種のインシデント生成条件フィルタリングにより、IBM QRadar で基本的なルールまたはフィルターを変更することなく、違反を絞り込み、作成する不要なセキュリティインシデントの数を制限することができます。追加のフィルター条件を設定する場合、すべての条件に一致する違反のみがインシデントにマップされます。

> **注:**
> 違反フィールドの名前に特殊文字 (引用符 (“)、ハイフン (‘)、アンダースコア (-)、アンパサンド (@) など) が含まれる場合、フィルタリングのために特殊文字を置き換える必要があることがありますが、数値サフィックスは重複する違反名で別のフィールドに追加されます。たとえば、最初の違反フィールドが alerts.alert で、2 番目の違反フィールドが alerts@alerts の場合、残りの標準的なテキスト文字は同じであるため、これらのフィールドは一意に識別されません。この場合、サフィックスが 2 番目の違反フィールドに追加され、[フィルター条件] リストに表示されるときにフィールド名が「alerts@alert(1)」に変更されます。

類似の違反を処理して重複インシデントを防止する違反集計基準

類似の重複する可能性があるインシデントを作成するのではなく、既存の SIR セキュリティインシデントに受信違反を集計する追加の違反集計基準を定義します。この追加の集計機能では、各プロファイルのフィールド一致値基準を使用して、関連するすべての違反データを単一のセキュリティインシデントに配置することで、アクティブな重複するセキュリティインシデントの数を減らすことができます。基準を設定するには、以下のステップを実行します。

自動翻訳

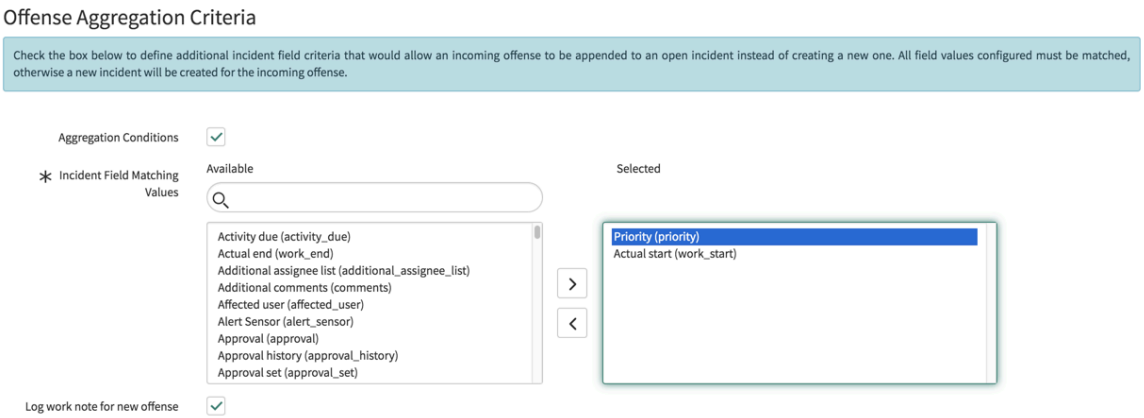
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. フォームで [違反集計基準] セクションにスクロールして、[集計条件] チェックボックスをオンにして、このオプションを有効にします。

   [値が一致するインシデントフィールド] 列が表示されます。これらのフィールド名は、SIR セキュリティインシデントで構成されたカスタムフィールドを含むセキュリティインシデントのフィールドです。

2. [利用可能] リストから、Now Platform の既存のセキュリティインシデントで照合するフィールド値を選択し、[選択済み] リストに移動させます。

   この受信アラートを既存のセキュリティインシデントに追加するには、選択するすべてのフィールド値が一致する必要があります。これには、複数の違反フィールド値がマッピングされている可能性がある [観測事象] や [構成アイテム] などのフィールドが含まれます。すべての値が一致している必要があります。値のサブセットのみが一致した場合、違反集計条件は満たされず、新しいセキュリティインシデントが作成されます。複数値フィールドのマッピングについては、以下のスクリーンショットを参照してください。



   新しい違反が、マッピングステップの集計フィールド条件で選択されたすべての値と一致する場合、新しい違反が同じフィールド値を持つ最新のオープンセキュリティインシデントに自動的に追加されます。セキュリティインシデントを扱う sn_si.analyst ロールを持つユーザーは、セキュリティインシデントの関連リストで、追加されたすべての集計違反を表示できます。このリストには、関連するタイムスタンプと集計されたフィールド値の詳細が表示されます。この情報は、これらの違反が既存のセキュリティインシデントに集計される理由を理解するのに役立ちます。このタブが表示されない場合は、 [関連リンク] の下のレコードの左側にスクロールし、[すべての関連リストを表示] リンクをクリックします。

3. セキュリティインシデントで最近追加された新しい違反の作業メモを記録するには、このチェックボックスをオンにしてこのオプションを有効にします。作業メモには、新しい違反が追加され、違反の詳細へのリンク、およびマッピングセクションの作業メモフィールドに追加されたその他の詳細が記録されます。

   IBM QRadar 違反からセキュリティインシデントのフィールドに値が正常にマッピングされました。また、インシデント生成フィルタリング基準を使用してセキュリティインシデントの作成を制限する追加条件も構成しました。違反フィールド値が設定した集計基準に一致する場合は、追加された違反が既存のセキュリティインシデントに追加されました。

4. [続行] をクリックして、プロファイル設定を続行します。次のステップでは、SIR セキュリティインシデントにマッピングしたフィールドをプレビューします。

IBM QRadar 統合でのセキュリティインシデントのプレビュー

マッピングステップを完了したら、SIR セキュリティインシデントでマッピングした値をプレビューします。このプレビューステップでは、セキュリティインシデントに表示するすべての違反フィールドがマッピングされていることを確認できます。

自動翻訳

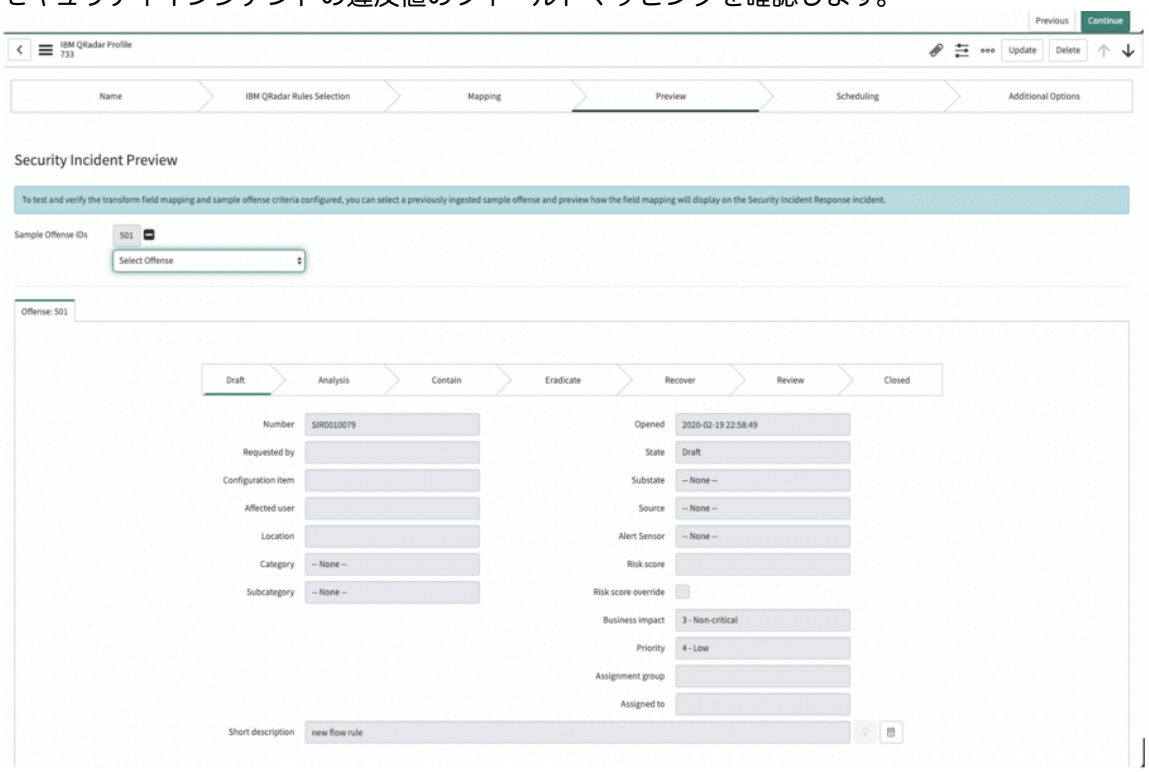
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_si.admin

このタスクについて
sn_si.admin ロールを持つユーザーは、セキュリティインシデントをプレビューし、必要に応じてマッピングを再編集して、エラーのあるフィールドを修正するか、欠落しているデータを入力します。プレビューが正常に完了しない場合、スケジュール設定ステップに進むことはできません。SIR セキュリティインシデントのプレビューは、セキュリティインシデントレスポンス 製品の実際のインシデントとして保存されません。

手順

1. セキュリティインシデントのプレビューが表示されない場合は、進捗状況バーの [プレビュー] をクリックします。
2. [サンプル違反 ID] 選択リストから、アイテムを選択します。
   セキュリティインシデントが表示されます。このビューは読み取り専用であり、このセキュリティインシデントのレコードは保存されません。
3. セキュリティインシデントの違反値のフィールドマッピングを確認します。



前の画像は、取り込まれたサンプルのマッピングエラーのあるプレビューの例です。

4. このエラーを解決するには、進捗状況バーの [マッピング] をクリックします。
5. マッピングを編集して誤った値を修正するか、欠落しているデータを入力します。
6. マッピングを再度プレビューし、エラーメッセージに記載されているエラーの修正を続行します。

次のタスク
エラーメッセージが表示されず、セキュリティインシデントのフィールドマッピングに問題がない場合は、次のステップでスケジュールを定義します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

IBM QRadar 統合のスケジュール定義

違反の取り込みのスケジュールを定義できます。このステップでは、必要に応じて、違反取得のデフォルトの設定を確認したり、スケジュールを変更したりすることができます。このステップでは、日付範囲を使用して履歴違反を取得することもできます。

始める前に

必要なロール：sn_si.admin

このタスクについて

[スケジュール] ステップで履歴違反を取り込むかどうかを選択できます。また、プロファイル構成に一致する将来の新しい違反と更新された違反をポーリングする頻度も選択します。

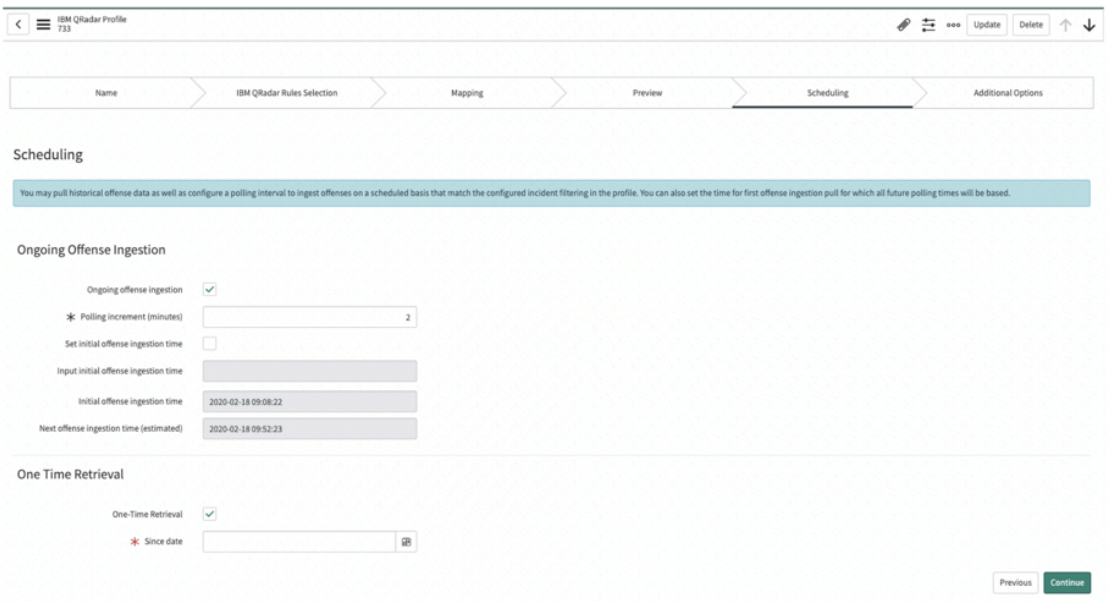
sn_si.admin ロールを持つユーザーは、これらのポーリング間隔をプロファイルごとに設定します。IBM QRadar 違反の取り込み統合のパフォーマンスは、ポーリング間隔が異なると影響を受ける可能性があります。スケジューリングでは、IBM QRadar サーバーのポーリングのオーバーヘッドを減らすことと、違反が作成または更新されたときにできるだけ早く通知することのバランスを取ることをお勧めします。どのプロファイルにも 5 分のデフォルト値が設定されていますが、必要に応じてこの設定を 1 分に変更することもできます。

新規および更新された違反のプル

ポーリングスケジュールが設定されると、スケジュール済みジョブは、以前にプルされたが、インシデントのフィルター条件を満たしていなかった新規違反と更新された違反の両方をプルします。これにより、違反が最初に作成されたときに存在しなくても、たとえば調査フェーズ中に更新が発生した後に存在する可能性がある条件に基づいて、インシデントを作成できます。特定の違反に対してインシデントが作成されると、その後の更新は無視されます。これは、違反がアクティブな ServiceNow セキュリティインシデントとして扱われていることが想定されるためです。ただし、以前に取り込まれたが、インシデント生成条件を満たしていない他のすべての違反は引き続きプルされ、アクティブなインシデントの一部になるまでインシデント生成条件と照合されます。

手順

1. 進捗状況バーに [スケジュール] ページが表示されない場合は、[スケジュール] を選択します。
2. IBM QRadar コンソールから違反をプルする方法とタイミングをスケジュールするものを選択します。



3. [続行] をクリックして、[他のオプション] ページに移動します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

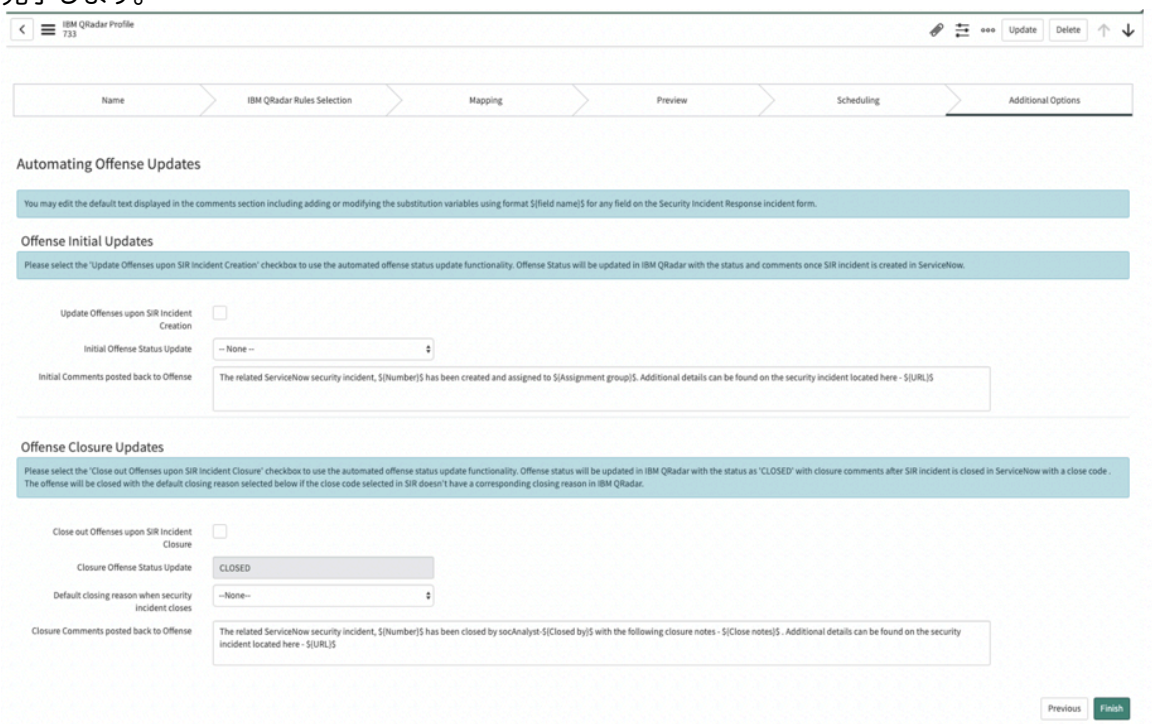
SIR インシデント状況に基づく違反の更新とクローズの自動化

IBM QRadar 統合には、違反からセキュリティインシデントを作成する機能と、セキュリティインシデント番号、アサイン先グループ、セキュリティインシデント URL などの関連するインシデントの詳細を使用して、セキュリティインシデントが作成および/またはクローズされると違反を更新する機能を許可する双方向インターフェイスがあります。

始める前に
必要なロール：sn_si.admin

手順

1. 進捗状況バーに [その他のオプション] ページが表示されない場合は、[その他のオプション] を選択します。
2. 以下の手順に従って、セキュリティインシデントが作成されたときに違反を更新するための構成を完了します。



3. [完了] をクリックして構成を完了し、プロファイルを [待機中] ステータスに移行します。
確認ダイアログが表示されます。これで統合のセットアップと構成が正常に完了しました。このプロファイルをアクティブ化して、スケジューリングに基づいて IBM QRadar コンソールから違反をプルします。

IBM QRadar 統合設定

このオプションを使用して、IBM QRadar 取り込み統合のデフォルトのシステムプロパティを変更します。

システムプロパティを変更するには、 *sn_si.admin* ロールを持つユーザーとしてログインし、次の場所に移動します。 **IBM QRadar** 統合 > **IBM QRadar** 統合の設定.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

IBM QRadar 統合の設定

プロパティ名	説明
24 時間内に作成できるセキュリティインシデント数の制限を強制します。 sn_sec_qradar.max_si_per_day	24 時間内に作成できるセキュリティインシデントの最大数を指定します。 • タイプ：整数 • デフォルト値：1000
単一のインシデントに集計できる違反数の制限を強制します。 sn_sec_qradar.max_aggregation_per_si	セキュリティインシデントの違反集計制限。たとえば、102 件の違反がある場合、最初の 100 件は security incident_1 に集計され、残りの 2 件は security incident_2 に集計されます。 • タイプ：整数 • デフォルト値：100
このプロパティは、AQL の期間を設定し、特定の違反について最新のイベント/フローをフェッチします。 sn_sec_qradar.on_demand_recent_days_limit	特定の違反について最新のイベントまたはフローをフェッチする日数を指定します。 • タイプ：整数 • デフォルト値：7
このプロパティは、特定の違反について取得された最近のイベントの数を制限します。 sn_sec_qradar.on_demand_event_limit	違反に対して取得されるイベントの数を指定します。イベントのタイムスタンプに基づいて、最新のイベントが最初に取得されます。 • タイプ：整数 • デフォルト値：100
このプロパティは、特定の違反についてフェッチされた最近のフローの数を制限します。 sn_sec_qradar.on_demand_flow_limit	違反に対して取得されるフローの数を指定します。フローのタイムスタンプに基づいて、最新のフローが最初に取得されます。 • タイプ：整数 • デフォルト値：100
このプロパティは、特定の違反について最近のフロー/イベントをフェッチする AQL のタイムアウト値 (秒) を設定します。 sn_sec_qradar.on_demand_timeout	• タイプ：整数 • デフォルト値：300
違反の AQL をポーリングするための、キューにあるレコードの検索 ID のタイムアウト (秒)。 sn_sec_qradar.sid_ttl	セキュリティインシデントを作成する前のキュー内の違反に対する AQL のタイムアウト。たとえば、90 件の違反がある場合、最初のバッチの AQL データに対して最初の 50 件の違反が処理され、残りの 40 件の違反は同じポーリング間隔で処理されます。 • タイプ：整数 • デフォルト値：300

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

IBM QRadar 統合の設定 (続く)

プロパティ名	説明
スケジュールされた統合でトリガーされたときに IBM QRadar で実行できる検索の数を制御するしきい値。 job.sn_sec_qradar.records_threshold_in_que_for_ad	ポーリング間隔で単一のバッチでフェッチする違反の数を指定します。 • タイプ：整数 • デフォルト値：50
これは、統合テーブルがクリーンアップされる日数です。 sn_sec_qradar.queue_item_expire	以下は統合テーブルです。 • sn_sec_qradar_events - IBM QRadar イベント • sn_sec_qradar_flows - IBM QRadar フロー • sn_sec_qradar_offense_updates - IBM QRadar 違反の更新 • sn_sec_qradar_offense_to_task - タスクに対する IBM QRadar 違反 • タイプ：整数 • デフォルト値：30
1 回限りの取得または進行中の取り込みのいずれかにおける、各プロファイルでのスケジュール済みジョブ実行ごとの違反制限。 sn_sec_qradar.max_offense_limit_per_run	1 回の取得で Now Platform にフェッチする違反の数を指定します。 • タイプ：整数 • デフォルト値：1000
違反の更新機能をアクティブ化するには、このプロパティを設定します。 sn_sec_qradar.get_offense_updates	**注:** この設定を有効にすると、セキュリティインシデントの作成が遅れる可能性があります。 • タイプ：true | false • デフォルト値：false

変更した統合設定は、プロファイルで定義されている次のポーリング間隔で適用されます。

オプション： **IBM QRadar** プロファイルをコピー

新しいプロファイルを作成する代わりに、既存のプロファイルとその関連設定をコピーします。複数のプロファイルを作成していて、既存のプロファイルの設定を再利用する場合は、時間を節約するためにプロファイルをコピーすることをお勧めします。

始める前に

必要なロール：sn_si.admin

このタスクについて

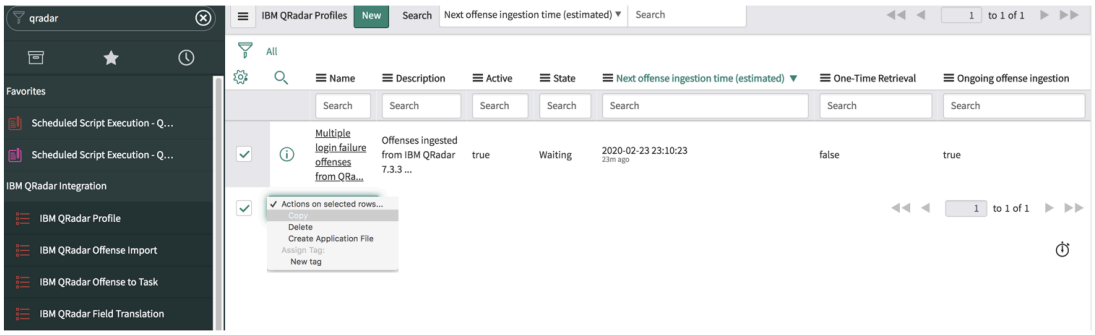
sn_si.admin ロールを持つユーザーがプロファイルをコピーすると、プロファイルの重複を避けるためにプロファイル名が最初に変更されます。また、コピーされたプロファイルは無効 (false) であるため、構成が完了する前に誤って有効になることはありません。既にプレビューおよび検証したセキュリティインシデントのプロファイルをコピーし、既存のマップを使用します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

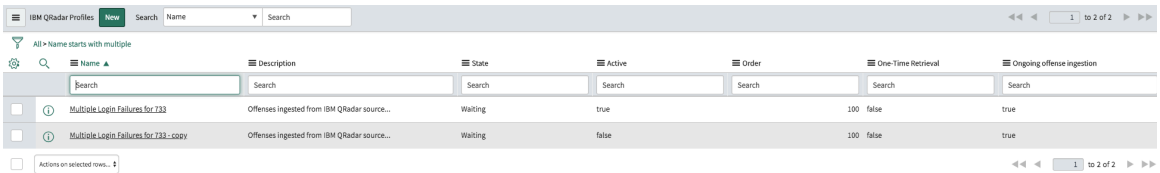
手順

1. 次のように移動する。 **All** (すべて) > **IBM QRadar** 統合 > **IBM QRadar** プロファイル.
2. 表示される [IBM QRadar プロファイル] リストでコピーするプロファイルを選択し、 [選択した行のアクション] 選択リストから [コピー] をクリックします。



プロファイルがコピーされ、リストに表示されます。コピーには、マッピングとスケジュール設定を含む元のプロファイルのすべての設定が含まれます。プロファイルの名前に「copy」が含まれています。元のプロファイルは有効ですが (true)、この時点でコピーは無効になります (false)。必要に応じて、コピーしたプロファイルの値を編集して名前を変更し、構成設定を新しいプロファイルに適用することもできます。

注:
プロファイルに別のソースを選択する場合は、プロファイルに新しいルール (IBM QRadar ルールの選択) を選択する必要があります。ただし、同じソースを使用して新しいルールを選択すると、サンプル違反はクリアされます。



既存のプロファイルから新しいプロファイルに設定が正常にコピーされました。プロファイルをアクティブ化する必要があるため、[アクティブ] 列のステータスが false に設定されていることに注意してください。

次のタスク
構成ステップが完了すると、新しいプロファイルをアクティブ (有効) にするように求められます。

ドメインセパレーションと **IBM QRadar** 違反の取り込み

IBM QRadar 違反の取り込みではドメインセパレーションがサポートされています。 ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル：ベーシック

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- アプリケーションサービスプロバイダーのユースケースに合わせてデータが適切なドメインに送られるようにするビジネスロジックが存在します。
- このアプリケーションは、ドメインセパレーションを完全にサポートしています。ドメインセパレーションには、ユーザーインターフェイス、キャッシュキー、レポート、ロールアップ、および集計からのドメインの分離が含まれます。
- インスタンスのオーナーは、複数のテナント間で正常に機能するようにアプリケーションをセットアップする必要があります。

サンプルユースケース：サービスプロバイダーがチャットを使用してテナント顧客のメッセージに応答する場合、お客様がサービスプロバイダーの応答を確認できるようにする必要があります。

サポートレベルの詳細については、「アプリケーションでのドメインセパレーションのサポート」を参照してください。

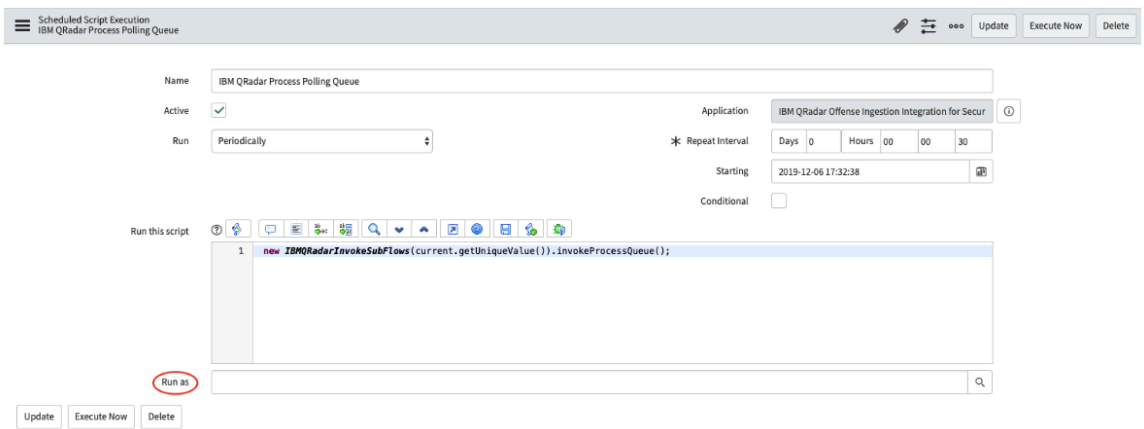
IBM QRadar 違反の取り込みにおけるドメインセパレーションの仕組み

ドメインセパレーションを実現するには、次の手順に従います。

- それぞれのドメインで *sn_si.admin* ロールを持つユーザーを作成します。

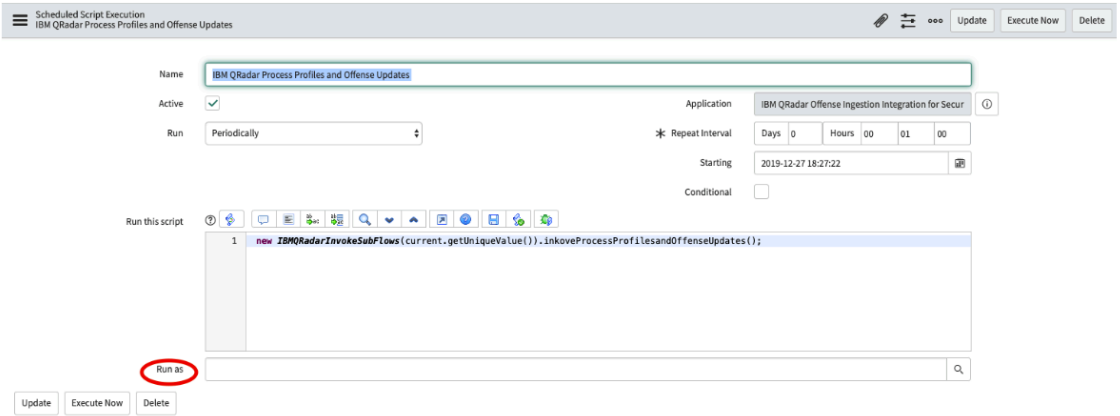
> **注:**
> プロファイルを作成するときは、ドメインピッカーを使用して特定のドメインを選択します。親ドメインにユーザーを作成して、後でプロファイルのドメインを変更しないでください。プロファイルのドメインごとに *sn_si.admin* ロールを持つ特定のユーザーが必要です。このユーザーを使用して、プロファイルの設定を作成または変更します。

- 既存のスケジュール済みジョブを無効にします。
- すべてのドメインの IBM QRadar プロセスポーリングキュー、IBM QRadar プロセスプロファイル、および違反の更新スケジュール済みジョブを複製します。
- [実行方法] をシステムユーザーからそれぞれのドメインの *sn_si.admin* ロールを持つユーザーに変更してから、スケジュール済みジョブを実行します。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



関連情報

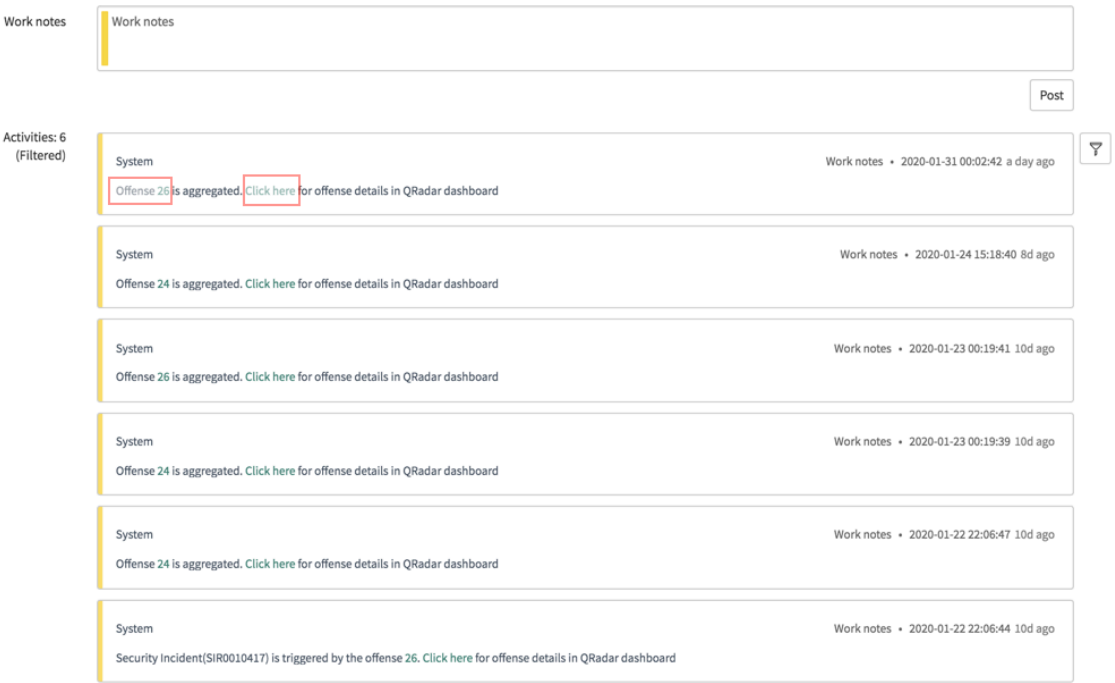
サービスプロバイダーのドメインセパレーション

違反取り込み後のセキュリティインシデントレスポンスフォーム

IBM QRadar 違反が取り込まれると、セキュリティインシデントが作成され、そのセキュリティインシデントレコードに対応する更新が実行されます。

作業メモ

セキュリティインシデントをトリガーした違反の詳細を含む作業メモが投稿されます。

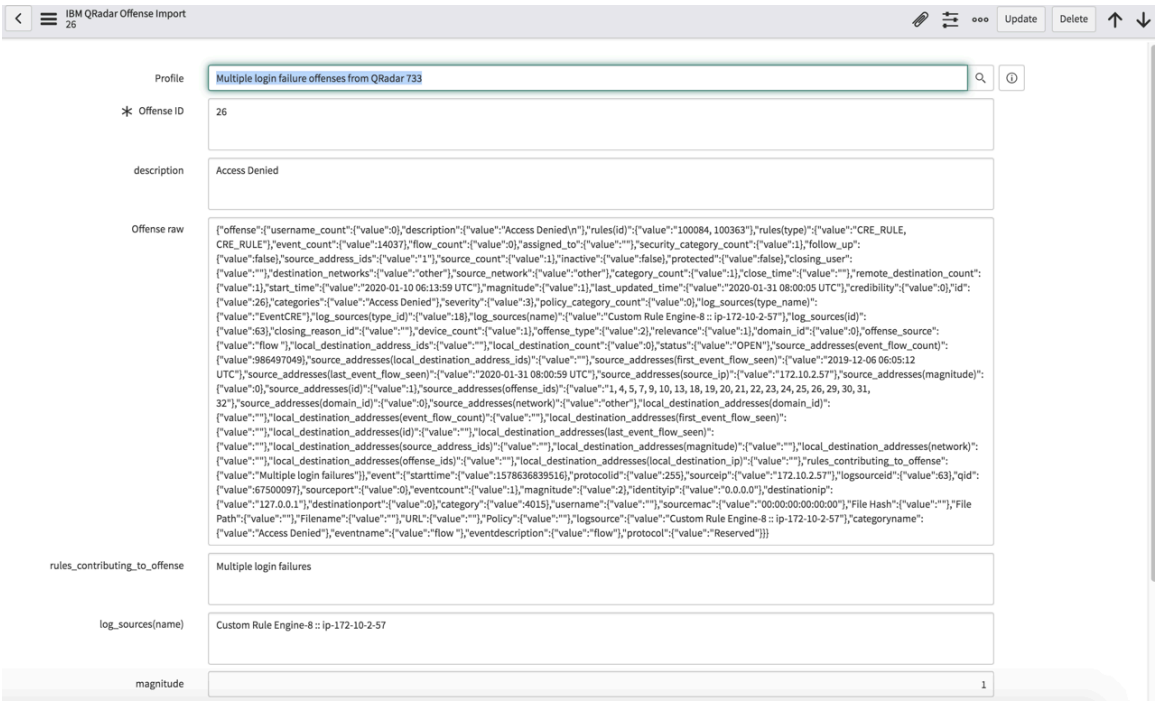


違反リンクをクリックして、内部セキュリティインシデントレコードに移動します。[ここをクリック] ハイパーリンクをクリックすると、違反の詳細を表示できる IBM QRadar ダッシュボードに移動します。

IBM QRadar 違反フィールドのセキュリティインシデントレスポンスフィールドへのマッピング で説明されているように、違反集計基準で [新規違反の作業メモを記録] オプションを選択した場合、違反が集計されると作業メモが投稿されます。

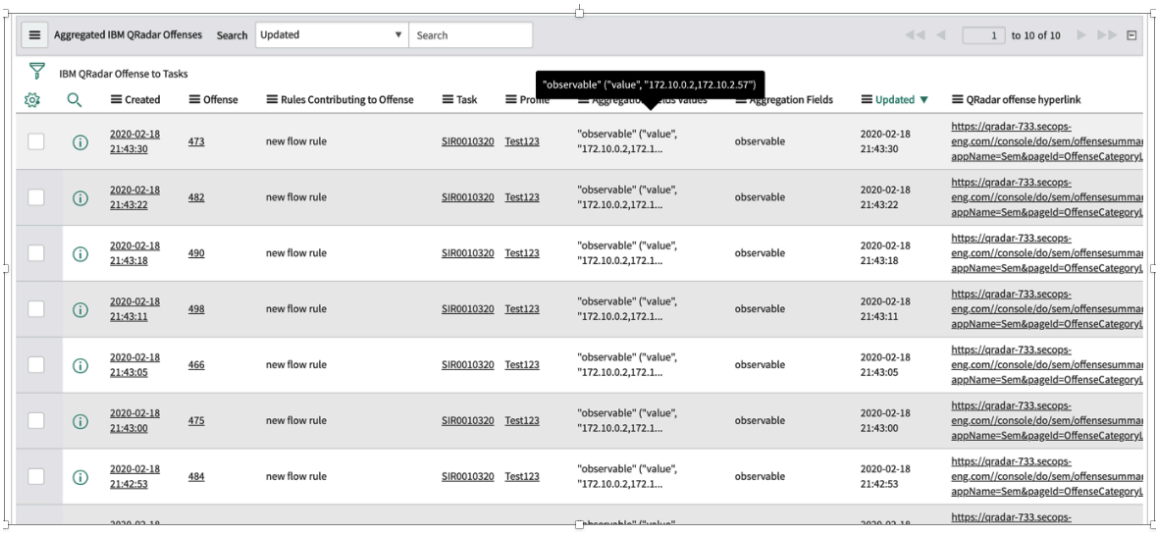
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



集計された違反

クリックします 関連リスト > 集計された **IBM QRadar** 違反 セキュリティインシデントに集計された違反を表示します。QRadar 違反のハイパーリンクをクリックして、IBM QRadar ダッシュボードで違反を表示します。

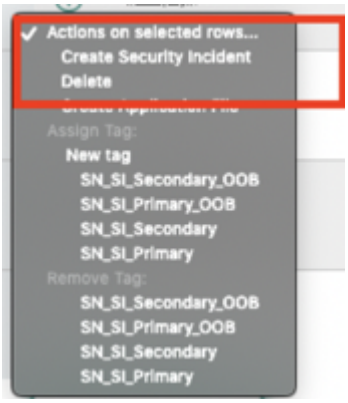


セキュリティインシデントの作成：リストから違反を選択し、[アクション] メニューをクリックして、[セキュリティインシデントの作成] をクリックします。このオプションは、違反のセキュリティインシデントを作成します。この違反は親セキュリティインシデントからは集計されません。

違反レコードの削除：リストから違反を選択し、[アクション] メニューをクリックして、[削除] をクリックします。このオプションは、違反レコードを削除します。

自動翻訳

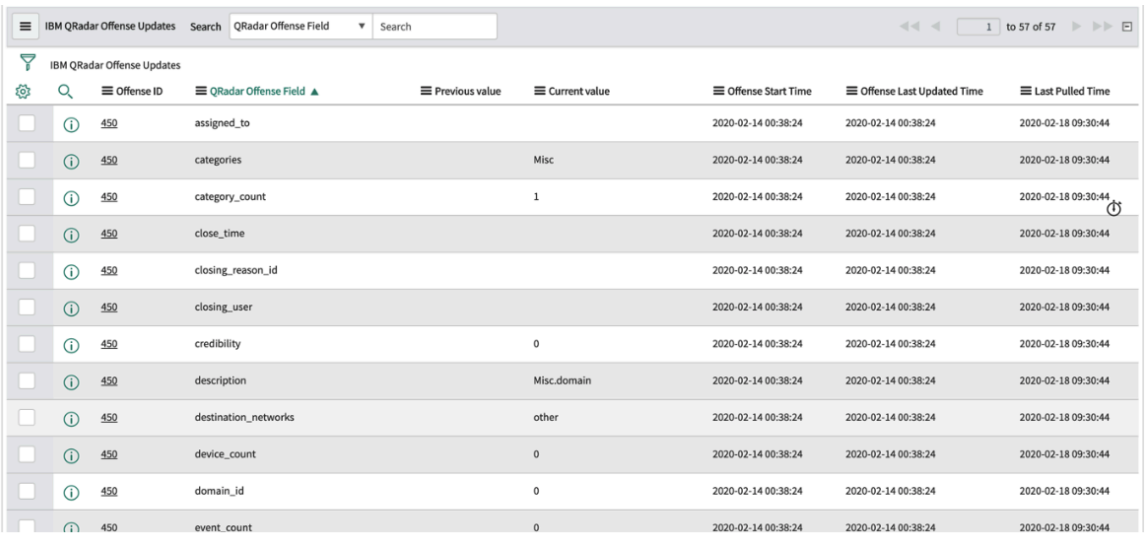
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



IBM QRadar 違反の更新

これにより標準違反フィールドとカスタム違反フィールドが表示され、ポーリング間隔ごとに違反の変更が追跡されます。IBM QRadar ダッシュボードに移動せずに違反の更新が直接表示されるため便利です。値の変更は [前の値] フィールドと [現在の値] フィールドに表示されます。

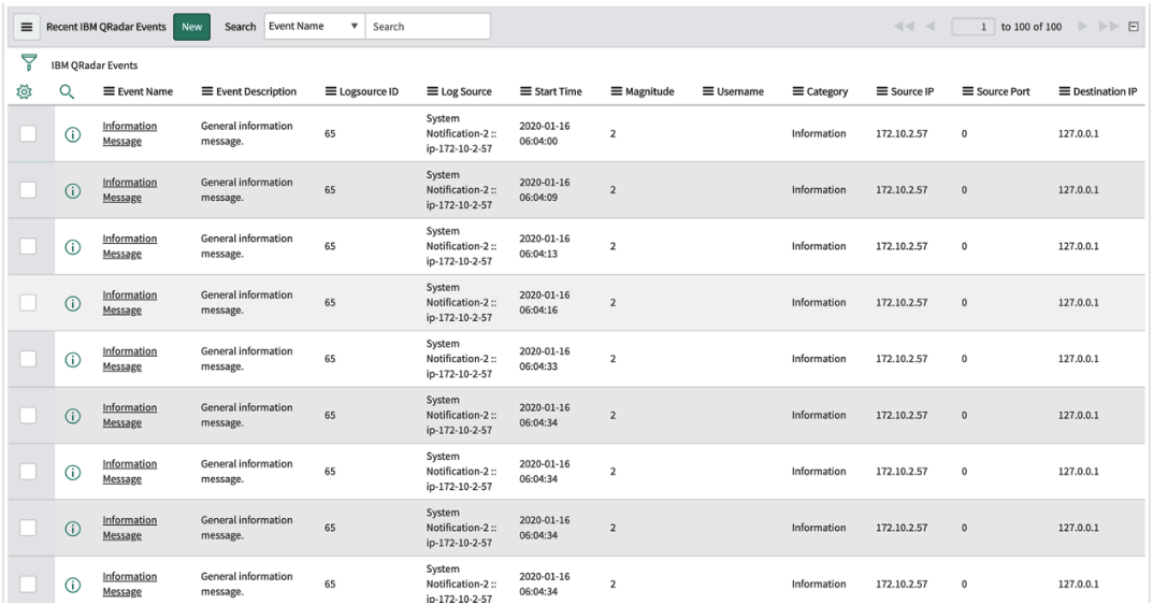
違反更新機能を有効にするには、次に移動します: **IBM QRadar** 統合 > **IBM QRadar** 統合の設定 をクリックし、「 違反の更新機能を有効にするには、このプロパティを設定します」を有効にします。デフォルトでは、この設定は無効になっています。



最新の IBM QRadar イベント

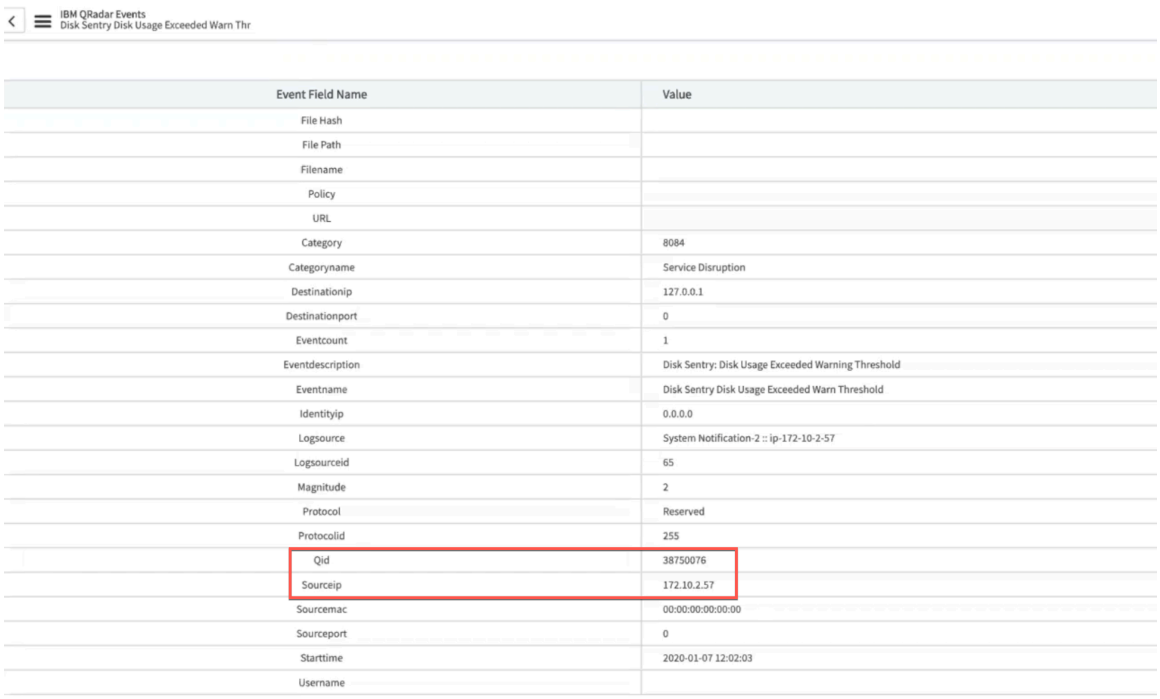
[関連リンク] の [最近の **IBM QRadar** イベントをフェッチ] オプションをクリックして、最新の IBM QRadar イベントを表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



デフォルトでは、最大 100 件のイベントが表示されます。このデフォルト設定は IBM QRadar 統合設定 で変更できます。

注:
上の画像は、違反に関連付けられた標準イベントフィールドを示しています。カスタムイベントフィールドを設定してマッピングした場合 (「IBM QRadar 違反フィールドのセキュリティインシデントレスポンスフィールドへのマッピング」を参照)、[イベント名] リンクをクリックして [リストビュー] に表示できます。

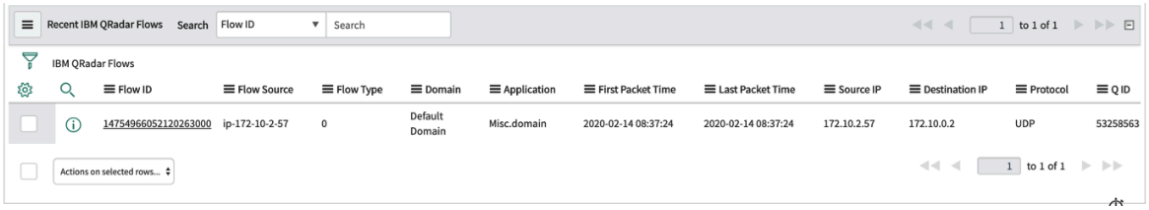


最近の **IBM QRadar** フロー

Integration Hub とフローデザイナーを使用すると、いくつものフロー、サブフロー、およびアクションを IBM QRadar 統合で使用できます。[関連リンク] の [最近の **IBM QRadar** フローをフェッチ] オプションをクリックすると、最新のフローが取得されます。これらのフローを表示するには、[最近の **IBM QRadar** フロー] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳



デフォルトでは、最大 100 件のフローが表示されます。このデフォルト設定は IBM QRadar 統合設定 で変更できます。

注:
上の画像は、違反に関連付けられた標準フローフィールドを示しています。カスタムフローフィールドを設定してマッピングした場合 (「IBM QRadar 違反フィールドのセキュリティインシデントレスポンスフィールドへのマッピング」を参照)、[フロー ID] リンクをクリックして [リストビュー] に表示できます。

フローデザイナーと **Integration Hub** を使用した **IBM QRadar** 違反の取り込み統合

フローデザイナーと Integration Hub 機能を使用して、いくつかのサブフローとアクションが IBM QRadar 違反の取り込み統合の一部としてビルドされました。

次の IBM QRadar サブフローを利用できます。

- 接続と資格情報の検証：初期設定でホストと認証情報を検証するために構成タイルで使用されます。
- IBM QRadar ルールの取得：IBM QRadar 内のすべてのアクティブなルールを取得するために、プロファイルセットアップの [ルール] セクションで使用されます。このサブフローは非同期にトリガーされます。
- IBM QRadar からサンプル違反データをフェッチ：サンプルデータをフェッチするために、プロファイルセットアップの [マッピング] セクションで使用されます。このサブフローは非同期にトリガーされます。
- IBM QRadar 違反ステータスの更新：スケジュール済みジョブで毎分トリガーされ、セキュリティインシデントが作成またはクローズされたときに IBM QRadar 内の違反を更新します。
- スケジュール済みジョブとキュー違反からプロファイルを処理：スケジュール済みジョブで毎分トリガーされ、ポーリング間隔に基づいてプロファイルごとに違反を取得します。これにより違反が取得され、さらに処理するためにポーリングテーブルのキューに入れられます。
- 一括でポーリングキューとポーリングを処理：ポーリングテーブルキューを処理するために、スケジュール済みジョブで 30 秒ごとにトリガーされます。
- 最新の IBM QRadar フローを取得：違反の最新フローを取得するために、セキュリティインシデントフォームリンクからトリガーされます。
- 最新の IBM QRadar イベントをフェッチ：違反の最新イベントを取得するために、セキュリティインシデントフォームリンクからトリガーされます。

これらのサブフローを表示するには、 *sn_si.admin* ロールを持つユーザーとしてログインし、次の場所に移動します。 **Flow Designer** > デザイナー. 上記のサブフローの [名前] リンクをクリックすると、サブフローの詳細が表示されます。

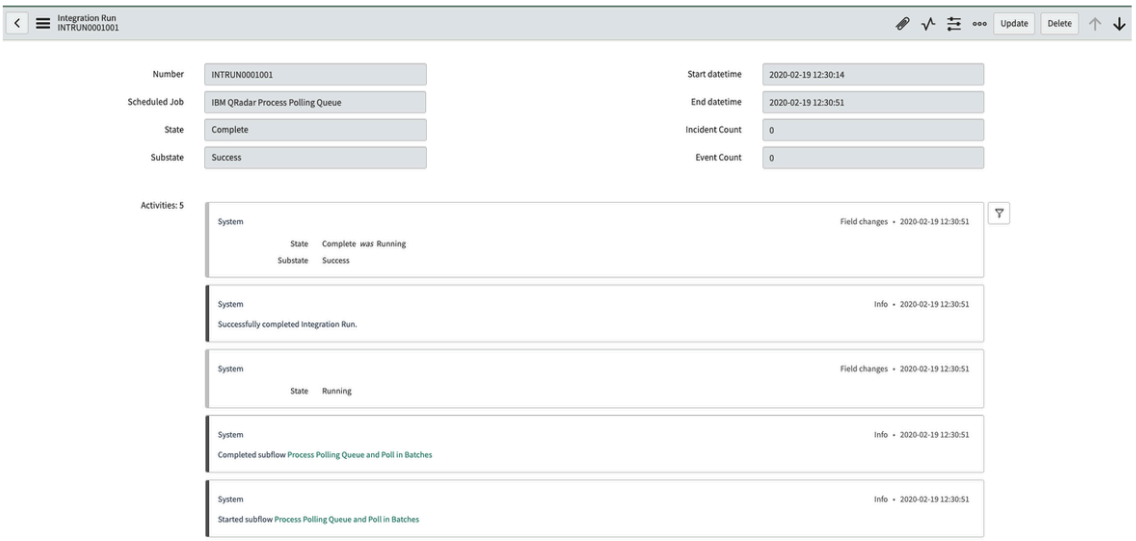
IBM QRadar 違反の取り込み統合のトラブルシューティング

このセクションでは、IBM QRadar 違反の取り込み統合に関連する重要なトラブルシューティングのヒントとよくある質問について説明します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 統合の実行：スケジュール済みジョブの実行が開始されると、ログ、エラー、および警告を含む統合実行レコードが表示されます。取得した違反の数と、スケジュール済みジョブの実行で作成されたインシデントの数も表示されます。sn_si.analyst ロールを持つユーザーは、統合の実行中にエラー/プロファイルの取得に失敗したかどうかを確認できます。

  統合実行の作業メモで、実行されたサブフローへのリンクが提供されます。sn_si.analyst ロールを持つユーザーは、sn_event_ingestion_integration_run テーブルで発生したエラーを確認できます。統合の問題をトラブルシューティングするには、最初に統合の実行を確認する必要があります。エラーは、スケジュール済みジョブの実行ごとに統合実行レコードに作業メモとして記録されます。



- SSL の問題：IBM QRadar クラウドインスタンスに接続する場合は、インスタンスに期限切れでない有効な CA 証明書があることを確認してください。RSA または独自の証明書をプラットフォームにインポートし、証明書の共通名がホスト名と一致しているか確認できます。詳細については、「https://support.servicenow.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D55ecefd61bf3774cada243f6fe4bcb44」を参照してください。
- 不完全なプロファイル：プロファイルの設定中に、[他のオプション] (SIR インシデント状況に基づく違反の更新とクローズの自動化) セクションで [完了] ボタンをクリックして、プロファイルが取り込みを待機していることを示す [待機中] ステータスに移行したことを確認する必要があります。
- プロファイルの検証：統合が正常に機能しているかどうかを検証するには、プロファイルステータス、プロファイルの前回の取得日、違反インポートテーブル、タスクに対する違反テーブルの各レコードを確認します。
- MID サーバー構成：IBM QRadar アプリケーションをオンプレミスにインストールする場合は、MID サーバーを構成した後に MID サーバーアプリケーションを作成する必要があります。統合の構成タイルでは、MID サーバー名ではなく MID サーバーアプリケーション名を使用する必要があります。

  注:
  デフォルトの MID サーバータイムアウトは 30 秒です。タイムアウト期間を無効にする手順については、「<link>」を参照してください。これはシステム全体の変更であり、他の統合に影響を与える可能性があることに注意してください。

- 違反の更新：*sn_sec_qradar.get_offense_updates* プロパティを有効にしていて、セキュリティインシデントの作成の遅延に気付いた場合は、このプロパティを無効にします。ポーリング間隔が短く、QRadar の違反負荷が高いと、キューの負荷が増加するため、このプロパティを有効にしないでください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- セキュリティインシデントのイベント、フローデータ、remote_ip、またはユーザーデータの欠落：セキュリティインシデントにイベント、フローデータ、remote_ip、またはユーザーのデータがない場合は、*sn_sec_qradar.sid_ttl* パラメーターのタイムアウト (秒) を増やします。期間を長くすると、AQL が各違反の解析を完了するまでセキュリティインシデントの作成が遅延します。
- タイムアウト：アプリケーションログでタイムアウトエラーを表示する場合は、次のフローデザイナーアクションを確認して変更します。

フローデザイナーアクション

パラメーター	アクション
サンプル違反をフェッチ `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 60000);`	期間をミリ秒単位で確認および更新します。
サンプル違反をフェッチ `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs);`	*executeAction* のパラメーターを追加し、期間をミリ秒単位で入力します。
ポーリングテーブルのプロファイルレコードとキューレコードの違反をフェッチ `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 180000);`	期間をミリ秒単位で確認および更新します。
テスト接続 **REST** のためのラッパー `var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.test_connection_rest', rest_inputs);`	*executeAction* のパラメーターを追加し、期間をミリ秒単位で入力します。
API 認証情報 **REST**を検証するラッパー `var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.validate_credentials_rest', rest_inputs);`	*executeAction* のパラメーターを追加し、期間をミリ秒単位で入力します。
IBM QRadar 違反更新の **REST** ステップ `var result = sn_fd.FlowAPI.executeAction('sn_sec_qradar.'+restStep, inputs,60000);`	期間をミリ秒単位で確認および更新します。

IBM QRadar - インシデント拡張統合

IBM QRadar - インシデント拡張統合はログを検索し、関連するサイティング情報をセキュリティインシデントに追加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

探索	セットアップ
セキュリティインシデントレスポンス の統合	• IBM QRadar の開始 - インシデント拡張統合 • サイティング検索設定レコードの作成

使用	開発
• サイティング検索の実行 • Security Operations Integration - サイティング検索フロー • Security Operations - QRadar サイティング検索フロー • サイティング検索の詳細の表示 • サイティング検索結果の表示	• ServiceNow セキュリティオペレーション 統合開発のガイドライン • 統合を作成するためのヒント • 開発者トレーニング • 開発者ドキュメント

トラブルシューティングとヘルプ

- 統合のトラブルシューティング
- Security Operations Community で質問や回答をする
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

自動翻訳

IBM QRadar の開始 - インシデント拡張統合

IBM QRadar は、 セキュリティオペレーション と簡単に統合できるエンタープライズセキュリティ情報およびイベント管理 (SIEM) 製品です。IBM QRadar - インシデント拡張統合を使用する前に、ServiceNow Store から統合をダウンロードし、適切な API Base URL と API キーを追加する必要があります。

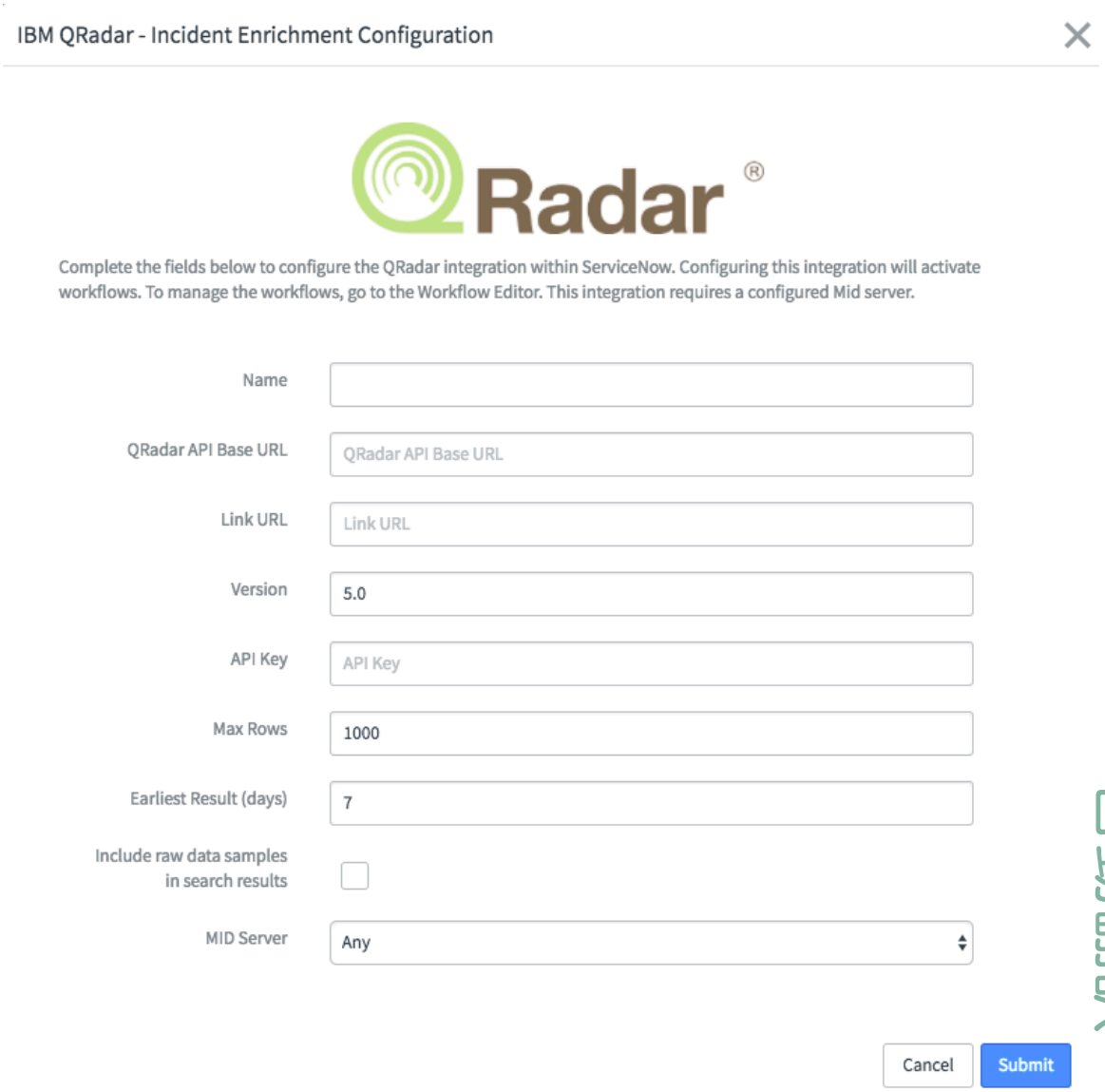
始める前に

必要なロール：sn_si_admin

手順

1. から統合をダウンロードします ServiceNow Store.
2. インストールが完了したら、IBM QRadar にアクセスし、IBM QRadar プロファイルの下の API Base URL と API キーを取得します。
3. インスタンスで、 セキュリティオペレーション > 統合 > 統合設定.
   利用可能なセキュリティ統合が一連のカードとして表示されます。
4. IBM QRadar - インシデント拡張カードで、[新規] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

5. 必要に応じて、フィールドに入力します。

フィールド	説明
名前	この構成の名前。
QRadar API のベース URL	IBM QRadar サイトから取得したベース URL。
リンク URL	[オプション] IBM QRadar インスタンスに接続するリンク URL (利用可能な場合)。
バージョン	IBM QRadar バージョン。 5.0 がデフォルトです。
API キー	IBM QRadar サイトから取得した API キー。
最大行数	検索する行の最大行数。
最も早い結果 (日数)	表示する最も早い結果 (日数単位)。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
検索結果に生データサンプルを含める	サイティング検索結果に生データのサンプルを含めるには、これを選択します。返されるデータの量は、[セキュリティインシデントレスポンス] プロパティの [生データの行数] プロパティの設定によって異なります。
MID サーバー	[任意] を選択して、 任意のアクティブな MID サーバーを使用するか、特定の MID サーバー名を選択します。

注:
この統合を設定すると、ワークフローが有効になります。ワークフローを管理するには、[ワークフローエディター] に移動します。

6. **[Submit]** をクリックします。
   統合構成カードが表示されます。
7. 新しい構成カードを表示すると、[構成] または [削除] をクリックして、構成を変更または削除できます。
8. 統合構成カードの元のリストに戻るには、[構成を表示] ドロップダウンから [いいえ] を選択します。

LogRhythm の概要

この統合のマッピングの柔軟性により、アナリストはイベントと関連アラームデータを確認し、Now Platform セキュリティインシデントに統合してさらに調査および修正することができます。

アラームプロファイルが Now Platform インスタンスに作成され、Now Platform セキュリティインシデントでのさまざまな LogRhythm アラームフィールドの表示方法をカスタマイズできます。提供されているアラームフィールドのデフォルトマッピングは、顧客固有のニーズに合わせて編集できます。

次の図は顧客の環境の例です。イベントが Now Platform® インスタンスでのセキュリティインシデントの作成をトリガーすると、MID サーバーを介して、またはそれなしで LogRhythm クライアントコンソールからアラームをプルする要求が Now Platform® インスタンスから送信されます。

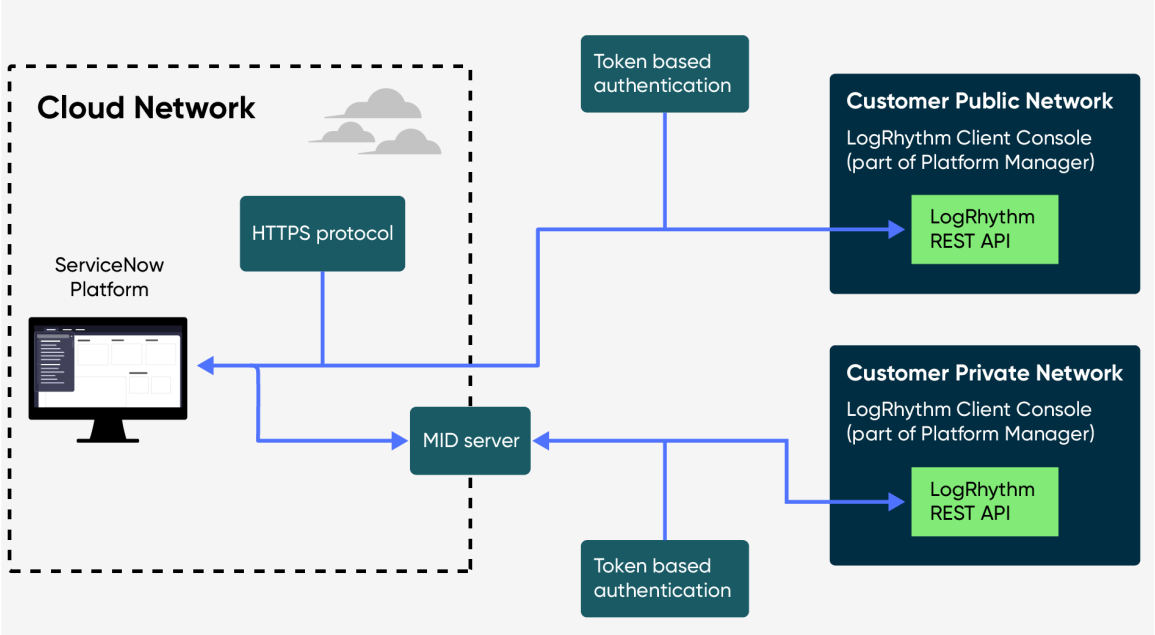
REST API キーは、LogRhythm クライアントコンソールでの Now Platform® による認証に使用されます。この接続により、Now Platform インスタンスは設定されたプロファイルに基づいて個々の LogRhythm アラームをプルできます。

REST API は、REST API によってアクセスされないメッセージの詳細を収集するために使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

LogRhythm 統合



主な機能

この統合の主な機能は次のとおりです。

- フィッシングやマルウェアなど、さまざまなアラームタイプに対して複数のアラームプロファイルを作成できる柔軟性
- 関連付けられている SIR セキュリティインシデントフィールドへの LogRhythm アラームフィールド値のドラッグアンドドロップによるマッピング
- LogRhythm のサンプルアラームに基づく SIR セキュリティインシデントのレイアウトのプレビュー
- 履歴アラームと、構成可能な間隔で進行中の将来のアラームの取り込み
- SIR インシデントクローズ時の LogRhythm の自動アラームクロージャー。簡単に参照できるように、SIR インシデントへの URL とインシデント ID が表示されます。

Now Platform のサポートされているリリース

この統合は、Now Platform® の Quebec 以降のリリースと互換性があります。

LogRhythm のサポートされているバージョン

この統合は、LogRhythm 7.8 以降と互換性があります。以前のバージョンは、API の制限によりサポートされていません。

注:
次のトピックには番号が付けられています。スムーズにインストールし、想定通りの結果が得られるように、記載されている順序でトピックに従ってください。

LogRhythm の **REST API** の設定

LogRhythm REST API キーを使用して、個々のアラームフィールドの追加イベントの詳細を収集します。API キーを使用することで、LogRhythm REST API では利用できない詳細を確認できます。

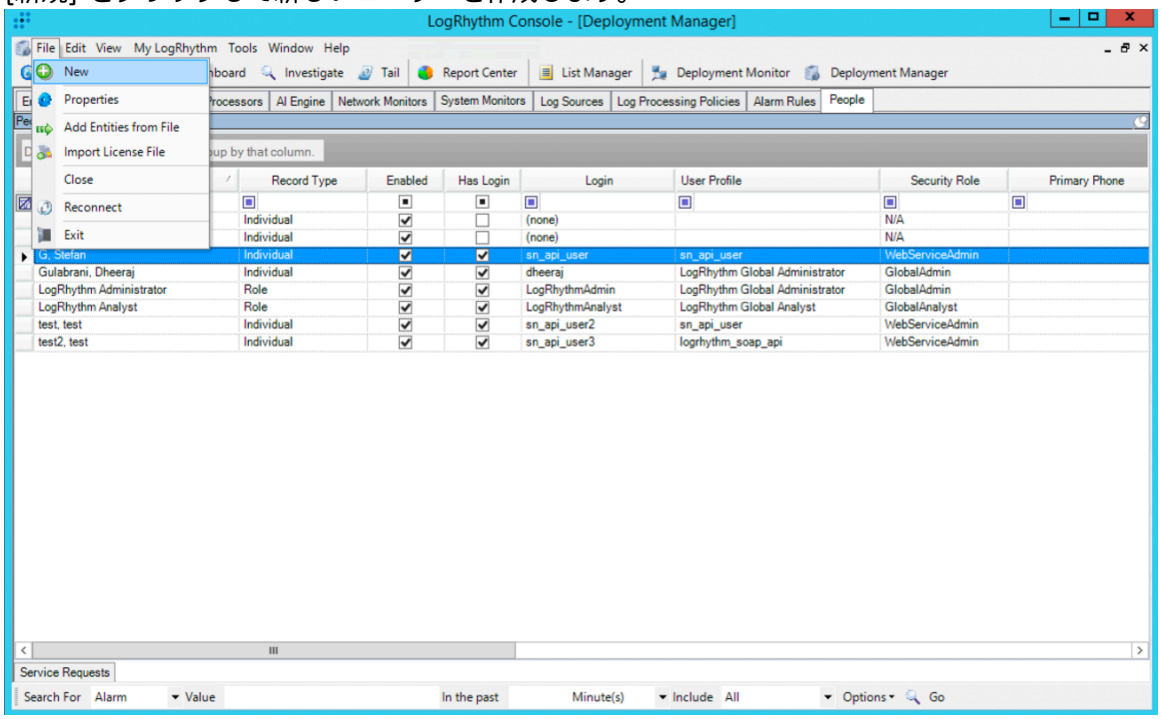
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：LogRhythm クライアントコンソール/プラットフォームマネージャーアドミニストレーター

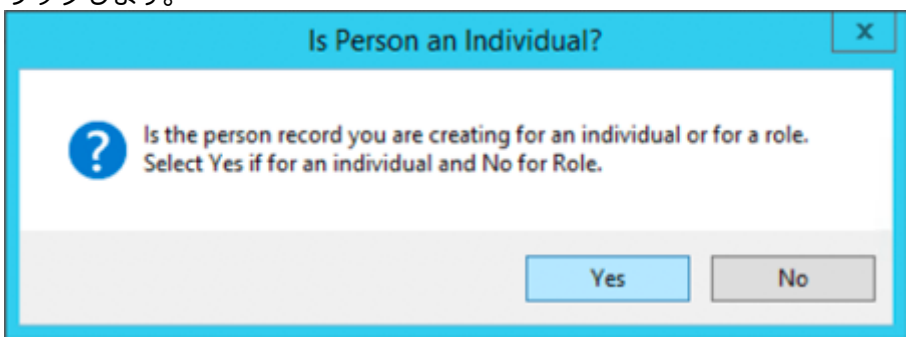
このタスクについて
このタスクは LogRhythm クライアントコンソールで実行します。ServiceNow Store からプラグインをインストールする前に LogRhythm REST API を設定します。

手順

1. LogRhythm クライアントコンソールに移動し、[ファイル] メニューを選択します。
2. [新規] をクリックして新しいユーザーを作成します。



3. [ユーザーは個人ですか？ **(Is Person an Individual?)]** ダイアログが表示されたら、[はい] をクリックします。

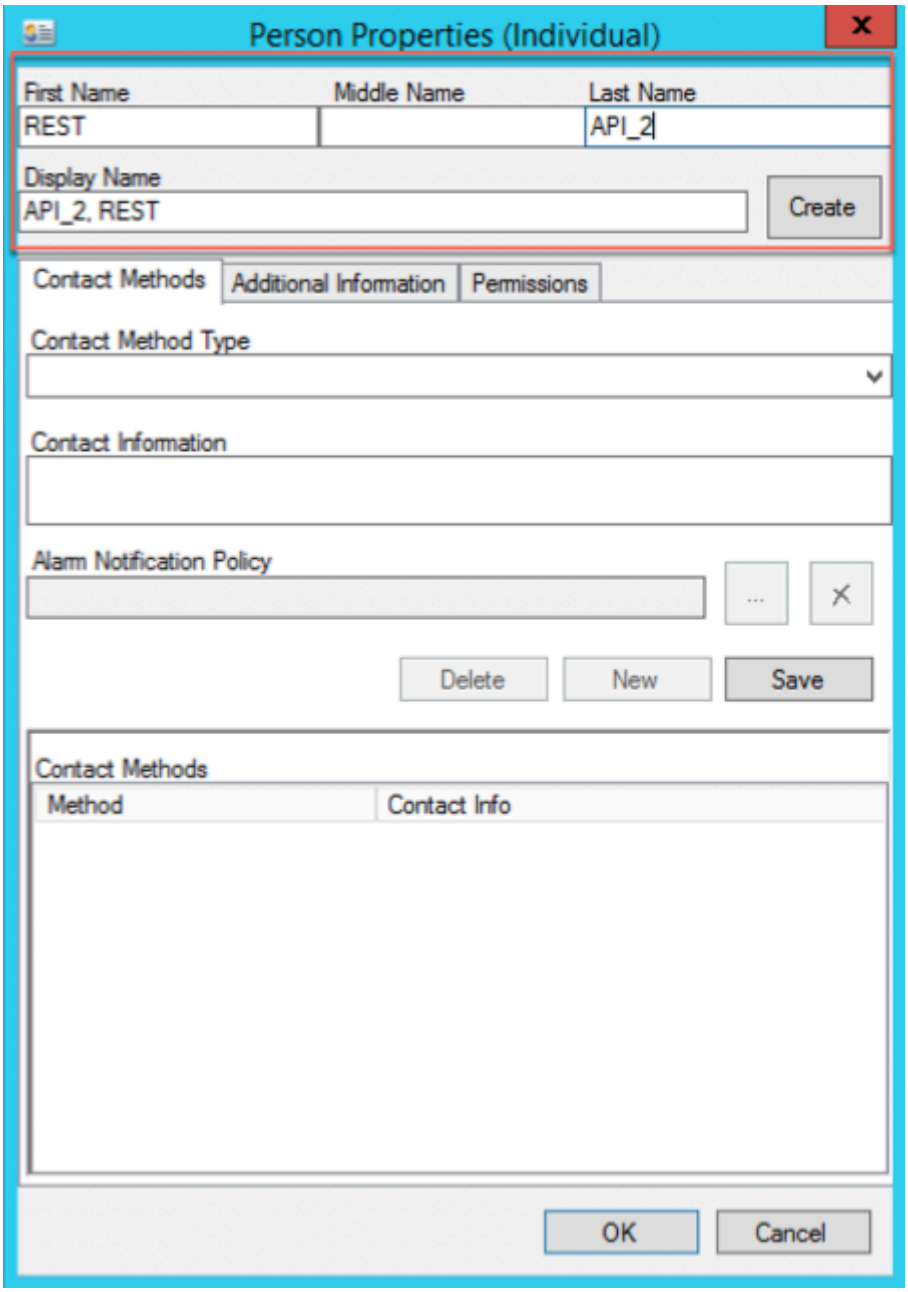


4. 表示される [個人のプロパティ (Person Properties)] ダイアログで、[名前] フィールドに入力します。

   REST API の作成に使用したものとは異なる名前 (「REST API_2」など) を LogRhythm REST API に使用します。

自動翻訳

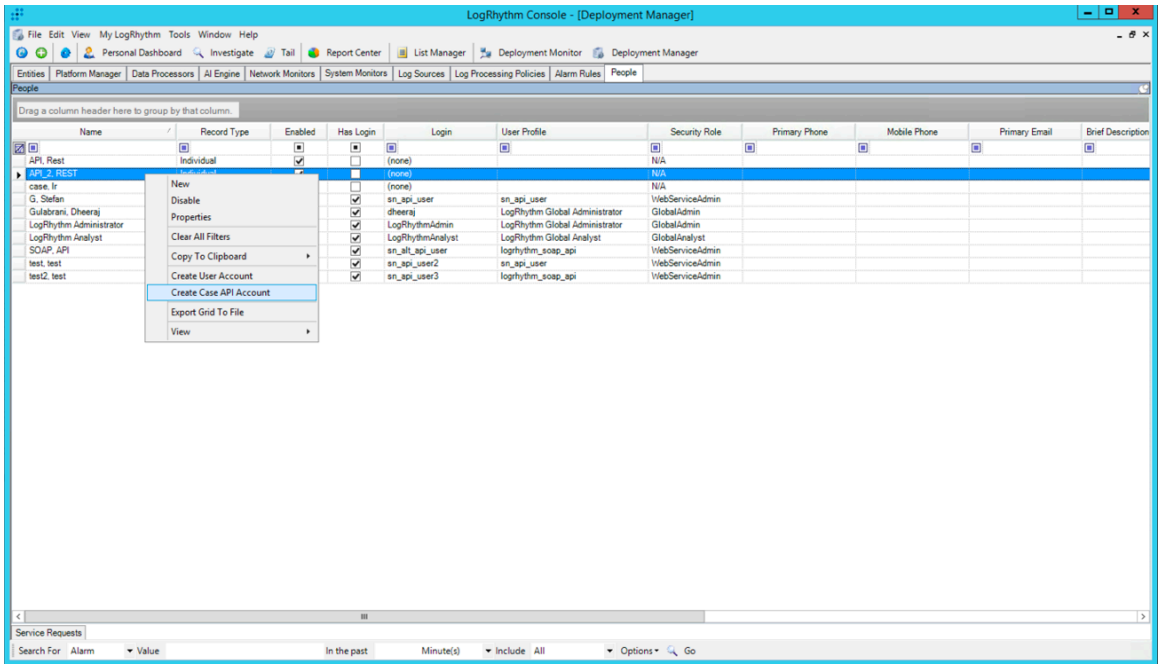
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. **[OK]** をクリックします。
6. [名前] 列の新しいリスト (**API_2_REST**) を右クリックし、選択リストで [ケース **API** アカウントを作成 **(Create Case API Account)]** を選択します。

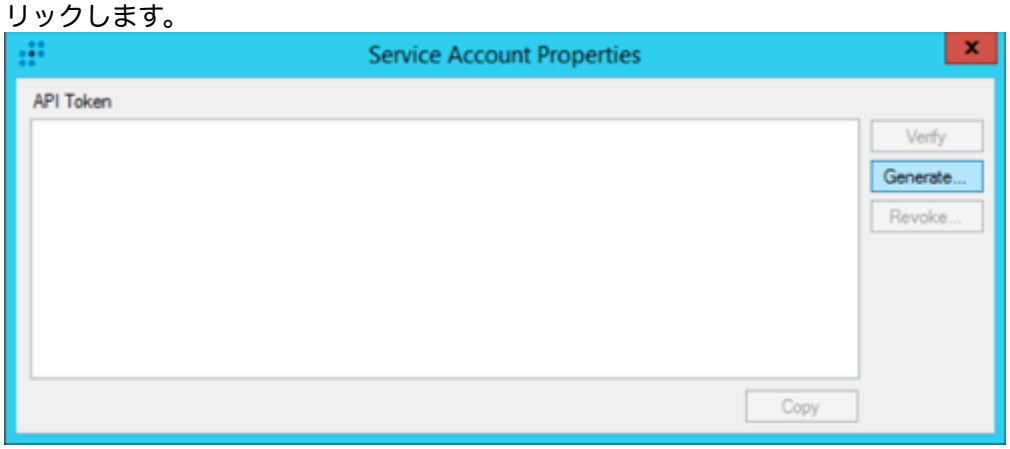
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

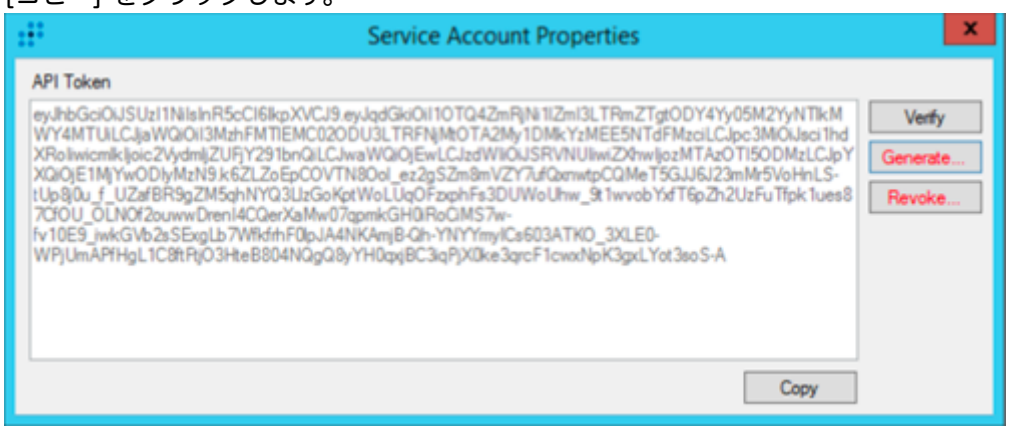


注:
ケース API は使用されませんが、ケース API アカウントと LogRhythm REST API の認証情報は同じです。

7. [サービスアカウントのプロパティ (Service Account Properties)] ダイアログで、[生成] をクリックします。



8. [コピー] をクリックします。



これで LogRhythm REST API が設定されました。「プラグインのインストールおよび LogRhythm の構成」に記載されている設定手順で、前の手順でコピーした文字列を LogRhythm REST API トークンのフィールドの Now Platform インスタンスに貼り付けます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のタスク
これで、「プラグインのインストールおよび LogRhythm の構成」に進む準備が整いました。

プラグインのインストールおよび **LogRhythm** の構成

インスタンスで統合を実行する前に、インストールと構成の手順を完了して、アプリケーションが Now Platform® の セキュリティオペレーション と適切に統合されるようにします。

始める前に
必要なロール：admin

インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。最新の LogRhythm バージョンは 7.8 以降です。

注:
既存のアラームプロファイルは最新の LogRhythm バージョンではサポートされなくなるため、新しいアラームプロファイルを作成して必要な構成を実行する必要があります。

セットアップタスク	説明

必要な Now Platform® およびセキュリティインシデントレスポンス (SIR) のロールがアサインされていることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。
	• システムアドミニストレーター (admin) は、アプリケーションプラグインをインストールし、セキュリティインシデントアドミン (sn_si.admin) ロールをアサインします。
	• (sn_si.admin) は、次のタスクを監督します。
	  ○ アラームプロファイルに名前を付け、作成し、編集します。
	  ○ アラームのマッピングとフィルタリング：セキュリティインシデントを作成する特定の LogRhythm アラームを識別し、これらのアラームフィールドを Now Platform セキュリティインシデントにマッピングする方法を設定します。
	  ○ 構成を確定する前に、正確性を確認するためにセキュリティインシデントの詳細をプレビューします。
	  ○ 履歴アラームを取り込み、プルされたアラームをスケジュールします。
	  ○ セキュリティインシデントアナリスト (sn_si.analyst) ロールをアサインします。
	  ○ このロールは セキュリティオペレーション モジュールにもアクセスできます。
	• セキュリティインシデントアナリスト (sn_si.analyst) は、アラームプロファイル設定に基づいて作成されたセキュリティインシデントに対応します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
LogRhythm API のユーザー名とパスワードを取得し、バージョン LogRhythm 7.8 以降を使用していることを確認します。	API キーの詳細やアカウントの作成方法については、LogRhythm Enterprise の Web サイト を参照してください。アプリケーションをインストールする前に、ユーザーアカウント、認証情報、および証明書を適切に設定する必要があります。 統合には、LogRhythm バージョン 7.8 以降と LogRhythm REST API が必要です。 「LogRhythm の REST API の設定」を参照してください。
MID サーバーがインストールおよび設定されていることを確認します。	Now Platform 環境には MID サーバーが必要です。MID サーバーの設定方法および構成方法については、ServiceNow 製品ドキュメント Web サイト を参照してください。
統合用のアプリケーションをインストールする前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	Rome リリース以降のファミリリリースでは、セキュリティインシデントレスポンス Dependency プラグイン (com.snc.si_dep) が必要です。このプラグインは、セキュリティインシデントレスポンス 製品をサポートするために必要なすべての依存関係を自動的にインストールします。統合に必要な他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。 次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。 **1.** セキュリティインシデントレスポンス **2.** Security Integration Framework **3.** Security Support Common **4.** セキュリティサポートオーケストレーション 統合のための Now Platform インスタンスのセットアップの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

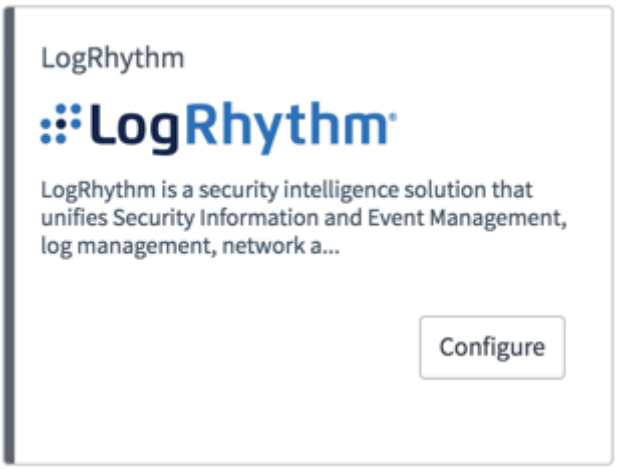
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

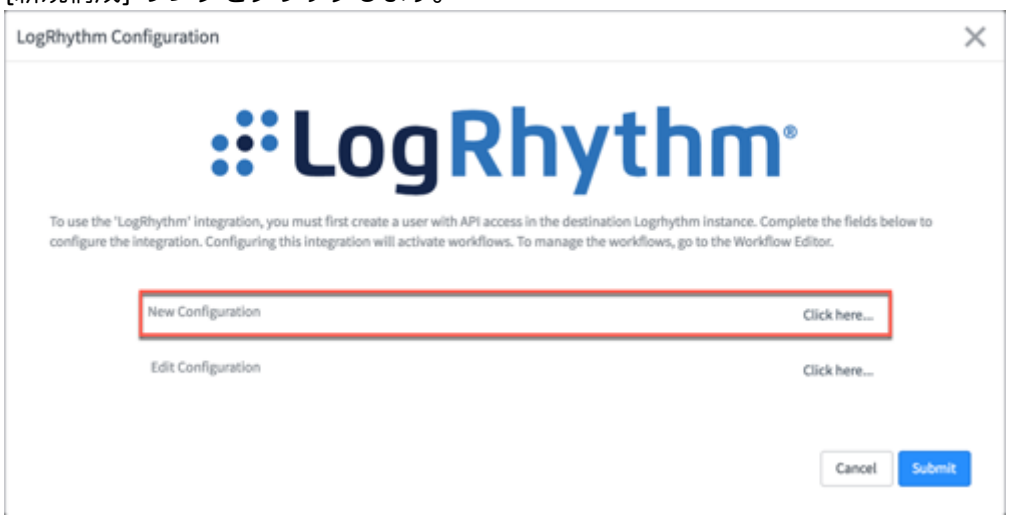
重要:
LogRhythm クライアントコンソールへの接続に問題がある場合は、「LogRhythm の接続性の確認」を参照してください。

手順

1. 統合用のアプリケーションをインストールしていない場合は、「セキュリティオペレーション 統合のインストール」を参照し、手順に従ってインストールしてください。
2. インストールが完了したら、次に移動します: 統合 > 統合構成 をクリックし、 LogRhythm タイルを見つけます。
3. [構成] をクリックします。



4. [新規構成] リンクをクリックします。



5. フォームのフィールドに入力します。

LogRhythm 構成

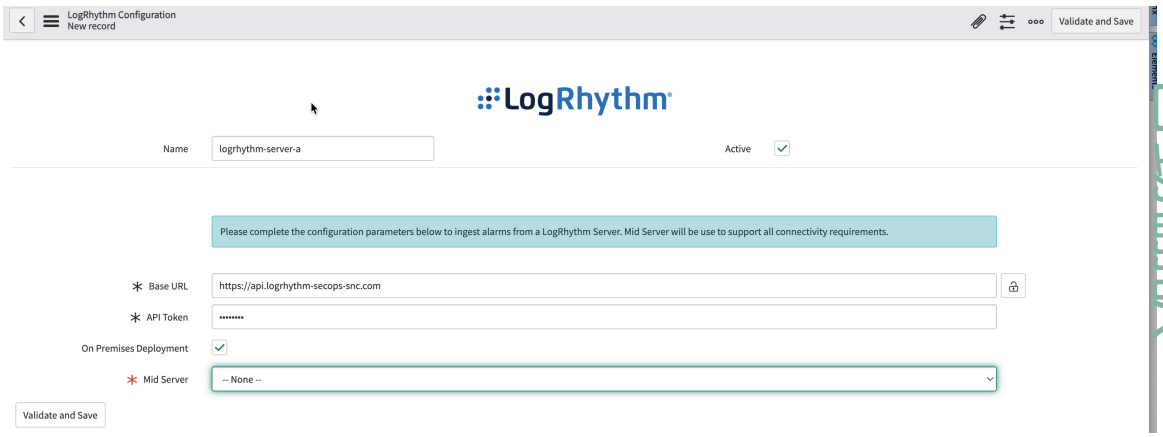
フィールド	説明
名前	LogRhythm サーバー名 (例：logrhythm-server-a)
ベース URL	LogRhythm REST API をホストするベース URL。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	MID サーバーは、LogRhythm クライアントコンソールがホストされているネットワークへのアクセスを許可します。この URL は、そのネットワーク内で LogRhythm サーバーがホストされている場所です。右端のロックアイコンをクリックしてフィールドを編集し、URL のテキストを入力します (例：https://logrhythm.secops-eng.com:8501/)。
API トークン	LogRhythm クライアントコンソールで作成した REST API に関連付けられているトークンを入力します。
オンプレミス展開	LogRhythm オンプレミス展開の場合に選択するオプション。
MID サーバー	環境に設定されている MID サーバーを指定します。この選択リストからはアクティブで検証済みの MID サーバーのみを使用できます。

次の図は、完成したフォームの例です。



6. [検証して保存] をクリックします。
   検証が正常に完了すると、メッセージが表示され、[LogRhythm 構成] ページが再ロードされます。次のステップでは、アラームプロファイルを作成します。

次のタスク

検証が正常に完了したら、次のステップは「LogRhythm のアラームプロファイルの作成」です。

LogRhythm のアラームプロファイルの作成

作成して名前を付けたアラームプロファイルで、LogRhythm クライアントコンソールからプルするアラームを指定します。また、それらを Now Platform セキュリティインシデントのフィールドにどのようにマッピングするかも定義します。

始める前に

必要なロール：sn_si.admin

このタスクについて

設定されたアラームプロファイルに基づいて、1 つのアラームプロファイルですべてのタイプのアラームをそのまま取り込むことができますが、フィルター基準を使用して特定のタイプのアラームを取り込むこともできます。この Now Platform 統合を使用すると、設定されたすべてのアラーム

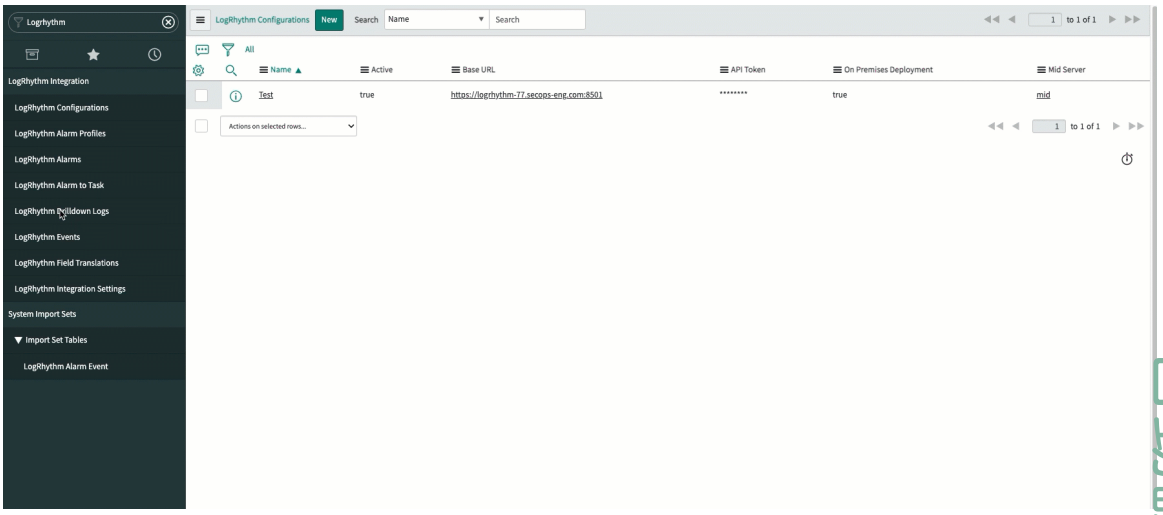
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ルールまたは作成されたプロファイルに基づく特定のルールが取り込まれます。続いて、リスクレベルが高いアラームのみなどのアラームルールをフィルタリングして、セキュリティインシデントを作成するアラームを指定できます。セキュリティインシデントが作成される前に、フィルタリングされたアラームの個々のフィールド値が Now Platform セキュリティインシデントの対応するフィールドにマッピングされます。この設定は、Now Platform インスタンス内のアラームプロファイルを介して行われます。

手順

1. 次のように移動する。 **All** (すべて) > **LogRhythm** 統合.
2. **[LogRhythm** アラームプロファイル] モジュールを選択して、[アラームプロファイル] リストを表示します。

アラームプロファイル



3. 新しいアラームプロファイルを作成するには、[新規] をクリックします。
新しいアラームプロファイルのフォームが表示されます。進捗状況バーのページ上部の [名前] が選択されます。このバーは、構成中の進捗状況を追跡します。
4. フォームの各フィールドに入力します。

アラームプロファイル

フィールド	説明
名前	アラームプロファイルの名前。この名前は、「無許可のアクセス」 (*VPN*)、「マルウェア」、「フィッシング」 などのアラームタイプを識別するのに役立ちます。
簡単な説明	アラームのタイプやアラームカテゴリなどのアラームプロファイルに関する補足情報の短いテキスト。説明の例：All alarms associated with unauthorized Powershell and Sudo access attempts. (無許可の PowerShell および sudo アクセス試行に関連するすべてのアラーム。)
ソース	選択リストのソースサーバー。このリストは既に設定した LogRhythm 構成から成ります (例：logrhythm-server-a)。「プラグインのイ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	ンストールおよび LogRhythm の構成」を参照してください。
順序	アラームプロファイルの優先度。このフィールドは、2 つ以上のアラームプロファイルがトリガー条件を共有する場合にアラームプロファイルが実行される順序を示します。
アクティブ	デフォルトでは、このオプションは選択されていません。すべてのアラームプロファイルのセットアップ手順を完了して [完了] をクリックすると、このチェックボックスをオンにしてアラームプロファイルをアクティブにするように求められます。アラームプロファイルがアクティブな場合、LogRhythm クライアントコンソールから自動的にアラームがプルされます。

5. [続行] をクリックしてデータを保存し、[マッピング] フォームに進みます。

   検証が正常に行われると、ページが再ロードされ、[マッピング] フォームが表示されます。接続と資格情報を正常に検証するまで、設定を続行できません。

関連情報

セキュリティインシデントへの LogRhythm アラームのマッピング

セキュリティインシデントへの **LogRhythm** アラームのマッピング

取り込む LogRhythm ソースを選択したら、個々の LogRhythm アラームフィールドを Now Platform セキュリティインシデントのフィールドにマッピングする必要があります。

アラームのマッピングには、次のタスクが含まれます。

- LogRhythm アラームをマッピングします。このタスクでは、アラーム ID または LogRhythm クライアントコンソールから最新のアラームを使用して、サンプルアラームをリストして取り込みます (プルします) 。
- [サンプルアラーム] フィールドは、次の 3 つのグループに分類されます。
  - [アラーム] フィールド：利用可能なアラームフィールドとそれに対応する値が表示されます。
  - [イベント] フィールド：利用可能なイベントフィールドとそれに対応する値が表示されます。
  - [ドリルダウンログ] フィールド：利用可能なドリルダウンログフィールドとそれに対応する値が表示されます。
- プルした各アラーム ID はタブとして表示されます。[アラーム ID] タブで、フォームの左側にある [アラームサンプル取り込み] セクションのすべての重大なアラームのフィールドが、フォームの右側の [SIR インシデントフィールドマッピング] セクションにマッピングされていることを確認します。
- アラームを [SIR インシデントフィールドマッピング] フィールドにマッピングすると、アラームカテゴリが [入力式] フィールドにも表示されます。例：${Alarm: alarmid}$
- セキュリティインシデントのフィールドを追加または削除することで、設定を変更できます。提供されている色分けを使用して、見落とされているフィールドや重複フィールドを追跡します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- アラームをフィルタリングして、SIR アプリケーションに取り込むアラームを指定することができます。アラームを直接フィルタリングするか、アラームカテゴリを使用して、[アラーム]、[イベント]、または [ドリルダウンログ] に基づいて検索を絞り込むことができます。
- セキュリティインシデントの [優先度] フィールドと [カテゴリ] フィールドの値をフォーマットする場合は、スクリプトエディターを使用します。

次のステップは「LogRhythm アラームフィールドのセキュリティインシデントフィールドへのマッピング」です。

関連情報

LogRhythm アラームフィールドのセキュリティインシデントフィールドへのマッピング

スクリプトエディターを使用した LogRhythm 値のフォーマット

LogRhythm のアラームのフィルタリング

LogRhythm アラームフィールドのセキュリティインシデントフィールドへのマッピング

個々のアラームフィールドをセキュリティインシデントフィールドにマッピングします。事前設定されたマッピングは編集できます。フィールドに用意されている色分けは、既にマッピングされているアラームを監視するのに役立ちます。このステップは、編集がセキュリティインシデントのフィールドにどのように影響するかを視覚化するのに役立ちます。

始める前に

必要なロール：sn_si.admin
LogRhythm アラームを使い慣れていない場合は、LogRhythm クライアントコンソールに移動して、サンプルアラーム ID を確認してください。次の例では、LogRhythm アラーム「9468」と「9474」を使用して、アラームをセキュリティインシデントにマッピングしています。

このタスクについて

このフォームを使用して、左側の LogRhythm アラームルールを右側のセキュリティインシデントフィールドにマッピングします。

次の図は、各アラームプロファイルに事前設定されたアラームのデフォルトマッピングを示しています。このデフォルトマッピングは編集できます。このフォームを使用して、セキュリティインシデントを設定するフィールドをカスタマイズします。このマッピングを完了すると、アラームフィールドを追加または削除することでセキュリティインシデントのフィールド値にどのように影響するかを確認できます。

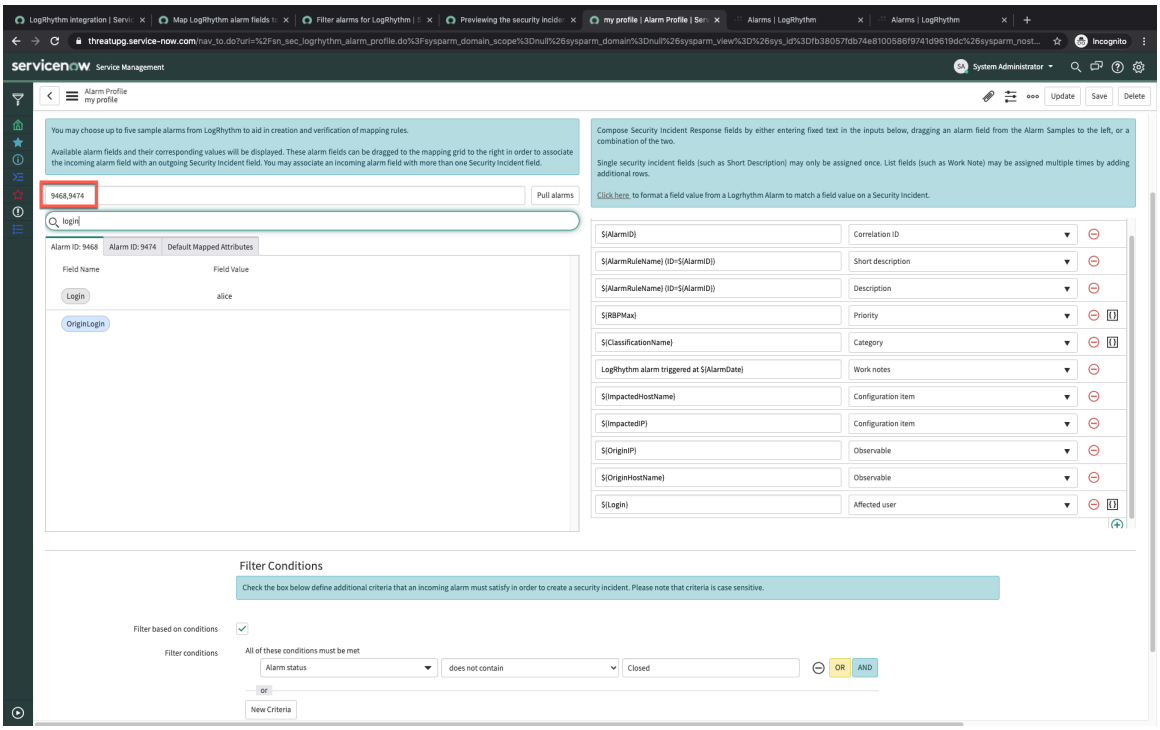
次の図のこのフォームの左側に LogRhythm アラームルールの概要が示されています。これらのアラームルールの値は、フォームの右側のセキュリティインシデントフィールドにマッピングされます。

手順

1. LogRhythm のアラームプロファイルを作成した後、進捗状況バーの [マッピング] をクリックします。
2. [アラームサンプル取り込み] フィールドに、最大 5 つのサンプル LogRhythm アラーム ID をカンマで区切って入力します (9468,9474)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. アラームフィールドの横にある [プルアラーム] をクリックします。

   サンプルアラームのプルには少し時間がかかる場合があります。トランザクションが機能していることを示すメッセージが画面の上部に表示されます。

   サンプルアラーム ID が送信され、LogRhythm サーバーから正常にプルされると、アラームフィールドとそれに対応する値がタブに表示されます。

   注:
   アラーム ID が正常にプルされた後、Now Platform は次のメッセージを返す場合があります。「The following new fields will be available for filtering shortly. Please reload this profile in a few minutes if filtering based on these fields is required. itemspacketsin, itemspacketsout」([itemspacketsin]、[itemspacketsout] の新しいフィールドが間もなくフィルタリングに使用できるようになります。これらのフィールドに基づいてフィルタリングする必要がある場合は、数分後にこのプロファイルを再ロードしてください)

   このメッセージは、プルされた単一のアラームに、Now Platform によって以前に処理されたことがないフィールド名が含まれている場合に生成されます。これらのフィールドはマッピングに使用できますが、このメッセージが表示された場合は、フォームを再ロードして、フィルタリング条件を設定する準備ができたときにこれらのフィールドを表示し、条件ビルダーのフィルター選択リストで使用できるようにします。

   これらのサンプルアラームをアラームプロファイル構成に取り込むと、値が含まれていないセキュリティインシデントにアラームフィールドがマッピングされるのを防ぐことができます。また、アラームフィールドをセキュリティインシデントの該当するフィールドに合わせて調整します。この手順により、重要なアラームフィールドがすべてマッピングされ、セキュリティインシデントに欠落しているフィールド値がないことが確認されます。

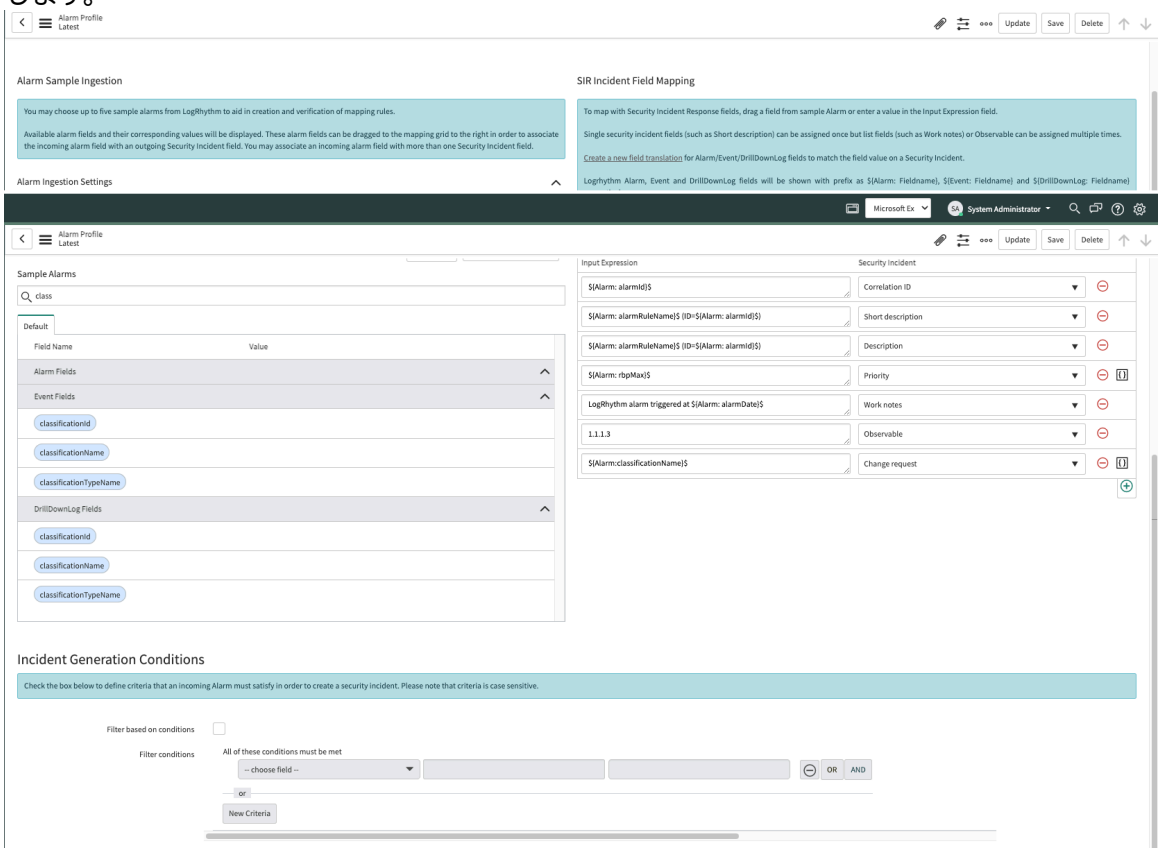
   マッピングプロセスでアラームが見落とされたり重複したりしないように、アラームフィールドは色分けされています。水色のアラームフィールド (「Account」、「AlarmRuleID」、「AlarmStatus」など) は、セキュリティインシデントへのマッピング用にフィールドがまだ選択されていないことを示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

灰色のフィールド (「AlarmDate」、「AlarmID」、および「AlarmRuleName」) は、フィールドが既に選択され、セキュリティインシデントのフィールドにマッピングされていることを示しています。場合によっては、アラームフィールドがセキュリティインシデントの複数のフィールドにマッピングされる可能性があるため、この色分けはマッピングの追跡に役立ちます。たとえば、「Observables」および「Work Note」のフィールドには複数の値を含めることができます。

4. サンプルアラームデータをクリアするには、[サンプルアラームデータのクリア] をクリックします。
5. セキュリティインシデントのデフォルト構成を編集するには、次の手順に従ってフィールドを追加します。



a. フォームの右下にあるプラスアイコンをクリックします。
新しいフィールドが表示されます。

b. [セキュリティインシデント] 列で、選択リストから利用可能なフィールドを選択します。

展開された選択リストでは、一部のフィールドが網掛けされています。たとえば、「Category」の背景は灰色で、セキュリティインシデントにマッピングされていることを示しています。LogRhythm アラームフィールドの色分けと同様に、セキュリティインシデントフィールドのこの色分けにより、アラームフィールドの値が誤って同じセキュリティインシデントフィールドにマッピングされることがなくなります。

上の図では、アラームルール「${Alarm:classificationName}$」は、このプロファイルのセキュリティインシデントの「Category」のフィールドに既にマッピングされています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[観測事象] フィールドは、複数の観測事象を表示できるように、同じセキュリティインシデントの複数のフィールドにマッピングできます。同様に、「Configuration Item」のフィールドと「Work notes」のフィールドは、複数の値を表示するようにマッピングできます。

フォームの [アラームサンプル取り込み] 側で青色になっている場合は、アラームルールフィールドがマッピングされていないことを示します。灰色の場合は、マッピングされていることを示します。フォームの [SIR インシデントフィールドマッピング] 側の選択リストで白色になっている場合は、フィールドがマッピングされていないことを示します。灰色の場合は、フィールドがマッピングされていることを示します。この色分けを使用することで、フィールドマッピングを追跡できます。

上の図では、「Affected user」がセキュリティインシデントの新しいフィールドとして選択リストから選択されています。

c. フォームの左側にある [アラームサンプル取り込み] セクションで左クリックし、[入力式] フィールドに取り込むアラーム ID を選択します。

上の図では「Login」が選択されています。

d. クリアされたフィールドにドラッグして放します。
[SIR インシデントフィールドマッピング] セクションの左側の列に、「Affected User」のフィールドの新しい値が表示されます。この場合、LogRhythm アラームの「Login」値がセキュリティインシデントの「Affected user」のフィールドに表示されます。

6. または、[入力式] 列のフィールドに手動で値を入力するには、[入力式] フィールドにカーソルを置き、目的のアラーム値を入力します。

たとえば、上の図では、セキュリティインシデントフォームに別のフィールドが追加され (「Assignment group」)、「セキュリティインシデントアサイン」がフィールドに手動で入力されています。

7. 必要に応じて、事前設定されたマッピングの編集を続行します。
LogRhythm アラームフィールドの値をセキュリティインシデントのフィールドでサポートされている値に変換する必要がある場合は、スクリプトエディターを使用できます。「スクリプトエディターを使用した LogRhythm 値のフォーマット」を参照してください。

次のタスク
フィールドマッピングが完了したら、次のステップは「LogRhythm のアラームのフィルタリング」です。

LogRhythm のアラームのフィルタリング

フィールドをマッピングした後にアラームのフィルタリング基準を設定すると、SIR アプリケーションに取り込む必要があるアラームを決定するのに役立ちます。アラームをフィルタリングすると、アラームプロファイルがアクティブになったときに取り込むアラームの数を大幅に減らすことができます。

始める前に
必要なロール：sn_si.admin

このタスクについて
マッピングフォームの下部にあるフィルタリング条件を使用して、特定のアラームを除外したり、特定のフィールドレベルの基準を満たすアラームのみに取り込みを制限したりします。フィルタリングすると、アラームプロファイルがアクティブになったときに取り込むアラームの数を大幅に減らすこ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

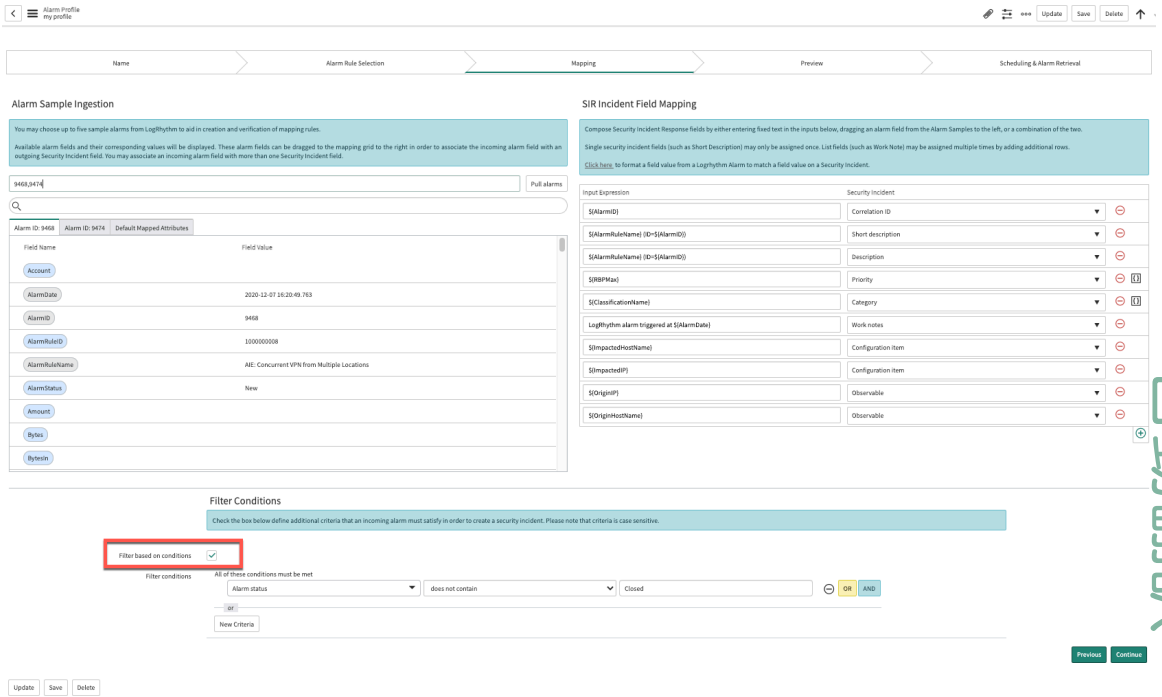
自動翻訳

とができます。フィルタリングを使用して、Security Operations Center (SOC) のスタッフが対応できる管理可能な量のアラームを取り込みます。

注:
次の例は、「Alarm status-does-not-contain-Closed」がデフォルト設定であるデフォルトのフィルター設定を示しています。このフィルターはアクティブなアラームのみをプルし、この設定により、プルされるアラームの数が減少します。次の手順は、重大度または優先度の値が最も高いアラームのみを含む、別の便利なフィルターを追加する方法を示しています。

手順

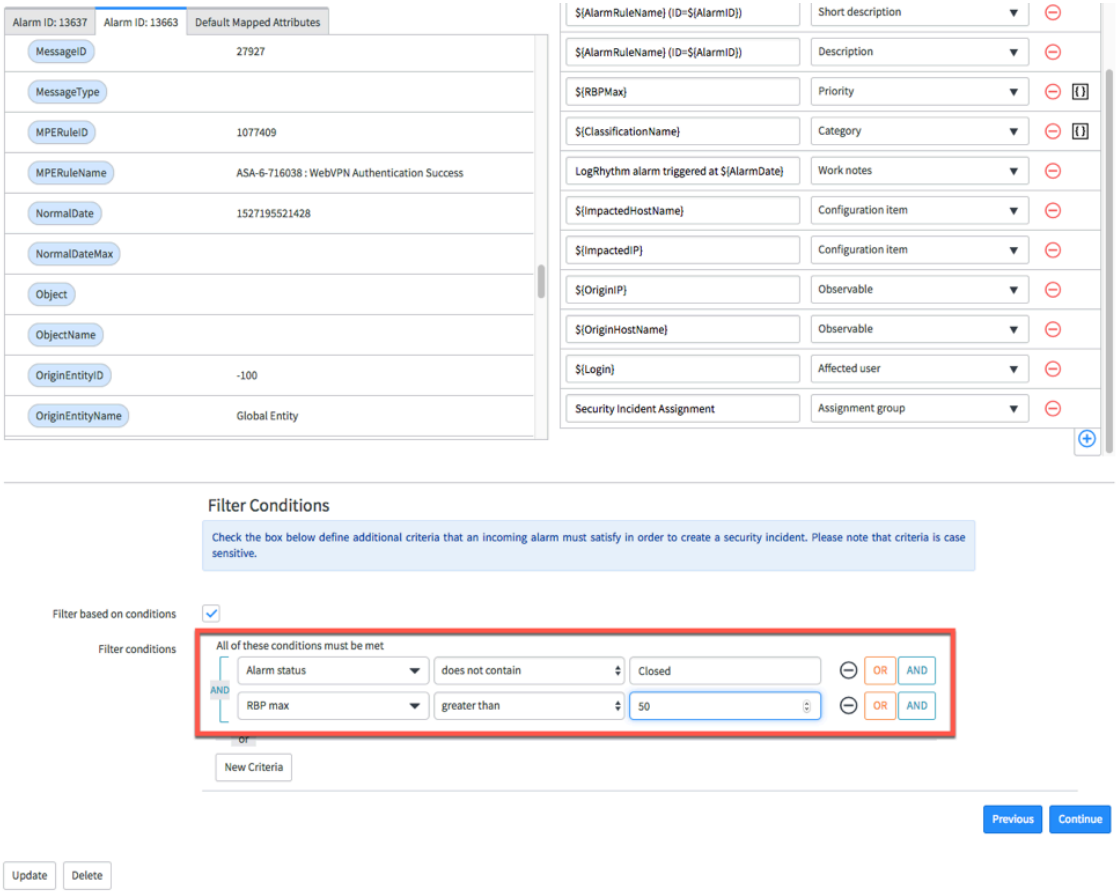
1. フィルタリング基準を編集するには、[条件に基づいてフィルター] チェックボックスをオンにします。



2. [フィルター条件] フィールドの右側の **[OR]** または **[AND]** をクリックします。
3. 表示される新しい行で、選択リストからフィルタリング条件を選択します。

   次の画像は、リスクベースの優先度 (RBP max) が 50 より大きい基準に追加されたフィルターを示しています。このフィルター設定では、リスクベースの優先度値が 50 より大きい LogRhythm アラームのみがプルされます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. すべての重大な LogRhythm アラームフィールドが Now Platform セキュリティインシデントにマッピングされ、アラームの取り込みを制限するフィルタリング基準を設定したことを確認したら、いずれかを選択して設定を続行します。

次のタスク

次のステップでは、セキュリティインシデントにマッピングしたフィールドをプレビューします。「マッピングされた LogRhythm アラーム値を使用したセキュリティインシデントのプレビュー」を参照してください。

マッピングされた **LogRhythm** アラーム値を使用したセキュリティインシデントのプレビュー

マッピングステップを完了したら、セキュリティインシデントのフィールドにマッピングした値をプレビューします。このプレビューステップでは、セキュリティインシデントに表示する重大な LogRhythm アラートフィールドがすべてマッピングされていることを確認できます。

必要なロール：sn_si.admin

セキュリティインシデント

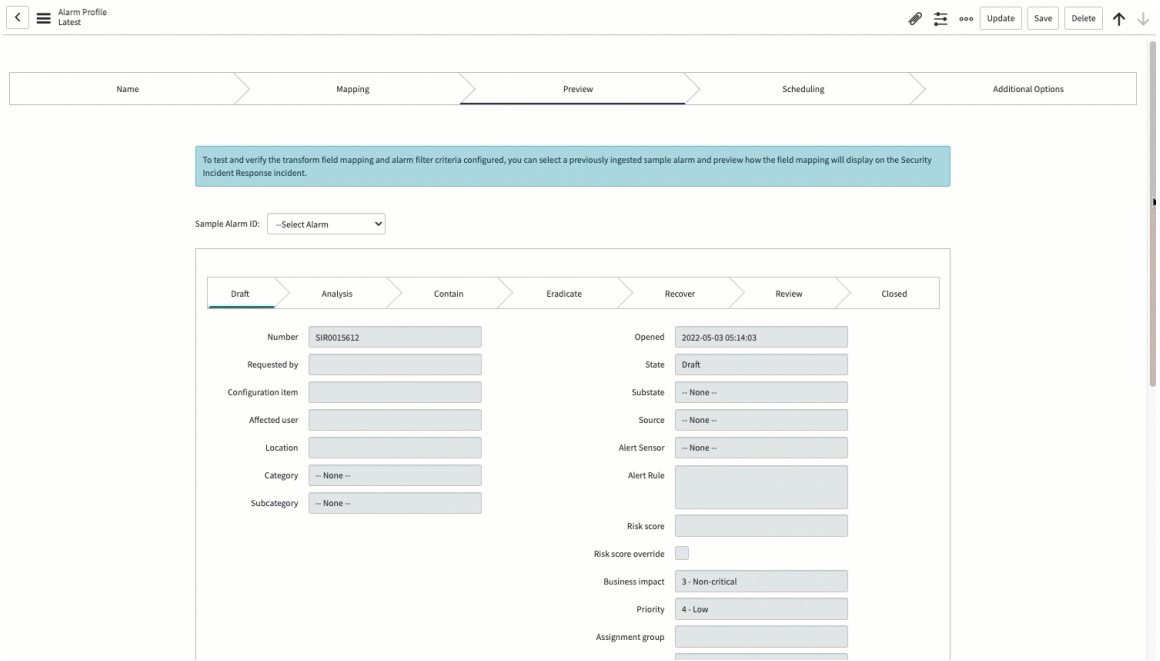
セキュリティインシデントのプレビューが表示されない場合は、進捗状況バーの [プレビュー] をクリックします。

Now Platform セキュリティインシデント全体のプレビューの例を次の 2 つの図に示します。このセキュリティインシデントのプレビューの例では、サンプルアラーム「13663」からマッピングされた LogRhythm アラームフィールドが入力されています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図では、セキュリティインシデントの「Configuration item」、「Affected user」、「Priority」、「Assignment Group」、および「Short description」のフィールドが入力されています。

セキュリティインシデントの上半分



セキュリティインシデントフォームの下半分に「Description」のフィールドが設定されます。[関連アイテム] セクションの「Configuration item」、「Observable」、および「Work note」のフィールドに値が入力されます。これらのフィールドの複数の値がマッピングされている場合、これらのフィールドは複数の値を受け入れることができるため、各値がセキュリティインシデントに表示されます。

プレビューのエラー条件

セキュリティインシデントをプレビューすると、次の警告メッセージが表示される場合があります。サンプルアラームがフィルタリング基準を満たしていない場合、セキュリティインシデントは一部設定されません。

入力値が非検出

アラーム ID がフィルタリング条件内に含まれている場合でも、マッピングされた特定のフィールドで特定の入力値が見つからないと、警告メッセージが表示されることがあります。次の例では、レコードのプレビューで、マッピングされているにもかかわらず「Assigned to」のフィールドに値がないと仮定します。

このタイプのメッセージの場合は、[マッピング] レコードで入力値が正しいことを確認します。この場合は、セキュリティインシデントの「Assigned to」のフィールドのユーザーが Now Platform インスタンスで正しくありません。このアラームが取り込まれ、この条件でセキュリティインシデントが作成されると、この入力値 (Abel Tuter) を持つフィールドはセキュリティインシデントで空白のままになります。

残りの青色のメッセージは情報であり、これらのフィールドにはプレビューに表示する値がないことを示しています。このプレビューにより、アラームプロファイルを設定するセキュリティインシデントアドミニストレーターは、初期作成段階ではこれらのフィールドに値がないことを確認できるようになります。これは、セキュリティインシデントフィールドが後で自動的に入力される場合があるためです。他のマッピングエラーも表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

マッピングとセキュリティインシデントのプレビューに問題がない場合は、いずれかを選択して構成を続行します。

オプション	説明
進捗状況バーで [続行] または [スケジューリング] をクリックします。	[スケジューリングおよびアラームの取得] フォームに進みます。 進捗状況バーで [スケジューリングおよびアラームの取得] が選択されていることを確認します。次のステップでは、アラームの取得をスケジュールします。
[前へ] をクリックします。	アラームプロファイルに戻り、マッピングを続行します。
プレビューフォームの上部にある [サンプルアラーム **ID]** 選択リストに別のアラーム ID を入力します。	入力したアラーム ID ごとに [サンプルアラーム **ID]** 選択リストが表示されます。最大 5 つのアラームを選択できます。 このオプションを使用すると、セキュリティインシデントに関する別の LogRhythm アラーム ID をプレビューできます。

セキュリティインシデントをプレビューし、結果に問題がない場合は、次のステップは「LogRhythm アラームのスケジュールおよび取得」です。

LogRhythm アラームのスケジュールおよび取得

選択してマッピングした LogRhythm アラームを使用してセキュリティインシデントをプレビューしたら、アラームの取得をスケジュールする準備は完了です。このステップを完了すると、アラームプロファイルをアクティブにする準備ができます。

始める前に

必要なロール：sn_si.admin

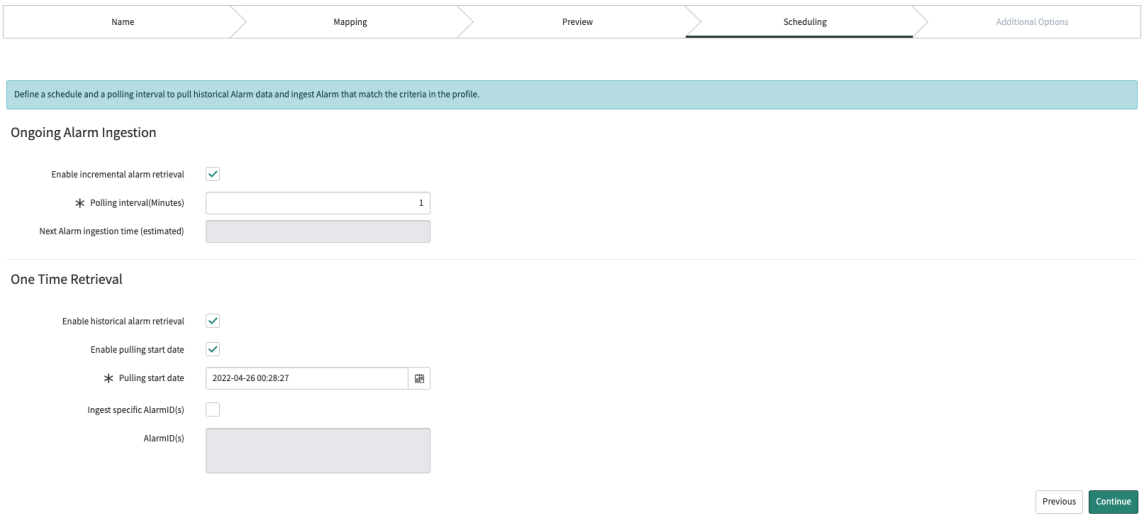
このタスクについて

スケジューリングでは、取得するのに選択したアラームのスケジュールとタイプを変更できます。取り込むアラームは、日付範囲または特定のアラーム ID に基づいてフィルタリングします。このステップでは、履歴アラームを取り込むかどうか、およびアラームプロファイル構成に一致する将来のアラームをポーリングする頻度を指定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 進捗状況バーの [スケジューリング] ステップをクリックします。

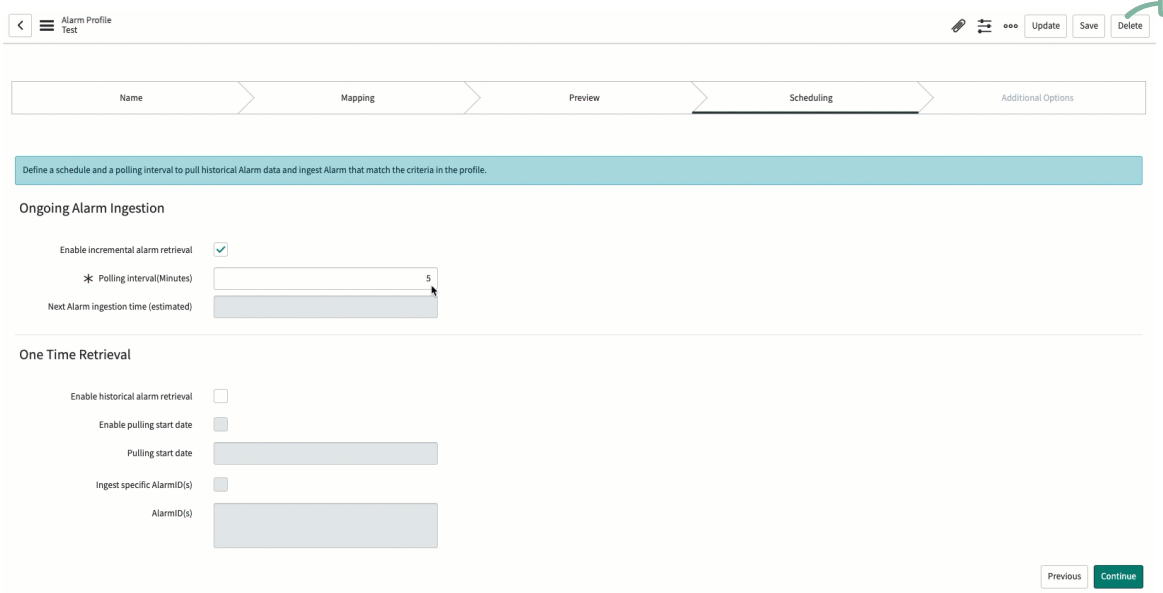


2. 次のオプションから選択して、アラームの取得を設定します。

3. 履歴アラームの取得を編集するには、次のステップに従ってアラームの取得日または特定のアラーム ID を入力します。

   a. [プル開始日を有効にする] をオンにし、[プル開始日] を選択します。

   b. [プル開始日] フィールドで、表示されるカレンダーをクリックし、日付を選択してから緑色のチェックマークを選択したら、エントリを保存します。



   日付が表示されます。

   c. または、[特定のアラーム **ID** を取り込む **(Ingest specific Alarm ID(s))]** オプションを選択し、**[AlarmID]** フィールドに履歴データの特定のアラーム ID を入力して特定のアラーム ID を取得します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

最大 5 つのアラームをカンマで区切って入力できます。

d. [更新] をクリックします。

4. 次のいずれかのオプションを選択して編集を続行するか、設定を完了します。

次のタスク

[継続的なアラームの取り込み] と [1 回限りの取得] の詳細を設定したら、次のステップは「LogRhythm アラームの他のオプション」です。

LogRhythm アラームの他のオプション

LogRhythm Enterprise 統合では、セキュリティインシデントに基づいて LogRhythm アラームを自動的に更新またはクローズする機能が使用できます。

始める前に

必要なロール：sn_si.analyst

このタスクについて

[アラームの初期更新] オプションを有効にすると、LogRhythm コメント内のアラームがアラームの初期更新によって自動的に更新されます。同様に、[アラームクロージャーの更新] オプションを有効にすると、アラームは SIR クローズコードとクローズコメントとともに LogRhythm で自動的にクローズされます。

LogRhythm アラーム ID は、インシデントのライフサイクル全体を通して Now Platform セキュリティインシデント ID に関連付けられます。この相関関係により、セキュリティインシデント/アラームクロージャーの同時の自動発生が許可されます。セキュリティインシデントレスポンス (SIR) セキュリティインシデントレコードがクローズされると、LogRhythm Web コンソールのアラームにコメントが投稿されます。このコメントは、Now Platform セキュリティインシデントのクローズに基づいてアラームがクローズされたことを示しています。インシデント番号と、参照のためにセキュリティインシデントにリンクする URL も、LogRhythm アラームのコメントセクションに含まれています。

手順

1. 進捗状況バーの [他のオプション] ステップをクリックします。

2. SIR インシデントの作成に自動アラーム更新を使用するには、次のオプションから選択してアラームの取得を設定します。

3. SIR インシデントのクローズに自動アラーム更新を使用するには、次のオプションから選択してアラームの取得を設定します。

4. [完了] をクリックしてアラームプロファイルを保存します。

Trouble?

セキュリティインシデントにアラームが正常にクローズされたことを示すメモが表示されない場合は、問題の解決方法の詳細について作業メモを確認してください。また、サーバー接続を確認してください。Now Platform セキュリティインシデントがクローズされていること、サーバーがタイムアウトしていないことを確認したら、LogRhythm Web コンソールでアラームを手動でクローズする必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

LogRhythm 統合の追加の構成

LogRhythm 統合の設定を使用して、事前設定されたシステムとトラブルシューティングのプロパティを要件に応じて変更します。

始める前に
必要なロール：sn_si.admin

手順

1. 次のように移動する。 **All** (すべて) > **LogRhythm** 統合 > **LogRhythm** 統合設定.
2. 要件に応じてシステムのプロパティを構成します。
3. フォームの各フィールドに入力します。

LogRhythm 統合のシステムのプロパティ

フィールド	説明
これにより、データが ServiceNow テーブルに保存される前にフィルターが適用されます。	データが ServiceNow テーブルに保存される前にフィルターを適用するかどうかを指定するオプション。 デフォルト値は [はい] に設定されています。
1 日に作成できるセキュリティインシデントの最大数	1 日に作成できるセキュリティインシデントの最大数を定義するオプション。 デフォルト値は [2000] に設定されています。
LogRhythm の定期的な取り込みは 1000 以上のアラームになる可能性があるため、ページネーションを使用してアラームを取り込みます。ページごとの制限により、ページあたりのアラーム数をフェッチできます。	1 つのページで取得するアラームの最大数を定義するオプション。 デフォルト値は 100 に設定されています。
指定された日数よりも古い「ソースからタスク」テーブルレコードを削除します。	指定された日数に違反したときに [ソースからタスク] テーブルレコードを削除するオプション。 デフォルト値は 30 に設定されています。

4. 要件に応じてトラブルシューティングプロパティを構成します。
5. フォームの各フィールドに入力します。

Logrhythm 統合のトラブルシューティングプロパティ

フィールド	説明
スケジュールされた取り込みをデバッグ：スケジュール済みジョブによって行われる取り込みのデバッグレベルのシステムログが有効になります。これにより、LogRhythm からアラーム/ドリルダウンログ/イベントをプルする際に、スケジュールされた取り込みによって生成されたすべてのメッセージ/例外がログに記録されます。	スケジュール済みジョブによって行われる取り込みのデバッグレベルのシステムログを有効にするオプション。 デフォルト値は [いいえ] に設定されています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
変換マップをデバッグ：変換マップのデバッグレベルのシステムログが有効になります。これにより、アラームインポートからセキュリティインシデントを作成するときに変換マップによって生成されたすべてのメッセージがログに記録されます。また、変換マップを再実行する、アラームインポートテーブルでの UI アクションも有効になります。	変換マップのデバッグレベルのシステムログを有効にするオプション。 デフォルト値は [いいえ] に設定されています。
アラームプロファイルでのサンプル取り込みのデバッグ：サンプル取り込みのデバッグレベルのシステムログが有効になります。これにより、サンプルの取り込み中に生成されたすべてのメッセージがログに記録されます。	サンプル取り込みのデバッグレベルのシステムログを有効にするオプション。 デフォルト値は [いいえ] に設定されています。
アラームプロファイルのデバッグプレビュー：これにより、アラームプロファイルのプレビューのデバッグレベルのシステムログが有効になります。サンプルアラームのプレビューのレンダリング中に生成されたすべてのメッセージがログに記録されます。	アラームプロファイルのプレビューのデバッグレベルのシステムログを有効にするオプション。 デフォルト値は [いいえ] に設定されています。
送信 REST 呼び出しをデバッグ：このプロパティを有効にすると、LogRhythm からの MID サーバーの有無にかかわらず、すべての REST 呼び出し (要求と応答) の実行について、システムログテーブルへのデバッグレベルのログ記録が可能になります。	LogRhythm からの MID サーバーの有無にかかわらず、すべての REST 呼び出しの実行についてシステムログテーブルのデバッグレベルのログ記録を有効にするオプション。 デフォルト値は [いいえ] に設定されています。

6. [保存] をクリックします。

スクリプトエディターを使用した **LogRhythm** 値のフォーマット

プルされたアラーム値および手動で入力したアラーム値から直接マッピングされたフィールドに加えて、オプションのマッピングステップでスクリプトエディターを使用してセキュリティインシデントのフィールド値をフォーマットできます。

始める前に

必要なロール：sn_si.admin

スクリプトエディターは、LogRhythm アラームの値を変更して、セキュリティインシデントの「Priority」および「Category」のフィールドにマッピングされる値がサポートされるようにします。

このタスクについて

LogRhythm アラーム値がセキュリティインシデントの「Priority」および「Category」のフィールドにマッピングされている場合は、マッピングされた値を編集することができます。LogRhythm アラームの値をセキュリティインシデントの「Priority」および「Category」のフィールドでサポートされている値に変換する場合は、スクリプトエディターを使用します。

自動翻訳

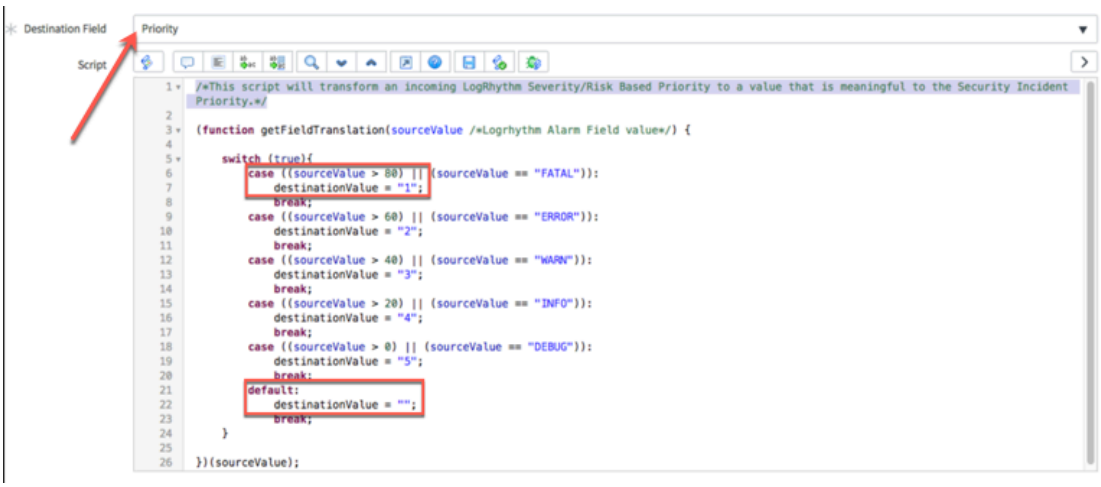
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. マッピングフォームを表示した状態で、[SIR インシデントフィールドマッピング] セクションで角括弧アイコン [{}] をクリックしてスクリプトエディターを開きます。

デフォルト値は、セキュリティインシデントの「Priority」および「Category」のフィールドに含まれています。これらの値は編集できます。

この例では、次の図に示すように、開いているエディターで [宛先フィールド] 選択リストに [優先度] が表示されていることを確認します。このフィールドは LogRhythm リスクベースの優先度ではなくセキュリティインシデントの優先度であることに注意してください。



場合によっては、[優先度] フィールドにスクリプトインクルードが適していることがあります。たとえば、LogRhythm アラームの場合、リスクベースの優先度スコアには 0 ～ 100 の値が割り当てられます。ただし、Now Platform では、セキュリティインシデントの [優先度] フィールドは 1 ～ 5 の値をサポートしています。前の図に示すように、スクリプトインクルードは、LogRhythm アラームフィールドの値を Now Platform のセキュリティインシデントのフィールドでサポートされている適切な値に変換します。

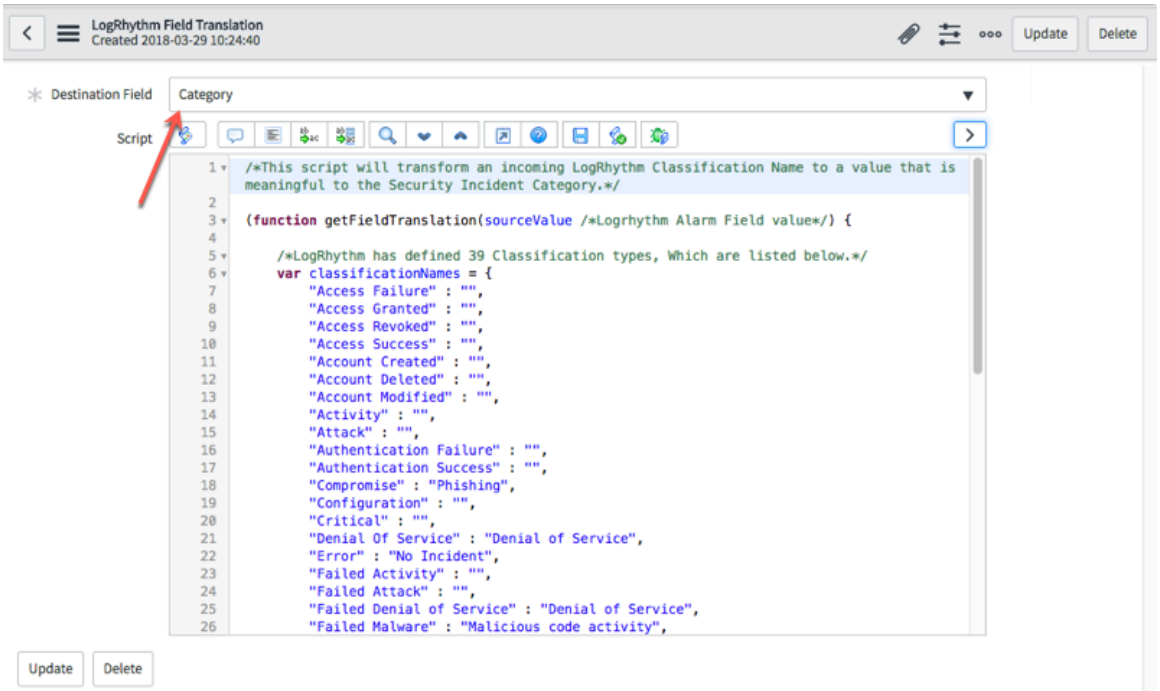
「Priority」のフィールドのこの例では、LogRhythm アラーム値が「80」以上の場合、[セキュリティインシデント] フィールド (Priority) には「1」と表示されます。この値は、セキュリティインシデントの「Critical」の優先度に変換されます。アラームの値がない場合、セキュリティインシデントのフィールドは null に設定されます。

2. 変更を入力し、[更新] をクリックして変更を保存します。
[LogRhythm フィールド変換] テーブルが表示されます。
3. テーブルを閉じて [マッピング] フォームに戻ります。

次の図は、[宛先フィールド] 選択リストで「Category」が選択されたスクリプトエディターを示しています。

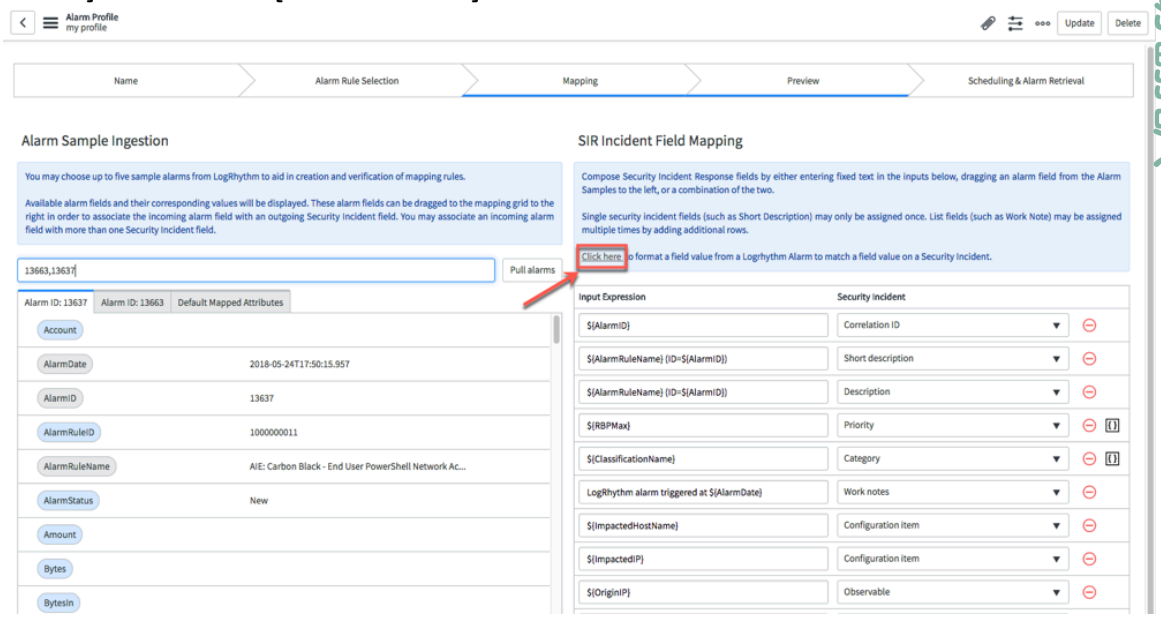
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [フィールド変換] リストに新しいフィールドを追加する場合は、次のステップに従って新しいレコードを追加します。

a. マッピングフォームを表示した状態で、[SIR インシデントフィールドマッピング] セクションの [ここをクリック] リンクをクリックしてます。

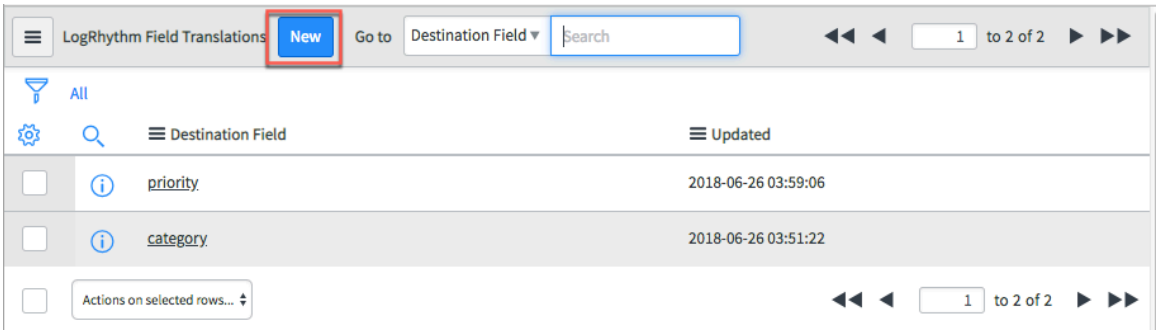


す。

「priority」と「category」の宛先フィールドを含む LogRhythm フィールド変換リストが表示されます。

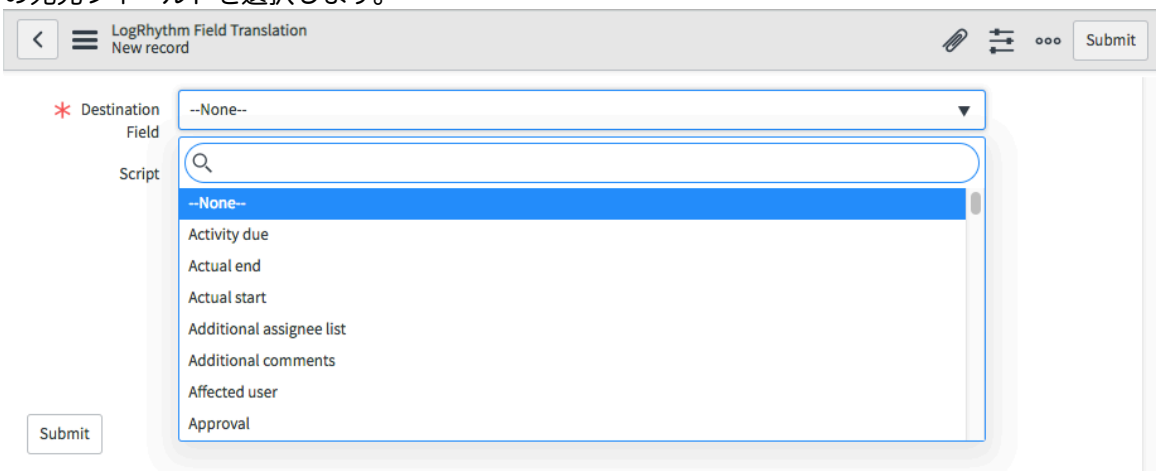
b. [新規] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



新しいレコードが表示されます。

c. [宛先フィールド] 選択リストから、スクリプト化された値を表示するセキュリティインシデントの宛先フィールドを選択します。



d. [送信] をクリックします。
スクリプトエディターが表示されます。

e. エディターに変更を入力し、[送信] をクリックして変更を保存します。
[LogRhythm フィールド変換] テーブルが新しいレコードとともに表示されます。

5. テーブルを閉じて [マッピング] フォームに戻ります。

LogRhythm のアラームプロファイルのコピー

新しいアラームプロファイルを作成する代わりに、既存のプロファイルとその関連設定をコピーします。さまざまなタイプのアラームに対して複数のアラームプロファイルを作成していて、既存のプロファイルの設定を再利用する場合は、アラームプロファイルをコピーして時間を節約できます。このプロセスはオプションです。

始める前に

必要なロール：sn_si.admin

このタスクについて

プロファイルをコピーすると、プロファイルの重複を避けるためにプロファイル名が最初に変更されます。また、コピーされたプロファイルは非アクティブに設定されるため、構成が完了する前に誤ってアクティブになることはありません。

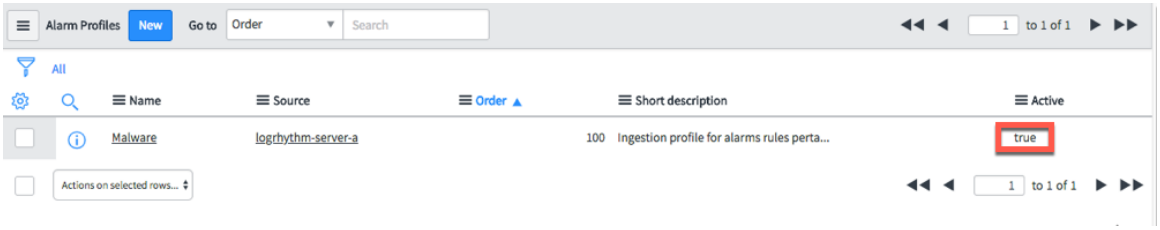
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

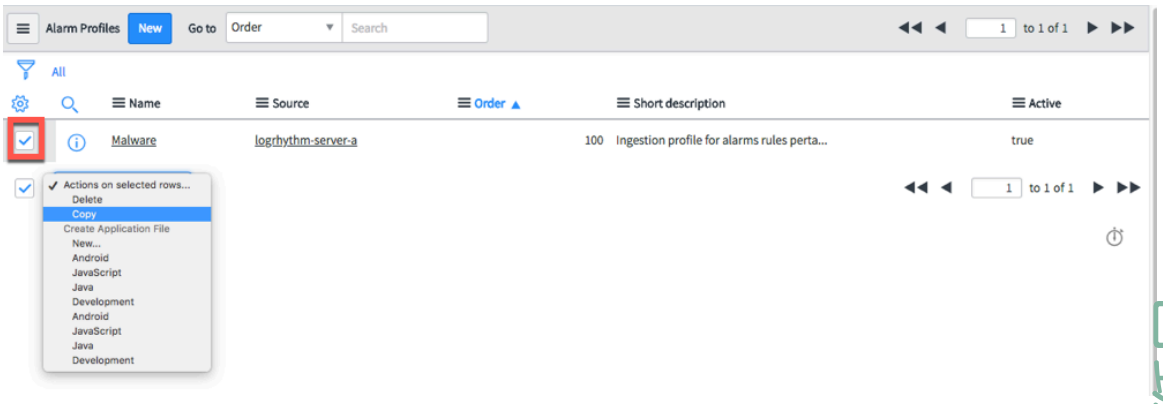
手順

1. 次のように移動する。 **All** (すべて) > **LogRhythm** 統合 > **LogRhythm** アラームプロファイル.

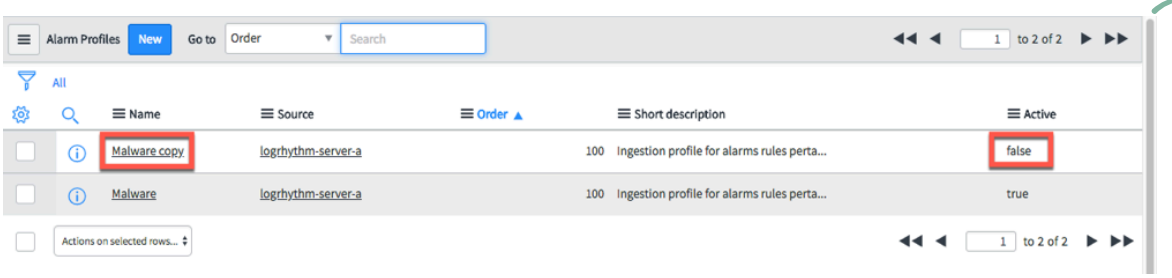
   表示されるリストの「Active」列は、プロファイルがアクティブ (true) かどうかを示します。



2. [名前] 列の左側のフィールドで、レコードの名前を選択します。
3. [選択した行のアクション] 選択リストから [コピー] を選択します。



[アラームプロファイル] リストに、コピーしたプロファイルと元のプロファイルの両方が表示されます。元のレコードはアクティブですが、この時点ではコピーは非アクティブです (false)。構成が終わったら、このコピーしたプロファイルをアクティブにします。



コピーしたプロファイルの値を編集し、名前を変更して、プルしたアラームルールを新しいプロファイルに適用できるようにします。構成ステップが完了すると、新しいプロファイルをアクティブにするように求められます。

LogRhythm の自動アラームクロージャーの無効化

LogRhythm Web コンソールでセキュリティインシデントのクローズ情報を表示しない場合は、自動アラームクロージャー機能を無効にします。非アクティブ化すると、Now Platform は LogRhythm Web コンソール内のアラームをクローズしなくなります。このプロセスはオプションです。

始める前に
必要なロール：sn_si.admin

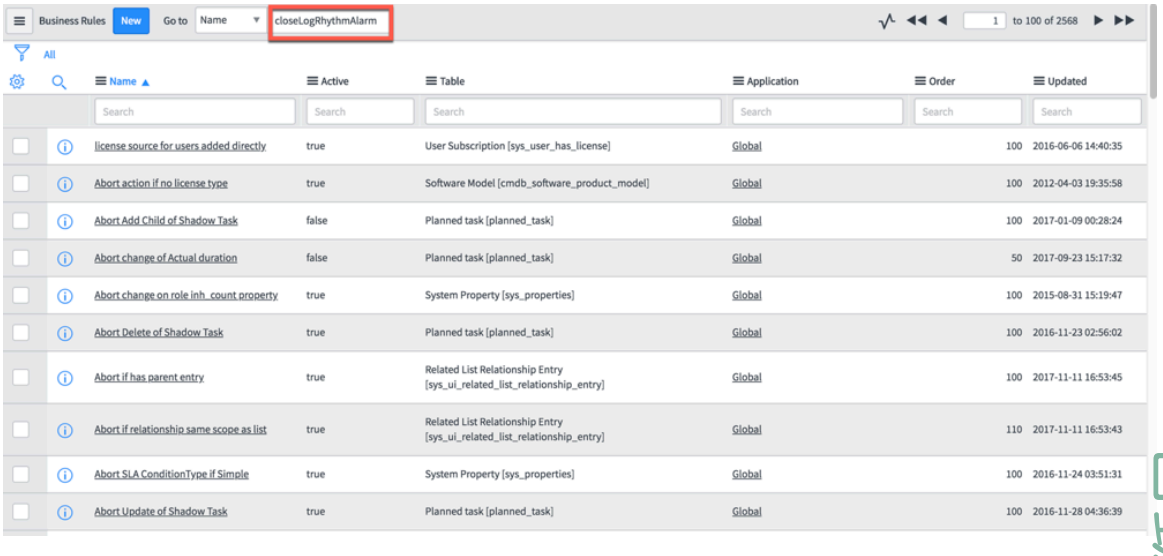
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
無効にすると、セキュリティインシデントに関するステータスメモやその他のクローズ情報が LogRhythm Web コンソールに表示されなくなります。

手順

1. 次のように移動する。 **All** (すべて) > システム定義 > ビジネスルール をクリックし、[ビジネスルール] モジュールを選択します。
2. [ビジネスルール] リストに表示されない場合は、検索フィールドに「**SI** クローズ時の **LogRhythm** クローズアラーム **(LogRhythm Close Alarm On SI Closure)**」と入力し、**Enter** を押します。



3. [名前] 列で **[SI** クローズ時の **LogRhythm** クローズアラーム **(LogRhythm Close Alarm On SI Closure)]** リンクをクリックし、レコードを開きます。
4. 表示されるレコードで、[アクティブ] チェックボックスをオフにします。
5. [更新] をクリックします。
   これで自動アラームクロージャー機能が無効になりました。

LogRhythm ドリルダウンイベントの表示

セキュリティインシデントの LogRhythm アラームに関連する生イベントまたはベースイベントを表示します。

始める前に
必要なロール：sn_si.admin

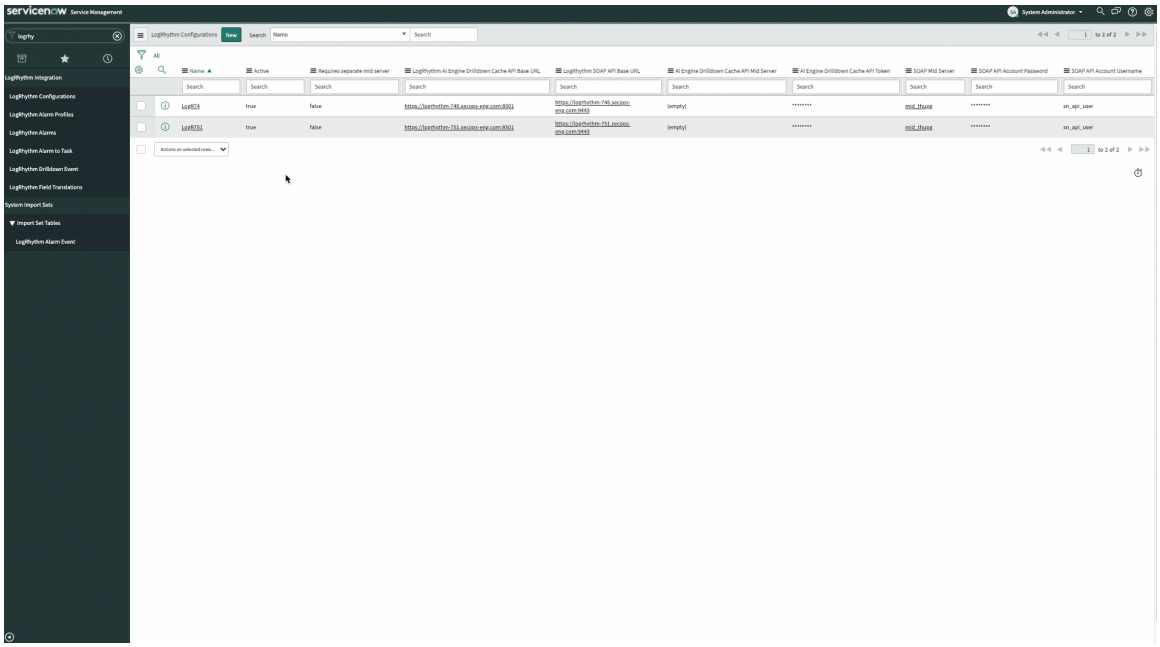
このタスクについて
セキュリティアナリストは、LogRhythm コンソールに戻ることなく、LogRhythm アラームの関連する生イベントまたはベースイベントを表示できます。これを行うには、SIR インシデントのすべてのドリルダウンイベントを含む関連リストに移動します。

手順

次のように移動する。 **All** (すべて) > **LogRhythm** 統合 > **LogRhythm** ドリルダウンイベント.

次の図は、**[LogRhythm** ドリルダウンイベント] モジュールに移動し、イベントのリストを [アラーム **ID** 別にグループ化 **(Group By Alarm ID)]** でイベントのリストをソートし、関連するセキュリティインシデントをクリックする方法を示しています。セキュリティインシデントでは、関連リンクに **[LogRhythm** ドリルダウンイベント] タブがあります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



Logrhythm 統合のトラブルシューティング

接続性とアラームの取り込みの問題をトラブルシューティングします。

トラブルシューティングについては、次のトピックを参照してください。

- LogRhythm の接続性の確認
- LogRhythm のスクリプト実行とシステムログ

LogRhythm の接続性の確認

LogRhythm REST API をテストするために curl 要求を送信して、LogRhythm クライアントコンソールへの接続を確認します。検証プロセスはオプションです。

始める前に
必要なロール：sn_si.admin

このタスクについて
LogRhythm REST API を設定した後に LogRhythm クライアントコンソールへの接続が正常に機能していることを確認するには、「プラグインのインストールおよび LogRhythm の構成」で設定した MID サーバーをホストするコンピューターから 2 つの curl 要求を送信します。

LogRhythm REST API は認証に WSSE を使用します。これには、Curl および Postman と連携させるための外部スクリプトが必要です。

LogRhythm REST API は認証にトークンを使用するため、統合で使用する実際の検証呼び出しを行うことができます。URL の末尾の「0」は LogRhythm アラーム ID です。デフォルト構成の LogRhythm REST API にはポート 8501 が必要です。このポート番号は、テストに使用する予定の URL に含める必要があります。

手順

「curl -k -i -v --trace-time -o /dev/null -H "Content-Type: text/json" -H "Authorization: Bearer <api token>" "https://<cache drilldown url>/lr-drilldown-cache-api/drilldown/0"」の curl 要求の URL **<LogRhythm REST url>** とトークン **<api token>** を更新して送信し、LogRhythm REST API を検証します。
LogRhythm REST API に正常に接続するには、HTTP 404 を受信する必要がありますが、応答本文に「Alarm ID: 0 not found」(アラーム ID：0 非検出) が含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

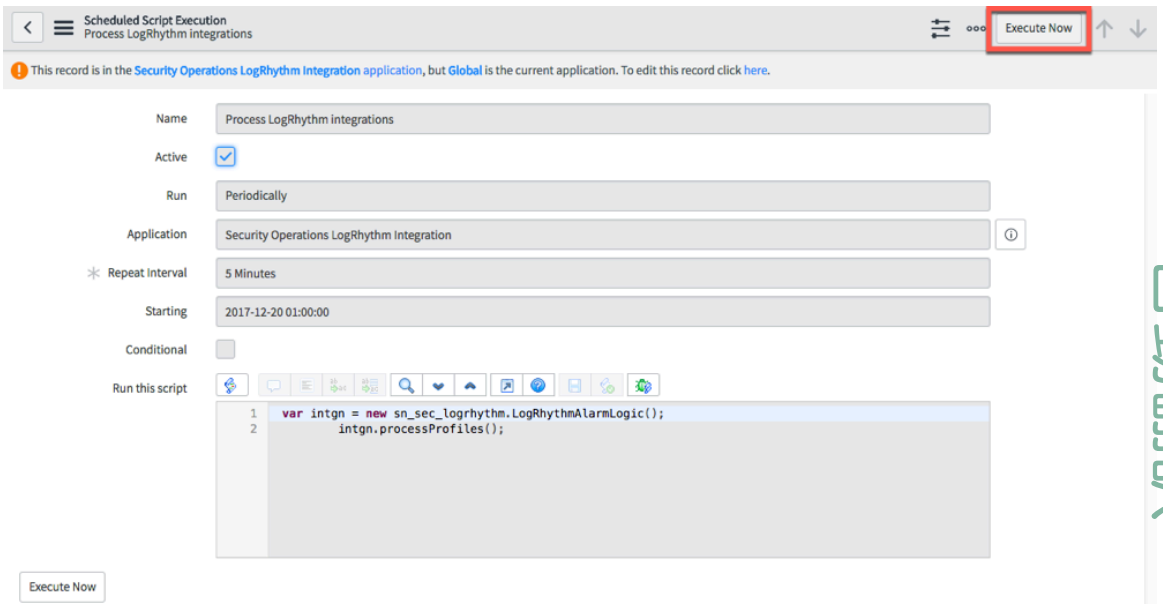
LogRhythm のスクリプト実行とシステムログ

アラームの取り込みの問題をトラブルシューティングする場合は、デフォルトの 5 分間のポーリング間隔を上書きすることで結果をすぐに表示することができます。このシナリオでは、スクリプトの実行を手動で呼び出してポーリングを実行します。この実行はオプションです。

始める前に
必要なロール：sn_si.admin

手順

1. 次のように移動する。 **All** (すべて) > スケジュール済みジョブ > スケジュール済みジョブ をクリックし、[スケジュール済みジョブ] モジュールを選択します。
2. [LogRhythm 統合の処理 (Process LogRhythm integrations)] ジョブレコードをクリックします。
3. 表示される [スケジュール済みスクリプト実行] レコードで、[今すぐ実行] をクリックします。



自動翻訳

さらにトラブルシューティングのヘルプが必要な場合は、LogRhythm クエリのシステムログにアクセスできます。

4. その他の一般的なトラブルシューティングの問題については、次のステップに従ってシステムログにアクセスしてください。

   a. 次のように移動する。 システムログ > **All** (すべて) をクリックし、[すべて] を選択します。

   b. フィルター (Go to) を [ソース] に設定し、「sn_sec_logrhythm」と入力します。

   c. **[Enter]** を押します。
   統合によって生成されたメッセージはこのテーブルに表示されます。リストされているメッセージから統合の実行中のプロセスに関するインサイトが得られる可能性があり、今後のトラブルシューティングに役立つ場合があります。

McAfee ePO の統合

McAfee ePO 統合 Endpoint Detection and Response (EDR) 機能は、Security Operations Center (SOC) のアナリストが、サイバー脅威を特定し、悪意のあるファイルによる損害を修復する際に役立ちます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

概要

この統合で使用される McAfee ePO 機能のセットは 2 つあります。ホストの隔離やマルウェアスキャンの開始などのアクションを呼び出す機能と、クエリを実行してシステムの詳細や脅威イベントを収集する機能です。アクションとクエリのいずれのタイプの機能も、Now Platform インスタンスから呼び出されます。これらの機能をグループ化して特定のタイプのセキュリティイベントが発生したときに自動的に実行されるようにすることも、Now Platform セキュリティインシデントから手動で機能を呼び出すこともできます。

この統合では、次の McAfee ePO 機能を使用できます。

システムの詳細を取得

オペレーティングシステムの詳細を含むシステムの詳細を収集します。

マルウェアスキャンを開始 (Initiate Malware Scan)

スキャン設定とスケジュールに基づいて、影響を受けるエンドポイントのスキャンを開始します。

ホストを隔離/ホストの隔離を解除

調査対象のネットワークアクセスからシステムを削除し、ネットワークへのアクセスを復元します。

脅威イベントのリスト表示 (List Threat Events)

コンプライアンスのステータスと最新の脅威イベントを収集します。

主な機能

この統合の主な機能は次のとおりです。

- インシデント条件に基づく McAfee ePO クエリの自動トリガーをサポートします。
- オンデマンドアクションを実行する Now Platform セキュリティインシデントレスポンス (SIR) セキュリティインシデントからの、手動での McAfee ePO 機能の起動をサポートします。
- さまざまなタイプの McAfee ePO および Now Platform セキュリティオペレーション 機能をトリガーするための複数のプロファイルを柔軟に作成できます。作成したプロファイルによって、マルウェアなど特定のインシデントカテゴリの条件に基づいて、脅威イベント情報が収集されたりアクションが実行されたりします。
- SIR セキュリティインシデントに関する McAfee ePO の結果のプレビューを使用して、プロファイル構成を検証します。
- タグ付けが有効になっている場合、セキュリティタグは、ワークフローによって最初に起動される McAfee ePO 機能と、クエリまたはアクションがいつ正常に完了したかを識別します。
- McAfee ePO のクエリとアクションの完全な監査記録が SIR のセキュリティインシデントに関する作業メモに投稿され、Now Platform から実行されたコマンドが McAfee ePO コンソールに記録されます。
- 複数の McAfee ePO コンソールをサポートします。

ServiceNow のプラグイン

com.snc.si_dep プラグインが必要です。このプラグインは、セキュリティインシデントレスポンス製品をサポートするために必要なすべての依存関係を自動的にインストールします。他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。

次の セキュリティオペレーション アプリケーションを、ServiceNow Store からインストールしてアクティブ化する必要があります。スムーズにインストールできるように、アプリケーションを次のリストの順番で、一度に 1 つずつインストールしてアクティブ化します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

1. Security Integration Framework
2. Security Support Common
3. セキュリティサポートオーケストレーション
4. セキュリティインシデントレスポンス
5. セキュリティインシデントレスポンスワークスペース

統合のための Now Platform インスタンスのセットアップの詳細については、「McAfee ePO 統合での Now Platform インスタンスの設定」を参照してください。

ServiceNow 拡張プラグイン

この統合には ServiceNow Security Operations Extension for McAfee ePO® 拡張プラグインが必要です。この ServiceNow プラグインを McAfee ePO コンソールにインストールします。詳細については、「McAfee ePO 統合での Now Platform インスタンスの設定」を参照してください。

MID サーバー

この統合では、McAfee ePO サーバー (コンソール) に接続するため、Now Platform® インスタンスに MID サーバーをインストールして構成する必要があります。MID サーバーの詳細については、ServiceNow 製品ドキュメント Web サイト を参照してください。

サポートされている McAfee のバージョン

この統合は、McAfee ePO のバージョン 5.9.1 および 5.10 をサポートしています。McAfee Agent 5.5.1.388 をサポートしています。 McAfee 製品と ePolicy Orchestrator の詳細については、McAfee 製品の Web サイト を参照してください。

この統合は、McAfee Endpoint Security Threat Prevention 製品のバージョン 10.5 をサポートしています。バージョン 10.5 が動作していない場合は、McAfee ePO アドミニストレーターに問い合わせて、お使いのバージョンがタグアクションを介したオンデマンドスキャンをサポートできるかどうかを確認してください。

この統合では McAfee ePO セキュリティタグを使用します。セキュリティタグは McAfee ePO コンソールで作成する必要があります。セキュリティタグの詳細については、「McAfee ePO コンソールを セキュリティインシデントレスポンス (SIR) と統合するように設定する」を参照してください。

参照

参照	ドキュメント識別子	ドキュメントタイトル
1	McAfee 製品の Web サイト	McAfee 製品の Web サイト
2	ePolicy Orchestrator Cloud の McAfee ビジネス製品ドキュメント	McAfee 製品ドキュメント
3	ServiceNow 製品ドキュメント Web サイト	ServiceNow 製品ドキュメント Web サイト

統合のセットアップ、インストール、および結果の検証の進行状況を追跡するためのチェックリストについては、「McAfee ePO 統合のチェックリスト」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

アプリケーションをスムーズにインストールし、想定通りの結果が得られるように、記載されている順序でトピックに従ってください。

関連情報

McAfee ePO の統合アーキテクチャ

McAfee ePO の統合アーキテクチャ

次のトピックでは、システムアーキテクチャの概要と統合の主な機能について説明します。また、ServiceNow Storeからアプリケーションをインストールする前に Now Platform インスタンスと McAfee ePolicy Orchestrator (McAfee ePO) コンソールで完了する必要があるセットアップ手順についても説明します。

McAfee ePO の統合に関する主な用語

次の用語は、統合のインストールと構成に関するドキュメント全体で使用されます。

Now Platform

エンタープライズ ServiceNow 製品。Now Platform をベースとして、セキュリティインシデントレスポンス (SIR)、IT Service Management (ITSM)、その他の製品といった、個々のコンポーネントがビルドされています。

セキュリティインシデントレスポンス (SIR)

検出と初期分析から、封じ込め、根絶、復旧、および最終的なインシデントの事後レビューとクローズに至るまで、セキュリティインシデントの進捗状況を追跡する Now Platform アプリケーション。

プラグイン

プラグインは、Now Platform インスタンス内で特定の機能を提供するソフトウェアコンポーネントです。統合プラグインのインストールと構成の詳細については、「McAfee ePO 統合用のアプリケーションのインストールとサーバーの構成」を参照してください。

ePolicy Orchestrator (McAfee ePO)

McAfee のサービス、製品、および設定を管理するユーザーコンソール。

McAfee 拡張プラグイン

この統合には ServiceNow 拡張プラグインが必要です。このプラグインは McAfee ePO コンソールにあり、McAfee ePO コンソールを Now Platform インスタンスに接続します。

機能

Now Platform インスタンスから開始されて McAfee ePO コンソールで実行される自動アクティビティで、拡張クエリを実行し、資産に対するアクションを実行します。

プロファイル

いつ、どのような条件で拡張クエリを実行し、資産に対してアクションを実行するかを指定するために構成する、McAfee ePO の機能の設定。

MID サーバー

Now Platform と外部アプリケーション、データソース、サービスの間の通信やデータの移動を支援するアプリケーション。

ServiceNow アドミン (admin)

SIR および McAfee ePO プラグインを Now Platform インスタンスにダウンロードしてインストールするユーザーのロール。このロールを持つユーザーは、必要に応じて Security Incident Management者ロールのアサインも行います。

ServiceNow セキュリティインシデントアドミン (sn_si.admin)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このロールを持つユーザーは、必要に応じて、Now Platform インスタンス内での セキュリティインシデントレスポンス (SIR) 製品との McAfee ePO 統合の設定を行います。このロールを持つユーザーは、必要に応じてセキュリティインシデントアナリストロールのアサインも行います。

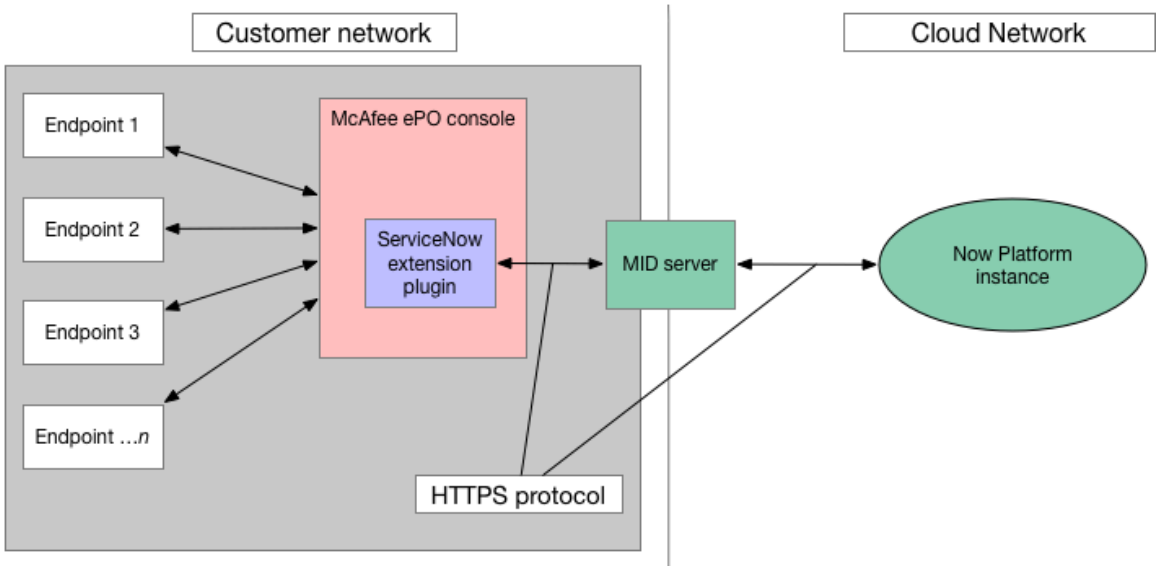
ServiceNow セキュリティインシデントアナリスト (sn_si.analyst)

このロールを持つユーザーは、SIR 製品で発生したセキュリティインシデントに対応して分析します。

システムの接続とデータフロー

次の図は顧客の環境の例です。Now Platform インスタンスが ServiceNow 拡張プラグインを介して McAfee ePO サーバー (コンソール) に接続するには、Now Platform MID サーバーが必要です。接続後、Now Platform から機能を呼び出してマルウェアスキャンを開始し、ホストマシンを隔離してネットワークに戻し、前回のスキャン結果を取得して、資産のシステムの詳細を収集します。呼び出した機能によって資産の中で検索条件に一致する結果が返されると、MID サーバーを介してデータが Now Platform インスタンスにプルされます。データは Now Platform セキュリティインシデントレスポンス (SIR) セキュリティインシデントの関連リストに表示されます。次の図で、1 つのエンドポイントグループを 1 台の McAfee ePO コンソールで管理した場合のデータフローを示します。

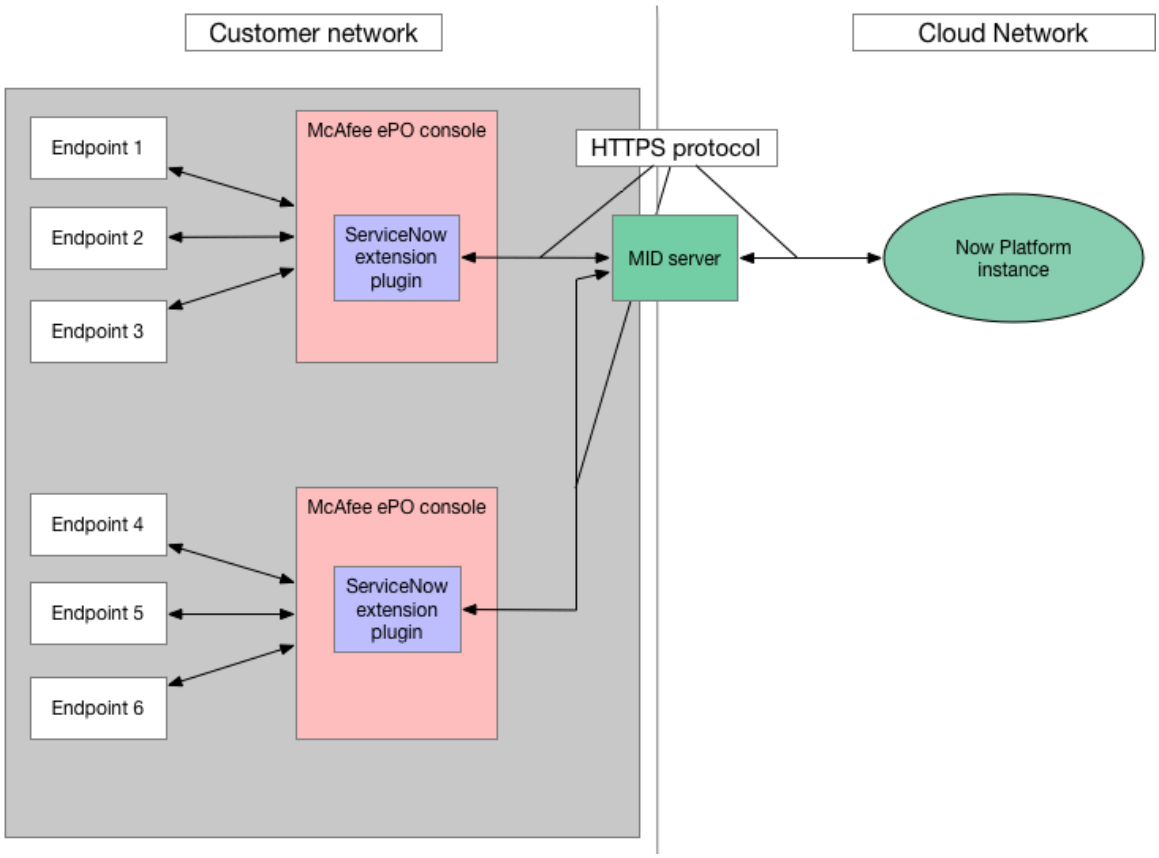
単一エンドポイントの構成



次の図に示すように、この統合では複数の McAfee ePO コンソールをサポートできます。あるエンドポイントのグループを 1 台の McAfee ePO コンソールで管理し、別のエンドポイントのグループを別の McAfee ePO コンソールで管理することができます。複数の McAfee ePO コンソールからのデータは、単一の MID サーバーを介してプルされます。ただし、組織の必要に応じて、複数の MID サーバーを構成することもできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

複数の **MID** サーバーの構成



McAfee ePO の統合のためのワークフロー

この統合には、次のワークフローが含まれます。これらのワークフローは、この統合用に特別に事前設定および設計されたものです。必要に応じて、組織のニーズに合わせてワークフローを編集してもかまいません。ワークフローとワークフローエディターの使用に関する一般的な情報については、「ワークフローの概要」を参照してください。

- Security Operations McAfee EPO 統合 - ホストの詳細を取得
- Security Operations McAfee EPO 統合 - マルウェアスキャンを開始 (Initiate Malware Scan)
- Security Operations McAfee EPO 統合 - ホストを隔離
- Security Operations McAfee EPO 統合 - 脅威イベントのリスト表示 (List Threat Events)
- Security Operations McAfee EPO 統合 - 隔離を削除

外部システム接続

統合では、MID サーバーが HTTPS プロトコル接続を介して McAfee ePO コンソールと通信する必要があります。

McAfee ePO 統合のチェックリスト

このチェックリストを使用して、統合のすべてのタスクをガイドします。次のチェックリストには、セットアップとインストールのタスク、および統合の予想される結果を含むユースケースの例が含まれています。

始める前に
必要なロール：ロールは各ステップに記載されています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
次のテーブルを使用して、統合のセットアップ、インストール、および構成の進捗状況を追跡します。次のステップに進む前に、ステップのすべてのタスクを完了してください。テーブルの各行にタスクがリストされており、タスクの実行に必要なロールが特定されています。インストールおよび構成ガイドの番号付けされたトピックも参照されます。

手順

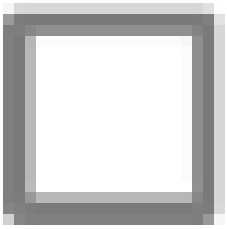
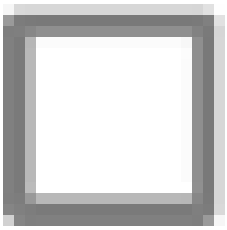
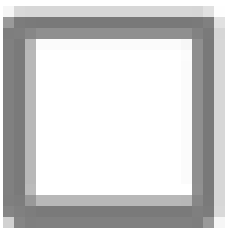
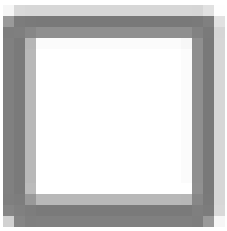
テーブル内のステップを記載されている順に実行します。

チェックリスト

アイテム	説明
☐	Now Platform® アドミンロールを持つユーザーとして、Now Platform® インスタンスを設定します。 **a.** Now Platform® ロールと セキュリティインシデントレスポンス ロールをアサインします。 **b.** 統合をサポートする ServiceNow セキュリティインシデントレスポンス や他のプラグインがインストールされ、Now Platform® のリリース用にアクティブ化されていることを確認します。 **c.** Now Platform® インスタンスに MID サーバーをインストールして構成します。 **d.** 隔離ホストに対してセキュリティインシデントアナリストから送信された要求を処理し、マルウェアスキャンのアクションを開始する場合は、承認グループを作成します。 詳細については、「McAfee ePO 統合での Now Platform インスタンスの設定」を参照してください。
☐	McAfee ePO アドミニストレーターとして、McAfee ePO コンソールを設定します。 **a.** McAfee ePO のバージョン 5.9 を使用していることを確認します。 **b.** ServiceNow 拡張プラグインを McAfee ePO コンソールにインストールします。 **c.** 隔離されたホストに対するセキュリティタグを McAfee ePO コンソールで作成したことを確認し、マルウェアスキャンアクションを開始します。 詳細については、「McAfee ePO コンソールを セキュリティインシデントレスポンス (SIR) と統合するように設定する」を参照してください。 詳細を確認し、拡張プラグインファイルを取得するには、 Now Platform インスタンスで ナレッジ > 記事 > **All** (すべて) をクリックし、[検索] フィールドに「 ServiceNow Security Operations Extension for McAfee ePO」と入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アイテム	説明
	Now Platform アドミンロールを持つユーザーとして、ServiceNow Store から McAfee ePO アプリケーションをインストールしてサーバーを設定し、McAfee ePO コンソールに接続します。 詳細については、「McAfee ePO 統合用のアプリケーションのインストールとサーバーの構成」を参照してください。
	Now Platform セキュリティインシデントアドミンロールを持つユーザーとして、McAfee ePO コンソールで作成したタグ名と一致するように Now Platform インスタンスでセキュリティタグ名を編集します。 詳細については、「McAfee ePO 統合用の Now Platform のセキュリティタグの編集」を参照してください。
	セキュリティインシデントアドミンロールを持つユーザーとして、McAfee ePO の機能のプロファイルを作成します。 プロファイルの詳細については、「McAfee ePO 統合機能プロファイル」を参照してください。プロファイルの作成に必要なステップについては、「McAfee ePO 統合の機能プロファイルの作成」を参照してください。
	セキュリティインシデントアドミンロールを持つユーザーとして、プロファイルを設定し、セキュリティインシデントをテストします。 **a.** トリガー条件と設定に関する情報を確認します。 **b.** プロファイルを設定します。 **c.** セキュリティインシデントをテストしてプレビューします。 **d.** セキュリティインシデントの関連リストで検索結果やその他の詳細を特定します。 **e.** さまざまなタイプのプロファイルを作成して設定し、タイプごとにセキュリティインシデントをテストします。 トリガー条件と代替 CI フィールドの詳細については、「McAfee ePO のプロファイルの構成アイテム (CI) フィールドを使用したトリガー条件の定義」を参照してください。プロファイルの設定、テスト、およびセキュリティインシデントのプレビューに必要な手順、またプロファイルタイプの例については、McAfee ePO 統合のためのプロファイルの構成 の後に記載の例を参照してください。
	Now Platform セキュリティインシデントアナリストのロールを持つユーザーとして、マルウェアスキャンと脅威イベントのリスト表示の要求を追加で送信します。詳細については、「セキュリティインシデントからの McAfee ePO プロファイルの手動トリガー」を参照してください。 Now Platform で、承認ロールを持つユーザーまたは承認グループのメンバーとして、ホスト隔離の要求と隔離の削除の要求を承認します。 承認要求の処理の詳細については、「承認グループの作成」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップ手順を完了し、アプリケーションをインストールおよび構成して、統合の結果が予想どおりであることを確認しました。

McAfee ePO 統合での Now Platform® インスタンスの設定

次のセクションでは、McAfee ePO 統合のためのアプリケーションをインストールする前に Now Platform® インスタンスで完了する必要があるセットアップタスクを説明します。

設定の要件

必要なロール：Now Platform アドミニストレーター (admin)。McAfee ePO 統合での Now Platform® インスタンスの設定の前に、次の情報を確認します。

次の表は、アプリケーションのセットアップ要件のリストです。ServiceNow Store から統合用のアプリケーションをインストールする前に、次のタスクを完了していることを確認してください。

設定タスク	説明
必要な Now Platform® および セキュリティインシデントレスポンス (SIR) のロールがアサインされていることを確認します。	以下のロールが必要です。 • アプリケーションをインストールするためのシステムアドミニストレーター (admin) ロールを持つユーザー。 • Security Incident Management者 (sn_si.admin) ロールを持つユーザーアプリケーションを設定し、プロファイルを作成、アクティブ化、および削除します。 • セキュリティインシデントアナリスト (sn_si.analyst) ロールを持つユーザーは、セキュリティインシデントを処理します。タスクには、セキュリティインシデントから手動でプロファイルを起動するタスクが含まれます。構成ステップ中にプロファイルで承認オプションが選択された場合、ホストを隔離してネットワークに戻すための要求の送信も、このロールを持つユーザーが行います。
McAfee ePO のバージョン 5.9 を使用していることを確認します。	この統合は McAfee ePolicy Orchestrator バージョン 10.4.3 をサポートしています。
ServiceNow 拡張プラグインを McAfee ePO コンソールにインストールしていることを確認する。	ServiceNow プラグインを McAfee ePO コンソールにインストールします。 詳細を確認し、プラグインファイルを取得するには、 Now Platform インスタンスで ナレッジ > 記事 > **All** (すべて) さらに、[検索] フィールドに「ServiceNow Security Operations Extension for McAfee ePO」と入力します。
統合用のアプリケーションをインストールする前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	セキュリティインシデントレスポンス依存関係プラグイン (com.snc.si_dep) が必要です。このプラグインは、セキュリティインシデントレスポンス 製品をサポートするために必要なすべての依存関係を自動的にインストールします。統合に必要な他の セキュリティオペレーション アプリケーションをインストールしてアクティブ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

設定タスク	説明
	化する前に、このプラグインをインストールしてアクティブ化します。 次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。 **1.** セキュリティインシデントレスポンス **2.** セキュリティインシデントレスポンスワークスペース **3.** Security Integration Framework **4.** Security Support Common **5.** セキュリティサポートオーケストレーション Security Operations コアアプリケーションのインストールの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。
MID サーバーがインストールおよび設定されていることを確認します。	Now Platform® インスタンスに、MID サーバーがインストールおよび設定されている必要があります。MID サーバーの詳細については、ServiceNow 製品ドキュメント Web サイト を参照してください。
プロファイルの承認プロセスを有効にする場合に、要求を処理する承認グループが作成されていることを確認する。	ホストマシンの隔離やネットワークへの復元に使用できるオプションの承認プロセスがあります。 このオプションを有効にすると、ホストマシンを隔離してネットワークに復元する前に、事前承認が必要となります。 組織でこれらのアクションをより詳細に制御する必要がある場合は、プロファイルの構成時に [承認が必要] オプションを有効にします。 デフォルトでは、承認権限は Now Platform® Security Incident Management者 (sn_si.admin) にアサインされます。この権限は承認グループに再アサインできます。グループ内では、どのメンバーが要求を承認または却下する権限を持ってもかまいません。 プロファイルセットアップの構成ステップで、アクティブな承認グループを選択します。詳細

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

設定タスク	説明
	については、「承認グループの作成」を参照してください。

McAfee ePO コンソールを セキュリティインシデントレスポンス (SIR) と統合するように設定する

次のセクションでは、統合する対象の ServiceNow Store からアプリケーションをインストールする前に McAfee ePO コンソールで完了する必要があるセットアップ手順を示します。

始める前に

必要なロール：McAfee ePO アドミニストレーター

McAfee ePO アドミン権限を持つユーザーとして、McAfee ePO コンソールに Servicenow.zip 拡張プラグインがインストールされていることを確認します。この拡張プラグインが統合に必要となります。詳細を確認し、プラグインを取得するには、 Now Platform インスタンスで ナレッジ > 記事 > **All** (すべて). [検索] フィールドに「ServiceNow Security Operations Extension for McAfee ePO」と入力します。

このタスクについて

ServiceNow 拡張プラグインは、Now Platform インスタンスを McAfee ePO コンソールに接続します。接続することで、ホスト隔離とマルウェアスキャンの開始のアクションに対して McAfee ePO コンソールで作成したセキュリティタグを、Now Platform インスタンスの機能プロファイルに対して参照できるようになります。

McAfee ePO コンソールのセキュリティタグは、Now Platform インスタンスの機能レコードのセキュリティタグと一致する必要があります。

次の手順では、拡張プラグインをインストールし、McAfee ePO コンソールでセキュリティタグを作成して、そのタグにアクションをアサインする方法を説明します。McAfee ePO コンソールのセキュリティタグの詳細については、McAfee 製品ドキュメント Web サイトを参照してください。

注:
次のセクションの図は McAfee ePO コンソールのものです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. McAfee ePO コンソールに ServiceNow 拡張プラグインをインストールしていない場合は、次の手順に従ってインストールします。

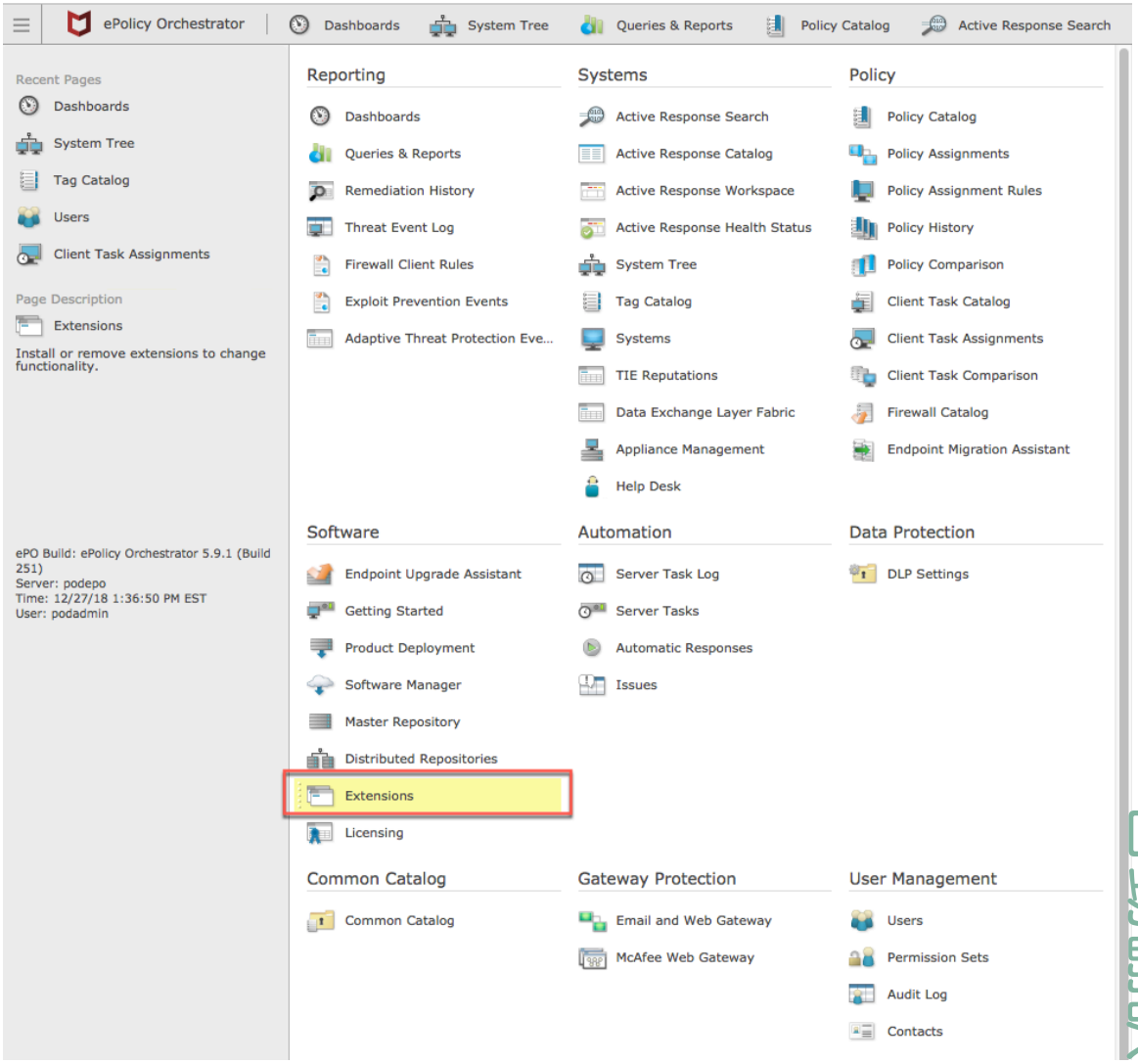
   a. McAfee ユーザー名とパスワードを使用して McAfee ePO コンソールにログインします。

2. 次の図で示すページが表示されない場合は、ホームページのバナーの左上にあるメニューアイコンをクリックして表示します。

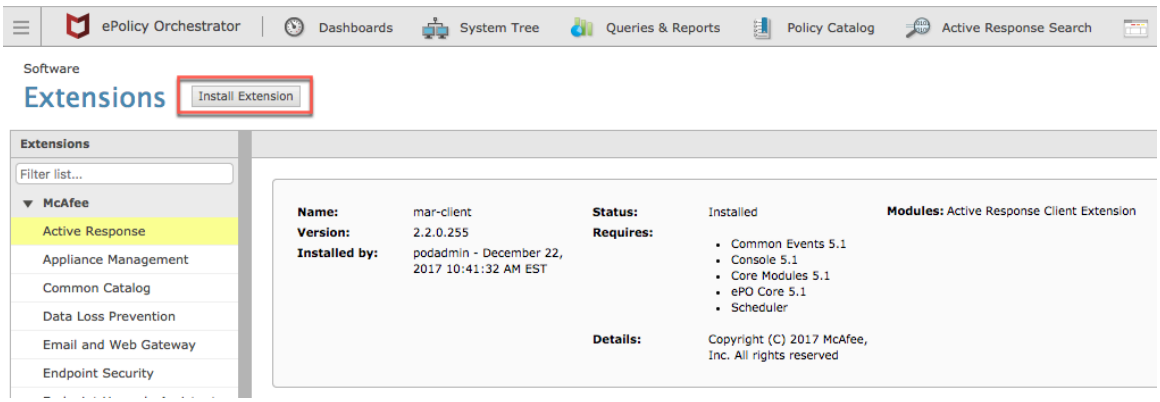
3. [ソフトウェア] セクションで [拡張] リンクをクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

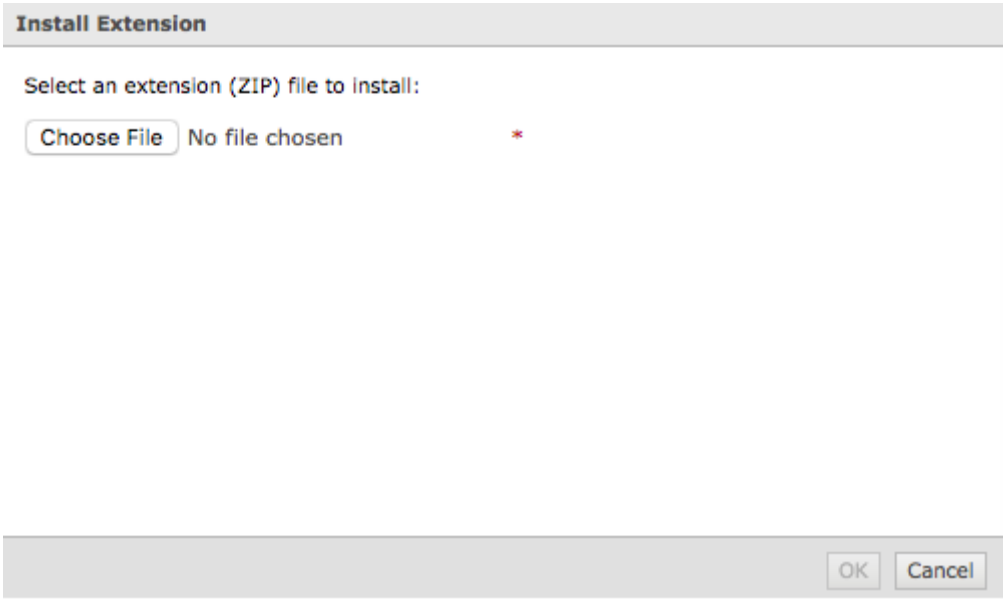


4. 表示される [拡張ファイル] ページで、[拡張ファイルをインストール] をクリックします。

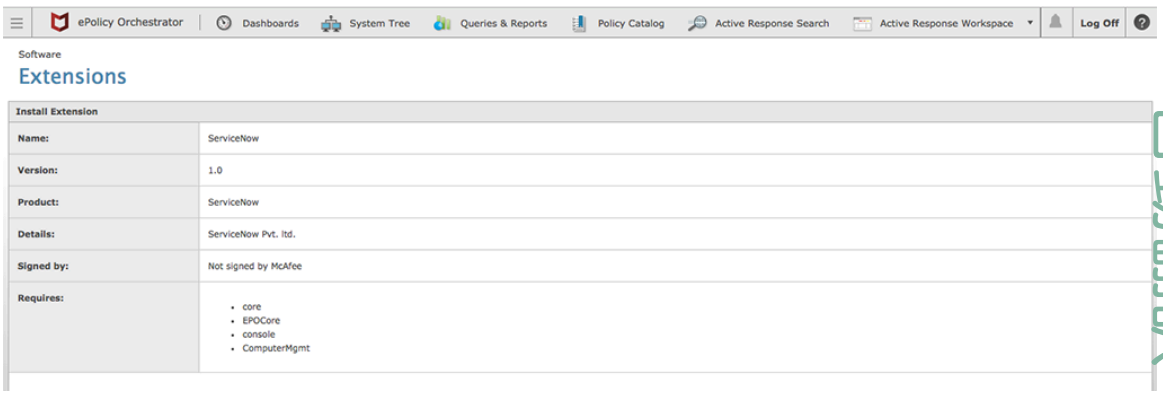


5. [拡張ファイルをインストール] ダイアログで [ファイルの選択] をクリックし、システム上の Servicenow.zip ファイルに移動して、**[OK]** をクリックしてダウンロードします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



ダウンロードが完了すると、[ソフトウェア] の [拡張ファイル] ページが表示され、ServiceNow の拡張ファイルプラグインが一覧表示されます。



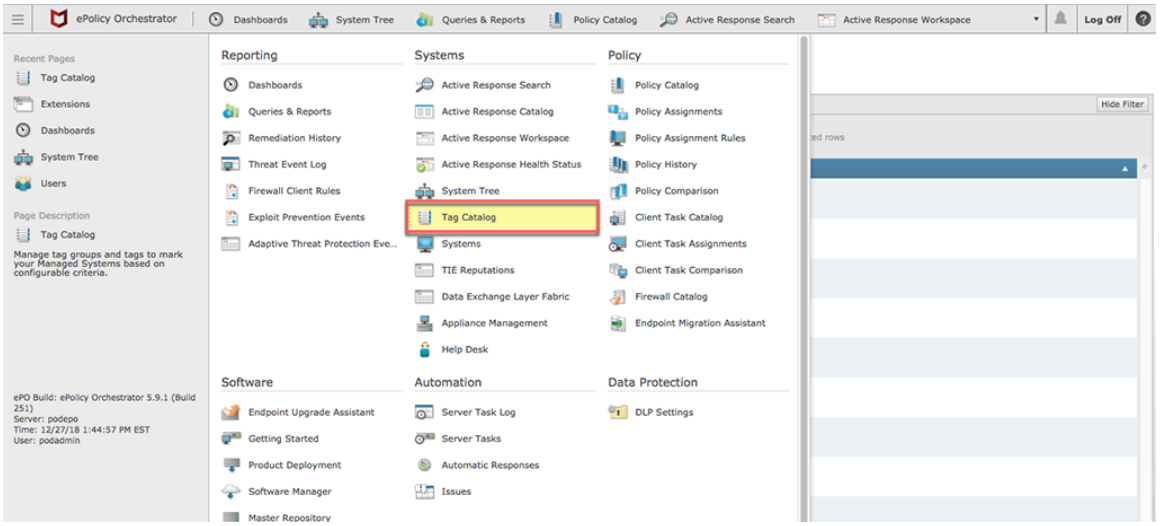
自動翻訳

McAfee ePO コンソールに ServiceNow プラグインの拡張ファイルが正常にインストールされました。

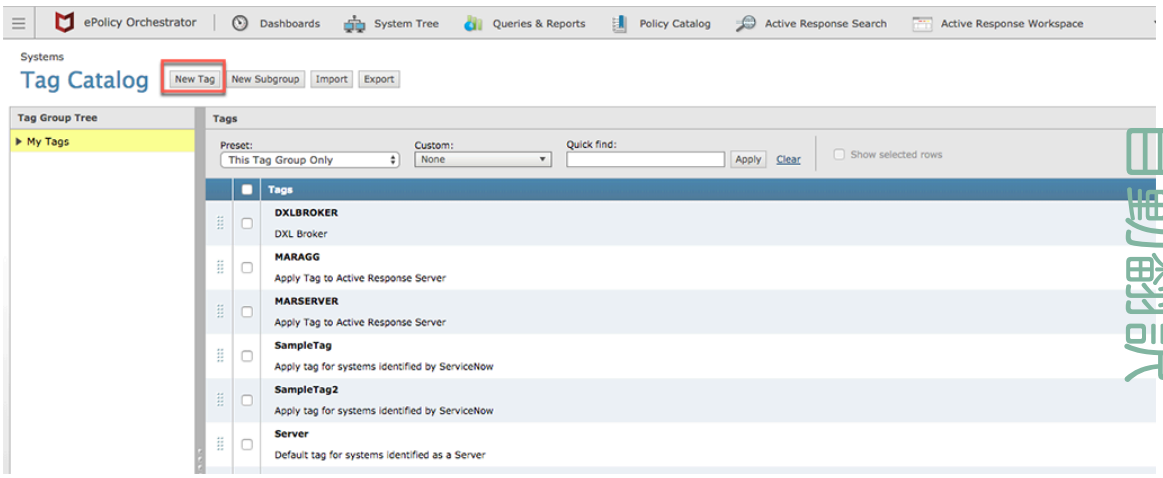
6. マルウェアスキャンの開始およびホストの隔離アクションのセキュリティタグを McAfee ePO コンソールで作成していない場合は、次の手順を実行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. ホームページに移動し、[タグカタログ] リンクをクリックします。

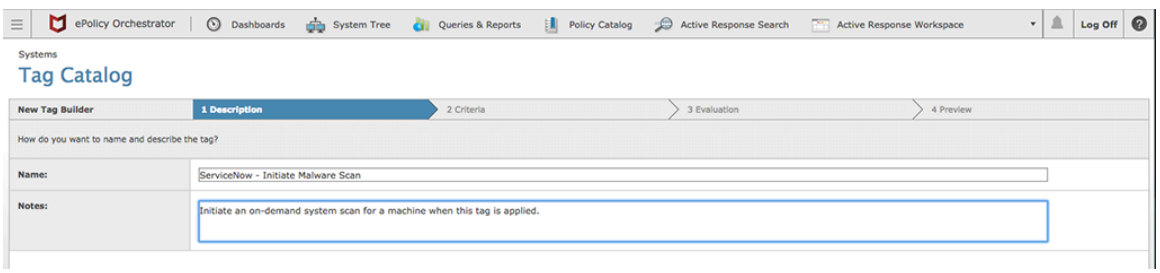


b. 表示される [タグカタログ] ページで、[新しいタグ] をクリックします。



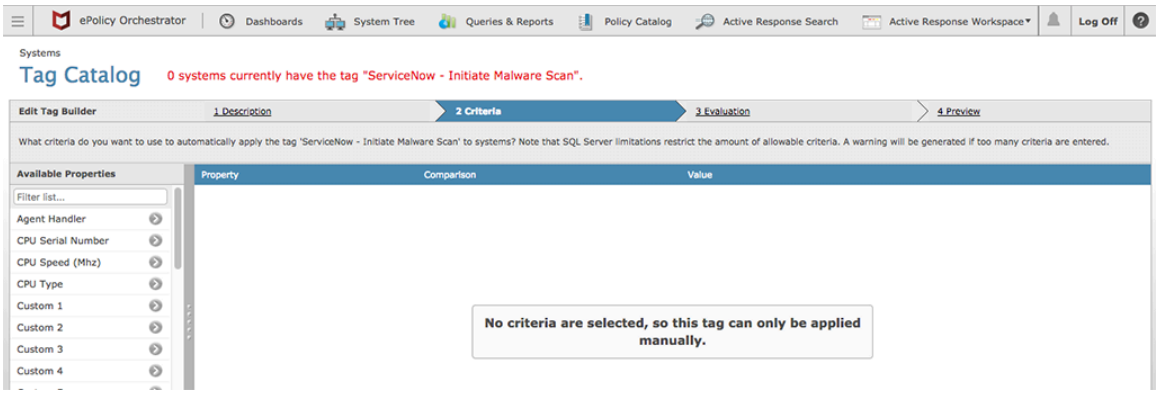
c. 表示される進行状況バーで [説明] ステップを選択した状態で、タグの名前と説明を入力します。

この例では、[マルウェアスキャンを開始 (Initiate Malware Scan)] 機能の名前と説明が記入されたタグが表示されます。このタグ名は、Now Platform インスタンスで照合および参照されたものです。

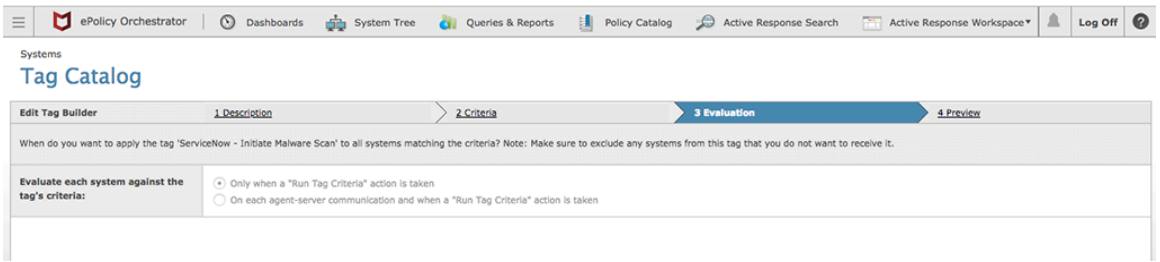


d. 条件のステップに進むには、進捗状況バーの [条件] をクリックします。
表示されているメッセージは、現在このタグにアサインされているアクションがないために手動でしかタグが適用できないことを示しています。

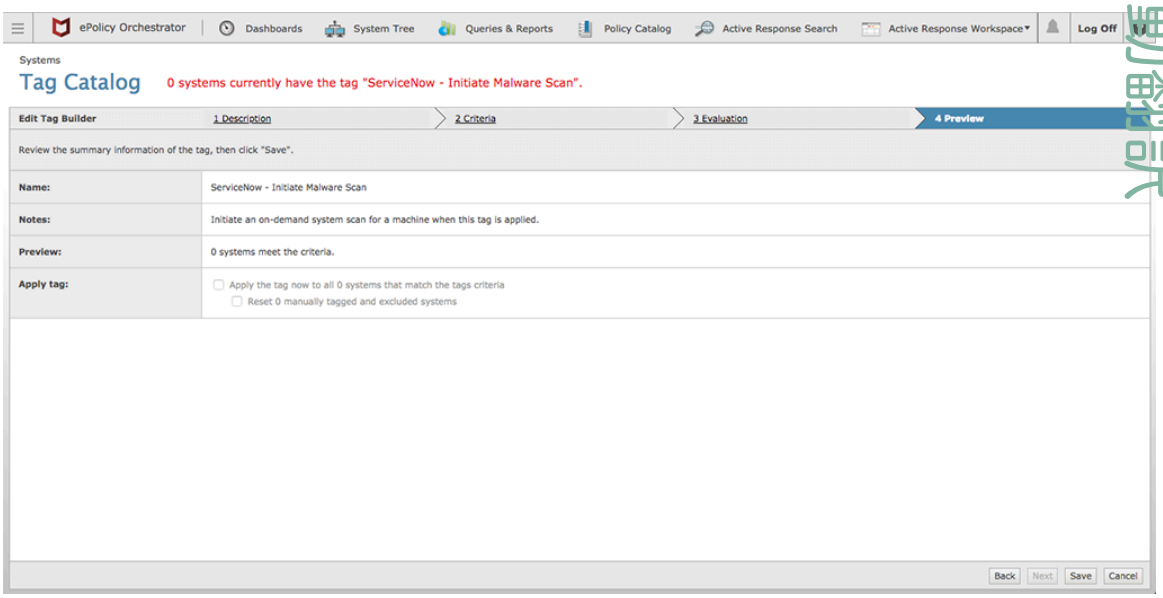
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



e. 進捗状況バーの [評価] をクリックして続行します。



f. [タグカタログ] ページの [評価] ステップを表示した状態で、このページの設定をデフォルトのままにして、進捗状況バーで [プレビュー] をクリックします。

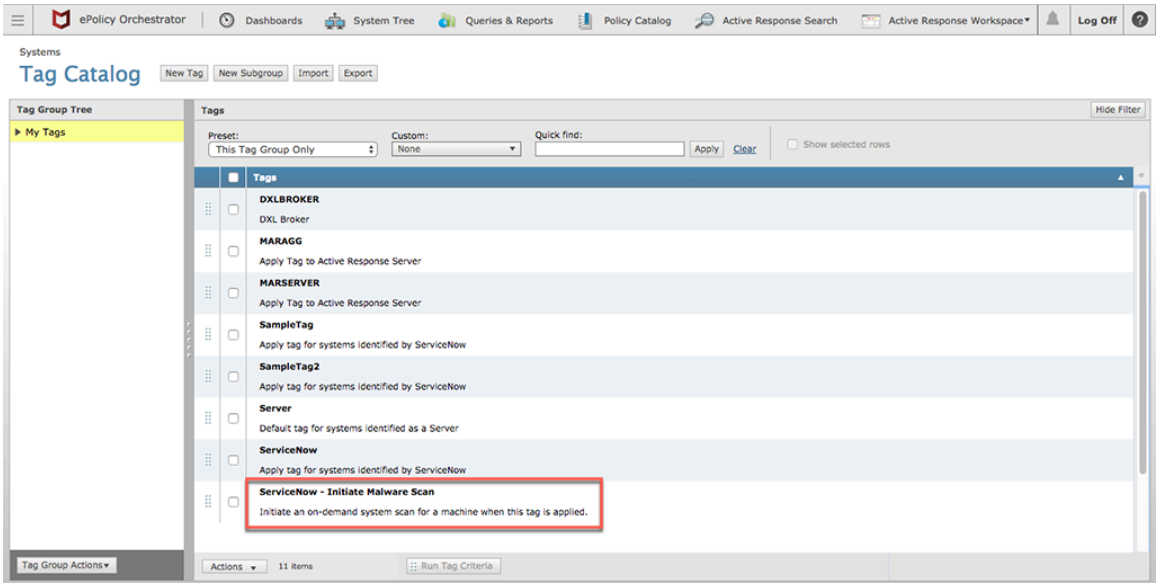


g. [プレビュー] ページを表示した状態で、ページの右下にある [保存] をクリックしてレコードを保存します。

自動翻訳

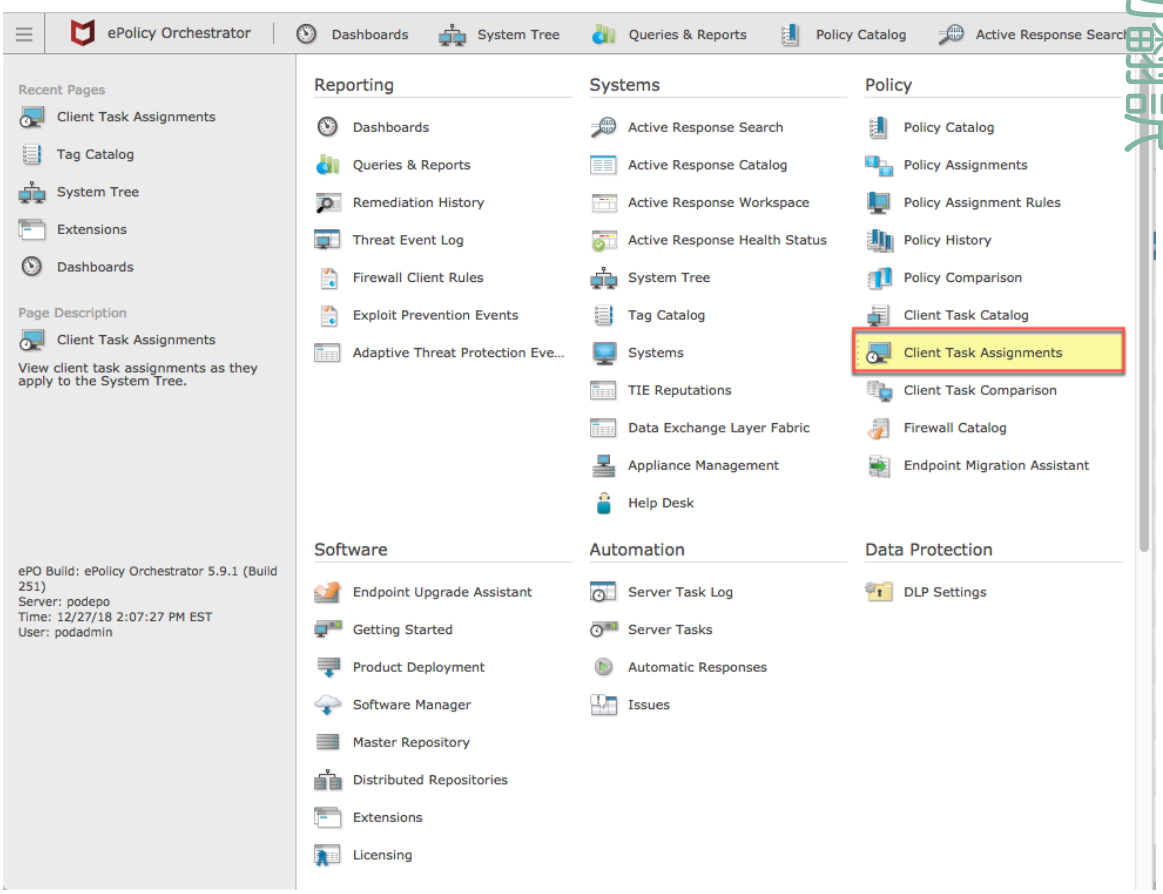
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図で示すように、新しいタグがタグカタログに表示されます。



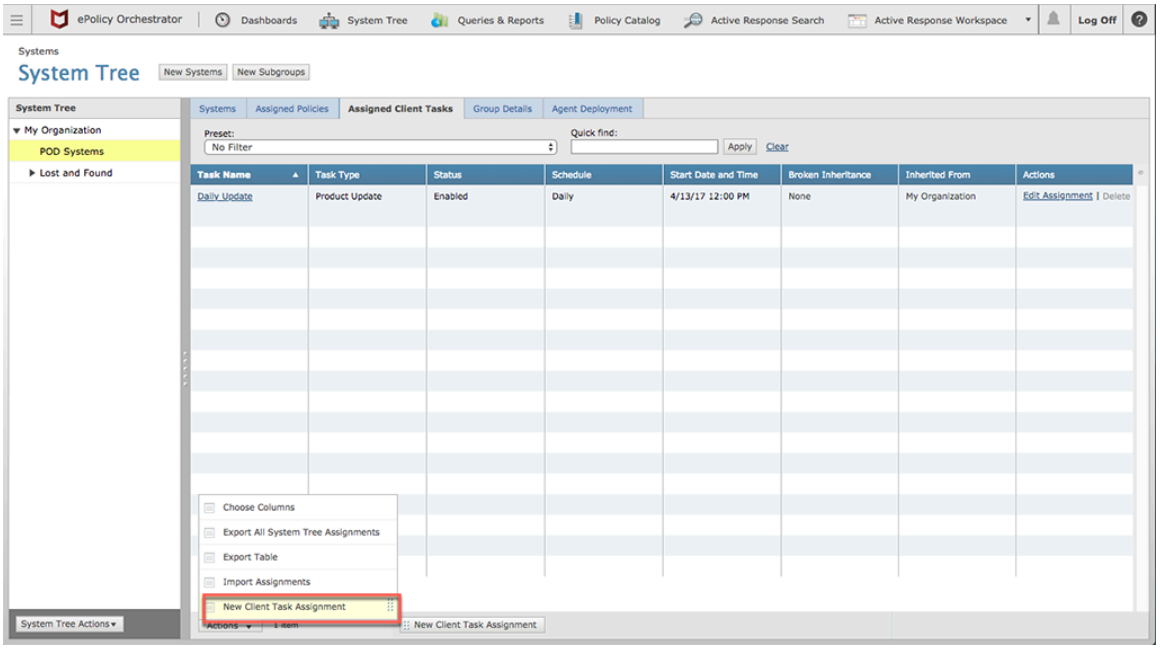
7. 前の手順を繰り返して、ホスト隔離アクションのセキュリティタグを作成します。
両方のタグを作成すると、新しいタグにアクションをアサインできるようになります。
8. 新しいタグにアクションを追加するには、次の手順に従います。

   a. ホームページに移動し、[ポリシー] セクションで [クライアントタスクの割り当て] リンクをクリックします。

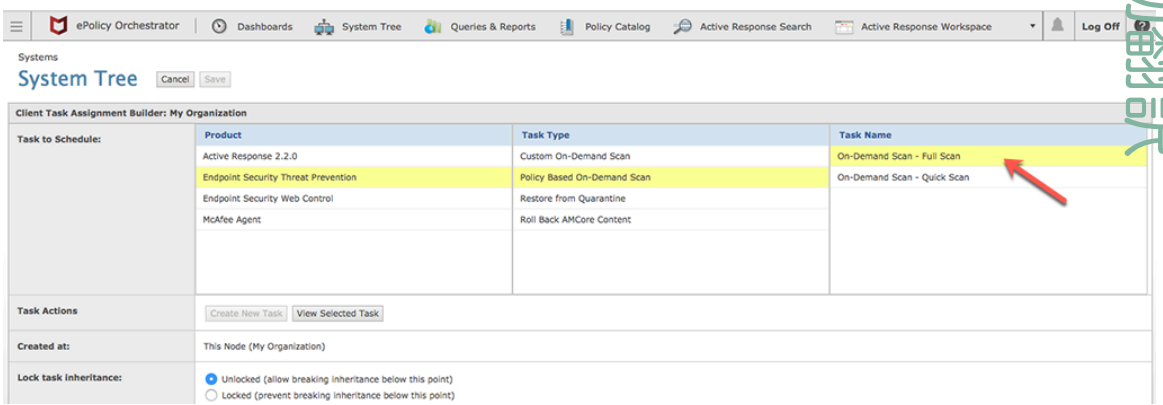


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

b. 表示される [システムツリー] ページの下部で、[アクション] メニューを展開し、 [新しいクライアントタスクの割り当て] を選択します。

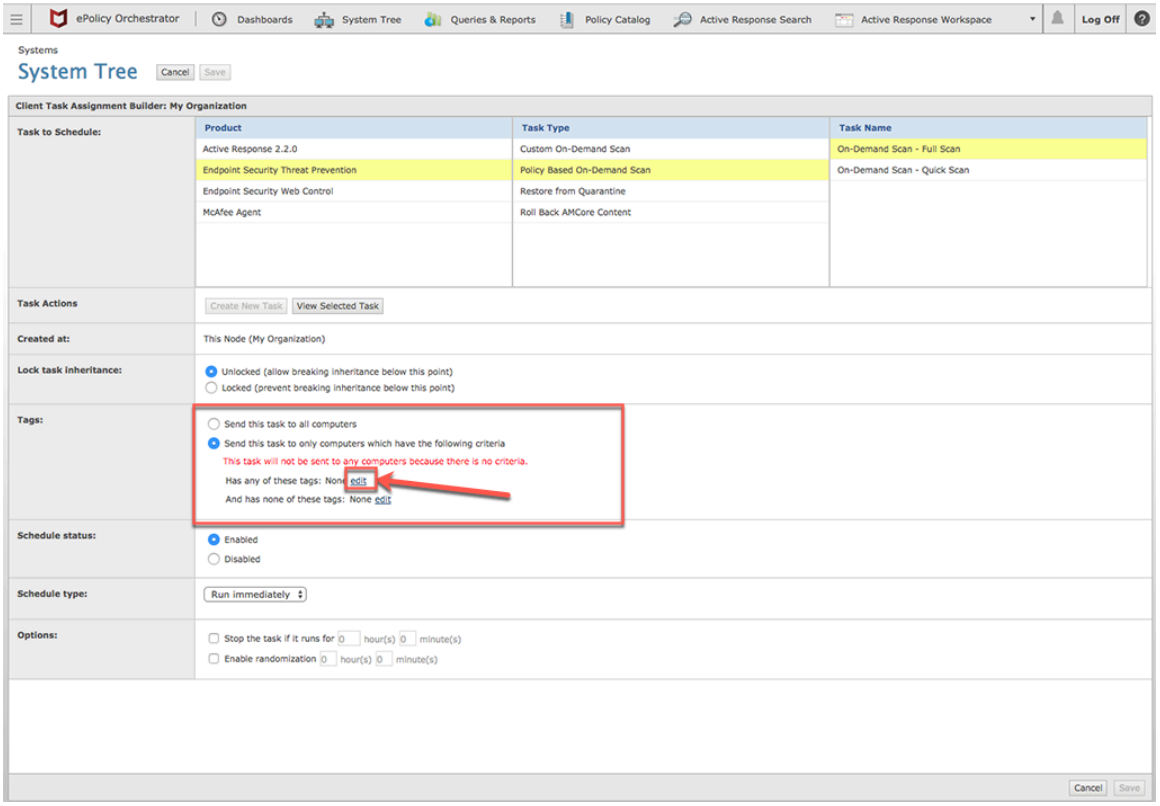


c. 表示されるページで、次の場所に移動します: エンドポイントセキュリティの脅威防止 > オンデマンドスキャンに基づくポリシー > オンデマンドスキャン:フルスキャン 次の図に示すようにパスを選択します。

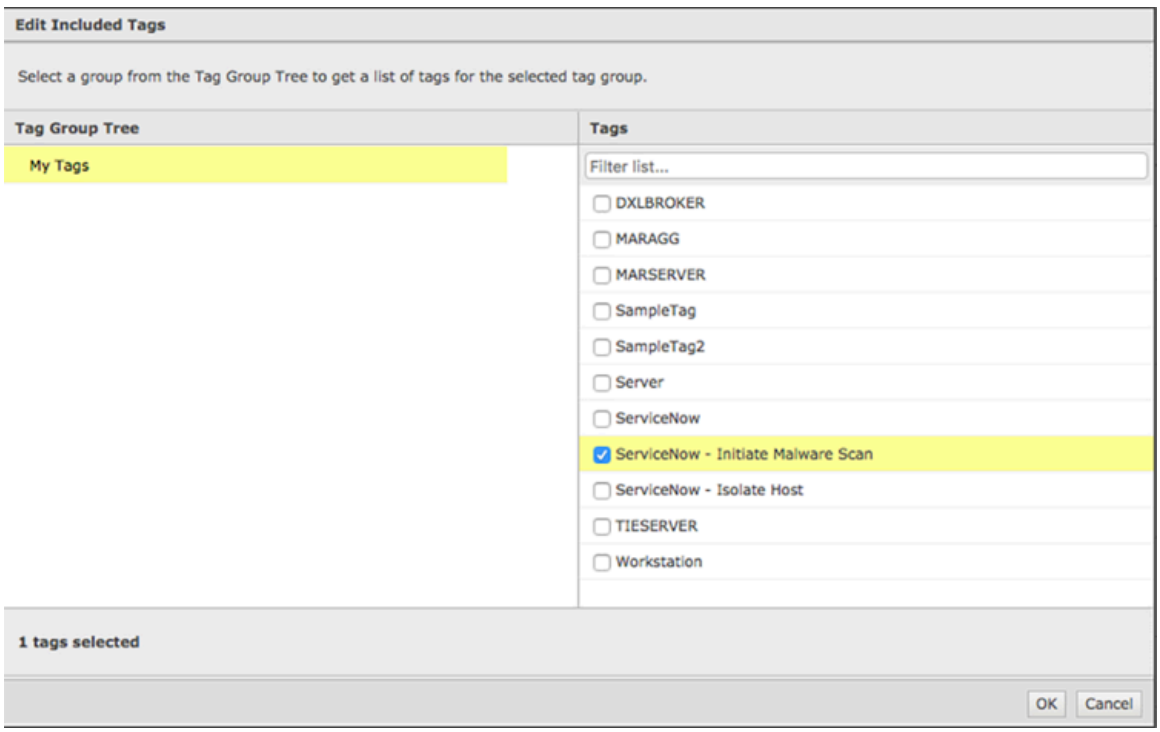


d. [タグ] セクションで、ラジオボタンの下の [次のいずれかのタグがある：(Has any of these tags:)] の横にある [編集] リンクをクリックして、タグの条件を編集します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



e. 表示されるダイアログで、前の手順で作成した [マルウェアスキャンを開始 (Initiate Malware Scan)] の ServiceNow タグを選択し、**[OK]** をクリックします。



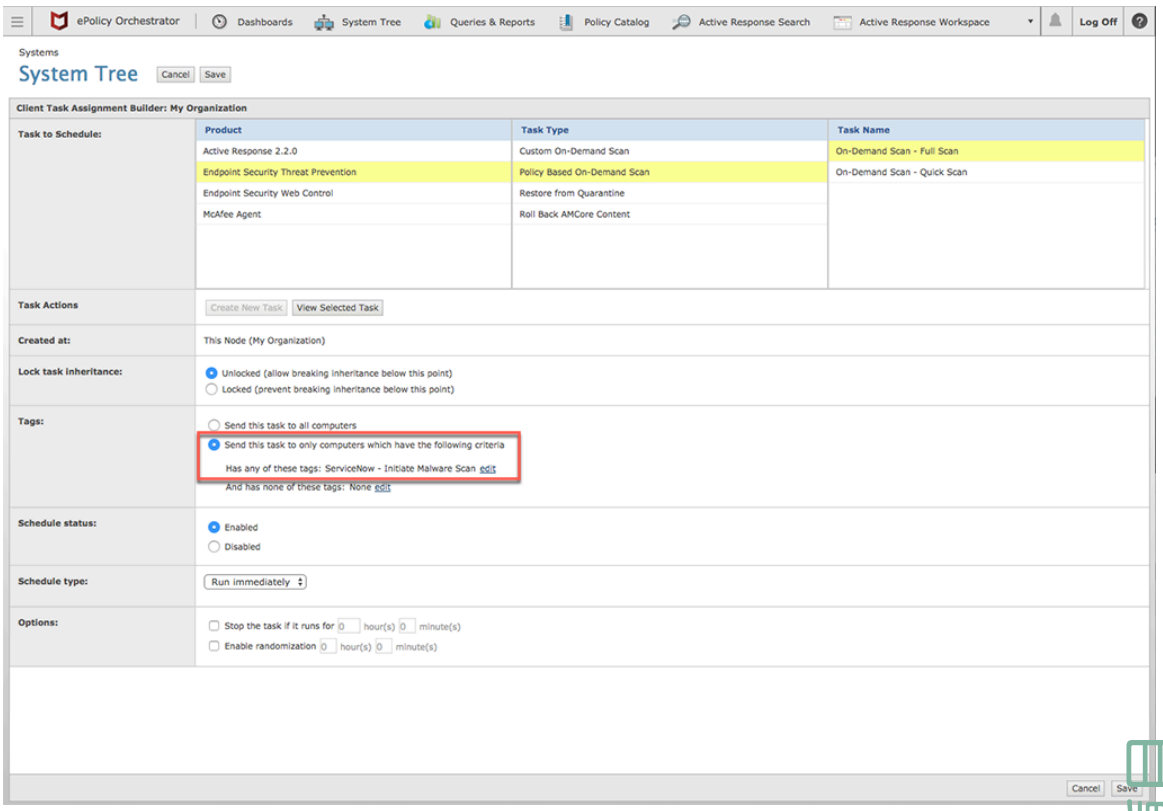
作成した [ServiceNow マルウェアスキャンを開始 (ServiceNow Initiate Malware Scan)] タグが、[オンデマンドスキャン] アクションにアサインされます。

f. [OK] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

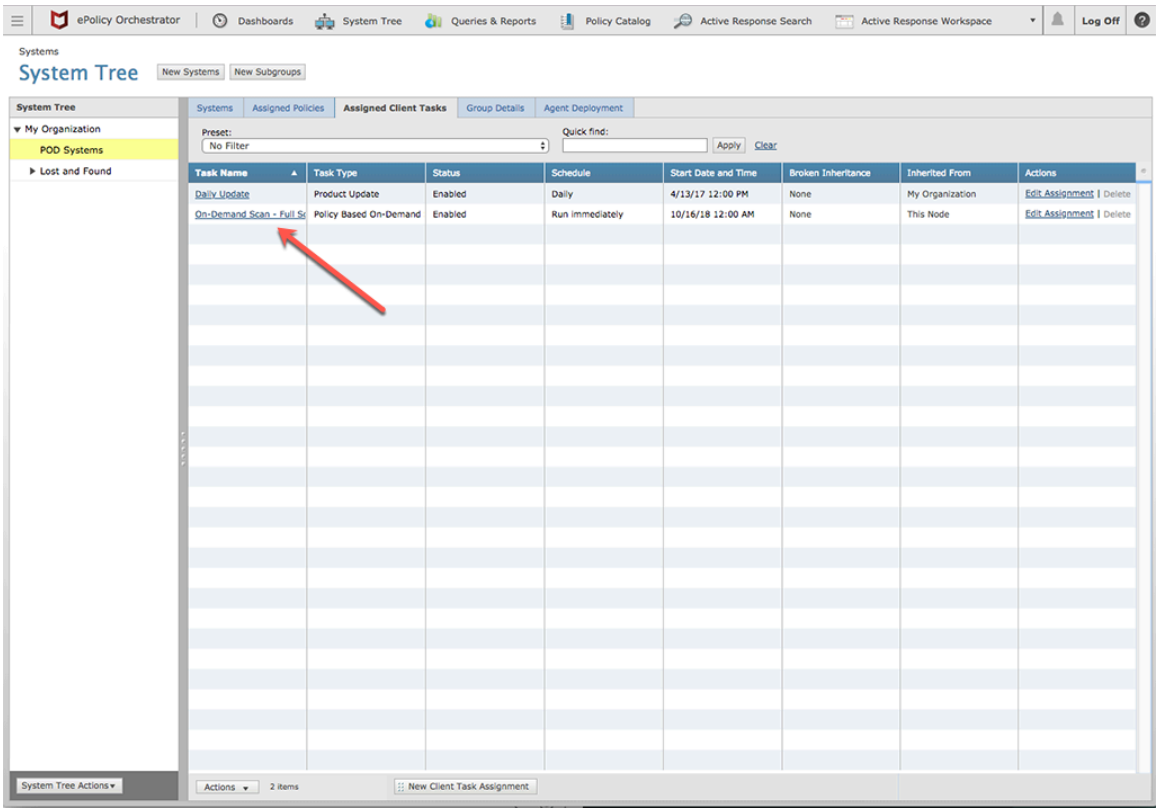
[タグ] セクションのラジオボタンの下の [次のいずれかのタグがある：(Has any of these tags:)] の横に、[マルウェアスキャンを開始 (Initiate Malware Scan)] タグが表示されます。



g. [保存] をクリックします。
[システムツリー] ページで、[割り当て済みのクライアントタスク] リスト (タブ) にタスクが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



h. [ホストを隔離] アクションにアクションをアサインしていない場合は、前の手順を繰り返してアサインします。

拡張プラグインが正常にインストールされ、セキュリティタグが作成され、タグにタスクがアサインされました。McAfee ePO コンソールでの統合のセットアップが完了しました。次のステップでは、Now Platform インスタンスでサーバーを構成します。

McAfee ePO 統合用のアプリケーションのインストールとサーバーの構成

統合のワークフローを呼び出す前に、Now Platform インスタンスで ServiceNow Store から McAfee ePO アプリケーションをインストールして構成します。この構成は McAfee ePO コンソールに接続するために必要です。

始める前に

必要なロール：Now Platform アドミニストレーター (admin)

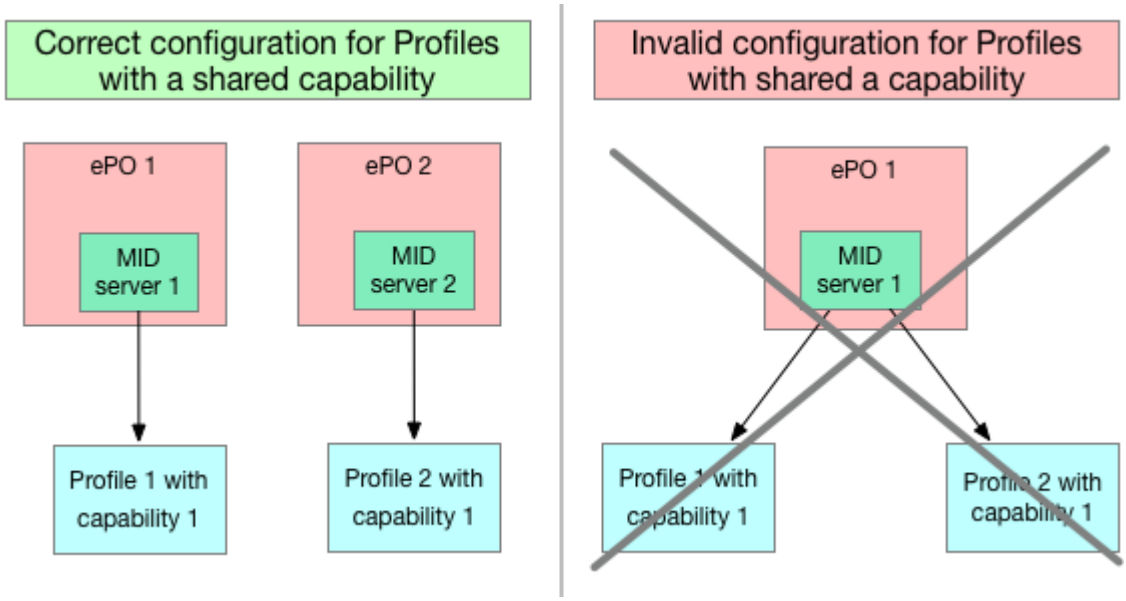
このタスクについて

統合では複数のサーバーをサポートしますが、同じトリガー条件を共有するプロファイル間の競合を回避するため、同じ McAfee ePO サーバーを使用する複数のプロファイルと McAfee ePO 機能を共有することはできません。たとえば、次の図に示すように、それぞれの McAfee ePO サーバーが機能 1 を持つ一意のプロファイルにマッピングされている限りは、複数のプロファイルに機能 1 を持たせることができます。

自動翻訳

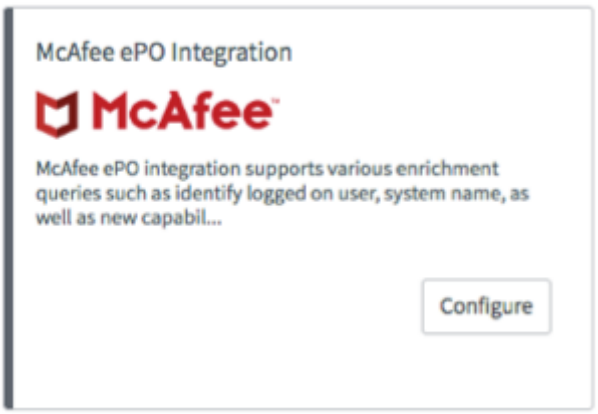
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

McAfee 共有プロファイルの制約事項



手順

1. ServiceNow Store から McAfee ePO for セキュリティオペレーション をダウンロードして、インストールします。
2. 次のように移動する。 セキュリティオペレーション > 統合 > 統合設定.
3. McAfee ePO for セキュリティオペレーション 統合タイルを検索し、[構成] をクリックします。



4. フォームのフィールドに入力します。

McAfee ePO 統合構成 (McAfee ePO Integration Configuration)

フィールド	説明
名前	統合の名前 (例：demo-1)。
ePO サーバー名	McAfee ePO サーバーの名前。使用するサーバーが 1 つの場合の例としては、McAfee HQ (McAfee 本社) があります。この名前で、サーバーおよび関連する認証情報を認識します。

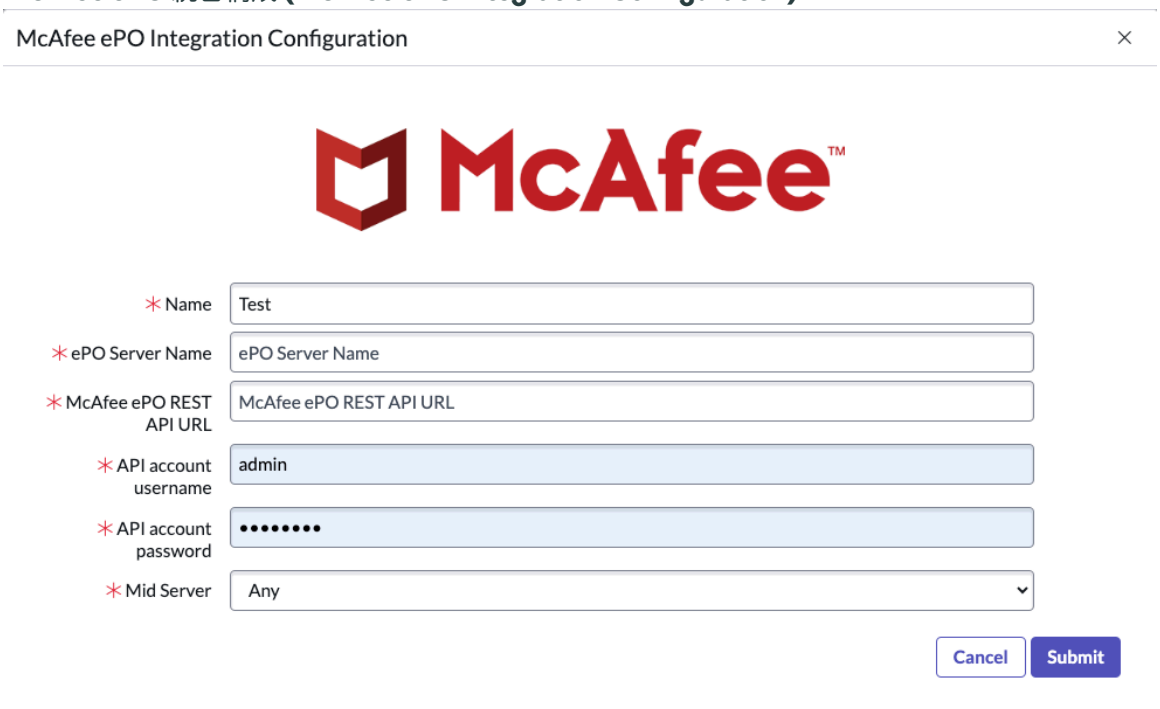
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	複数のサーバーに対するサポートが必要な場合は、各サーバーの名前を入力してこのプロセスを繰り返します。
McAfee ePO REST API URL	McAfee ePO REST API をホストするベース URL。https:// プロトコルを使用して URL を入力します (例：https://corp.epo_server:8443)。
API アカウントユーザー名	一意のアカウントユーザー名 (例：ServiceNow API)。
API アカウントパスワード	API アカウントの一意のパスワード。
MID サーバー	Now Platform インスタンスのセットアップ中に構成した MID サーバーの名前を選択します。 リストから特定の MID サーバーを選択するか、[任意] を選択して、リストからこの統合に対して有効な MID サーバーの自動選択を有効にすることができます。 **注:** ○ この構成で選択された MID サーバーは、この統合全体に適用されます。 ○ このリストには、アクティブで検証済みの MID サーバーのみが表示されます。デフォルト値は [任意] に設定されています。 サンプル名は、secops_local_midserver です。

自動翻訳

McAfee ePO 統合構成 (McAfee ePO Integration Configuration)



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. **[Submit]** をクリックします。
   新しい設定レコードを含む McAfee ePO 構成リストが表示されます。これで McAfee ePO サーバーの構成が完了しました。

   注:
   複数のサーバーに対するサポートが必要な場合は、この手順を繰り返します。

McAfee ePO 統合用の **Now Platform** のセキュリティタグの編集

統合のセットアップの一環として、Now Platform インスタンスの McAfee ePO コンソールで作成したセキュリティタグ名を編集します。Now Platform インスタンスのタグ名は、McAfee ePO コンソールのタグ名と一致するように編集します。

始める前に
必要なロール：Now Platform Security Incident Management者 (sn_si_admin)

このタスクについて
McAfee ePO コンソールでのマルウェアスキャンの開始およびホスト隔離のアクションのセキュリティタグ名は、Now Platform インスタンスでのこれらの機能のレコード内のセキュリティタグ名と一致する必要があります。

機能を実行する機能プロファイルを作成する前に、利用可能な McAfee ePO 機能のリストを表示し、McAfee ePO コンソールのセキュリティタグ名と一致するように Now Platform インスタンスのセキュリティタグを編集します。

McAfee ePO コンソールでのセキュリティタグ名の作成の詳細については、「McAfee ePO コンソールを セキュリティインシデントレスポンス (SIR) と統合するように設定する」を参照してください。

手順

1. 次のように移動する。 **All** (すべて) > **McAfee ePO** 統合 > デフォルト設定.
2. McAfee ePO 統合のセキュリティタグ名を編集するには、[デフォルト構成] をクリックします。

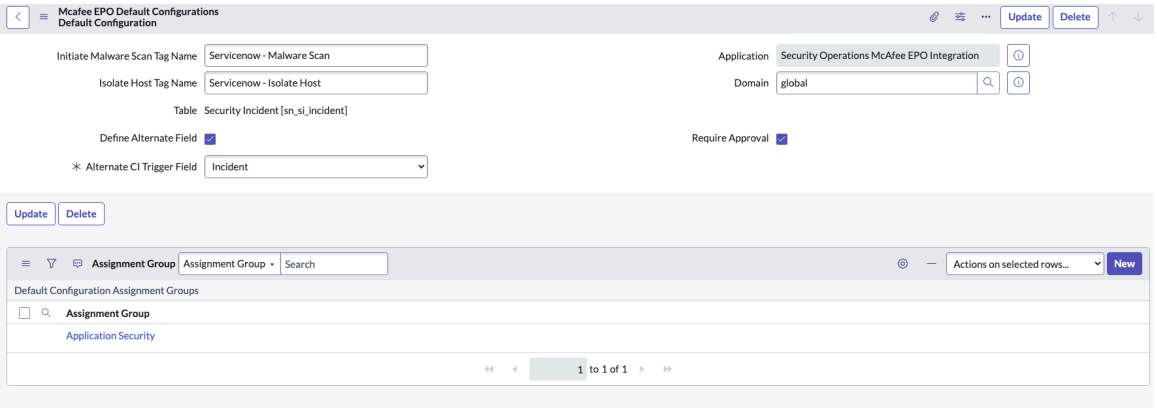
   注:
   McAfee ePO 統合をインストールした後で、この構成を必ず実行してください。

3. McAfee ePO コンソールでスキャンの開始アクション用に作成したセキュリティタグの名前を [マルウェアスキャン開始のタグ名 (Initiate Malware Scan Tag Name)] フィールドに入力します。
   たとえば「ServiceNow - Malware Scan」などです。
4. McAfee ePO コンソールでホスト隔離アクション用に作成したセキュリティタグの名前を [ホストタグ名を隔離 (Isolate Host Tag Name)] フィールドに入力します。
   たとえば「ServiceNow - Isolate Host」などです。
5. インシデントの作成時に CI トリガーフィールドを使用しない場合は、[代替フィールドを定義] チェックボックスをオンにします。
   このオプションを有効にすると、[代替 CI トリガー] フィールド選択リストが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティタグの編集



6. 選択リストから代替フィールドを選択して、CI 検索条件を確認します。
この例では、sn_si.admin ロールを持つユーザーは、インシデントの作成時にセキュリティインシデントで [CI] フィールドに値が入力されないと考えています。一方、FQDN、ホスト名、または IP アドレスの CI 情報がセキュリティインシデントの [識別された CI] フィールドに入力されると考えているため、[CI] フィールドの代わりに [識別された CI] フィールドを選択します。この例では [識別された CI] を選択しますが、セキュリティインシデントのフィールドであればどれでも代替 CI として使用できます。
7. [ドメイン] フィールドで、検索オプションを使用してこの構成のドメインまたはグループを選択します。
たとえば、 global です。
8. [ホストを隔離] および [隔離を削除] 機能を使用している場合は、[承認が必要] フィールドで [承認が必要] チェックボックスをオンにします。

   注:
   [マルウェアスキャンを開始 (Initiate Malware Scan)]、[脅威イベントのリスト表示 (List Threat Events)]、および [システムの詳細を取得] 機能には承認は必要ありません。

9. [更新] をクリックします。
EPO タグ名が更新され、[McAfee ePO デフォルト構成 (McAfee ePO Default Configurations)] リストに表示されます。Now Platform インスタンスでのマルウェアスキャンのアクションのセキュリティタグ名が、McAfee ePO コンソールでのスキャンに対する名前と一致しています。

   Now Platform インスタンスのマルウェアスキャンおよびホスト分離の機能の EPO タグ名を正常に編集しました。次のステップでは、機能のプロファイルを作成します。

関連情報

McAfee 製品ドキュメント

承認グループの作成

ホストマシンの隔離およびネットワークへの復元の要求を承認できる McAfee ePO for セキュリティオペレーション 統合の承認グループを作成します。

始める前に

インスタンスの承認グループを使用できる場合を除き、グループに承認権限を再アサインできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
McAfee ePO 統合のためのプロファイルの構成 の承認オプションは、[ホストを隔離] および [ホスト隔離削除] 機能に対してのみ表示されます。

必要なロール：Now Platform® Security Incident Management者 (sn_si_admin)

このタスクについて
ホストマシンを隔離および隔離を解除するためにセキュリティインシデントアナリストによって送信される承認要求は、デフォルトでは sn_si.admin ロールを持つユーザーにアサインされます。このロールを持つユーザーは、プロファイルの構成ステップでこの承認権限を再アサインできます。承認グループに権限を再アサインする前に、Now Platform インスタンスの [グループ] リストで承認グループが使用可能になっている必要があります。

手順

1. 次のように移動する。 **All** (すべて) > ユーザー管理 **(User Administration)** > グループ.
2. [グループ] リストで、[新規] をクリックします。
3. フォームのフィールドに入力します。

[承認グループ] フォーム

フィールド	説明
名前	承認要求が送信されたときに表示されるグループの名前 (例：McAfee ホスト隔離承認者 (Approvers McAfee host isolation))。
グループ メール	グループのメール配布リストまたは連絡先メールアドレス (グループマネージャーや McAfeeapproval@servicenow.com など)
マネージャー	グループマネージャーの名前。検索アイコンをクリックしてリストを表示します。
親	(オプション) このグループがメンバーである他のグループ (このグループに親がある場合)。
説明	このグループに関する補足情報。
含めるメンバー	このグループにメンバーを含めるオプション。
デフォルトの担当者	このグループのデフォルトのアサイニーとしてユーザーを選択するオプション。ユーザーのリストを開くには [検索] オプションを使用します。
ロール	このグループのロールを選択するオプション。ロールを追加および削除するには、[追加] オプションと [削除] オプションを使用します。
タイプ	このグループのカテゴリを選択するオプション。グループタイプのリストを開くには [検索] オプションを使用します。
ベンダー	このグループのベンダーを選択するオプション。ベンダーのリストを開くには [検索] オプションを使用します。

4. **[Submit]** をクリックします。
新しいグループが [グループ] リストに表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このプロファイルの構成で [承認が必要] オプションが有効になっている場合、このグループは要求を処理できます。

承認グループの各メンバーは、sn_si.analyst ロールを持つユーザーが送信した要求を監視および処理するには、Now Platform で [自分の承認] タブに移動します。

McAfee ePO 統合機能プロファイル

セキュリティインシデントアドミン (sn_si.admin) ロールを持つユーザーとして、Now Platform® インスタンスで McAfee ePO の機能のプロファイルを作成します。プロファイル内のクエリやアクションをグループ化して、新しいセキュリティインシデントが作成されたときに実行する McAfee ePO の機能を決定します。

機能プロファイル

プロファイル™ を作成すると、McAfee ePO の機能をグループ化し、Now Platform® インスタンスからその機能の設定を構成できます。その機能に対して複数のプロファイルを柔軟に作成できるため、セキュリティインシデントレスポンス (SIR) のインシデントが作成されたときにどのアクションやクエリを呼び出すかを決定できます。組織のニーズに合わせて、プロファイルを 1 つ作成し、そのプロファイルでシステムの詳細に対するクエリを実行したり、マルウェアスキャンを開始したり、ホストマシンを隔離したりすることができます。あるいは、複数のプロファイルを作成して、それぞれに 1 つの McAfee ePO 機能を持たせることなども可能です 。

プロファイルタイプと必要な **McAfee ePO** の機能

プロファイルの主な目的	設定の要件	このプロファイルタイプに必要な **McAfee ePO** の機能
システムの詳細を取得	なし	ホストの詳細を取得
ホストを隔離	McAfee ePO コンソールでホスト隔離アクションのセキュリティタグを作成したことを McAfee ePO アドミニストレーターに確認します。詳細については、「McAfee ePO コンソールを セキュリティインシデントレスポンス (SIR) と統合するように設定する」を参照してください。	ホストの隔離
ホスト上の脅威のスキャンと検索	McAfee ePO コンソールでマルウェアスキャン開始アクションのセキュリティタグを作成し	マルウェアスキャンを開始 **(Initiate Malware Scan)**

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロファイルタイプと必要な **McAfee ePO** の機能 (続く)

プロファイルの主な目的	設定の要件	このプロファイルタイプに必要な **McAfee ePO** の機能
	たことを McAfee ePO アドミニストレーターに確認します。詳細については、「McAfee ePO コンソールを セキュリティインシデントレスポンス (SIR) と統合するように設定する」を参照してください。	**注:** McAfee ePO のマルウェアスキャンの一環として、[脅威イベントのリスト表示 (List Threat Events)] 機能が自動的に呼び出されます。ただし、マルウェアスキャン機能を備えたプロファイルに [脅威イベントのリスト表示 (List Threat Events)] 機能を追加する必要はありません。マルウェアスキャンの結果は、セキュリティインシデントの [脅威イベントの詳細] タブに表示されます。
ホストの隔離を削除	McAfee ePO コンソールでホスト隔離アクションのセキュリティタグを作成したことを McAfee ePO アドミニストレーターに確認します。詳細については、「McAfee ePO コンソールを セキュリティインシデントレスポンス (SIR) と統合するように設定する」を参照してください。	隔離を削除
脅威に関する拡張データを収集します。	なし	脅威イベントのリスト表示 **(List Threat Events)**

McAfee ePO 統合の機能プロファイルの作成

プロファイルを作成し、そのプロファイルで実行する McAfee ePO 機能を選択します。

始める前に

必要なロール：Now Platform® Security Incident Management者 (sn_si_admin)

このタスクについて

構成のこのステップでは、McAfee ePO の機能のプロファイルを作成します。プロファイルを作成するときは、プロファイルの意図についてよく考えてから McAfee ePO の機能を追加してください。プロファイルを作成するときは、次の表を参照してください。

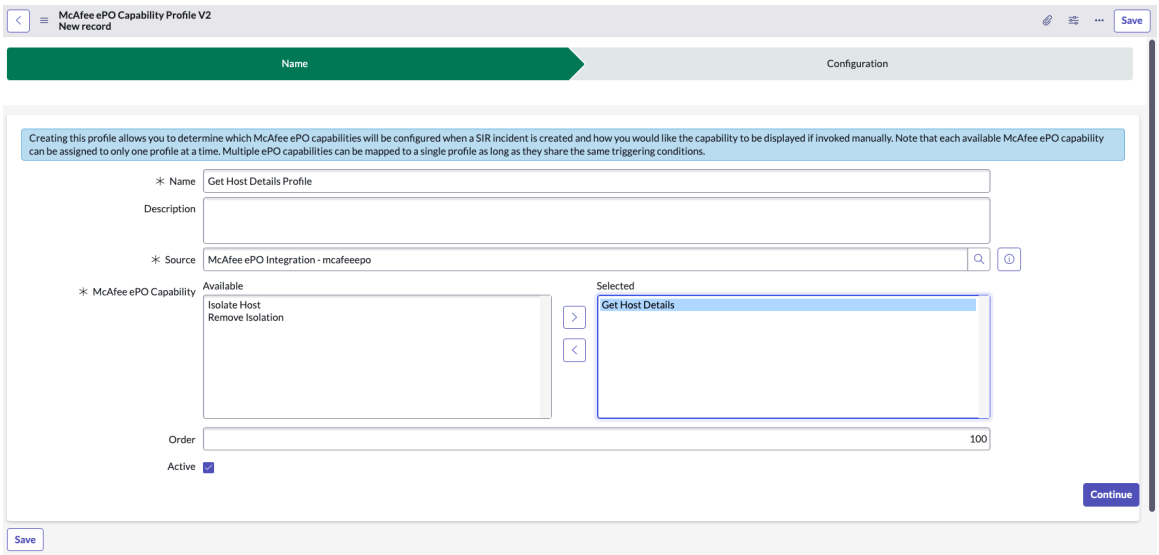
次の表は、プロファイルで特定のクエリまたはアクションを実行する場合にプロファイルに追加する必要がある機能を示しています。プロファイルを 1 つ作成し、そのプロファイルでホストの詳細に対するクエリを実行したり、マルウェアスキャンを開始したり、隔離を解除したり、ホストマシンを隔離したり、複数のプロファイルを作成してそれぞれに 1 つの機能を持たせたりすることが可能です 。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **McAfee ePO** 統合 > **McAfee ePO** 機能プロファイル.
   McAfee ePO の機能プロファイルのリストが表示されます。
2. [新規] をクリックします。
3. フォームの各フィールドに入力します。



4. プロファイルを保存して検証するには、[続行] をクリックします。
   検証が正常に行われると、ページが再ロードされ、[構成] フォームが表示されます。

次のタスク
次のステップは、プロファイルを設定することです。プロファイルの設定を構成する前に、プロファイルとトリガー条件の構成の概念を確認することをお勧めします。詳細については、「McAfee ePO コンソールを セキュリティインシデントレスポンス (SIR) と統合するように設定する」と「McAfee ePO のプロファイルの構成アイテム (CI) フィールドを使用したトリガー条件の定義」を参照してください。

McAfee ePO のプロファイルの構成アイテム **(CI)** フィールドを使用したトリガー条件の定義

プロファイルを作成し、そのプロファイルで実行する McAfee ePO 機能を選択したら、一連の特定の条件が満たされた場合にのみ実行されるようにプロファイルの設定を構成します。

これらのトリガー条件は柔軟に設定できるため、Now Platform® セキュリティインシデントレスポンス セキュリティインシデントで一致するデフォルトのフィールド値に基づいて、プロファイルが自動的に実行されます。または、セキュリティインシデントで特定したフィールド値の一致を検索するようにプロファイルを設定することもできます。

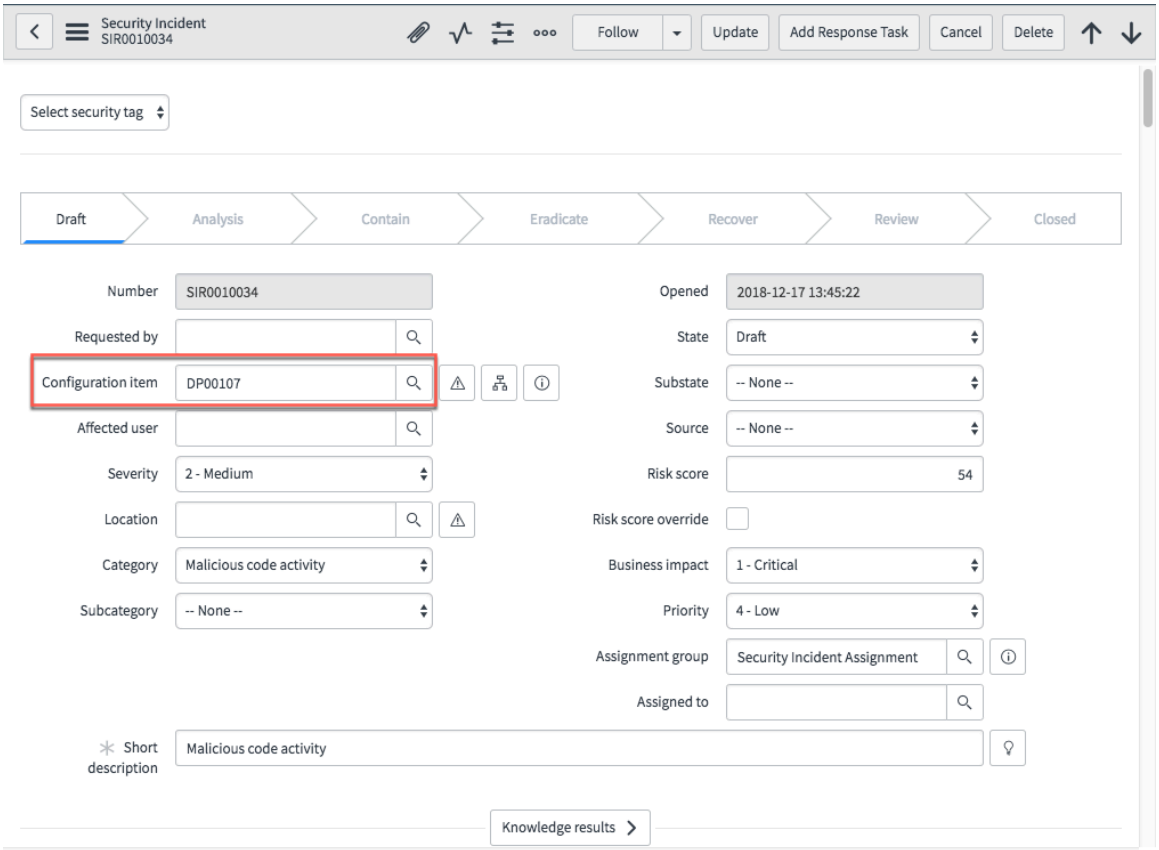
Now Platform® セキュリティインシデントレスポンス (SIR) セキュリティインシデントの [構成アイテム (CI)] フィールドは、統合の機能とプロファイルの動作の重要な要素の 1 つです。このフィールドの値は、セキュリティインシデントの原則値です。この値は、資産の ID を Now Platform® データベースに格納されている情報と照合するために使用されます。セキュリティイベントによって SIR セキュリティインシデントが作成され、プロファイルがアクティブ化されると、この [構成アイテム] フィールドの値に基づいて、完全修飾ドメイン名 (FQDN)、ホスト名、または IP アドレスの一致する値に対して、資産がスキャンされます。

理想的なケースでは、一致する値がデータベース内で見つかり、一致する資産のデータを McAfee ePO コンソールから収集し、Now Platform® インスタンスにプルして、セキュリティインシデントの関連リストに表示できます。次の図は、SIR セキュリティインシデントのホスト名が入力された [構成アイテム] フィールドの例を示しています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[セキュリティインシデント] の [構成アイテム]



セキュリティインシデントの [構成アイテム (CI)] フィールドに値が入力されていない場合、またはデータベースと一致する FQDN、ホスト名、または IP アドレスに対する一致が見つからない場合は、セキュリティインシデントの代替フィールドを選択して、資産のスキャン中に見つかった一致する CI 拡張データを表示できます。

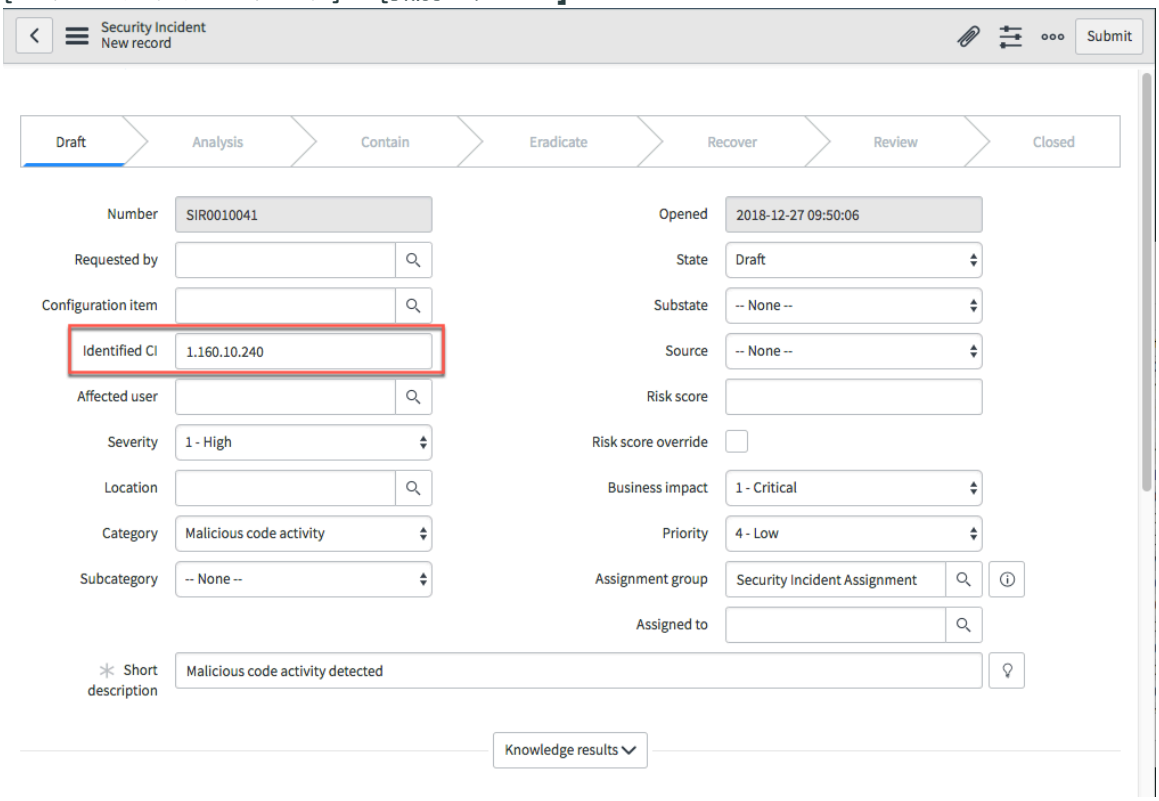
プロファイルセットアップの構成手順では、エンドポイント識別用の代替 CI トリガーフィールドを選択して、McAfee ePO ルックアップからの CI 拡張データを関連するセキュリティインシデントに入力することができます。作成したカスタムフィールドを含む、セキュリティインシデントの任意のフィールドを代替 CI トリガーフィールドとして選択できます。この代替 CI フィールドをバックアップとして選択することで、インシデントの作成時に、関連するセキュリティインシデントに CI フィールドが設定されていない場合でもプロファイルが実行されるようにします。

例として、Security Operations Center (SOC) のアナリストとして、セキュリティインシデントのカスタムフィールド「自分のセキュリティインシデントの IP アドレス (IP Address on my security incident)」を作成します。インシデントの作成時にこのカスタムフィールドの値がセキュリティインシデントの [構成アイテム] フィールドに表示されないと思われる場合は、この IP アドレスをスキャンするようにプロファイルを設定できます。一致すると、選択したフィールドのセキュリティインシデントに IP アドレスが表示されます。次の図では、この例の IP アドレスの代替フィールドとして [識別された CI] フィールドが選択されています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[セキュリティインシデント] の [識別された **CI**]

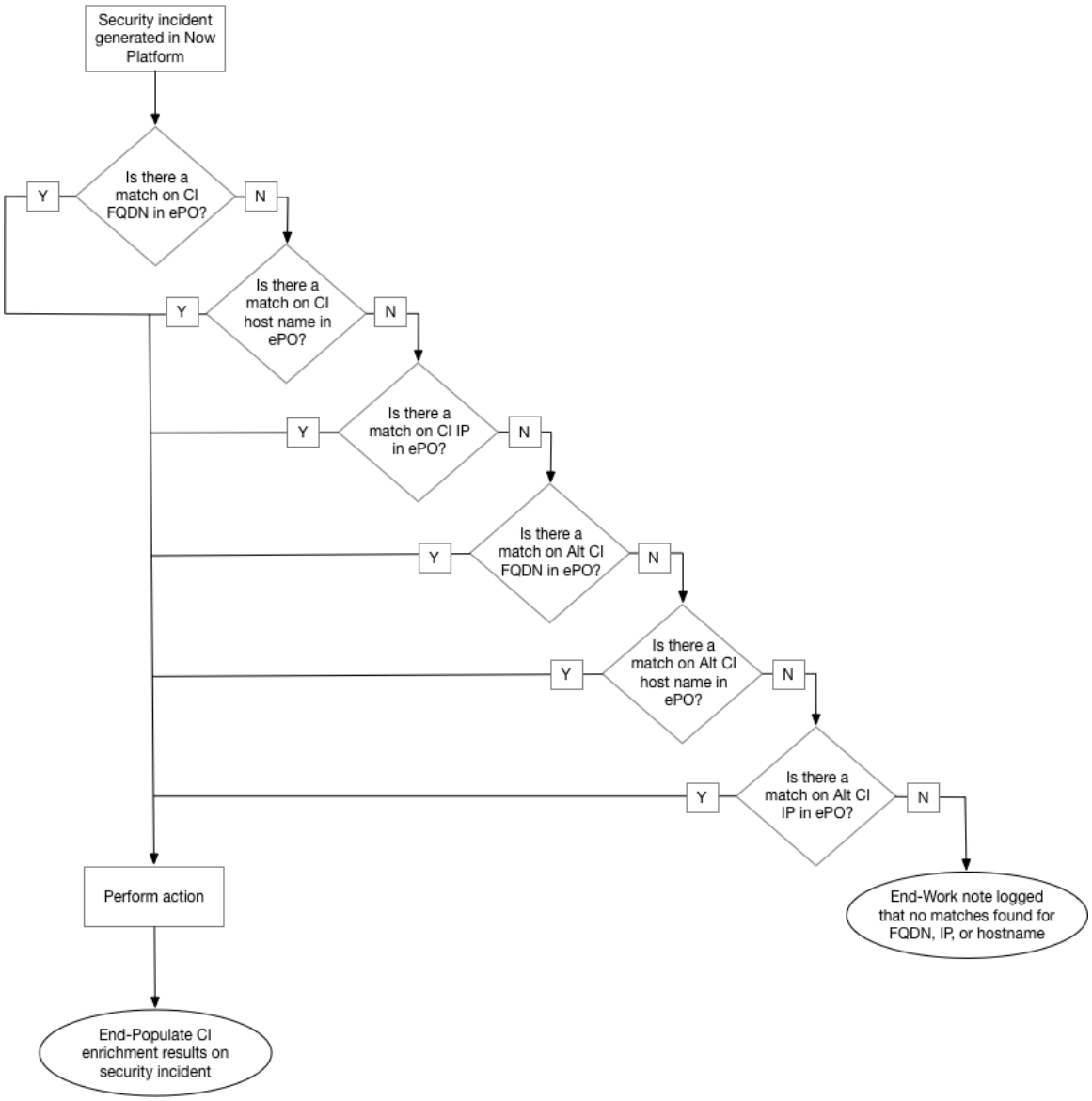


次の図は、ワークフローの最初の検索で構成アイテムへの一致をスキャンする方法を示しています。代替 CI トリガーフィールドが有効になっている場合、2 番目の検索で代替値の一致がスキャンされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

構成アイテムのワークフロー



CI フィールドまたは代替 CI フィールドに対して一致する ID が見つからない場合は、作業メモがログに記録され、セキュリティインシデントにメッセージが表示されます。一致するものが見つからない場合、イベントに関連するセキュリティインシデントに拡張データは入力されません。

代替 CI トリガーフィールドを有効にし、プロファイルの構成手順中に一致する ID を表示するフィールドを選択します。代替 CI フィールドを有効にするこの手順については、他のプロファイル構成要件とともに McAfee ePO 統合のためのプロファイルの構成で説明されています。

McAfee ePO 統合のためのプロファイルの構成

プロファイルを作成し、そのプロファイルで実行する McAfee ePO 機能を選択したら、自分が定義した特定の条件でのみプロファイルが呼び出されるように設定を構成します。

プロファイルの設定

このステップでは、指定した条件が満たされた場合にのみ実行されるように機能プロファイルを構成します。そのプロファイルに対して自分が選択した McAfee ePO 機能を自動的にトリガーするセキュリティインシデントの条件を定義します。[構成アイテム (CI)] フィールドに対して代替フィールドを選択し、トリガーイベントに関連するセキュリティインシデントのみが自動的にプロファイルを起動するようにフィルタリング条件を設定することもできます。この構成手順では、プロファイルに対して次のように構成フォームを設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

代替構成アイテム (CI) トリガーフィールド

Now Platform® セキュリティインシデントレスポンス (SIR) セキュリティインシデントの [構成アイテム (CI)] フィールドに値が入力されていない場合、またはデータベース内に一致が見つからない場合は、セキュリティインシデントの代替フィールドを選択して、資産のスキャン中に見つかった一致する CI 拡張データを表示できます。セキュリティインシデントの [構成アイテム] および [代替構成アイテム] フィールドの詳細については、「McAfee ePO のプロファイルの構成アイテム (CI) フィールドを使用したトリガー条件の定義」を参照してください。

セキュリティタグ

隔離されたホストマシンのステータスを追跡し、マルウェアスキャンがいつ開始されたかを追跡するには、オプションのタグ付け機能を利用します。デフォルトでは、プロファイルの構成フォームではこのオプションが無効になっています。構成手順の過程でこのオプションを有効にすると、セキュリティタグ名が構成フォームに表示されます。表示される名前は、関連するセキュリティインシデントに表示されるタグの名前です。これらのタグにより、ホスト隔離アクションが正常に開始されたときと承認されたときに通知が行われます。ホストが正常にネットワークに戻ると、セキュリティインシデントからセキュリティタグが自動的に削除されます。マルウェアスキャンの場合、スキャンのスケジュールが設定されると、関連するセキュリティインシデントにタグが表示されます。スキャンが終了すると、スケジュール設定済みのタグが、スキャンが正常に完了したことを示すタグに自動的に置き換わります。

インシデントに基づく自動トリガー

[インシデントに基づく自動トリガー] オプションが有効になっている場合は、フィルター条件ビルダーが利用可能であるため、プロファイルを自動的に実行するタイミングを指定するフィルター条件を設定する必要があります。一般的なフィルターは、[カテゴリ] が [悪意のあるコードアクティビティ] で [ビジネスインパクト] が [1-重大] です。この 2 つのフィルターを使用すると、悪意のあるコードに関連していてビジネスに重大な影響を与えるセキュリティインシデントのみがプロファイルを起動します。自動トリガーオプションを使用すると、プロファイルを自動的に呼び出すセキュリティインシデントの数を減らすことができます。

承認

ホストマシンの隔離やマルウェアスキャンの開始といったアクションをより細かく制御する必要がある場合は、プロファイルの構成時に [承認が必要] オプションを有効にします。

たとえば、あるプロファイルに対して承認機能とタグ付け機能の両方が有効になっている場合、ホストマシンを隔離する要求やネットワークに戻す要求が承認のために送信されると、関連するセキュリティインシデントが自動的にタグ付けされ、アクションが開始されます。デフォルトでは、要求は sn_si.admin ロールを持つユーザーに承認のために送信されますが、組織のニーズに合わせてこの承認作業を別の個人や承認グループに再アサインすることができます。承認者は、Now Platform® インスタンスの [自分の承認] で要求を処理します。セキュリティタグは関連するセキュリティインシデントに表示されます。すべてのワークフローアクティビティは、作業メモにも監査記録の作成のため記録されます。

McAfee ePO コンソールの ServiceNow 監査ログ

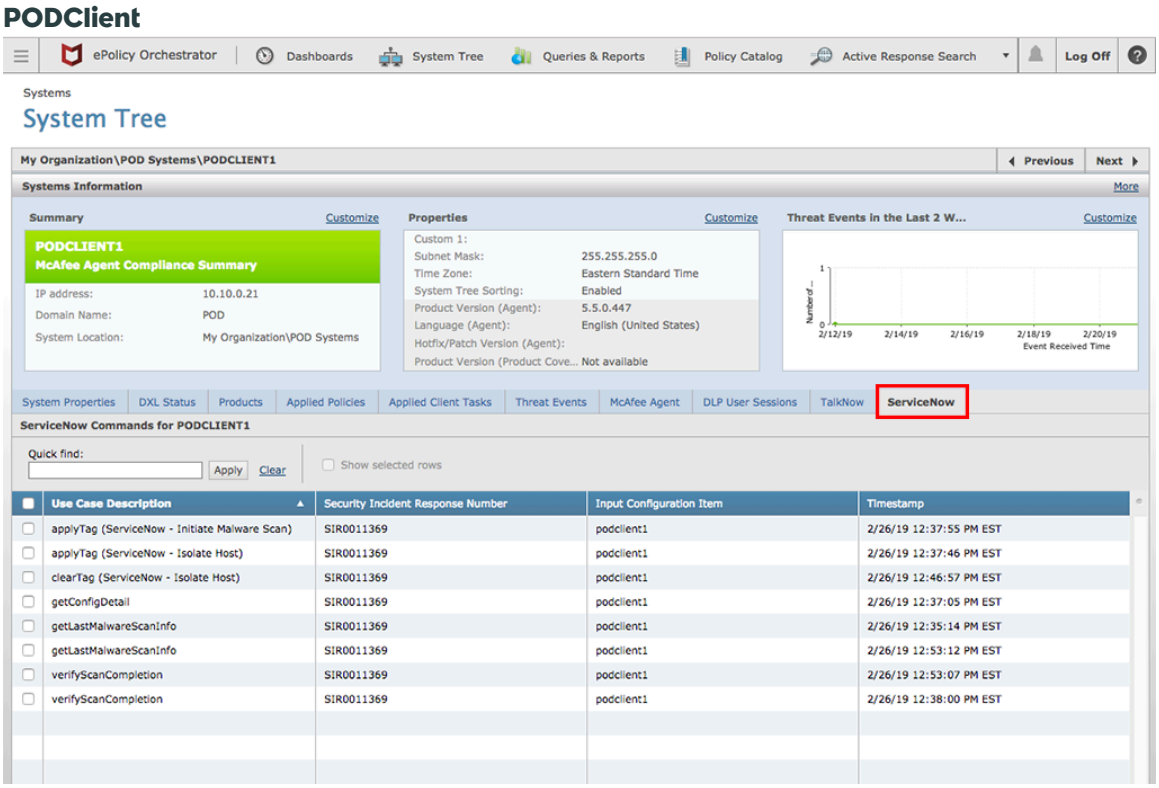
McAfee ePOのバージョン 5.10.0 では、ServiceNow タブが表示され、Now Platform® インスタンスから開始されたコマンドのログがそこに示されます。McAfee ePO コンソールのホストマシン (エンドポイント) で Now Platform® インスタンスのプロファイルからアクションまたはクエリが呼び出されると、McAfee ePO コンソールに ServiceNow コマンドの監査ログが作成されます。このログは McAfee ePO コンソールの [システムツリー] に表示され、特定のエンドポイントに送信されたコマンドの時間を監査するために役立ちます。特定のマシンでログに記録された ServiceNow イベントを McAfee ePO コンソールで表示するには、次の手順を実行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

1. McAfee ePO コンソールの [システムツリー] に移動し、ServiceNow タブを探します。
2. タブをクリックすると、ホストマシンのリストが開きます。
3. [名前] 列で、ホスト名をクリックして監査ログを開きます。

次の画像は、ホスト (PODCLIENT1) のログの例を示しています。



Now Platform® インスタンスのプロファイルから開始されたイベントが記録され、ログに表示されます。ホストマシンのステータスを調べて、ログに一覧表示されるイベントがホスト上で正常に完了したことを確認します。

プロファイルの例

次のトピックでは、プロファイルを構成してセキュリティインシデントをテストする方法の例を説明します。これらの例では、この統合で利用可能なすべての McAfee ePO 機能のプロファイルを使用します。

McAfee ePO 統合のシステム拡張クエリに対するプロファイルとセキュリティインシデントの構成

設定した条件でのみプロファイルがトリガーされるように、プロファイル設定を構成します。

始める前に
必要なロール：Now Platform® セキュリティインシデントアドミン (sn_si_admin)

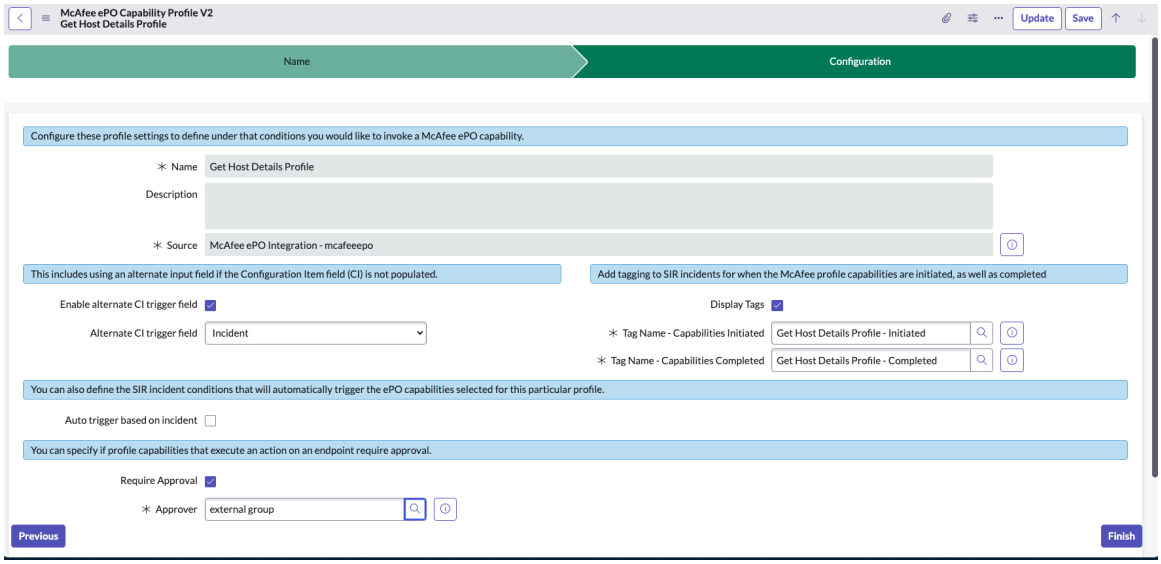
このタスクについて
プロファイルに対して選択した McAfee ePO 機能を自動的にトリガーする条件を定義します。[構成アイテム] (CI) フィールドの代替入力フィールドを選択することもできます。この代替フィールドでは、トリガーイベントに関連するセキュリティインシデントのみが自動的にプロファイルをトリガーするように、フィルタリング条件を設定できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. [構成] ページが表示されない場合は、進捗状況バーで [構成] をクリックします。
2. フォームの各フィールドに入力します。



3. 代替 CI フィールドオプションを有効にし、このプロファイルを自動的に呼び出すフィルター条件を設定するには、次の手順を実行します。

   a. [代替 **CI** トリガーフィールドを有効にする] チェックボックスをオンにします。
   代替 CI トリガーフィールドが表示されます。この例では、sn_si.admin ロールを持つユーザーは、インシデントの作成時にセキュリティインシデントで [CI] フィールドに値が入力されないと考えています。一方、FQDN、ホスト名、または IP アドレスの CI 情報がセキュリティインシデントの [識別された CI] フィールドに入力されると考えているため、[CI] フィールドの代わりに [識別された CI] フィールドを選択します。この例では [識別された CI] を選択しますが、セキュリティインシデントのフィールドであればどれでも代替 CI として使用できます。

   b. 表示される [代替 **CI** トリガーフィールド] 選択リストから、[識別された **CI]** フィールドを選択します。

   カスタムフィールドを含む、セキュリティインシデントで利用可能なすべてのフィールドが、リストに表示されます。[代替 CI トリガーフィールド] に、[識別された CI] が表示されます。

   このプロファイルが呼び出され、イベントの最初のトリガー時に関連するセキュリティインシデントで [CI] フィールドが入力されていない場合、プロファイルは代わりに [識別された CI] フィールドの値を検索で使用します。

   c. [インシデントに基づく自動トリガー] チェックボックスをオンにします。
   フィルター条件ビルダーが表示されます。このオプションでは、フィルター条件を設定し、セキュリティインシデントの作成時にプロファイルが自動的に呼び出されるタイミングを指定します。

   d. この特定のプロファイルに対して ePO 機能を自動的にトリガーする SIR インシデント条件を定義します。

   e. エンドポイントでアクションを実行するプロファイル機能に承認が必要な場合は、[承認が必要] チェックボックスをオンにします。

   f. 検索アイコンを使用して承認を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [完了] をクリックします。
   インシデントの作成時にプロファイルが自動的にトリガーされ、一致する CI 結果の入力の際に代替フィールドが使用されるように、プロファイルが正しく構成されました。

セキュリティインシデントからの **McAfee ePO** プロファイルの手動トリガー

Now Platform セキュリティインシデントレスポンス (SIR) セキュリティインシデントから機能プロファイルを手動でトリガーします。

始める前に
必要なロール：sn_si.admin

> **注:**
> McAfee ePO 統合のためのプロファイルの構成 の承認オプションは、[ホストを隔離] および [ホスト隔離削除] 機能に対してのみ表示されます。

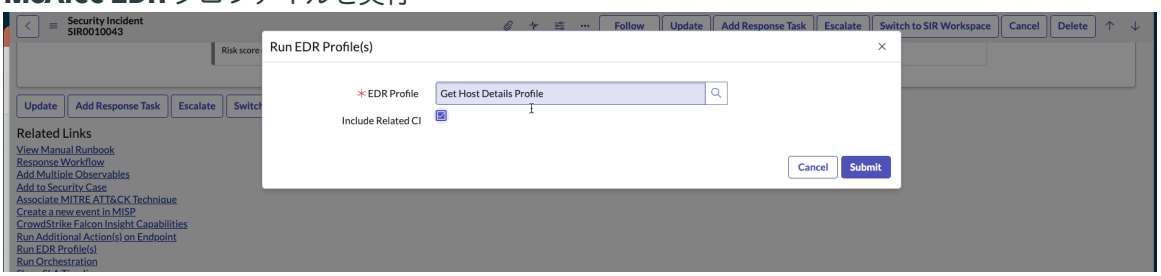
このタスクについて
プロファイルで指定したトリガー条件がセキュリティインシデントの条件と一致していれば、マシンの [ホストの詳細を取得]、[ホストマシンの隔離 (Isolate Host machine)]、または [隔離を解除 (Remove Isolation)] の要求を自動的に呼び出すことができます。逆に、要求を手動で送信するには、セキュリティインシデントから直接要求を送信します。

構成されたトリガー条件に基づいてプロファイルをアクティブ化すると、Now Platform セキュリティインシデントのクエリ結果を表示できます。McAfee ePO 統合により、プロファイルを使用せずに構成アイテム (CI) に対して個々の機能を実行することもできます。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. McAfee ePO 情報で確認するセキュリティインシデントを選択します。
3. 関連リストのセクションで、**[EDR** プロファイルを実行] をクリックします。

McAfee EDR プロファイルを実行

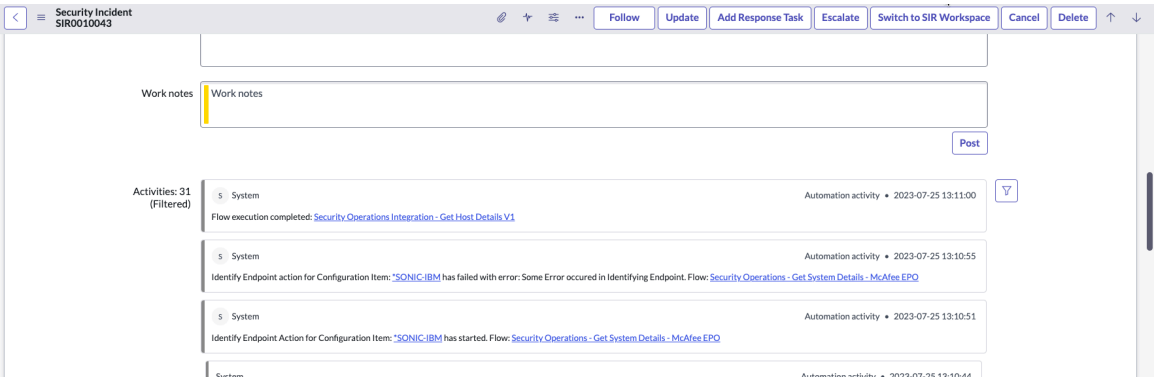


4. 利用可能なプロファイルのリストを参照してプロファイルを選択します。
   利用可能なプロファイルのリストは、[ホストの詳細を取得]、[ホストマシンの隔離]、および [隔離の削除] です。たとえば、[ホストの詳細を取得] を選択します。
5. プロファイルのすべての関連 CI に対してこのプロファイルを実行するには、[関連 **CI** を含める **(Include Related CI)]** を選択します。
   たとえば、セキュリティインシデントに 5 つの CI が関連付けられている場合、選択したプロファイルは 5 つの CI すべてに対して実行されます。
6. **[Submit]** をクリックします。
   選択したプロファイルは手動でトリガーされます。[作業メモとアクティビティ] セクションを表示し、[作業メモ] セクションのプロファイル開始済みタグとプロファイル完了済みタグを確認できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

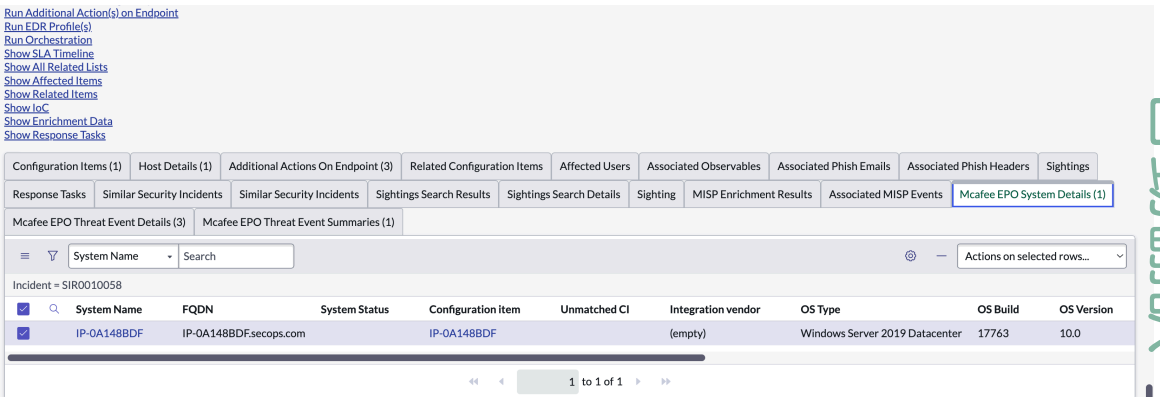
自動化アクティビティの作業メモ



結果は、[ホストの詳細を取得]、[ホストマシンの隔離 (Isolate Host machine)]、[隔離を削除 (Remove Isolation)] などの関連リストの形式で表示されます。

注:
すべての関連リストテーブルはベーステーブルを拡張したものです。この例では、「McAfee ePO システムの詳細 (McAfee EPO System Details)」は、「ホストの詳細」ベーステーブルの拡張テーブルです。

McAfee 関連リスト



7. 構成アイテム (CI) に対して個々の機能を実行するには、次の手順を実行します。

a. [構成アイテム] 関連リストで、必要な CI を選択します。

b. [選択した行のアクション...] ドロップダウンリストをクリックし、選択した CI に対して実行する必要な機能を選択します。
たとえば [ホストを隔離] などです。

c. [ホストを隔離] をクリックして、選択した CI に対して実行します。
選択した CI がネットワークから隔離されます。

McAfee ePO 統合での他のアクションのトリガー

[脅威イベントのリスト表示 (List Threat Events)] および [マルウェアスキャンを開始 (Initiate Malware Scan)] 機能は、[他のアクションを実行] からトリガーできます。

始める前に
必要なロール：sn_si.admin

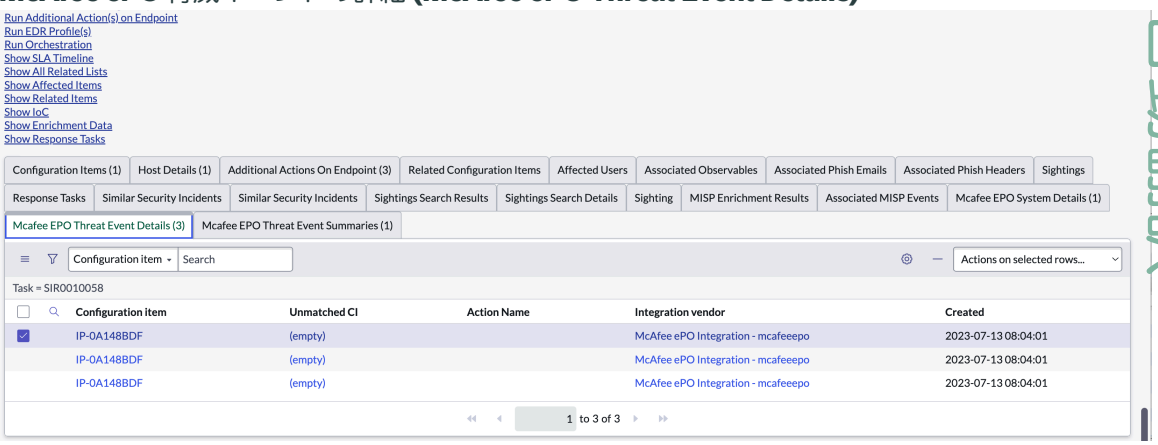
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
[エンドポイントで他のアクションを実行 **(Run Additional Actions on Endpoint)]** を使用して、McAfee ePO 統合で他のアクションを構成してトリガーできます。このアクションには、[McAfee ePO 脅威イベントのリスト表示 (McAfee ePO List Threat Events)] および [McAfee ePO マルウェアスキャンを開始 (McAfee ePO Initiate Malware Scan)] 機能が含まれます。

手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. 他のアクションを実行するセキュリティインシデントを選択します。
3. [関連リンク] セクションで、[エンドポイントで他のアクションを実行 **(Run Additional Action(s) on Endpoint)]** をクリックします。
4. 他のアクションのリストを参照して、トリガーする機能実装を選択します。
   たとえば、[McAfee ePO 脅威イベントのリスト表示 (McAfee ePO List Threat Events)] などです。
5. プロファイルのすべての関連 CI に対してこの他のアクションを実行するには、[関連 **CI** を含める **(Include Related CI)]** を選択します。
   たとえば、セキュリティインシデントに 5 つの CI が関連付けられている場合、選択したプロファイルは 5 つの CI すべてに対して実行されます。
6. [他のアクションを実行] をクリックします。

McAfee ePO 脅威イベントの詳細 (McAfee ePO Threat Event Details)



注:
すべての関連リストテーブルはベーステーブルを拡張したものです。この例では、「McAfee ePO 脅威イベントの詳細 (McAfee ePO Threat Event Details)」テーブルは、「エンドポイントでの追加アクション」ベーステーブルの拡張テーブルです。

7. 関連リストで [McAfee ePO 脅威イベントの詳細 (McAfee ePO Threat Event Details)] を表示して検証します。

アナリストワークスペースでの **McAfee ePO** 統合の使用

McAfee ePO 統合を使用して、SIR アナリストワークスペースで McAfee ePO 機能を活用します。

始める前に
必要なロール：sn_si.admin

セキュリティインシデントレスポンスワークスペースで McAfee ePO 統合を使用する前に、ServiceNow Store からこの統合をダウンロードして構成する必要があります。詳細については、「McAfee ePO 統合での Now Platform インスタンスの設定」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

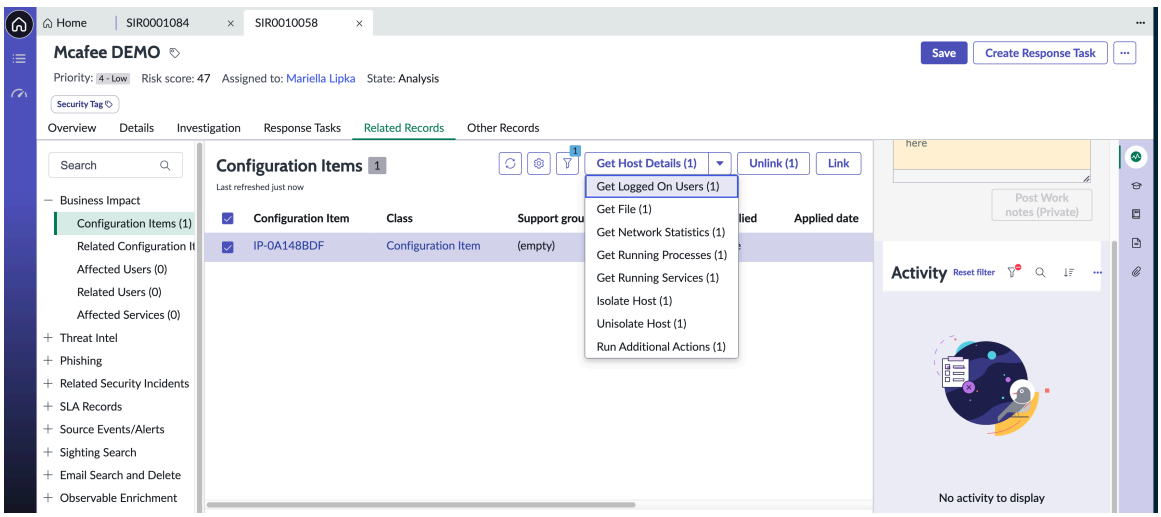
このタスクについて
McAfee ePO 統合を使用すると、セキュリティインシデントレスポンス ワークスペースを使用して、エンドポイントに対してリアルタイムで修復アクションを実行し、プロファイルを使用してホストに関する詳細情報を収集し、エンドポイントに対して特定のクエリまたはアクションを実行できます。

McAfee ePO 統合により、アナリストは セキュリティインシデントレスポンス アナリストワークスペースで次の McAfee ePO 機能を使用できます。

- ホストの詳細を取得
- ホストの隔離
- 隔離を削除
- エンドポイントで他のアクションを実行

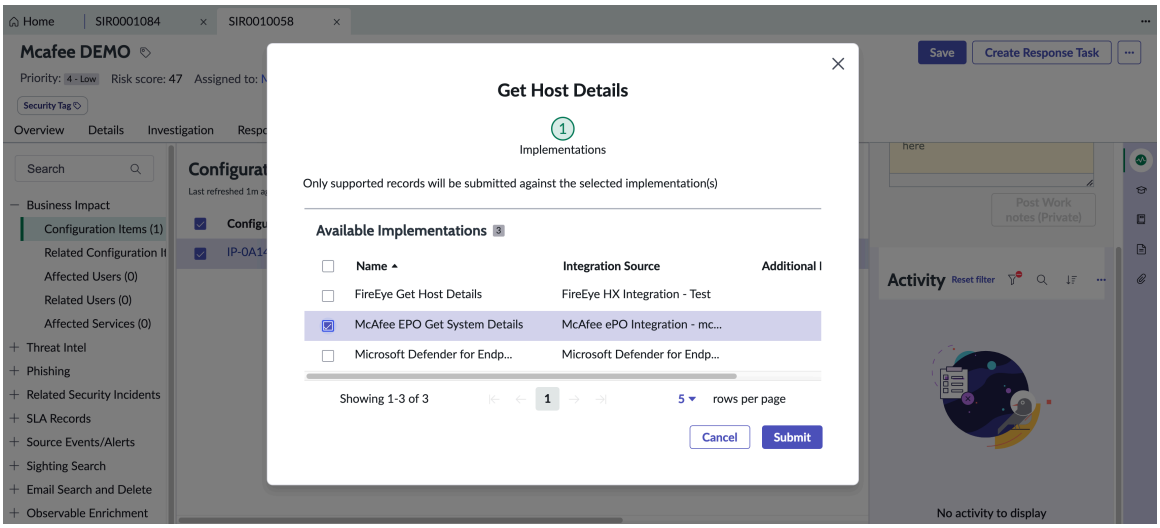
手順

1. SIR ワークスペースでセキュリティインシデントを開くには、セキュリティインシデントで **[SIR ワークスペースに切り替え (Switch to SIR Workspace)]** をクリックします。
2. SIR ワークスペースで [関連レコード] タブを選択します。
3. 任意の構成アイテムを選択し、関連リストのドロップダウンアクションからトリガーする McAfee ePO 機能を選択します。
   たとえば、[ホストの詳細を取得] などです。

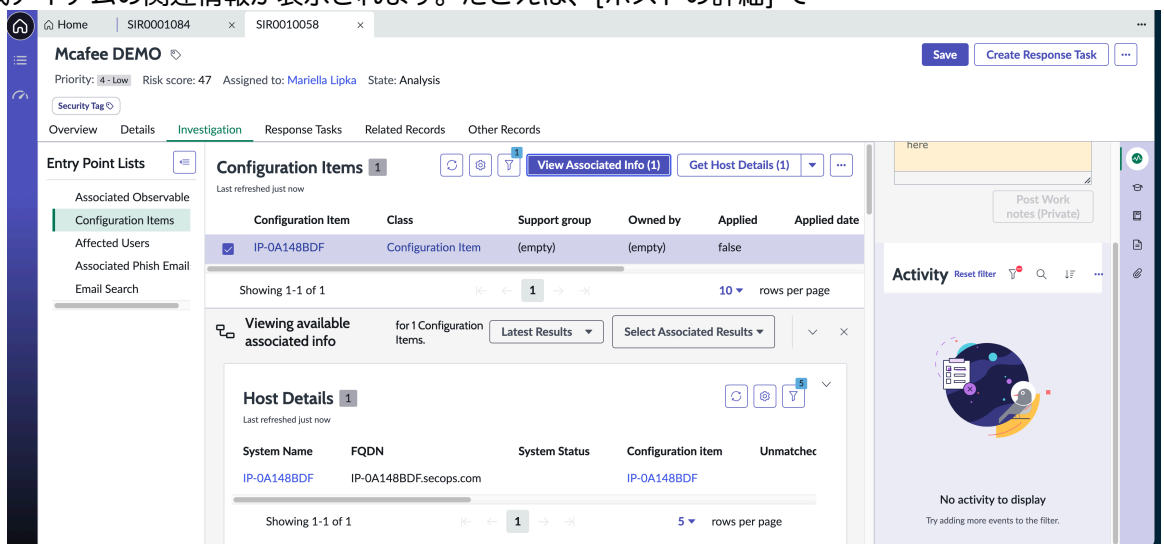


4. [ホストの詳細を取得] ポップアップで、**McAfee ePO** 実装を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. **[Submit]** をクリックします。
   [ホストの詳細を取得] 機能が CI に対して呼び出されます。作業メモで結果と検出結果を確認できます。
6. トリガーされた機能のデータを表示するには、[調査] タブを選択します。
7. [構成アイテム] を選択し、[関連情報を表示] アクションをクリックします。
   構成アイテムの関連情報が表示されます。たとえば、[ホストの詳細] で



す。

8. [構成アイテム] をクリックして、ホストの詳細を表示します。
   同様に、SIR アナリストワークスペースでセキュリティインシデントに他の McAfee ePO 機能を使用してみることができます。
9. 分析には、**[Endpoint Detection and Response (EDR)]** 関連リストの McAfee ePO 機能を使用できます。
10. 利用可能なプロファイルのリストを参照してプロファイルを選択します。
    利用可能なプロファイルのリストは、[ホストの詳細を取得]、[ホストマシンの隔離]、および [隔離の削除] です。たとえば、[ホストの詳細を取得] を選択します。
11. **McAfee ePO** 実装を選択し、[送信] をクリックします。

McAfee ESM - メールパーサー統合

ESM - メールパーサー統合は、セキュリティインシデントを作成するために ESM からのメール通知を消費するメールパーサーを使用してサポートされています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

McAfee ESM - メールパーサー統合の構成

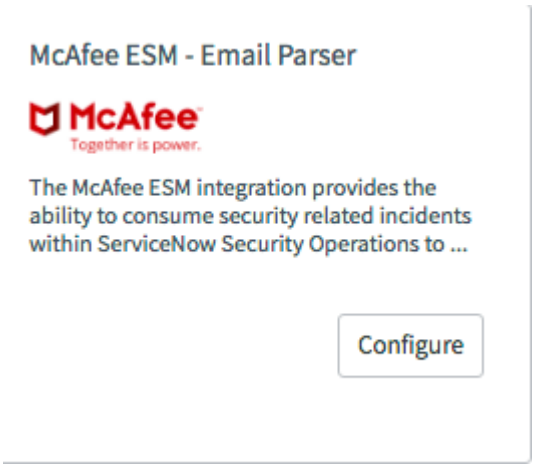
McAfee ESM - メールパーサー統合では、ESM からのメール通知を使用して拡張および応答ワークフローを推進します。

始める前に
必要なロール：sn_si_admin

このタスクについて
統合に使用する McAfee ESM メールパーサーテンプレートが提供されています。統合が行われる前に、構成してアクティブ化する必要があります。パーサーを更新すると有効になります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > 統合 > 統合設定.
   利用可能なセキュリティ統合が一連のカードとして表示されます。



2. McAfee ESM - メールパーサーカードで、[構成] をクリックします。
3. **[McAfee ESM -** メールパーサー構成 **(McAfee ESM - Email Parser Configuration)]** ダイアログボックスで、[メールパーサーの設定] リンクをクリックします。
4. **[McAfee ESM]** リンクをクリックして、提供されたテンプレートメールパーサーの設定を編集します。
   少なくとも、[メールの送信元] フィールドに入力します。独自のメールパーサーを作成するには、「Security Operations でのメールパーサーの作成」を参照してください。
5. [アクティブ] ボックスをオンにします。
6. [メールパーサー] フォームで [更新] をクリックします。
   メールパーサーは有効です。[統合構成] に戻る必要はありません。

McAfee ESM - インシデント拡張統合

McAfee ESM - インシデント拡張統合はログを検索し、関連するサイティング情報をセキュリティインシデントに追加します。

探索　　セットアップ

セキュリティインシデントレスポンス の統合

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

- McAfee ESM の開始 - インシデント拡張統合
- サイティング検索設定レコードの作成

使用	開発
• サイティング検索の実行 • Security Operations Integration - サイティング検索フロー • Security Operations - McAfee ESM サイティング検索フロー • サイティング検索の詳細の表示 • サイティング検索結果の表示	• ServiceNow セキュリティオペレーション 統合開発のガイドライン • 統合を作成するためのヒント • 開発者トレーニング • 開発者ドキュメント

トラブルシューティングとヘルプ

- 統合のトラブルシューティング
- Security Operations Community で質問や回答をする
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

自動翻訳

McAfee ESM の開始 - インシデント拡張統合

McAfee ESM は、ウイルス、スパイウェア、トロイの木馬などのマルウェアの脅威からエンドポイントを保護し、セキュリティオペレーション と簡単に統合できます。McAfee ESM - インシデント拡張統合を使用する前に、ServiceNow Store から統合をダウンロードし、適切な API Base URL とログイン認証情報を追加する必要があります。

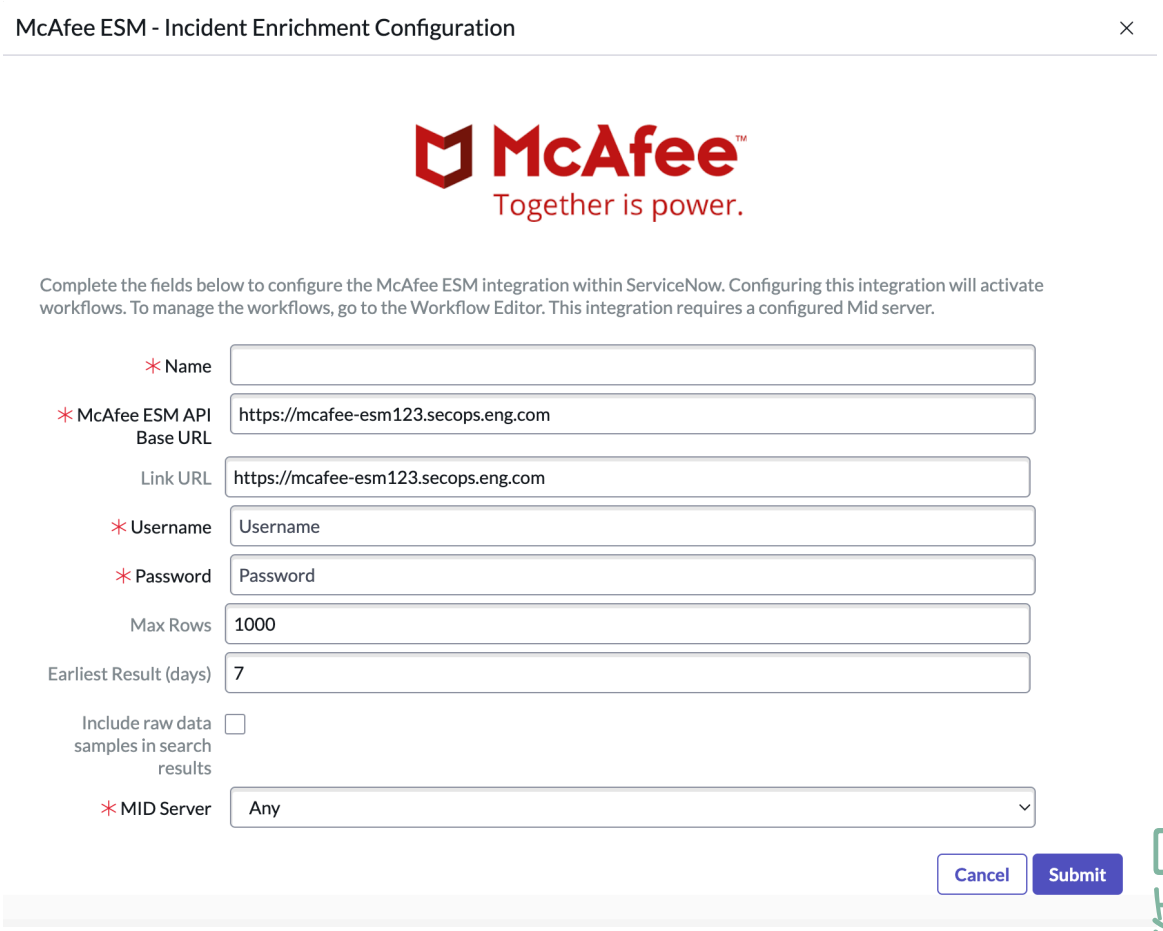
始める前に

必要なロール：sn_si_admin

手順

1. から統合をダウンロードします ServiceNow Store.
2. インストールが完了したら、次に移動します: セキュリティオペレーション > 統合 > 統合設定.
   利用可能なセキュリティ統合が一連のカードとして表示されます。
3. McAfee ESM - インシデント拡張カードで、[新規] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. 必要に応じて、フィールドに入力します。

フィールド	説明
名前	この構成の名前。
McAfee ESM API のベース URL	McAfee ESM サイトから取得したベース URL。
リンク URL	[オプション] McAfee ESM インスタンスに接続するリンク URL (利用可能な場合)。 **注:** エラーが発生した場合は、McAfee ESM API のベース URL を使用してください。
ユーザー名	McAfee ESM ユーザー名。
パスワード	McAfee ESM パスワード。
最大行数	検索する行の最大行数。
最も早い結果 (日数)	表示する最も早い結果 (日数単位)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
検索結果に生データサンプルを含める	サイティング検索結果に生データのサンプルを含めるには、これを選択します。返されるデータの量は、[セキュリティインシデントレスポンス] プロパティの [生データの行数] プロパティの設定によって異なります。
MID サーバー	[任意] を選択して、 任意のアクティブな MID サーバーを使用するか、特定の MID サーバー名を選択します。

注:
この統合を設定すると、ワークフローが有効になります。ワークフローを管理するには、[ワークフローエディター] に移動します。

5. **[Submit]** をクリックします。
   統合構成カードが表示されます。
6. 新しい構成カードを表示すると、[構成] または [削除] をクリックして、構成を変更または削除できます。
7. 統合構成カードの元のリストに戻るには、[構成を表示] ドロップダウンから [いいえ] を選択します。

Microsoft Azure Sentinel の統合

Microsoft Azure Sentinel は、クラウドベースのセキュリティ情報イベント管理 (SIEM) およびセキュリティオーケストレーション自動応答 (SOAR) ソリューションです。Microsoft Azure Sentinel 統合を使用して Azure Sentinel インシデントを取り込み、セキュリティインシデントレスポンス でセキュリティインシデントを自動的に作成できます。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

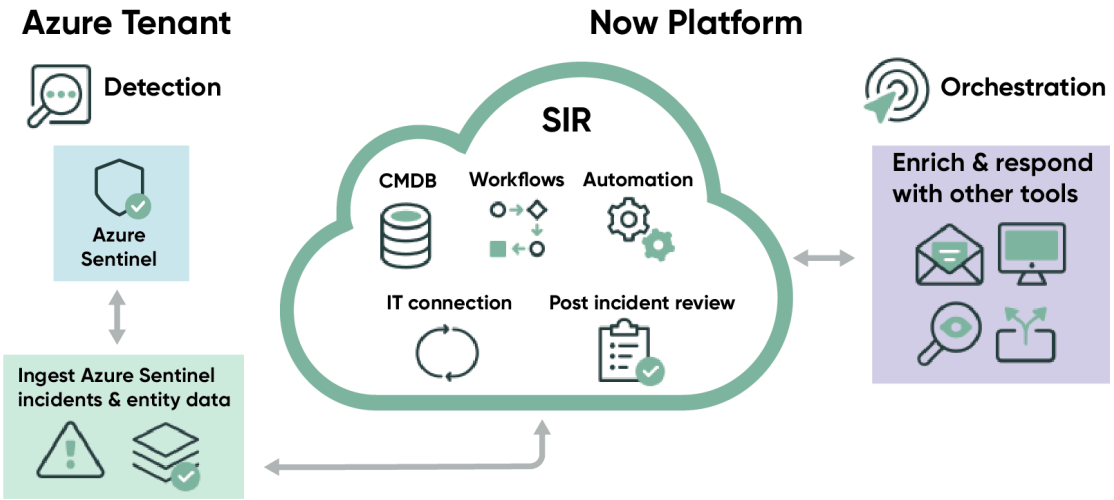
概要

Microsoft Azure Sentinel を Now Platform セキュリティオペレーション アプリケーションと統合する方法については、次の図を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Now Platform - Azure Sentinel integration overview



主な機能

この統合の主な機能を使用して、次のアクションを実行します。

- セキュリティインシデントの候補である Microsoft Azure Sentinel インシデントを検出し、これらのセキュリティインシデントの作成を自動化します。
- Microsoft Azure Sentinel インシデントおよびエンティティフィールドを SIR セキュリティインシデントフィールドにマッピングします。
- Microsoft Azure Sentinel インシデントをフィルターします。
- 重複するセキュリティインシデントを作成する必要がないように、インシデントを既存のオープンセキュリティインシデントに集計します。
- セキュリティインシデントレスポンスの Microsoft Azure Sentinel インシデント状況の更新を自動化して、セキュリティインシデントを作成してクローズできるようにします。

  注:
  ServiceNow は、セキュリティインシデントの作成またはクローズに基づいて Microsoft Azure Sentinel インシデントのステータスを更新します。この更新には、集計済みインシデントと新しいインシデントのコメントも含まれています。

- インシデントの取り込みをスケジュールして、セキュリティインシデントを定期的に作成します。
- Microsoft Azure Sentinel インシデントコメントを SIR の作業メモと同期します。

この統合の詳細

ドキュメント識別子	ドキュメントタイトル
Microsoft 製品ドキュメント Web サイト	Microsoft 製品ドキュメント Web サイト
ServiceNow 製品ドキュメント Web サイト	ServiceNow 製品ドキュメント Web サイト

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Microsoft Azure Sentinel 統合を開始する

Security Operations プラグイン用の Microsoft Azure Sentinel - Incident Ingestion をアクティブ化して、Now Platform インスタンスおよび セキュリティインシデントレスポンス 製品と連動するように設定できます。

始める前に

必要なロール：Microsoft Azure アプリケーションアドミニストレーター、Microsoft Azure テナントアドミン

Microsoft Azure Sentinel 統合を使用する前に、ServiceNow Store からダウンロードする必要があります。

このタスクについて

次のセットアップチェックリストを確認し、スムーズな統合のためのすべてのタスクを完了したことを確認します。

チェックリスト

セットアップタスク	説明
必要な Now Platform および セキュリティインシデントレスポンス ロールをアサインして確認します。	期待される結果を構成および検証するには、次のロールが必要です。 • admin ロールは、ServiceNow Store から統合をインストールし、sn_si.admin ロールをアサインします。 • 次のタスクを実行するには、sn_si.admin ロールが必要です。 ◦ 統合を構成します。 ◦ インシデントプロファイルを作成します。 ◦ Microsoft Azure Sentinel インシデントデータフィールドをセキュリティインシデントフィールドにマッピングします。 ◦ 進行中のインシデントの取り込みをスケジュールします。 ◦ セキュリティインシデントレスポンス インシデントが作成されてクローズされたときに、インシデントの更新を有効にします。 ◦ セキュリティインシデントアナリスト (sn_si.analyst) ロールをアサインします。
Microsoft Azure に必要なロールをアサインします。	アプリケーションを登録して構成するには、Microsoft Azure で次のロールが必要です。 • アプリケーションを登録するアプリケーション開発者。 • アドミン同意エンドポイントを呼び出してアプリケーションに権限を付与するテナントアドミン。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト (続く)

セットアップタスク	説明
この統合を構成する前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	ServiceNow 統合ハブ Starter Pack Installer [com.glide.hub.integrations] プラグインが必要です。 セキュリティインシデントレスポンス プラグイン (com.snc.security_incident) が必要です。このプラグインは、セキュリティインシデントレスポンス 製品をサポートするために必要なすべての依存関係を自動的にインストールします。統合に必要な他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。 次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化する必要があります。 **1.** セキュリティインシデントレスポンス **2.** セキュリティインシデントレスポンス UI **3.** ServiceNow 統合ハブランタイム (com.glide.hub.integration.runtime) **4.** ServiceNow 統合ハブアクションステップ - REST (com.glide.hub.action_step.rest)
でアプリケーションを登録して構成します。 Microsoft Azure ありません	Microsoft Azure ポータルにアプリケーションを登録し、アプリケーションへの読み取りおよび書き込みアクセス権をユーザーに付与します。

Microsoft Azure ポータルの登録と構成

Microsoft Azure ポータルにアプリケーションを登録し、アプリケーションへの読み取りおよび書き込みアクセス権をユーザーに付与します。

始める前に
必要なロール：Microsoft Azure アプリケーションアドミニストレーター、Microsoft Azure テナントアドミン

手順

1. Microsoft Azure ポータルにサインインします。

2. [アプリの登録] を検索して選択します。

3. [新規登録] をクリックします。

4. フォームのフィールドに入力します。

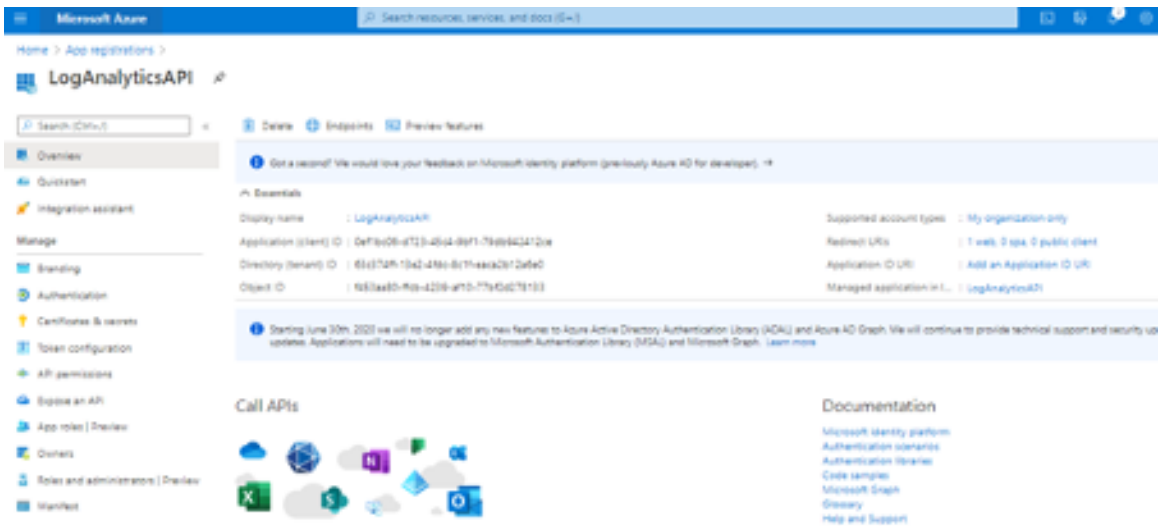
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーションフォームの登録

フィールド	説明
名前	アプリケーションのユーザーに表示される表示名。例：LogAnalyticsAPI。
サポートされているアカウントの種類	このアプリケーションを使用できる、または API にアクセスできるアカウントタイプ。
リダイレクト URI	リダイレクト URI。ユーザーを正常に認証すると、認証応答がこの URI に送信されます。

5. [登録] をクリックします。
アプリケーションを正常に登録すると、概要ページが表示されます。



6. 次のように移動する。 管理 > 証明書とシークレット.
7. [クライアントシークレット] セクションで、[新しいクライアントシークレット **(New client secret)]** をクリックします。
後でクライアントシークレットを表示することはできないため、このステップでクライアントシークレットをコピーして保存してください。クライアントシークレットを忘れた場合は、ステップ 4 と 5 の指示に従って新しいシークレットを生成できます。
8. 次のように移動する。 管理 > **API** 権限.
9. [アクセス許可の追加] をクリックします。
10. [API 権限の要求 (Request API permissions)] ウィンドウで、[組織が使用する **API (APIs my organization uses)]** タブをクリックします。
11. **[Log Analytics API]** アプリ名を検索して選択します。
12. Log Analytics API 権限で、[アプリケーション権限 **(Application permissions)]** を選択します。
この権限を有効にすると、サインインしているユーザーがいなくてもアプリケーションをバックグラウンドサービスまたはデーモンとして実行できます。
13. [データ] セクションで、**[Data.Read (Data.Read)]** を選択します。
14. [アクセス許可の追加] をクリックします。
権限が更新されます。
15. ステップ 13 で有効にした Data.Read API 権限の [デフォルトディレクトリに対してアドミンの同意を得る **(Grant admin consent for Default Directory)]** オプションを有効にします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

16. **[Log Analytics** ワークスペース **(Log Analytics workspaces)]** を検索して選択します。
17. Sentinel Log Analytics ワークスペースを選択します。
    Sentinel Log Analytics ワークスペースの [概要] ページが表示されます。
18. 次のように移動する。 アクセス制御 **(IAM)** > ロールのアサイン.
19. [追加] をクリックし、[ロールのアサインを追加 **(Add role assignment)]** を選択します。
20. フォームのフィールドに入力します。

ロールアサインの追加フォーム

フィールド	説明
ロール	このアプリケーションを使用できるアカウントタイプ。**[Azure Sentinel Responder (Azure Sentinel Responder)]**を選択します。
アクセス権のアサイン	定義する権限スコープ。[ユーザー]、[グループ]、または [サービスプリンシパル] を選択します。
選択	ステップ 4 で作成したアプリケーション。たとえば、LogAnalyticsAPI です。

21. [保存] をクリックします。

Microsoft Azure Sentinel 統合のインストールと構成

Now Platform インスタンスの ServiceNow Store から Microsoft Azure Sentinel 統合をインストールして構成し、Azure Sentinel インシデントの取り込みを開始します。

始める前に
必要なロール：sn_si.admin

手順

1. Microsoft Azure Sentinel 統合を ServiceNow Store からダウンロードしてインストールします。
2. 次のように移動する。 セキュリティオペレーション > 統合 > 統合設定.
3. Microsoft Azure Sentinel タイルを検索し、[構成] をクリックします。
4. フォームのフィールドに入力します。

Microsoft Azure Sentinel - インシデント取り込み構成フォーム

フィールド	説明
名前	Microsoft Azure クラウド インスタンス構成の名前。
ID URL	Microsoft Azure クラウド テナントの ID URL。例：login.microsoftonline.com。詳細については、Microsoft Azure のドキュメント を参照してください。
Azure Resource Manager	Microsoft Azure クラウド テナントの Azure Resource Manager エンドポイント。例：management.azure.com。詳細について

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	は、Microsoft Azure のドキュメント を参照してください。
テナント ID	Microsoft Azure Sentinel テナント ID。これは、Microsoft Azure ポータル内のすべてのインシデントが取得されるインスタンスです。
クライアント ID	Microsoft Azure ポータルで登録済みアプリケーションのクライアント ID。
クライアントシークレット	登録済みアプリケーションのクライアントシークレット。
サブスクリプション ID	登録済みアプリケーションのサブスクリプション ID。
リソースグループ名	登録済みアプリケーションのリソースグループ名。
ワークスペース名	登録済みアプリケーションのワークスペース名。

5. **[Submit]** をクリックします。

タスクの結果
構成の検証と送信が正常に完了すると、各インシデント取り込みサーバー構成が [セキュリティ統合] ページにタイルとして保存されます。

Microsoft Azure Sentinel のプロファイルの作成

Now Platform インスタンスでインシデントプロファイルを作成し、セキュリティインシデントの作成に適した Microsoft Azure Sentinel インシデントを決定します。

始める前に
必要なロール：sn_si.admin

このタスクについて
統合により、不正なアクセス試行やマルウェアなどのさまざまなタイプのインシデントを作成できます。これらのインシデントは、Now Platform インスタンスで構成したプロファイルに基づいて作成されます。すべてのインシデントは、最初にプロファイル内の設定されたインシデントタイプに対して作成されます。作成されたインシデントをさらにフィルタリングして、セキュリティインシデントを作成するインシデントを指定できます。

Microsoft Azure テナントの選択基準を満たし、Microsoft Azure Sentinel API を介して利用可能なすべてのインシデントが、最初に Now Platform インスタンスに取り込まれます。

手順

1. 次のように移動する。 **All** (すべて) > **Microsoft Azure Sentinel** 統合 > **Azure Sentinel** のインシデントプロファイル.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Microsoft Azure Sentinel - インシデント取り込み構成フォーム

フィールド	説明
名前	プロファイルの名前。 この名前は、プロファイルタイプを識別するのに役立ち、このプロファイルに関連付けられているセキュリティタグのデフォルト名でもあります。
アクティブ	プロファイルがアクティブであることを示すインジケーター。 プロファイルがアクティブな場合、Now Platform が Azure Sentinel インシデントをアクティブにポーリングしていること、フィルタリング条件が一致すると、対応するセキュリティインシデントが SIR に作成されることを意味します。
ソース	インシデントを取り込むように構成した Microsoft Azure テナント。複数のテナントが構成されている場合は、プロファイルに取り込む予定のインシデントタイプに適したテナントを選択します。
順序	フロー優先度。このフィールドの値は、2 つ以上のプロファイルがトリガー条件を共有する場合にフローが実行される順序を示します。 番号が最も小さいフローの優先度が最も高くなります。 操作の順序を設定するには、値を入力します。例：100、200、300、400。 デフォルトは 100 です。
説明	このプロファイルを他のプロファイルと区別するための追加テキスト。

4. [マッピング] セクションに移動するには、[続行] をクリックします。

次のタスク
個々の Microsoft Azure Sentinel インシデントフィールドを Now Platform SIR セキュリティインシデントのフィールドにマッピングします。

Microsoft Azure Sentinel インシデントフィールドのマッピング

マッピングされたデータを使用してインシデントを作成できるように、個々の Microsoft Azure Sentinel インシデントフィールドを SIR セキュリティインシデントのフィールドにマッピングします。

始める前に
必要なロール：sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. マッピングページの [Azure Sentinel フィールドマッピング (Azure Sentinel Field Mapping)] セクションで、いずれかの [サンプルの取り込み方法] を選択します。

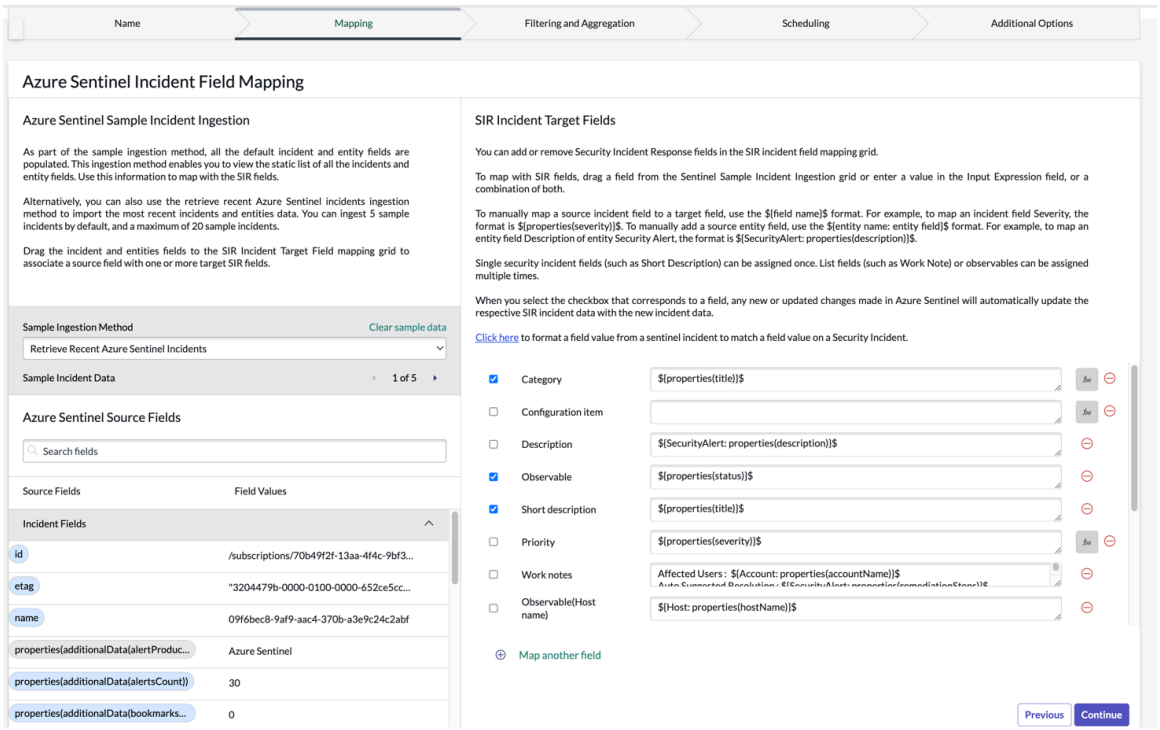
サンプルの取り込み方法

フィールド	説明
すべてのデフォルトのインシデントおよびエンティティフィールド (All default Incident and entity fields)	すべてのインシデントとエンティティフィールドの静的リストを表示するには、この取り込み方法を使用します。この方法には、値のないデフォルトのフィールド名のみが含まれます。 この情報を使用して SIR フィールドとマッピングできます。
最新の Azure Sentinel インシデントを取得 (Retrieve Recent Azure Sentinel incidents)	最新のインシデントとエンティティデータをインポートするには、この取り込み方法を使用します。 Azure Sentinel インシデントにエンティティデータが含まれている場合、エンティティデータが取得され、[Azure Sentinel ソースフィールド (Azure Sentinel Source Fields)] セクションでマッピングできます。Azure Sentinel のインシデントにエンティティデータが含まれていない場合があり、そのようなシナリオではエンティティフィールドをマッピングできません。 Azure Sentinel インシデントに複数のアラートが含まれている場合、インシデントの一部である最も古いアラートがマッピングセクションに表示されます。取り込み中も、最も古いセキュリティアラートフィールド値が使用されます。 デフォルトでは 5 つのサンプルインシデント、最大で 20 のサンプルインシデントを取り込むことができます。 サンプルインシデントフィールド値は、プロファイルがサンプルインシデントを取り込むときに入力されます。これらのインシデントを **[SIR インシデントターゲットフィールド (SIR Incident Target Fields)]** にマッピングできます。インシデントのフィールドと値が個別のタブとして表示されます。
サンプルデータをインポート (Import Sample Data)	Azure Sentinel からサンプルインシデントをインポートするには、[サンプルデータをインポート **(Import Sample Data)]** をクリックします。 このボタンは、インシデント取り込み方法として [最新の Azure Sentinel インシデン

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	トを取得 (Retrieve Recent Azure Sentinel incidents)] を選択すると表示されます。 Microsoft Azure Sentinel サーバーからサンプルインシデントを取得するには時間がかかる場合があります。 取得されたインシデントを **[SIR** インシデントターゲットフィールド **(SIR Incident Target Fields)]** にマッピングできます。インシデントのフィールドと値が個別のタブとして表示されます。



2. セキュリティインシデントに表示されるデフォルトのフィールドにフィールドを追加するには、次のアクションを実行します。

   a. [SIR インシデントターゲットフィールド (SIR Incident Target Fields)] セクションで、 Map another field をクリックします。[別のフィールドをマッピング (Map another field)] ボタンをクリックします。
   SIR フィールドのリストが表示され、表示する新しいフィールドのフィールドを選択できます。

   b. [セキュリティインシデント] 列で表示されているリストを展開し、フィールドを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> 同じセキュリティインシデントに複数の観測事象を表示できます。たとえば、[観測事象] フィールドは異なる値で複数回マッピングできます。同様に、[構成アイテム] フィールドと [作業メモ] フィールドは複数の値をサポートします。複数の値をサポートできないフィールドに 2 つの値をマッピングしようとすると、このフィールドは複数の値をサポートしていないというエラーメッセージが表示されます。同様に、セキュリティインシデントのフィールドに複数のオプションを選択できるリストがあり、リストに表示されていないフィールドにオプションをマップしようとすると、そのフィールドはセキュリティインシデントに入力されません。

c. [Azure Sentinel ソースフィールド (Azure Sentinel Source Fields)] セクションから、フィールドをドラッグアンドドロップして新しいフィールドにマッピングします。

d. フィールドに対応するチェックボックスをオンにすると、Azure Sentinel で行われた新しい変更または更新された変更によって、それぞれの SIR インシデントデータが新しいインシデントデータで自動的に更新されます。

> **注:**
> ベースシステムでは、SIR にリンクされた新しいアラートに関連する Microsoft Azure Sentinel 更新を受信するために、システムプロパティ sn_sec_sentinel.incident_updates はデフォルトで True に設定されています。

- デフォルトでは、[影響を受けるユーザー]、[構成アイテム]、および [観測可能] フィールドはオンになっています。つまり、新しい観測可能項目、関連する構成アイテム、または影響を受けるユーザーがインシデントに追加されるたびに、その情報が自動的に抽出され、そのポーリング間隔中にセキュリティインシデントレスポンス (SIR) のそれぞれの関連リストに入力されます。
- その他のフィールドについては、Azure Sentinel 内の Azure Sentinel インシデントレコードに加えられた新規変更または更新された変更のフィールドに対応するチェックボックスを選択する必要があります。これにより、それぞれの SIR インシデントデータが新しいインシデントデータで自動的に更新されます。

> **重要:**
> 既存のデータを上書きすると、アナリストのデータが不安定になり、セキュリティインシデントのフィールド値によっても設定されている他の自動化も影響を受ける可能性があるため、この機能を選択する前にデューデリジェンスを行う必要があります。そのため、上書き機能を選択する前にデューデリジェンスを行うことが非常に重要です。

3. フィールドを削除するには、[SIR インシデントターゲットフィールド (SIR Incident Target Fields)] セクションの入力式フィールドの横にある ⊖ [アイテムを削除] ボタンを使用します。

4. [Azure Sentinel ソースフィールド (Azure Sentinel Source Fields)] セクションのフィールド値を [SIR インシデントターゲットフィールド (SIR Incident Target Fields)] セクションのフィールドにマップするには、次のいずれかのアクションを使用します。

a. フィールド名 ([ID] など) をドラッグし、[SIR インシデントターゲットフィールド (SIR Incident Target Fields)] 列のフィールド名の横にドロップします。

[Azure Sentinel ソースフィールド (Azure Sentinel Source Fields)] セクションの任意の値を [SIR インシデントターゲットフィールド (SIR Incident Target Fields)] セクションのフィールドと照合できます。マッピングプロセスでインシデントフィールドを見落としたり重複したりしないように、フィールドは色分けされています。ライトブルーのフィールドは、インシデントフィールドがまだ未選択で、セキュリティインシデントにマップされていないことを示します。受信インシデントフィールドをセキュリティインシデントの 1 つ以上のフィールドに関連付け

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ることができます。灰色のフィールドは、フィールドが選択され、セキュリティインシデントのフィールドにマッピングされていることを示します。色分けすることで、セキュリティインシデントに追加されたフィールド値、およびマップされていない残りの重要なインシデント情報を視覚的に把握できます。

b. テキストとフィールドの組み合わせを追加できます。
たとえば、Incident name is ${name}$ です。${name}$ は [Azure Sentinel ソースフィールド (Azure Sentinel Source Fields)] セクションからマッピングされますが、Incident name is は手動で入力できます。

c. ソースインシデントまたはエンティティフィールドを手動で直接入力して、ターゲットフィールドにマッピングできます。

- ソースインシデントフィールドを手動でマッピングするには、${field name}$ 形式を使用します。たとえば、インシデントフィールドの [重大度] をマッピングする場合、形式は ${properties(severity)}$ です。
- ソースエンティティフィールドを手動で追加するには、${entity name: entity field}$ 形式を使用します。たとえば、エンティティセキュリティアラートのエンティティフィールド [説明] をマッピングする場合、形式は ${SecurityAlert: properties(description)}$です。

この統合は、特定の観測事象サブタイプを分類します。Azure Sentinel フィールドを SIR 観測事象フィールドにマッピングすると、Now Platform によって観測事象が自動的に分類されます。受信 Azure Sentinel 観測事象を SIR の観測事象タイプに汎用的にマッピングする場合は、[観測事象] フィールドに Azure Sentinel のフィールドをドラッグアンドドロップします。ただし、SIR の受信 Azure Sentinel 観測事象の観測事象タイプを認識している場合は、SIR の [観測事象タイプ] フィールドに具体的にマッピングします。SIR の具体的な観測事象タイプの例には、[観測事象 (ドメイン名) (Observable(Domain name))]、[観測事象 (メールアドレス) (Observable(Email address))]、[観測事象 (IP アドレス (V4)) (Observable(IP address (V4)))]、および [観測事象 (ホスト名) (Observable(Host name))] が含まれます。

受信 Azure Sentinel フィールドに MITRE-ATT&CK 情報が含まれている場合は、それを [MITRE-ATT&CK テクニック] フィールドにマッピングします。受信 Azure Sentinel フィールドに MITRE-ATT&CK テクニック ID またはテクニック名が含まれていることを確認します。

Microsoft Azure Sentinel のインシデントフィールド値は SIR セキュリティインシデントのフィールドに直接変換されないことがあります。これらの値については、マッピングステップでスクリプトエディターを使用してセキュリティインシデントのフィールド値をフォーマットできます。類似しているが同一ではない値をフォーマットする場合は、スクリプトエディターを使用します。

5. セキュリティインシデントのフィールド値と一致するように、Azure Sentinel インシデントの新しいフィールドのフィールド変換をフォーマットするには、**[SIR** インシデントターゲットフィールド **(SIR Incident Target Fields)]** ヘッダーの [ここをクリック] リンクをクリックします。

6. フィールド変換をサポートするフィールドを変更するには、 スクリプトフォーマットフィールド変換アイコンをクリックします。
フィールドの翻訳をサポートしているフィールドは、[カテゴリ]、[構成アイテム]、および [優先度]です。たとえば、[カテゴリ] の横にある アイコンをクリックします。[Azure Sentinel フィールド翻訳] スクリプトエディターが開きます。

7. スクリプトへの変更を入力し、[更新] をクリックして変更を保存し、 [マッピング] ページに戻ります。
たとえば、カテゴリの場合はスクリプトエディターで次のように定義します。

```
"<Incoming Sentinel Incident Field Value>" : "<Category to assign to the Security Incident>".
```

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このマッピングにより、プロファイルが構成済みのカテゴリのみを使用するようになります。

8. フィールド値を追加または削除して、マッピングを続行します。
   インシデント生成条件ビルダーで同じフィールド値を使用して、セキュリティインシデントを作成する際に受信インシデントを満たす必要がある追加の条件を定義することができます。
9. [フィルタリングと集計] セクションに移動するには、[続行] をクリックします。

次のタスク
フィルター条件を定義して設定することで、セキュリティインシデントを作成するインシデントを指定できます。インシデント生成条件ビルダー ([フィルタリングと集計] セクションにあります) で同じフィールド値 ([マッピング] セクションで定義) を使用して、セキュリティインシデントを作成する際に受信インシデントを満たす必要がある追加の条件を定義することができます。

フィルターと集計基準の定義

フィルター条件を定義して設定することで、セキュリティインシデントを作成する受信 Microsoft Azure Sentinel インシデントを指定できます。インシデントを作成する代わりに、受信インシデントをオープンセキュリティインシデントに追加できるように、追加のインシデントフィールド基準を定義することもできます。

セキュリティインシデントのフィルタリング条件の設定

フィルタリング条件が一致した場合にのみセキュリティインシデントが作成されるように、フィルタリング条件を設定します。

始める前に
必要なロール：sn_si.admin

このタスクについて
このタイプのフィルタリングは、セキュリティインシデントを分離し、作成するセキュリティインシデントの数を制限するのに役立ちます。追加のフィルター基準を設定すると、クエリまたはトリガーされたインシデント構成を変更することなく、必要なインシデントのみが取り込まれます。

手順

1. セキュリティインシデントを作成するために受信される Microsoft Azure Sentinel インシデントが満たすべき条件を定義するには、[条件に基づいてフィルター] を選択します。

   フィルター条件の最初のフィールドのオプションは、取り込まれたインシデントの [Azure Sentinel サンプルインシデントの取り込み (Azure Sentinel Sample Incident Ingestion)] セクションに表示されるフィールドと一致します。これらのフィールドは動的で、取り込むインシデントに応じて変更されます。入力する基準は大文字と小文字を区別します。定義した基準がインシデントの値と一致していることを確認します。

   複数の値を持つ次のフィールドに対して、フィルター条件包含を使用します。

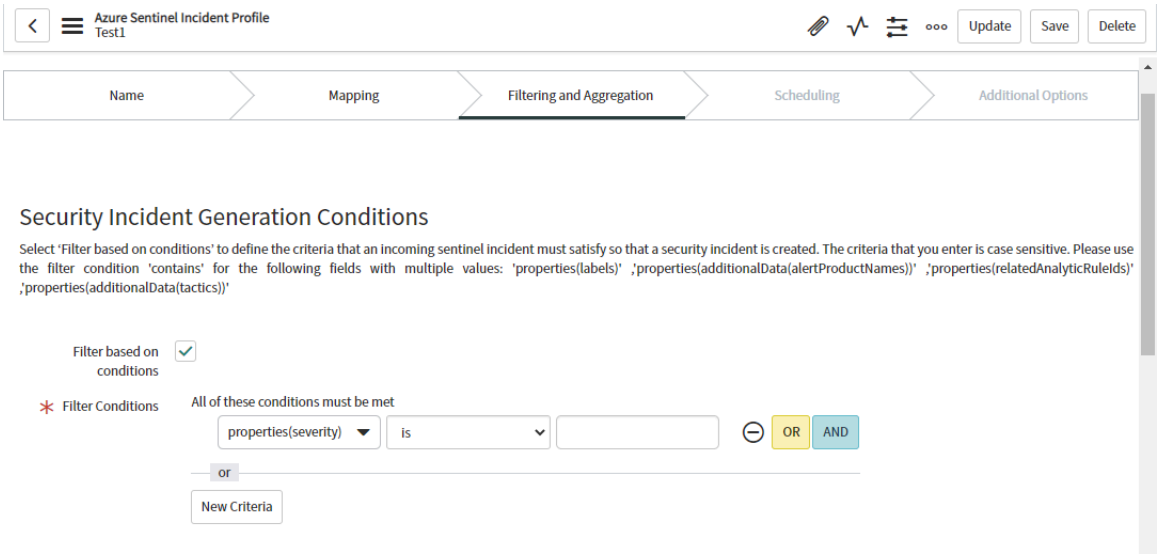
   - properties(labels)
   - properties(additionalData(alertProductNames))
   - properties(relatedAnalyticRuleIds)
   - properties(additionalData(tactics))

   フィルター条件は文字列のみ取得できるため、これらのフィールドに包含フィルター条件を使用して、データが正確にフィルタリングされるようにする必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデント生成条件



2. 条件ビルダーのリストとフィールドを使用して、最初の行のフィルターを設定します。

3. 条件を追加するには、**[AND]** または **[OR]** をクリックします。

- [**AND**] を選択した場合は、すべての条件に一致する必要があります。
- **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。

4. 2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。

アグリゲーション条件の定義

類似の重複する可能性があるインシデントを作成するのではなく、既存の SIR セキュリティインシデントに受信インシデントを集計する追加のインシデント集計基準を定義します。この追加の集計では、各プロファイルのフィールド一致値基準を使用して、関連するすべてのインシデントデータを単一のセキュリティインシデントに配置することで、アクティブな重複するセキュリティインシデントの数を減らすことができます。

始める前に

必要なロール：sn_si.admin

このタスクについて

新しいインシデントが、マッピングステップの集計フィールド条件で選択されたすべての値と一致する場合、新しいインシデントは、同じフィールド値を持つ最新のオープンセキュリティインシデントに自動的に追加されます。セキュリティインシデントを扱う sn_si.analyst ロールを持つユーザーは、セキュリティインシデントの関連リストで、追加されたすべての集計インシデントを表示できます。

セキュリティインシデントの集計されたインシデントはすべて、[Azure Sentinel の集計済みインシデント] 関連リストに表示されます。このリストには、関連するタイムスタンプと集計されたフィールド値の詳細が表示されます。この情報は、インシデントが既存のセキュリティインシデントに追加される理由を理解するのに役立ちます。

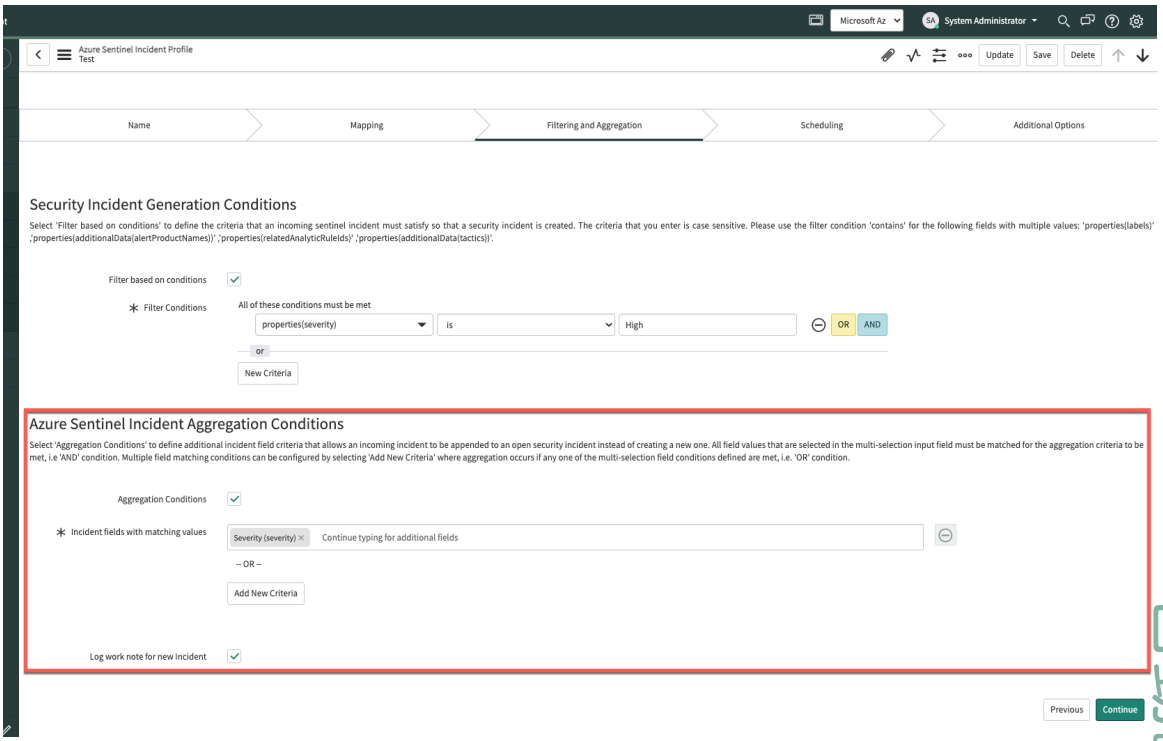
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 新しいインシデントを作成する代わりに、受信 Microsoft Azure Sentinel インシデントをオープンセキュリティインシデントに追加できるように、追加のインシデントフィールド基準を定義するには、次の図に示すように [集計条件] オプションを選択します。

集計条件



2. [値が一致するインシデントフィールド **(Incident fields with matching values)**] フィールドに、Now Platform インスタンスの既存のセキュリティインシデントで照合するフィールド値を入力します。
集計基準が満たされ、この受信インシデントを既存のセキュリティインシデントに追加できるように、複数選択入力フィールドで選択したすべてのフィールド値が一致する必要があります。この選択は、複数のフィールド値を持つ可能性がある [観測事象] や [構成アイテム] などのフィールドがマッピングされる *AND* 条件を意味します。値のサブセットのみが一致した場合、Azure Sentinel インシデント集計条件は満たされず、新しいセキュリティインシデントが作成されます。
3. 複数のフィールド一致条件を追加するには、[新しい基準を追加] をクリックします
定義した複数選択フィールド条件のいずれかが満たされると、集計が行われます。この選択は *OR* 条件を意味します。
4. 新しいインシデントがセキュリティインシデントに追加されたときにその作業メモを更新するには、[新規インシデントの作業メモを記録] を選択します。

   作業メモには、新しいインシデントが追加されたことが記録され、インシデントの詳細へのリンクが含まれています。作業メモの記録では、マッピングセクションの作業メモフィールドに追加した詳細も更新されます。

5. スケジュールを設定するには、[続行] をクリックします。

次のタスク
インシデントデータ、およびプロファイルの基準に一致する取り込み済みインシデントを取得するスケジュールを設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Microsoft Azure Sentinel インシデントの取得のスケジュール設定

インシデントデータを取得し、プロファイルの基準に一致する Microsoft Azure Sentinel インシデントを取り込むスケジュールを設定します。

始める前に

必要なロール：sn_sni.admin

このタスクについて

インシデントプロファイル構成に一致する将来の Microsoft Azure Sentinel インシデントをポーリングする頻度を設定できます。

インシデントの自動取り込みを有効にするには、プロファイルをアクティブ化する前に、スケジュールとインシデントの取得を設定する必要があります。最初の取り込みの具体的な日時を定義するには、[インシデントの取り込み時刻を設定] を有効にします。それ以降の取り込みはポーリング間隔の時間に基づいて決まります。

ポーリング間隔は、各プロファイルで個別に設定されます。ポーリング間隔が異なると、Microsoft Azure Sentinel インシデント統合のパフォーマンスに影響する可能性があります。スケジュールを設定するときは、インシデントの緊急度とシステム負荷のバランスを取るように計画してください。すべてのプロファイルに 1 分のデフォルト値が設定されています。この設定は、インシデントの緊急度とシステムの予想される負荷に基づいて変更できます。

特定のポーリング間隔でインシデントに追加されたアラートがある場合は、プロセスが実行されてから、Azure Sentinel アラート関連リストに追加され、作業メモも投稿されます。

手順

1. スケジュールフォームで、フィールドに入力します。

   Microsoft Azure テナントからインシデントをプルする方法とタイミングを定義するスケジュールを設定します。

   スケジュールフォーム

フィールド	説明
進行中のインシデントの取り込み	Now Platform インスタンスが Microsoft Azure テナントから新しいインシデントを取得する、進行中のインシデントの取り込み。トリガーされたインシデントが検出され、インシデント生成のフィルター基準が一致すると、セキュリティインシデントが作成されます。
ポーリングインクリメント (分)	定義されたポーリング頻度 (分単位)。
インシデントの取り込み時刻を設定	構成された日時に基づくインシデントの取り込み。 このオプションを使用して、最初の取り込みに対する特定の日時を定義できます。それ以降の取り込みはポーリング間隔の時間に基づいて決まります。
インシデントの取り込み時刻を入力	インシデントの取り込みに指定した日時。
1 回限りの取得	Azure Sentinel の過去のインシデントを 1 回だけ取得し、データの調整を行うことを許可するには、このチェックボックスをオンにします。このチェックボックスを選択すると、約 6 か月間までのすべてのオープ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	ンおよびクローズ済みの Azure Sentinel インシデントがプルされます。 データを処理するときは、進行中のインシデントと履歴データの両方がプルされますが、進行中のインシデントの処理は履歴プルよりも優先され、それ以外の場合は、期間と取り込むインシデントの数に基づいて、履歴プルに時間がかかることがあります。 **注:** 取得された履歴 Azure Sentinel インシデントは、セキュリティインシデントレスポンスアプリケーション内での重複を防ぐために重複排除チェックが行われます。
開始日	履歴インシデントが Azure Sentinel から取り込まれてからの日付。 **注:** インシデントデータは、およそ過去 6 か月間から取得されたものです。

[スケジュール] ページでは、Microsoft Azure テナントからインシデントをプルする方法とタイミングを定義できます。

2. [他のオプション] ページに移動するには、[続行] をクリックします。

SIR インシデント状況によるインシデントの更新とクローズの自動化

SIR インシデント状況によって、インシデントの更新とクローズを自動化します。Microsoft Azure Sentinel 統合には、両方のインシデントがセキュリティインシデントを作成し、セキュリティインシデントが作成またはクローズされた後にインシデントを更新できるようにする、双方向のインターフェイスがあります。

始める前に
必要なロール：sn_si.admin

手順

1. フォームで、詳細を入力します。
手順に従って、SIR でセキュリティインシデントを作成またはクローズしたときにインシデントを更新するための構成を完了します。

[インシデントの更新の自動化] フォーム

カテゴリ	フィールド	説明
インシデントの作成の最新情報	SIR インシデントの作成時に Azure Sentinel インシデント状況を更新	自動インシデント更新機能を使用できるようにするオプション。Microsoft Azure Sentinel インシデント状況は、SIR インシデントが Now Platform に作成された後にコメントとともに Microsoft Azure インシデントで更新されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

カテゴリ	フィールド	説明
	最初のインシデントのステータスの更新	Microsoft Azure Sentinel 環境で更新される最初のインシデント状況。ステータスとして [新規] または [アクティブ] を選択できます。
	最初のコメントがインシデントに投稿されました	Microsoft Azure Sentinel 環境でインシデントに投稿される最初のコメント。 SIR インシデントフォームの任意のフィールドでフォーマット ${field name}$ を使用して置換変数を追加または変更することで、[コメント] セクションに表示されるデフォルトテキストを編集することができます。
インシデントのクローズの更新	SIR インシデントのクローズ時に Azure Sentinel インシデントをクローズ	インシデント状況の自動更新機能を使用できるようにするオプション。Microsoft Azure Sentinel インシデントは、SIR インシデントが Now Platform でクローズされた後に指定されたコメントとともに Microsoft Azure インシデントでクローズされます。
	クローズインシデントのステータスの更新	SIR でインシデントがクローズされると、Microsoft Azure Sentinel インシデントでステータスが更新されます。
	クローズコメントがインシデントに投稿されました	SIR でインシデントがクローズされたときに、Microsoft Azure Sentinel インシデントでインシデントに投稿されるコメント。 SIR インシデントフォームの任意のフィールドでフォーマット ${field name}$ を使用して置換変数を追加または変更することで、[コメント] セクションに表示されるデフォルトテキストを編集することができます。
	インシデント分類とクローズ理由	Microsoft Azure Sentinel 環境でインシデントをクローズするために使用される、インシデントの分類方法とクローズ理由。 Microsoft Azure Sentinel 環境でインシデントをクローズするには、方法として [デフォルトのインシデント分類とクローズ理由] を選択します。この方法を選択する場合は、[デフォルトのインシデント分類とクローズ理由] を定義する必要があります。SIR でインシデントをクローズすると、指定された [デフォルトのインシデ

自動翻訳

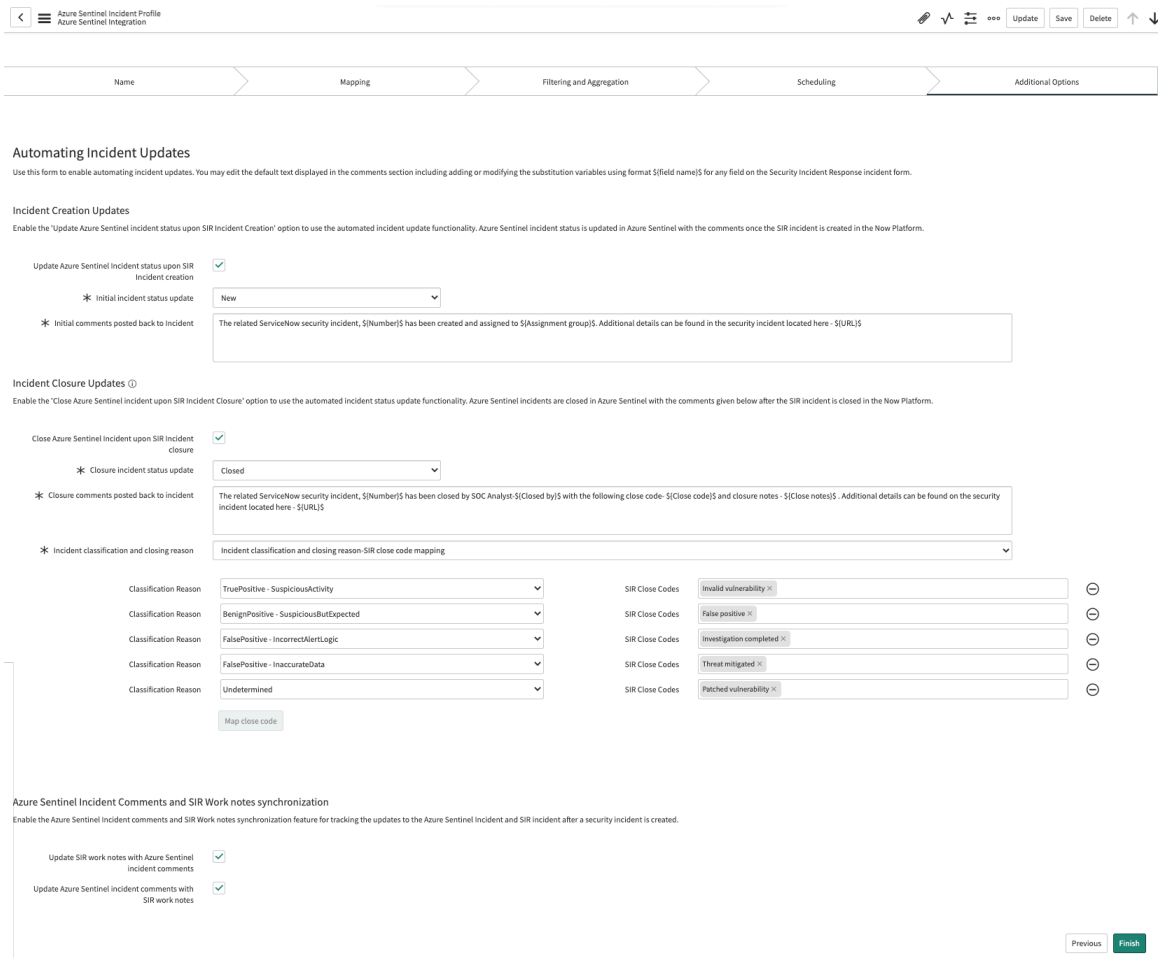
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

カテゴリ	フィールド	説明
		ント分類とクローズ理由] で Azure Sentinel のインシデント状況もクローズされます。 インシデントをクローズし、分類理由を SIR クローズコードにマッピングするには、方法として [インシデントの分類とクローズ理由：**SIR** クローズコードマッピング] を選択します。複数の SIR クローズコードを単一の分類理由にマップできます。クローズコードを使用して SIR でインシデントをクローズすると、マッピングされたインシデント分類とクローズ理由で Azure Sentinel のインシデント状況もクローズされます。 分類理由と SIR クローズコードがマッピングされていない場合、または一致が見つからない場合、Microsoft Azure Sentinel 環境で「未定」というデフォルトの分類理由を使用してインシデントがクローズされます。
Azure Sentinel インシデントコメントと SIR 作業メモの同期	Azure Sentinel インシデントコメントで SIR 作業メモを更新	SIR 作業メモの Microsoft Azure Sentinel コメントを更新するために選択できるオプション。SIR 作業メモのコメントは、「*`Comment from Sentinel`*」というプリフィックス付きで表示されます。コメントには、Sentinel ID、アナリストの詳細、およびタイムスタンプも含まれています。
	SIR 作業メモで Azure Sentinel インシデントコメントを更新	Microsoft Azure Sentinel インシデントコメントの SIR 作業メモを更新するために選択できるオプション。Microsoft Azure Sentinel のコメントは、「*`Comment from ServiceNow`*」というプリフィックス付きで表示されます。

次の例は、インシデントの更新を自動化するために使用できる構成オプションを示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



2. [完了] をクリックします。

次のタスク
プロファイルは [待機中] ステータスに移行します。セットアップと構成が完了したことを示す確認メッセージが表示されたら、プロファイルを有効にできます。

Microsoft Azure Sentinel プロファイルのコピー

プロファイルを作成する代わりに、既存のプロファイルとその関連設定をコピーします。複数のプロファイルを作成する場合は、これらのプロファイルをコピーすることで、既存のプロファイルの設定を再利用できます。

始める前に
必要なロール：sn_si.admin

このタスクについて
プロファイルをコピーすると、重複したプロファイルの作成を避けるためにプロファイル名が最初に変更されます。コピーされたプロファイルは、構成を完了する前に誤ってアクティブ化しないようにオフになります (false に設定)。既にプレビューおよび検証したセキュリティインシデントのプロファイルをコピーし、既存のマップを使用できます。

手順

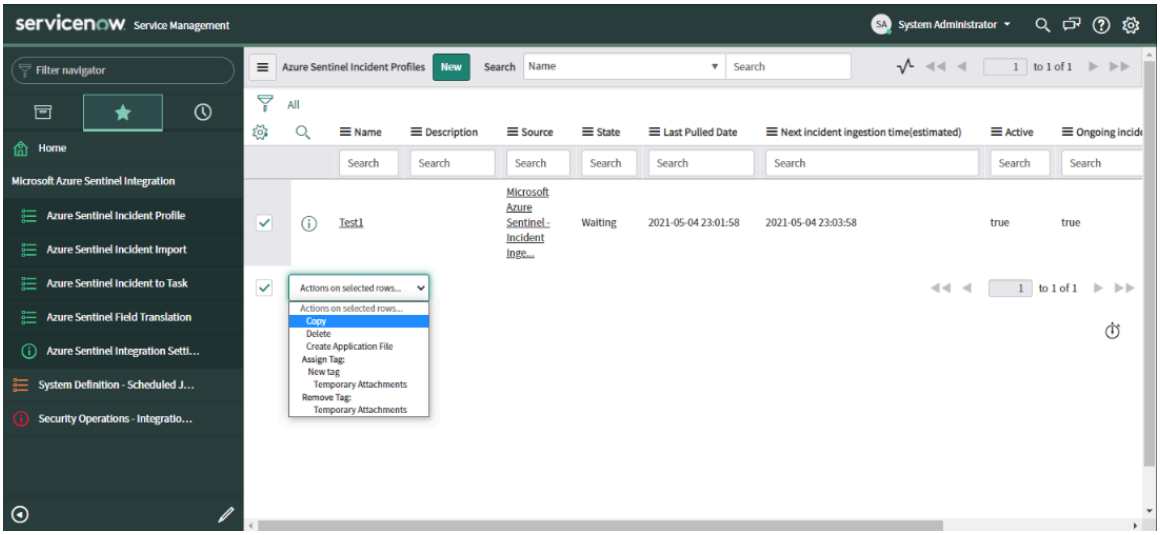
1. 次のように移動する。 **All** (すべて) > **Microsoft Azure Sentinel** 統合 > **Azure Sentinel** のプロファイル.

2. [Azure Sentinel のプロファイル] リストでコピーするプロファイルを選択し、[選択した行のアクション] リストから、次の例に示すように [コピー] をクリックします。

自動翻訳

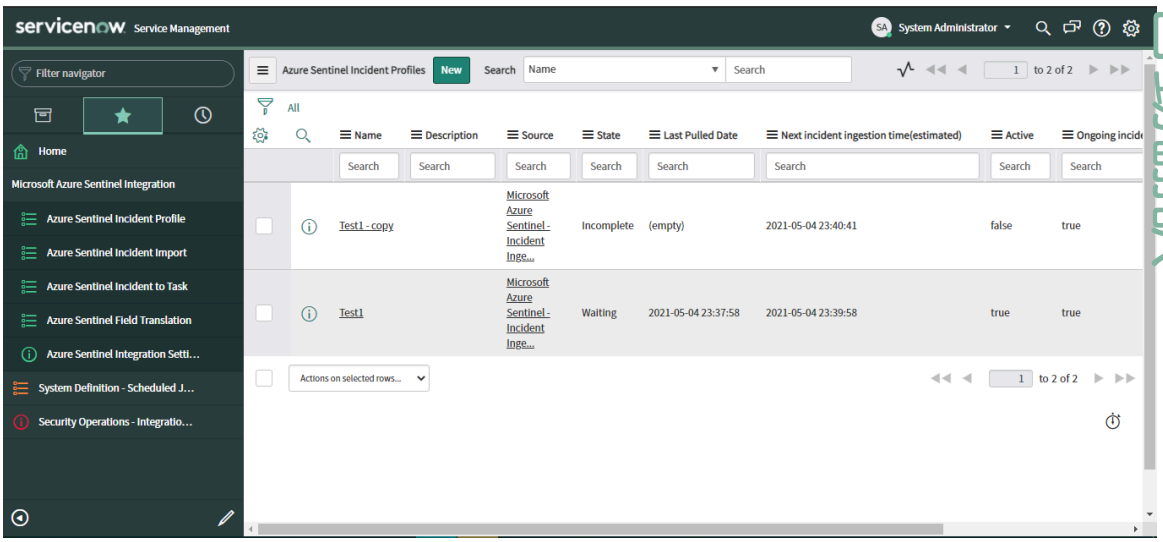
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロファイルのコピー



プロファイルがコピーされ、次の例に示すようにリストに表示されます。コピーには、マッピングとスケジュール設定を含む元のプロファイルのすべての設定が含まれます。プロファイルの名前に「copy」という語が含まれています。元のプロファイルは有効ですが (true)、この時点でコピーはオフになります (false)。必要に応じて、コピーしたプロファイルの値を編集して名前を変更し、構成設定を新しいプロファイルに適用することもできます。

コピーされたインシデントプロファイルの表示



既存のプロファイルから新しいプロファイルに設定が正常にコピーされました。[アクティブ] 列のステータスが false に設定されます。これは、プロファイルをアクティブ化する必要があることを示しています。

インシデントの取り込み後の **SIR** フォーム

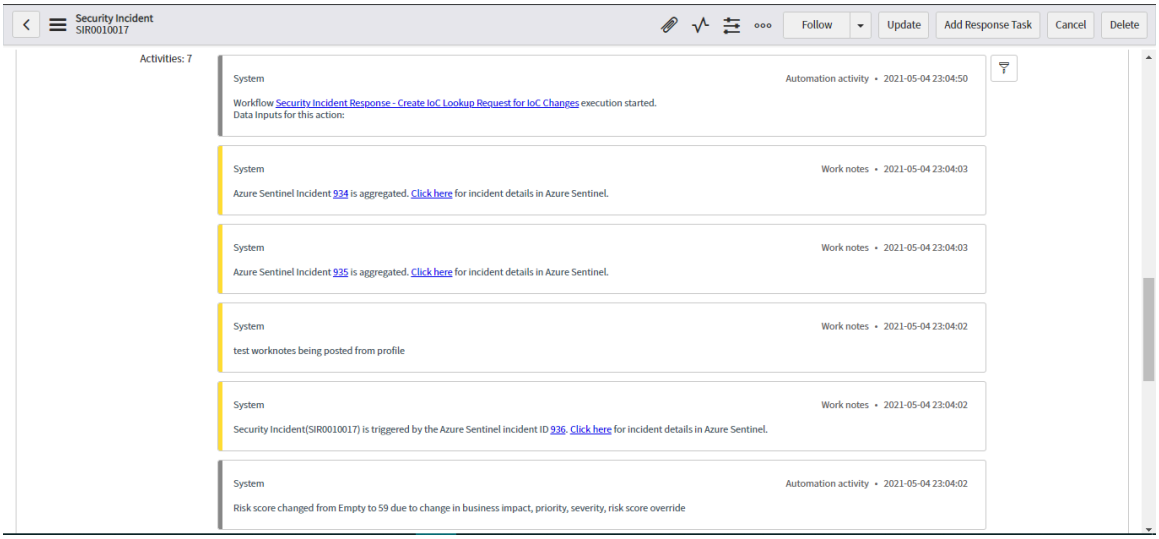
Now Platform に Microsoft Azure Sentinel インシデントが取り込まれると、セキュリティインシデントが作成され、そのセキュリティインシデントレコードに対して更新が実行されます。

作業メモ

インシデントが集計され、[インシデント集計基準] で [新規インシデントの作業メモを記録] オプションを構成した場合、作業メモが投稿されます。次の例は、SIR の作業メモを示しています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SIR での作業メモの表示

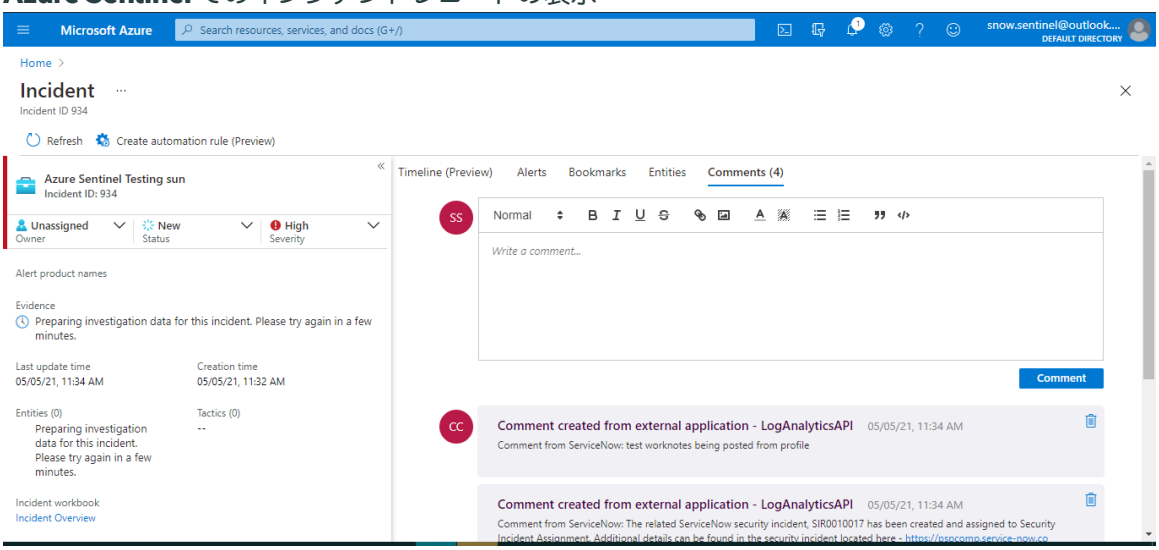


インシデント番号をクリックすると、生のインシデントデータを含む内部インシデントインポートレコードを表示できます。次の例は、SIR の生のインシデントデータを示しています。

SIR でのインシデント生データの表示

[ここをクリック] リンクをクリックすると、Microsoft Azure Sentinel 環境でレコードを表示できます。次の例は、Microsoft Azure Sentinel 環境でのレコードを示しています。

Azure Sentinel でのインシデントレコードの表示

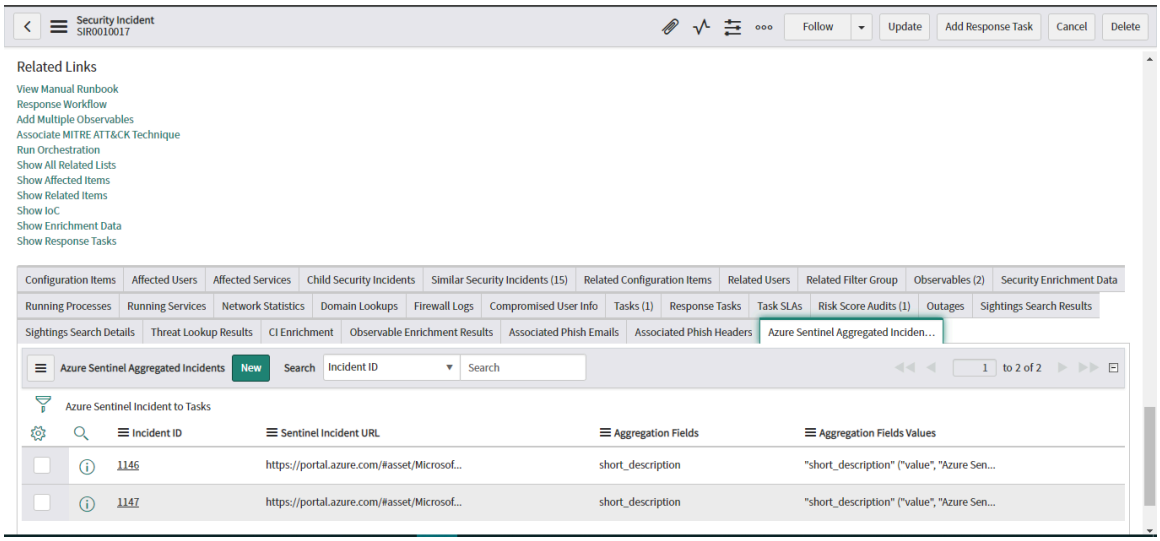


自動翻訳

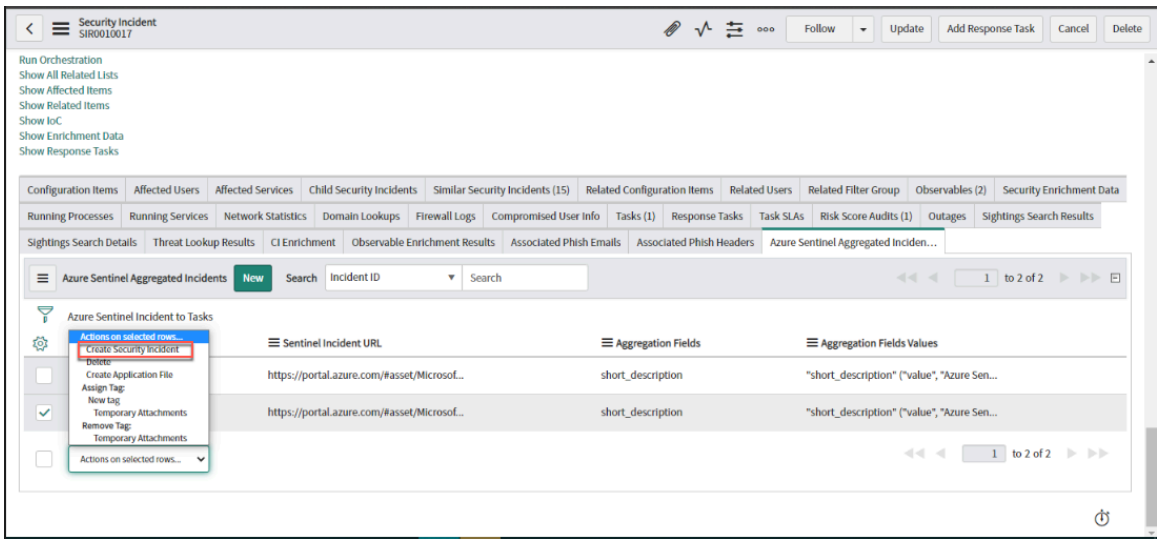
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

集計された **Sentinel** インシデント

集計された Sentinel インシデントの表示：セキュリティインシデントに集計されたインシデントを表示します。次のように移動する。 すべての関連リストを表示 > 集計された **Microsoft Azure Sentinel** インシデント.



セキュリティインシデントの作成：リストからインシデントを選択し、[アクション] メニューをクリックして、[セキュリティインシデントの作成] をクリックします。このオプションで、インシデントの新しいセキュリティインシデントを作成できます。このインシデントは親セキュリティインシデントからは集計されません。



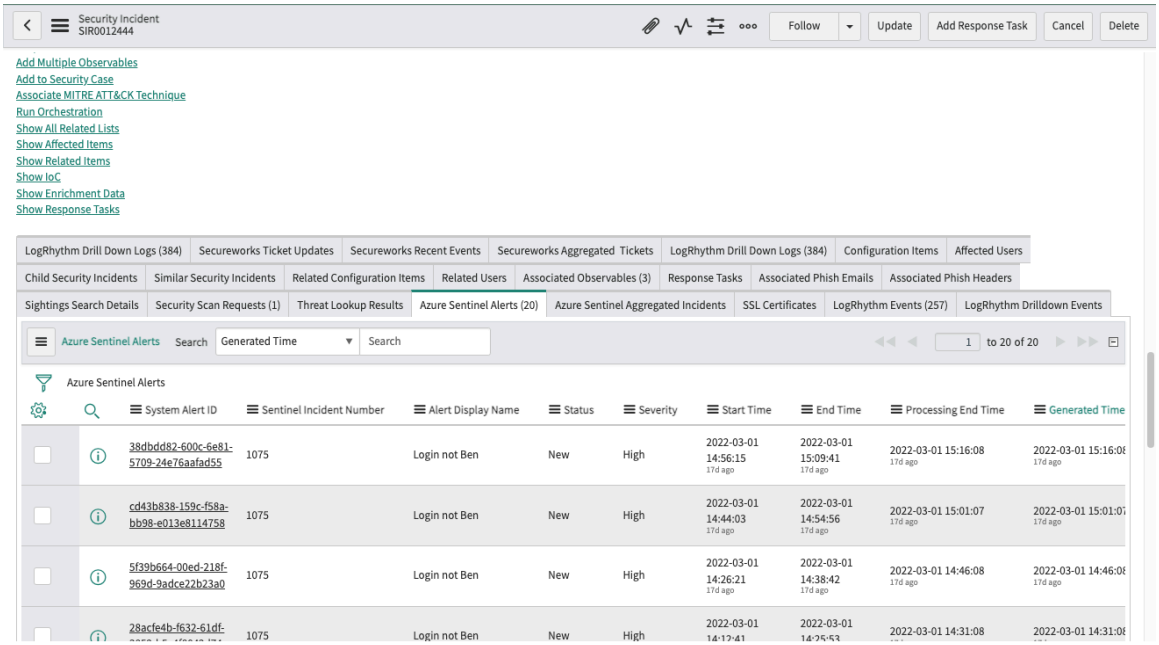
Azure Sentinel のアラート

セキュリティインシデントをトリガーした Sentinel インシデントに関連付けられているアラートを表示するには、次に移動します: すべての関連リストを表示 > **Azure Sentinel** のアラート.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Azure Sentinel のアラート



Microsoft Azure Sentinel 統合設定を確認する

Microsoft Azure Sentinel 統合設定を確認し、環境に合わせてシステムプロパティを変更できるようにします。

始める前に
必要なロール：sn_si.admin

手順

1. 次のように移動する。 **All** (すべて) > **Microsoft Azure Sentinel** 統合 > **Azure Sentinel** 統合の設定.
2. 必要に応じて次の設定を変更します。

Microsoft Azure Sentinel 統合の設定

プロパティ名	説明
サンプルデータをフェッチできる日数を強制的に制限します。 sn_sec_sentinel.max_num_of_days_for_sample_data	Microsoft Azure Sentinel 環境からサンプルデータをフェッチできる最大日数。 タイプ：整数 デフォルト値：7
SIR にリンクされている新しいアラートに関連する更新を受信します。 sn_sec_sentinel.incident_updates	インシデントの更新を受信するオプションを有効にします。 タイプ：ブーリアン デフォルト値：True
Microsoft Azure Sentinel フィールドマッピングで値を分割する区切り文字。 sn_sec_sentinel.delimiter	Microsoft Azure Sentinel フィールドマッピングで値を分割する区切り文字。 タイプ：文字列

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ名	説明
	デフォルト値：', ' (カンマとスペース)
フェッチできるサンプルインシデントの数を強制的に制限します。 sn_sec_sentinel.max_num_of_sample_incidents_to_call	取り込みのために Microsoft Azure Sentinel 環境からフェッチするサンプルインシデントの最大数。 タイプ：整数 デフォルト値： 5 サンプル最大値：20
単一のインシデントに集計できる Sentinel インシデント数の制限を強制します。 sn_sec_sentinel.max_aggregations_per_si	セキュリティインシデントのインシデント集計制限。たとえば、102 件のインシデントがある場合、最初の 100 件は security incident_1 に集計され、残りの 2 件は security incident_2 に集計されます。 タイプ：整数 デフォルト値：100
24 時間内に作成できるセキュリティインシデント数の制限を強制します。 sn_sec_sentinel.max_si_per_day	Now Platform で 24 時間内に作成できるセキュリティインシデントの最大数。 タイプ：整数 デフォルト値：1000
1 回の REST 呼び出しでのインシデントデータのフェッチに関するページネーションの上限。 sn_sec_sentinel.max_page_size	Microsoft Azure Sentinel 環境からの 1 回の REST 呼び出しでのインシデントデータのフェッチに関するページネーションの上限。 タイプ：整数 デフォルト値：100
インシデントの API バージョン値。 sn_sec_sentinel.sentinel_security_incident_api_version	Sentinel インシデントを取得するための Microsoft API バージョン。 デフォルト値：2021-10-01
アラートの API バージョン値。 sn_sec_sentinel.sentinel_security_alert_api_version	Sentinel アラートを取得するための Microsoft API バージョン。 デフォルト値：2021-10-01
エンティティの API バージョン値。 sn_sec_sentinel.sentinel_security_entities_api_version	Sentinel エンティティを取得するための Microsoft API バージョン。 デフォルト値：2021-10-01
sn_sec_sentinel.logging.verbosity	アプリケーションのログの詳細度レベル、すなわち情報のタイプの名前。値を次のオプションに更新することもできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ名	説明
	○ エラー ○ 警告 ○ 情報 ○ **debug** デフォルト値：**info**。

3. [保存] をクリックします。
   変更した統合設定は、プロファイルで定義されている次のポーリング間隔で適用されます。

ドメインセパレーションと **Microsoft Azure Sentinel** 統合

このアプリケーションでは、ドメインセパレーションがサポートされています。 ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル：ベーシック

- アプリケーションサービスプロバイダーのユースケースに合わせてデータが適切なドメインに送られるようにするビジネスロジックが存在します。
- このアプリケーションは、ドメインセパレーションを完全にサポートしています。ドメインセパレーションには、ユーザーインターフェイス、キャッシュキー、レポート、ロールアップ、および集計からのドメインの分離が含まれます。
- インスタンスのオーナーは、複数のテナント間で正常に機能するようにアプリケーションをセットアップする必要があります。

サンプルユースケース：サービスプロバイダーがチャットを使用してテナント顧客のメッセージに応答する場合、お客様がサービスプロバイダーの応答を確認できるようにする必要があります。

サポートレベルの詳細については、「アプリケーションでのドメインセパレーションのサポート」を参照してください。

Microsoft Azure Sentinel 統合でのドメインセパレーションの機能の仕組み

ドメインセパレーションを実現するには、次の手順に従います。

- それぞれのドメインで sn_si.admin ロールを持つユーザーを作成します。

  注:
  プロファイルを作成するときは、ドメインピッカーを使用してドメインを選択します。親ドメインにユーザーを作成して、後でプロファイルのドメインを変更しないでください。プロファイルのドメインごとに sn_si.admin ロールを持つユーザーが必要です。このユーザーを使用して、プロファイルの設定を作成または変更します。

- 既存のスケジュール済みジョブを無効にします。
- すべてのドメインについて次のスケジュール済みジョブを複製します。

自動翻訳

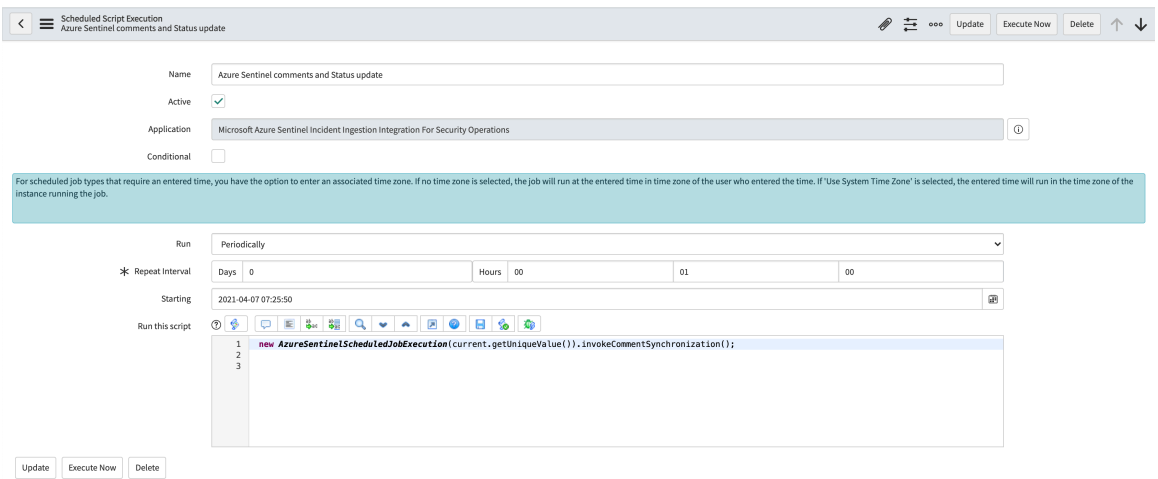
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- Azure Sentinel のアラートとエンティティのフェッチ
- Azure Sentinel のコメントの同期
- Azure Sentinel のステータスの更新
- Azure Sentinel のプロファイルプロセス
- Azure Sentinel プロセス生データ
- Azure Sentinel のデータクリーンアップ
- Azure Sentinel の履歴コメントのプル

注:
スケジュール済みジョブを複製した後、ナビゲーターを使用してモジュールアクセスポリシーモジュールを検索し、[ターゲットスクリプト] に新しく作成されたスケジュール済みジョブが表示される、最近作成されたレコードを表示します。[結果] フィールドの値を [追跡] に変更します。

- [実行方法] をシステムユーザーからそれぞれのドメインの sn_si.admin ロールを持つユーザーに変更してから、スケジュール済みジョブを実行します。

次の例は、Azure Sentinel のコメントとステータスの更新ジョブを複製し、システムユーザーとしてジョブを実行する方法を示しています。



関連情報

サービスプロバイダーのドメインセパレーション

SIR との Microsoft Azure Sentinel 統合と Microsoft Graph Security API 統合の比較

Microsoft Azure Sentinel 統合と Microsoft Graph Security API 統合の違いを確認し、Now Platform インスタンスとの適切な統合を選択できます。

Microsoft Azure Sentinel - Incident Ingestion の概要

Microsoft Azure Sentinel は、クラウドベースのセキュリティ情報イベント管理 (SIEM) およびセキュリティオーケストレーション自動応答 (SOAR) ソリューションです。Microsoft Azure Sentinel は、企業全体のインテリジェントなセキュリティ分析と脅威インテリジェンスを提供します。アラートの検出、脅威の可視化、積極的なハンティング、および脅威の対応に単一のソリューションを提供します。

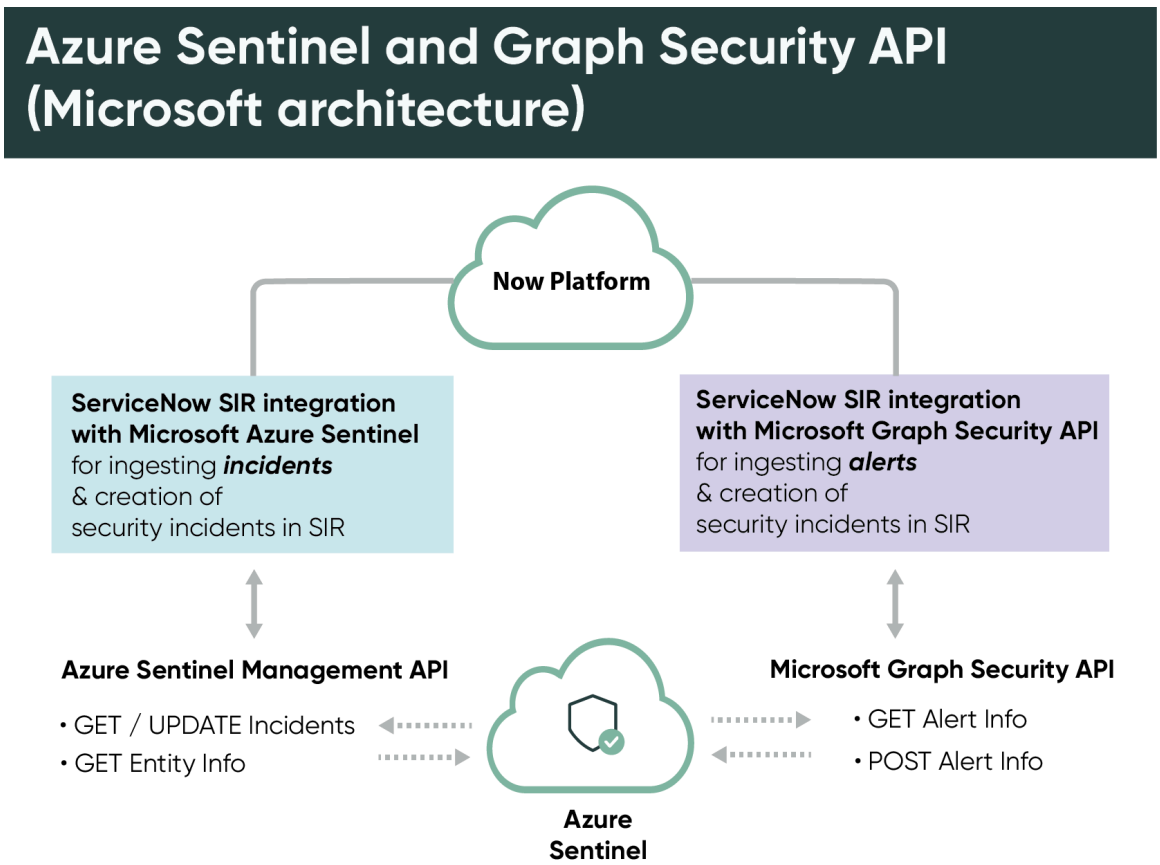
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Microsoft Graph Security API の概要

Microsoft Graph Security API は、複数のセキュリティプロバイダー (Microsoft ネイティブおよび ServiceNow パートナー) を接続する単一のプログラムインターフェイスを提供する中間サービス (またはブローカー) です。

Microsoft Graph Security API 統合では、Microsoft Graph Security API を使用して Azure Sentinel、Microsoft Defender Advanced Threat Protection、Azure Advanced Threat Protection などのさまざまな Microsoft セキュリティ技術と接続することで、これらの問題に対処します。Microsoft セキュリティプロバイダーからのアラートが取り込まれ、自動で セキュリティインシデントレスポンス にセキュリティインシデントが作成されます。

機能の違いの概要



Microsoft Azure Sentinel 対 Microsoft Graph Security API

Microsoft Azure Sentinel	Microsoft Graph Security API
Microsoft Azure Sentinel インシデントをエンティティ情報 (利用可能な場合) とともに取り込み、SIR でのセキュリティインシデントの作成を自動化します。	複数のセキュリティプロバイダー (Azure Sentinel を含む) からのアラートを標準スキーマに取り込み、SIR でのセキュリティインシデントの作成を自動化します。
セキュリティインシデントレスポンスの Microsoft Azure Sentinel インシデント状況の更新を自動化して、セキュリティインシデントを作成してクローズできるようにします。	選択したセキュリティプロバイダーのアラートの更新 (アラートステータスの変更とアラートのクローズ) をサポートします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Microsoft Azure Sentinel 対 **Microsoft Graph Security API** (続く)

Microsoft Azure Sentinel	Microsoft Graph Security API
注: ServiceNow は、セキュリティインシデントの作成またはクローズに基づいて Microsoft Azure Sentinel インシデントのステータスを更新します。	注: Microsoft Graph Security API でサポートされているセキュリティプロバイダーの詳細については、Microsoft のドキュメント を参照してください。
シナリオに次の条件が含まれている場合は、この統合を使用します。 • 予備的なインシデント調査が Microsoft Azure Sentinel にあり、後続の調査が SIRにある • Microsoft Azure Sentinel インシデントを SIR に取り込む	シナリオに次の条件が含まれている場合は、この統合を使用します。 • インシデント調査を SIR で実行する。 • Microsoft Azure Sentinel のアラートを SIR に取り込む。 • インシデントは Microsoft Azure Sentinel に作成されない。
アラートは Microsoft Azure Sentinel のエンティティです。Microsoft Azure Sentinel Management API を使用してスタンドアロンまたは特定のアラートを取得することはできません。インシデントに関連付けられたアラートデータのみを取得できます。この統合を使用して利用できるアラートデータは、Microsoft Graph Security API を使用して利用できるアラートデータよりも豊富です。	Microsoft Azure Sentinel で正規化されたアラートデータが利用可能です。Microsoft Graph Security API で内部的にマッピングされていて Microsoft Graph Security API で利用可能な Microsoft Azure Sentinel アラートフィールドをこの統合で使用できます。
	この統合を使用して Microsoft Azure Sentinel のアラートを更新することはできません。

Microsoft Defender for Endpoint の統合

Microsoft Defender for Endpoint を使用すると、エンドポイントの既知および未知の脅威を積極的に検査、分析、および封じ込めることができます。

Microsoft Defender for Endpoint 統合により、セキュリティアナリストはツール間を移動することなくセキュリティインシデントを効率的に調査および修正できます。

この統合を使用して、構成を作成し、ホストの詳細、ログインしているユーザーの詳細、関連するマシンの詳細、およびその他の拡張機能を取得できます。マシンをネットワークへのアクセスから隔離するか、隔離からマシンを削除するように要求できます。要求は承認者によって承認または却下されます。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

主な機能

Microsoft Defender for Endpoint の主な機能は次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- エンタープライズセキュリティ検索を実行して、エンドポイント間で潜在的な悪意のある可能性のある観測事象を検出し、是正措置を実行する。
- ホストの隔離、分離の削除、アプリの実行の制限、アンチウイルススキャンの実行、アプリ制限の削除、ファイルを停止して隔離する。
- インジケーターを作成または更新する。
- 観測事象の拡張を実行し、インジケーターに関連するデータを取得する。

Microsoft Defender for Endpoint

探索	インストール	構成
Microsoft Defender for Endpoint を開始します	統合用のアプリケーションのインストールとソースの構成	Microsoft Defender for Endpoint のプロファイルとセキュリティインシデントを構成します
機能プロファイル	**その他の構成**	**その他**
Microsoft Defender for Endpoint 統合の機能プロファイルを作成します。	Microsoft Defender for Endpoint で実行できる追加の構成	Microsoft Defender for Endpoint を使用して、サイティング検索とインジケーターのプロファイルを作成および構成します。

自動翻訳

Microsoft Azure ポータルにおける **Microsoft Defender for Endpoint** の登録と構成

Microsoft Azure ポータルに Microsoft Defender for Endpoint アプリケーションを登録し、アプリケーションへの読み取りおよび書き込みアクセス権を付与します。

始める前に
必要なロール：アプリケーションアドミニストレーター、テナントアドミン

手順

1. Microsoft Azure ポータルにログインします。
2. [検索] ボックスに「App registrations」と入力し、[新規登録をクリック **(Click New registration)]** をクリックします。
3. アプリケーションの名前とリダイレクト URI を入力し、[登録] をクリックします。
   たとえば、「Microsoft Defender for Endpoint」という名前にします。リダイレクト URI は、アプリケーションに対してアドミン同意を提供するときに使用されます。
4. [アプリの登録 **(App registrations)]** ページで、ステップ 3 で登録したアプリケーションを選択します。
5. [管理] で、[証明書とシークレット **(Certificates & secrets)]** を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. クライアントシークレットを作成するには、[新しいクライアントシークレット **(New client secret)]** を選択します。
7. クライアントシークレットをコピーして保存します。

   クライアントシークレットを忘れた場合は、新しいクライアントシークレットを生成できます。
8. 次のように移動する。 管理 > **API** 権限.
9. [アクセス許可の追加] をクリックします。
10. [API 権限の要求 (Request API permissions)] ウィンドウで、[組織が使用する **API (APIs my organization uses)]** タブをクリックします。
11. **[WindowsDefenderATP (WindowsDefenderATP)]** を検索して選択します。
12. WindowsDefenderATP (WindowsDefenderATP) 権限で、[アプリケーション権限 **(Application permissions)]** を選択します。
    この権限を有効にすると、サインインしているユーザーがいなくてもアプリケーションをバックグラウンドサービスまたはデーモンとして実行できます。
13. 次のアプリケーションレベルの権限を追加し、新しく追加された API 権限に対してアドミンの同意を付与します。

権限	権限表示名
Machine.Read.All	すべてのマシンプロファイルを読み込む (Read all machine profiles)
User.Read.All	ユーザープロファイルを読み込む (Read user profiles)
Machine.Isolate	マシンを隔離
Machine.RestrictExecution	コードの実行を制限 (Restrict code execution)
Machine.Scan	マシンをスキャン (Scan machine)
Machine.StopAndQuarantine	停止と隔離 (Stop and Quarantine)
URL.Read.All	読み込み URL
File.Read.All	ファイルプロファイルを読み込み (Read file profiles)
Ip.Read.All	IP アドレスプロファイルを読み込み (Read IP address profiles)
Ti.ReadWrite.All	インジケーターを読み書き (Read and write Indicators)

Microsoft Defender for Endpoint 統合を開始する

次のセクションでは、ServiceNow Store から Microsoft Defender for Endpoint アプリケーションをインストールする前に Now Platform インスタンスで完了する必要があるセットアップタスクを示します。

始める前に
必要なロール：admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スムーズなインストールと構成を行うために、 アプリケーションをダウンロードしてインストールする前に、次のテーブルを参照して、リストされたすべてのタスクを完了していることを確認してください。

セットアップタスク	説明
必要な Now Platform および セキュリティインシデントレスポンス (SIR) のロールがアサインされていることを確認します。	以下のロールが必要です。 **1.** 統合用にアプリケーションをインストールするには、システムアドミニストレーター (admin) ロールが必要です。 **2.** 統合を構成し、プロファイルを作成、アクティブ化、および削除するには、セキュリティインシデントアドミン (sn_si.admin) ロールが必要です。 **3.** セキュリティインシデントを操作するには、セキュリティインシデントアナリスト (sn_si.analyst) ロールが必要です。このロールを持つユーザーは、統合で利用可能なすべての機能を開始できます。
アプリケーションをインストールする前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化する必要があります。 **1.** セキュリティインシデントレスポンス **2.** ServiceNow 統合ハブランタイム (com.glide.hub.integration.runtime) **3.** ServiceNow 統合ハブアクションステップ - REST (com.glide.hub.action_step.rest)
プロファイルの承認オプションを有効にする前に、承認グループが作成されていることを確認します。	オプションの承認ワークフローは、ホストマシンの隔離、ネットワークへの復元、エンドポイントでの追加アクションの実行に使用できます。 組織でこれらのアクションをより詳細に制御する必要がある場合は、プロファイルの構成時に [承認が必要] オプションを有効にします。 プロファイルが利用可能なシナリオでは、承認用のプロファイル構成が優先されます。プロファイルが利用できないシナリオでは、承認はデフォルト設定に基づいて処理されます。 セキュリティアドミニストレーターは、プロファイルとデフォルト設定を構成するときに承認を設定できます。承認グループは、インスタンスの [グループ] リストで使用できる必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	sn_si.analyst ロールを持つユーザーによって送信された要求を監視および処理するには、承認グループの各メンバーは、Now Platform® で [自分の承認] に移動する必要があります。または、承認者は [承認] モジュールで Microsoft Defender for Endpoint 統合専用に送信された要求を見つけることができます。ユーザーグループの作成方法の詳細については、「ユーザーグループの作成」を参照してください。

次のタスク
Microsoft Defender for Endpoint 統合のために Now Platform® インスタンスが正常に設定されました。次のステップでは、統合のために ServiceNow Store から Microsoft Defender for Endpoint アプリケーションをインストールします。

統合用のアプリケーションのインストールとソースの構成

Now Platform インスタンスの ServiceNow Store から Microsoft Defender for Endpoint 統合をインストールして構成します。構成を使用して機能プロファイルの作成を開始します。

始める前に
必要なロール：sn_si.admin

手順

1. ServiceNow Store から Microsoft Defender for Endpoint 統合をダウンロードしてインストールします。
2. 次のように移動する。 セキュリティオペレーション > 統合 > 統合設定.
3. [Microsoft Defender for Endpoint] タイルを検索し、[構成] をクリックします。
4. フォームで次のフィールドに入力します。

Microsoft Defender for Endpoint の構成

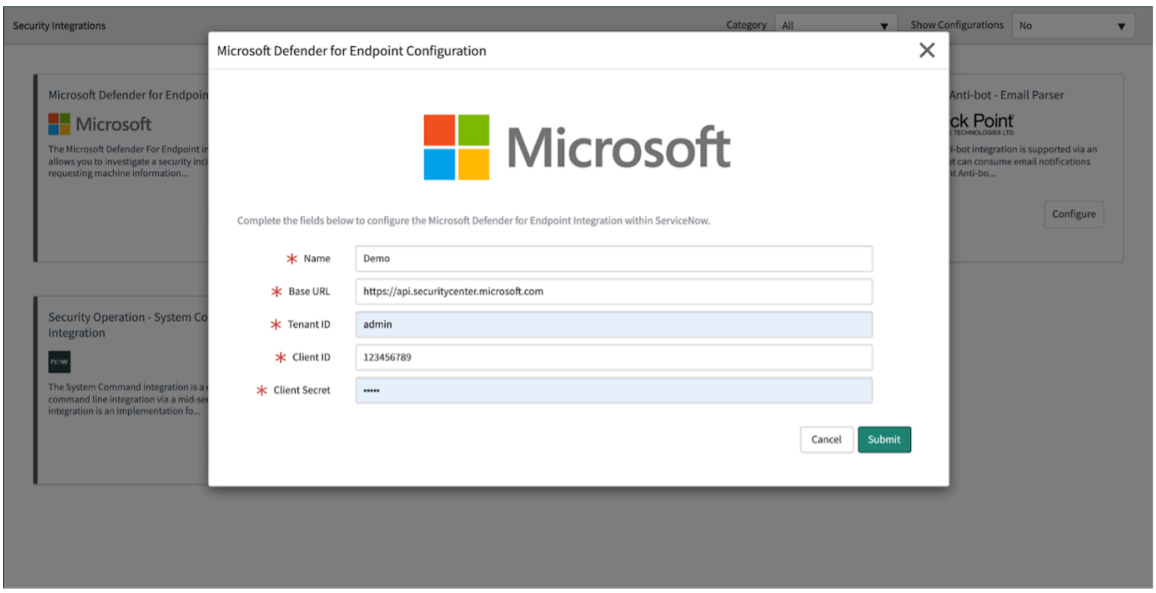
名前	Microsoft Defender for Endpoint インスタンス構成の名前。
ベース URL	Microsoft Defender for Endpoint のサービスベース URL
テナント ID	Microsoft Defender for Endpoint テナント ID。すべてのアクションがこのインスタンスで実行されます。
クライアント ID	Microsoft Azure ポータルで登録済みアプリケーションのクライアント ID。
クライアントシークレット	登録済みアプリケーションのクライアントシークレット。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. **[Submit]** をクリックします。

アプリケーションのインストールと構成



タスクの結果
新しい設定レコードを含む Microsoft Defender for Endpoint 構成リストが表示されます。これで Microsoft Defender for Endpoint の構成が完了しました。

Microsoft Defender for Endpoint のデフォルト設定

インストール完了後に実行が必要な追加の構成設定があります。

インストールが完了すると、左側のナビゲーションペインの Microsoft Defender for Endpoint アプリケーションの下に [デフォルト設定] モジュールが表示されます。これには、さまざまな Microsoft Defender for Endpoint 機能のデフォルト設定が含まれています。

必要なロール：sn_si.admin、sn_si.analyst (読み取り専用)。

追加の構成

追加の構成設定は次のとおりです。

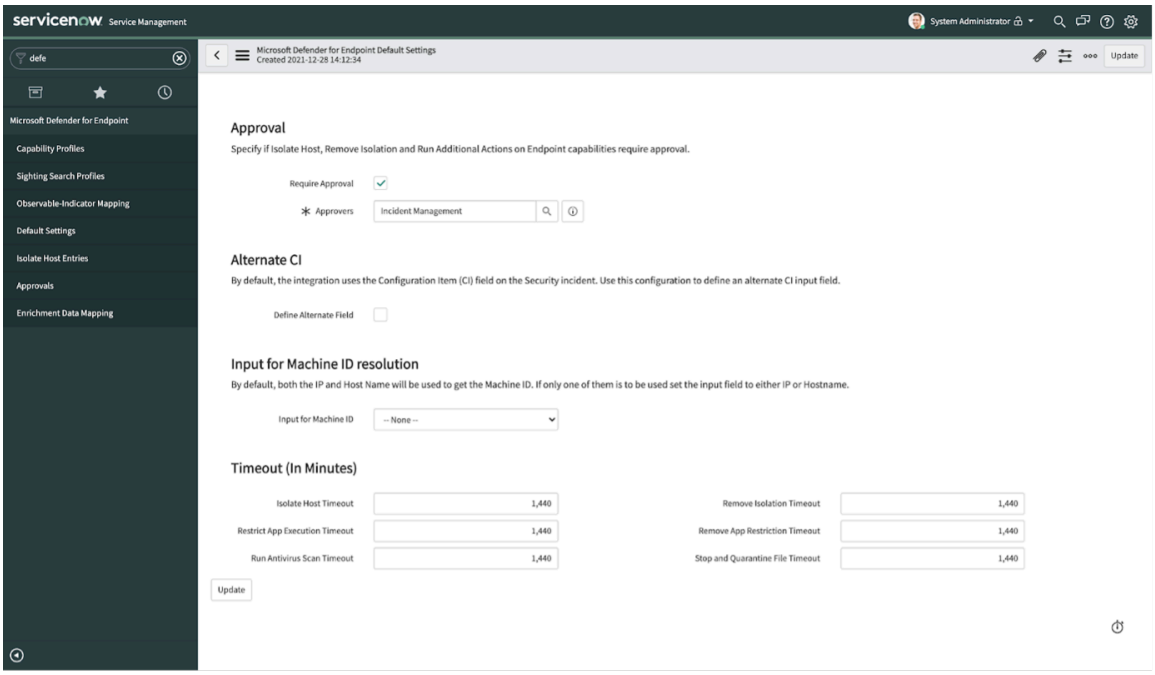
- [承認]：この承認は、特に、[ホストを隔離]、[ホスト隔離削除]、さらに [アプリの実行を制限]、[アプリ制限を削除]、および [ウイルス対策スキャンを実行] などの追加アクションに対するものです。この承認は、アクションが関連リストから直接トリガーされ、既存のプロファイルがない場合にのみ使用できます。これらの機能の既存のプロファイルがある場合、プロファイルの承認構成が優先されます。
  - [承認が必要]：[承認が必要] を有効にすると、フォームで [承認者] フィールドが使用可能になります。
  - [承認者]：承認者グループのリスト。要求が送信された後、要求を完了するにはグループからの承認が必要です。
- [代替 **CI**]：このチェックボックスを有効にすると、代替 CI を機能に渡すために使用できるフィールドのリストが表示されます。デフォルトでは、統合はセキュリティインシデントの構成アイテム (CI) フィールドを使用します。この構成は、[エンドポイントで他のアクションを実行] 機能にのみ適用されます。この構成は、[エンドポイントで他のアクションを実行] 機能のみの代替 CI 入力フィールドを定義するために使用します。その他の機能については、プロファイルセクションの設定を使用します。プロファイルで代替 CI が定義されていない場合、機能は [セキュリティインシデント] フォームの [CI] フィールドを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [エージェント **ID** 解決の入力 **(Input for Agent ID resolution)]**：デフォルトでは、IP とホスト名を使用してエージェント ID を取得します。いずれか一方のみを使用する場合は、入力フィールドを [IP] または [ホスト名] に設定します。
- [タイムアウト]：
  - [ホスト隔離のタイムアウト] (分)：[ホスト隔離] 機能の実行しきい値を示します。
  - [隔離解除のタイムアウト] (分)：[隔離解除のタイムアウト] 機能の実行しきい値を示します。
  - [アプリ実行の制限のタイムアウト] (分)：[アプリの実行を制限] 機能の実行しきい値を示します。
  - [アプリ制限の解除のタイムアウト] (分)：[アプリ制限を削除] 機能の実行しきい値を示します。
  - [ウイルス対策スキャン実行のタイムアウト] (分)：[ウイルス対策スキャンを実行] 機能の実行しきい値を示します。
  - [ファイルの停止と隔離のタイムアウト] (分)：[ファイルの停止と隔離] 機能の実行しきい値を示します。

デフォルト設定



Microsoft Defender for Endpoint インジケータータイプのマッピング

ServiceNow 観測事象タイプを Microsoft Defender for Endpoint インジケータータイプとマッピングします。このマッピングは、Microsoft Defender の [観測事象の拡張] および [インジケーターを作成] アクションで使用されます。

始める前に

必要なロール：sn_si.admin または sn_si.analyst (読み取り専用)

このタスクについて

観測事象タイプがインジケータータイプにマッピングされていないシナリオでは、そのような観測事象は Microsoft Defender for Endpoint での観測事象の拡張およびインジケーターの作成の対象になりません。

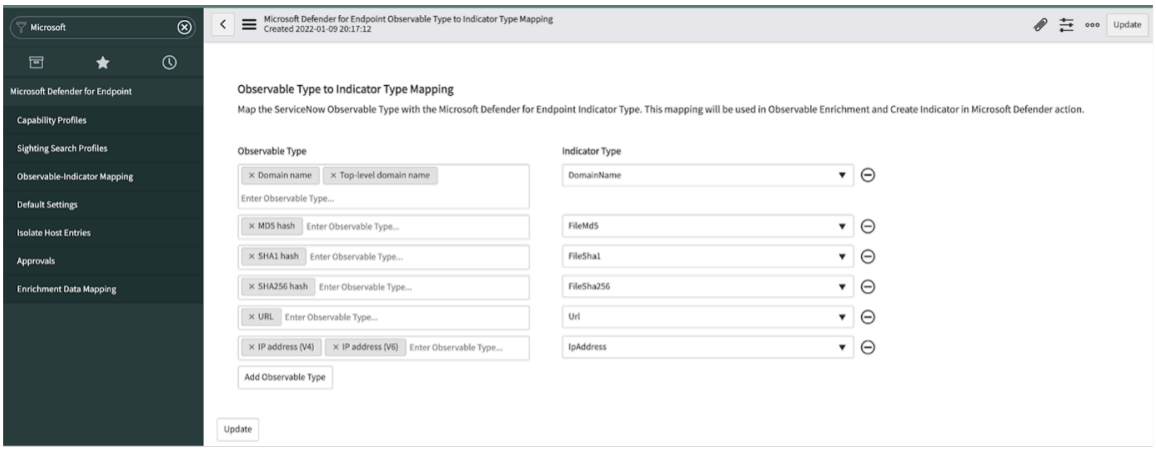
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **Microsoft Defender for Endpoint** > 観測事象からインジケーターへのマッピング.

観測事象からインジケーターへのマッピング



2. 次のいずれかの方法で、観測事象タイプを追加または更新します。
   - 新しいマッピングを追加するには、[観測事象タイプを追加 **(Add Observable Type)]** をクリックします。
   - 観測事象からインジケータータイプへのマッピングを更新するには、既存の行をクリックします。
3. マッピングを保存するには、[更新] をクリックします。

Microsoft Defender for Endpoint 統合の機能プロファイルの作成

プロファイルを作成し、そのプロファイルで実行する Microsoft Defender for Endpoint 機能を選択します。

始める前に

必要なロール：sn_si.admin

このタスクについて

プロファイルを作成して機能が結合またはグループ化され、アナリストが簡単に調査や修復を行うのに役立ちます。プロファイルに次の機能を追加できます。

- ホストの詳細を取得
- ログオンユーザーを取得
- ホストを隔離
- 隔離を削除

プロファイルの作成中に、[ホストの隔離] および [ホスト隔離削除] の機能を他の機能と結合することはできません。これらの機能のプロファイルは個別に作成する必要があります。一方、[ホストの詳細を取得] 機能と [ログオンしているユーザーを取得] 機能は組み合わせて使用できます。プロファイルは個別に作成することも、必要に応じてすべてまたは一部を組み合わせて作成することもできます。

注:
プロファイルに含まれた機能は、同じソースから別のプロファイルに含めることはできません。

自動翻訳

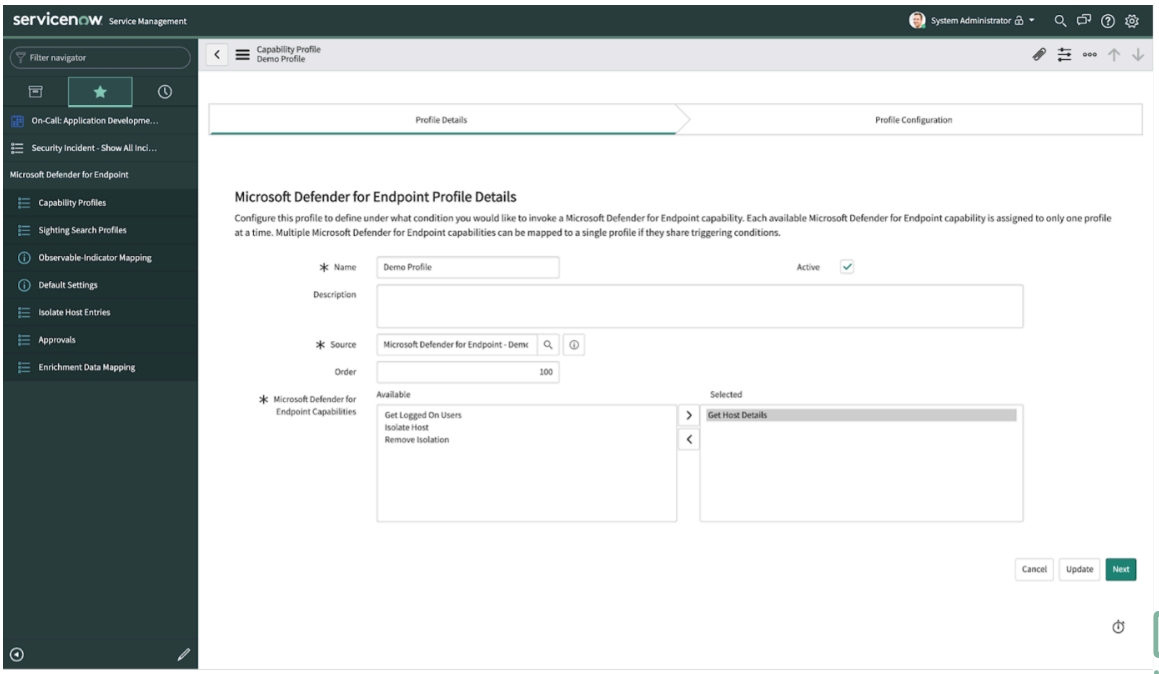
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **Microsoft Defender for Endpoint** > 機能プロファイル.

   Microsoft Defender for Endpoint の機能プロファイルリストが表示されます。

プロファイル設定



2. クリックします 新規.
3. フォームのフィールドに入力します。

機能プロファイルフォーム

フィールド	説明
名前	Microsoft Defender for Endpoint 機能プロファイルの名前。この名前は、プロファイルタイプを識別して説明するのに役立ちます。
説明	プロファイルをさらに説明する、プロファイルに関する追加情報。
ソース	Microsoft Defender for Endpoint ソースの名前。リストからは、設定されたソースのみを使用できます。
Microsoft Defender for Endpoint の機能	Microsoft Defender for Endpoint プロファイルの機能。このプロファイルの機能を [利用可能] 列から選択し、それを [選択済み] 列に移動します。
順序	フロー優先度。デフォルトは 100 です。このフィールドの値は、2 つ以上のプロファイルがトリガー条件を共有する場合にフローが実行される順序を示します。 番号が最も小さいフローの優先度が最も高くなります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	操作の順序を設定するには、値を入力します。例：100、200、300、400。
アクティブ	プロファイルがアクティブであることを示すオプション。プロファイルがアクティブになると、構成で指定したフィルター条件に一致するセキュリティインシデントが作成されたときに、自動的にトリガーされます。

4. プロファイル構成に進むには、次をクリックします 次.

次のタスク

次のステップは、プロファイルを設定することです。プロファイルの設定を構成する前に、プロファイルの構成方法とトリガー条件を確認することをお勧めします。詳細については、「構成アイテムにおける条件のトリガー」を参照してください。

構成アイテムにおける条件のトリガー

プロファイルを作成し、そのプロファイルで実行する Microsoft Defender for Endpoint 機能を選択したら、一連の特定の条件が満たされた場合にのみプロファイルが実行されるようにプロファイル設定を構成します。

構成アイテムにおける条件のトリガー方法

トリガー条件を設定して、トリガー条件に一致するセキュリティインシデントが作成されるたびにプロファイルが自動的に実行されるようにすることができます。トリガー条件が設定されていない場合は、セキュリティインシデントの [EDR プロファイルを実行] フォームをクリックしてプロファイルを選択することで、これらのプロファイルを手動で実行できます。

デフォルトでは、統合はセキュリティインシデントの構成アイテム (CI) フィールドを使用します。この値は、資産の ID を Now Platform 構成管理データベース (CMDB) に格納されている情報と照合するために使用されます。セキュリティインシデントが作成され、プロファイルが自動または手動で実行されると、CI フィールドの値に基づいて CMDB が検索され、ホスト名や IP アドレスが取得されます。ホスト名や IP は、Microsoft Defender for Endpoint でエージェント ID を解決してエンドポイントを識別するために使用されます。

理想的なシナリオでは、一致する値がデータベースで見つかり、一致する資産に関して Microsoft Defender for Endpoint コンソールからデータが収集されます。さまざまな機能のデータが Now Platform 構成管理データベース (CMDB) インスタンスにプルされ、セキュリティインシデントの関連リストに表示されます。セキュリティインシデントの構成アイテム (CI) フィールドにホスト名、またはデータベースと一致する IP アドレスが入力されていない場合は、セキュリティインシデントでホスト名または IP のいずれかを含む代替フィールドを選択して、エージェント ID の解決を実行できます。

プロファイルセットアップの構成手順では、エンドポイント識別用の代替 CI フィールドを選択して、Microsoft Defender for Endpoint でエンドポイントを識別できるようにすることができます。作成したカスタムフィールドを含む、セキュリティインシデントの任意のフィールドを代替 CI トリガーフィールドとして選択できます。この代替 CI フィールドをバックアップとして選択することで、インシデントの作成時に CI フィールドが設定されていない場合でもプロファイルが実行されるようにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
代替 CI フィールドは、プロファイルに追加できる機能に対してのみ考慮されます。これらの機能には、[ホストの詳細を取得]、[ログオンユーザーを取得]、[ホストを隔離]、および [隔離を削除] が含まれます。すべての追加アクションでは、[デフォルト設定] モジュールから代替 CI が構成される必要があります。

Microsoft Defender for Endpoint統合のためのプロファイルとセキュリティインシデントの構成

プロファイルを作成し、そのプロファイルで実行する Microsoft Defender for Endpoint 機能を選択します。定義された条件でのみプロファイルがトリガーされるように設定を構成する必要があります。

始める前に
必要なロール：sn_si.admin、sn_si.analyst (読み取り専用)

このタスクについて
指定した条件が満たされた場合にのみ実行されるように機能プロファイルを構成します。必要に応じて構成アイテム (CI) フィールドの代替入力フィールドを選択し、トリガー条件を満たすセキュリティインシデントが作成されたときにプロファイルが自動的にトリガーされるようにフィルタリング条件を設定できます。

注:
[プロファイルの詳細] ページを入力した後にのみ、[プロファイル設定] ページに移動できます。

手順

1. 次のように移動する。 **Microsoft Defender for Endpoint** > 機能プロファイル.
2. [プロファイルの詳細] セクションを完了したら、 次.
   セクションを確認して構成します。
3. [インシデント基準の定義] ([自動化] 内) セクションで、プロファイルで Microsoft Defender for Endpoint 機能を自動的にトリガーするように [インシデント基準の定義] オプションを選択します。
   [インシデント基準の定義] ([自動化] 内)：プロファイルに対して Microsoft Defender for Endpoint 機能を自動的にトリガーするセキュリティインシデント条件を定義します。[インシデント基準の定義] オプションを選択しない場合、プロファイルと基盤となる機能はセキュリティインシデントから手動で呼び出すことができます。

   注:
   [ホストを隔離] および [ホスト隔離削除] 機能は自動的にトリガーされません。

   a. [フィルター条件] で、必要なフィールドを選択します。
   b. [新しい基準] を追加し、**OR** または **AND** 条件も定義します。
4. [承認] セクションで、[承認が必要] チェックボックスをオンにして、追加レベルの制御を提供します。

   このオプションを選択すると、ホストマシンの隔離、ネットワークへの復元、ファイルの取得で Microsoft Defender for Endpoint の機能を使用してより詳細に制御できます。

   プロファイル構成の [承認] オプションは、[ホストを隔離] および [ホスト隔離削除] 機能に対してのみ表示されます。
5. [追加の構成] セクションで [代替フィールドを定義 **(Define Alternative Field)]** オプションを選択して、代替入力フィールドを定義します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[追加の構成]：セキュリティインシデントの構成アイテム (CI) フィールドにホスト名、またはデータベースと一致する IP アドレスが入力されていない場合は、セキュリティインシデントで代替フィールドを選択して、Microsoft Defender for Endpoint API をクエリできます。

> **注:**
> 詳細については、「構成アイテムにおける条件のトリガー」を参照してください。

a. [代替フィールドを定義 **(Define Alternative Field)]** オプションを選択します。

b. から入力フィールドを選択 代替 **CI** トリガーフィールド.

6. [タグ] セクションで、[タグを表示] チェックボックスをオンにしてセキュリティインシデントのタグ付けを有効にします。タグを有効にすると、プロファイル名がプリフィックスとして付きます。

   オプションで、プロファイル開始、プロファイル完了、およびプロファイル失敗のタグをセキュリティインシデントにタグ付けできます。デフォルトでは、このオプションはすべてのプロファイルでオフになっています。

7. クリックします 完了.

トリガー条件フィルターの確認

プロファイルを検証し、構成したトリガー条件フィルターが想定どおりに機能することを確認します。

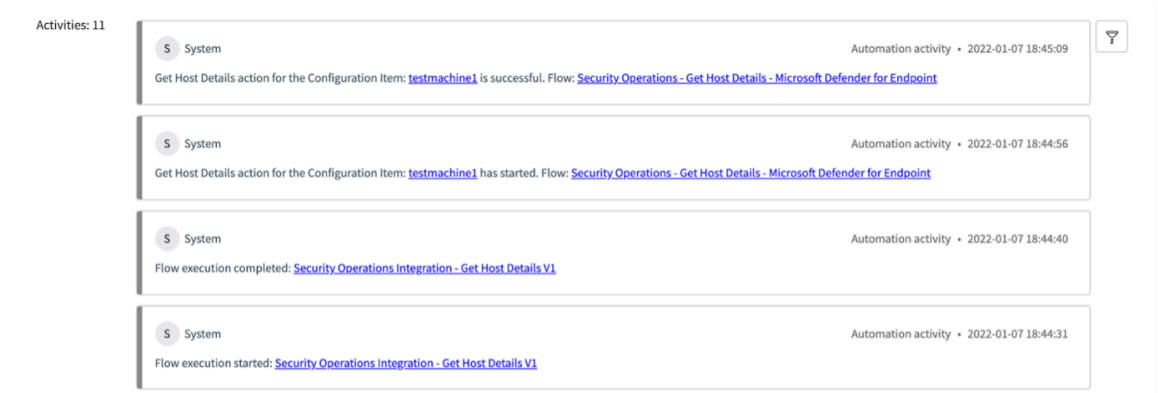
始める前に
必要なロール：sn_si.admin または sn_si.analyst

このタスクについて
構成されたトリガー条件に基づいてプロファイルをアクティブ化すると、Now Platform® セキュリティインシデントのクエリ結果を表示できます。

手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. 新しいセキュリティインシデントを作成するには、次を選択します 新規.
3. それぞれのプロファイルをトリガーするには、機能プロファイルで指定されたフィルター条件を指定します。
4. クリックします **Save** (保存).
5. 作業メモとアクティビティセクションを検証するには、プロファイル開始、プロファイル完了、またはプロファイル失敗のタグが付けられたレコードを表示して確認します。

作業メモとアクティビティ



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. 関連リスト内のすべてのデータを検証するには、[すべての関連リストを表示] をクリックします。
7. 任意の [関連リスト] タブをクリックして詳細を検証します。
   たとえば、[ホストの詳細] です。

関連リンクから **Microsoft Defender for Endpoint** 機能のトリガー

関連リンクからセキュリティインシデントを確認した後、機能プロファイルを手動でトリガーします。

始める前に
必要なロール：sn_si.admin または sn_si.analyst

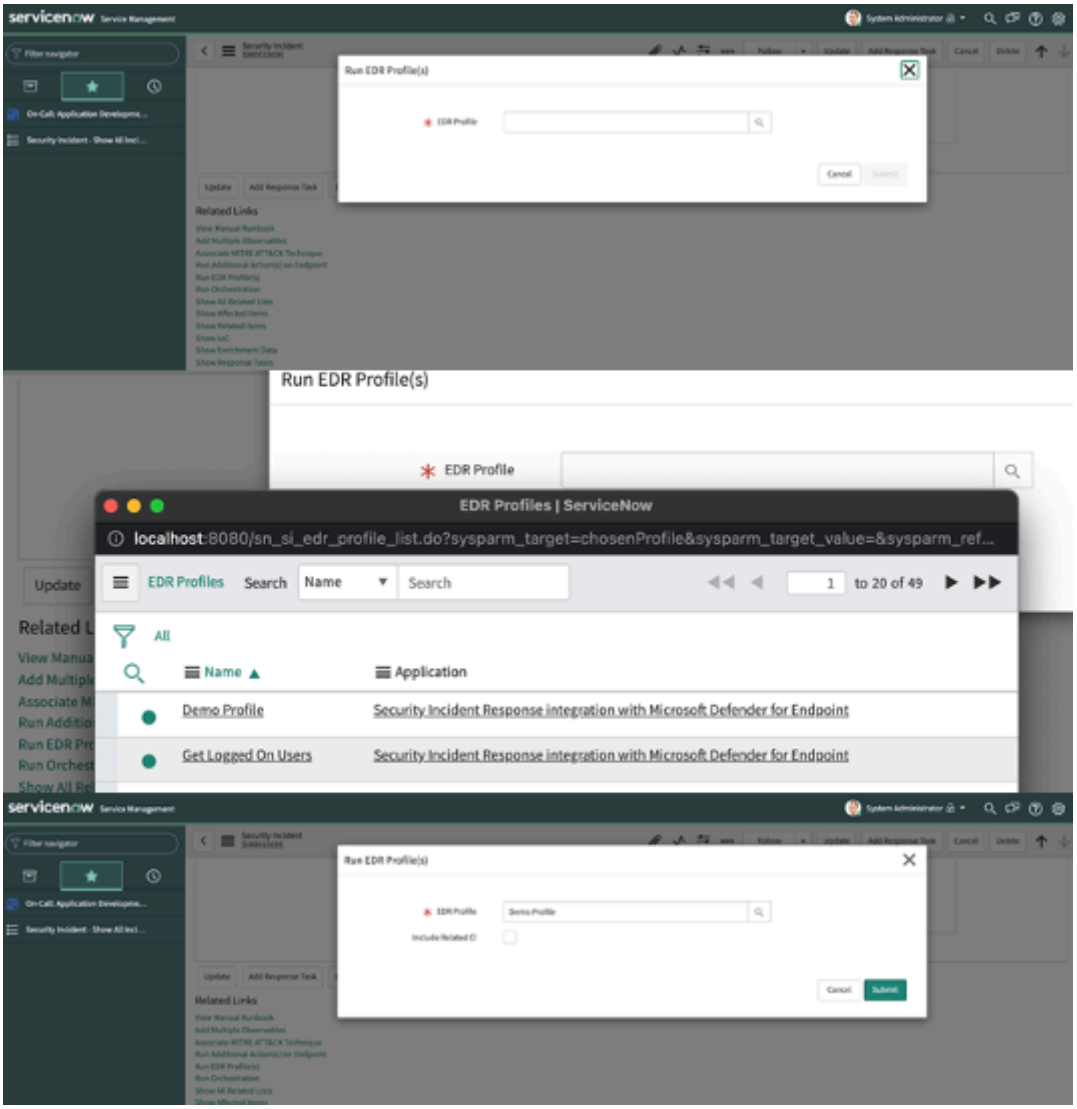
このタスクについて
セキュリティインシデントの CI または代替 CI のプロファイルを実行することに加えて、ダイアログボックスの [関連 **CI** を含める **(Include Related CI)]** を選択して、構成アイテム関連リストに存在する CI 値のプロファイルを実行することもできます。これにより、関連リストに存在する CI 値のデータも取得されます。または、関連リストに存在する CI 値に対してのみプロファイルを実行することもできます。

手順
1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. Microsoft Defender for Endpoint 情報で確認するセキュリティインシデントを選択します。
3. [関連リンク] セクションで、**[EDR** プロファイルを実行] をクリックします。
4. 利用可能なプロファイルのリストからプロファイルを参照して選択し、[送信] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロファイルを選択します。



選択したプロファイルは手動でトリガーされます。

5. 作業メモセクションとアクティビティセクションを検証します。
6. タグを表示し、関連リストでデータを検証します。

構成アイテム関連リストから **Microsoft Defender for Endpoint** のトリガー

構成アイテム関連リストから機能プロファイルを手動でトリガーします。

始める前に
必要なロール：sn_si.admin または sn_si.analyst

手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. Microsoft Defender for Endpoint 情報で確認するセキュリティインシデントを選択します。
3. クリックします すべての関連リストを表示.
4. [構成アイテム] 関連リストをクリックします。
5. 追加した構成アイテムを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. 選択した行の [アクション] から、機能を選択します。
   選択した機能は手動でトリガーされます。
7. 作業メモセクションとアクティビティセクションを検証します。
8. タグを表示し、関連リストでデータを検証します。

Microsoft Defender for Endpoint の追加の構成

Microsoft Defender for Endpoint 統合は、標準アクション以外に追加アクションの実行をサポートしています。

Microsoft Defender for Endpoint は次の追加構成をサポートしています。

Microsoft Defender for Endpoint の [ホストを隔離] 機能の構成

攻撃の重大度に基づいて、Microsoft Defender for Endpoint 内のネットワークへのアクセスからホストを隔離します。ホストをネットワークから隔離することで、他のホストに対する悪意のあるアクティビティや潜在的な攻撃を防ぐことができます。

始める前に
必要なロール：sn_si.admin または sn_si.analyst

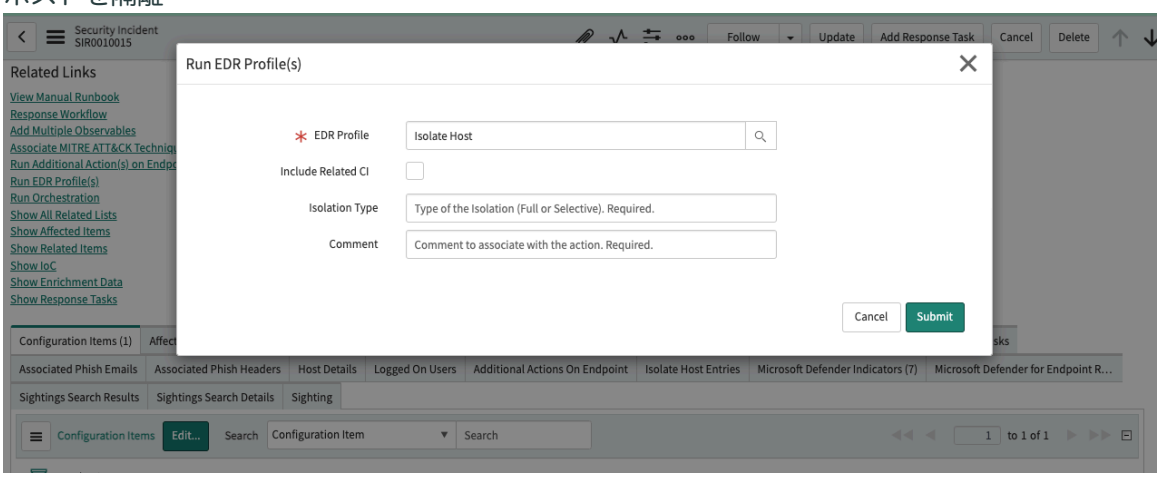
[ホストを隔離] 機能の要件

機能	必須	説明
ホストを隔離	隔離タイプ	(必須) 隔離のタイプ ([完全] または [選択的 (Selective)])。
	コメント	(必須) アクションに関連付けるコメント。

手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. Microsoft Defender for Endpoint 情報で確認するセキュリティインシデントを選択します。
3. [関連リンク] セクションで、**[EDR** プロファイルを実行] をクリックします。
4. 利用可能なプロファイルのリストから [ホストを隔離] 機能が選択されているプロファイルを参照して選択し、[送信] をクリックします。

ホストを隔離



または、次の手順を実行できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

a. 関連リストセクションの [すべての関連リストを表示] をクリックします。

b. [構成アイテム] 関連リストをクリックします。

c. [ホストを隔離] を選択し、対応する機能を選択します。

5. 自動化アクティビティとアクティビティセクションを検証し、データが予想どおりであることを確認します。
6. データを表示し、関連リストの隔離されたホストの詳細を検証します。

Microsoft Defender for Endpoint の [ホスト隔離削除] 機能の構成

必要に応じて、Microsoft Defender for Endpoint で以前にネットワークから隔離されたホストの隔離を削除します。他のホストに対する悪意のあるアクティビティや潜在的な攻撃を防ぐことができます。

始める前に

[隔離を削除] 機能の要件

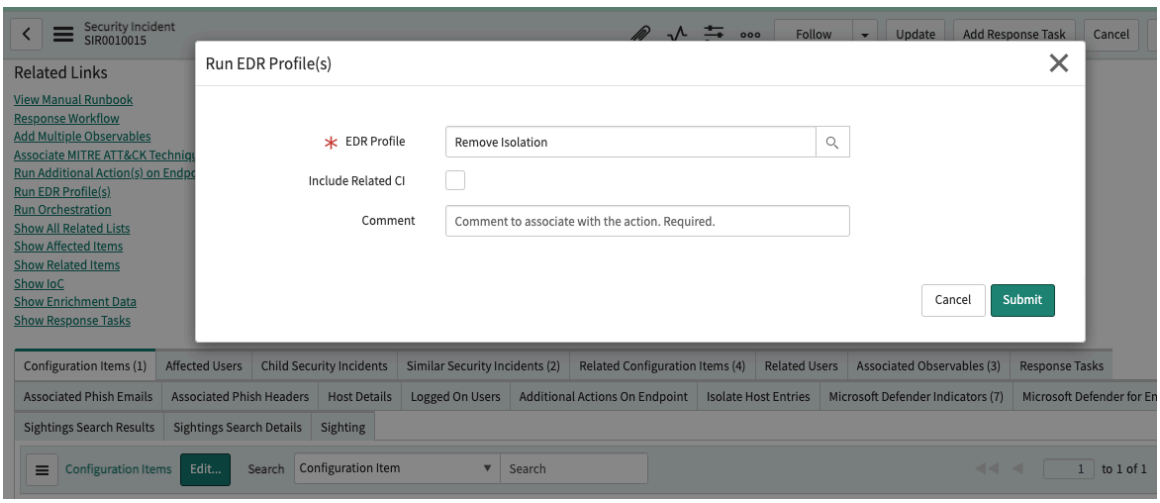
機能	必須入力	説明
隔離を削除	コメント	(必須) アクションに関連付けるコメント。

必要なロール：sn_si.admin または sn_si.analyst

手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. Microsoft Defender for Endpoint 情報で確認するセキュリティインシデントを選択します。
3. [関連リンク] セクションで、**[EDR** プロファイルを実行] をクリックします。
4. 利用可能なプロファイルのリストから [隔離を削除] 機能が選択されているプロファイルを参照して選択し、[送信] をクリックします。

隔離を削除



または、次の手順を実行できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. 関連リストセクションの [すべての関連リストを表示] をクリックします。

b. [構成アイテム] 関連リストをクリックします。

c. [隔離を削除] を選択し、対応する機能を選択します。

5. 自動化アクティビティとアクティビティセクションを検証します。

6. データを表示し、関連リストの隔離されたホストの詳細を検証します。

7. 実行の自動化アクティビティを検証します。

Microsoft Defender for Endpoint の [ウイルス対策スキャンを実行] 機能の構成

ウイルス対策スキャンをリモートで開始し、侵害されたデバイスに存在する可能性があるマルウェアを特定して修復できます。調査または対応プロセスの一部としてスキャンを実行します。

始める前に
必要なロール：sn_si.admin または sn_si.analyst

[ウイルス対策スキャンを実行] 機能の要件

入力	説明
スキャンタイプ	(必須) スキャンのタイプ ([完全] または [クイック])。
コメント	(必須) アクションに関連付けるコメント。

手順

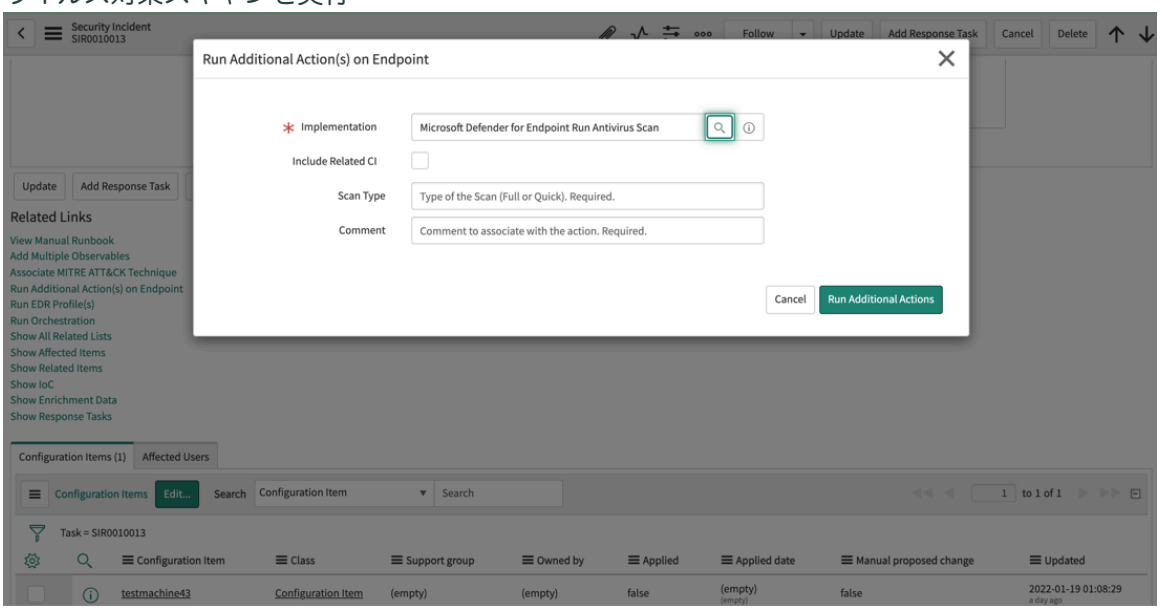
1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.

2. Microsoft Defender for Endpoint 情報で確認するセキュリティインシデントを選択します。

a. 関連リンクセクションで、 エンドポイントで他のアクションを実行.

b. 必要な機能を参照して選択します。
たとえば、[ウイルス対策スキャンを実行] 機能をクリックします。

ウイルス対策スキャンを実行



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

または、次の手順を実行できます。

a. 関連リストセクションの [すべての関連リストを表示] をクリックします。

b. [構成アイテム] 関連リストをクリックします。

c. 追加した構成アイテムを選択し、[選択した行のアクション] から、[エンドポイントで他のアクションを実行] を選択します。

[ウイルス対策スキャンを実行] 機能の実装を選択すると、[追加のスキャンタイプ **(Additional Scan Type)]** および [コメント入力 **(Comment input)]** フィールドが表示されます。

3. 実行する [スキャンタイプ] ([クイック] または [完全]) を選択し、スキャンを実行する前にコメントを追加します。
4. ウイルス対策スキャンを開始するには、[他のアクションを実行] をクリックします。
5. 実行の自動化アクティビティを表示し、検証します。
6. [エンドポイントでの追加アクション] 関連リストでアクションのステータスを検証します。

Microsoft Defender for Endpoint の [アプリの実行を制限] 機能の構成

攻撃を封じ込めるには、デバイスを制限またはロックし、悪意のある可能性があるプログラムが実行されないようにします。

始める前に

[アプリの実行を制限] 機能の要件

入力	説明
コメント	(必須) アクションに関連付けるコメント。

必要なロール：sn_si.admin または sn_si.analyst

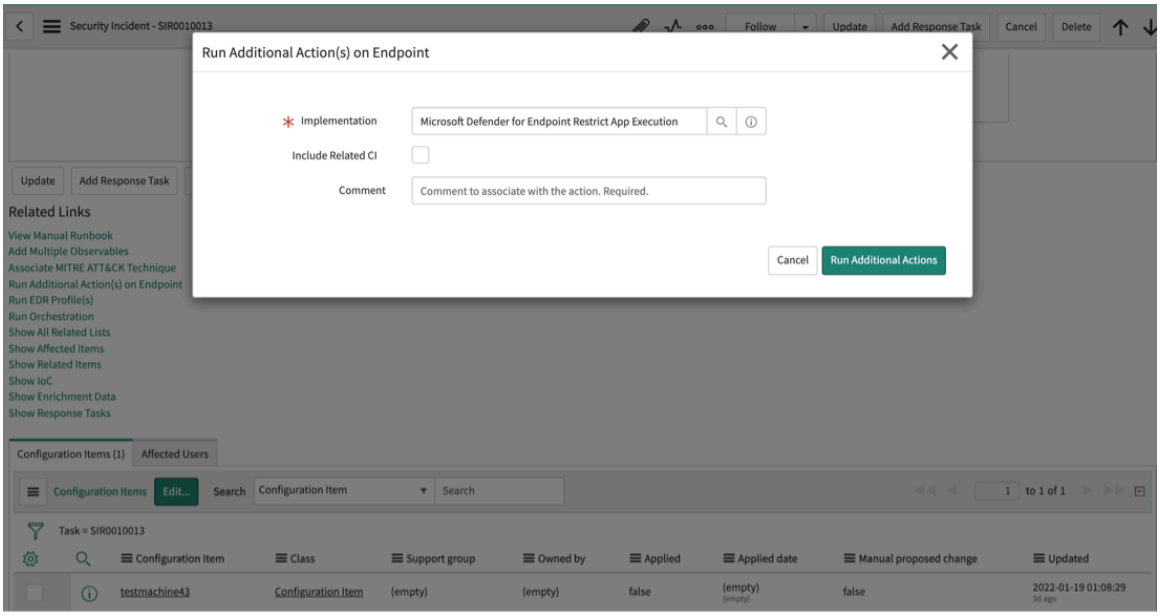
手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. Microsoft Defender for Endpoint 情報で確認するセキュリティインシデントを選択します。
   a. 関連リンクセクションで、 エンドポイントで他のアクションを実行.
   b. [アプリの実行を制限] 機能を参照して選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリの実行を制限



または、次の手順を実行できます。

a. 関連リストセクションの [すべての関連リストを表示] をクリックします。

b. [構成アイテム] 関連リストをクリックします。

c. 追加した構成アイテムを選択します。

d. [選択した行のアクション] から、[エンドポイントで他のアクションを実行] を選択します。

3. マシンで [アプリの実行を制限] を有効にするには、[他のアクションを実行] をクリックします。

4. 実行の自動化アクティビティを表示し、検証します。

5. [エンドポイントでの追加アクション] 関連リストでアクションのステータスを検証します。

自動翻訳

Microsoft Defender for Endpoint の [アプリ制限を削除] 機能の構成

必要に応じて、デバイス上のアプリケーションの制限を削除します。

始める前に

必要なロール：sn_si.admin または sn_si.analyst

[アプリ制限を削除] 機能の要件

入力	説明
コメント	(必須) アクションに関連付けるコメント。

手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.

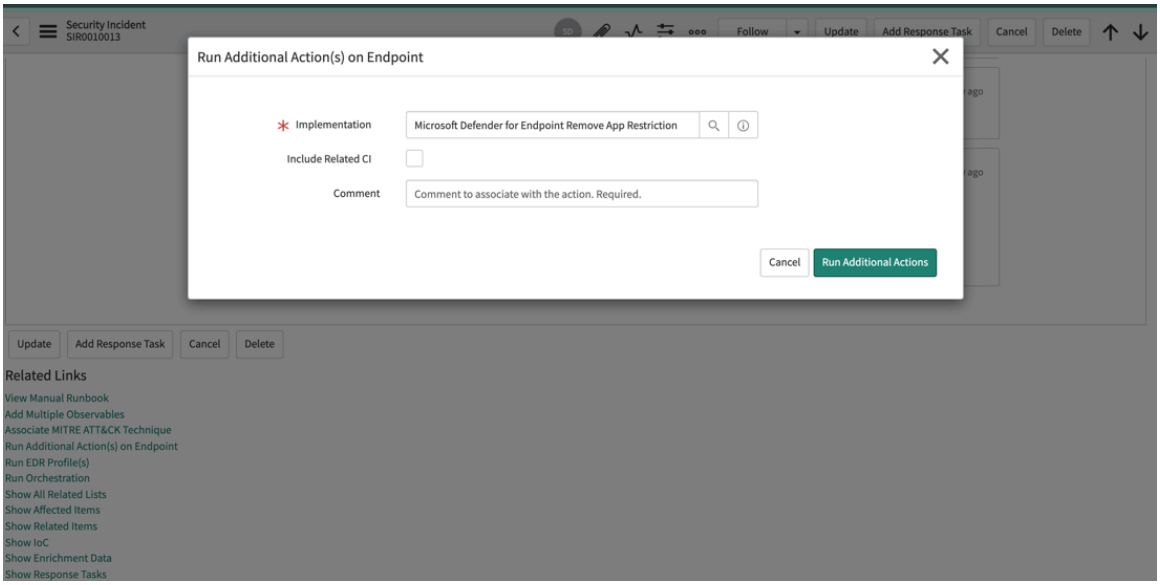
2. Microsoft Defender for Endpoint 情報で確認するセキュリティインシデントを選択します。

a. 関連リンクセクションで、 エンドポイントで他のアクションを実行.

b. [アプリ制限を削除] 機能を参照して選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリ制限を削除



または、次の手順を実行できます。

a. 関連リストセクションの [すべての関連リストを表示] をクリックします。

b. [構成アイテム] 関連リストをクリックします。

c. 追加した構成アイテムを選択します。

d. [エンドポイントで他のアクションを実行] を選択します。
[追加コメント] 入力フィールドが表示されます。

3. アプリ制限を削除するには、[他のアクションを実行] をクリックします。

4. 実行の自動化アクティビティを表示し、検証します。

5. [エンドポイントでの追加アクション] 関連リストでアクションのステータスを検証します。

自動翻訳

Microsoft Defender for Endpoint における **[Defender** から関連マシンを取得] 機能の構成

特定の観測事象の関連マシンのリストを取得します。

始める前に

注:
サポートされている観測事象タイプ：[ドメイン名]、[SHA1 ハッシュ]、および [ユーザー名]

必要なロール：sn_si.admin または sn_si.analyst

このタスクについて

特定の観測事象にアクセスしたマシンのリストを取得できます。リストは [Microsoft Defender for Endpoint の関連マシンの詳細] テーブルに格納できます。[関連する観測事象] 関連リストから [Defender から関連マシンを取得] 機能をトリガーできます。

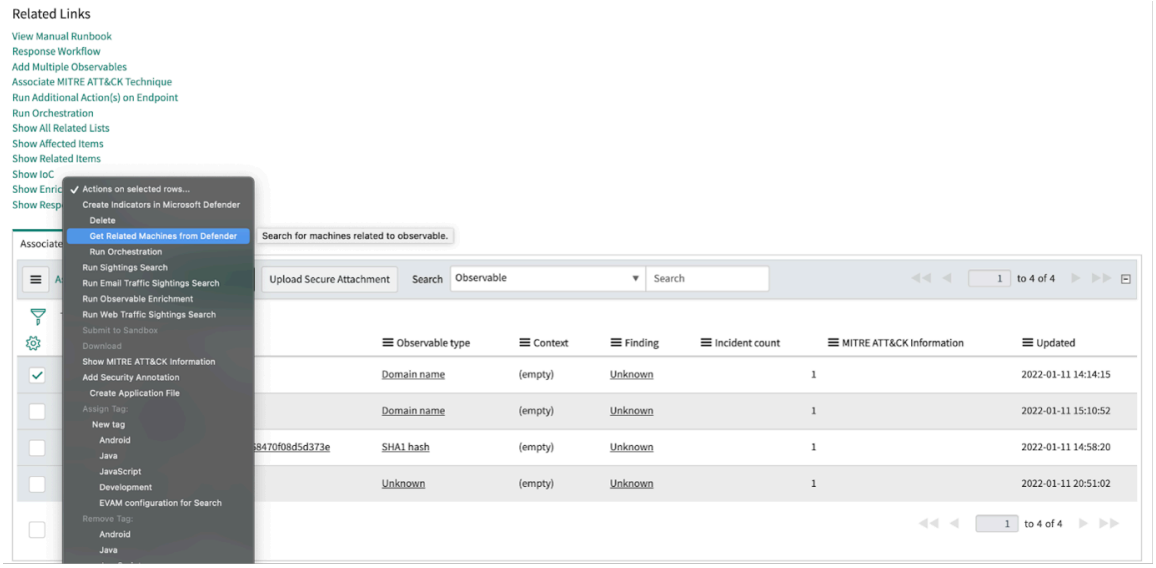
手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.

2. Microsoft Defender for Endpoint 情報で確認するセキュリティインシデントを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Defender から関連マシンを取得



3. [関連リンク] セクションで、**[IoC を表示]** をクリックします。
4. [関連する観測事象] 関連リストをクリックします。
5. 関連する観測事象を選択します。
6. [アクション] リストから、**[Defender** から関連マシンを取得] 機能を選択します。
7. 自動化アクティビティとアクティビティセクションを検証します。
8. データを表示し、関連リストの [Microsoft Defender for Endpoint の関連マシンの詳細] を確認します。
9. 実行の自動化アクティビティを表示し、検証します。

Microsoft Defender for Endpoint の [ファイルの停止と隔離] 機能の構成

Microsoft Defender プラットフォームからファイルを停止して隔離します。

始める前に
サポートされる観測事象タイプ：SHA1 ハッシュ。

[ファイルの停止と隔離] 機能の要件

入力	説明
コメント	(必須) アクションに関連付けるコメント。

必要なロール：sn_si.admin または sn_si.analyst

このタスクについて
[ファイルの停止と隔離] アクションは、SHA1 タイプの特定の観測事象に対してのみ実行できます。[エンドポイントでの追加アクション] テーブルに詳細を保存します。[ファイルの停止と隔離] 機能は、[Microsoft Defender for Endpoint の関連マシンの詳細] 関連リストからトリガーできます。

手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. Microsoft Defender for Endpoint 情報で確認するセキュリティインシデントを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. 関連リストセクションの [すべての関連リストを表示] をクリックします。
4. [Microsoft Defender for Endpoint の関連マシンの詳細] 関連リストをクリックします。
5. 1 つ以上のレコードを選択します。
6. 選択した行の [アクション] から、[ファイルの停止と隔離] 機能を選択します。
7. 自動化アクティビティとアクティビティセクションを検証します。
8. データを表示し、関連リストでデータを検証します。
9. 実行の自動化アクティビティを表示し、検証します。

Microsoft Defender for Endpoint 統合によるサイティング検索のプロファイルの作成と構成

Microsoft Defender for Endpoint を使用してサイティング検索プロファイルを自動的に作成および構成します。

始める前に
必要なロール：sn_si.admin、sn_si.admin

このタスクについて
サイティング検索ワークフローを使用して、サイティング検索を実行できます。このワークフローは、観測事象のリストを受け入れ、実装機能を検索し、サイティング検索設定に基づいてクエリを作成し、設定されたワークフローに基づいて検索を実行します。

Microsoft Defender for Endpoint は、自動サイティング検索を設定できるベースシステムのサイティング検索プロファイルを提供しています。このプロファイルを使用すると、組織の関連する観測事象サイティング情報にアクセスしたり、他の組織からのサイティングを確認したりすることもできます。

手順
1. 次のように移動する。 統合 > サイティング検索構成.
2. [**New**] をクリックします。
3. フォームで次のフィールドに入力します。

[サイティング検索構成] フォーム

フィールド	説明
名前	サイティング検索プロファイルの名前。
保存された検索	検索構成を保存するオプション。保存された検索構成クエリはサンプルクエリです。必要に応じて、自分の環境のパラメーターに置き換えて、保存された検索構成を追加で作成できます。
サイティング検索ソース	Microsoft Defender for Endpoint 統合でのサイティング検索用に構成されたソース。
検索	クエリを形成するネイティブ検索文字列。
アクティブ	保存された検索構成を有効にするオプション。アクティブな検索構成のみがサイティング検索を実行できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
観測可能タイプ	観測事象カテゴリのタイプ。たとえば、IP アドレス、ハッシュ値、URL、ドメイン名などです。
検索あたりの最大観測事象の数	検索クエリから表示できる観測事象の最大数。この統合では、この値を 1 に設定します。
サイティング検索パラメーター	指定されたログストアでサポートされているロジックやその他の演算子を含むより複雑なクエリを定義するパラメーター。

4. **[Submit]** をクリックします。

Microsoft Defender for Endpoint で手動サイティング検索を実行する

個々のまたは複数の観測事象を選択し、Microsoft Defender for Endpoint で手動サイティング検索を実行することで、脅威のまん延を時系列で見極めることができます。

始める前に
必要なロール：sn_si.admin、sn_si.analyst

このタスクについて
サポートされている観測事象タイプは次のとおりです。

- ドメイン名
- IP アドレス (V4)
- IP アドレス (V6)
- MD5 ハッシュ
- SHA1 ハッシュ
- SHA256 ハッシュ

手順

1. [セキュリティインシデント] に移動します。
2. 既存の SIR を開くか、新しい SIR を作成します。
3. [関連リンク] で、**[IoC** を表示] をクリックします。
4. [関連する観測事象] 関連リストをクリックします。
5. 観測事象を選択します。
6. [アクション] リストから、[観測事象の拡張を実行] をクリックします。
7. 観測事象を選択し、選択した行の [アクション] から [サイティング検索を実行] をクリックします。

   注:
   サイティング検索は、ドメイン名、IP アドレス (V4)、IP アドレス (V6)、MD5 ハッシュ、SHA1 ハッシュ、および SHA256 ハッシュ観測事象タイプでそれぞれサポートされています。

8. 検索の期間を指定し、[検索] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> Microsoft Defender for Endpoint は、過去 30 日間のサイティング検索のみをサポートしています。範囲クエリが過去 30 日より前の場合、サイティング検索はデータを取得しません。範囲クエリが過去 30 日と重複する場合は、過去 30 日間のサイティングのみが取得され、範囲クエリが過去 30 日以内の場合は、定義された開始時刻から現在時刻までのサイティングが取得されます。

9. 検索が完了したら、関連リストで結果と詳細を検証します。
10. [サイティング検索の詳細] をクリックして、サイティング検索の詳細を表示します。
11. 詳細については [サイティング] タブをクリックし、検索結果については [サイティング検索結果] タブをクリックします。

    特定のサイティングに関連する追加情報を [サマリー] フィールドに表示できます。

Microsoft Defender for Endpoint における観測事象の自動拡張の実行

Microsoft Defender for Endpoint で観測事象の自動拡張を実行して、さまざまなソースからの追加情報で観測事象を拡張します。

始める前に

[セキュリティインシデントレスポンス] システムプロパティが有効になっていることを確認します。このオプションは、観測事象がセキュリティインシデントに関連付けられるたびに、SIR で観測事象の拡張機能をトリガーします。

必要なロール：sn_si.admin、sn_si.analyst

このタスクについて

この機能を使用して、インシデント応答の調査中に、識別された脅威を封じ込めることができます。新しい観測事象がセキュリティインシデントに関連付けられると、Microsoft Defender for Endpoint の観測事象の拡張を自動的に実行できるようになります。

手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. Microsoft Defender for Endpoint 情報で確認するセキュリティインシデントを選択します。
3. 新しい観測事象がセキュリティインシデントに関連付けられたら、自動化アクティビティを検証します。
4. セキュリティインシデントの [インジケーター] 関連リストでエンリッチメント結果を表示します。
   観測事象の拡張の詳細については、次のテーブルを参照してください。

Microsoft Defender インジケーター

フィールド	説明
インジケーター ID	インジケーターエンティティの ID。[開く] をクリックして、Now Platform インスタンスでレコードの詳細を表示します。
観測事象	結果に関連付けられた観測事象。
タイトル	インジケーターのタイトル。
インジケータータイプ	インジケーターのタイプ。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
アクション	インジケーターによって実行されるアクション。
推奨アクション	インジケーターに対する推奨アクション。
統合ベンダー	データの取得元である Defender ソース統合。
有効期限	インジケーターの有効期限。
取得日	拡張レコードが作成された日付。

Microsoft Defender for Endpoint における観測事象の手動拡張の実行

個々のまたは複数の観測事象を選択し、手動で観測事象の拡張を行うことで、Microsoft Defender for Endpoint からの追加情報で観測事象を拡張できます。

始める前に

必要なロール：sn_si.analyst

このタスクについて

Microsoft Defender for Endpoint 統合により、[観測事象からインジケーターへのマッピング] モジュールでマッピングされているすべての観測事象タイプを拡張できます。

手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. Microsoft Defender for Endpoint 情報で確認するセキュリティインシデントを選択します。
3. [すべての関連リストを表示] をクリックします。
4. [関連する観測事象] タブをクリックします。
5. 観測事象を選択します。
6. [アクション] リストから、[観測事象の拡張を実行] をクリックします。
7. Microsoft Defender for Endpoint ソースを選択し、それを [選択済み] 列に移動して、選択した観測事象を拡張するために使用する実装を指定します。
8. **[Submit]** をクリックします。
9. 実行のステータスを検証するには、作業メモを表示します。
10. 結果を表示するには、**[Microsoft Defender** インジケーター] タブをクリックします。
    観測事象の拡張の詳細については、次のテーブルを参照してください。

Microsoft Defender インジケーター

フィールド	説明
インジケーター ID	インジケーターエンティティの ID。[開く] をクリックして、Now Platform インスタンスでレコードの詳細を表示します。
観測事象	結果に関連付けられた観測事象。
タイトル	インジケーターのタイトル。
インジケータータイプ	インジケーターのタイプ。
アクション	インジケーターによって実行されるアクション。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
推奨アクション	インジケーターに対する推奨アクション。
統合ベンダー	データの取得元である Defender ソース統合。
有効期限	インジケーターの有効期限。
取得日	拡張レコードが作成された日付。

Microsoft Defender for Endpointでのインジケーターの作成

Microsoft Defender for Endpoint を使用して、セキュリティインシデントの関連する観測事象からインジケーターを作成します。

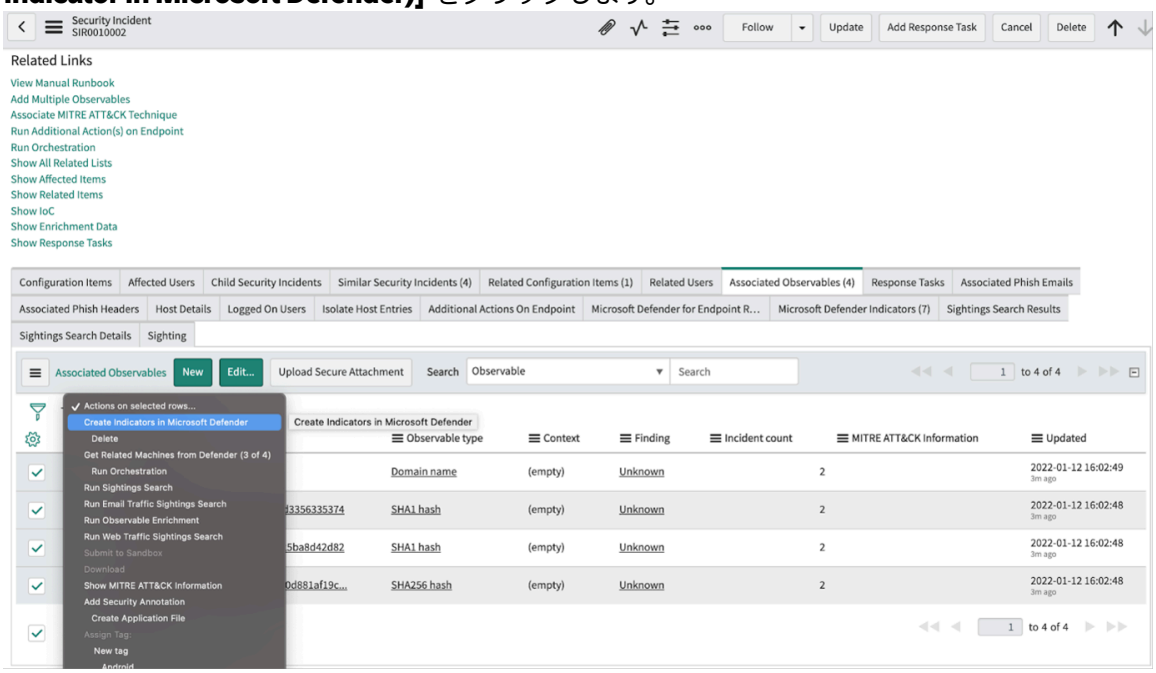
始める前に
必要なロール：sn_si.admin、sn_si.analyst

このタスクについて
Microsoft Defender for Endpoint 統合により、[観測事象からインジケーターへのマッピング] モジュールでマッピングされているすべての観測事象タイプを拡張できます。

[インジケーターを作成] では、検出、およびブロックの防止と対応のためのインジケーターのリストを設定できます。セキュリティインシデントの関連する観測事象からインジケーターを作成できます。

手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. Microsoft Defender for Endpoint でインジケーターを作成する観測事象を含むセキュリティインシデントを選択します。
3. [関連する観測事象] 関連リストをクリックします。
4. 既存の観測事象を追加するか、新しい観測事象を作成します。
5. 観測事象を選択します。
6. 選択した行の [アクション] から、**[Microsoft Defender** でインジケーターを作成 **(Create Indicator in Microsoft Defender)]** をクリックします。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

7. フォームのフィールドに入力します。

フィールド	説明
選択した観測事象 (Selected Observables)	影響を受ける観測事象。このアクションを使用して、複数の観測事象のインジケーターを作成できます。観測事象を選択解除する場合は、リストから観測事象を選択解除します。 **注:** サポートされている観測事象タイプがマッピングされていない場合、そのような観測事象のインジケーターは Microsoft Defender で作成されません。
タイトル	インジケーターのタイトル。
説明	インジケーターの説明。
有効期限	インジケーターの有効期限。
推奨アクション	インジケーターに対して実行する必要がある推奨アクション。
ソース	インジケーターを作成するための統合構成。
アクション	組織内でインジケーターが検出された場合に実行されるアクション。可能な値は次のとおりです。 ○ 警告 ○ ブロック ○ 監査 ○ **'BlockAndRemediate** ○ 許可される
アプリケーション	インジケーターに関連付けられている Microsoft Defender for Endpoint アプリケーション。このフィールドは新しいインジケーターにのみ適用され、既存のインジケーターには使用できません。
重大度	インジケーターの重大度。可能な値は次のとおりです。 ○ 低 ○ 中 ○ 高
RBAC グループ名	インジケーターが適用される RBAC グループ名。名前はカンマ区切りのリストです。

8. [インジケーターを作成] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

9. アクティビティと UI メッセージを検証します。
10. **[Microsoft Defender** インジケーター] タブをクリックして結果を表示します。

Microsoft Defender for Endpoint のインジケーターの更新

リストのコンテキストメニューから、または Microsoft Defender インジケーターのフォームビューから、Microsoft Defender for Endpoint の既存のインジケーターを更新します。

始める前に
必要なロール：sn_si.admin、sn_si.analyst

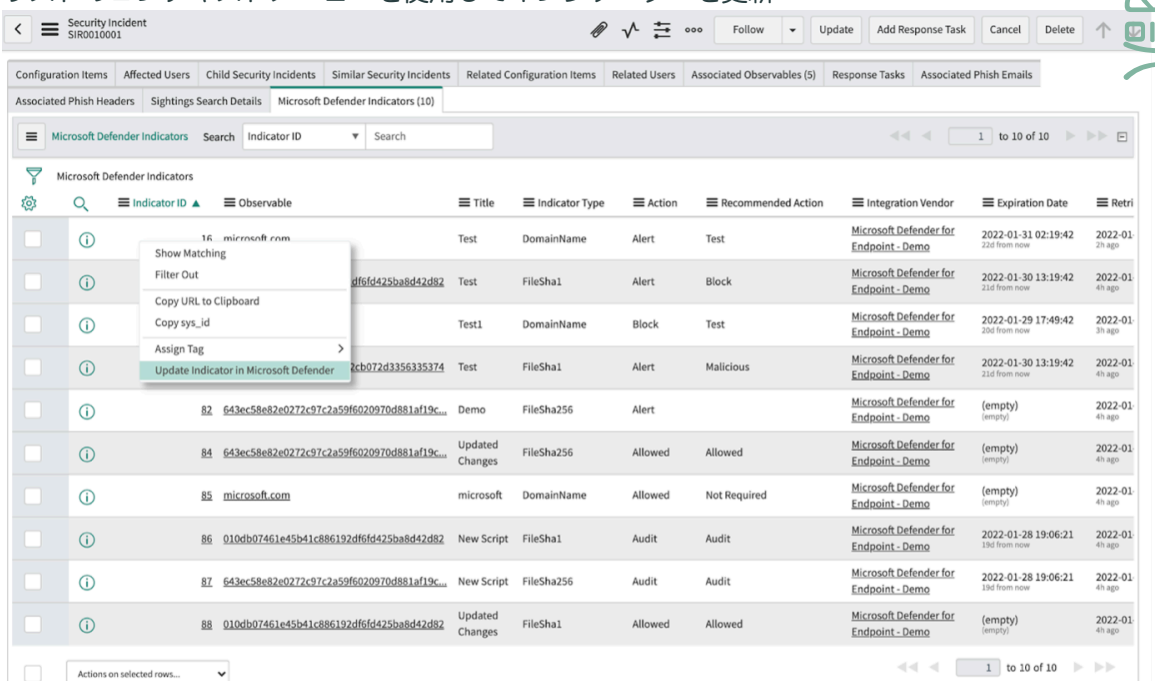
手順

1. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示.
2. [すべての関連リストを表示] をクリックし、**[Microsoft Defender** インジケーター] タブをクリックします。

> **注:**
>
> [セキュリティインシデント] 関連リストに表示される Microsoft Defender インジケーターの関連リストを構成する必要があります。詳細については、「フォーム UI アクション」を参照してください。

3. 次のいずれかの方法で、Microsoft Defender for Endpoint インジケーターを更新します。
   - リストのコンテキストメニューからインジケータを更新するには、更新するインジケータの行を選択し、**[Microsoft Defender** でインジケーターを更新 **(Update Indicator in the Microsoft Defender)]** オプションをクリックします。

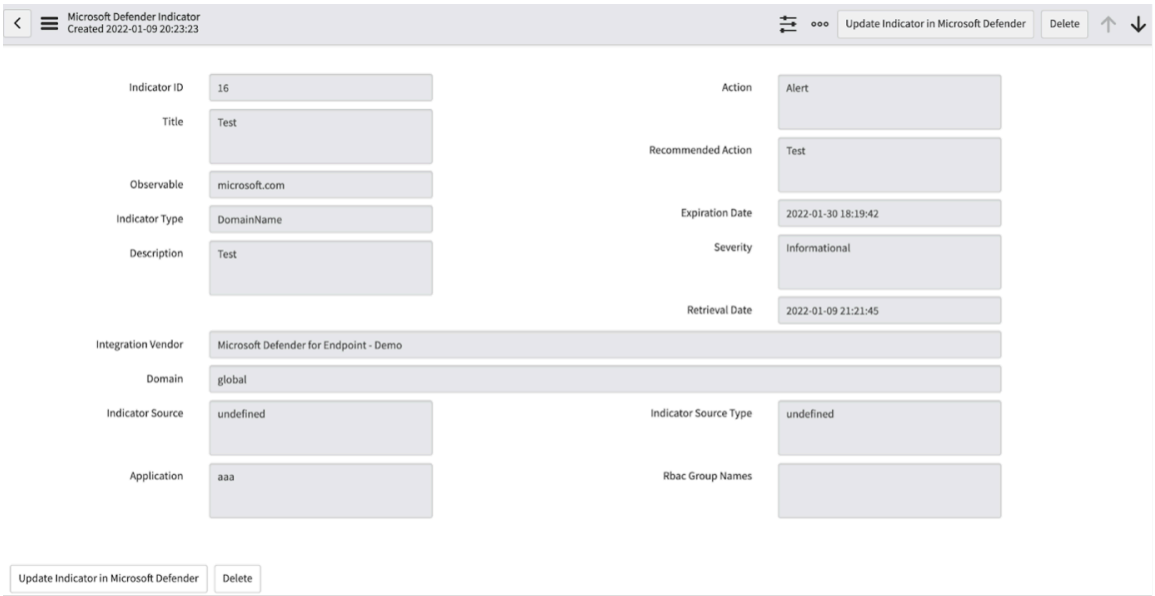
リストのコンテキストメニューを使用してインジケーターを更新



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- フォームビューからインジケーターを更新するには、フォームビューで **[Microsoft Defender でインジケーターを更新]** をクリックします。

フォームビューを使用してインジケーターを更新



4. フォームのフィールドに入力します。

Microsoft Defender インジケーターフォーム

フィールド	説明
タイトル	インジケーターのタイトル。
説明	インジケーターの説明。
有効期限	インジケーターの有効期限。
推奨アクション	インジケーターに対して実行する推奨アクション。
ソース	インジケーターを作成するための統合構成。
アクション	組織内でインジケーターが検出された場合に実行されるアクション。可能な値は次のとおりです。 ○ 警告 ○ ブロック ○ 監査 ○ **BlockAndRemediate** ○ 許可される
アプリケーション	インジケーターに関連付けられている Microsoft Defender for Endpoint アプリケーション。このフィールドは新しいインジケーターにのみ適用され、既存のインジケーターには使用できません。
重大度	インジケーターの重大度。可能な値：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ 低 ○ 中 ○ 高
RBAC グループ名	インジケーターが適用される RBAC グループ名。名前はカンマ区切りのリストです。

5. [インジケーターを更新] をクリックします。
6. アクティビティと UI メッセージを検証します。

Microsoft Defender for Endpoint 統合でのドメインセパレーション

Microsoft Defender for Endpoint 統合では、ドメインセパレーションがサポートされています。ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。その後、どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル
サポート：ベーシック

ドメインセパレーションには次の手順を使用します。

1. それぞれのドメインで sn_si.admin ロールを持つユーザーを作成します。
2. 適切なドメインで Microsoft Defender for Endpoint 統合の手順を実行します。

Microsoft Defender for Endpoint 統合のレート制限構成

API のレート制限と Microsoft Defender for Endpoint 統合のレート制限のタイムアウトを設定します。

始める前に
必要なロール：sn_si.admin、sn_si.analyst (読み取り専用)

手順
1. ナビゲーションフィルターで、「sys.properties.list」と入力します。
   システムプロパティ [sys_properties] テーブル内のプロパティの全リストが表示されます。
2. 要件に応じて、次のプロパティを検索して変更します。

プロパティ名	説明
sn_sec_defender_ep.rate_limit_timeout_in_minutes	指定された期間内に要求が実行されない場合、実行は停止され、適切なエラーメッセージが表示されます。 デフォルト値：75。
sn_sec_defender_ep.request_per_hour_limit	構成された API 呼び出しが 1 時間以内に同じエンドポイントで行われた場合、しきい値に達するか設定されたタイムアウトになるまで、要求はキューに入れられます。 デフォルト値：1500。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

プロパティ名	説明
sn_sec_defender_ep.request_per_minute_limit	構成された API 呼び出しが 1 分以内に同じエンドポイントで行われた場合、しきい値に達するか設定されたタイムアウトになるまで、要求はキューに入れられます。 デフォルト値：100。
sn_sec_defender_ep.import_indicator_request_per_minute_limit	構成された API 呼び出しが 1 分以内にエンドポイントで行われた場合、しきい値に達するか設定されたタイムアウトになるまで、要求はキューに入れられます。 デフォルト値：30。

Microsoft Exchange Online の統合

ServiceNow の Microsoft Exchange Online Integration アプリケーションの場合、 Now Platform セキュリティインシデントレスポンス (SIR) 製品は、MicrosoftOffice 365 製品スイートのクラウドベースのサービスの 1 つである Microsoft Exchange Online サービスと統合されます。Security Operation Center (SOC) アナリストは、メール検索および削除機能を使用して、会社のメール環境からセキュリティ関連の脅威を検索し、フィッシングメールを削除できます。

概要

セキュリティインシデントアナリストがセキュリティアナリストインターフェイスから統合を実行すると、ワークフローは検索条件に一致するメールメッセージの詳細を返します。メール検索は、件名、送信者や受信者のメールアドレスを含む条件に基づいています。メール検索の完了後、Microsoft Exchange Online サービスから不審なメールを削除できます。また、メールを削除する前に承認を要求するように、オプションの承認プロセスを設定できます。

このメール検索と削除の統合は、より広範なフィッシング対応インシデントワークフローまたは Runbook で使用できます。企業ユーザーまたは従業員が不審なメールを受信し、それを会社のフィッシング応答チームまたは受信ボックスに報告すると、報告されたメールが Now Platform に転送され、セキュリティインシデントとして分類されます。メールがフィッシング攻撃であることを確認した後、フィッシングインシデントの調査を担当するアナリストは、メール検索を開始して、他の企業ユーザーがこのフィッシングメールを受信したかどうかを判断できます。検索を実行することで、同じフィッシングキャンペーンからの関連メールを特定できます。また、フィッシングメールを受信して閲覧し、悪意のある URL をクリックしたり添付ファイルを開いたりした可能性がある他の被害者を特定できます。

主な機能

この統合の主な機能は次のとおりです。

- メールメッセージの送信者、受信者、件名の各フィールドの組み合わせに基づいて、 セキュリティインシデントレスポンスでフィッシング脅威の検索条件を設定します。
- 大規模で時間がかかるメール検索の場合、検索が正常に完了したときに、一致したメッセージの件数とともにセキュリティインシデントアナリストにメールで通知されます。
- 個々のメッセージのステータスから、受信者が不審なメールを閲覧したか削除したかを判断できます。
- オプションの承認プロセスを設定すると、事前の承認がないと不審なメールを削除できなくなります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 削除されたメールの件数を含む、削除要求の完全な監査記録がセキュリティインシデントの作業メモに記録されます。
- タグ付けが設定されている場合、セキュリティインシデントに関するメールの検索と削除のワークフローがいつ開始され、いつ正常に完了したかがセキュリティタグに記録されます。

サポートされている **Microsoft Exchange Online** のバージョン

この統合は、Microsoft Office 365 スイートの一部である Microsoft Exchange Online サービスをサポートしています。ホストされた Microsoft Exchange 環境はサポートされません。Microsoft は、Microsoft Exchange Online サービスを Exchange 2016 バージョンで実行しています。

必須条件

com.snc.si_dep プラグインは、どの Now Platform バージョンにも必要です。このプラグインは、セキュリティインシデントレスポンス 製品をサポートするために必要なすべての依存関係を自動的にインストールします。他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。

次の セキュリティオペレーション アプリケーションを、ServiceNow Store からインストールしてアクティブ化する必要があります。スムーズにインストールできるように、アプリケーションを次のリストの順番で、一度に 1 つずつインストールしてアクティブ化します。

1. Security Integration Framework
2. Security Support Common
3. セキュリティサポートオーケストレーション
4. セキュリティインシデントレスポンス

統合アーキテクチャとシステム接続

重要な用語や外部システム接続の詳細など、統合のアーキテクチャの詳細については、「Microsoft Exchange Online 統合の統合アーキテクチャと外部システム接続」を参照してください。

チェックリスト

次のトピックには番号が付けられています。アプリケーションのインストールと設定をスムーズに行えるように、以下のトピックを記載されている順に実行してください。

これらの手順の印刷可能なチェックリストについては、「Microsoft Exchange Online 統合のチェックリスト」を参照してください。このリストを使用して、進捗を監視しながら、統合のセットアップ、設定、結果の検証のタスクをエンドツーエンドで進めることができます。

ServiceNow Microsoft Exchange Online Integration のための **Microsoft Azure** アカウントのセットアップ

この統合のために ServiceNow アプリケーションをインストールする前に、Microsoft Azure ポータルで次のセットアップタスクを実行してください。このアカウントは、メールメッセージの詳細について Microsoft Exchange Online テナントへのアクセスを許可します。

始める前に

必要なロール：Microsoft Azure ポータルアドミン

このアカウントは、Microsoft Exchange Online テナントにアクセスして追加のメールメッセージの詳細を収集し、メールメッセージを削除するために必要です。このアカウントは、Microsoft Azure ポータルでセットアップします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

以下のタスクの画像は特権のある専有物です。Microsoft から許可を得て使用しています。このコンテンツは、Microsoft による更新の対象となります。最新のコンテンツにアクセスできることを確認するには、Microsoft ドキュメント Web サイトを参照してください。

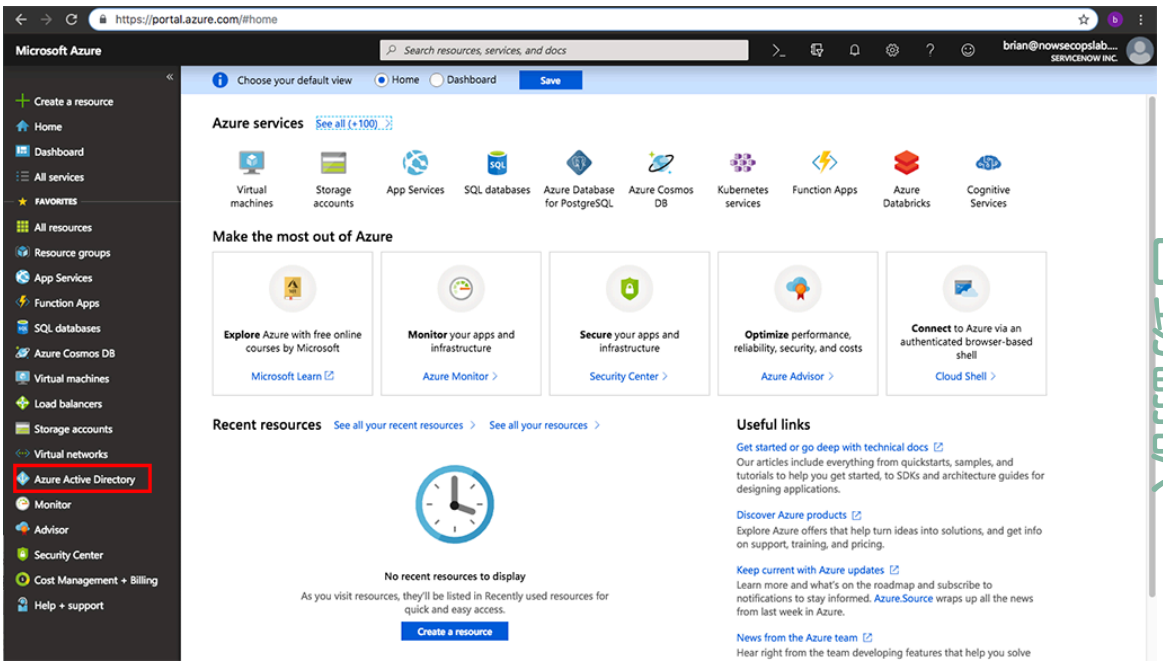
次の画像では、Azure ポータルの例のアカウント名に ServiceNow Inc. が表示されています。お使いの Azure ポータルアカウントでは、Azure ポータルの自分のアカウントの会社名が表示されます。

手順

Microsoft Azure ポータルで OAuth 認証のアプリケーション ID を作成していない場合は、次の手順に従います。

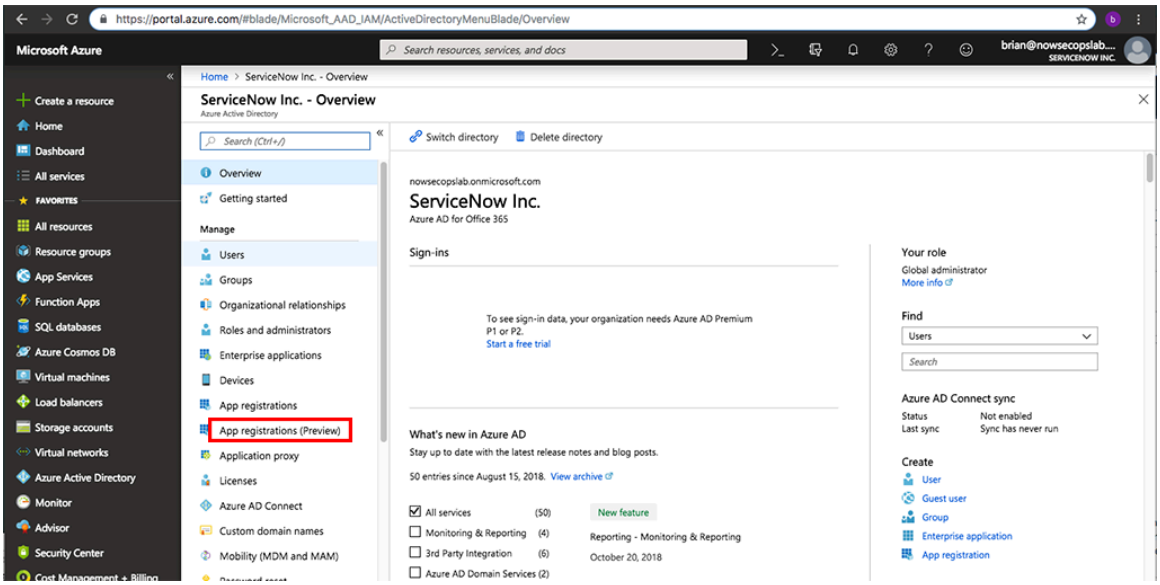
a. Azure ポータルアドミンの認証情報を使用して、Microsoft Azure ポータルにログインします。

b. 左側のナビゲーションパネルで、**[Azure Active Directory]** を選択します。

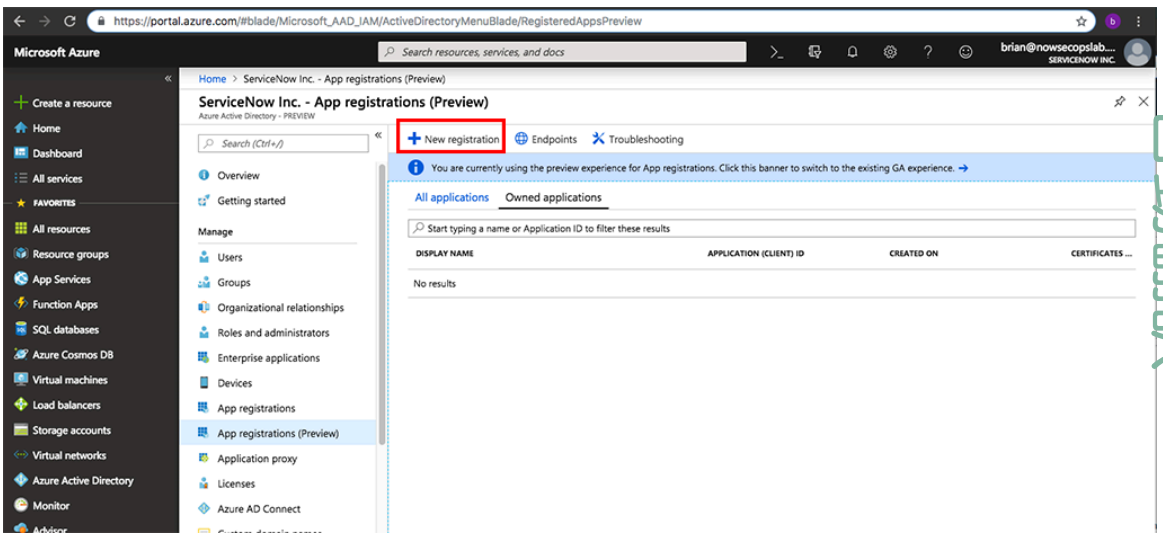


c. 表示される [概要] ペインで、[アプリの登録 (プレビュー)] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



d. 表示される [アプリの登録 (プレビュー)] ペインで、[新規登録 **(New registration)]** をクリックします。



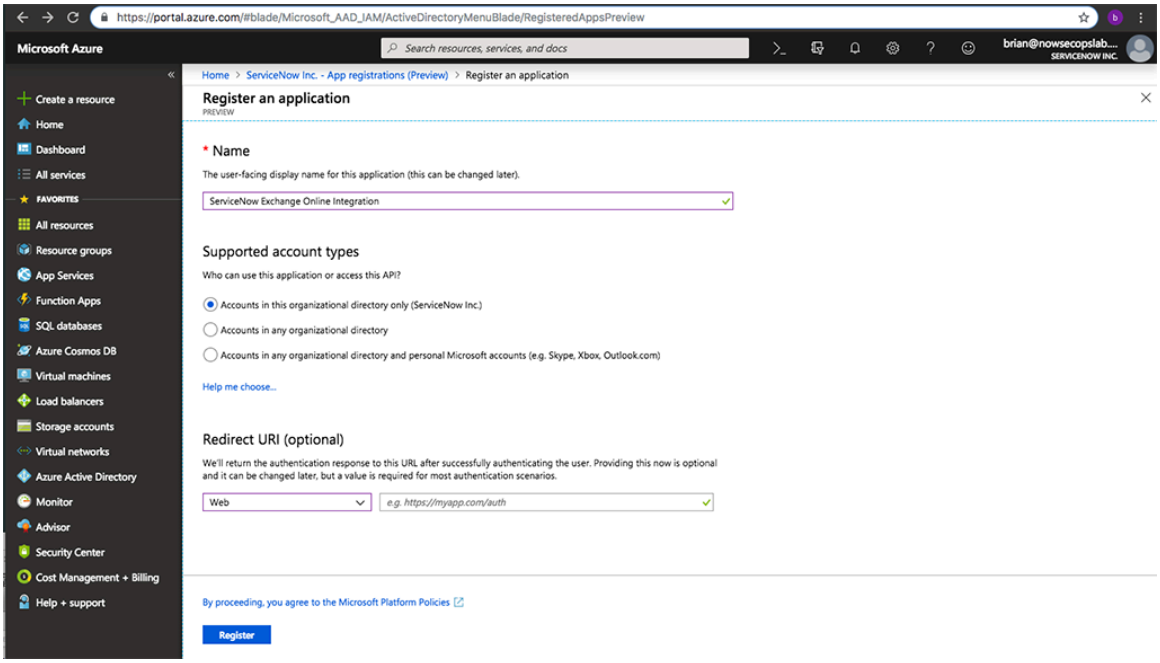
e. 表示される [アプリケーションを登録 (Register an application)] フォームに入力します。

入力したフォームの例を表の下に示します。

フィールド	説明
名前	アプリケーションの名前。この例では、「ServiceNow Exchange Online Integration」と入力されています。
サポートされているアカウントの種類	このアカウントの場合、 [サポートされているアカウントの種類] で [この組織内のディレクトリのアカウントのみ **(ServiceNow Inc.) (Accounts in this organizational directory only (ServiceNow Inc.))]** をクリックします。このドメインはメールの検索に使用されます。

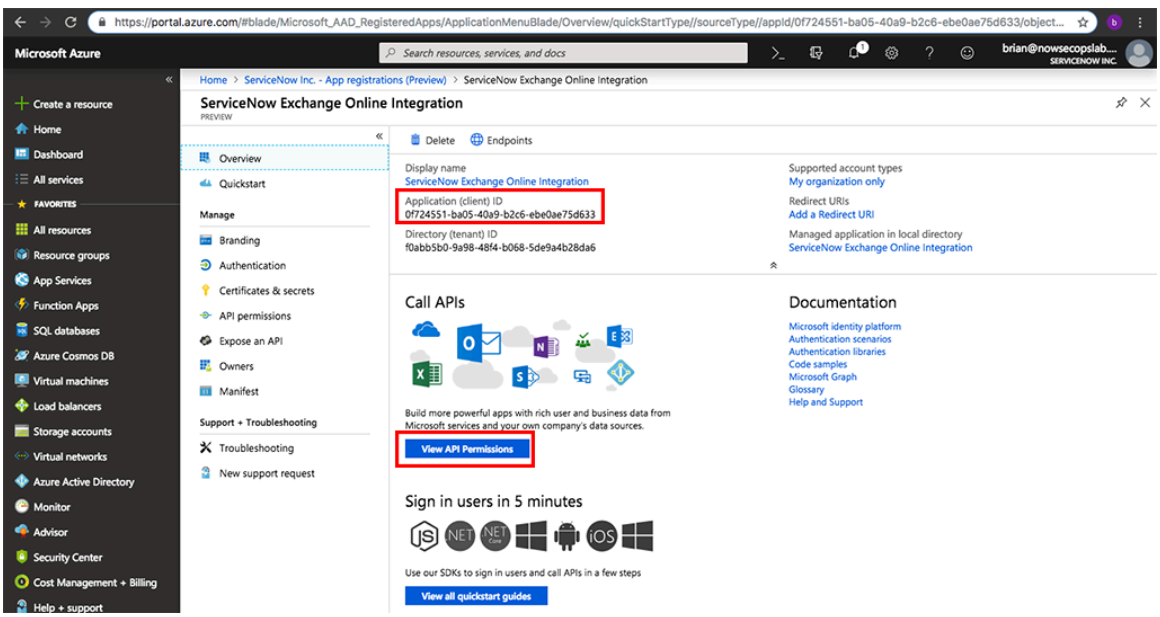
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
リダイレクト **URL** (オプション)	このフィールドに値を入力しても、統合では使用されません。



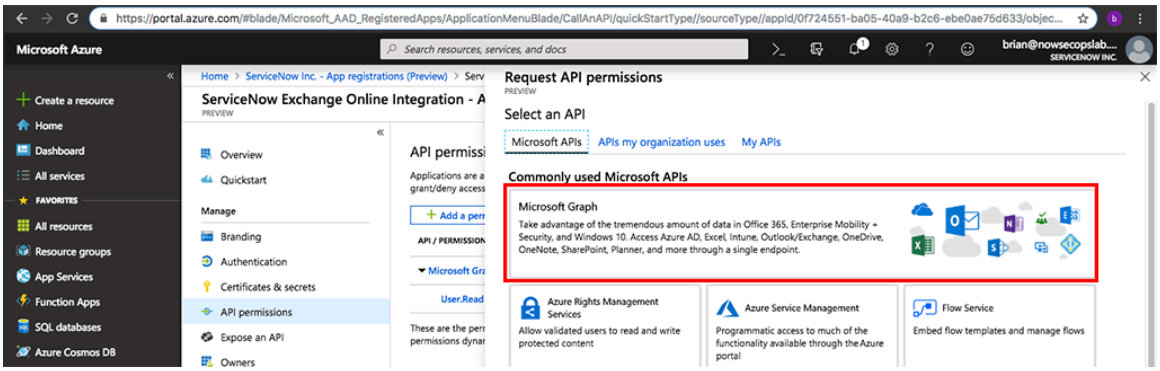
f. [登録] をクリックします。
アプリケーション ID が作成されます。この ID はユーザー名に似ています。この値は、「Now Platform インスタンスと Microsoft Exchange Online の統合の設定」で説明されている Now Platform インスタンスの設定手順で、**[OAUTH アプリケーション ID]** フィールドの設定ページで入力します。

g. [ServiceNow Exchange Online Integration] ペインにアプリケーション (クライアント) ID が表示されている状態で、**[API のアクセス許可の表示 (View API Permissions)]** をクリックします。

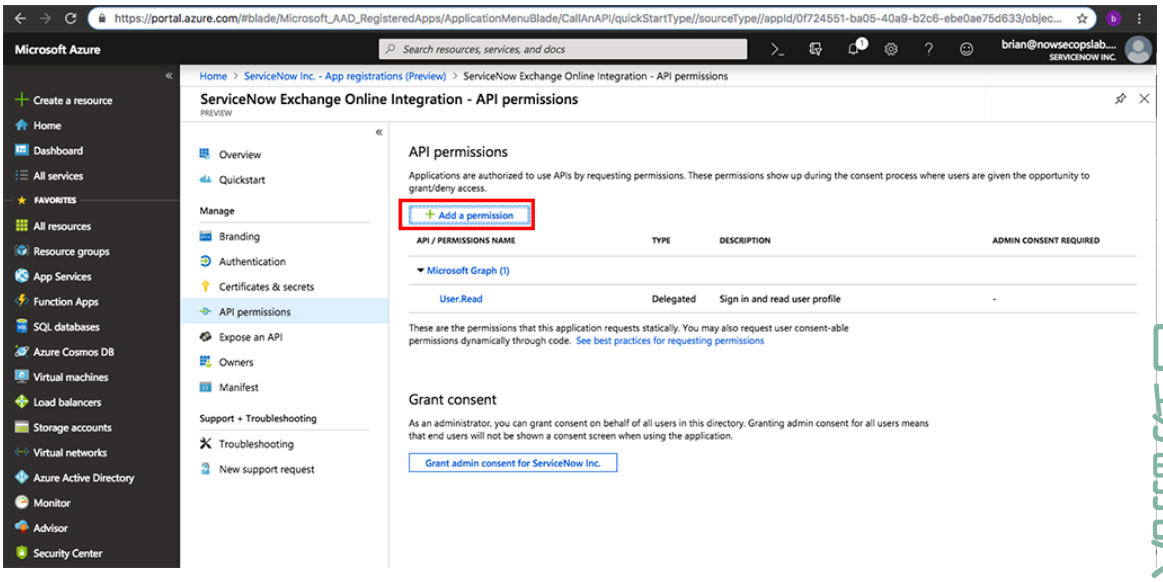


h. 表示される [API のアクセス許可の要求 (Request API permissions)] ペインで、**[Microsoft Graph]** をクリックします。

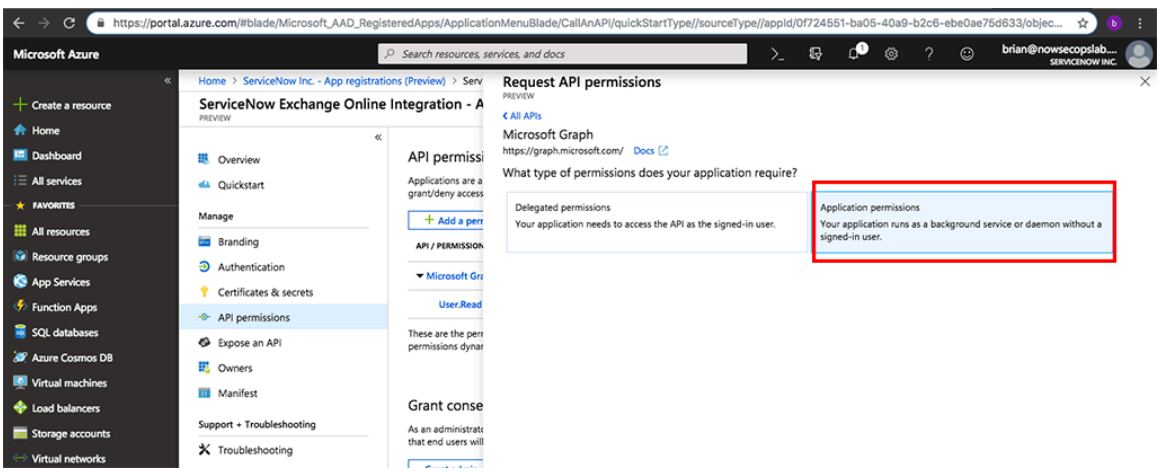
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



i. 表示される [ServiceNow Exchange Online Integration - API のアクセス許可] ペインで、[アクセス許可の追加 **(Add a Permission)]** をクリックします。

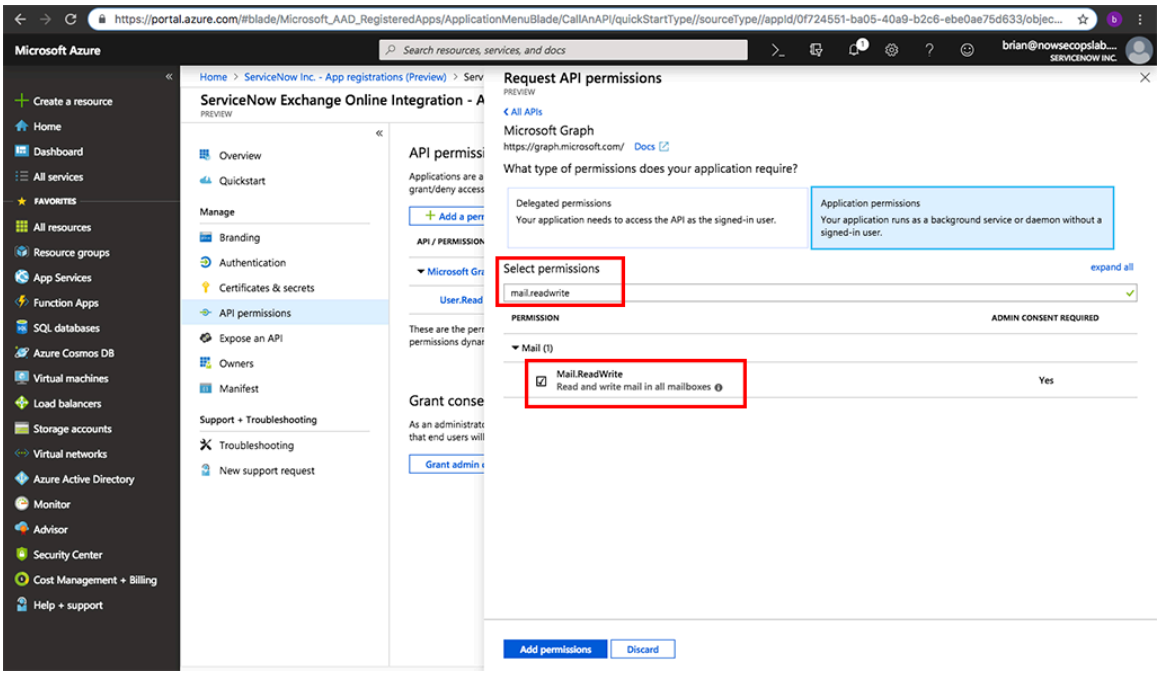


j. 表示される [API のアクセス許可の要求 (Request API permissions)] ペインで、[アプリケーションのアクセス許可] をクリックします。



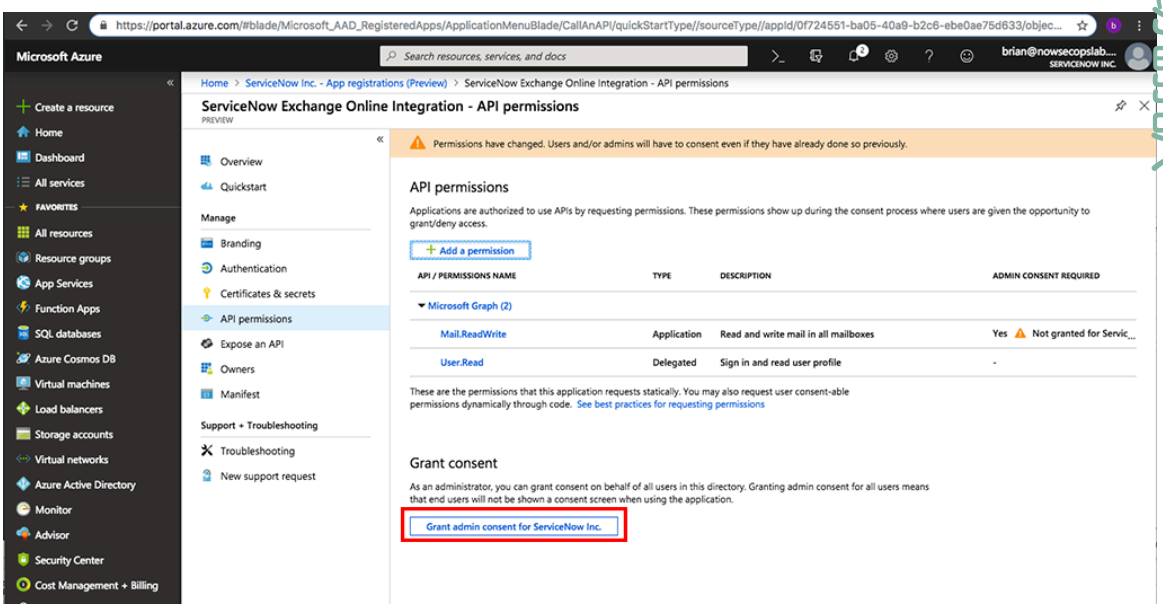
k. 表示される [アクセス許可の選択] フィールドで、「**Mail.ReadWrite**」と入力し、**[Mail.ReadWrite]** チェックボックスをオンにします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



l. [アクセス許可の追加] をクリックします。

m. 表示される [ServiceNow Exchange Online Integration - API のアクセス許可] ペインで、**[<組織名> のアドミンの同意を付与 (Grant Admin Consent for <your organization name>)]** をクリックします。

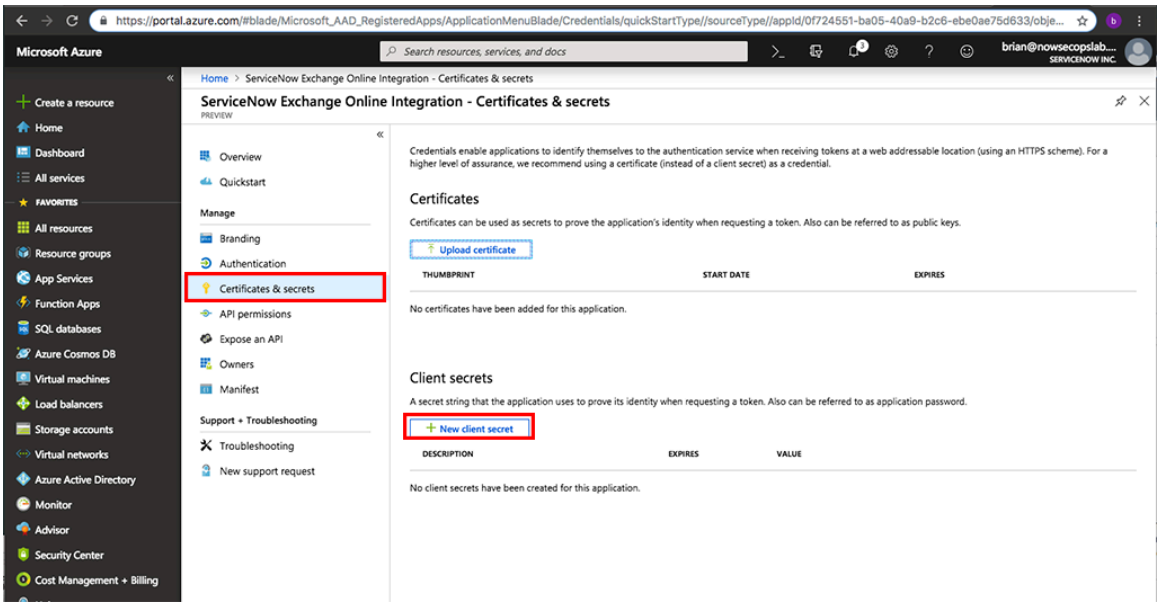


n. 以前に入力した API 選択 (Microsoft Graph API) を確定するには、[確定] をクリックします。

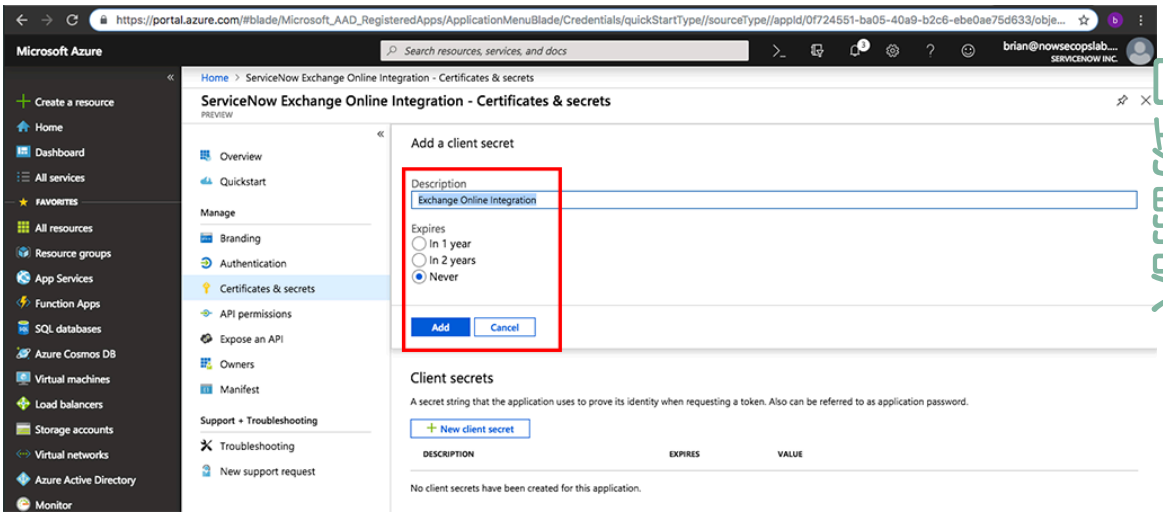
o. [ServiceNow Exchange Online Integration - 証明書とシークレット (Certificates & secrets)] ペインで、[証明書とシークレット **(Certificates & secrets)]**、[新しいクライアント シークレット **(New Client secret)]** (パスワード) を順にクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

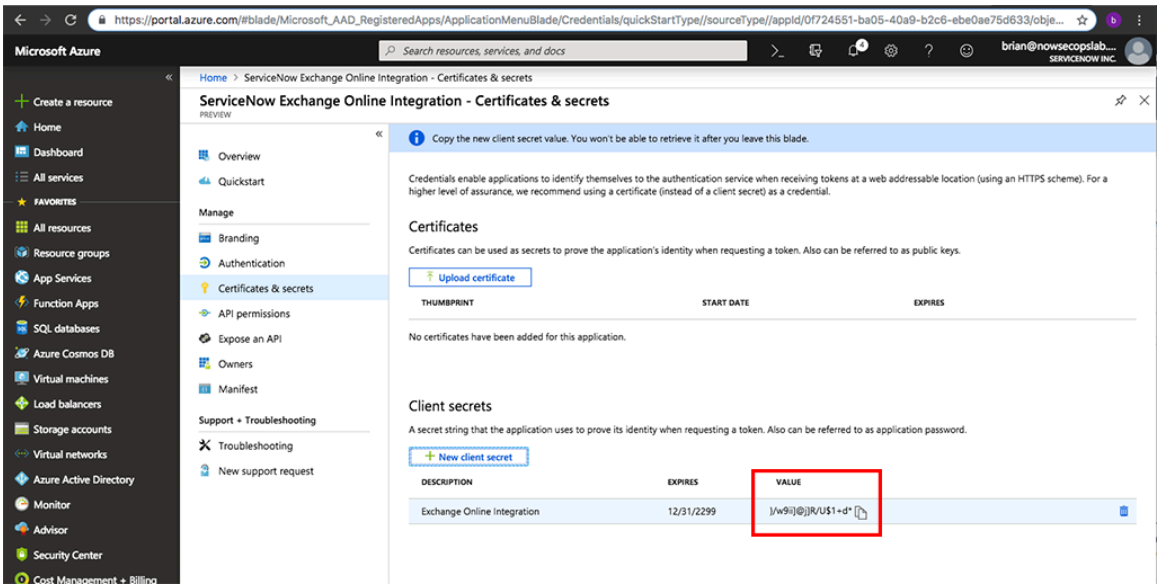


p. [ServiceNow Exchange Online Integration - 証明書とシークレット (Certificates & secrets)] ペインに表示されるフォームの [説明] フィールドに、アプリケーションの名前を入力し、有効期限のオプションをクリックして、[追加] をクリックします。



表示される [証明書とシークレット (Certificates & secrets)] ペインで、[クライアント シークレット] セクションの [値] の下の行に新しいクライアントシークレット (パスワード) が表示されます。このパスワードを安全な場所に保存します。このページから移動すると、このパスワード値は表示されなくなります。このパスワードは、Now Platform インスタンスの統合の設定手順で、設定ペインの **[OAUTH** クライアントシークレット] フィールドに入力します。統合の設計手順については、Now Platform インスタンスと Microsoft Exchange Online の統合の設定で説明しています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



これで、Microsoft Azure ポータルで OAuth 認証用のアプリケーション ID を作成できました。

次のタスク

次は統合用に Now Platform® インスタンスをセットアップします。

証明書ベースの認証またはアプリ専用の認証の設定

アプリケーションオブジェクトを使用した認証には、初期オンボーディングが必要です。アプリケーションとサービスのプリンシパルは相互に代替できます。ただし、アプリケーションはクラスオブジェクトのようなものですが、サービスのプリンシパルはクラスのインスタンスのようなものです。

Azure Active Directory におけるアプリケーションとサービスプリンシパルのオブジェクトの詳細については、「Application and service principal objects in Azure Active Directory (Azure Active Directory のアプリケーションとサービスプリンシパルのオブジェクト)」を参照してください。Azure AD でのアプリケーション作成に関する詳細な視覚的フローについては、「Create an Azure Active Directory application and service principal that can acess resources (リソースにアクセスできる Azure Active Directory アプリケーションとサービスプリンシパルの作成)」を参照してください。

証明書ベースの認証またはアプリ専用の認証を設定するには、次の手順を実行します。

1. Azure AD でアプリケーションを登録します。
2. アプリケーションに API 権限を割り当てます。

   アプリケーションオブジェクトがリソースにアクセスするには、アプリケーション権限 Exchange.ManageAsApp と Mail.ReadWrite が必要です。

3. 自己署名証明書を生成し、秘密キーへのアクセス権を付与します。

   自己署名 X.509 証明書を作成して構成します。これは、アプリ専用アクセストークンを要求するときに、Azure AD に対してアプリケーションを認証するために使用します。次世代 (CNG) 証明書は、Exchange を使用したアプリ専用の認証ではサポートされていません。CNG 証明書は、最新の Windows バージョンではデフォルトで作成されます。CSP キープロバイダーからの証明書を使用する必要があります。(-Provider = 'Microsoft Strong Cryptographic Provider')。

4. 証明書を Azure AD アプリケーションに添付します。
5. アプリケーションに Azure AD ロールを割り当てます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーションには、`コンプライアンスアドミニストレーター` Azure AD のロールが割り当てられている必要があります。

6. 新しいサービスプリンシパルを作成します。

ステップ 1：Azure AD でアプリケーションを登録する

1. Azure AD ポータル を開きます。
2. ページの上部にある [検索] ボックスに、「アプリの登録」と入力します。
3. [サービス] セクションの結果から [アプリの登録] を選択します。

   または、https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade を使用して [アプリの登録] ページに移動することもできます。
4. [アプリの登録] ページで、[新規登録] を選択します。
5. [アプリケーションの登録] ページで、次の設定を構成します。

フィールド	説明
名前	わかりやすい名前を入力します。例：ExO PowerShell CBA。
サポートされているアカウントの種類	[この組織のディレクトリ内のアカウントのみ **(<自分の組織名> のみ - シングルテナント)** **(Accounts in this organizational directory only (<YourOrganizationName> only - Single tenant))]** が選択されていることを確認します。 Exchange Online の委任されたシナリオでアプリケーションをマルチテナントにするには、[任意の組織ディレクトリ (任意の Azure AD ディレクトリ - マルチテナント)(any organizational directory (Any Azure AD directory - Multitenant))] 内の [アカウント] 値を選択します。

6. アプリの登録が完了したら、[登録] を選択し、アプリのページを閉じます。

ステップ 2：アプリケーションに API 権限を割り当てる

このセクションの手順では、新しいアプリに対して自動的に構成されたデフォルトのアクセス権限が置き換えられます。置き換えられたデフォルトのアクセス権限は、アプリに必要ありません。

1. アプリのページで、[管理] の [マニフェスト] を選択します。
2. [マニフェスト] ページで、`requiredResourceAccess` エントリを探します (およそ 47 行目)。
3. 次のコードスニペットに示すように、`resourceAppId`、`resourceAccess id`、および `resourceAccess type` の値を変更します。

```
"requiredResourceAccess": [
 {
  "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
  "resourceAccess": [
   {
    "id": "dc50a0fb-09a3-484d-be87-e023b12c6440",
    "type": "Role"
   }
  ]
 },
 {
  "resourceAppId": "00000003-0000-0000-c000-000000000000",
  "resourceAccess": [
   {
    "id": "e2a3a72e-5f79-4c64-b1b1-878b674786c9",
    "type": "Role"
   }
  ]
 }
],
```

4. [保存] を選択します。
5. [マニフェスト] ページで、[管理] の **[API** 権限] を選択します。
6. **[API** 権限] ページで、フィールドに入力します。

フィールド	説明
API / Permissions name (API/権限の名前)	値 Exchange.ManageAsApp と Mail.ReadWrite が表示されていることを確認します。
ステータス	現在は **[<組織>** に付与されません]という正しくない値であるため、この値を変更する必要があります。 **[<組織>** にアドミンの同意を付与する] を選択し、表示される確認ダイアログを読んで、[はい] を選択します。 これで、[ステータス] の値が **[<組織>** に付与] になりました。

7. ブラウザーのタブではなく、現在の API アクセス権のページを閉じて、アプリの登録ページに戻ります。

ステップ 3：自己署名証明書を生成し、秘密キーへのアクセス権を付与する

次の手順を実行して、自己署名 x.509 証明書を作成します。

- 昇格された Windows PowerShell セッションで New-SelfSignedCertificate、Export-Certificate、および Export-PfxCertificate コマンドレットを使用して (アドミニストレーターとして実行)、自己署名証明書を要求し、.cer および .pfx (デフォルトでは SHA1) にエクスポートします。例：

```
# Create certificate
$mycert = New-SelfSignedCertificate -DnsName "snowsecops.onmicrosoft.com"
 -CertStoreLocation "cert:\LocalMachine\My" -NotAfter (Get-Date).AddYears(2) -KeySpec
 KeyExchange -Provider "Microsoft Strong Cryptographic Provider"
```

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

```
# Generate password fro private key
$mypwd = ConvertTo-SecureString -String '<password>' -Force -AsPlainText

# Export certificate to .pfx file
$mycert | Export-PfxCertificate -FilePath mycert.pfx -Password $mypwd

# Export certificate to .cer file
$mycert | Export-Certificate -FilePath mycert.cer
```

- 次の手順を使用して、MID サービスユーザーに秘密キーのアクセス権を提供します。
  1. **MMC (Microsoft** 管理コンソール) を開きます。
  2. Microsoft 管理コンソール (MMC) から、 証明書 (ローカルコンピューター) > パーソナル > 証明書.

     (MMC にメニュー項目がない場合は、 ファイル > 追加/削除スナップイン.
  3. 生成した証明書を右クリックします。
  4. 展開 すべてのタスク > 秘密キーの管理
  5. **[MID** サービスユーザー **(MID service user)]** をアクセサーリストに追加します。

ステップ 4：証明書を **Azure AD** アプリケーションに添付する

証明書をアプリケーションに登録したら、認証にサムプリントを使用できます。

1. ステップ 2 の最後にある [アプリの登録] ページの [所有アプリケーション] タブから、アプリケーションを選択します。

   [アプリの登録] ページに戻る必要がある場合は、https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/%7E/RegisteredApps を使用して、[所有アプリケーション] タブが選択されていることを確認し、アプリケーションを選択します。
2. [管理] で、[証明書 **&** シークレット] を選択します。
3. 開いた [証明書 **&** シークレット] ページで、[証明書をアップロード] を選択します。
4. ステップ 3 で作成した自己署名証明書 (.cer ファイル) を参照します。
5. 完了したら、[追加] を選択します。

   証明書が [証明書] セクションに表示されています。
6. CertificateThumbPrint を書き留めて、現在の [証明書 **&** シークレット] ページを閉じます。

ステップ 5：アプリケーションに **Azure AD** ロールを割り当てる

1. Azure AD ポータル を開きます。
2. ページ上部の [検索] フィールドで、[ロールとアドミン **(Roles and Administrators)]** を探します。
3. [サービス] セクションの結果から **[Azure AD** のロールとアドミン **(Azure AD roles and administrators)]** を選択します。

   または、https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade を使用して **[Azure AD** のロールとアドミン **(Azure AD roles and administrators)]** ページに移動することもできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. **[Azure AD** のロールとアドミン **(Azure AD roles and administrators)]** ページで、チェックボックス内ではなく、結果内のロールの名前をクリックして、サポートされているロールのいずれかを見つけて選択します。

   [コンプライアンスアドミニストレーター] ロールを探して選択します。

5. [割り当て] ページで、[割り当ての追加 **(Add assignments)]** を選択します。
6. [割り当ての追加 **(Add assignments)]** ポップアップで、ステップ 1 で作成したアプリを探して選択します。
7. 完了したら、[追加] を選択します。
8. [割り当て] ページに戻り、ロールがアプリに割り当てられていることを確認します。

ステップ 6：新しいサービスプリンシパルを作成する

重要:
新しいサービスプリンシパルを作成する手順を完了する前に、**Security & Compliance PowerShell** に接続していることを確認してください。PowerShell に接続せずに新しいサービスプリンシパルを作成することはできません (新しいサービスプリンシパルを作成するには、Azure アプリ ID とオブジェクト ID が必要です)。

1. 次の変数で以下のコマンドを実行して、ステップ 1 で登録した Azure アプリケーション (<AppName>) の詳細を保存します。

```
Install-Module -Name AzureAD
Import-Module -Name AzureAD
Connect-AzureAD
$AADApp = Get-AzureADServicePrincipal -SearchString"<AppName>"
```

   構文とパラメーターの詳細については、「Get-AzureADServicePrincipal」を参照してください。

2. 同じ PowerShell ウィンドウで、Security & Compliance PowerShell に接続します。

```
Import-Module ExchangeOnlineManagement
Connect-IPPSSession -CertificateThumbPrint "<Your_Certificate_ThumbPrint>" -AppID
 $AADApp.AppId -Organization "<Your_organization>
```

   次のコマンドを実行して、Azure アプリケーションのサービスプリンシパルオブジェクトを作成します。

```
New-ServicePrincipal -AppId $AADApp.AppId -ObjectId $AADApp.ObjectId -DisplayName
"<Descriptive Name>"
```

   構文とパラメーターの詳細については、「New-ServicePrincipal」を参照してください。

Microsoft Exchange Online 統合での Now Platform® インスタンスの設定

次のセクションでは、Microsoft Exchange Online アプリケーションをインストールする前に Now Platform インスタンスで完了する必要があるセットアップタスクを示します。インストールと設定をスムーズに行うため、統合のための Microsoft Exchange Online アプリケーションをダウンロードしてインストールする前に、チェックリストを確認し、これらのタスクを完了していることを確認してください。

自動翻訳

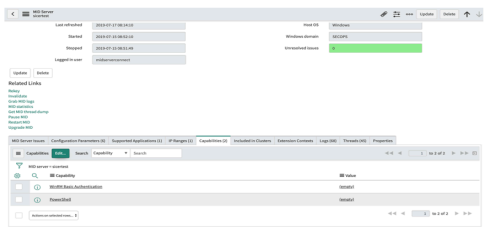
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に

セットアップタスク	説明
必要な Now Platform® および セキュリティインシデントレスポンス (SIR) のロールがアサインされていることを確認します。	次の ServiceNow ロールが必要です。 • システムアドミニストレーター (admin) は、アプリケーションをインストールし、Security Incident Management者 (sn_si.admin) ロールをアサインします。 • Security Incident Management者 (sn_si.admin) は、統合のためのアプリケーションを設定します。必要に応じて、Security Incident Management者ロールは、セキュリティインシデントアナリスト (sn_si.analyst) にメールの読み取りおよび書き込みロール (sn_sec_cmn.cap_email_write および sn_sec_cmn.cap_email_read) もアサインします。(sn_sec_cmn.cap_email_read) および (com.snc.security_incident) ロールは セキュリティインシデントレスポンス 製品とともにインストールされます。デフォルトでは、Security Incident Management者にアサインされ、必要に応じて再アサインできます。 • セキュリティインシデントアナリスト (sn_si.analyst) は、メールの検索と削除を行います。このロールは、メールが削除されたことの確認やセキュリティインシデントの処理も担当します。 ◦ 書き込みロールにより、sn_si.analyst はメール検索の編集、作成、実行とメッセージの削除を行うことができます。メッセージの削除に必要な別個のロールはありません。 ◦ 読み取りロールにより、sn_si.analyst はセキュリティインシデントの関連リストの結果を表示できます。 **注:** sn_si.analyst は、メール検索結果を表示し、メール検索クエリを作成して実行するため、(sn_sec_cmn.cap_email_read) および (sn_sec_cmn.cap_email_write) ロールが必要です。 アサインされていない場合、(sn_sec_cmn.cap_email_read) および (sn_sec_cmn.cap_email_write) ロールをセキュリティインシデントアナリストに割り当てる方法については、以下の手順を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	セキュリティインシデントレスポンス でのロールを割り当てる方法の詳細については、「Roles installed with SIR (SIR でインストールされるロール)」を参照してください。
Now Platform インスタンスで Windows MID サーバーをセットアップしたことを確認します。	Now Platform 環境には MID サーバーが必要です。Microsoft Exchange Online 製品と Now Platform はどちらもクラウド製品ですが、この統合には MID サーバーが必要です。PowerShell スクリプトは、顧客環境の Windows サーバーから実行され、MID サーバーを経由して Microsoft Exchange Online サーバーに接続します。 Microsoft Exchange Online for セキュリティオペレーション 統合のバージョン 10.5 以降では、MID サーバーに Exchange Online PowerShell V2 モジュールをインストールする必要があります。詳細については、Exchange Online PowerShell V2 モジュール に関する Microsoft ドキュメント を参照してください。 統合が Microsoft Exchange Online サービステナントから情報を取得できるようにするには、MID サーバーからの送信 HTTPS 接続が必要です。 MID サーバーの詳細については、「MID サーバー」を参照してください。 統合の設定手順でアプリケーションをインストールした後、インスタンスと Windows MID サーバー間の接続をテストします。
Microsoft Exchange Online のクエリを処理するように Windows MID サーバー をセットアップします。	• 指定された MID サーバー で、Exchange Online 証明書ベースの認証を設定します。 • Exchange Online 証明書ベースの認証と PowerShell 機能を指定された MID サーバーに割り当てます。
 現在の MID Server 環境では、すべての MID サーバーの機能を [すべて] に設定している場合、すべての MID サーバーに **Exchange Online** 証明書ベースの認証が自動的に追加されます。この場	

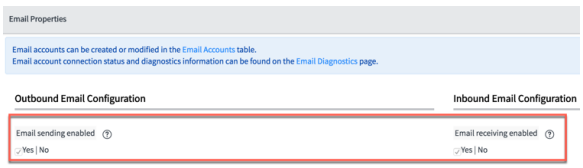
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
合、環境内のどの MID サーバーも、Microsoft Exchange Online 統合の検索要求を受信する可能性があります。 検索要求が指定された MID サーバーにのみ送信され、誤った検索ルーティングを防ぐには、[編集] をクリックし、次の手順を実行します。 • 必要な **Exchange Online** 証明書ベースの認証機能のない MID サーバーからすべての機能を削除します。 • 次に示すように必要な機能を選択し、[保存] をクリックします。	
統合用のアプリケーションをインストールする前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	セキュリティインシデントレスポンス の依存関係プラグイン (com.snc.si_dep) が必要です。このプラグインは、セキュリティインシデントレスポンス 製品のサポートに必要なすべての依存関係を自動的にインストールします。統合に必要な他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。 次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。 **1.** セキュリティインシデントレスポンス **2.** Security Integration Framework **3.** Security Support Common **4.** セキュリティサポートオーケストレーション 統合のための Now Platform インスタンスのセットアップの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。
組織で Now Platform のメール通知を使用する計画がある場合は、メールの送受信機能が有効になっていることを確認します。	Now Platform ® インスタンスでメールの送受信機能が有効になっていることを確認するには、次の手順に従います。この機能は、検索要求と削除要求が開始され、正常に完了したときに、ユーザーにメールで通知します。 **1.** 次のように移動する。 メールプロパティ > アドミニストレーション > メールプロパティ. **2.** [送信メール設定] で、［メール送信の有効化 (Email sending enabled)］と［メール受信の有効化 (Email receiving enabled)］が選択されていることを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	このメール送受信機能は、セキュリティインシデントアナリストが Now Platform から送信されるメール通知を受け取るために必要です。削除承認機能が有効になっている場合、メールの削除要求もメールで承認者に送信されます。このメールプロパティを有効にする以外に、Now Platform でメールを送受信するために必要なセットアップはありません。
	

必要なロール：admin

このタスクについて
Now Platform セキュリティインシデントアドミン (sn_si.admin) は、セキュリティインシデントレスポンス (SIR) 製品をダウンロードしたときに、メールの読み取り (sn_sec_cmn.cap_email_read) ロールと書き込み (sn_sec_cmn.cap_email_write) ロールが自動的にアサインされます。セキュリティインシデントアドミニストレーターは、これらのロールをセキュリティインシデントアナリスト (sn_si.analyst) または別のロールにアサインします。これらのロールをセキュリティインシデントアナリストまたは別のロールにアサインしていない場合は、次の手順に従ってアサインします。

手順

1. 次のように移動する。 組織 > ユーザー.
2. [ユーザー] モジュールをクリックします。

   a. 表示される [ユーザー] リストで、[新規] をクリックします。

   b. 表示される新規ユーザーフォームで、フォームに入力します。

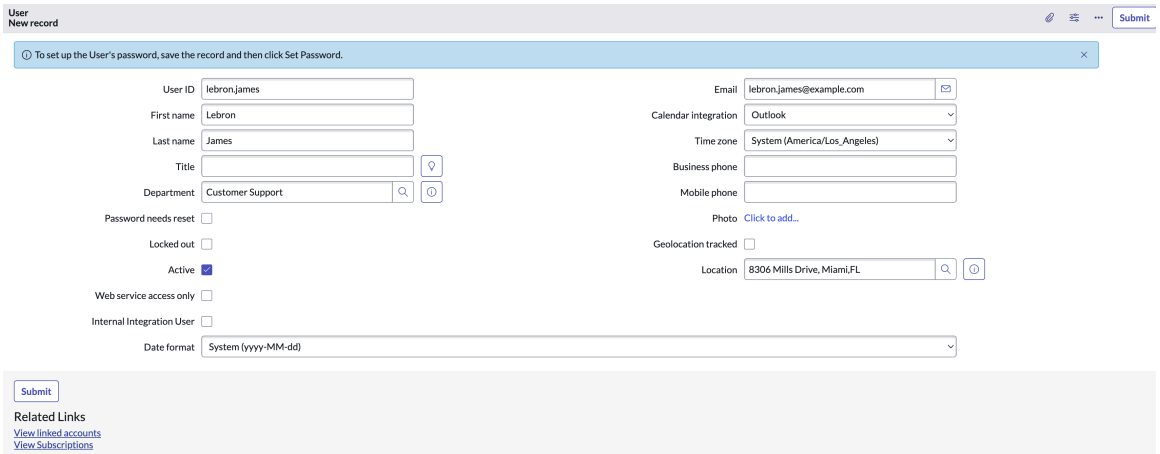
フィールド	説明
UserID	Now Platform セキュリティインシデントアナリストロールのユーザー ID (jferguson など)
メール	会社のメールアドレス。メールの検索結果とメールの削除の確認の通知は、このメールアドレスに送信されます。この例では、jferguson@servicenow.com が使用されていますが、必要に応じて、会社の任意のメールアドレスを使用してこれらのメール通知を受信できます。
名	名
姓	姓
タイトル	たとえば、セキュリティインシデントアナリスト、 セキュリティアナリスト、 セキュリ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	ティオペレーションセンター (SOC) アナリストなどです。

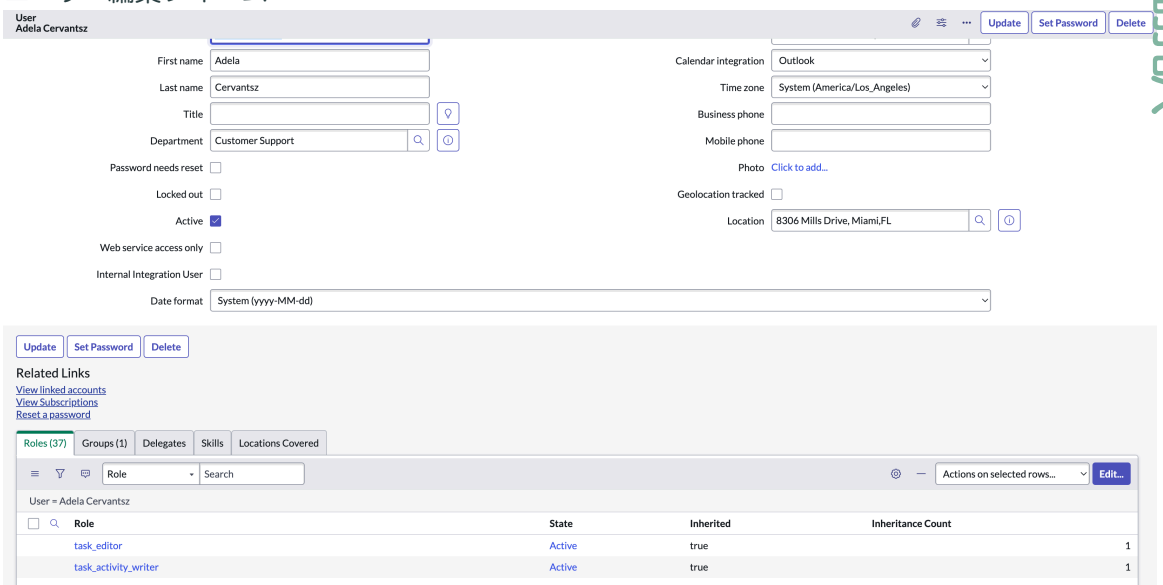
新規ユーザーフォーム



c. **[Submit]** をクリックします。
新しいユーザーが [ユーザー] リストに表示されます。

3. [ユーザー ID] 列の [ユーザー] リストで、sn_sec_cmn.cap_email_read および sn_sec_cmn.cap_email_read ロールをアサインするユーザーの名前をクリックします。
4. [関連リンク] セクションの開いているレコードで、 [編集] をクリックします。

ユーザー編集フォーム

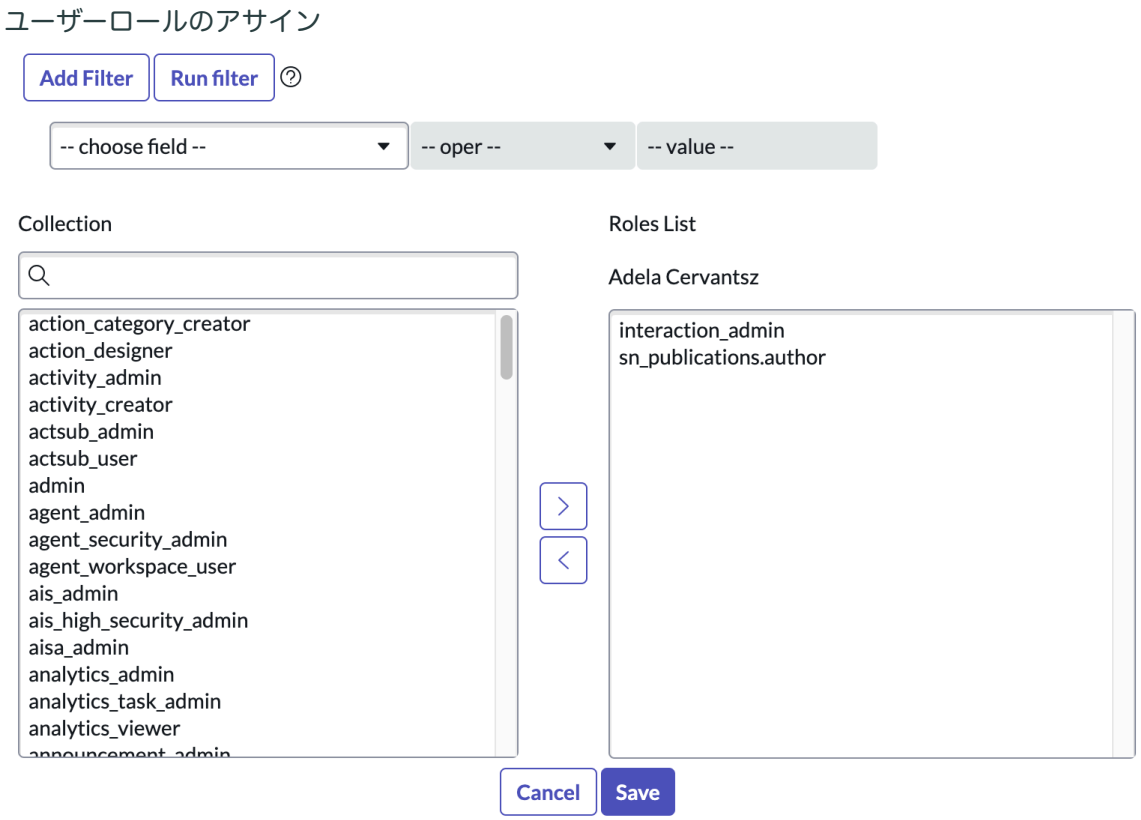


5. 表示される［メンバーの編集］フォームで、[コレクション] フィールドに「sn_sec_cmn.cap_email_read」と入力します。

注:
フィールドの下の列は自動的に入力されます。ユーザーに sn_si.analyst ロールがアサインされていない場合は、 [コレクション] フィールドに「sn_si.analyst」も入力します。次の図では、sn_si.analyst ロールがすでに Joe ferguson にアサインされています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [コレクション] 列で、[sn_sec_cmn.cap_email_read]、[sn_sec_cmn.cap_email_read]、[sn_si.analyst] (まだアサインされていない場合) を選択して、[ロール] リストに移動します。



7. [保存] をクリックします。
sn_sec_cmn.cap_email_read および sn_sec_cmn.cap_email_read ロールがセキュリティアナリスト (jferguson) にアサインされます。
8. ユーザーを追加し、組織に必要なロールをアサインします。
9. オプション: メールの削除要求の承認機能を有効にしたい場合は、次の手順に従って、承認グループを作成します。

   a. 次のように移動する。 ユーザー管理 **(User Administration)** > グループ.

   b. 表示される [グループ] リストで、[新規] をクリックします。

   c. フォームの各フィールドに入力します。

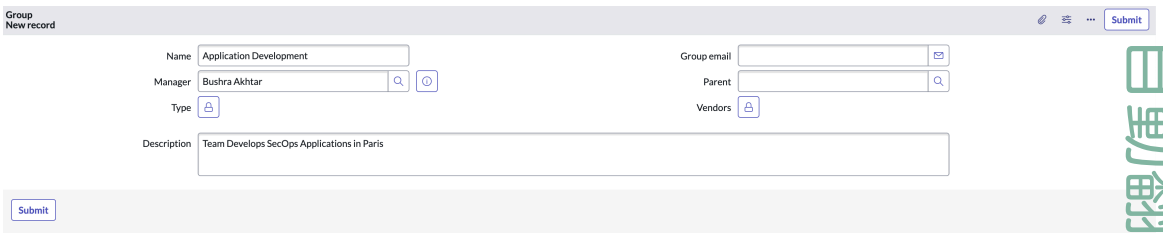
フィールド	説明
名前	メールの削除要求が送信されたときに承認を処理するグループの名前 (Exchange Online Approvers など)。
グループ メール	グループのメール配布リストまたは連絡先メールアドレス (グループマネージャーなど) が必要な場合は、メールアドレスを入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	(Optional) グループの各ユーザーのメールアドレスに個別にメール通知が送信されるようにしたい場合は、このフィールドを空白のままにします。
マネージャー	(オプション) グループマネージャーの名前。検索アイコンをクリックしてリストを表示します。
親	(オプション) このグループに親がある場合、このグループがメンバーであるその他のグループ
タイプ	(オプション) グループのカテゴリを定義します。
ベンダー	(オプション) 組織のベンダー管理プロセスに関与するユーザーに vendor_manager ロールをアサインします。
説明	(オプション) グループに関する補足情報。

グループの作成フォーム



グループの作成とロールのアサインの詳細については、「Create a user group (ユーザーグループの作成)」を参照してください。

d. **[Submit]** をクリックします。
[グループ] リストの [名前] 列に新しいグループが表示されます。

このグループにさらにユーザーを追加できます。ユーザーは、ユーザーが属するすべてのグループからロールを継承します。ロールをユーザーに直接アサインすることもできます。詳細については、「Managing roles」を参照してください。各ユーザーは、セキュリティアナリストによって送信されたメール削除要求を承認できます。要求の承認または却下に必要なのはユーザー 1 人だけです。

組織でこの統合によるメールの削除をさらに詳細に制御する必要がある場合は、オプションの承認機能を有効にします。承認を有効にするには、設定手順中に [追加の設定] タブの **[Enable** (有効化)] チェックボックスをオンにします。前の例では、 Exchange Online Approvers グループの各ユーザーがメール通知から削除要求を処理できます。

ServiceNow Microsoft Exchange Online 統合用の **Microsoft Exchange Online** アプリケーションのインストール

インスタンスで統合を実行する前に、 統合用の Microsoft Exchange Online アプリケーションを ServiceNow Store からインストールします。

始める前に

Now Platform インスタンスの ServiceNow Store から アプリケーションをインストールする前に、前提条件のチェックリストに記載されているすべてのタスクを完了してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

必要なロール：admin

重要:

- Microsoft Exchange Online 証明書ベースの認証は、Microsoft Exchange Online for Security Operations バージョン 10.5.4 以降でサポートされています。
- デモデータをインストールすると、認証情報のないデモ設定が自動的に作成されます。これがエラーの原因になることがあります。詳細については、KB0751287 を参照してください。

手順

1. 統合用のアプリケーションをインストールしていない場合は、「セキュリティオペレーション 統合のインストール」を参照し、手順に従ってインストールしてください。
2. ServiceNow Store からアプリケーションをインストールした後、Now Platform インスタンスに接続するようにアプリケーションを設定します。

関連情報

ServiceNow Microsoft Exchange Online Integration のための Microsoft Azure アカウントのセットアップ

証明書ベースの認証またはアプリ専用の認証の設定

Microsoft Exchange Online 統合での Now Platform インスタンスの設定

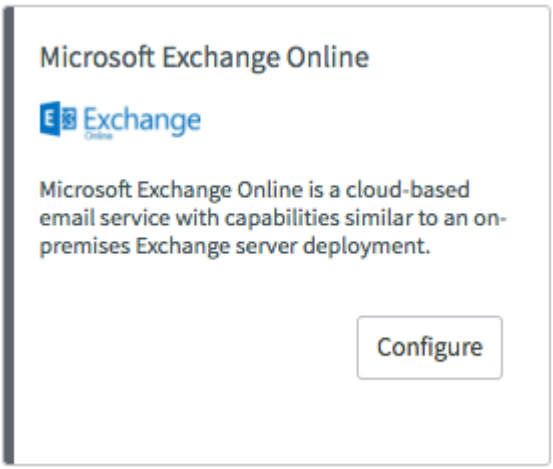
Now Platform インスタンスと **Microsoft Exchange Online** の統合の設定

ServiceNow Store からアプリケーションをインストールした後、Now Platform インスタンスに接続するようにアプリケーションを設定します。このアクティベーションにより、検索と削除のワークフローが有効になります。

始める前に
必要なロール：sn_si.admin

手順

1. Now Platformインスタンスで、 セキュリティオペレーション > 統合 > 統合設定.
2. Microsoft Exchange Online タイルを見つけます。
3. [構成] をクリックします。

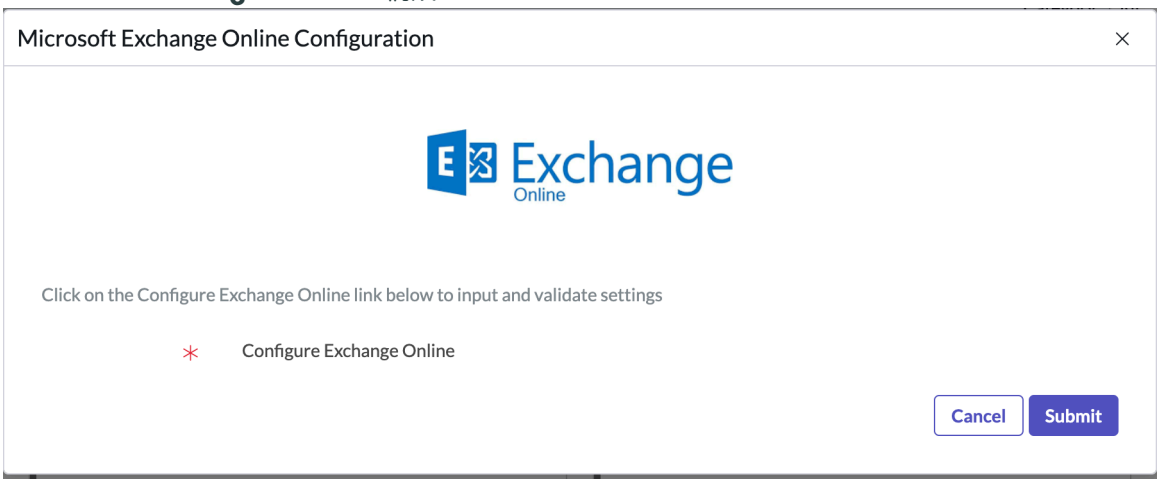


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

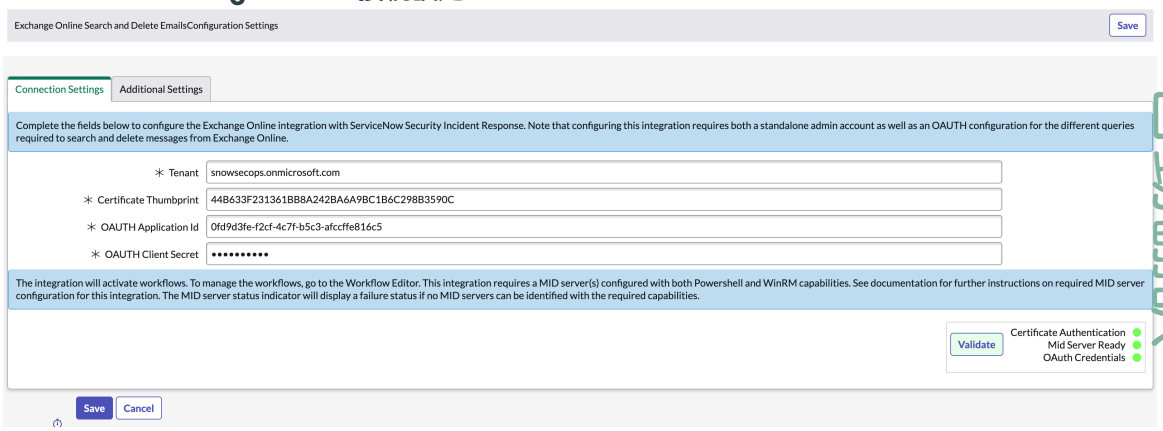
4. 表示される [Microsoft Exchange Online の構成 (Microsoft Exchange Online Configuration)] ダイアログで、**[Exchange Online を構成 (Configure Exchange Online)]** をクリックします。

   完成および検証済みのフォームの例を表の後に示します。

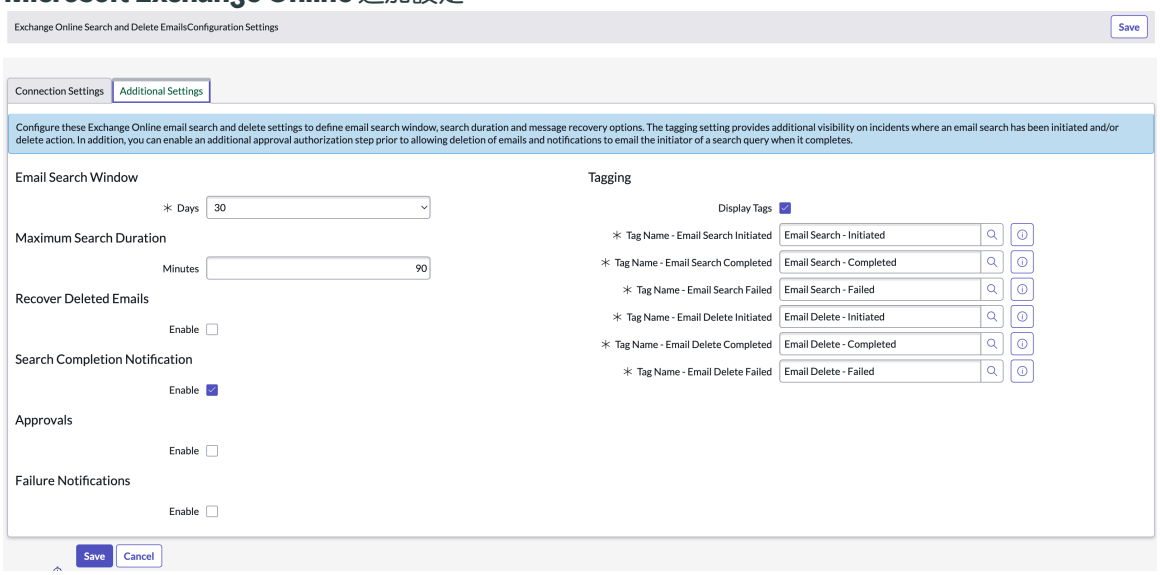
Microsoft Exchange Online の構成



Microsoft Exchange Online 接続設定



Microsoft Exchange Online 追加設定



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. 1 つ選択して続行します。

Trouble?
エラーメッセージが表示された場合、または [検証] ボタンの右側にあるインジケーターが 1 つ以上赤くなった場合は、入力したユーザーアカウントの認証情報が有効であることを確認します。認証情報を入力し、もう一度 [保存] をクリックします。

検証の失敗

[検証] ボタンと色付きアイコンの詳細については、次の表を参照してください。

[検証] ボタンとインジケーターのステータス	説明
[検証] ボタンが緑色で、小さな色付きインジケーターもすべて緑色です。	MID サーバー接続と資格情報 (証明書認証および OAuth) が有効であることを示します。
[検証] ボタンは薄い赤で、境界が青くなっており、1 つまたはすべての小さな色付きインジケーターがオレンジ色です。	検証の処理中です。検証が完了するまでに少し時間がかかる場合があります。
[検証] ボタンは薄い赤で、1 つまたはすべての小さな色付きインジケーターが赤くなっています。	• Exchange Online 証明書ベースの認証または OAuth 認証情報のボタンが赤：Exchange Online 証明書ベースの認証または OAuth 認証情報が無効であることを示します。 • Exchange Online 証明書ベースの認証および MID サーバー準備完了のボタンが赤：MID サーバーに到達できないため、MID サーバーを介した Exchange Online 証明書ベースの認証に失敗したことを示します。 • Exchange Online 証明書ベースの認証インジケーターは赤だが、MID サーバー準備完了のボタンは緑：MID サーバーはアクティブで正しく構成されているが、Exchange Online 証明書ベースの認証が正しくないことを示します。

メール検索条件の定義と **Microsoft Exchange Online** サービスに対する検索の要求

sn_si.analyst ロールを持つユーザーとして、検索条件を定義し、セキュリティインシデントレコードのインシデントの詳細に基づいてメール検索要求を送信します。

始める前に
必要なロール：sn_si.analyst

この手順の図は、 [システムの設定] で選択されたタブ付きフォームで示します。タブ付きフォームのオン/オフの詳細については、ServiceNow 製品ドキュメント Web サイト の「フォームレイアウトを設定する際のタブ付きフォームの表示 (Display tabbed forms in Configuring the form layout)」セクションを参照してください。

必要なロール：sn_si.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
検索クエリに一致する個々のメッセージのステータスと検索結果は、セキュリティインシデントレコードで報告されます。メール通知が有効になっている場合は、メールメッセージから検索結果を表示できます。

検索条件には、メッセージの送信者アドレス、受信者アドレス、件名を含めることができます。次のようなメッセージの件名、送信者、受信者の検索パラメーターの組み合わせは、1 つの特定のフィッシングキャンペーンの一部である可能性があるフィッシング関連のメールメッセージを検索するためによく使用されます。

- 1 つのフィッシングアカウントから送信されたすべての元のメールを検索する：送信者で検索します。
- 1 つのフィッシングキャンペーンのすべての元のメールを検索する：件名と送信者で検索します。
- 1 つのフィッシングキャンペーンのすべての受信メールを検索する (元のメールと転送の両方、送信者を問わない)：件名で検索します。
- 1 人のユーザーから送信された 1 つのフィッシングメールのすべての転送メールを検索する：受信者と件名で検索します。
- 1 人のユーザーに送信されたすべてのフィッシング関連メールを検索する：送信者と受信者で検索します。

注:
初期セットアップ時に検索範囲を短く設定していない限り、検索は過去 30 暦日以内に送信または受信されたメールに対して行われます。メールが削除できるようになる前に、メールの検索を成功させる必要があります。

次の例は、Now Platform セキュリティインシデントから検索を開始する方法を示しています。組織の Microsoft Exchange Online サーバー内の疑わしいフィッシング攻撃の元のメールに基づいて、セキュリティインシデントが作成されます。この例では、検索条件は送信者 (差出人) と件名で、[差出人] は phisher@cbazyx.com、[件名]は「アカウントへのログイン (log in to your account)」です。

入力した検索条件に一致するキーワードを含むテキスト文字列が検索で見つかると、件名の検索結果が返されます。この例では、件名は「アカウントへのログイン (log in to your account)」です。**AND** 演算子を使用して検索条件の差出人と件名を分離し、これらの検索条件を含むすべてのメールメッセージの結果が返されるようにします。次の手順では、特定のフィッシングアカウントから送信された件名テキストを含むメールのみを発見する検索をセットアップする方法について説明します。

手順

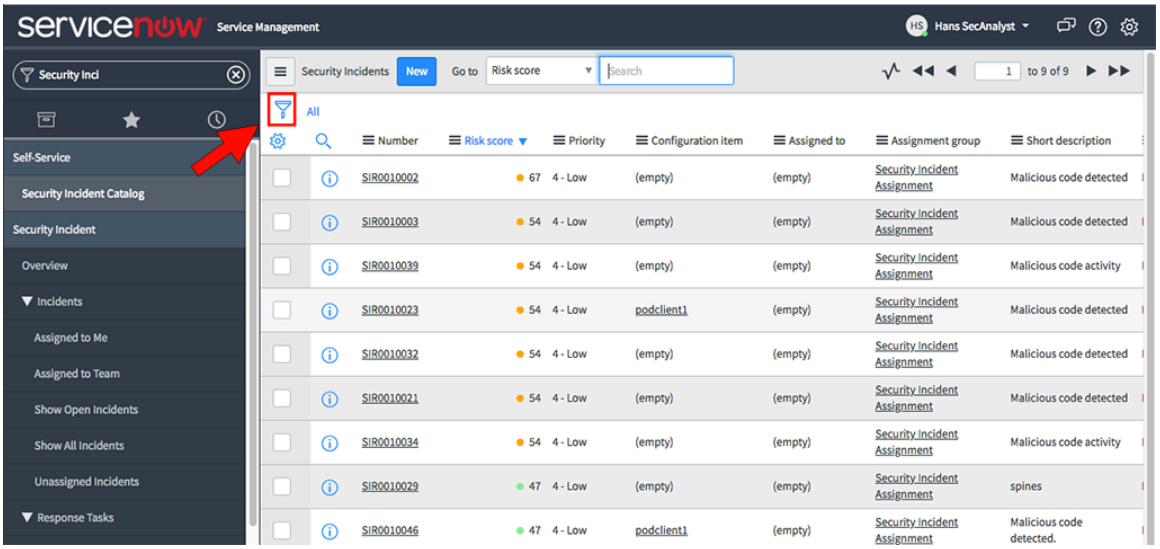
1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示 をクリックし、目的のセキュリティインシデントを見つけます。
2. または、次の手順に従ってフィルターを設定して実行し、フィッシングイベントによって作成されたセキュリティインシデントのみが表示されるようにします。

   a. 次のように移動する。 セキュリティインシデント > すべてのインシデントを表示 をクリックして [セキュリティインシデント] リストを開きます。

   b. 表示されたリストの左上隅にあるフィルターアイコンをクリックします。

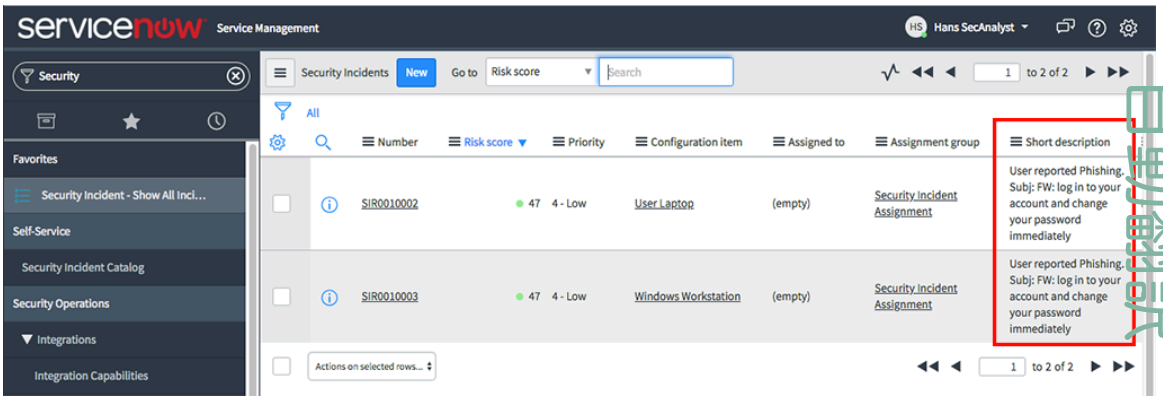
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



c. 表示されるフィールドで、 簡単な説明 > 次の値を含む を選択し、「 ユーザーから報告されたフィッシング 」と入力して 、[実行] をクリックします。

フィッシング関連のセキュリティインシデントが表示されます。



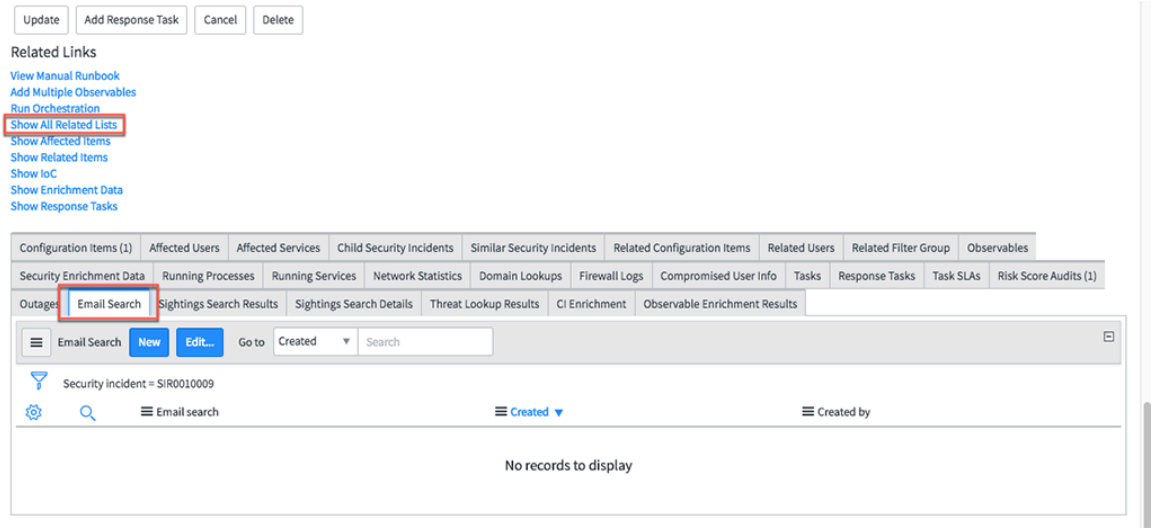
d. [簡単な説明] 列のテキストを使用すると、目的のセキュリティインシデントを見つけることができます。

e. [番号] 列で、セキュリティインシデントをクリックしてレコードを開きます。

3. [セキュリティインシデント] レコードの一番下までスクロールし、[メールの検索 (Email Search)] 関連リストをクリックします。

[メールの検索 (Email Search)] 関連リストが表示されない場合は、 [すべての関連リストを表示] 関連リンクをクリックして、この関連リストを表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

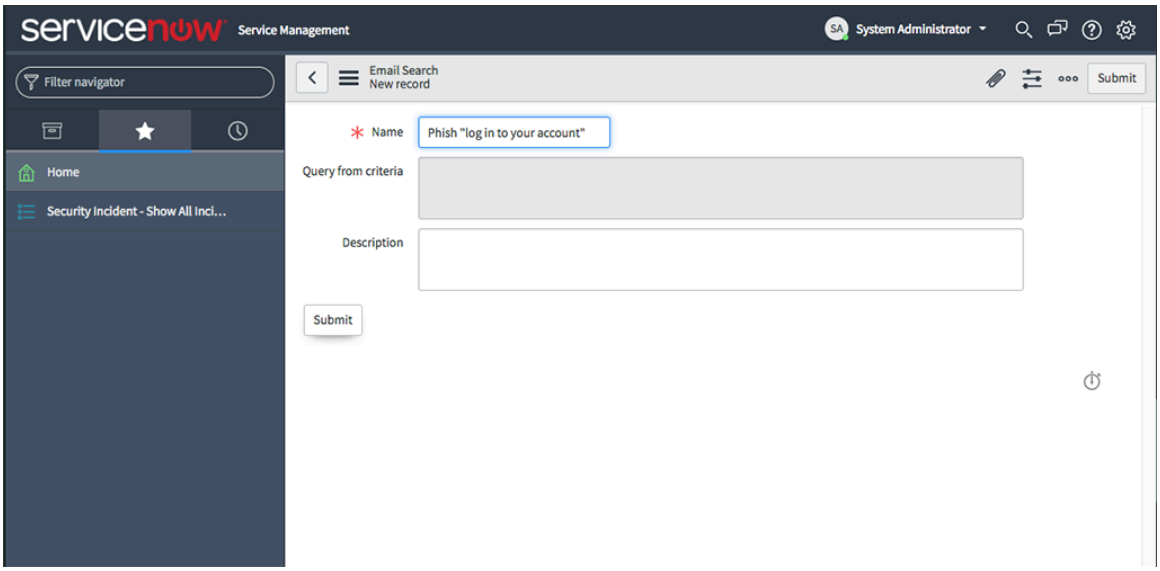


4. [メールの検索 (Email Search)] 関連リストで、 [新規] をクリックして新しいメール検索レコードを作成します。
   [メールの検索 (Email Search)] フォームが表示されます。この検索クエリを少し変更して、同じフィッシング関連インシデントに対して再実行したい場合は、この検索クエリレコードを再利用できます。ただし、フィッシングキャンペーンは動的であり、送信者とメッセージのフィールドは頻繁に変更されるため、この検索を別のフィッシング関連のインシデントに使用するようなことはほとんどありません。
5. オプション: 既存の検索クエリレコードを編集するには、[編集] をクリックします。
6. [メールの検索 (Email Search)] フォームで、フィールドに入力します。

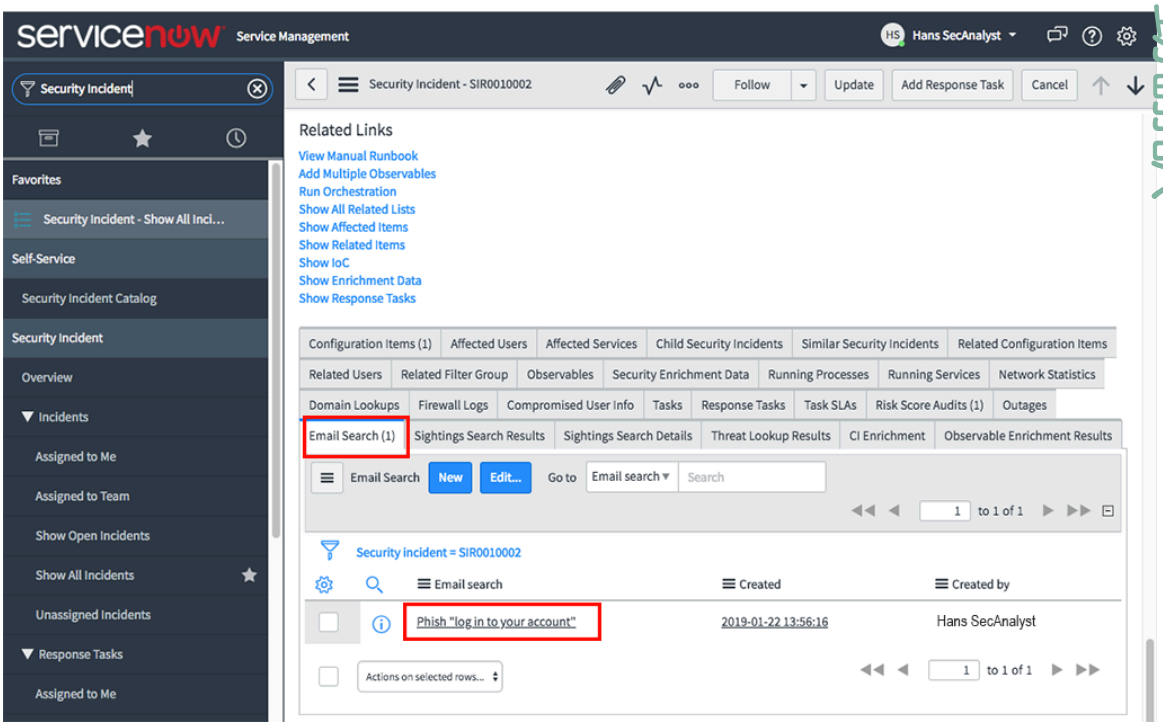
フィールド	説明
名前	検索のタイプを説明する情報。この例では、差出人 (From) + 件名 (Subject) 検索の名前は、「フィッシング「アカウントへのログイン」(Phish "log in to your account")」です。
説明	メールサーバー内の検索に関する情報。この検索の例は、From=phisher@cbazyx.com + Subject=log in to your account です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

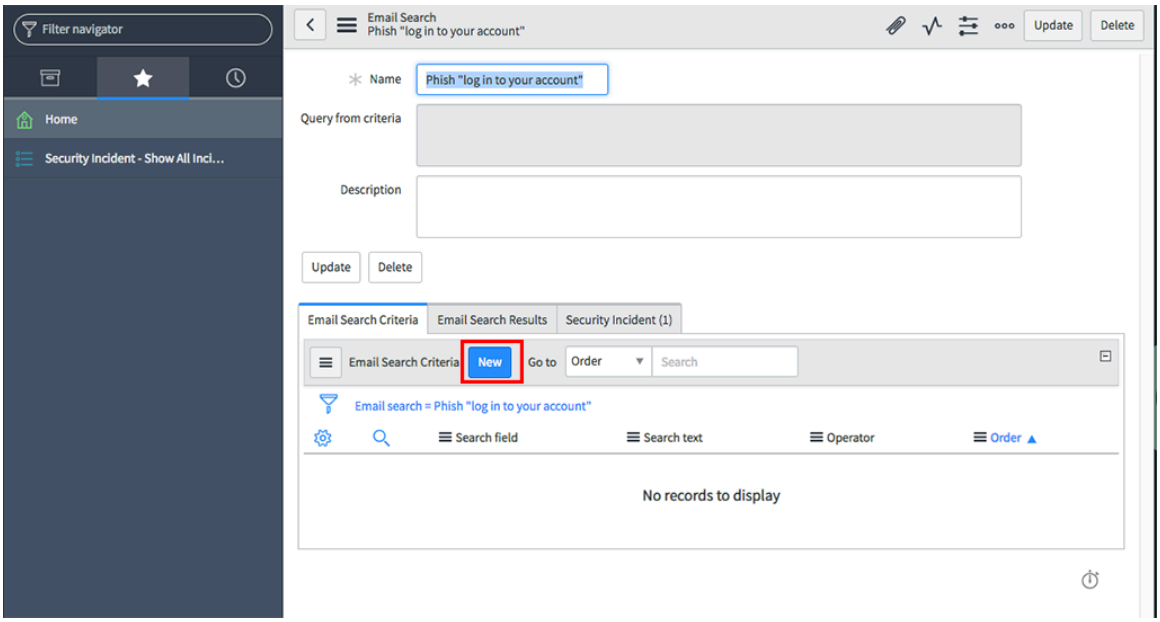


7. **[Submit]** をクリックします。
   セキュリティインシデントが表示され、メール検索の名前が [メールの検索 (Email Search)] 関連リストの [メールの検索 (Email Search)] 列に表示されます。検索レコードの検索条件を定義してからでないと、この新しい検索クエリは使用できません。
8. 検索条件を定義するには、[メールの検索 (Email Search)] 関連リストを選択した状態で、[メールの検索 (Email Search)] 列で [フィッシング「アカウントにログイン」**(Phish "log in to your account")]** をクリックします。



9. 表示されるメール検索レコードで、[メール検索基準] 関連リストをクリックし、[新規] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



10. [メール検索基準] フォームで、フィールドに入力します。

完成したフォームの例が表の後に表示されます。

フィールド	説明
メールの検索	[メールの検索 (Email Search)] レコードに入力した名前がフィールドに自動的に入力されます。
検索アイコン	リストを使ったルックアップ。 保存された検索のリスト。アイコンをクリックすると、保存済みのメール検索のリストが開きます。このリストのアイテムをクリックすると、現在の検索が削除され、以前に保存されたメール検索が選択されます。
情報アイコン	[メールの検索 (Email Search)] レコードを表示するために使用するアイコン。[メールの検索 (Email Search)] レコードを表示するためのアイコンをクリックします。
検索フィールド	検索条件 ([件名]、[差出人]、または [受信者])。選択リストから検索条件を選択し、テキストフィールドで検索する値を定義します。この例では、[差出人] phisher@cbazyx.com (フィッシングメールの送信者のメールアドレス) から始まります。
アクティブ	検索をアクティブ化するためのオプション。 検索はデフォルトで有効になります。 このオプションをオフにすると、このレコードは検索に含まれなくなります。

自動翻訳

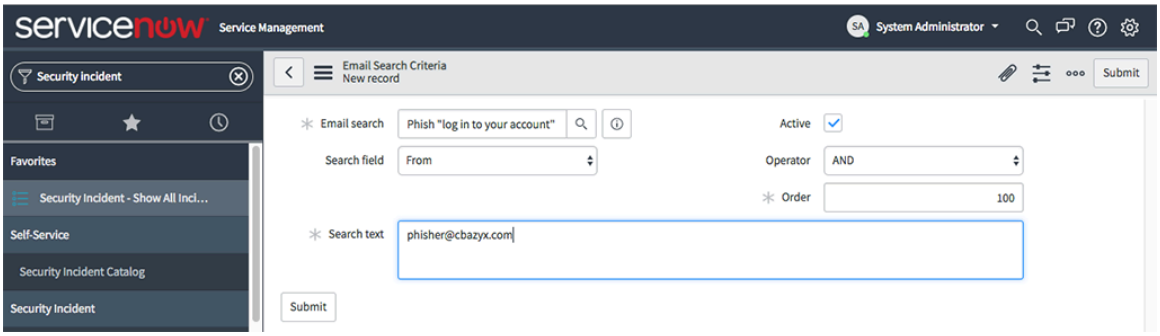
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
演算子	検索を細かく定義するための演算子 (**AND**、**OR**)。 **AND**：システムは **AND** で区切られた条件を検索し、すべての条件が満たされた場合にのみ結果を返します。送信者プラス件名の検索では、**AND** 演算子を使用して、メールの検索時に両方の検索条件が満たされるようにします。 この例では、**AND** 演算子を使用し、クエリは [差出人] (sender) = phisher@cbazyx.com **AND** [件名] (subject) = log in to your account になっています。 **OR**：システムは検索を実行し、**OR** で区切られた条件のいずれかが満たされた場合に結果を返します。 たとえば、[差出人] (sender) = phisher@cbazyx.com **OR** [差出人] (sender) = phisher-2@cbazyx.com です。
順序	3 つ以上の検索条件を入力する場合は、 [順序] を使用して条件の優先順位を決めます。デフォルトは 100 です。各条件に 1 ～ 100 の値を入力します (例：100、95、90、80)。最も小さい数値が割り当てられた条件は、条件のグループの中で検索優先度が最も高くなります。
検索テキスト	検索 (メールアドレスまたは件名) のテキスト値 (キーワード)。 検索フィールドには、検索で使用されるテキストが含まれます (例： phisher@cbazyx.com)。 検索で送信者 (差出人) と受信者の正確な検索結果が返されるようにするには、検索文字列が完全に一致する必要があります。件名検索の場合、長い文字列の一部であるキーワードを検索文字列に含めることができます。たとえば、件名に、転送または返信のメッセージヘッダーで一致した検索文字列そのものが含まれている場合があります。たとえば、 転送：アカウントにログインし、パスワードをすぐに変更してください (FW: log in to your account and change your password immediately) などです。 たとえば、アカウントにログイン (Log in to your account) は、アカウントにログインし、パスワードをすぐに変更してください (log in to your account and change your password immediately) という文字列に含まれるキーワードそのものです。 [含む *(contains)*] タイプの検索をサポートするためにワイルドカード (*) を指定する必要はあ

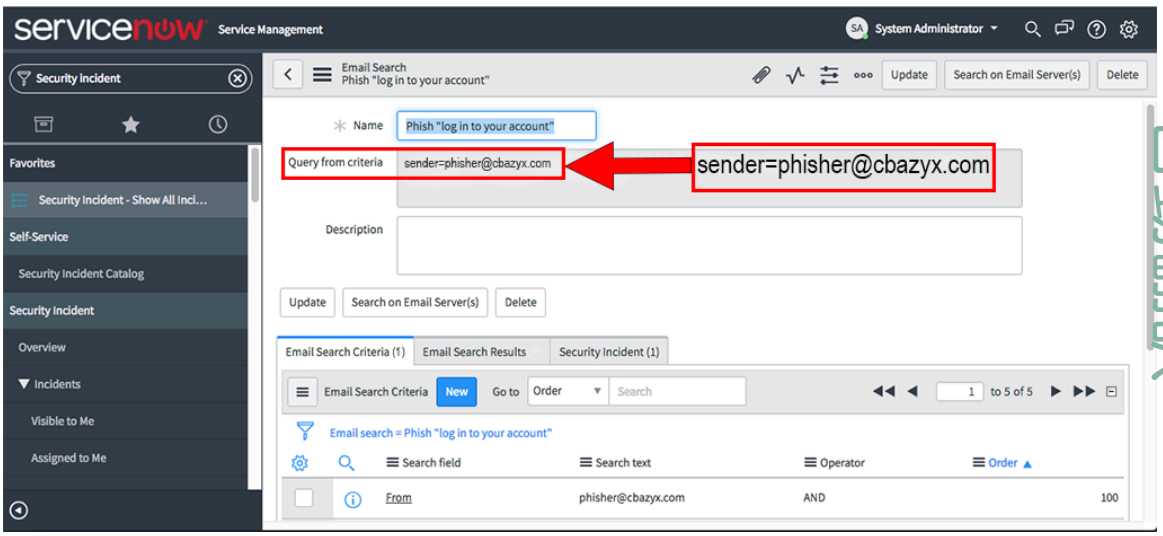
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	りません。現在のところ、長いテキスト文字列の一部ではない検索文字列そのものに一致させるためのフィルタリング方法はありません。



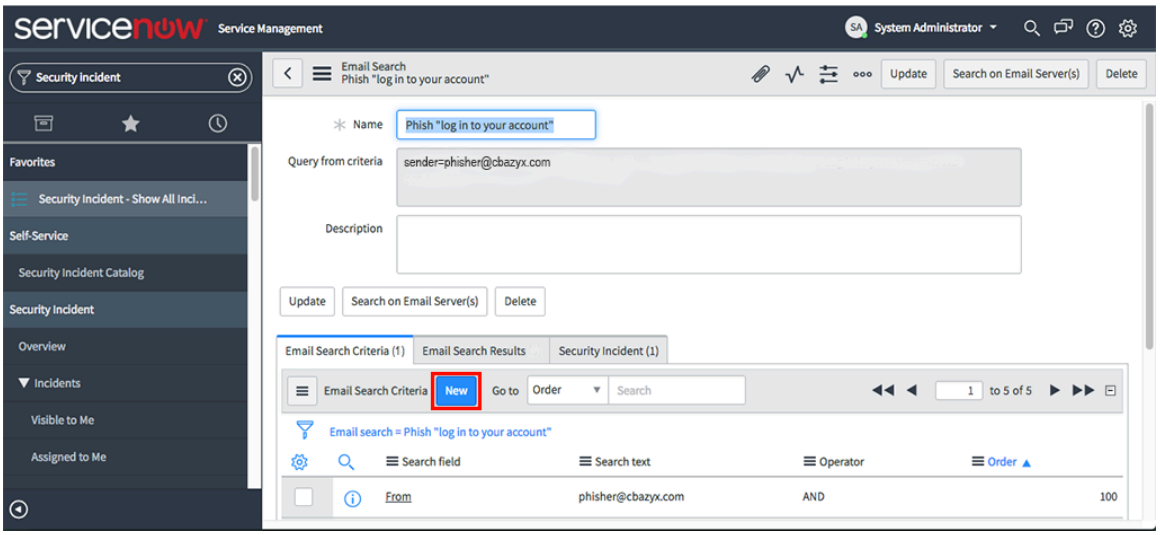
11. **[Submit]** をクリックします。
[メールの検索 (Email Search)] レコードが表示されます。[条件から生成されたクエリ] フィールドに、送信者 (sender) について追加した検索条件が表示されます。



12. このメール検索条件を追加情報で更新し、必要な件名と送信者の条件がクエリに含まれるようにするには、次の手順に従って別の検索条件を追加します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

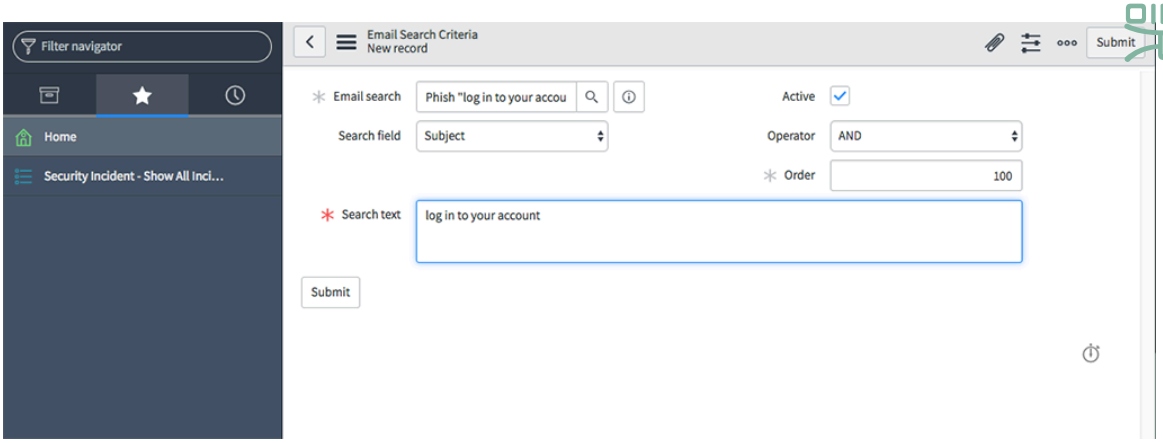
a. [メール検索基準] 関連リストで、[新規] をクリックします。



b. 表示される [メール検索基準] レコードで、[検索フィールド] リストから、[件名]を選択します。

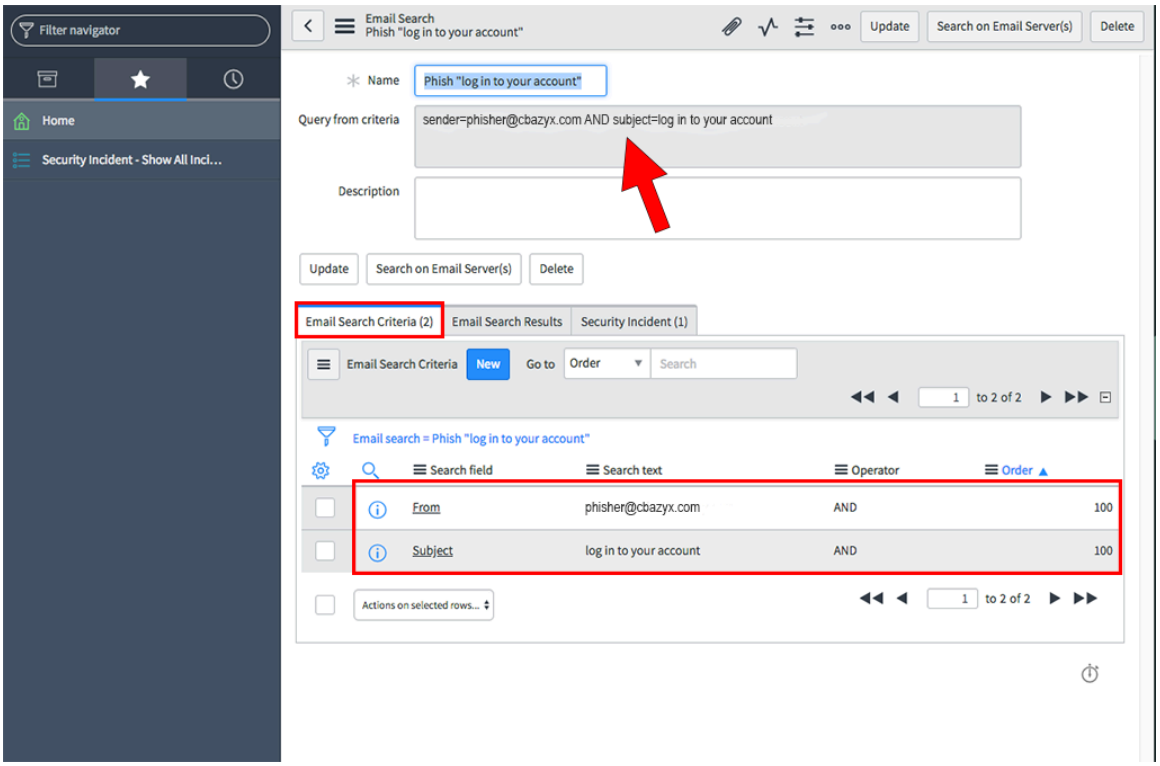
c. [演算子] リストから、**[AND]** または **[OR]** を選択します。
[OR] を選択した場合、件名のテキスト文字列のキーワードが一致するか、メールアドレスの条件が一致すると、検索結果が返されます。この例では **[AND]** が選択されているため、件名のテキスト文字列のキーワードを含み、かつ送信者のメールアドレスと一致するメールの検索結果のみが返されます。

d. [テキストを検索] フィールドに件名のテキストの値「アカウントにログイン (log in to your account)」を入力します。



e. [Submit] をクリックします。
[メール検索条件] 関連リストに新しい条件が表示され、両方の条件が [条件から生成されたクエリ] フィールドに **AND** 演算子で区切られて表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



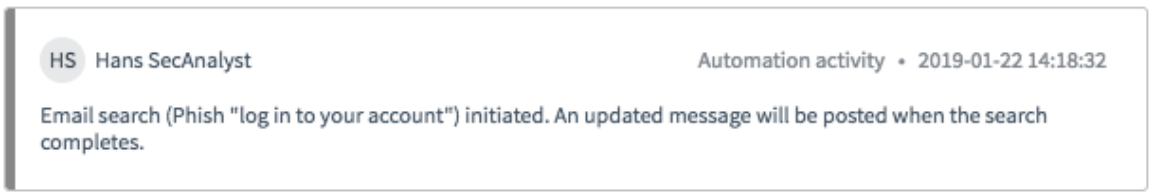
f. オプション: 検索条件が 3 つ以上あり、**[AND]** を選択して各条件を区切る場合は、順序値を設定して優先順位を決めます。

g. 必要に応じて検索条件の追加、変更、または削除を続け、[更新] をクリックしてレコードへの変更を保存します。

13. オプションを 1 つ選択して続行します。

14. メール検索を開始するには、メール検索レコードで [メールサーバーを検索 **(Search on Email Servers(s))]** をクリックします。
検索要求が送信されたことを示すメッセージが表示されます。

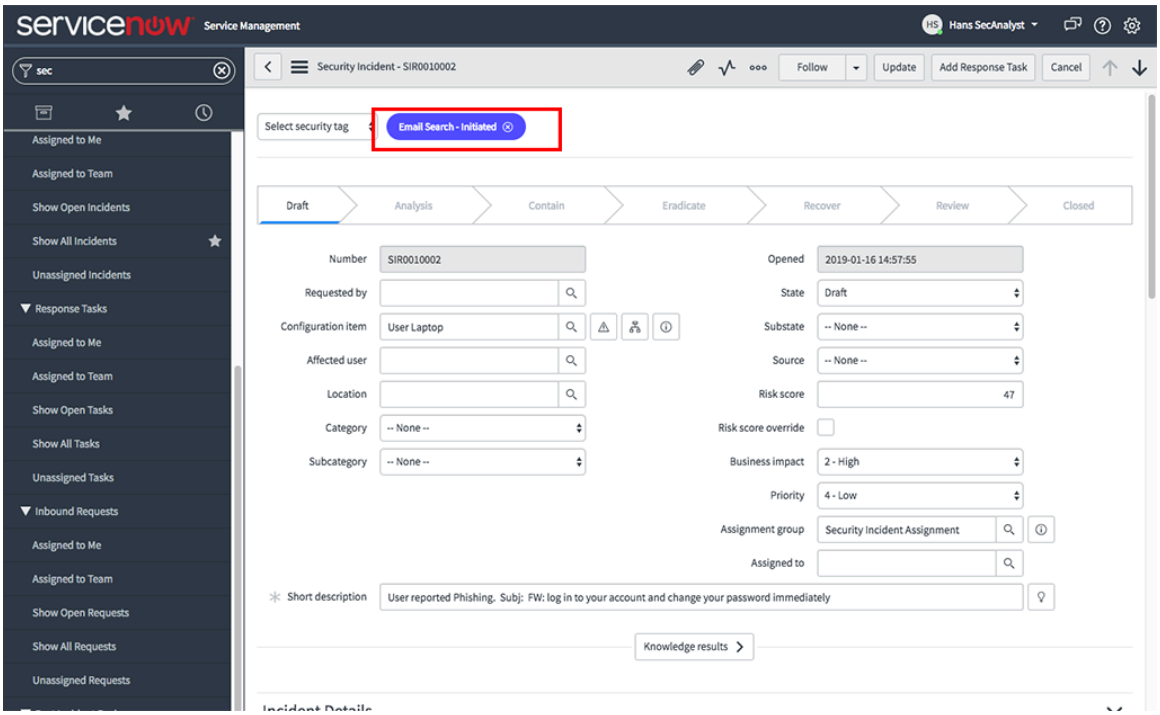
セキュリティインシデントレコードに、検索が開始されたことを示す作業メモが表示されます。



タグ付けが有効になっている場合は、セキュリティインシデントレコードの上に、[メールの検索 - 開始 (Email Search - Initiated)] セキュリティタグが表示されます。

自動翻訳

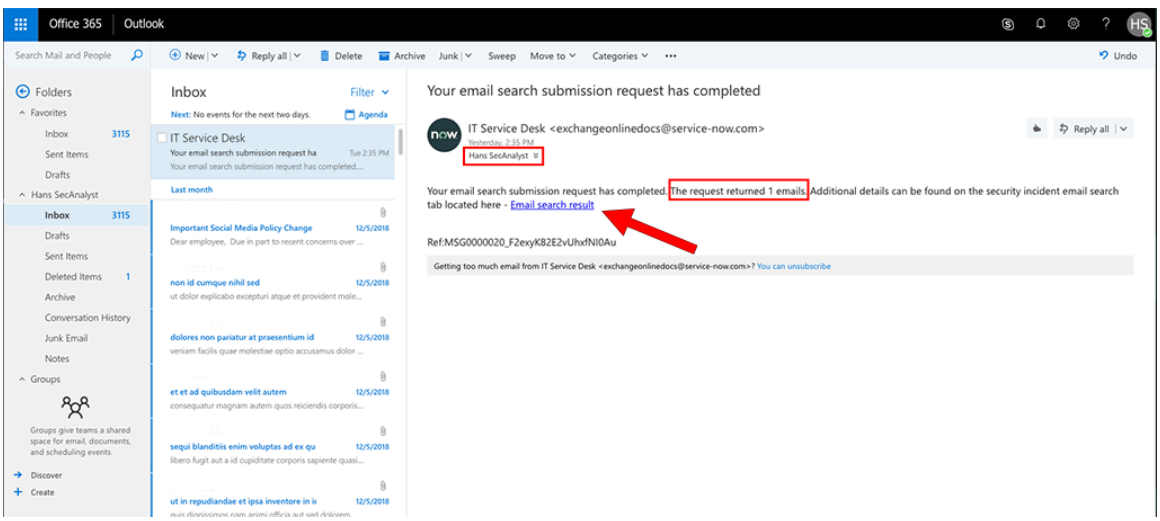
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



メール通知が有効になっている場合、検索が正常に完了すると、検索を開始した個人のメールアドレスにメールが送信されます。

この例では、sn_si.analyst ロールを持つユーザー、Hans SecAnalyst が、この検索を送信しました。次の画像は、この通知が Microsoft Exchange Online のアカウントに送信されることを示しています。ただし、これらの通知は、必要に応じて別のメールサービスに送信することもできます。

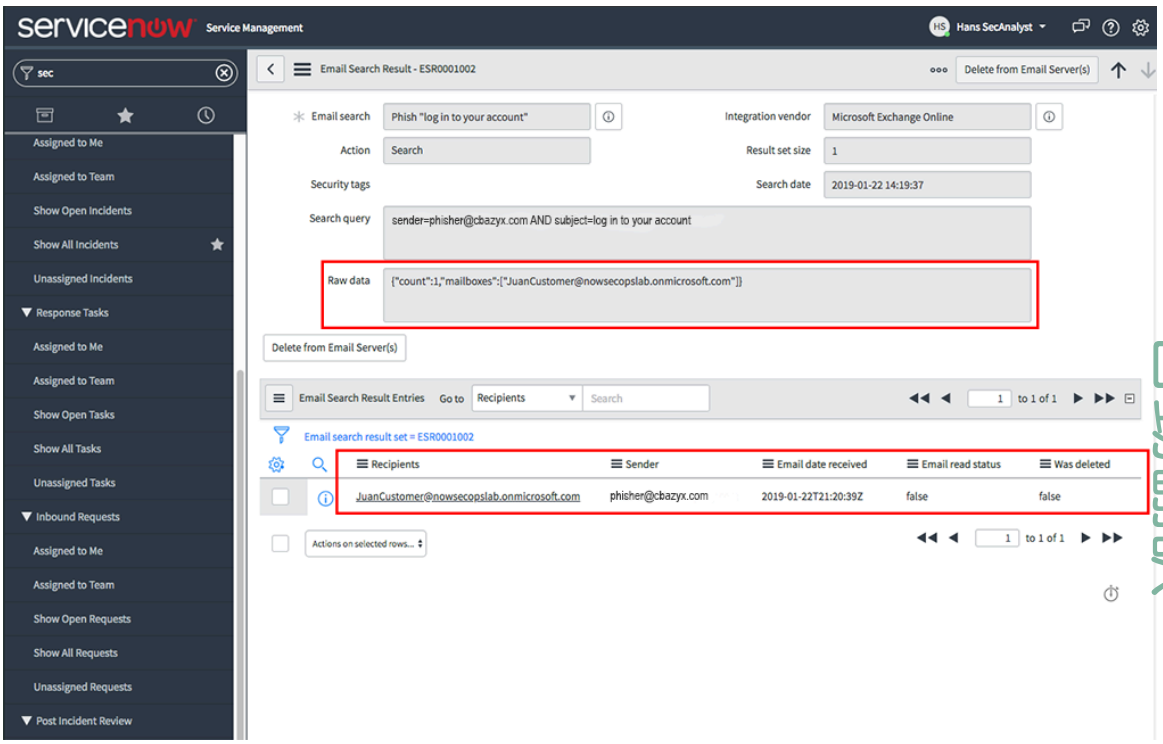
この通知では、フォローアップや削除が必要な、条件に一致した結果を確認できます。次の例は、検索条件に一致したメールが 1 件あることを示しています。Now Platform インスタンスのメール検索結果レコードへの [メール検索結果] リンクも表示されます。検索レコードを表示するには、このリンクをクリックします。



15. このメールから検索結果を表示するには、[メールの検索結果] リンクをクリックします。
メールの検索結果レコードが表示されます。このレコードでは、次のデータを検証およびレビューできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [生データ] フィールドには、検索条件に一致したメールの件数 {"count":1} とメールが見つかったメールボックスアドレス ["JuanCustomer@nowsecopslab.onmicrosoft.com"] が表示されます。
- [受信者] 列には、受信者 (JuanCustomer@nowsecopslab.onmicrosoft.com) が表示されます。
- [送信者] 列にはメールのソースが表示されます。
- [メール受信日 (Email date received)] 列には、メールを受信した日時が表示され、フィッシングキャンペーンのタイムラインを追跡するのに役立ちます。
- [メール読み取りステータス] 列では、この例のメールは未読です (false)。メールが既読の場合は、true が表示されます。
- [削除済み] 列では、この例のメールは削除されていません。メールが削除済みの場合は、true が表示されます。

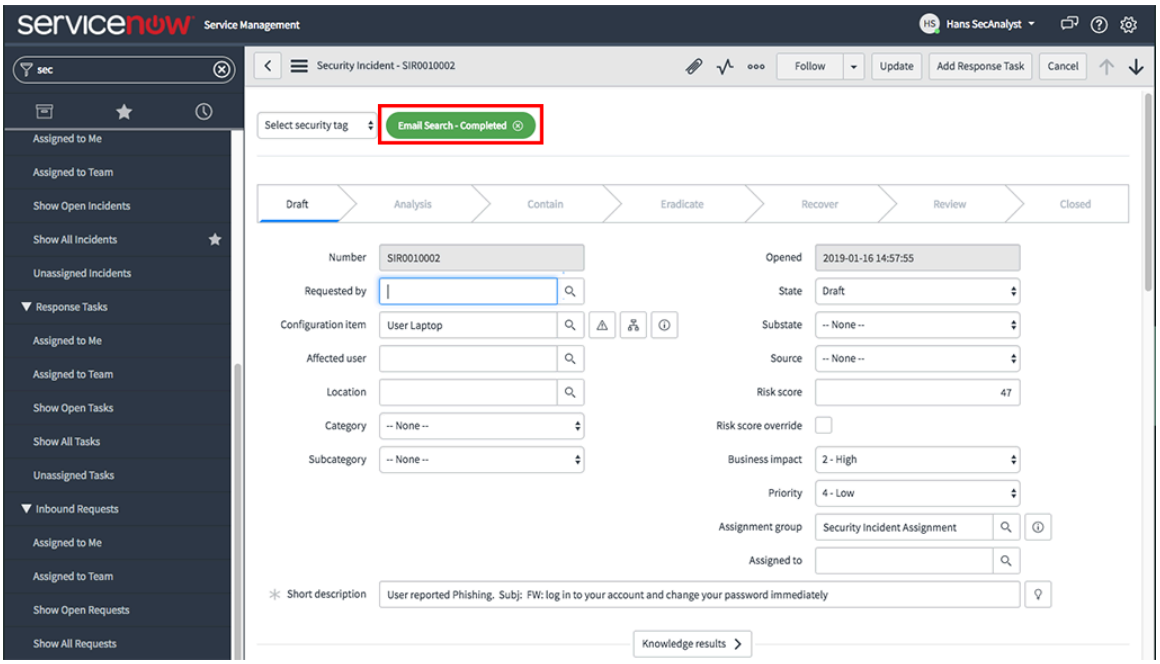


16. または、セキュリティインシデントから検索結果を表示するには、次の手順に従います。

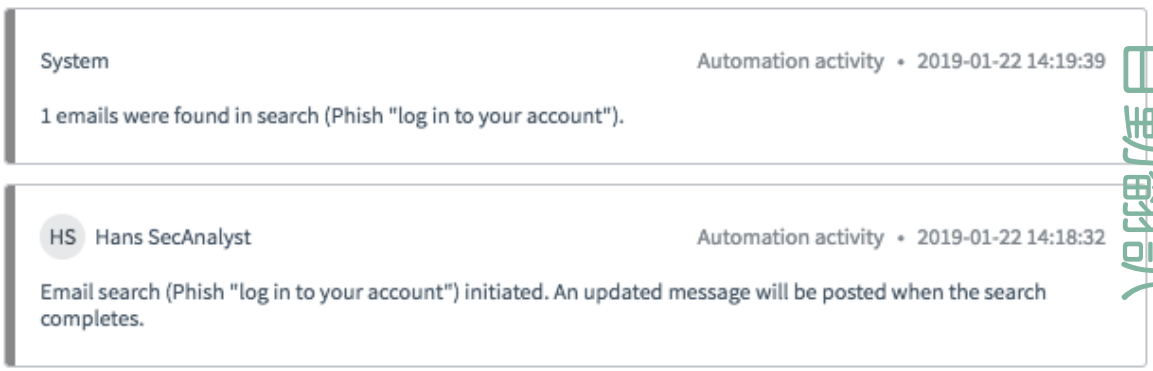
a. 次のように移動する。 セキュリティインシデント > インシデント をクリックし、操作しているセキュリティインシデントを開きます。
レコードの上部で、検索が正常に完了すると、[メールの検索 - 開始 (Email Search - Initiated)] セキュリティタグが [メールの検索 - 完了 (Email Search - Completed)] セキュリティタグで置き換わります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



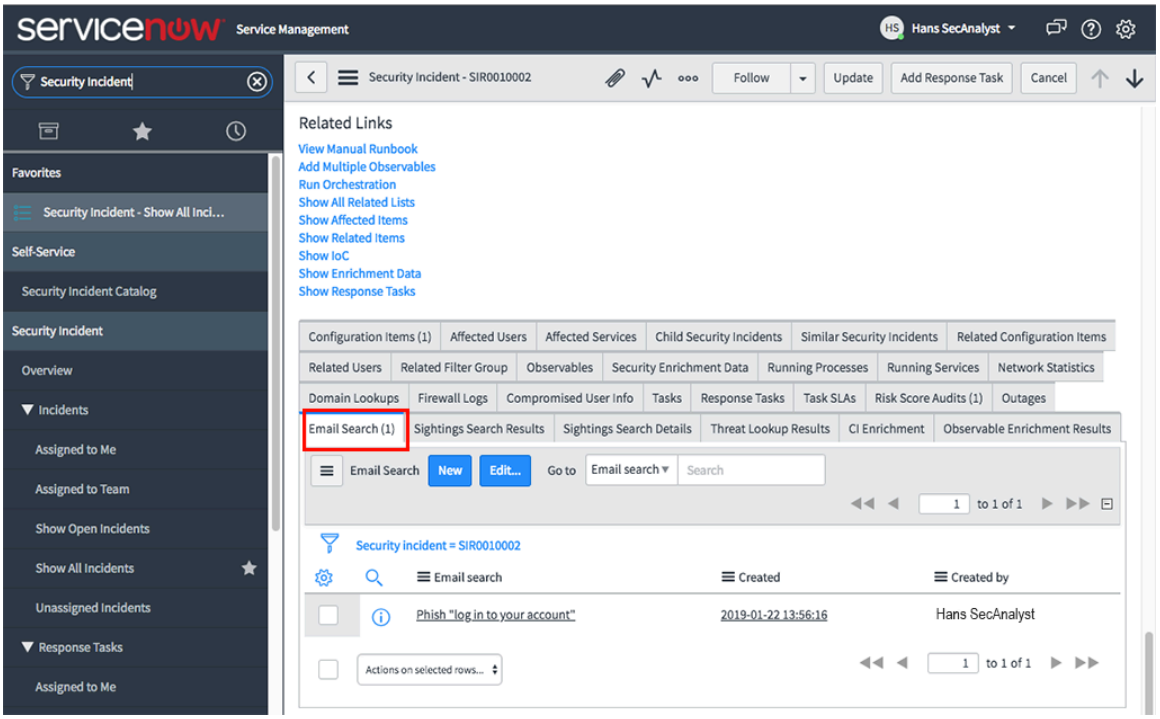
検索が正常に完了し、条件に一致するメールが 1 件見つかったことを示す作業メモが表示されます。



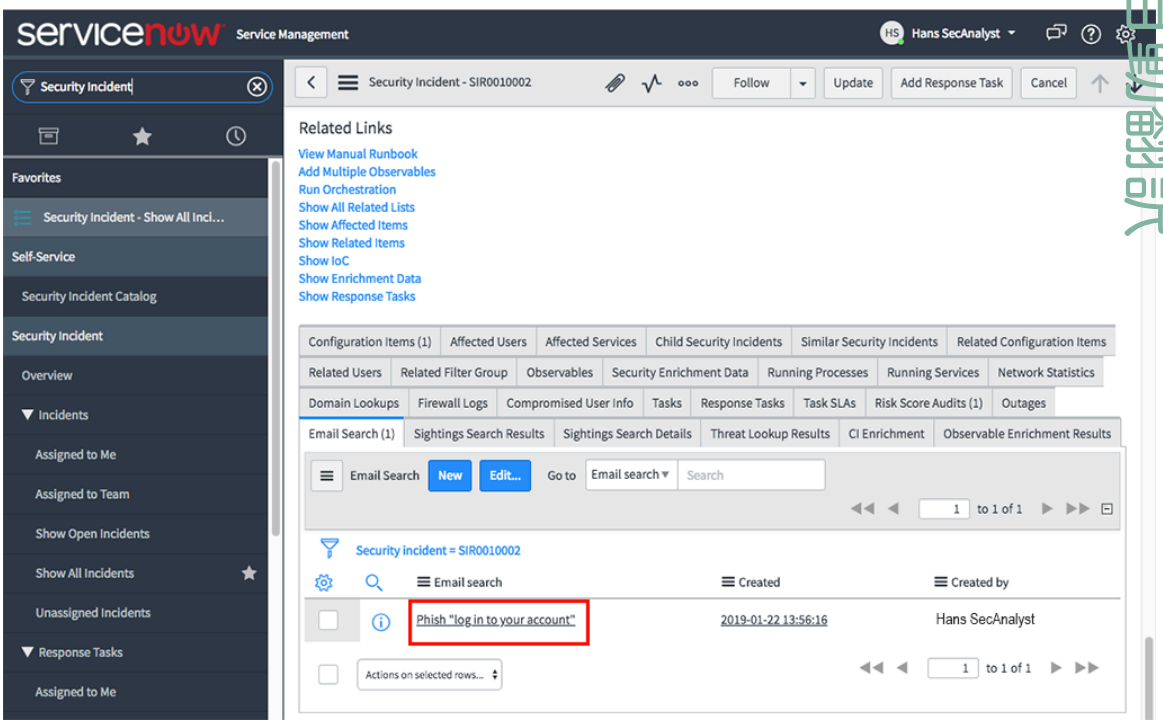
b. [セキュリティインシデント] レコードの一番下までスクロールし、[メールの検索 (Email Search)] 関連リストをクリックします。

[メールの検索 (Email Search)] 関連リストが表示されない場合は、[すべての関連リストを表示] 関連リンクをクリックして、この関連リストを表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



c. [メールの検索 (Email Search)] 関連リストを選択した状態で、[メールの検索 (Email Search)] 列で検索の名前をクリックします。

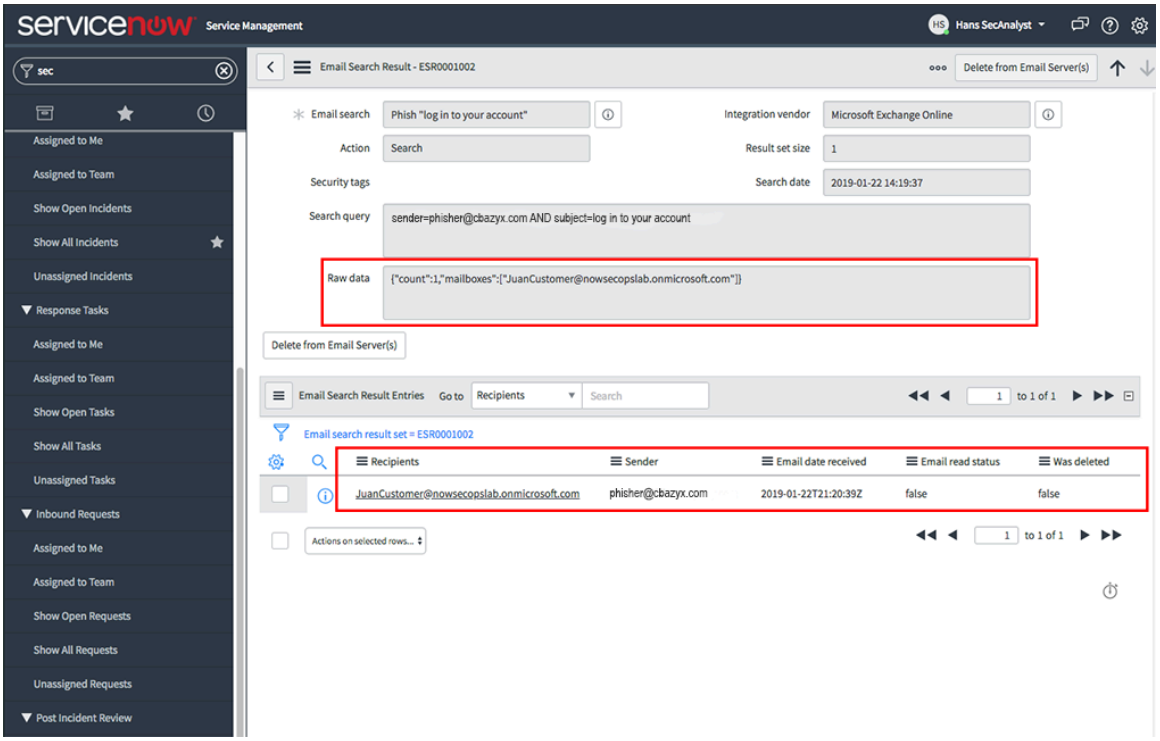


d. [メールの検索 (Email Search)] レコードで、 [メールの検索結果] 関連リストをクリックします。

e. [検索日] 列で、データを表示する検索の日付をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

メールの検索結果レコードが表示されます。



メール検索が正常に完了したら、結果を評価します。メールの修正が必要であると判断した場合は、これでメールを削除するか、削除承認を要求する準備ができています。

Microsoft Exchange Online サービスのメールの削除承認の要求

メールの検索が正常に完了し、一致するメッセージが特定された後、セキュリティインシデントとフィッシングキャンペーンに関連するすべての不審なメールを Microsoft Exchange Online サービスから完全に削除できます。

始める前に

必要なロール：sn_si.analyst

システムは、最後に成功した検索結果に対して削除を実行します。

このタスクについて

承認とメール通知が有効になっている場合は、メールを削除する前に承認グループにメールの削除要求を送信します。

メールの検索結果は、受信したあらゆるメッセージと併せて表示されます。フィッシングメールが正常に削除されたことを確認するため、関連するセキュリティインシデントの作業メモに削除結果が投稿されます。タグ付けが有効になっている場合は、関連するセキュリティインシデントにセキュリティタグも表示されます。メールが正常に削除されなかった場合は、作業メモでも通知されます。

組織のポリシーによっては、フィッシングメールを削除する前に承認を要求する必要があります。削除承認プロセスでは、削除するメールの件数に関する情報が必要です。場合によっては、他のメッセージの詳細へのアクセスが必要になることもあります。削除要求を処理するため、一致するメールメッセージの件数、完全なメッセージの詳細にアクセスするためのセキュリティインシデントリンク、承認/却下リンクがメール通知で承認者に提供されます。承認者は、このメールのリンクを使用してメール通知の削除要求を承認または却下できます。作業メモの承認ステータスがいつ変更されたかを追跡する、タイムスタンプ付きの完全な監査記録も利用できます。承認グループがアサインされている場合、グループのユーザー 1 人がグループ全体の要求を処理できます。承認グループの各メンバーは、要求のメール通知を受け取ります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

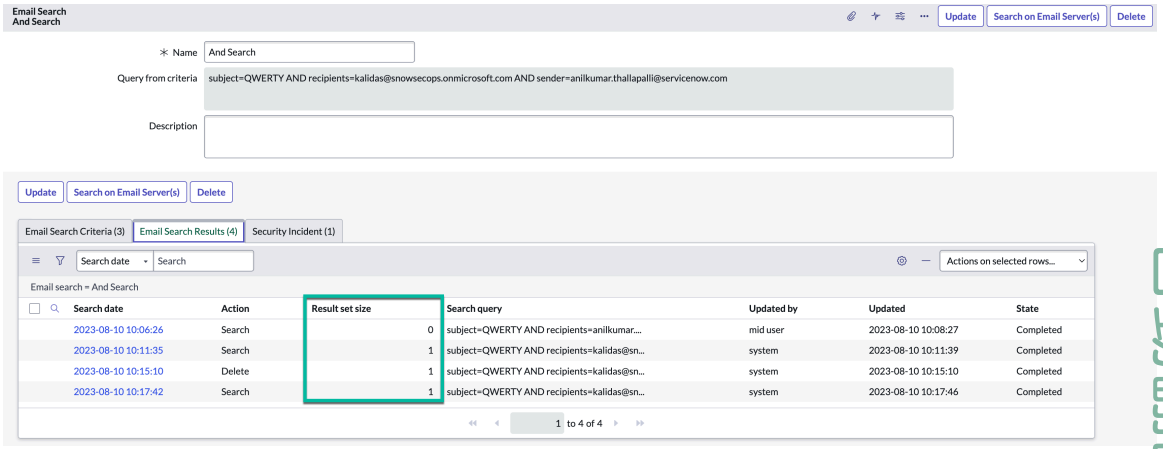
sn_si.analyst ロールを持つユーザーとして、メールの是正処置が必要であると判断した場合は、必要な手順に従ってメールを削除します。承認が有効になっている場合は、Microsoft Exchange Online サービスからメールを削除する承認を要求します。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント**>** すべてのインシデントを表示.
2. [メールの検索 **(Email Search)]** 関連リストをクリックします。
3. [メールの検索 (Email Search)] 関連リストを選択した状態で、[メールの検索 (Email Search)] 列で検索の名前をクリックします。
   検索結果は、[メールの検索結果] 関連リストに表示されます。

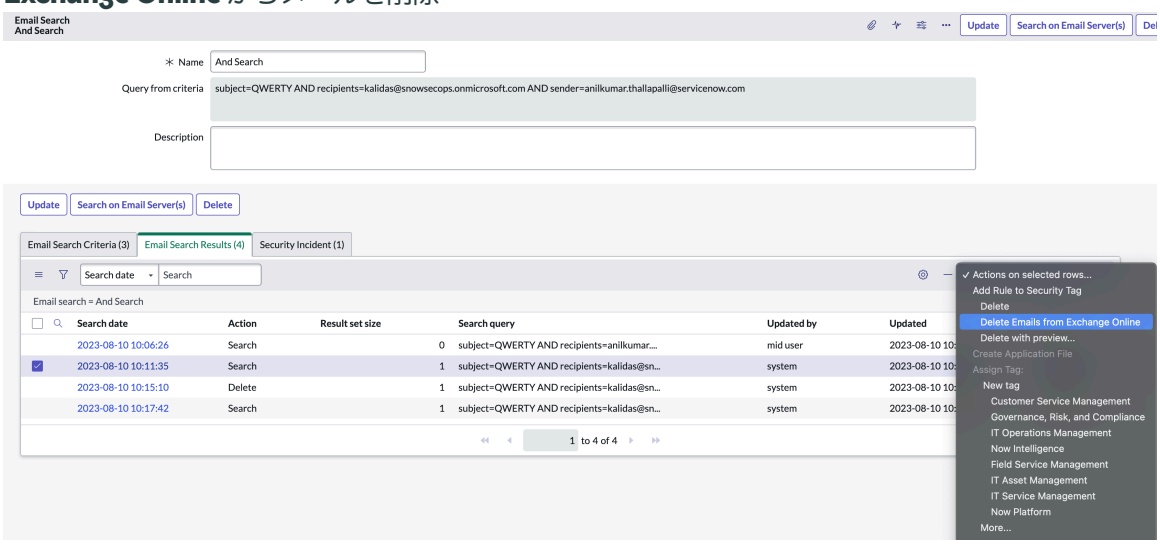
   この例では、この検索で検索条件に一致するメールが見つかっています。レコードには 2 つの検索アクションがリストされています。一方の検索では一致するメールがなく (0)、もう一方の検索で一致するメールが 1 件見つかっています (1)。

メールの検索結果セットのサイズ



4. 検索に関連付けられたメールアイテムを削除するには、[検索日] 列の左側にある検索結果セットのチェックボックスをオンにします。
   リストから 1 つの結果セットまたは複数の結果セットを選択できます。
5. 削除したい結果セットを選択します。

Exchange Online からメールを削除



自動翻訳

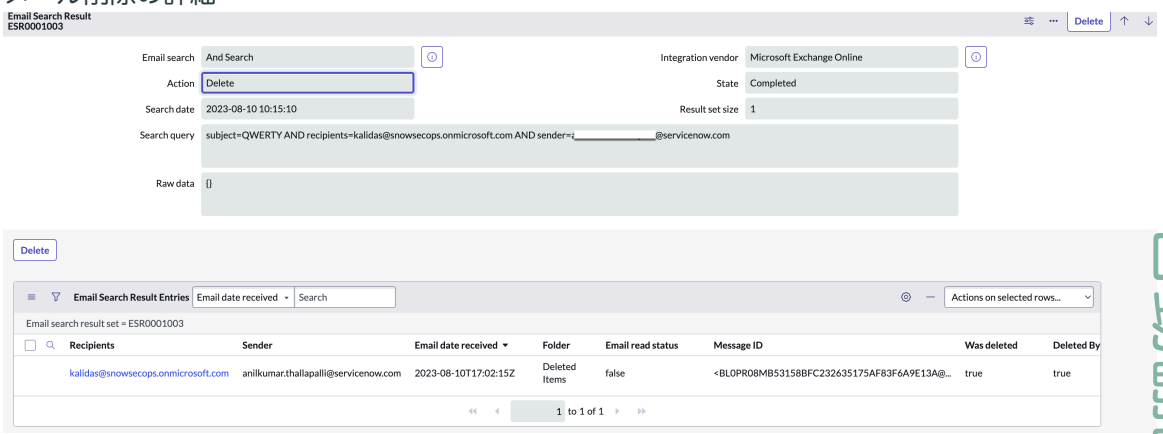
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [メールの検索結果] 関連リストの下部にある [選択した行のアクション] リストから、**[Exchange Online からのメールを削除]** を選択して、Exchange Online サーバーの 1 つ以上の結果セットに関連付けられたすべてのメールアイテムを削除します。
結果セットに複数のメールが含まれていても、[メールの検索結果] レコードを開いてメールを個別に選択して削除する必要はありません。**[Exchange Online からメールを削除]** を選択すると、[メールの検索結果] レコードの [削除済み] 列でステータスが false のすべてのメールアイテムが削除されます。

   結果セット内のメールアイテムがすでに削除されている場合、メール検索結果レコードの [削除済み] 列のステータスは true です。これらのアイテムは再度削除されません。

   設定手順で承認オプションを無効にしている場合は、**[Exchange Online からメールを削除]** を選択すると、結果セットに関連付けられているメールが削除されます。結果セット自体は削除されません。ただし、結果セットの削除されたすべてのメールアイテムのステータスが、[メールの検索結果] レコードの [削除済み] 列で、true に更新されます。承認機能の詳細については、「Now Platform インスタンスと Microsoft Exchange Online の統合の設定」を参照してください。

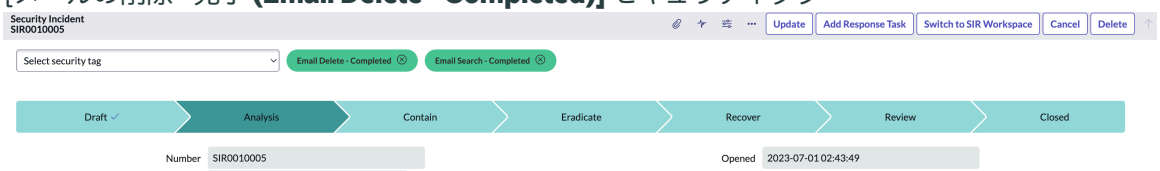
   メール削除の詳細

   これらのメールは、検索を実行した Microsoft Exchange Online テナントから削除されます。メールが正常に削除されると、作業メモが表示されます。

   セキュリティインシデントレコードに、［メールの削除 - 完了 (Email Delete - Completed)］セキュリティタグが表示されます。

   [メールの削除 - 完了 **(Email Delete - Completed)]** セキュリティタグ

   削除要求の承認が無効になっている場合は、Microsoft Exchange Online テナントからメールを正常に削除できています。

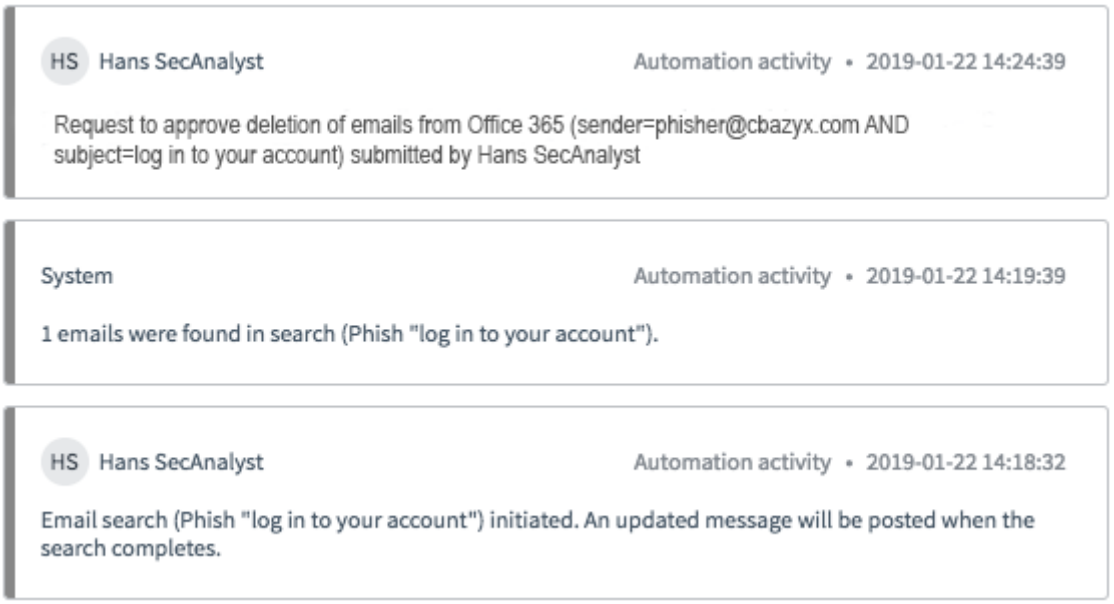
   設定手順で削除要求の承認を有効にしている場合は、**[Exchange Online からメールを削除]** を選択すると、設定手順で選択した承認グループの各メンバーにメール通知が送信されます。

   設定手順でタグ付けが有効になっている場合は、関連するセキュリティインシデントレコードに、［メールの削除 - 開始 (Email Delete - Initiated)］セキュリティ タグが表示されます。タグ付けの詳細については、「Now Platform インスタンスと Microsoft Exchange Online の統合の設定」を参照してください。

   sn_si.analyst ロールを持つユーザー (Hans SecAnalyst) からメールを削除する要求が送信されたことを示す作業メモが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

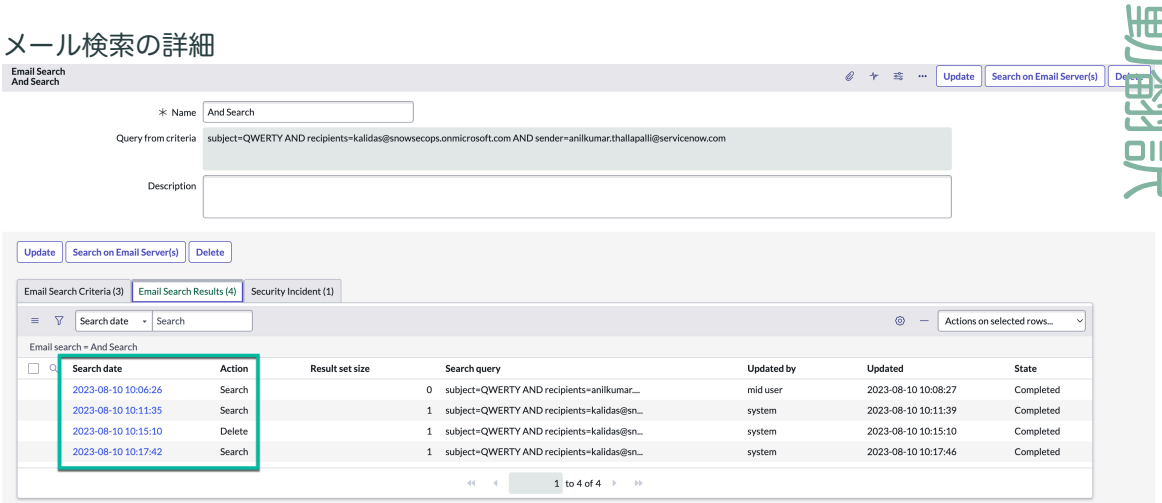
自動翻訳



承認が有効になっている場合、次のステップは削除要求の処理です。

7. または、メールを削除したり、削除要求を送信したりする前に、検索レコードの詳細や個々のメールアイテムを表示したい場合は、次の手順に従います。

   a. [メールの検索結果] 関連リストを選択した状態で、[検索日] 列で、確認したい検索の日付をクリックします。



自動翻訳

メールに関する次の情報が表示されます。

- 受信者
- 送信者
- メール受信日
- メール読み取りステータス (true または false)
- 削除済み (true または false)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 統合によって削除済み (true または false)

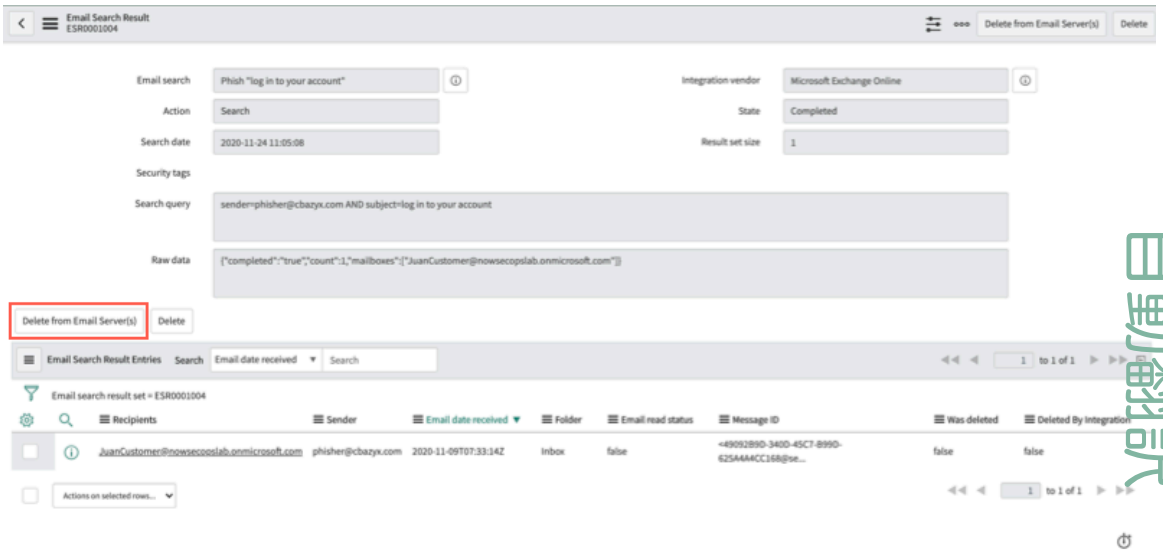
  注:

  アナリストが [メールサーバーから削除] を開始して、メールが削除されると、値が true に設定されます。

  作業メモは、統合とユーザーによって削除されたレコードを含む、削除済みレコードの合計数で更新されます。

b. データを確認した後、すべてのメールを削除するか、すべてのメールを削除する要求を送信するには、[メールサーバーから削除] をクリックします。

前の例で説明したように、検索結果レコードに複数のメールがリストされている場合は、それらを削除するために個々のメールを選択する必要はありません。削除要求は、最新の検索結果の [削除済み] 列に false が表示されている場合、検索に関連付けられているすべてのメールを削除します。



承認が有効になっている場合は、これでメールの削除要求が正常に送信されています。前の例で説明したように、セキュリティタグと作業メモが関連するセキュリティインシデントレコードに表示されます。承認者としての次のステップは削除要求の処理です。

Microsoft Exchange Online 統合のメール削除要求の承認

Now Platform インスタンスで承認オプションが有効になっている場合、メールの削除要求が承認グループの各メンバーにメールで送信されます。設定手順で承認グループを選択します。承認を有効にすると、組織はいっそう細かくメールの削除を制御できるようになります。

始める前に
Exchange Online メール検索および削除の [構成設定] フォームの [追加の設定] タブで [承認] オプションが選択されていることを確認します。

承認要求用の Now Platform インスタンスで [メール送信の有効化] および [メール受信の有効化] オプションを有効にしていることを確認します。詳細については、「Microsoft Exchange Online 統合での Now Platform インスタンスの設定」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

sn_si.analyst ロールを持つユーザーがメール削除要求を送信すると、デフォルトでは、これらの要求はメールで sn_si.admin に送信されます。承認グループを作成した場合、グループの各メンバーは通知を受け取ります。承認者は、メール通知からメールの削除要求を直接処理できます。または、Now Platform インスタンスのメール検索結果レコードから要求を処理することもできます。このトピックでは、両方の承認方法を示します。

次の情報は、メール通知に含まれる要求についての説明です。

メール検索結果のレコード番号

監査記録の一部として Now Platform によって検索レコードに割り当てられた一意の番号

要求を送信したアナリストの名前

監査記録の一部として要求を送信した人物の名前

セキュリティインシデントへのリンク

フィッシングイベントに関連するセキュリティインシデントへのリンク。作業メモ、メール検索、メール検索結果を含むセキュリティインシデントをメールから直接表示します。

承認または却下リンク

メール通知から要求を承認または却下するためのリンク。どちらかのリンクをクリックすると、関連するワークフローが自動的に開始され、作業メモがセキュリティインシデントレコードに投稿されます。

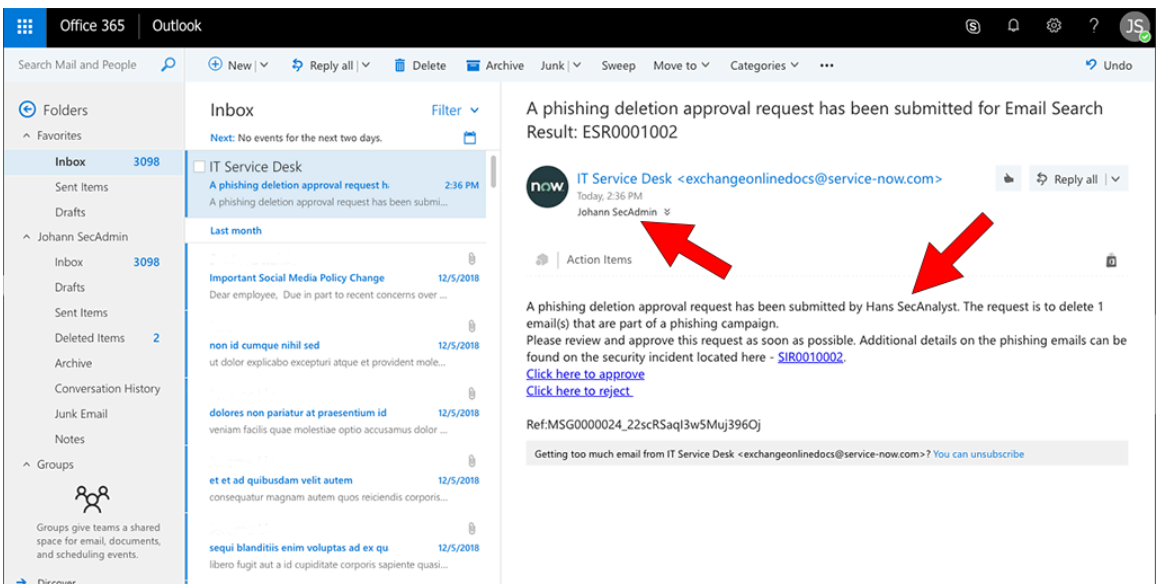
必要なロール：sn_si.admin またはアサインされた承認グループのメンバー全員

手順

1. メール通知から削除要求を処理するには、次の手順に従います。

   a. 承認者として、Now Platform ユーザー アカウントで設定したメールアカウントで通知メールを見つけます。

   この例では、sn_si.analyst ロールを持つユーザー (Hans SecAnalyst) が 1 件のメールを削除する要求を送信します。Johann SecAdmin は承認グループのメンバーです。

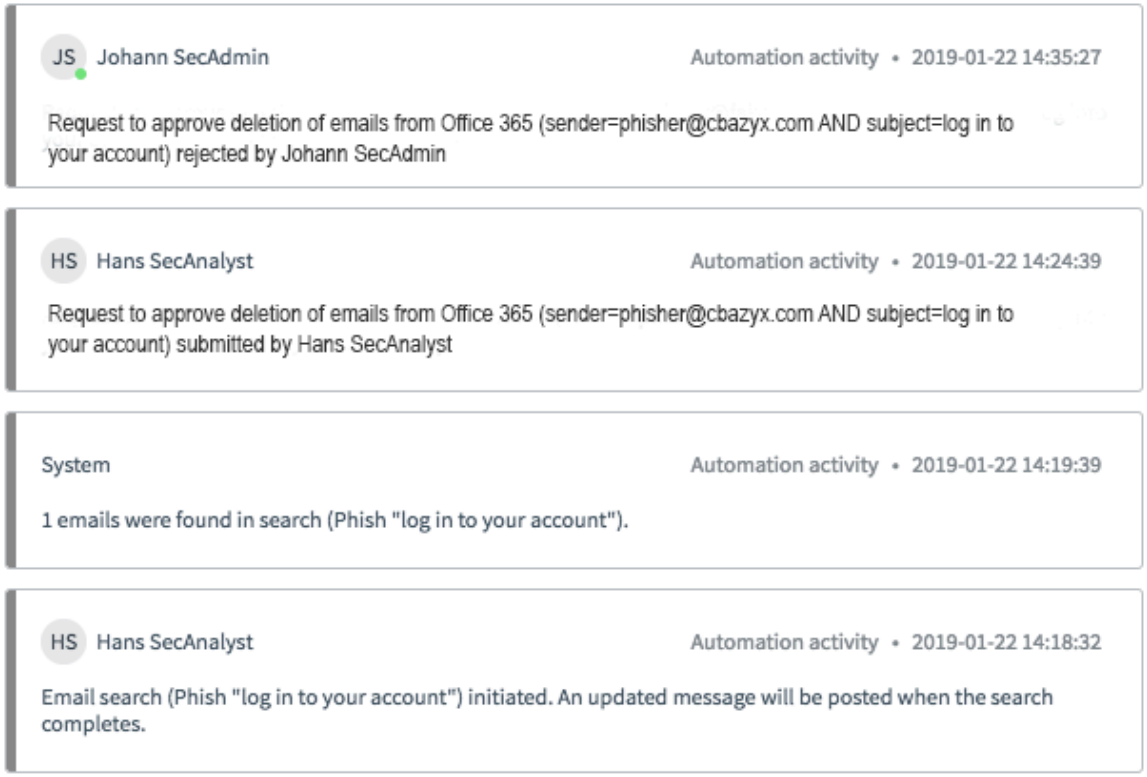


   b. メール通知でオプションを 1 つ選択して続行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

次の画像は、この例の関連セキュリティインシデントレコードの作業メモによって作成された監査記録の例を示しています。承認者がメール通知から要求を却下すると、作業メモは要求を却下したユーザーによって投稿されます。Johann SecAdmin はこの要求を却下します。



要求を却下したユーザー (Johann SecAdmin) の Now Platform インスタンスで、 **[Self-Service] > [My Approvals]** を選択します。、[ステータス] 列に［却下 ］と表示されます。

承認グループのメンバーの誰か 1 人によって要求が却下された後、sn_si.analyst ロールを持つユーザーとして、それらのメールを削除する必要があると判断した場合は、それらを削除する新しい要求を送信する必要があります。

この例では、要求が却下された後、sn_si.analyst ロールを持つユーザーが新しい要求を送信します。

承認グループの別のメンバーである John Approver は、前の例に示したようなメールを受信します。John Approver もこの要求を処理できます。

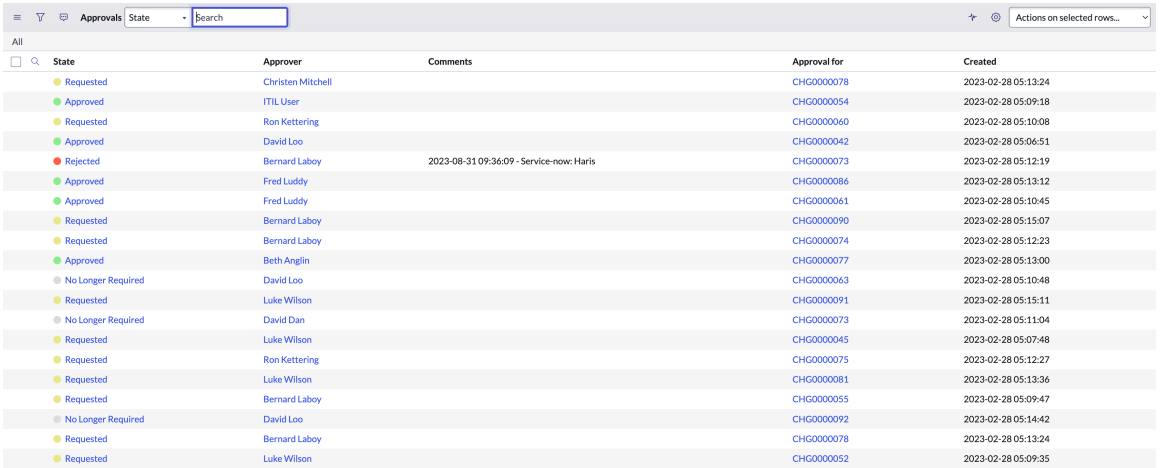
2. または、承認者は次の場所に移動します。 **[Self-Service] > [My Approvals]** を選択します。 削除要求を表示および処理するために、 Now Platform インスタンスで行います。
[自分の承認 **(My Approvals)]** からの要求を処理するには、次の手順に従います。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. 次のように移動する。 **[Self-Service] > [My Approvals]** を選択します。.

自分の承認リスト



Approvals | State | Search | Actions on selected rows...

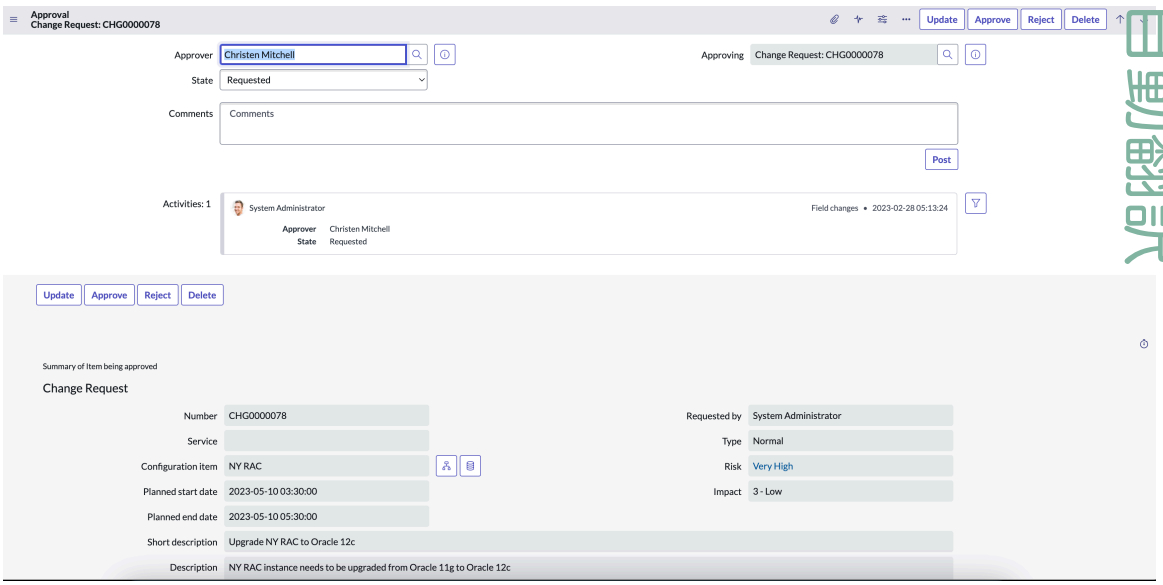
All

State	Approver	Comments	Approval for	Created
Requested	Christen Mitchell		CHG0000078	2023-02-28 05:13:24
Approved	ITIL User		CHG0000054	2023-02-28 05:09:18
Requested	Ron Kettering		CHG0000060	2023-02-28 05:10:08
Approved	David Loo		CHG0000042	2023-02-28 05:06:51
Rejected	Bernard Laboy	2023-08-31 09:36:09 - Service-now: Haris	CHG0000073	2023-02-28 05:12:19
Approved	Fred Luddy		CHG0000086	2023-02-28 05:13:12
Approved	Fred Luddy		CHG0000061	2023-02-28 05:10:45
Requested	Bernard Laboy		CHG0000090	2023-02-28 05:15:07
Requested	Bernard Laboy		CHG0000074	2023-02-28 05:12:23
Approved	Beth Anglin		CHG0000077	2023-02-28 05:13:00
No Longer Required	David Loo		CHG0000063	2023-02-28 05:10:48
Requested	Luke Wilson		CHG0000091	2023-02-28 05:15:11
No Longer Required	David Dan		CHG0000073	2023-02-28 05:11:04
Requested	Luke Wilson		CHG0000045	2023-02-28 05:07:48
Requested	Ron Kettering		CHG0000075	2023-02-28 05:12:27
Requested	Luke Wilson		CHG0000081	2023-02-28 05:13:36
Requested	Bernard Laboy		CHG0000055	2023-02-28 05:09:47
No Longer Required	David Loo		CHG0000092	2023-02-28 05:14:42
Requested	Bernard Laboy		CHG0000078	2023-02-28 05:13:24
Requested	Luke Wilson		CHG0000052	2023-02-28 05:09:35

b. [ステータス (State)] 列で、要求アイテムをクリックします。

表示される承認レコードには、検索、検索要求、および検索結果に関するデータが一覧表示されます。

承認の詳細



Approval
Change Request: CHG0000078

Update | Approve | Reject | Delete

Approver: Christen Mitchell
State: Requested
Approving: Change Request: CHG0000078
Comments
Post
Activities: 1
System Administrator — Field changes • 2023-02-28 05:13:24
Approver: Christen Mitchell
State: Requested

Update | Approve | Reject | Delete

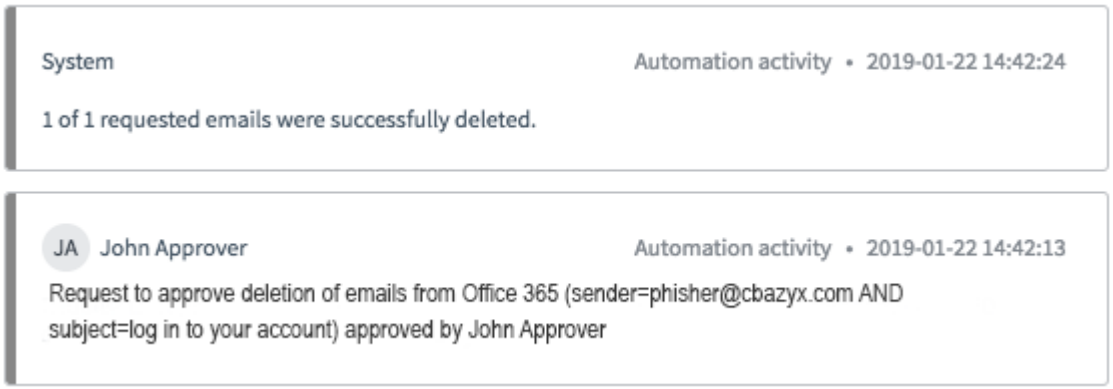
Summary of Item being approved

Change Request

Number	CHG0000078	Requested by	System Administrator
Service		Type	Normal
Configuration item	NY RAC	Risk	Very High
Planned start date	2023-05-10 03:30:00	Impact	3 - Low
Planned end date	2023-05-10 05:30:00		
Short description	Upgrade NY RAC to Oracle 12c		
Description	NY RAC instance needs to be upgraded from Oracle 11g to Oracle 12c		

c. このレコードで要求を承認するには、[承認] をクリックします。
要求が承認されると、システムが削除ワークフローを開始し、メールを削除します。次の画像は、この例の関連セキュリティインシデントレコードの作業メモによって作成された監査記録の例を示しています。この削除要求が再度送信されると、承認されます。要求の承認に使用された方法に関係なく、正常に削除されたメールの件数が作業メモに投稿されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



メールが正常に削除された後、タグ付けが有効になっている場合、関連するセキュリティインシデントレコードで、[メールの削除 - 開始 (Email Delete - Initiated)] タグが [メールの削除 - 完了 (Email Delete - Completed)] タグに置き換えられます。

メンテナンス **[Self-Service] > [My Approvals]** を選択します。 承認者 (John Approver) のステータスが [要求済み] から [承認済み] に変わります。

メンテナンス **[Self-Service] > [My Approvals]** を選択します。 承認グループの他のメンバー (Johann SecAdmin など) の場合、要求が承認されるとステータスが [不要] に変わります。

3. または、関連するセキュリティインシデントレコードのメール検索結果レコードでメールが削除されていることを確認するには、次の手順に従います。

a. 次のように移動する。 セキュリティインシデント**>**すべてのインシデントを表示 フィッシング関連のセキュリティインシデントを特定します。
レコードの下部に関連リストが表示されます。

b. [メールの検索 **(Email Search)]** 関連リストをクリックします。

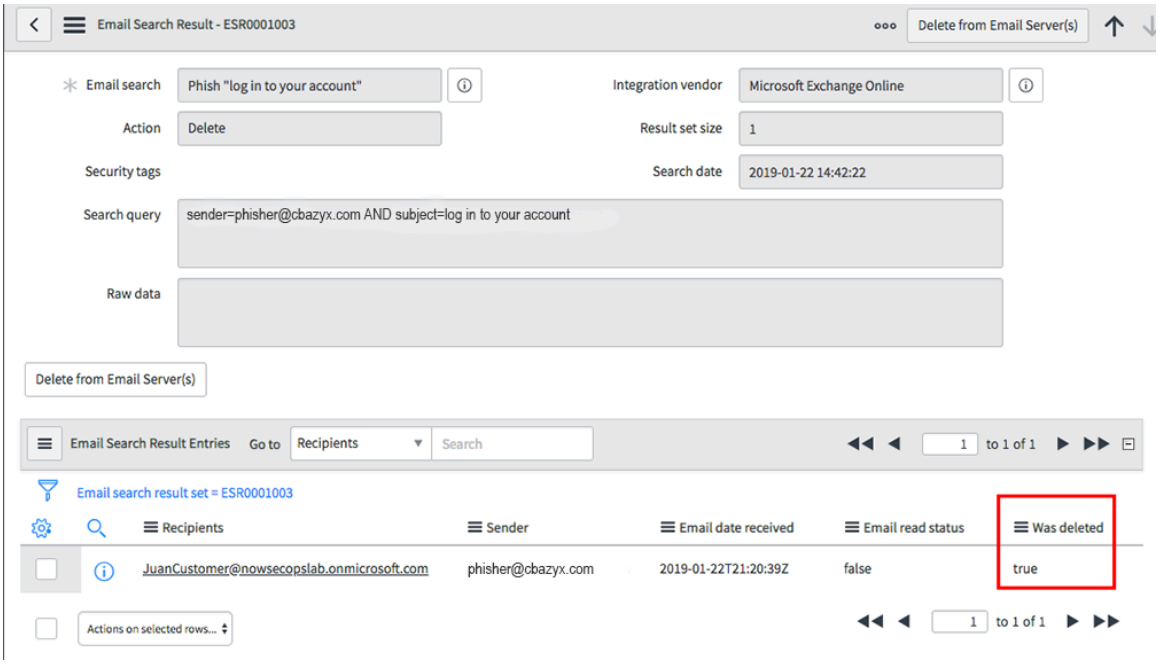
c. [メールの検索 (Email Search)] 列で検索の名前をクリックします (フィッシュ「アカウントへのログイン」 (Phish "log in to your account"))。
[メールの検索 (Email Search)] レコードが表示されます。[メールの検索 (Email Search)] 関連リストが表示されない場合は、[すべての関連リストを表示] リンクをクリックします。

d. [メールの検索結果] 関連リストをクリックします。
[検索日] 列には、メールの検索および削除アクションが対応する日付とともに表示されます。

e. [検索日] 列で、削除アクションに対応するアイテムをクリックします。
表示される [メールの検索結果] レコードの [削除済み] 列ステータスは、メールが削除されたことを示しています (true)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



これでメール通知と承認レコードの両方からのメール削除要求を承認し、メールが削除されたことを確認できました。[メールの検索結果] レコードを特定する方法の詳細については、「メール検索条件の定義と Microsoft Exchange Online サービスに対する検索の要求」を参照してください。

Microsoft Exchange Online 統合の統合アーキテクチャと外部システム接続

Microsoft Exchange Online 統合アーキテクチャは、 Microsoft Exchange Online サービスのメール脅威の検索および削除機能をサポートするために開発されました。この概要では、なぜ ServiceNow アプリケーションをインストールする前に Microsoft アカウントでいくつかのセットアップ手順を完了する必要があるのかについて説明します。

統合アーキテクチャは、現在利用可能なアプリケーションプログラミングインターフェイスの評価に基づいており、Microsoft の統合担当者の助言を得ています。この情報は、 Now Platform および Microsoft Exchange Online サービスに関する重要な用語と併せて、統合の概念的な操作を明確にするために提供されています。

この統合で使用される重要な用語

インストールと構成では、次の重要な用語が使用されます。以下の用語の詳細については、ServiceNow の製品ドキュメント Web サイト および Microsoft のドキュメント Web サイト を参照してください。

Now Platform

エンタープライズ ServiceNow 製品。Now Platform はベースであり、その上に、セキュリティインシデントレスポンス (SIR)、IT Service Management (ITSM)、その他の製品などの個々のコンポーネントがビルドされています。

セキュリティインシデントレスポンス (SIR)

セキュリティインシデントの発見と初期分析から、封じ込め、根絶、復旧、インシデント後の最終レビューとクローズまで、その進捗を追跡する Now Platform アプリケーション。

Microsoft Exchange Online

Microsoft 製品の Office 365 スイートの一部である Microsoft Exchange Online のメールサービスオファリング。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Global Graph API

Microsoft によって提供され、Microsoft Exchange Online のメールボックス情報にアクセスするために使用される API。

証明書ベースの認証

この認証により、アプリケーションとブラウザーのサインインのために、Azure Active Directory (Azure AD) に対して X.509 証明書を使用した直接認証をユーザーに許可するか、要求することができます。

OAuth 認証

追加のメールメッセージの詳細を収集し、 Microsoft Exchange Online のメールを削除するのに使用する、Microsoft Azure ポータルで作成される ID。

Windows ホスト

この統合で使用される特定のタイプの仮想マシン。

MID サーバー

Now Platform と外部アプリケーション、データソース、サービスの間の通信やデータの移動を支援する Now Platform アプリケーション。通常、MID サーバーが必要になるのはオンプレミステクノロジーと統合するときですが、統合に顧客提供のコンポーネントが必要な場合に、Now Platform とクラウドベースのオファリングの間に MID サーバーが展開されることがあります。この Microsoft Exchange Online サービス統合では、MID サーバーは Now Platform と PowerShell サーバーの間の通信を支援します。

PowerShell サーバー

PowerShell サーバーは、Microsoft アカウントの認証情報を必要とする Microsoft アプリケーションです。

セキュリティインシデントアドミン (sn_si.admin)

sn_si.admin ロールを持つユーザーは、Now Platform インスタンス内の SIR 製品との統合の設定を監督します。このロールを持つユーザーは、デフォルトでメールの削除要求の承認を担当し、必要に応じて sn_si.analyst ロールをアサインします。このロールを持つユーザーは、すべての サービス管理 データを完全に制御できます。

セキュリティインシデントアナリスト (sn_si.analyst)

sn_si.analyst ロールを持つユーザーは、SIR 製品でセキュリティインシデントに対応し、分析します。

メールの検索と削除のための外部システム接続

このアプリケーションは、Office 365 セキュリティ/コンプライアンスセンター PowerShell サービスと Global Graph API サービスを使用して、Office 365 Exchange Online サービステナントから情報を取得します。統合が正しく機能するには、MID サーバーからこの環境への送信 HTTPS 接続が必要です。

この統合アーキテクチャは、Microsoft Exchange Online サービスにおけるメールの検索および削除機能をサポートします。この統合アーキテクチャは、組織のセキュリティを侵害する可能性のあるフィッシングメールやその他のメール脅威をターゲットにしています。Now Platform は、指定された検索クエリ条件に一致するメールを取得するため、Windows サーバーで PowerShell を実行する MID サーバーを使用して、Microsoft Exchange Online サービステナントに接続します。

Now Platform が Microsoft Exchange Online サービスに接続された後、統合は以下のレベルのメール検索をサポートするようになります。

- 一致するメッセージ：この検索は、Now Platform のコンポーネントである Windows MID サーバーを通じて、Microsoft PowerShell コマンドレットで実行されます。この検索は、セキュリティインシデントに基づいて、Now Platform で設定した条件で実行されます。検索の最初のコ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

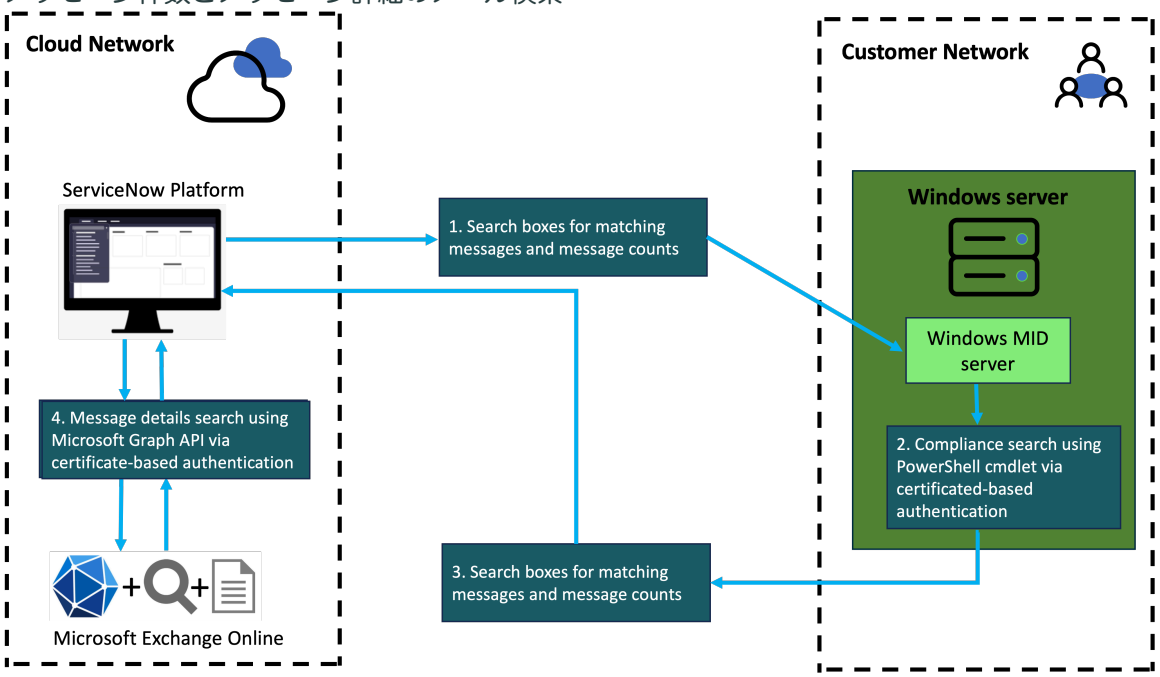
自動翻訳

ンポーネントは、 Microsoft Exchange Onlineでこれらのメッセージを見つけることができる特定のメールボックスアドレスに加えて、設定した検索条件に一致するすべてのメールメッセージを返します。サポートされている検索パラメーターは、メールメッセージの件名、送信者、受信者 (メールメッセージの [To] フィールドに表示される値) です。

- メッセージの詳細： 最初の PowerShell コマンドレットベースの検索で一致するメッセージが特定された後、この検索では Microsoft Global Graph API を使用して追加のメッセージ情報が取得されます。返されるメールの結果には、次のメッセージの詳細が含まれます。
  - 読み取りステータス：True または False のステータスでユーザーがいつメールを読んだかを追跡します。
  - 送信者アドレス
  - 受信者アドレス：個人、グループ、メッセージの CC および BCC として指定された個人が含まれます。
  - 削除ステータス：True または False のステータスで削除されたメールを追跡します。
  - メッセージ ID：メールメッセージの英数字の識別子

次の図に、メッセージの件数とメッセージ詳細を調べるメール検索の基本的なデータフローを示します。

メッセージ件数とメッセージ詳細のメール検索



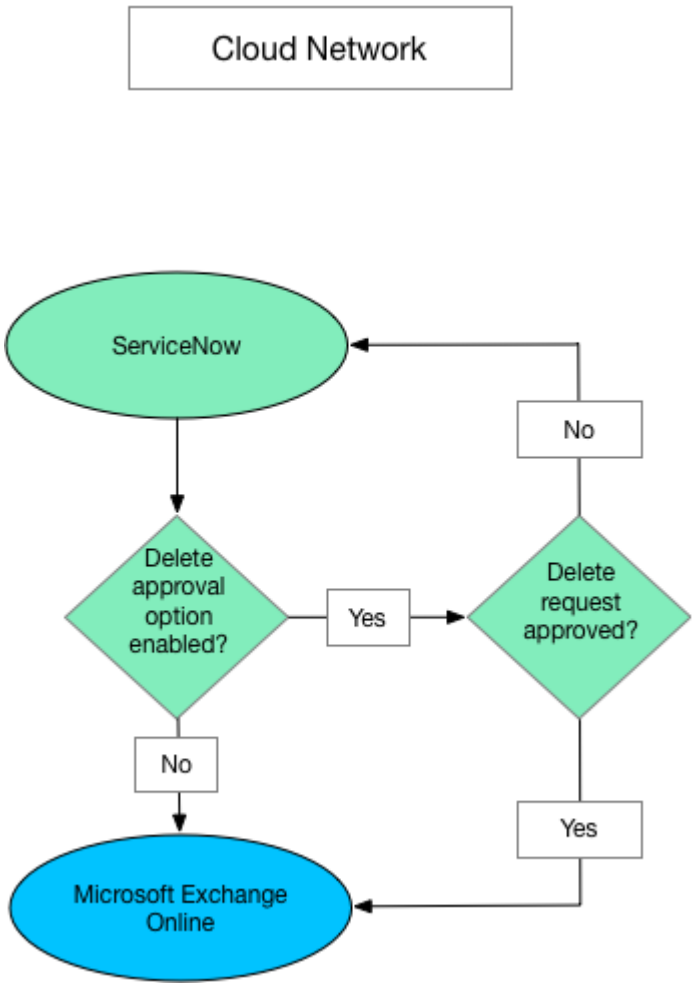
メールの削除の場合、統合は Global Graph API を使用します。削除されたメールの復元は、設定手順でオプションとして利用できます。詳細については、「Now Platform インスタンスと Microsoft Exchange Online の統合の設定」を参照してください。

事前設定された承認プロセスを使用したメール削除のデータフローを次の図に示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

メールの削除



フロー

メールの検索と削除のための Microsoft Exchange Online アプリケーションには、次のフローが含まれています。

- Exchange Online-メールの削除。
- Exchange Online メール詳細を取得します。
- Microsoft Exchange Online - メールの検索と削除

これで、統合に必要なアカウントをセットアップする準備ができました。

Microsoft Exchange Online サービスで削除されたメールの復旧

(オプション) インシデントの修正に、この統合のワークフローによって削除されたメールの復旧が必要な場合、Microsoft Exchange アドミニストレーターは削除されたメールを復元できます。

始める前に
この統合でどのようにメールが削除されるかの詳細については、「Now Platform インスタンスと Microsoft Exchange Online の統合の設定」を参照してください。

ユーザーメールボックス内の削除済みアイテムの復元に関する情報などの、 Microsoft Office 365 製品の管理ロールの詳細 については、「Exchange Online アドミンロールについて (About the Exchange Online admin role)」を参照してください。

必要なロール：Microsoft Exchange アドミン

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
設定手順で [追加の設定] タブの [削除されたメールの復元 **(Recover Deleted Emails)**] オプションを選択すると、Microsoft Exchange Online テナントで削除されたメールの復元が有効になります。この統合の削除ワークフローを使用して削除されたメールは、Microsoft Exchange Online サービスのユーザーのメールボックスにある [回復可能なアイテム] フォルダーの [削除済みアイテム] サブフォルダーに配置されます。ユーザーのアカウントが Microsoft Exchange Online テナントで [削除済みアイテム] フォルダーを表示できるように設定されている場合、ユーザーは Web 上の Microsoft Outlook サービスを使用してこれらのメールを復元できます。または、Microsoft Exchange Online アドミニストレーターがユーザーの [削除済みアイテム] フォルダーから削除されたメールを復元することもできます。詳細については、「Outlook Web App で削除済みのアイテムやメールを復元する」を参照してください。

必要なロール： Microsoft Exchange Online アドミニストレーターまたは Microsoft グローバルアドミニストレーター (削除されたメールの復元)

必要なロール：Now Platform の sn_si.admin ([削除されたメールの復元 (Recover Deleted Emails)] オプションの有効化)

必要なロール：Now Platform の sn_si.analyst (メールの検索を正しく実行し、復元の前にメールが正常に削除されたことを検証する)

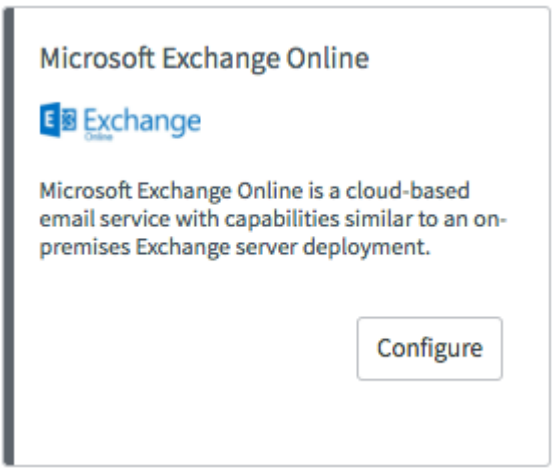
手順

メール復元オプションを有効にするには、次の手順に従います。

a. 次のように移動する。 セキュリティオペレーション > 統合 > 構成.

b. Microsoft Exchange Online タイルを見つけます。

c. [構成] をクリックします。

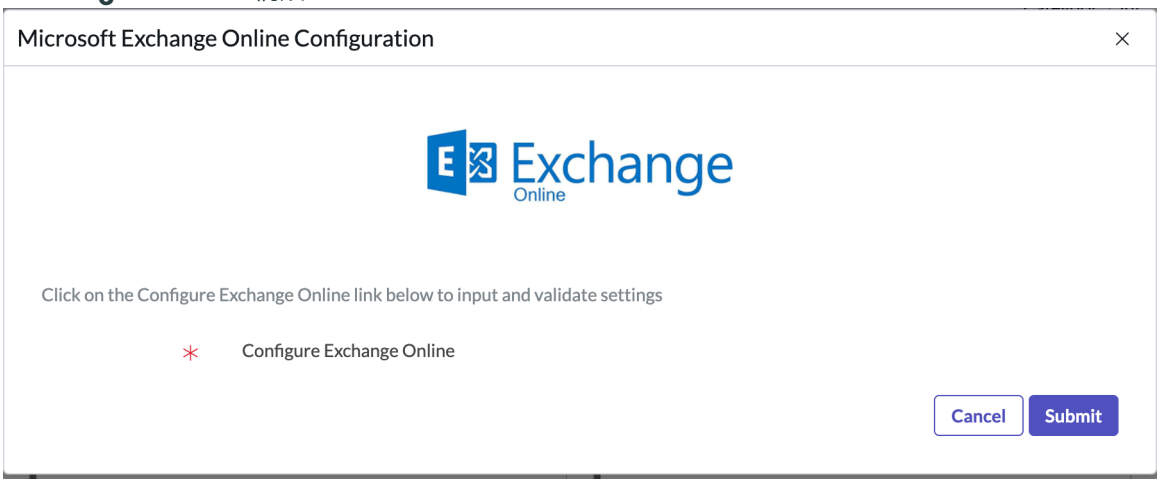


d. 表示される [Microsoft Exchange Online の構成 (Microsoft Exchange Online Configuration)] ダイアログボックスで、**[Exchange Online** を構成 **(Configure Exchange Online)]** をクリックします。

自動翻訳

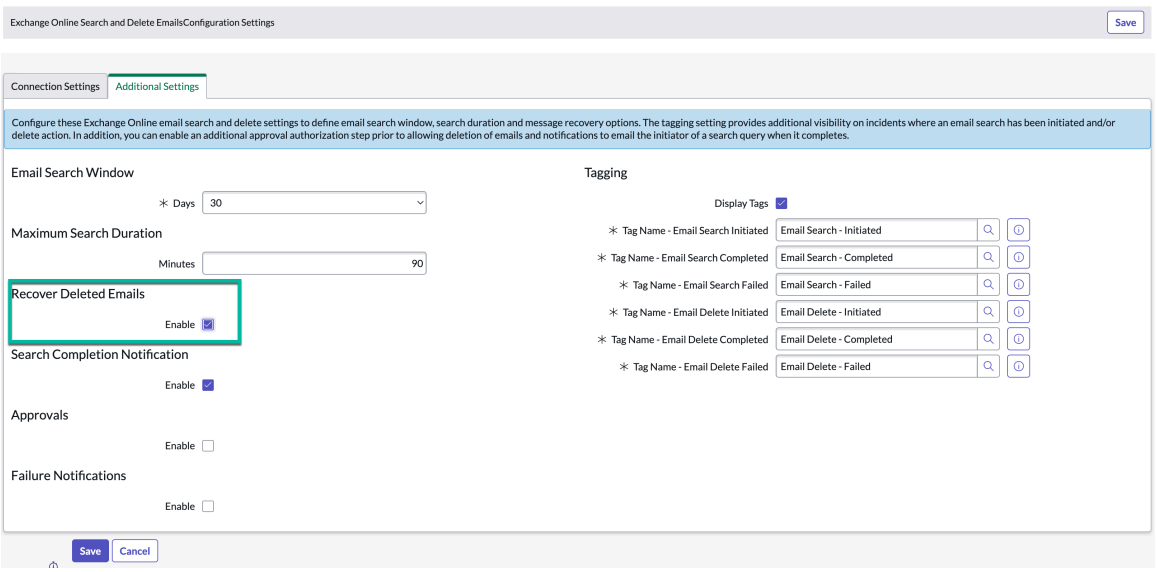
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Exchange Online の構成



e. [追加の設定] タブの [削除されたメールの復元 (Recover Deleted Emails)] で、[有効化] チェックボックスをオンにします。

削除されたメールを復元



f. その他の設定を確認し、[送信] をクリックします。

g. 復元したいメールメッセージの検索と削除が正常に完了していることを確認するには、メールの検索と削除のワークフローを記録したセキュリティインシデントに移動します。

h. 作業メモを見つけて、システムがメッセージを正常に削除したことを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

i. Microsoft Exchange Online アドミニストレーターまたはグローバルアドミニストレーターとして、Microsoft Office 365 アカウントにログインします。

j. Microsoft ドキュメント Web サイトの「Outlook Web App で削除済みのアイテムやメールを復元する」で説明されている手順に従います。

Microsoft Exchange Online 統合用の Now Platform のセキュリティタグの編集

Microsoft Exchange Online 統合用の Now Platform インスタンスのセキュリティタグは、名前と色を編集できます。これらのセキュリティタグは、メール検索が完了または失敗したときに、すばやく識別するのに役立ちます。また、メールの削除要求が開始されたとき、およびメールアイテムが正常に削除されたときも識別します。

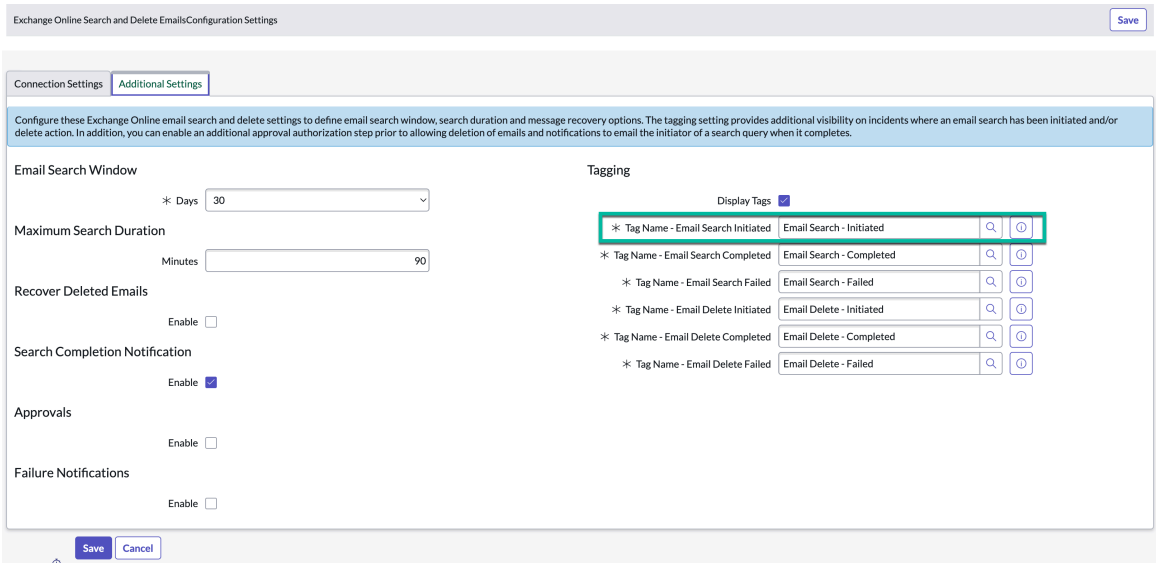
始める前に

デフォルトでは、設定手順で[タグを表示] オプションを選択した場合、Now Platform インスタンスでセキュリティタグが有効になります。タグの色と名前を編集して、セキュリティタググループにタグをアサインし、Now Platform インスタンスでタグを整理するのに役立てることができます。たとえば、機能の開始タグをある色に、完了タグを別の色に変更することで、Now Platform インスタンスで有効になっている他のセキュリティタグと一致させることができます。さまざまな色を設定することで、ワークフローが開始したとき、正常に完了したときにすばやく識別できます。特定のタグが必要ないと判断した場合は、統合でタグ付けを無効にするのではなく、タグレコードからタグを 1 つだけ無効にすることもできます。無効にすると、このタグは関連するセキュリティインシデントに表示されなくなります。セキュリティタググループとタグのセットアップの詳細については、Servicenow 製品ドキュメント Web サイトの「セキュリティタググループとタグのセットアップ (Set up security tag groups and tags)」を参照してください。

必要なロール：sn_si.admin

手順

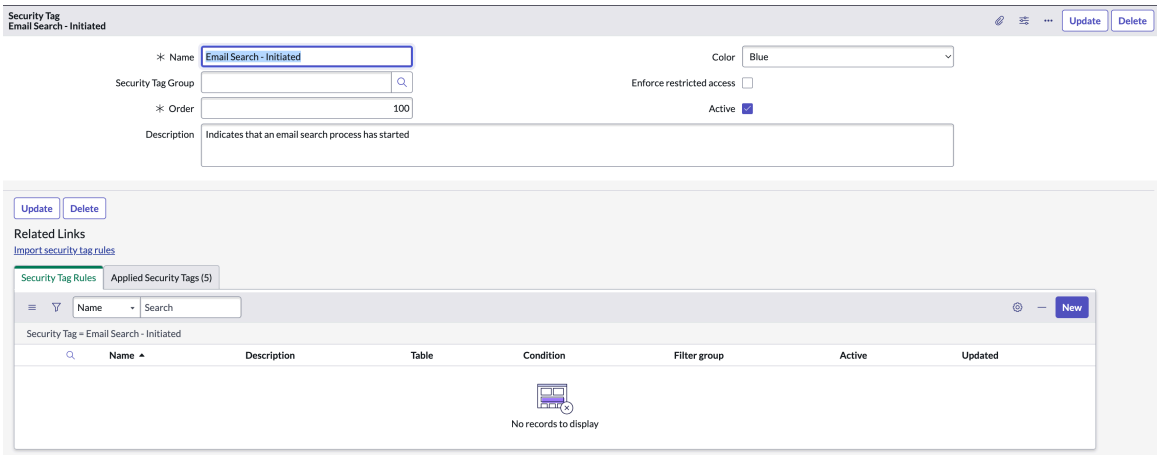
1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > 統合 > **Exchange Online** 設定.
2. [追加の設定] タブをクリックして選択します。
3. 表示されるタブで、[タグを表示] オプションがクリアされている場合、選択してタグ名を表示します。
4. タグ名を表示した状態で、タグの右にある情報アイコンをクリックします。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. 表示される [セキュリティタグ] ダイアログで、[レコードを開く] をクリックします。
6. 表示されるレコードで、フィールドを編集します。
7. [更新] をクリックして変更を保存します。



これでセキュリティタグのタグレコードを正しく編集できました。

Microsoft Exchange Online 統合のチェックリスト

このチェックリストを使用して、統合のエンドツーエンドのタスクをガイドします。次のチェックリストには、セットアップとインストールのタスク、およびアプリケーションのユースケースの例と予想される結果が含まれています。

始める前に

次のテーブルを使用して、統合のセットアップ、インストール、および構成の進捗状況を追跡します。次のステップに進む前に、ステップのすべてのタスクを完了してください。各ステップは、タスクの実行に必要なロールを識別し、この統合のインストールおよび設定ガイドの番号付きトピックを参照します。

必要なロール：ロールは次のテーブルのステップごとに記載されています。

手順

統合の進捗状況を追跡するには、テーブル内のステップを記載されている順に実行します。

チェックリスト

☐	Microsoft Office 365 アドミニストレーターとして、Microsoft Office 365 アカウントをセットアップします。 Microsoft Office 365 のセキュリティおよびコンプライアンスセンターへのアクセスを許可する API アカウントを作成します。
☐	Microsoft Azure アドミニストレーターとして、Microsoft Azure アカウントをセットアップします。 追加のメールメッセージの詳細を収集し、メールメッセージを削除するために、アプリケーション ID を使用するアカウントを作成します。アカウントのセットアップ手順については、「ServiceNow Microsoft Exchange Online

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

	Integration のための Microsoft Azure アカウントのセットアップ」を参照してください。
☐	Now Platform アドミニストレーターとして、統合のための Now Platform インスタンスをセットアップします。 タスクと詳細については、「Microsoft Exchange Online 統合での Now Platform インスタンスの設定」を参照してください。 **a.** Now Platform ロールをアサインします。 **b.** Now Platform インスタンスで MID サーバーをセットアップします。 **c.** Now Platform (SIR) および セキュリティオペレーション アプリケーションを ServiceNow Store からインストールし、インスタンスでアクティブ化します。 **d.** メールの送受信機能を有効にします。 **e.** sn_si.analyst にメールの読み取りおよび書き込みロールをアサインします。 **f.** 承認グループを作成します。
☐	Now Platform アドミニストレーターとして、ServiceNow Store から統合用のアプリケーションをインストールします。 インストール手順については、「ServiceNow Microsoft Exchange Online 統合用の Microsoft Exchange Online アプリケーションのインストール」を参照してください。
☐	sn_si.admin として、構成設定タブに入力して接続を確立し、検索と削除のワークフローをアクティブ化します。 接続と構成設定については、「Now Platform インスタンスと Microsoft Exchange Online の統合の設定」を参照してください。
☐	sn_si.analyst として、メール検索条件をセットアップし、Microsoft Exchange Online サーバーで条件に一致するメールの検索を要求します。例については、「メール検索条件の定義と Microsoft Exchange Online サービスに対する検索の要求」を参照してください。 **a.** フィッシングイベントに関連するセキュリティインシデントを特定します。 **b.** メール検索基準をセットアップします。 **c.** メールの検索を要求します。 **d.** セキュリティインシデントの関連リストで検索結果とメッセージの詳細を特定します。
☐	sn_si.analyst として、Microsoft Exchange Online サーバーからメールを削除します。例については、「Microsoft Exchange Online サービスのメールの削除承認の要求」を参照してください。 **a.** 検索結果を使用してセキュリティインシデントを特定します。 **b.** メールを削除するか、メール削除の承認を要求します。 **c.** セキュリティインシデントの作業メモおよび関連リストに投稿された結果からメールが削除されていることを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

	sn_si.admin として、または承認グループのメンバーとして、メール通知からメール削除要求を処理します。 例については、「Microsoft Exchange Online 統合のメール削除要求の承認」を参照してください。

これでセットアップ手順を完了し、統合に期待される結果を検証できました。

Microsoft Exchange Online Integration のトラブルシューティング

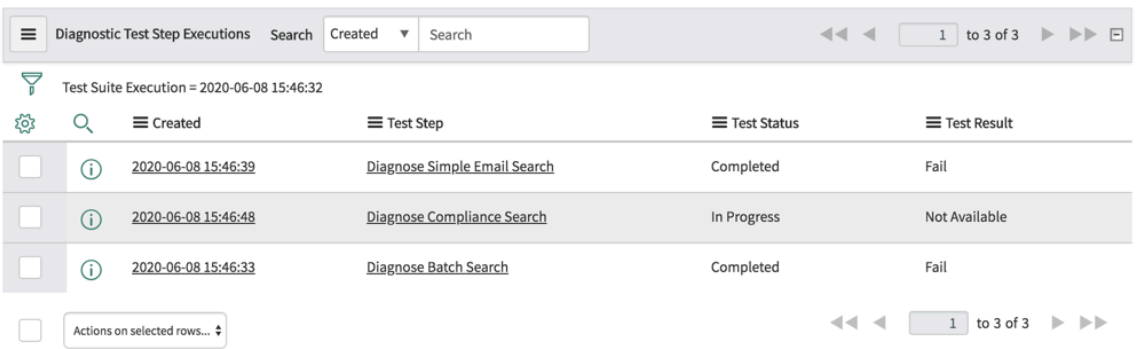
Microsoft Exchange Online アプリケーションを正しく設定し、Now Platform インスタンスをセットアップした後、メール検索の問題が発生した場合は、特定の基準に基づいて診断テストを実行できます。

始める前に
必要なロール：admin

このタスクについて
これらのテストの結果は、 ServiceNow カスタマーサポートが問題を特定してトラブルシューティングするのに役立ちます。

手順

1. 次のように移動する。 **All** (すべて) > **Exchange Online** 診断 > 診断テストの開始.
2. 以下の詳細を入力します。
   - 送信者と 1 件以上の受信者のメールアドレスを入力して検索条件を絞り込み、より正確な結果を提供できるようにします。
   - 診断テストを実行する件名を指定します。このフィールドは必須です。
3. [**Submit** (送信)] を選択します。
4. 診断テストの結果を表示するには、 **Exchange Online** 診断 > 診断テスト結果の表示.
   [ステータス] 列に次のステータスが表示されます。
   - 完了：合格：テストは正常に完了しました。
   - 完了：エラー：テストはいくつかのエラーが出て完了しました。
   - 処理中：テストはまだ実行中で、完了していません。
5. [診断テストスイート実行] をクリックすると、テスト実行の詳細が表示されます。



次のタイプの診断テストが実行されます。

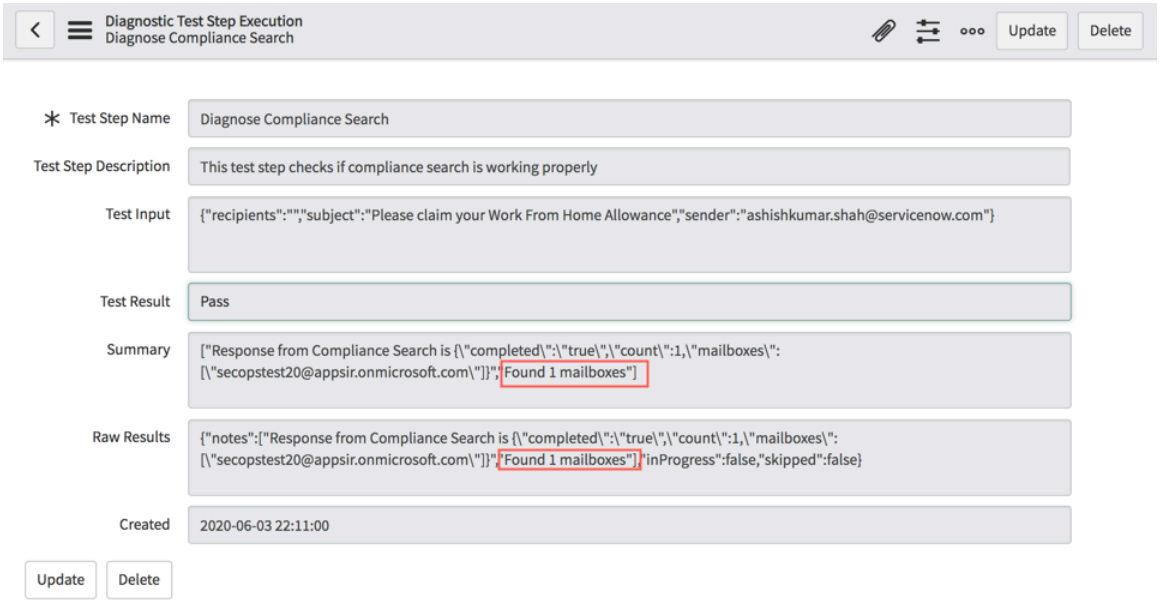
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- コンプライアンス検索を診断：コンプライアンス検索を実行して、受信者のメールボックスのリストを生成します。
- 簡易メール検索を診断 (Diagnose Simple Email Search)：個別に REST コールを実行して、受信者の各フォルダーを検索することで、メールボックスを検索します。
- バッチ検索の診断 (Diagnose Batch Search) – 1 つの REST コールに複数の検索を組み合わせることで、バッチクエリでメールボックスを検索します。

テスト 2 と 3 を実行するには、[診断テストの開始] ページで受信者のメールアドレスを指定する必要があります。指定されていない場合、テストは実行されません。

6. [診断テストスイートの実行] ページの [作成日時 (Created)] リンクをクリックすると、テスト結果の詳細が表示されます。



上の画像は、[コンプライアンス検索を診断] テストのステップ実行の詳細な結果と、検索で見つかったメールボックスの数を示しています。

重要:
その他のトラブルシューティングのシナリオと問題については、「KB1501969：Setup and troubleshooting of certificate based authentication for Exchange Online integration (Exchange Online 統合の証明書ベースの認証のセットアップとトラブルシューティング)」を参照してください

Microsoft Exchange On-Premises 統合

Microsoft Exchange On-Premises 統合は、オンプレミスインスタンスでフィッシングやスピアフィッシングのメール脅威を封じ込め、根絶するためのセキュリティアナリスト向けのツールを提供します。

詳細	セットアップ
セキュリティインシデントレスポンス の統合	Microsoft Exchange On-Premises 統合を開始する
使用	開発

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

フィッシングメールの検索と削除	• ServiceNow セキュリティオペレーション 統合開発のガイドライン • 統合を作成するためのヒント • 開発者トレーニング • 開発者ドキュメント • アプリケーションとともにインストールされているコンポーネントの検索

トラブルシューティングとヘルプ

- 統合のトラブルシューティング
- Security Operations Community で質問や回答をする
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

Microsoft Exchange On-Premises 統合を開始する

Microsoft Exchange On-Premises 統合は、オンプレミスインスタンスでフィッシングやスピアフィッシングのメール脅威を封じ込め、修正するためのセキュリティアナリスト向けのツールを提供します。Microsoft Exchange On-Premises 統合を使用する前に、ServiceNow Store からダウンロードし、適切な Exchange サーバーと MID サーバーを識別する必要があります。

始める前に

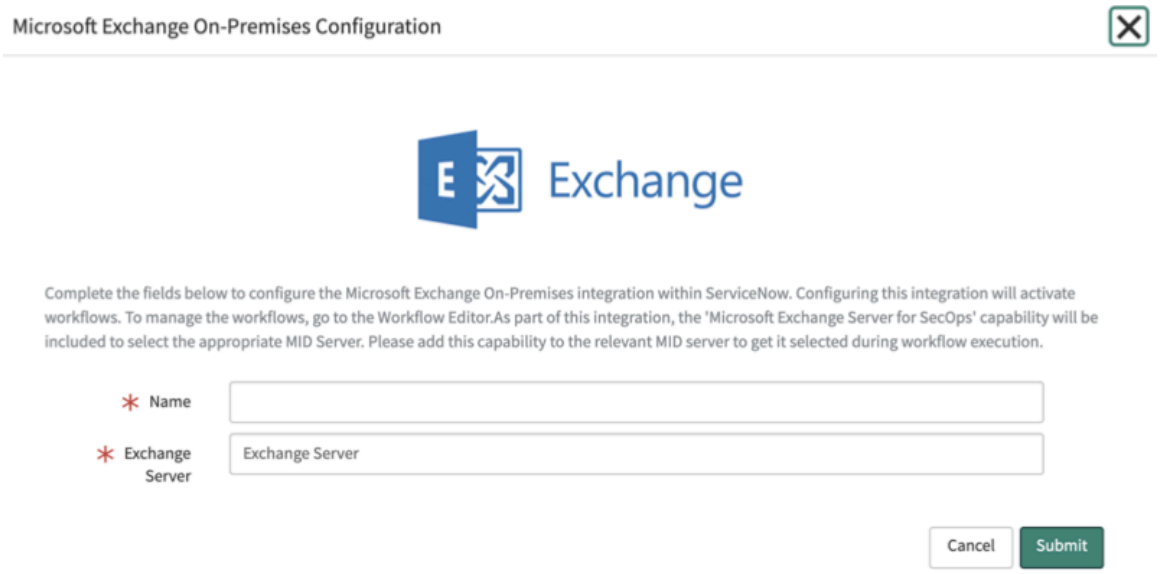
必要なロール：sn_si_admin

手順

1. から統合をダウンロードします ServiceNow Store.
2. インストールが完了したら、次に移動します: セキュリティオペレーション > 統合 > 統合設定. 利用可能なセキュリティ統合が一連のカードとして表示されます。
3. Microsoft Exchange On-Premises カードで、[新規] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. 必要に応じて、フィールドに入力します。

フィールド	説明
名前	この構成の名前。
Exchange Server	使用する Exchange サーバーを指定します。

> **注:**
> この統合を設定すると、フローが有効になります。フローを管理するには、ワークフロースタジオ/フローデザイナーに移動します。

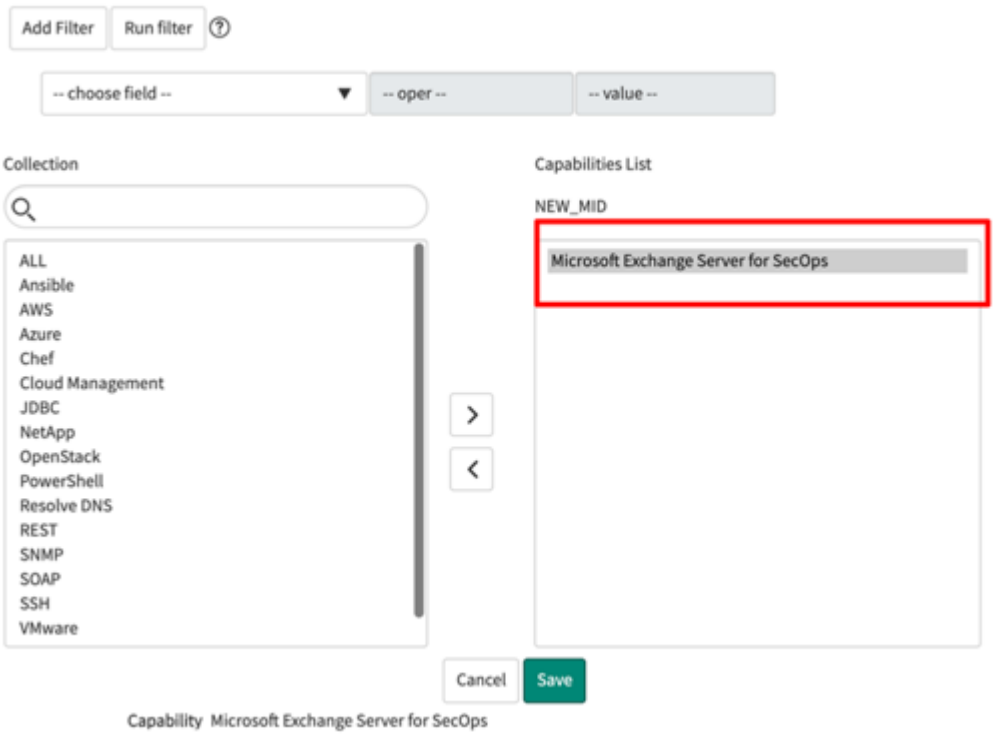
5. [**Submit** (送信)] を選択します。
   統合構成カードが表示されます。
6. 新しい構成カードを表示すると、[構成] または [削除] をクリックして、構成を変更または削除できます。
7. 統合構成カードの元のリストに戻るには、[構成を表示] ドロップダウンから [いいえ] を選択します。
8. 次のように移動する。 オーケストレーション > **MID Server**.
9. レコードを開き、Exchange サーバーに到達可能な MID サーバーのステータス、[ステータス] オプションが [稼働中] に設定されていること、[検証済み] オプションが [はい] に設定されていることを確認します。
10. MID サーバー機能を追加します。
    - 機能を追加するそれぞれの MID サーバーを選択します。
    - [機能] 関連リストをクリックし、[編集] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MID サーバーの機能

- [すべて] を削除して、**[Microsoft Exchange Server for SecOps (Microsoft Exchange Server for SecOps)]** を追加します。



- [関連リスト] セクションから **[IP** 範囲] を選択し、値を [すべて] または目的の値に設定します。
- [関連リスト] セクションから [サポートされているアプリケーション] を選択し、値を [すべて] または [オーケストレーション] に設定します。
- [保存] をクリックしてレコードを保存します。

11. 接続と資格情報を検証します。
12. 認証情報が検証されると、ServiceNow インスタンスの構成が完了し、この統合を使用してメールの検索および削除操作を実行できるようになります。

Microsoft Exchange - メールの検索と削除の実行フロー

[Microsoft Exchange - メールの検索と削除の実行 **(Microsoft Exchange - Perform Email Search and Deletion)]** フローが実行されると、指定された検索クエリを使用して Exchange サーバーが検索され、詳細がオンプレミスのインスタンスに返されます。

始める前に
必要なロール：sn_si.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
[**Microsoft Exchange -** メールの検索と削除の実行 **(Microsoft Exchange - Perform Email Search and Deletion**)] フローは、メール検索が設定され、[メールサーバーから削除] または [メールサーバーで検索] ボタンを押すと実行されます。

ここでは、この統合に固有のアクションについて説明します。他のアクションの詳細については、「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

フローアクションには次のものが含まれます。

- コンプライアンス検索アクションを作成
- コンプライアンス検索ステータスのチェックアクション

コンプライアンス検索プレビューアクションを作成

[コンプライアンス検索プレビューを作成] アクションは、作成されたコンプライアンス検索の Exchange サーバー上にプレビュータイプの新しいコンプライアンス検索アクションを作成します。

入力変数

アクションの初期動作が、入力変数によって決まります。

変数	説明
targetId	Exchange Server が配置されている必須のターゲットホスト識別子フィールド。
searchName	Exchange サーバーで作成されたコンプライアンス検索の必須名。

終了条件

このアクションの可能な終了条件は次のとおりです。

終了条件

変数	説明
完了	コンプライアンス検索アクションが正常に作成されたとき。
アクションの作成中にエラーが発生しました (Error Creating Action)	Exchange サーバーの例外によりコンプライアンス検索アクションの作成に失敗したとき。
エラー	フローアクションで例外が発生した場合。

プレビューアクションステータスの確認

プレビューアクションステータスは、プレビュータイプのコンプライアンス検索アクションのステータスをチェックし、受信者、送信者、件名、メールの受信日など、見つかったメールのプレビュー情報を返します。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

変数	説明
targetId	Exchange Server が配置されている必須のターゲットホスト識別子フィールド。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

変数	説明
searchName	Exchange サーバーで作成されたコンプライアンス検索の必須名。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。

出力変数

変数	説明
response	コンプライアンス検索の一部として見つかった、コンプライアンス検索アクションのステータスとプレビュー情報が含まれます。

終了条件

このアクションの可能な終了条件は次のとおりです。

終了条件

変数	説明
プレビューの進行状況	コンプライアンス検索アクションのステータスが進行中のとき。
メールが見つかりません (No Mail Found)	コンプライアンス検索アクションのステータスが完了で、コンプライアンス検索の一部としてメールが検出されていないとき。
プレビューが完了しました	コンプライアンス検索アクションのステータスが完了で、コンプライアンス検索の一部としてメールが検出されているとき。
ステータスの確認中にエラーが発生しました (Error Checking Status)	Exchange サーバーの例外によりステータスのチェックに失敗した場合。
エラー	ワークフローアクティビティで例外が発生したとき。

コンプライアンス検索削除アクションの作成

[コンプライアンス検索の作成] 削除アクションは、作成されたコンプライアンス検索の Exchange サーバー上に消去タイプの新しいコンプライアンス検索アクションを作成します。

入力変数

アクションの初期動作が、入力変数によって決まります。

変数	説明
targetId	Exchange Server が配置されている必須のターゲットホスト識別子フィールド。
searchName	Exchange サーバーで作成されたコンプライアンス検索の必須名。

終了条件

このアクションの可能な終了条件は次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

終了条件

変数	説明
完了	コンプライアンス検索アクションが正常に作成されたとき。
アクションの作成中にエラーが発生しました (Error Creating Action)	Exchange サーバーの例外によりコンプライアンス検索アクションの作成に失敗したとき。
エラー	フローアクションで例外が発生した場合。

削除アクションステータスの確認

[削除アクションステータスの確認 (Check Delete Action Status)] は、消去タイプのコンプライアンス検索アクションのステータスを確認し、コンプライアンス検索の一部として見つかったメールに対して Exchange サーバーで論理的な削除操作を実行します。

入力変数

アクションの初期動作が、入力変数によって決まります。

変数	説明
targetId	Exchange Server が配置されている必須のターゲットホスト識別子フィールド。
searchName	Exchange サーバーで作成されたコンプライアンス検索の必須名。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。

出力変数

変数	説明
response	コンプライアンス検索の一部として見つかった、コンプライアンス検索アクションのステータスと削除されたメールの数が含まれます。

終了条件

このアクションの可能な終了条件は次のとおりです。

終了条件

変数	説明
削除中	コンプライアンス検索アクションのステータスが進行中のとき。
メールが見つかりません (No Mail Found)	コンプライアンス検索アクションのステータスが完了で、コンプライアンス検索の一部としてメールが削除されていないとき。
削除完了	コンプライアンス検索アクションのステータスが完了で、コンプライアンス検索の一部としてメールが削除されているとき。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

終了条件 (続く)

変数	説明
ステータスの確認中にエラーが発生しました (Error Checking Status)	Exchange サーバーの例外によりステータスのチェックに失敗した場合。
エラー	フローアクションで例外が発生した場合。

コンプライアンス検索アクションを削除

[コンプライアンス検索を削除] アクションは、作成されたコンプライアンス検索を Exchange サーバーから削除します。

入力変数

アクションの初期動作が、入力変数によって決まります。

変数	説明
targetId	Exchange Server が配置されている必須のターゲットホスト識別子フィールド。
searchName	Exchange サーバーで作成されたコンプライアンス検索の必須名。

Microsoft Graph Security API アラート取り込み統合

Microsoft Graph Security API 統合を使用して、Microsoft Graph セキュリティプロバイダーからアラートを取り込み、自動でセキュリティインシデントを作成します。

概要

Microsoft Graph Security API は、複数のセキュリティプロバイダー (Microsoft ネイティブおよび ServiceNow パートナー) を接続する単一のプログラムインターフェイスを提供する中間サービス (またはブローカー) です。

Microsoft Graph Security API 統合では、Microsoft Graph Security API を使用して Azure Sentinel、Microsoft Defender Advanced Threat Protection、Azure Advanced Threat Protection などのさまざまな Microsoft セキュリティ技術と接続することで、これらの問題に対処します。Microsoft セキュリティプロバイダーからのアラートが取り込まれ、自動で セキュリティインシデントレスポンス にセキュリティインシデントが作成されます。

主な機能

この統合の主な機能は次のとおりです。

- セキュリティインシデントの候補である Microsoft Graph Security API アラートを検出し、セキュリティインシデントの作成を自動化します。
- アラートフィールドをセキュリティインシデントフィールドにマッピングします。
- 重複するセキュリティインシデントを作成するのではなく、既存のオープンセキュリティインシデントに類似したアラートを集計します。
- アラートフィールドの値をプレビューし、セキュリティインシデントのマッピングを検証します。
- セキュリティインシデントの作成とクローズに関するアラートステータスを自動更新します。
- アラートの取り込みをスケジュールして、セキュリティインシデントを定期的に作成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Microsoft Graph Security API 統合用の Now Platform インスタンス設定

次のセクションでは、ServiceNow Store からアプリケーションをインストールする前に Now Platform インスタンスで完了する必要があるセットアップタスクを示します。

始める前に

必要なロール：admin

このタスクについて

スムーズなインストールと構成を行うために、 アプリケーションをダウンロードしてインストールする前に、次のテーブルを参照して、リストされたすべてのタスクを完了していることを確認してください。

セットアップタスク	説明
必要な Now Platform ロールと セキュリティインシデントレスポンス ロールがアサインされていることを確認します。	Now Platform インスタンスで統合をインストール、セットアップ、および使用するには、次のロールが必要です。 • Now Platform アドミニストレーターロール (admin) を持つユーザーが ServiceNow Store からアプリケーションをインストールし、セキュリティインシデントアドミニストレーター (sn_si.admin) ロールをアサインします。 • sn_si.admin ロールを持つユーザーは、Now Platform で次のタスクを監督します。 ○ アラートプロファイルに名前を付け、作成し、編集します。 ○ Microsoft Graph Security API のアラートデータフィールドを選択してセキュリティインシデントフィールドにマップします。 ○ 構成を確定する前に、正確性を確認するためにセキュリティインシデントの詳細をプレビューします。 ○ 進行中のアラートの取り込みをスケジュールします。 ○ セキュリティインシデントレスポンス インシデントが作成されてクローズされたときに、アラートの更新を有効にします。 ○ セキュリティインシデントアナリスト (sn_si.analyst) ロールをアサインします。 ○ sn_si.analyst を持つユーザーは、セキュリティインシデントを処理します。 ロールとユーザーへのロールの割り当ての詳細については、Servicenow 製品ドキュメント Web サイト の「ロール」を参照してください。
Microsoft Azure ポータルでアプリケーションを登録します。	アラートを取り込む前に、Microsoft Azure ポータルでアプリケーションを構成する必要があります。詳細については、「Microsoft Azure ポータルの構成」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
統合用のアプリケーションをインストールする前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。 **1.** セキュリティインシデントレスポンス **2.** Security Operations のイベントとアラートの取り込み：このアプリケーションでは次のものが必要です。 ○ com.glide.hub.integration.runtime => ServiceNow 統合ハブランタイム ○ com.glide.hub.action_step.rest => ServiceNow 統合ハブアクションステップ - REST **注:** Integration Hub コンポーネントは、イベントおよびアラートの取り込みプラグインとともにインストールされます。これらがインストールされていない場合は、 カスタマーサポートに連絡してください。 セキュリティオペレーション コアアプリケーションのインストールの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

Microsoft Azure ポータルの構成

Microsoft Graph Security API を使用して Microsoft Azure テナントで利用可能なアプリケーションのセキュリティアラートを取得するには、アプリケーションを Microsoft Azure ポータルに登録し、セキュリティイベントに対しアプリケーションへの読み取りおよび書き込みアクセス権を付与する必要があります。

始める前に

必要なロール：

- アプリケーション開発者：アプリケーションの登録に必要です。
- テナントアドミン：Microsoft Azure テナントアドミンは、アドミン同意エンドポイントを呼び出してアプリケーションに権限を付与する必要があります。

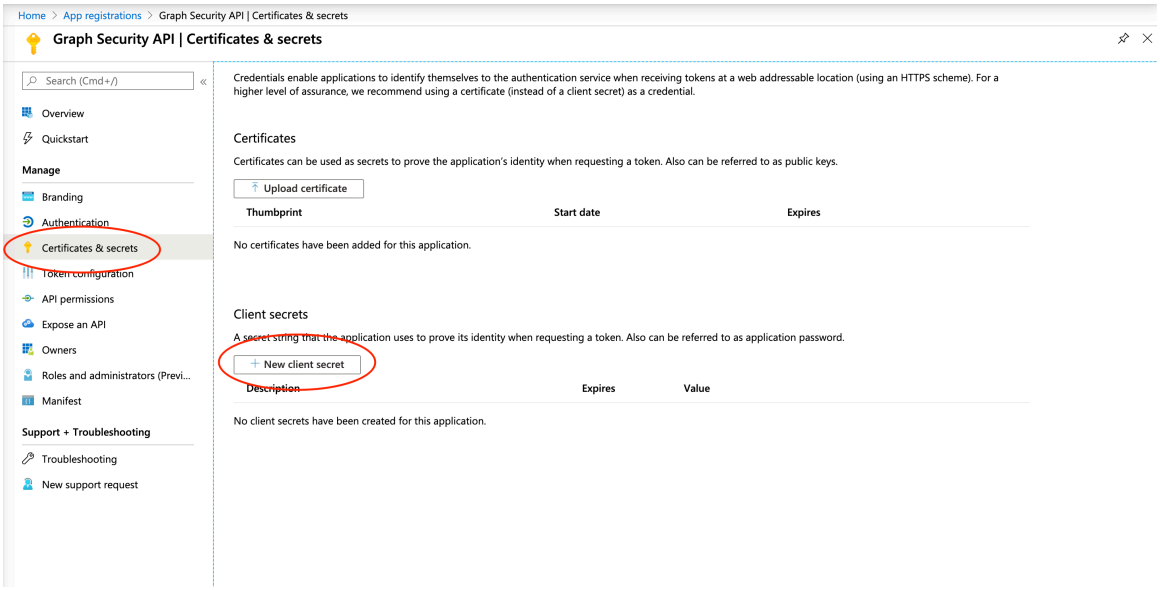
手順

1. Microsoft Azure ポータルにログインします。
2. [検索] ボックスに「**App registrations**」と入力します。
3. [新規登録] をクリックします。
4. アプリケーションの名前とリダイレクト URI (例：http://localhost) を入力し、[登録] をクリックします。
   リダイレクト URI は、アプリケーションに対してアドミン同意を提供するときに使用されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

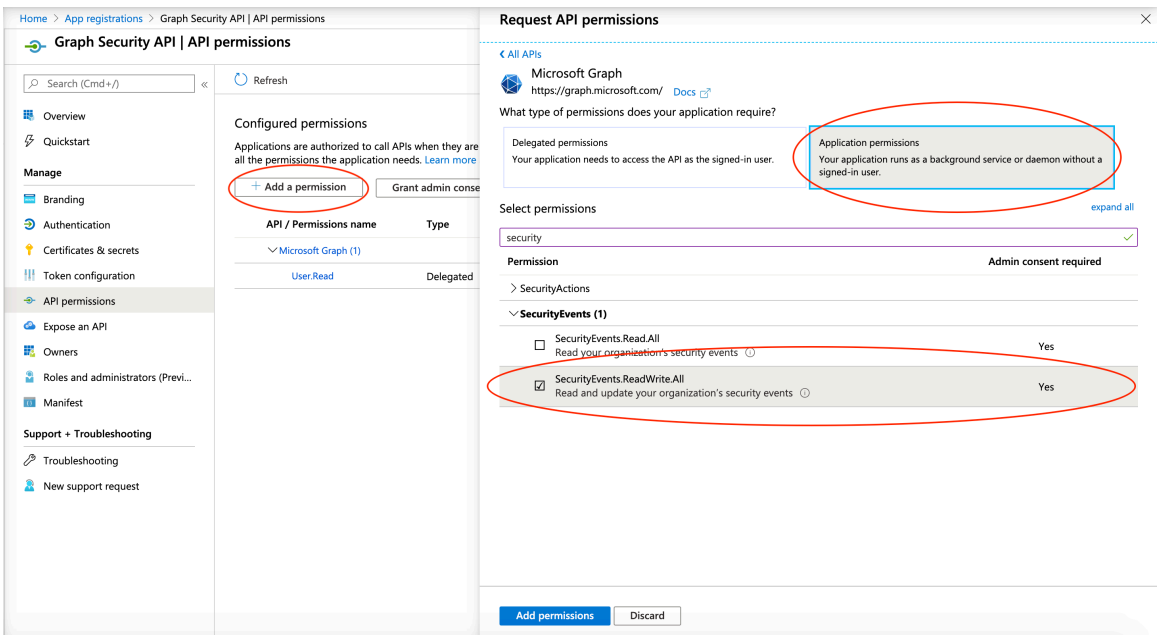
5. [アプリ登録 (App registrations)] ページで、登録したアプリケーション (Graph Security Demo など) を選択します。
6. [管理] で、[証明書とシークレット **(Certificates & secrets)]** を選択します。



7. [新しいクライアントシークレット **(New client secret)]** を選択して、クライアントシークレットを作成します。
クライアントシークレットは後で表示されなくなるため、コピーして保存してください。クライアントシークレットを忘れた場合は、新しいクライアントシークレットを生成できます。

> **注:**
> クライアントシークレットを忘れた場合は、ステップ 4 と 5 の指示に従って新しいシークレットを生成できます。

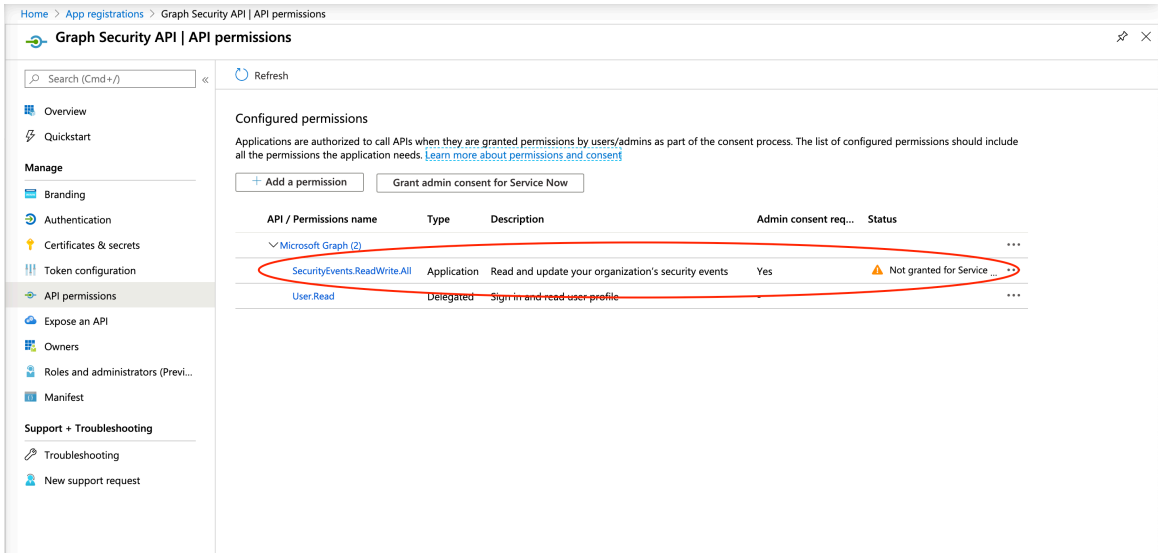
8. [概要] ページで **[API** のアクセス許可の表示 **(View API Permissions)]** をクリックします。
9. SecurityEvents.ReadWrite.All セキュリティイベントに対する新しいアプリケーションレベルの API アクセス許可を追加します。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

10. 新しく追加された API アクセス許可に対してアドミンの同意を付与します。
詳細については、「Microsoft Graph のアクセス許可のリファレンス」で Microsoft Graph アクセス許可モデルを参照してください。



11. テナントアドミンとしてログインし、アプリケーションに同意します。
手順は次のとおりです。

    a. 次の URL に移動します。https://login.microsoftonline.com/common/adminconsent?client_id=APPLICATION_ID&state=12345

    登録したアプリケーションの APPLICATION_ID を入力します。

12. [承認] をクリックして、上記で作成したアプリケーションによって要求されたアクセス許可を承認します。
その後、 アプリケーションを使用してセキュリティイベントを読み取ることができます。詳細については、Microsoft Graph Security 認証 に関するドキュメントを参照してください。

Microsoft Graph Security API アラート取り込み統合用の **ServiceNow** アプリケーションのインストールと設定

Now Platform® インスタンスで統合を実行する前に、これらのインストールと構成のステップを完了して、Now Platform インスタンスでアプリケーションが セキュリティインシデントレスポンス と セキュリティオペレーション 製品と適切に統合されるようにします。

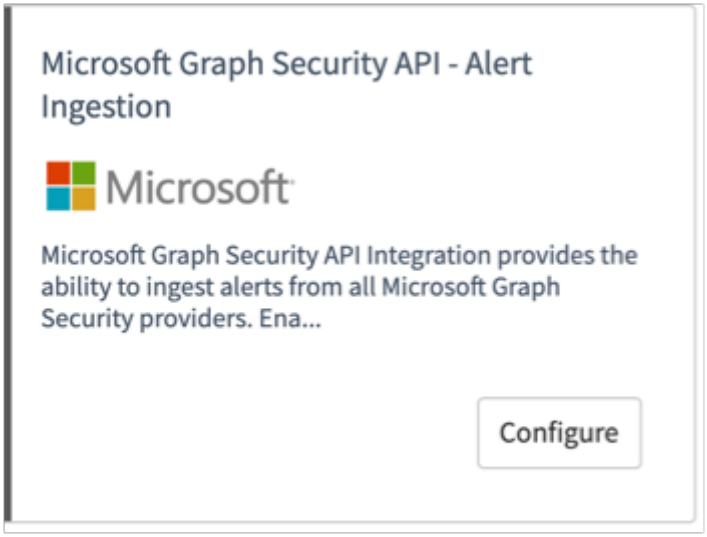
始める前に
必要なロール：sn_si.admin

手順

1. ServiceNow Store から統合用の Microsoft Graph Security API アプリケーションをインストールしていない場合は、「セキュリティオペレーション 統合のインストール」を参照し、ステップに従ってインストールしてください。
2. アプリケーションのインストールが完了したら、 統合 > 統合構成 に移動し、[Microsoft Graph Security API - アラートの取り込み (Microsoft Graph Security API - Alert Ingestion)] タイルを見つけます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. アプリケーションを構成するには、[構成] をクリックします。
4. 表示される [アラートの取り込み構成 (Alert Ingestions Configuration)] ダイアログで、フィールドに入力します。

5. **[Submit]** をクリックします。
   検証と送信が正常に完了すると、各アラート取り込みサーバー構成は [セキュリティ統合] ページにタイルとして保存されます。保存された構成タイルが右上隅にある [セキュリティ統合] ページに表示されていない場合、[構成を表示] 選択リストから [はい] をクリックします。

次のタスク
アプリケーションのインストールと設定が正常に完了しました。次のステップでは、アラートプロファイルを作成します。

Microsoft Graph Security API アラート取り込み統合のためのプロファイルの作成

sn_si.admin ロールを持つユーザーは、 Now Platform インスタンスにアラートプロファイルを作成し、セキュリティインシデントを作成するアラートを指定します。セキュリティインシデントが取り込まれたアラートから作成される前に、アラートのフィールド値が Now Platform セキュリティインシデントのレイアウトに表示されるため、実際のセキュリティインシデントがどのように表示されるかをプレビューできます。

始める前に
必要なロール：sn_si.admin

このタスクについて
統合では、不正なアクセス試行やマルウェアなどのさまざまなタイプのアラートを取り込めます。これらのアラートは、インスタンスの セキュリティオペレーション 環境で設定したプロファイルに基づいて取り込まれます。すべてのアラートは、最初にプロファイル内の設定されたアラートタイプに対して取り込まれます。取り込まれたアラートをさらにフィルタリングして、セキュリティインシデントを作成するアラートを指定できます。

たとえば、高リスクとして識別されたアラートに対してのみセキュリティインシデントを作成するフィルターを使用できます。プロファイルが有効になり、取り込まれたアラートからセキュリティインシデントが作成される前に、フィルタリングされたアラートの個々のフィールド値が、プレビュー用のセキュリティインシデントのレイアウトの対応するフィールドにマッピングされま

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

す。Microsoft Azure テナントの選択基準を満たし、Microsoft Graph Security API を介して利用可能なすべてのアラートが、最初に Now Platform インスタンスに取り込まれます。

プロファイルのソースの識別

プロファイルの名前とソースを指定します。

始める前に
必要なロール：sn_si.admin

手順

1. Now Platformインスタンスでアラートのプロファイルを作成するには、 **Microsoft Graph Security API** 連携 > **Microsoft Graph Security API** プロファイル.
2. [**New**] をクリックします。
3. フィールドに入力します。

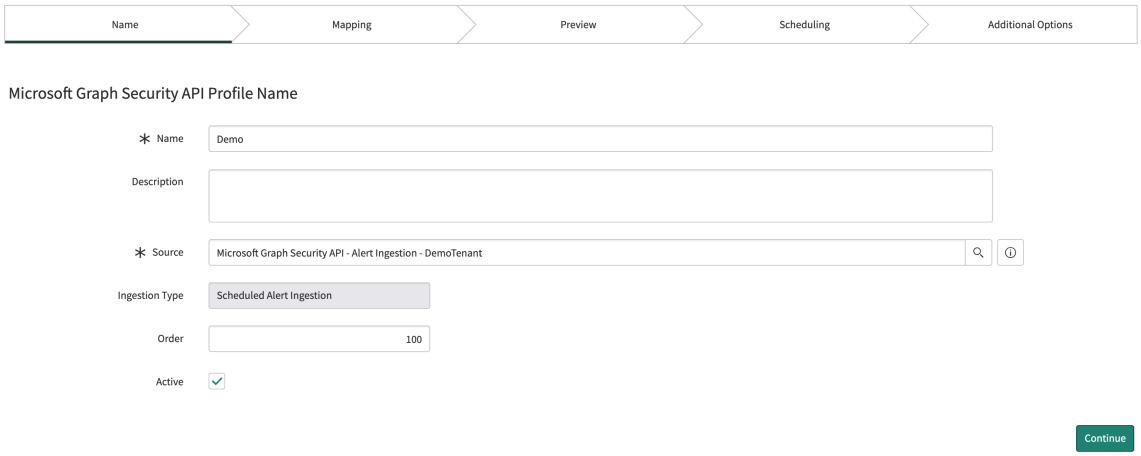
   完成したフォームの例が表の後に表示されます。

フィールド	説明
名前	プロファイルの一意の名前。名前が一意でない場合、エラーが表示され、重複するプロファイル名は保存されません。 Now Platform インスタンスのプロファイル名は一意である必要があります。
アクティブ	デフォルトでは、このチェックボックスはクリアされます。このオプションを無効にすると、プロファイルは非アクティブになります。 **注:** アクティブにする前に、プロファイルのすべてのセクションを完了する必要があります。
ソース	アラートを取り込むように構成した Microsoft Azure テナント。複数のテナントが構成されている場合は、プロファイルに取り込む予定のアラートタイプに適したテナントを選択します。値を入力する必要があります。
順序	デフォルトは 100 です。 複数のプロファイルを作成した場合、この値は、2 つ以上のプロファイルが同じトリガー条件を共有する場合の実行時の優先度を示します。順番の値が低いほど、優先度が高くなります。
(オプション) 説明	このプロファイルを他のプロファイルと区別するための追加テキスト。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図は、完成したフォームの例です。



次のタスク
次のステップでは、アラートフィールドをマッピングします。

Microsoft Graph Security API アラート取り込み統合のためのアラートフィールドのマッピング

スケジュール済みアラートの取り込みのソースを特定したら、次のステップでは、個々のアラートフィールドを Now Platform SIR セキュリティインシデントのフィールドにマッピングします。

マッピング手順では、最初に Microsoft Azure テナントからサンプルアラートを取り込む必要があります。関連するすべてのアラートフィールドデータが SIR インシデントフォームの適切な場所にマッピングされていることを確認する必要があります。そうすることで、SIR インシデントをプレビューセクションでビジュアル化できます。

サンプルアラートフィールドのマッピングには、次の手順が含まれます。

- サンプル Microsoft Graph Security API アラートの取り込み
- アラートのセキュリティインシデントレスポンスフィールドへのマッピング

サンプル **Microsoft Graph Security API** アラートの取り込み

Microsoft Azure テナントからサンプルアラートを取り込みます。

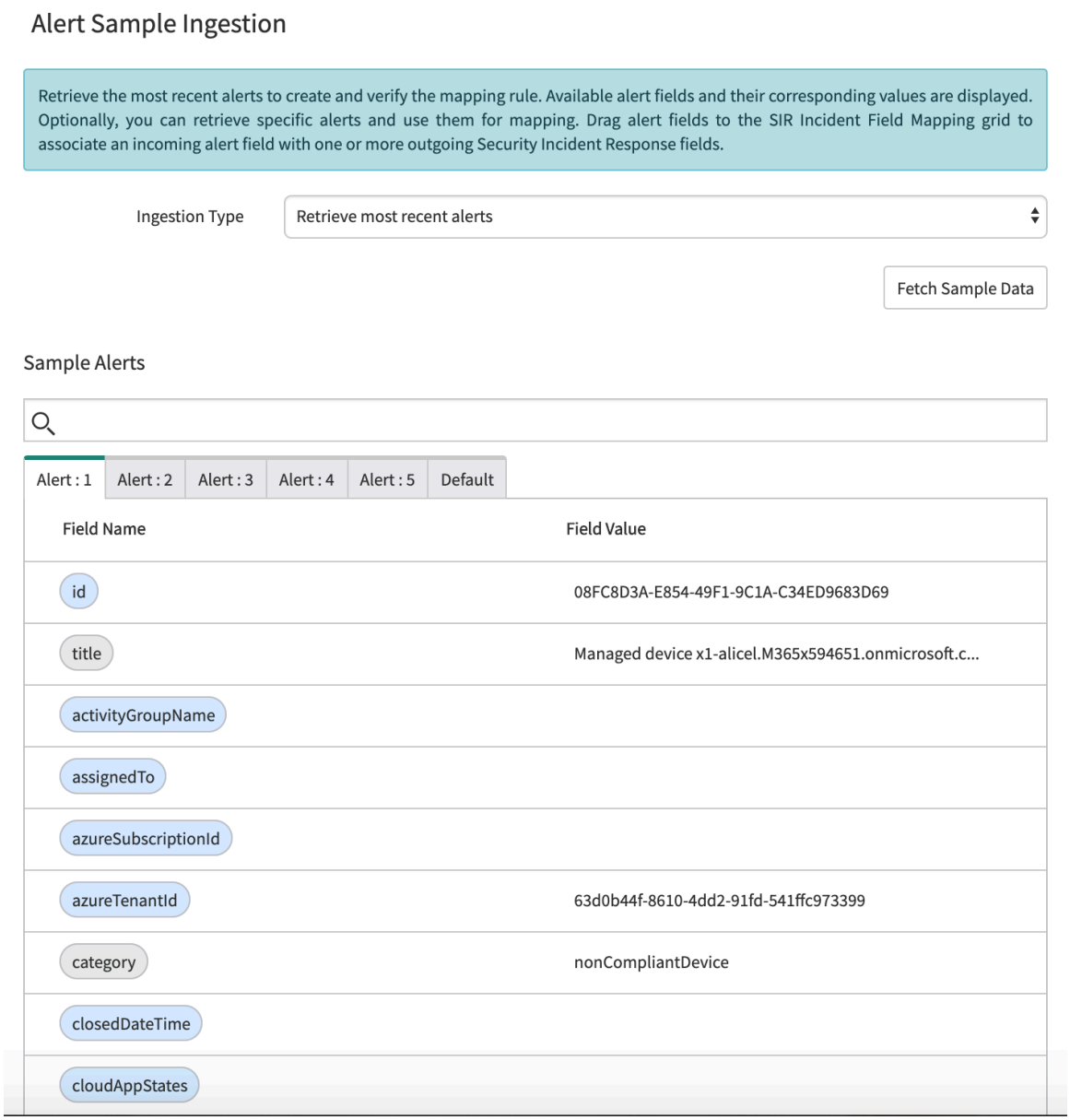
始める前に
必要なロール：sn_si.admin

手順

1. 最新の 5 つのサンプルアラートをプルするか、マッピングエクスペリエンスに使用する特定のアラートに一意のアラート ID を指定できます。
   [取り込み設定] 選択リストから、次のいずれかを選択します。
   - [最新のアラートを取得]：最新の 5 つのアラートが取得されます。
   - [アラート ID に基づいてアラートを選択 (Select alerts based on alerts ID)]：取得するアラートのアラート ID を指定します。最大 5 つのアラート ID をカンマで区切って指定できます。
2. [サンプルデータをフェッチ] をクリックして、Microsoft Azure テナントから最新のサンプルアラートデータをプルします。
   サンプルアラートのプルには少し時間がかかる場合があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サンプルアラートがプロファイルで取り込まれるとフォームの左側にサンプルアラートフィールド値が入力されます。これらは、SIR セキュリティインシデントフィールドにマップするアラートです。アラートフィールドと値の結果は、個別のタブとして表示されます。



次のタスク

サンプルデータをフェッチした後の次のステップでは、アラートフィールドをセキュリティインシデントにマップします。

アラートのセキュリティインシデントレスポンスフィールドへのマッピング

トリガーされたアラートの個々のアラートフィールドを Now Platform セキュリティインシデントのフィールドにマッピングします。

アラートフィールドマッピング

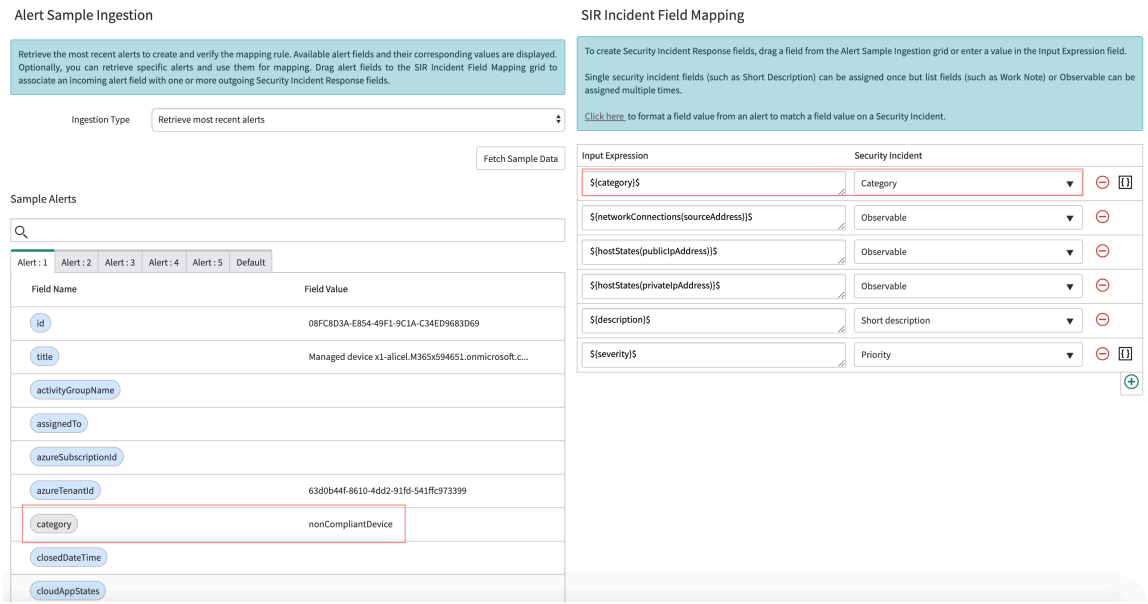
sn_si.admin ロールを持つユーザーとして、左側の [サンプルアラート] セクションからフィールドを使用し、右パネルの [SIR インシデントフィールドマッピング] 列の [セキュリティインシデント] フィールドにマップします。左側からアラートフィールドをドラッグし、右側の [SIR インシデント

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

マッピング] セクションにドロップして、マッピング構成を編集します。右側のマッピングで、[受信アラート] フィールドを [送信セキュリティインシデント] フィールドに関連付けることができます。

1. サンプルデータをフェッチした後の次のステップでは、アラートフィールドをセキュリティインシデントにマップします。フォームの左側からフォームの右側のセキュリティインシデントのフィールドにフィールド値をマッピングするには、フォームの左側で青色のフィールド名をクリックしたままにします。
2. フィールド名 (カテゴリなど) をドラッグして、[セキュリティインシデント] 列のフィールド名の横にある [入力式] 列のフィールドにドロップします。

   フィールド値が [入力式] 列に表示されます。次の画像では、category がセキュリティインシデントの [カテゴリ] フィールドにマップされます。



ただし、左側から右側のフィールドまでの任意の値を一致させることができます。プレビューステップで、セキュリティインシデントの値が正しくマッピングされていることを確認します。

マッピングプロセスでアラートフィールドが見落とされたり重複したりしないように、フィールドは色分けされています。マップされていない残りのフィールドはすべて青で表示されるのに対し、すでにマップされたフィールドはグレー表示されるため、アラートフィールドの色分けは、マップされたアラート値の追跡に役立ちます。色分けすることで、セキュリティインシデントに追加されたフィールド値、およびマップされていない残りの重要なアラート情報を視覚的に把握できます。

左側のライトブルーのフィールドは、アラートフィールドがまだ未選択で、セキュリティインシデントにマップされていないことを示します。受信アラートフィールドをセキュリティインシデントの 1 つ以上のフィールドに関連付けることができます。灰色のフィールドは、フィールドが選択され、セキュリティインシデントのフィールドにマッピングされていることを示します。この色分けは、マッピングを追跡するのに役立ちます。

注:

a. [入力式] フィールドに値を手動で入力するには、${fieldname}$ という形式で入力します。アラートフィールドがセキュリティインシデントフィールドにマッピングされます。

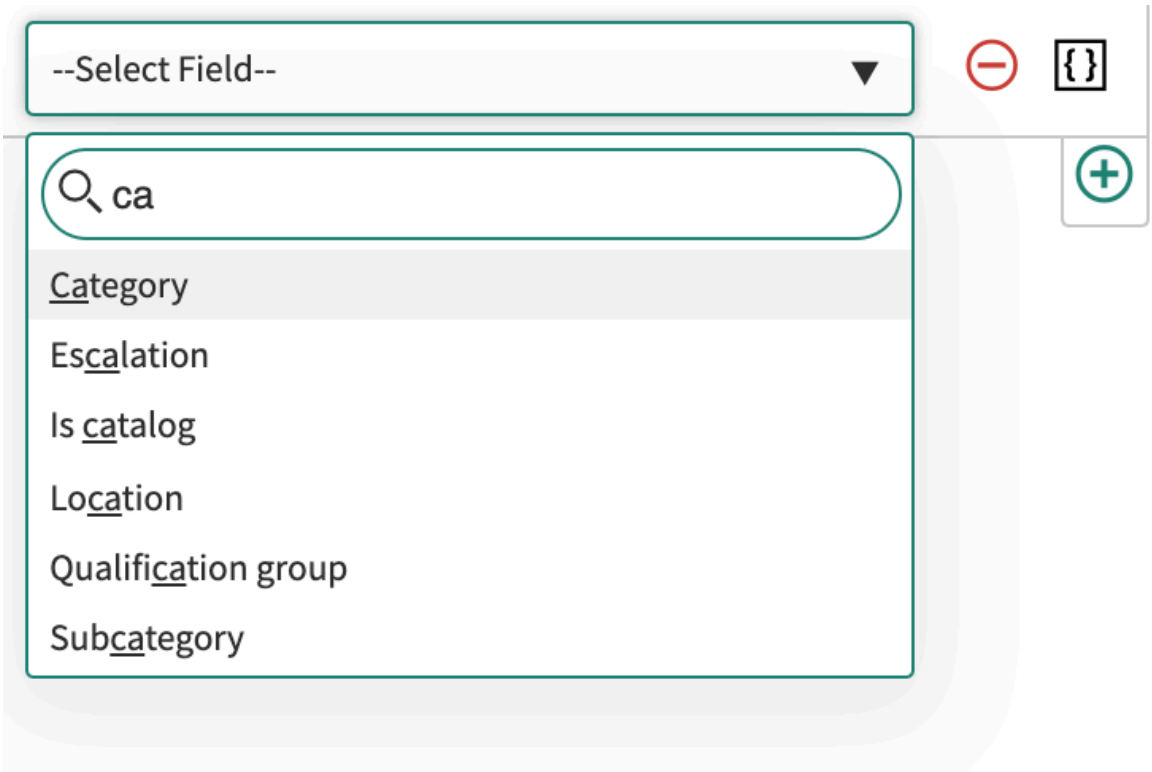
b. 取り込まれたアラートをセキュリティインシデントマッピングセクションの MITRE-ATT&CK フレームワークフィールドにマップすることはできません。それでもフィールドをマップする場合、情報はセキュリティインシデントフォームの MITRE-ATT&CK フレームワークセクションの MITRE-ATT&CK カードの一部として利用できません。MITRE-ATT&CK テクニックを関連付けるには、脅威インテリジェンス モジュールの MITRE-ATT&CK フレームワークの一部として利用可能な自動抽出機能を使用します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. フォームの右側のセキュリティインシデントに表示されるデフォルトのフィールドにフィールドを追加するには、次のステップを実行します。
   a. グリッドの下部にある [SIR インシデントフィールドマッピング] セクションのフォームの右側で、プラス (+) アイコンをクリックします。新しいフィールドが表示されます。
   b. [セキュリティインシデント] 列で表示されている選択リストを展開し、フィールドを選択します。

      新しいフィールドの展開された選択リストでは、一部のフィールドが網掛けされています。次の図では、セキュリティインシデントにマッピングされているため、カテゴリのバックグランドがグレーになっています。フォームの左側のアラートフィールドの色分け同様、右側のセキュリティインシデントフィールドのこの色分けも、すでにマップされた SIR インシデントフィールドを追跡するのに役立ちます。



      注:
      同じセキュリティインシデントに複数の観測事象を表示できるため、[観測事象] フィールドを異なる値で複数回マップできます。同様に、[構成アイテム] フィールドと [作業メモ] フィールドは複数の値をサポートします。複数の値をサポートできないフィールドに 2 つの値をマッピングしようとすると、インシデントをプレビューするときに、フィールドに値がないことを示すエラーメッセージが表示されます。同様に、セキュリティインシデントのフィールドに複数のオプションを選択できる選択リストがあり、選択リストに表示されていないフィールドにオプションをマップしようとすると、そのフィールドはセキュリティインシデントに入力されません。

   c. または、新しい行の [検索] フィールドに値を入力します。
   d. フォームの左側の [入力式] フィールドに入力する [アラート ID] を左クリックして選択します。ドラッグアンドドロップ機能を使用して、新しいフィールドの横にマッピングします。
4. フィールドの値をマッピングに追加するか、削除して、マッピングを続行します。

自動翻訳

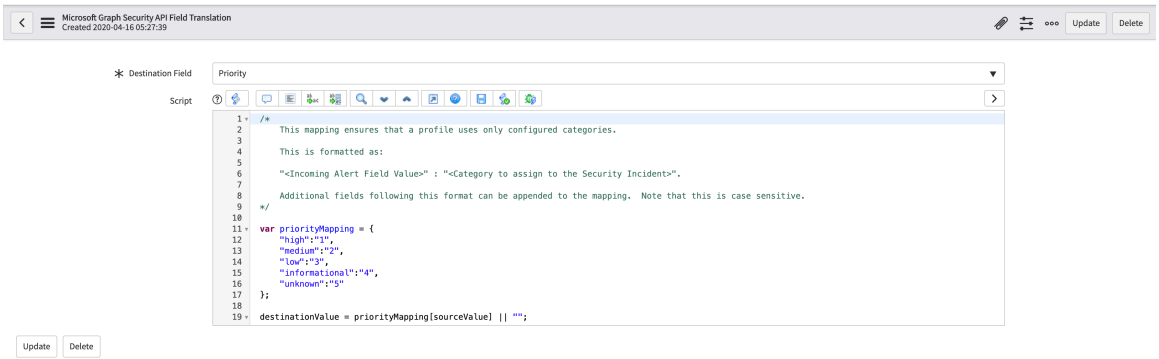
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. 先行するフィールドマッピングのステップを完了したら、インシデント生成条件ビルダーで同じフィールド値を使用して、セキュリティインシデントを作成するために受信アラートが満たす必要がある追加の条件を定義することができます。インシデント生成条件を設定するには、次のステップを実行します。

フォーマットフィールド変換

特定の場合、Microsoft Graph Security API のアラートフィールド値は SIR セキュリティインシデントのフィールドに直接変換されないことがあります。これらの値については、マッピングステップでスクリプトエディターを使用してセキュリティインシデントのフィールド値をフォーマットできます。類似しているが同一ではない値をフォーマットする場合は、スクリプトエディターを使用します。たとえば、スクリプトエディターで、マルウェアアラートとウィルス感染のカテゴリ値がソースカテゴリでは異なるフィールド値であっても、フォーマットフィールド変換機能を使用して、両方の値が SIR セキュリティインシデントで [カテゴリ] フィールドの一般的な悪意のあるコードアクティビティに変換される場合があります。

スクリプトエディターを使用するには、{} アイコンをクリックします。スクリプトエディターが表示されます。



インシデント生成条件

マッピングセクションが完了すると、フィルター条件を設定して、セキュリティインシデントを作成するアラートとフィルタリングで除外されるアラート (低優先度のアラートなど) を指定できます。インシデント生成条件ビルダーで同じフィールド値を使用して、セキュリティインシデントを作成する際に受信アラートを満たす必要がある追加の条件を定義することができます。インシデント生成条件を設定するには、次のステップを実行します。

1. フォームの [インシデント生成条件] セクションまでスクロールし、[条件に基づいてフィルター] オプションを選択します。フィルター条件ビルダーが表示されます。これらのフィルターを使用して、フィールドで説明されている特定の条件に一致するセキュリティインシデントを作成します。

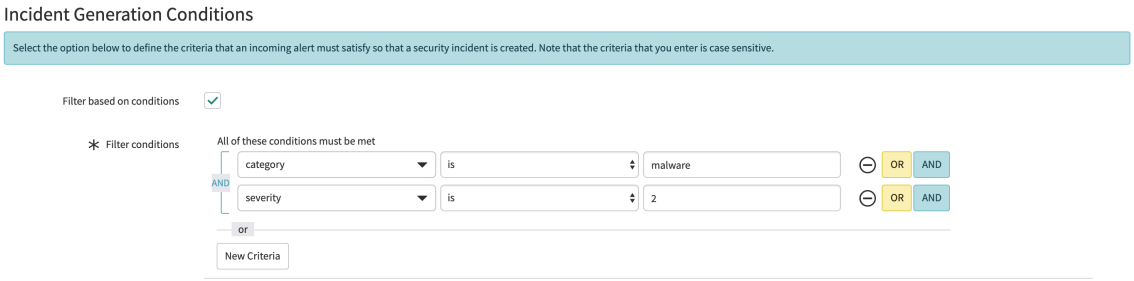
   フィルター条件ビルダーの最初のフィールドの選択肢リストオプションは、取り込まれたアラートの [アラートサンプルの取り込み] セクションに表示されるフィールドと一致します。これらのフィールドは動的であり、取り込むアラートに応じて変化します。入力する基準は大文字と小文字を区別し、アラートの値と正確に一致する必要があります。フィルターフィールドに入力する値が不明な場合、Microsoft Azure テナントに戻り、アラートをレビューしてキーワードを確認することができます。

2. 条件ビルダーの選択リストとフィールドを使用して、最初の行のフィルターを設定します。
3. 条件を追加するには、フィールドの右側にある **[AND]** または **[OR]** をクリックします。
   - **[AND]** を選択した場合は、すべての条件に一致する必要があります。
   - **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。
4. 2 行目で、2 番目のフィルター条件を設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の画像は、セキュリティインシデントが作成される前に一致する必要がある 2 つの条件を含む例です。



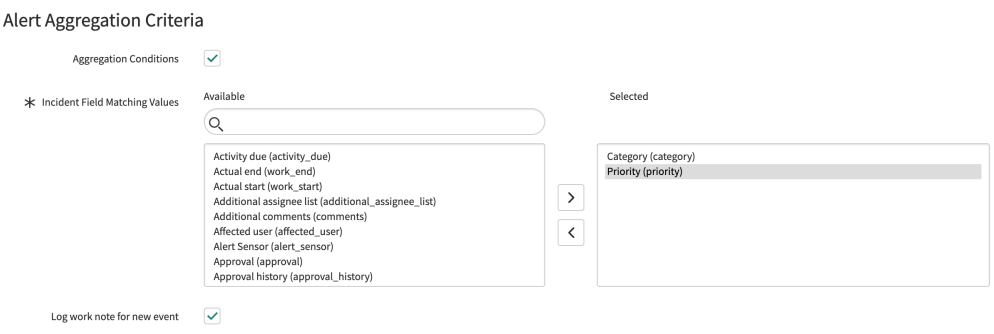
入力した両方のフィルタリング条件に一致した場合にのみセキュリティインシデントが作成されるように、トリガー条件を設定しました。

このタイプのフィルタリングは、セキュリティアラートを分離し、作成するセキュリティインシデントの数を制限するのに役立ちます。追加のフィルター条件を設定すると、クエリまたはトリガーされたアラート構成を変更することなく、必要なアラートのみが取り込まれます。

類似のアラートを処理して重複インシデントを防止するアラートアグリゲーション基準

類似の重複する可能性があるインシデントを作成するのではなく、既存の SIR セキュリティインシデントに受信アラートを集計する追加のアラートアグリゲーション基準を定義します。この追加の集計機能では、各プロファイルのフィールド一致値基準を使用して、関連するすべてのアラートデータを単一のセキュリティインシデントに配置することで、アクティブな重複するセキュリティインシデントの数を減らすことができます。基準を設定するには、以下のステップを実行します。

1. フォームで [アラートアグリゲーション基準] セクションにスクロールして、[集計条件] オプションをオンにします。[値が一致するインシデントフィールド] 列が表示されます。これらのフィールド名は、 SIR セキュリティインシデントで構成されたカスタムフィールドを含むセキュリティインシデントのフィールドです。
2. [利用可能] リストから、Now Platform の既存のセキュリティインシデントで照合するフィールド値を選択し、[選択済み] リストに移動させます。この受信アラートを既存のセキュリティインシデントに追加するには、選択するすべてのフィールド値が一致する必要があります。これには、複数のアラートフィールド値がマッピングされている可能性がある [観測事象] や [構成アイテム] などのフィールドが含まれます。すべての値が一致している必要があります。値のサブセットのみが一致した場合、アラートアグリゲーション条件は満たされず、新しいセキュリティインシデントが作成されます。複数値フィールドのマッピングについては、以下のスクリーンショットを参照してください。



新しいアラートが、マッピングステップの集計フィールド条件で選択されたすべての値と一致する場合、新しいアラートは、同じフィールド値を持つ最新のオープンセキュリティインシデントに自

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

動的に追加されます。セキュリティインシデントを扱う sn_si.analyst ロールを持つユーザーは、セキュリティインシデントの関連リストで、追加されたすべての集計アラートを表示できます。セキュリティインシデントの集計されたアラートはすべて、[集計された Microsoft Graph アラート] 関連リストに表示されます。このリストには、関連するタイムスタンプと集計されたフィールド値の詳細が表示されます。この情報は、アラートが既存のセキュリティインシデントに追加される理由を理解するのに役立ちます。このタブが表示されない場合は、 [関連リンク] の下のレコードの左側にスクロールし、[すべての関連リストを表示] リンクをクリックします。

3. (オプション) セキュリティインシデントで最近追加された新しいアラートの作業メモを記録するには、このチェックボックスをオンにしてこのオプションを有効にします。作業メモには、新しいアラートが追加され、アラートの詳細へのリンク、およびマッピングセクションの作業メモフィールドに追加された可能性のあるその他の詳細が記録されます。

   アラートから SIR セキュリティインシデントのフィールドに値を正常にマッピングしました。また、フィルター条件に基づいてセキュリティインシデントの作成を制限する追加条件も設定しました。既存の SIR セキュリティインシデントにアラートまたはイベントも追加しました。

4. [続行] をクリックして、プロファイル設定を続行します。次のステップでは、SIR セキュリティインシデントにマッピングしたフィールドをプレビューします。

Microsoft Graph Security API 統合でのセキュリティインシデントのプレビュー

マッピングステップを完了したら、Now Platform SIR セキュリティインシデントでマッピングした値をプレビューします。このプレビューステップでは、セキュリティインシデントに表示するすべてのアラートフィールドがマッピングされていることを確認できます。

始める前に

必要なロール：sn_si.admin

このタスクについて

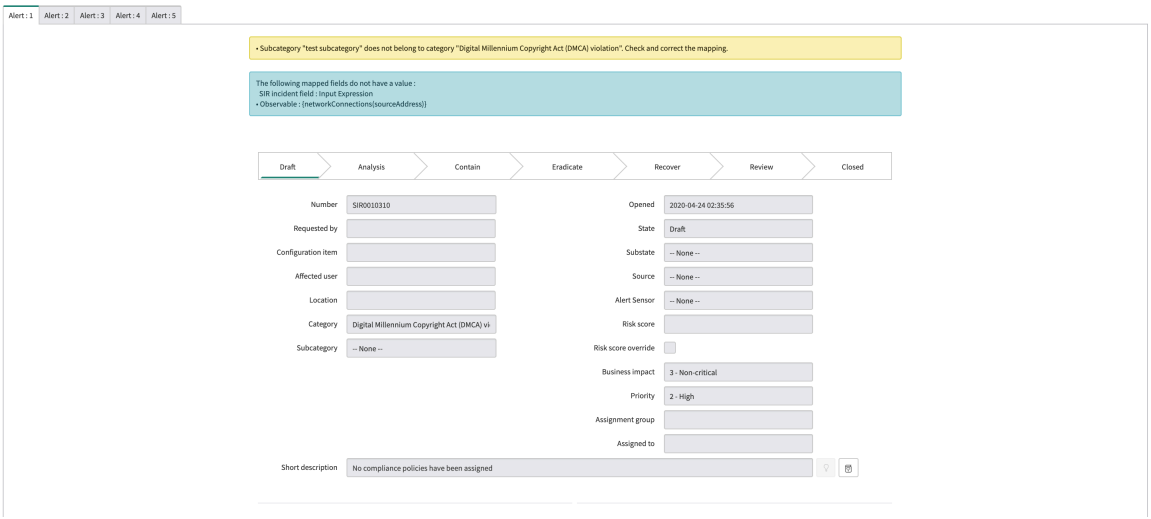
sn_si.admin ロールを持つユーザーは、セキュリティインシデントをプレビューし、必要に応じてマッピングを再編集して、エラーのあるフィールドを修正するか、欠落しているデータを入力します。プレビューが正常に完了しない場合、スケジュール設定ステップに進むことはできません。SIR セキュリティインシデントのプレビューは、セキュリティインシデントレスポンス 製品の実際のインシデントとして保存されません。

手順

1. セキュリティインシデントのプレビューが表示されない場合は、進捗状況バーの [プレビュー] をクリックします。
   取り込まれたアラートと、[マッピング] ページで定義されたフィールドマッピングのすべてが表示されます。
2. アラート ID をクリックすると、セキュリティインシデントのプレビューが表示されます。
   このビューは読み取り専用であり、このセキュリティインシデントのレコードは保存されません。
3. セキュリティインシデントのアラート値のフィールドマッピングを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



前の画像は、取り込まれたサンプルのマッピングエラーのあるプレビューの例です。

4. このエラーを解決するには、進捗状況バーの [マッピング] をクリックします。
5. マッピングを編集して誤った値を修正するか、欠落しているデータを入力します。
6. マッピングを再度プレビューし、エラーメッセージに記載されているエラーの修正を続行します。

次のタスク

エラーメッセージが表示されず、セキュリティインシデントのフィールドマッピングに問題がない場合は、次のステップでスケジュールを定義します。

Microsoft Graph Security API 統合のスケジュール定義

必要に応じて、アラート取得のデフォルトの設定を確認したり、スケジュールを変更したりすることができます。このステップでは、日付範囲に基づいてアラートの取得をフィルタリングできます。

始める前に

必要なロール：sn_si.admin

このタスクについて

また、アラートプロファイル構成に一致する将来のアラートをポーリングする頻度も選択します。自動アラート取り込みプロファイルの場合は、プロファイルをアクティブ化する前に、スケジュールとアラートの取得を確認して変更します。このステップは、スケジュール設定済みアラートプロファイルに必要です。

sn_si.admin ロールを持つユーザーは、これらのポーリング間隔をプロファイルごとに設定します。Microsoft Graph Security API アラートの取り込み統合のパフォーマンスは、ポーリング間隔が異なると影響を受けます。スケジュールするときは、インシデントの緊急度とシステム負荷のバランスを取るように計画してください。5 分間のデフォルト値が任意のプロファイルに設定されますが、インシデントの緊急度とシステムの予想される負荷に基づいて変更できます。

手順

1. 進捗状況バーに [スケジュール] ページが表示されない場合は、[スケジュール] を選択します。
2. Microsoft Azure テナントからアラートをプルする方法とタイミングをスケジュールするものを選択します。
3. [続行] をクリックして、[他のオプション] ページに移動します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SIR インシデント状況に基づくアラートの更新とクローズの自動化

Microsoft Graph Security API アラートには、アラートからセキュリティインシデントを作成する機能と、SIR インシデント番号、アサイン先グループ、SIR インシデント URL などの関連するインシデントの詳細を使用して、セキュリティインシデントが作成および/またはクローズされるとアラートを更新する機能を許可する双方向インターフェイスがあります。T

始める前に

必要なロール：sn_si.admin

注:
初期アラートとクローズアラートのステータスは、この機能がサービスプロバイダーによってサポートされている場合にのみ更新されます。詳細については、Microsoft Graph Security API のドキュメントおよびセキュリティプロバイダーのドキュメントを参照してください。

手順

1. 進捗状況バーに [その他のオプション] ページが表示されない場合は、[その他のオプション] を選択します。
2. 以下の手順に従って、セキュリティインシデントが作成されたときにアラートを更新するための構成を完了します。

3. [完了] をクリックして構成を完了し、プロファイルを [待機中] ステータスに移行します。
   確認ダイアログが表示されます。これで統合のセットアップと構成が正常に完了しました。このプロファイルをアクティブ化して、スケジューリングに基づいて Microsoft Azure テナントからアラートをプルします。24 時間以内に最大 1000 件のセキュリティインシデントを作成できます。

Microsoft Graph Security API 統合設定

このオプションを使用して、Microsoft Graph Security API 取り込み統合のデフォルトのシステムプロパティを変更します。

始める前に

必要なロール：sn_si.admin

このタスクについて

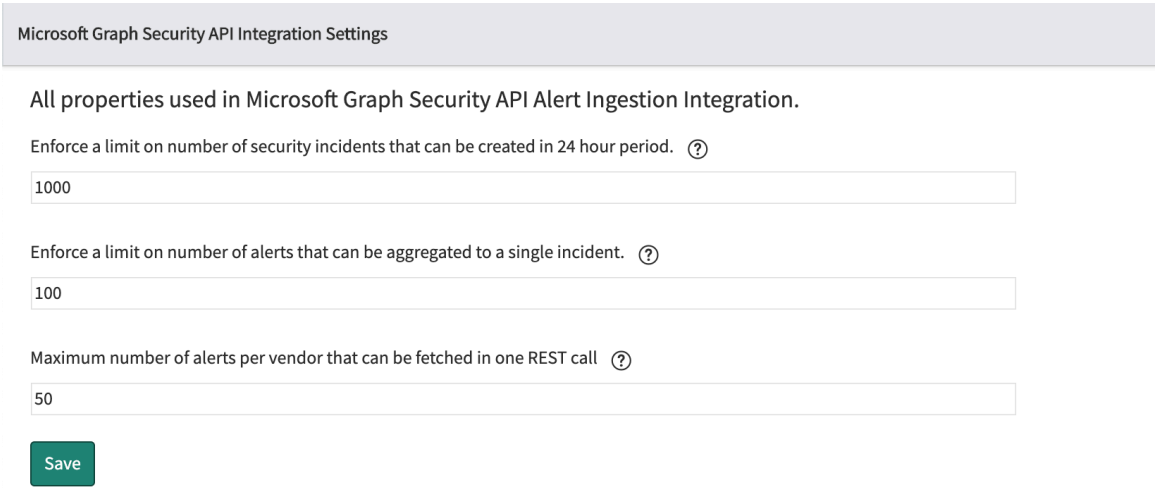
デフォルトの構成プロパティを変更して、24 時間の間に作成できるセキュリティインシデントの数、または 1 つのセキュリティインシデントに集計できるアラートの数を制限します。

システムプロパティを変更するには、 *sn_si.admin* ロールを持つユーザーとしてログインし、次の場所に移動します。 **Microsoft Graph Security API** 連携 > **Microsoft Graph Security API** 統合設定.

デフォルトの構成設定が表示されます。必要に応じて、これらの設定を変更できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



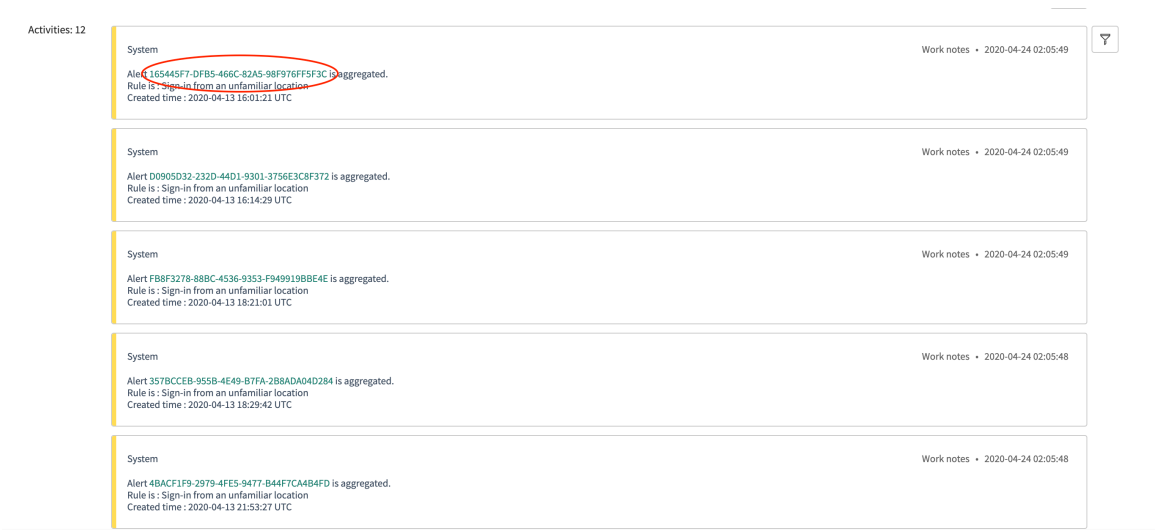
変更した統合設定は、プロファイルで定義されている次のポーリング間隔で適用されます。

アラート取り込み後の セキュリティインシデントレスポンスフォーム

Microsoft Graph Security API アラートが取り込まれると、セキュリティインシデントが作成され、そのセキュリティインシデントレコードに対応する更新が実行されます。

作業メモ

アラートのセキュリティインシデントレスポンスフィールドへのマッピング で説明されているように、アラートアグリゲーション基準で [新規アラートの作業メモを記録] オプションを選択した場合、アラートが集計されると作業メモが投稿されます。



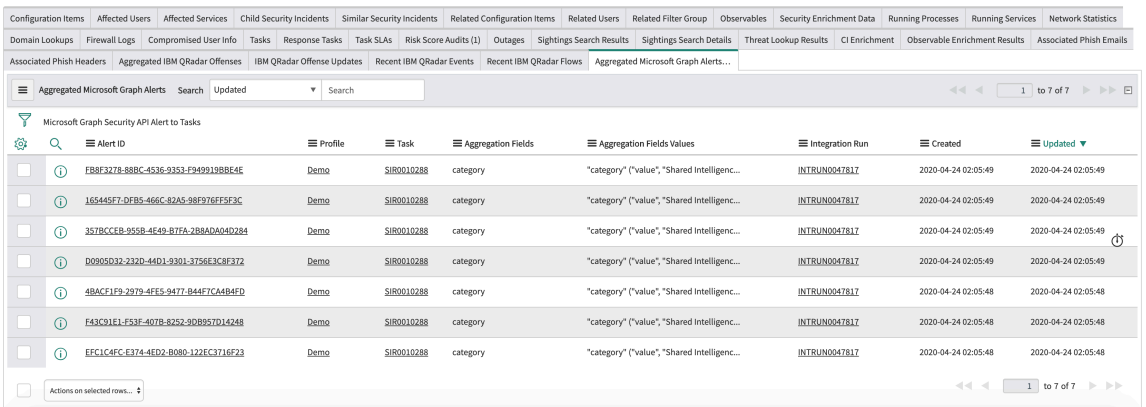
アラートリンクをクリックして、生のアラートデータを含む内部アラートインポートレコードに移動します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

集計されたアラート

クリックします 関連リスト > 集計された **Microsoft Graph Security** アラート セキュリティインシデントに集計されたアラートを表示します。



- セキュリティインシデントの作成：リストからアラートを選択し、[アクション] メニューをクリックして、[セキュリティインシデントを作成] をクリックします。このオプションで、アラートの新しいセキュリティインシデントを作成できます。このアラートは親セキュリティインシデントからは集計されません。
- アラートレコードの削除：リストからアラートを選択し、[アクション] メニューをクリックして、[削除] をクリックします。このオプションで、アラートレコードを削除できます。

オプション：**Microsoft Graph Security API** プロファイルのコピー

新しいプロファイルを作成する代わりに、既存のプロファイルとその関連設定をコピーします。複数のプロファイルを作成していて、既存のプロファイルの設定を再利用する場合は、時間を節約するためにプロファイルをコピーすることをお勧めします。

始める前に
必要なロール：sn_si.admin

このタスクについて
sn_si.admin ロールを持つユーザーがプロファイルをコピーすると、プロファイルの重複を避けるためにプロファイル名が最初に変更されます。また、コピーされたプロファイルは無効 (false) であるため、構成が完了する前に誤って有効になることはありません。既にプレビューおよび検証したセキュリティインシデントのプロファイルをコピーし、既存のマップを使用します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 **All** (すべて) > **Microsoft Graph Security API** 連携 > **Microsoft Graph Security API** プロファイル.
2. 表示される [Microsoft Graph Security API プロファイル (Microsoft Graph Security API Profiles)] リストでコピーするプロファイルを選択し、選択した行の [アクション] 選択リストで [コピー] をクリックします。
   プロファイルがコピーされ、リストに表示されます。コピーには、マッピングとスケジュール設定を含む元のプロファイルのすべての設定が含まれます。プロファイルの名前に「copy」が含まれています。元のプロファイルは有効ですが (true)、この時点でコピーは無効になります (false)。必要に応じて、コピーしたプロファイルの値を編集して名前を変更し、構成設定を新しいプロファイルに適用することもできます。

   既存のプロファイルから新しいプロファイルに設定が正常にコピーされました。プロファイルをアクティブ化する必要があるため、[アクティブ] 列のステータスが false に設定されていることに注意してください。

次のタスク
構成ステップが完了すると、新しいプロファイルをアクティブ (有効) にするように求められます。

ドメインセパレーションと **Microsoft Graph Security API** アラートの取り込み

このアプリケーションでは、ドメインセパレーションがサポートされています。Microsoft Graph Security API 統合は、Microsoft Graph セキュリティプロバイダーからアラートを取り込み、自動でセキュリティインシデントを作成します。 ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル：ベーシック

- アプリケーションサービスプロバイダーのユースケースに合わせてデータが適切なドメインに送られるようにするビジネスロジックが存在します。
- このアプリケーションは、ドメインセパレーションを完全にサポートしています。ドメインセパレーションには、ユーザーインターフェイス、キャッシュキー、レポート、ロールアップ、および集計からのドメインの分離が含まれます。
- インスタンスのオーナーは、複数のテナント間で正常に機能するようにアプリケーションをセットアップする必要があります。

サンプルユースケース：サービスプロバイダーがチャットを使用してテナント顧客のメッセージに応答する場合、お客様がサービスプロバイダーの応答を確認できるようにする必要があります。

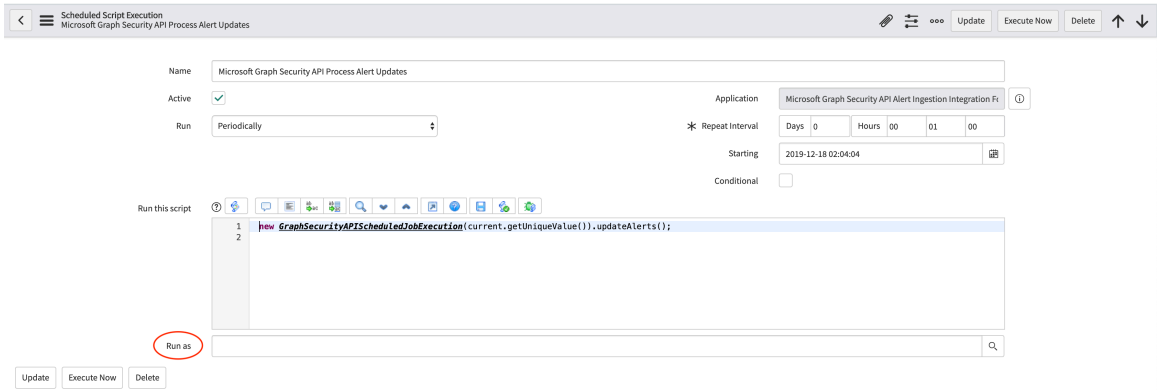
サポートレベルの詳細については、「アプリケーションでのドメインセパレーションのサポート」を参照してください。

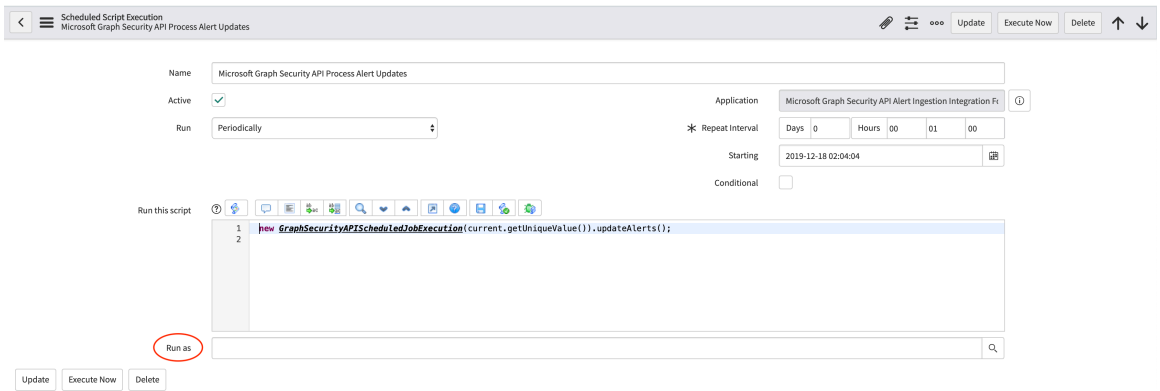
Microsoft Graph Security API におけるドメインセパレーションの仕組み

ドメインセパレーションを実現するには、[Microsoft Graph Security API プロファイルプロセス (Microsoft Graph Security API Profile Process)] および [SIR プロセスアラート更新 (SIR Process Alert Updates)] スケジュール済みジョブを複製し、[実行方法] のユーザーを変更します。デフォルトでは、システムユーザーがこれらのスケジュール済みジョブを実行します。[実行方法] をそれぞれのドメインの sn_si.admin ロールを持つユーザーに変更してから、スケジュール済みジョブを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。





関連情報

サービスプロバイダーのドメインセパレーション

Microsoft Graph Security API 統合でのフローデザイナーと Integration Hub の使用

フローデザイナーと Integration Hub 機能を使用して、いくつかのサブフローとアクションが Microsoft Graph Security API 統合の一部としてビルドされました。

次のサブフローを使用できます。

- [Microsoft Graph Security API 構成の検証]：これは、初期セットアップで認証情報を検証するために構成タイルで使用されます。
- [Microsoft Graph Security API の REST コール]：これは、REST コールを使用する Microsoft Graph Security API とのインタラクションに使用されます。
- [サンプルアラートを取得]：これは、サンプルデータをフェッチするためにプロファイルセットアップの [マッピング] セクションで使用されます。このサブフローは非同期にトリガーされます。

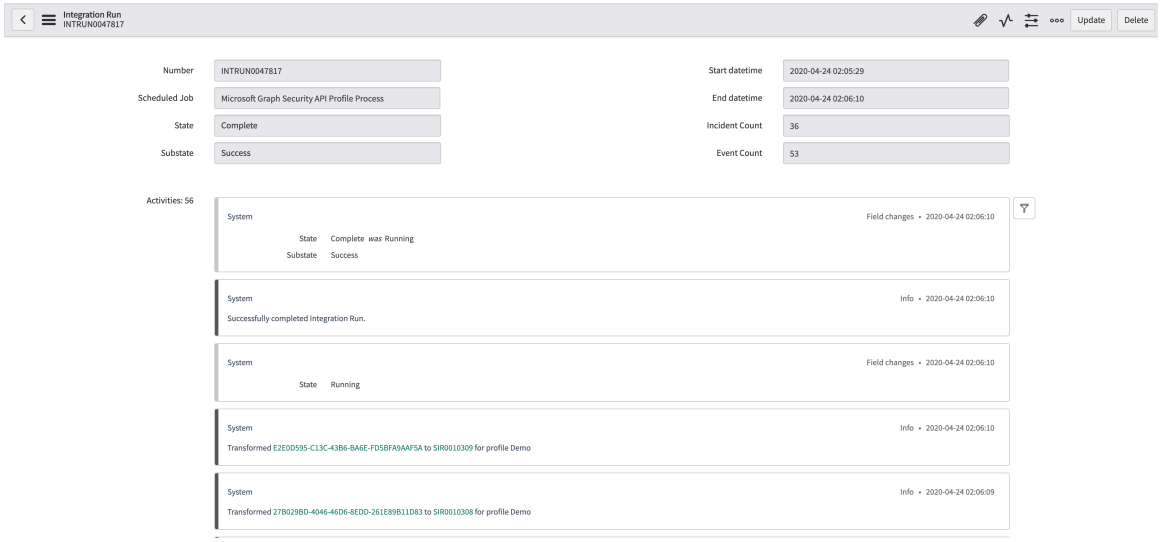
Microsoft Graph Security API 統合のトラブルシューティング

このセクションでは、Microsoft Graph Security API アラートの取り込み統合に関連する重要なトラブルシューティングのヒントとよくある質問について説明します。

- 統合の実行：スケジュール済みジョブの実行が開始されると、ログ、エラー、および警告を含む統合実行レコードが表示されます。取得したアラートの数と、スケジュール済みジョブの実行で作成されたインシデントの数も表示されます。sn_si.analyst ロールを持つユーザーは、統合の実行中にエラー/プロファイルの取得に失敗したかどうかを確認できます。sn_si.analyst ロールを持つユーザーは、sn_event_ingestion_integration_run テーブルで発生したエラーを確認できます。統合の問題をトラブルシューティングするには、最初に統合の実行を確認する必要があります。エラーは、スケジュール済みジョブの実行ごとに統合実行レコードに作業メモとして記録されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



- 不完全なプロファイル：プロファイルの設定中に、[他のオプション] (SIR インシデント状況に基づくアラートの更新とクローズの自動化) セクションで [完了] ボタンをクリックして、プロファイルが取り込みを待機していることを示す [待機中] ステータスに移行したことを確認する必要があります。
- プロファイルの検証：統合が正常に機能しているかどうかを検証するには、プロファイルステータス、プロファイルの前回の取得日、アラートインポートテーブル、タスクに対するアラートテーブルの各レコードを確認します。
- **SSL** の問題：Microsoft Graph Security API を介して接続する場合は、インスタンスに期限切れでない有効な CA 証明書があることを確認してください。RSA または独自の証明書をプラットフォームにインポートし、証明書の共通名がホスト名と一致しているか確認できます。詳細については、KB0778285 を参照してください。

Palo Alto Networks - AutoFocus の統合

Palo Alto Networks - AutoFocus 統合ベースシステムには、Palo Alto Networks - AutoFocus とインスタンスの統合に使用できるワークフローと一連のワークフローアクティビティが含まれています。

探索

セキュリティインシデントレスポンス の統合

セットアップ

Palo Alto Networks - AutoFocus 統合のアクティブ化と構成

使用

- [Security Operations Palo Alto Networks - 値のチェックとブロック (Security Operations Palo Alto Networks - Check and Block Value)] ワークフロー
- AutoFocus セッション情報拡張フローを取得

開発

- ServiceNow セキュリティオペレーション 統合開発のガイドライン
- 統合を作成するためのヒント
- 開発者トレーニング

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

- 開発者ドキュメント
- アプリケーションとともにインストールされているコンポーネントの検索

トラブルシューティングとヘルプ

- 統合のトラブルシューティング
- Security Operations Community で質問や回答をする
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

Palo Alto Networks - AutoFocus 統合のアクティブ化と構成

統合構成機能を使用すると、Palo Alto Networks - AutoFocus を含むサードパーティのセキュリティ統合をすばやくアクティブ化して設定できます。Palo Alto Networks - AutoFocus を使用する前に、ServiceNow Store からダウンロードする必要があります。

始める前に
必要なロール：sn_si_admin

手順

1. ServiceNow Store からのアプリケーションの初回ダウンロード。
2. インストールが完了したら、Palo Alto Networks サポートサイトにアクセスして API キーを取得します。
3. インスタンスで、 セキュリティオペレーション > 統合設定.
4. Palo Alto Networks AutoFocus カードで、[構成] をクリックします。
5. Palo Alto Networks サポートサイトから取得した **API** キーを入力します (または貼り付けます)。
6. **[Submit]** をクリックします。

AutoFocus セッション情報拡張フローを取得

[Security Operations Palo Alto Networks - AutoFocus セッション情報拡張を取得] フローが実行されると、指定されたソース IP に関する情報を収集するために、AutoFocus を使用して検索クエリがキューに入れられます。AutoFocus がその IP アドレスからの以前のセッションを認識している場合は、JSON 形式のレポートが返されます。

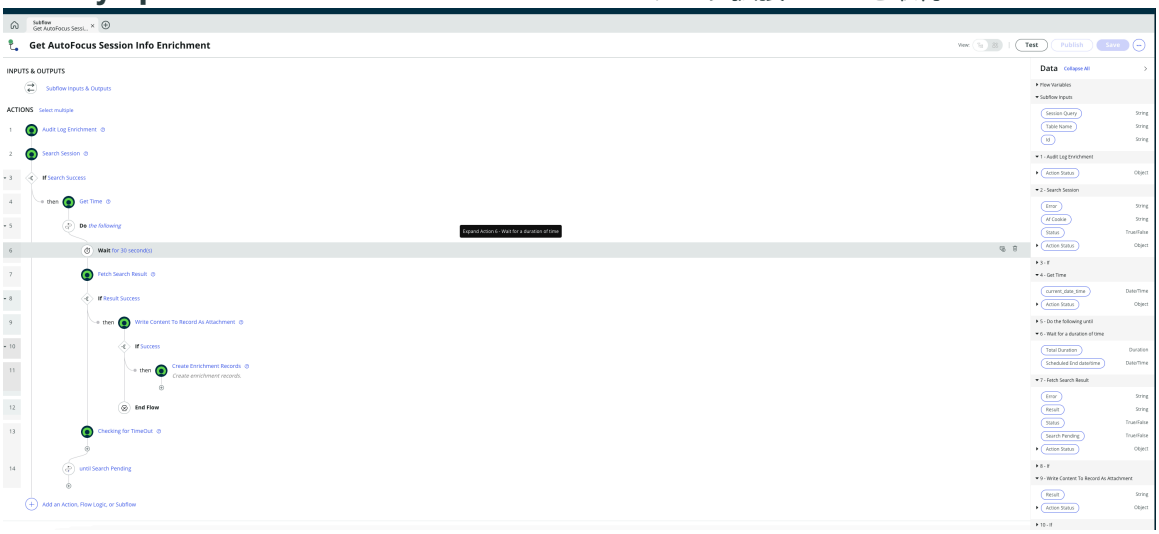
始める前に
必要なロール：sn_si.analyst

このタスクについて
[Security Operations Palo Alto Networks - AutoFocus セッション情報を取得 **(Security Operations Palo Alto Networks - Get AutoFocus Session Info Enrichment)**] フローは、セキュリティインシデントの [ソース **IP**] フィールドが変更され、レコードが更新されると実行されます。このフローは IP アドレスをフェッチし、クエリ要求を AutoFocus に送信します。AutoFocus がその IP アドレスからのセッションを識別したことがある場合は、JSON 形式のレポートが返されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Security Operations Palo Alto Networks - WildFire データ拡張フローを取得



手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > オープンインシデントを表示.
2. [セキュリティ侵害のインジケーター] タブをクリックし、[ソース **IP**] フィールドに入力します。
3. [更新] をクリックします。
   AutoFocus はこの IP アドレスからの情報をスキャンし、JSON 形式のテキストファイルがセキュリティインシデントに添付されます。

   ここでは、この統合に固有のアクションについて説明します。他のアクションの詳細については、「 一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

AutoFocus 検索セッションアクション

[AutoFocus 検索セッション] フローアクションは、セキュリティインシデントに割り当てられた IP アドレスから AutoFocus に情報をアップロードし、検索クエリのキューに入れます。

入力変数

> **注:**
>
> アクションが実行されると、指定されたソース IP の情報を収集するために、AutoFocus を使用して検索クエリがキューに入れられます。AutoFocus がその IP アドレスからのセッションを識別したことがある場合は、JSON 形式のレポートが返されます。

アクションの初期動作が、入力変数によって決まります。

入力変数

変数	説明
searchSessionQuery [文字列]	セッション情報の検索クエリ。

[検索結果をフェッチ] アクション

[検索結果をフェッチ] フローアクションは、Cookieによって識別された検索結果を、AutoFocus 検索セッションアクションによって開始された検索クエリにフェッチします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

入力変数

アクションの初期動作が、入力変数によって決まります。

入力変数

変数	説明
afcookie [文字列]	AutoFocus 検索セッションアクションによって生成された検索要求の AutoFocus cookie。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。

出力変数

変数	説明
searchPending [ブール]	検索要求がまだ AutoFocus で処理中の場合は True。
result [文字列]	検索結果データ。
status [ブール]	検索が完了し、結果が正常に生成された場合は True。
error [文字列]	アクションで発生したエラー (ある場合)。

Palo Alto Networks - Firewall の統合

Palo Alto Networks - Firewall 統合を実行するには、SSH 認証情報で MID サーバー が設定されていることを確認してください。ファイアウォールがまだ設定されていない場合は追加します。

探索

セキュリティインシデントレスポンス の統合

セットアップ

- Palo Alto Networks ファイアウォール統合のアクティブ化と構成
- MID サーバーへの SSH 認証情報の設定

使用

Security Operations Integration Palo Alto Networks ファイアウォールランチャーワークフロー

開発

- ServiceNow セキュリティオペレーション 統合開発のガイドライン
- 統合を作成するためのヒント
- 開発者トレーニング
- 開発者ドキュメント
- アプリケーションとともにインストールされているコンポーネントの検索

トラブルシューティングとヘルプ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

- 統合のトラブルシューティング
- Security Operations Community で質問や回答をする
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

MID サーバーへの **SSH** 認証情報の設定

Palo Alto Networks ファイアウォールは、API 呼び出しを MID サーバーに送信します。そのため、MID サーバーの SSH 認証情報が作成されていることを確認します。

始める前に

- オーケストレーションプラグインをアクティブ化する必要があります。

必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > オーケストレーション > 認証情報 **&** 接続 > 認証情報.
2. [**New**] をクリックします。
3. [インターセプター] 画面で、**[SSH** 認証情報] をクリックします。
4. 必要に応じて、フィールドに入力します。

SSH 認証情報

フィールド	説明
名前	認証情報の名前を入力します。
アクティブ	この認証情報をアクティブ化するには、このチェックボックスをオンにします。
適用先	[すべての **MID** サーバー] または [特定の **MID** サーバー] を選択します。
MID サーバー	[特定の **MID** サーバ] を選択した場合は、ロックアイコンをクリックし、これらの認証情報を適用する MID サーバーを選択します。
順序	サーバーが認証情報を試行する順番を選択します。数値が小さいものから先に試行します。
ユーザー名	これらの認証情報に関連付けられているユーザーのユーザー名を入力します (存在する場合)。
パスワード	[ユーザー名]を入力した場合は、ユーザーのパスワードを入力します。
タグ	検索条件に使用するタグを入力します。[タグ] フィールドには、[名前] と同じ値を入力する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

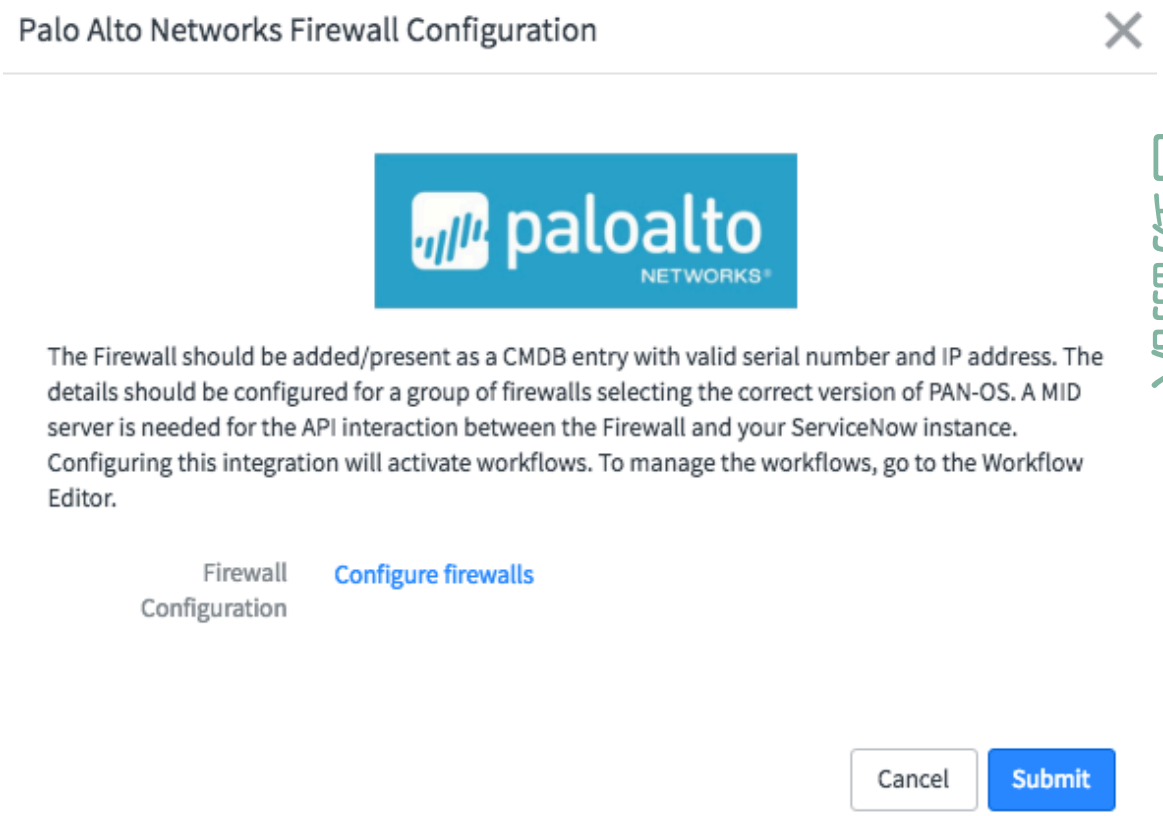
Palo Alto Networks ファイアウォール統合のアクティブ化と構成

統合構成機能を使用すると、Palo Alto Networks - Firewall を含むサードパーティのセキュリティ統合をすばやくアクティブ化して設定できます。Palo Alto Networks - Firewall を使用する前に、ServiceNow Store からダウンロードする必要があります。

始める前に
必要なロール：sn_si_admin

手順

1. 統合をアクティブ化して構成する前に、Palo Alto Networks ファイアウォールダッシュボードにアクセスします。
   ファイアウォールブロックに使用している IP 動的リスト、URL 動的リスト、またはドメイン動的リストの名前をメモします。
2. から統合をダウンロードします ServiceNow Store.
3. インストールが完了したら、次に移動します: セキュリティオペレーション > 統合設定.
   利用可能なセキュリティ統合が一連のカードとして表示されます。
4. Palo Alto Networks ファイアウォールカードで、[構成] をクリックします。



5. [ファイアウォールの設定 **(Configure firewalls)]** をクリックします。
6. [ファイアウォール設定] 画面で、[新規] をクリックします。
7. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
ファイアウォール	ロックアイコンをクリックし、設定するファイアウォールを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
ファイアウォールバージョン	Palo Alto Networks ファイアウォールバージョンを選択します。**PAN-OS-7.1** が推奨バージョンです。以前のバージョンを選択すると、一貫性のない結果が返される場合があります。
ユーザー名	REST エンドポイント経由でファイアウォールに接続するときに使用するユーザー名を入力します。
パスワード	接続するユーザーのパスワードを入力します。
IP 動的リスト	IP アドレスに使用する外部動的リストまたは動的ブロックリストの名前を入力します。
URL 動的リスト	URL に使用する外部動的リストまたは動的ブロックリストの名前を入力します。
ドメイン動的リスト	ドメインに使用する外部動的リストまたは動的ブロックリストの名前を入力します。

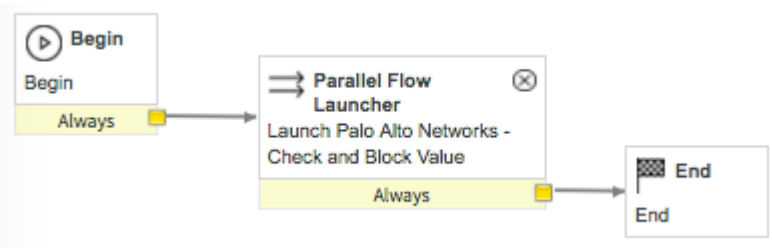
8. **[Submit]** をクリックします。

Security Operations Integration Palo Alto Networks ファイアウォールランチャーワークフロー

[Security Operations Integration Palo Alto Networks ファイアウォールランチャー] ワークフローは、**[Security Operations Integration -** 要求のブロック] 機能ワークフローによって起動される Palo Alto Networks ファイアウォール実装です。

始める前に
必要なロール：sn_si.analyst

このタスクについて
ワークフロープロセスアクティビティには次のものが含まれます。[Security Operations Palo Alto Networks - 値のチェックとブロック (Security Operations Palo Alto Networks - Check and Block Value)] ワークフロー。



[Security Operations Palo Alto Networks - 値のチェックとブロック **(Security Operations Palo Alto Networks - Check and Block Value)]** ワークフロー

潜在的な脅威を特定するためにセキュリティインシデントが作成され、トリアージされるため、**[Security Operations Palo Alto Networks -** 値のチェックとブロック **(Security Operations Palo Alto Networks - Check and Block Value)]** ワークフローを使用して、Palo Alto Networks - Firewall で定義された外部動的リストを使用して IP アドレス、URL、およびドメインを自動的にチェックおよび更新できます。

始める前に
必要なロール：sn_si.analyst

このタスクについて
ファイアウォールブロック要求が送信されると、**[Security Operations Palo Alto Networks -** 値のチェックとブロック **(Security Operations Palo Alto Networks - Check and Block Value)]** ワー

自動翻訳

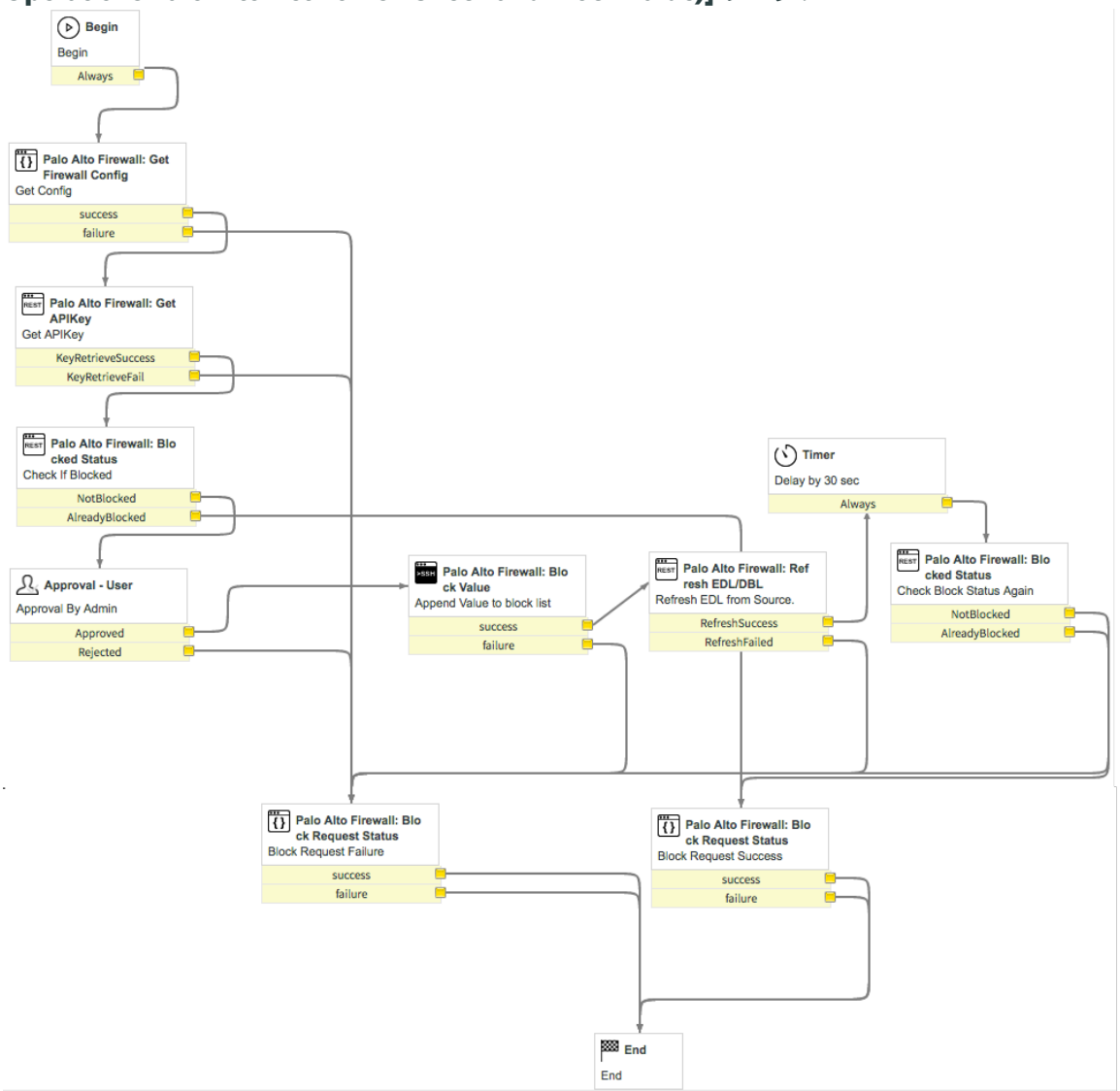
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

クフローが実行されます。ブロック要求では、使用するファイアウォール、チェックおよびブロックする観測事象のタイプ (必要な場合)、およびブロック値を指定します。つまり、問題の IP アドレス、URL、またはドメインです。

ワークフローの実行中に、 **Palo Alto Networks Integration** > ファイアウォール > コマンド 実行されています。表示タイプのコマンド (Show-IP-ExternalDynamicList など) は、値がファイアウォールに存在するかどうかを判断します。リフレッシュタイプのコマンド (Refresh-IP-ExternalDynamicList など) は、ファイアウォールに存在しない値をブロックリストに追加します。

[ブロック済みステータス] アクティビティが実行された後、ワークフローを続行するには、システムアドミニストレーターによる承認が必要です。

[Security Operations Palo Alto Networks - 値のチェックとブロック **(Security Operations Palo Alto Networks - Check and Block Value)]** ワークフロー



手順

1. 次のように移動する。 **Palo Alto Networks Integration** > ファイアウォール > ブロック要求.
2. **[New]** をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ファイアウォール	使用するファイアウォールを選択します。
ブロックタイプ	チェックする値のタイプを選択します。 ○ IP ○ URL ○ DOMAIN
ブロック値	ファイアウォールでチェックする、選択したタイプの値を入力します。

4. **[Submit]** をクリックします。

[Palo Alto ファイアウォール：ブロック要求ステータス] アクティビティ

このアクティビティは、他のアクティビティによって呼び出され、ファイアウォールブロック要求のステータスを成功または失敗に設定します。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

入力変数

変数	説明
firewallBlockRequestSysid [文字列]	ファイアウォールブロック要求のシステム ID。この入力変数は必須です。
status [文字列]	リフレッシュジョブが実行されたかどうかを success または failure で示します。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。出力は、ファイアウォール構成のデータと、動的に生成されたデータで構成されます。

出力変数

変数	説明
result [文字列]	リフレッシュジョブの成功または失敗を示します。

[Palo Alto ファイアウォール：ブロック値] アクティビティ

ワークフローがファイアウォール上にない値を識別すると、レコードは承認のためにルーティングされます。承認されると、このアクティビティは SSH 認証情報を介して MID サーバーに接続し、ファイアウォールの外部ブロックリストに値を追加するスクリプトを呼び出します。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
このアクティビティの入力変数を手動で入力し、ワークフローを公開 する必要があります。ワークフローが公開されていない場合、アドミン以外のユーザーでは入力変数は保存されません。

入力変数

変数	説明
toBeBlockedValue [文字列]	EDL に追加される値 (まだ存在しない場合)。この入力変数は必須です。
typeToBeBlocked [文字列]	ブロックする値のタイプ：IP、URL、またはドメイン。この入力変数は必須です。
targetHost [文字列]	スクリプトが実行される MID サーバー。
SSHCredentialTag [文字列]	MID サーバーで定義された SSH 認証情報タグ。
scriptCommand [文字列]	EDL に値を追加するために使用される AppendValueToList.sh スクリプト。MID サーバーへの完全パスが必要です。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
result [文字列]	EDL に渡される結果。

[Palo Alto ファイアウォール：ブロック済みステータス] アクティビティ

このアクティビティは、値 (IP、URL、またはドメイン) がファイアウォールのそれぞれの外部動的リスト/動的ブロックリスト (EDL/DBL) に含まれているかどうかを確認します。操作コマンドを使用してファイアウォールから EDL/DBL の詳細を取得し、ファイアウォールで値がブロックされているかどうかを確認するルーチンを実行します。

入力変数

アクティビティの初期動作が、入力変数によって決まります。リストされているすべての入力変数エントリーは必須です。

入力変数

変数	説明
valueToBeChecked [文字列]	ブロック要求の値。
showEDLDetailsCommand [文字列]	値がファイアウォールに存在するかどうかを判断するために使用される外部動的リストコマンド。
FirewallIpAddress [文字列]	使用されているファイアウォールの IP アドレス。
FirewallApiKey [文字列]	ファイアウォール API キー。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。出力は、ファイアウォール構成のデータと、Palo Alto ファイアウォール運用コマンド API メッセージを使用して動的に生成されたデータで構成されます。

出力変数

変数	説明
commandResult [文字列]	showEDLDetailsCommand コマンドに対するファイアウォールからの結果。
blockedStatus [ブール]	True はブロックされていることを示します。False はブロックされていないことを示します。
commandResponse [文字列]	showEDLDetailsCommand コマンドに対してファイアウォールから取得された応答ステータス。

Palo Alto ファイアウォール:API キー取得アクション

このアクションでは、ファイアウォールから API キーを取得します。

入力変数

アクションの初期動作が、入力変数によって決まります。リストされているすべての入力変数エントリーは必須です。

入力変数

変数	説明
Username [文字列]	ファイアウォールアドミンのユーザー名。
Password [文字列]	ファイアウォールアドミンのパスワード。
FirewallIpAddress [文字列]	ファイアウォールの IP アドレス。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。出力は、ファイアウォール構成のデータと、動的に生成されたデータで構成されます。

出力変数

変数	説明
APIKey [文字列]	ファイアウォール API キー。

Palo Alto ファイアウォール:ファイアウォール構成を取得アクション

[Palo Alto ファイアウォール:ファイアウォール構成を取得] フローアクションは、関連するすべてのファイアウォール構成情報をデータベースから取得し、後続のアクションで使用できるようにします。

入力変数

アクションの初期動作が、入力変数によって決まります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

入力変数

変数	説明
firewallSysid [文字列]	ファイアウォールのシステム ID。この入力変数は必須です。
typeOfValueToBeBlocked [文字列]	ファイアウォールでブロックする値のタイプ：IP、URL、またはドメイン。
firewallIPAddress [文字列]	ファイアウォールの IP アドレス。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。出力は、ファイアウォール構成のデータと、動的に生成されたデータで構成されます。

出力変数

変数	説明
ipEDLName [文字列]	IP アドレスの外部動的リスト名。
urlEDLName [文字列]	URL の外部動的リスト名。
domainEDLName [文字列]	ドメインの外部動的リスト名。
firewallVersionSysId [文字列]	ファイアウォールバージョンのシステム ID。
refreshEDLCommand [文字列]	ソースから EDL をリフレッシュするために使用するコマンド。
ShowEDLDetailsCommand [文字列]	EDL の詳細を取得するために使用するコマンド。
status [ブール]	True は成功を示します。False は失敗を示します。
error [文字列]	アクションで発生したエラー (ある場合)。
endpoint [暗号化]	データベースの暗号化されたエンドポイント。

[Palo Alto ファイアウォール：EDL/DBL をリフレッシュ] アクティビティ

このアクティビティは、ファイアウォール上で操作コマンドを実行して、ファイアウォール上に構成されたソースから外部動的リストをリフレッシュします。このアクティビティの出力は、リフレッシュジョブがキューに入れられているかどうかを示します。

入力変数

アクティビティの初期動作が、入力変数によって決まります。リストされているすべての入力変数エントリーは必須です。

入力変数

変数	説明
FirewallIpAddress [文字列]	リフレッシュされるファイアウォールの IP アドレス。
FirewallApiKey [文字列]	リフレッシュされるファイアウォールの API キー。
FirewallCommand [文字列]	リフレッシュジョブをキューに入れるために実行する操作コマンド。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。出力は、ファイアウォール構成のデータと、動的に生成されたデータで構成されます。

出力変数

変数	説明
activity.Output.result [文字列]	リフレッシュジョブが実行のためにキューに入れられたかどうかを示すテキスト文字列 (success または failure)。

ログデータ取得フロー

セキュリティインシデントレスポンス、脅威インテリジェンス、および Palo Alto Networks - Firewall が有効になっている場合、セキュリティインシデント内の観測事象のソース IP が変更されると、[**Security Operations Palo Alto Networks -** ログデータの取得] フローが自動的に実行されます。

始める前に

必要なロール：sn_si.analyst

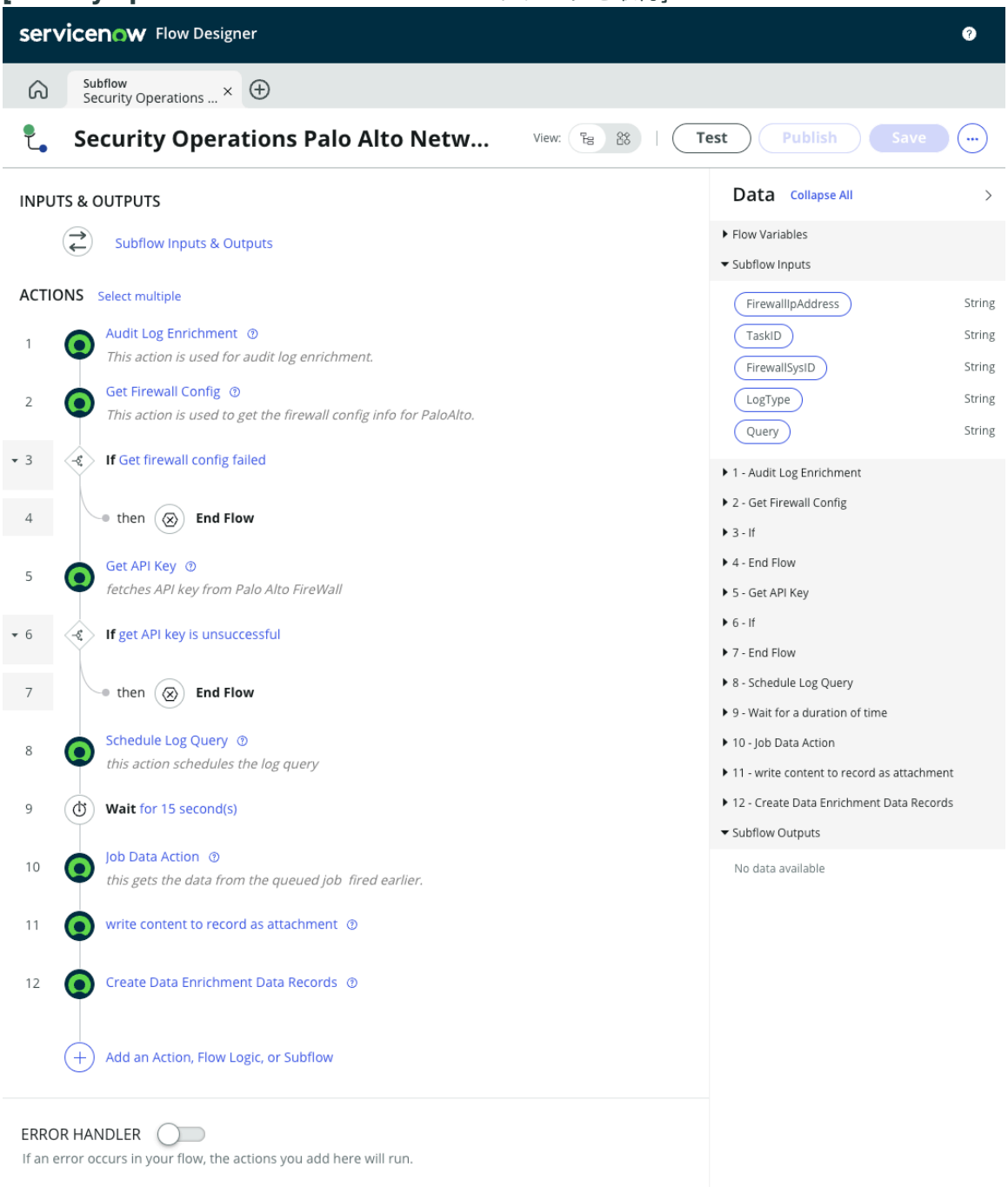
このタスクについて

フローの実行中、ファイアウォール構成情報がデータベースから取得され、API キーがファイアウォールから取得されます。「ログを取得」アクションは、ファイアウォールで検索クエリをキューに入れます。クエリが実行されると、ファイアウォールから脅威ログデータを取得するために使用されるジョブ ID が返されます。ログデータを XML ファイルとしてセキュリティインシデントに添付します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[Security Operations Palo Alto Networks - ログデータを取得] フロー



手順

1. 観測事象を含むセキュリティインシデントに移動します。
2. [セキュリティインシデント観測事象 **(Security Incident Observables)]** タブをクリックします。
3. [ソース **IP]** で、IP アドレスを追加または変更します。
4. **[Update** (更新)] をクリックします。
   [Security Operations Palo Alto Networks - ログデータを取得] フローが実行され、拡張された脅威ログデータがセキュリティインシデントに添付されます。この情報は解析され、[拡張データ] タブの [ファイアウォールログ] セクションにも表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Palo Alto ファイアウォール:API キー取得アクション

このアクションでは、ファイアウォールから API キーを取得します。

入力変数

アクションの初期動作が、入力変数によって決まります。リストされているすべての入力変数エントリーは必須です。

入力変数

変数	説明
Username [文字列]	ファイアウォールアドミンのユーザー名。
Password [文字列]	ファイアウォールアドミンのパスワード。
FirewallIpAddress [文字列]	ファイアウォールの IP アドレス。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。出力は、ファイアウォール構成のデータと、動的に生成されたデータで構成されます。

出力変数

変数	説明
APIKey [文字列]	ファイアウォール API キー。

Palo Alto ファイアウォール:ファイアウォール構成を取得アクション

[Palo Alto ファイアウォール:ファイアウォール構成を取得] フローアクションは、関連するすべてのファイアウォール構成情報をデータベースから取得し、後続のアクションで使用できるようにします。

入力変数

アクションの初期動作が、入力変数によって決まります。

入力変数

変数	説明
firewallSysid [文字列]	ファイアウォールのシステム ID。この入力変数は必須です。
typeOfValueToBeBlocked [文字列]	ファイアウォールでブロックする値のタイプ：IP、URL、またはドメイン。
firewallIPAddress [文字列]	ファイアウォールの IP アドレス。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。出力は、ファイアウォール構成のデータと、動的に生成されたデータで構成されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数

変数	説明
ipEDLName [文字列]	IP アドレスの外部動的リスト名。
urlEDLName [文字列]	URL の外部動的リスト名。
domainEDLName [文字列]	ドメインの外部動的リスト名。
firewallVersionSysId [文字列]	ファイアウォールバージョンのシステム ID。
refreshEDLCommand [文字列]	ソースから EDL をリフレッシュするために使用するコマンド。
ShowEDLDetailsCommand [文字列]	EDL の詳細を取得するために使用するコマンド。
status [ブール]	True は成功を示します。False は失敗を示します。
error [文字列]	アクションで発生したエラー (ある場合)。
endpoint [暗号化]	データベースの暗号化されたエンドポイント。

Palo Alto ファイアウォール:ログ取得アクション

[Palo Alto ファイアウォール:ログを取得] フローアクションは、ログを取得するためにファイアウォールでクエリをスケジュールし、ログデータの取得に使用される JobID を返します。

入力変数

アクションの初期動作が、入力変数によって決まります。

入力変数

変数	説明
FirewallIpAddress [文字列]	ファイアウォールの IP アドレス。この入力変数は必須です。
FirewallApiKey [文字列]	ファイアウォールの API アクセスキー。この入力変数は必須です。
FirewallLogType [文字列]	取得するログデータのタイプ (threat に設定)。この入力変数は必須です。
FirewallLogFilterQuery [文字列]	ファイアウォール上のログを検索するために実行されるクエリ。この入力変数は必須です。
LogDirection [文字列]	ログの表示を古い順にするか (逆方向)、新しい順 (順方向) にするかを指定します。
LogNumber [文字列]	取得するログの数を指定します。
LogSkipCount [文字列]	ログ取得時にスキップするログの数を指定します。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。出力は、ファイアウォール構成のデータと、動的に生成されたデータで構成されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数

変数	説明
QueuedJobID [文字列]	ファイアウォールから返されたジョブ ID。
JobScheduled [文字列]	ジョブがファイアウォールに送信されたかどうか (成功または失敗) を指定します。
error [文字列]	返されたエラー。

Palo Alto ファイアウォール:ジョブデータアクション

[Palo Alto ファイアウォール:ログを取得] アクションが検索クエリをファイアウォールにキューに入れてジョブを実行した後、[**Palo Alto** ファイアウォール:ジョブデータアクション] アクションがファイアウォールから脅威ログデータを取得します。

入力変数

アクションの初期動作が、入力変数によって決まります。すべての入力フィールドは必須です。

入力変数

変数	説明
FirewallIpAddress [文字列]	ファイアウォールの IP アドレス。
FirewallApiKey [文字列]	ファイアウォールの API アクセスキー。
JobID [文字列]	キューに格納されたジョブの ID。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。出力は、ファイアウォール構成のデータと、動的に生成されたデータで構成されます。

出力変数

変数	説明
commandStatus [文字列]	データがファイアウォールから取得されたかどうか (成功または失敗) を指定します。
JobData [文字列]	ファイアウォールから収集されたデータ。
error [文字列]	返されたエラー。

Palo Alto Networks - WildFire の統合

Palo Alto Networks - WildFire は、システムのファイアウォールとやり取りするクラウドベースのアプリケーションです。

探索　　セットアップ

セキュリティインシデントレスポンス の統合

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

(続く)

	Security Operations Palo Alto Networks - WildFire のアクティブ化
使用 WildFire データ拡張フローを取得	開発 • ServiceNow セキュリティオペレーション 統合開発のガイドライン • 統合を作成するためのヒント • 開発者トレーニング • 開発者ドキュメント • アプリケーションとともにインストールされているコンポーネントの検索
トラブルシューティングとヘルプ • 統合のトラブルシューティング • Security Operations Community で質問や回答をする • Known Error Portal で既知のエラー記事を検索 • 連絡先 カスタマーサービス & サポート	

自動翻訳

Security Operations Palo Alto Networks - WildFire のアクティブ化

Security Operations Palo Alto Networks - WildFire 統合を使用する前に、ServiceNow Store から統合をダウンロードする必要があります。

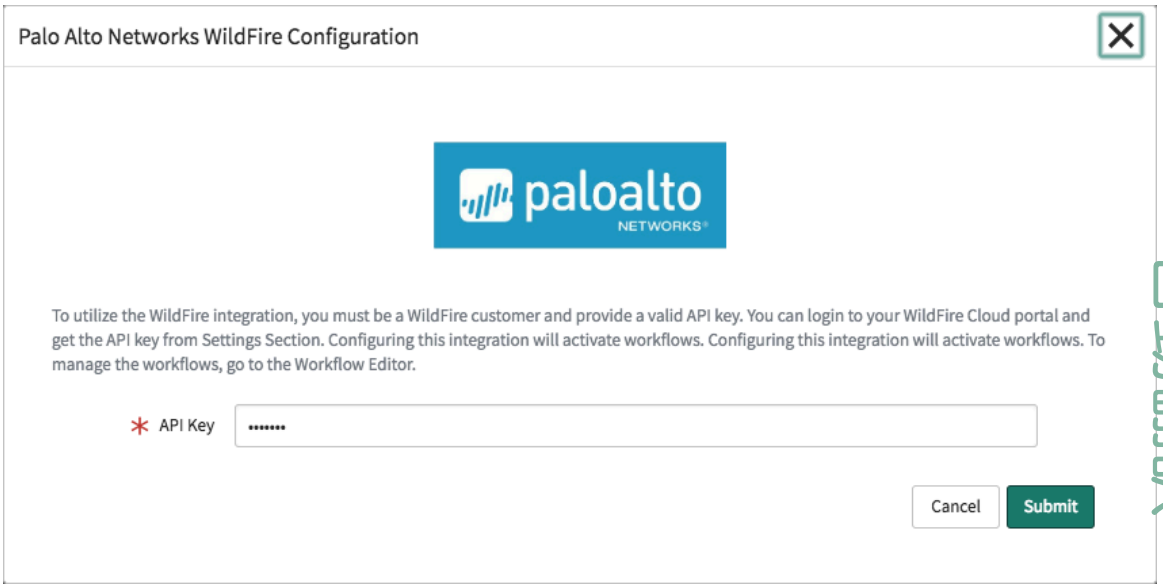
始める前に
必要なロール：admin

手順

1. から統合をダウンロードします ServiceNow Store.
2. 次のように移動する。 セキュリティオペレーション > 統合 > 統合設定.
   利用可能なセキュリティ統合が一連のカードとして表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. Carbon Black カードで、[構成] をクリックします。



4. API キーを入力し、[送信] をクリックします。
   統合構成カードが表示されます。
5. 統合構成カードの元のリストに戻るには、[構成を表示] ドロップダウンから [いいえ] を選択します。

WildFire データ拡張フローを取得

[Security Operations Palo Alto Networks - WildFire データ拡張を取得] フローが実行されると、ハッシュファイルが WildFire にアップロードされます。データが拡張され、潜在的なマルウェア攻撃の処理に役立つレポートがインスタンスにダウンロードされます。

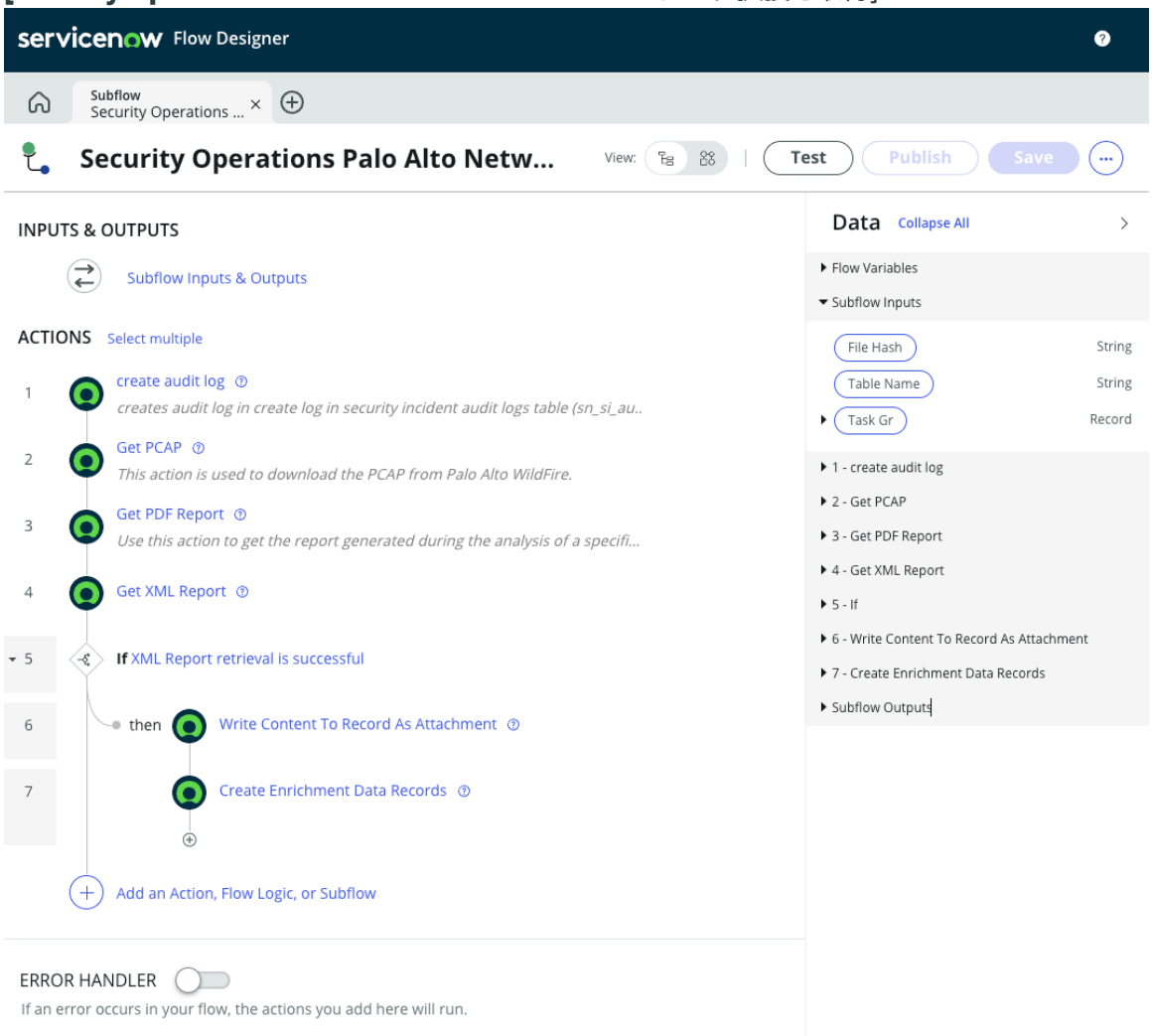
始める前に
必要なロール：sn_si.analyst

このタスクについて
[Security Operations Palo Alto Networks - WildFire データ拡張を取得 **(Security Operations Palo Alto Networks - Get WildFire Data Enrichment)**] フローは、Palo Alto Network ファイアウォールアプリケーションから受信したアラートからセキュリティインシデントが作成されると実行されます。ファイアウォールから受信したメール通知のマルウェアハッシュがセキュリティインシデントの **[IoC]** タブに入力され、レコードが更新されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[Security Operations Palo Alto Networks - WildFire データ拡張を取得] フロー



手順

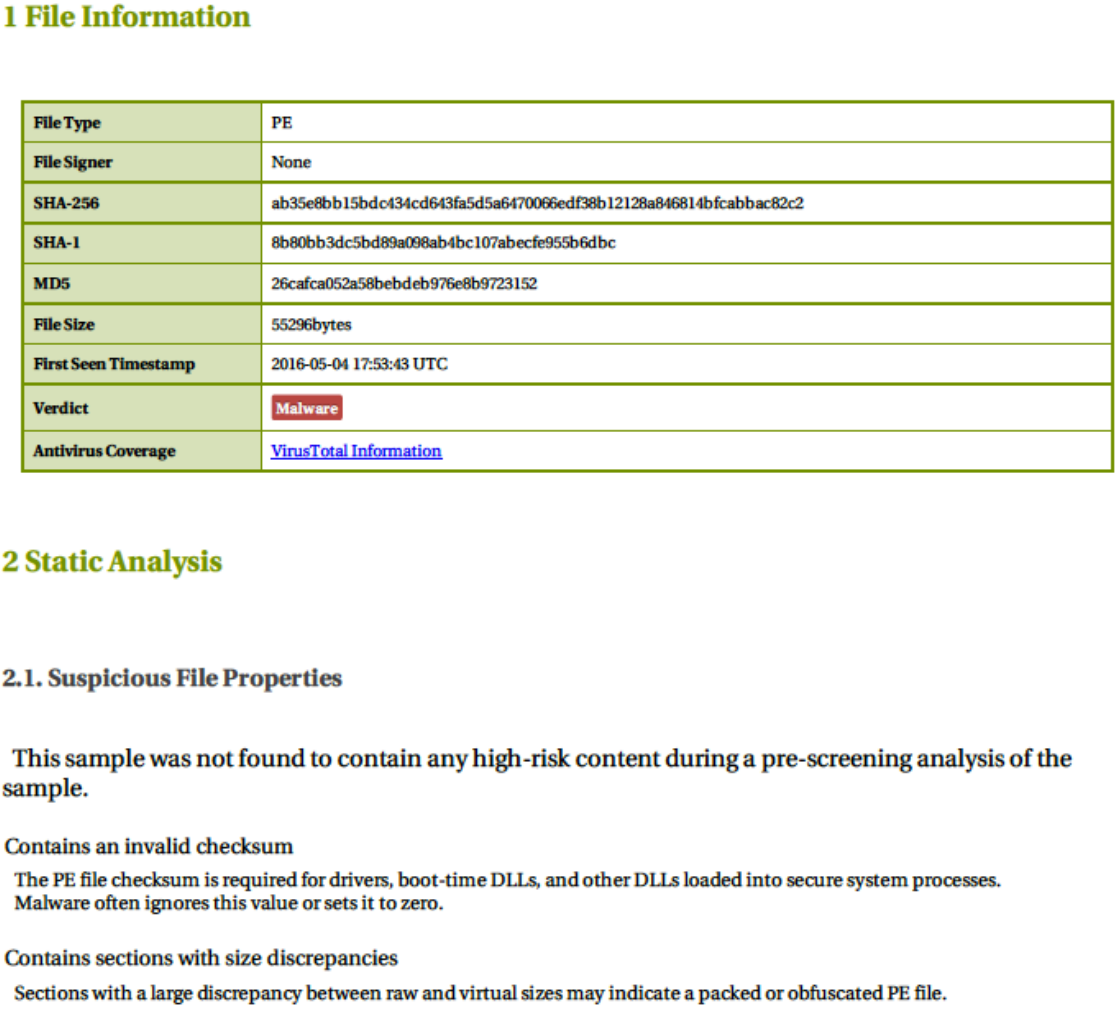
1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > オープンインシデントを表示.
2. ファイアウォールから受信したメール通知に基づいて、作成されたセキュリティインシデントを見つけて開きます。
3. [セキュリティ侵害のインジケーター] タブをクリックし、アラートで受信したハッシュを使用して [マルウェアのハッシュ] に入力します。
4. **[Update** (更新)] をクリックします。
   フローにより、ハッシュファイルが WildFire にアップロードされ、そこでデータが拡張されます。潜在的なマルウェア攻撃の処理に役立つように、PDF および XML 形式のレポートがインスタンス内のレコード (セキュリティインシデントまたは IoC) に添付されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
拡張データにパケットキャプチャ情報が含まれている場合は、PCAP 情報もダウンロードされます。PCAP データは、ファイルが実行していたアクションをキャプチャします。たとえば、ファイルが接続しているサーバーを報告できます。PCAP ファイルを表示するには、Wireshark などのパケットアナライザーが必要です。

Wildfire によって生成されたサンプル **PDF**



1 File Information

File Type	PE
File Signer	None
SHA-256	ab35e8bb15bdc434cd643fa5d5a6470066edf38b12128a846814bfcabbac82c2
SHA-1	8b80bb3dc5bd89a098ab4bc107abecfe955b6dbc
MD5	26cafca052a58bebdeb976e8b9723152
File Size	55296bytes
First Seen Timestamp	2016-05-04 17:53:43 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains an invalid checksum

The PE file checksum is required for drivers, boot-time DLLs, and other DLLs loaded into secure system processes. Malware often ignores this value or sets it to zero.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

自動翻訳

WildFire:PCAP を取得アクション

[WildFire:PCAP の取得] フローアクションは、WildFire で指定されたファイルハッシュの分析中に生成されたパケットキャプチャ (PCAP) 情報を取得します。このアクションの結果は、 **TableName** と **RecordId** で識別される特定のレコードに添付されます。

入力変数

アクションの初期動作が、入力変数によって決まります。

入力変数

変数	説明
FileSHA256Hash [文字列]	Palo Alto Network ファイアウォールアプリケーションから受信したファイルのハッシュ。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

入力変数 (続く)

変数	説明
TableName [文字列]	影響を受けるテーブル。
RecordId [文字列]	更新されるセキュリティインシデントまたは IoC。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。

出力変数

変数	説明
commandStatus [ブール]	結果が正常に取得され、添付された場合は True。
errorMessage	アクションで発生したエラー (ある場合)。

[WildFire:PDF レポートを取得] アクション

[WildFire:PDF レポートを取得] フローアクションは、WildFire で指定されたファイルハッシュの分析中に生成されたレポートを PDF 形式で取得します。このアクションの結果は、 **TableName** と **RecordId** で識別される特定のレコードに添付されます。

入力変数

アクションの初期動作が、入力変数によって決まります。

入力変数

変数	説明
TableName [文字列]	影響を受けるテーブル。
FileSHA256Hash [文字列]	Palo Alto Network ファイアウォールアプリケーションから受信したファイルのハッシュ。
RecordId [文字列]	更新されるセキュリティインシデントまたは IoC。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。

出力変数

変数	説明
commandStatus [ブール]	結果が正常に取得され、添付された場合は True。
errorMessage	アクションで発生したエラー (ある場合)。

[WildFire:XML レポートを取得] アクション

[WildFire:XML レポートを取得] フローアクションは、WildFire で指定されたファイルハッシュの分析中に生成されたレポートを XML 形式で取得します。このアクションの結果は、 **TableName** と **RecordId** で識別される特定のレコードに添付されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

入力変数

アクションの初期動作が、入力変数によって決まります。

入力変数

変数	説明
TableName [文字列]	影響を受けるテーブル。
FileSHA256Hash [文字列]	Palo Alto Network ファイアウォールアプリケーションから受信したファイルのハッシュ。
RecordId [文字列]	更新されるセキュリティインシデントまたは IoC。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。

出力変数

変数	説明
commandStatus [ブール]	結果が正常に取得され、添付された場合は True。
errorMessage	アクションで発生したエラー (ある場合)。

Palo Alto Networks Next-Generation Firewall の統合

インストールと設定が完了した後、セキュリティインシデントアナリストは、ServiceNow セキュリティインシデントレスポンス (SIR) 製品の外部動的リスト (EDL) 機能を使用して、悪意のある IP アドレス、URL、およびドメインをブロックすることができます。セキュリティインシデントアナリストは、ServiceNow SIR セキュリティインシデントで、悪意があると判断された観測事象から EDL のエントリーを作成します。

EDL は、外部 Web サーバーでホストされるテキストファイルです。この統合の場合、この Web サーバーは、お使いの Now Platform インスタンスです。ここからリストに含まれるオブジェクト、IP アドレス、URL、ドメインを Palo Alto Networks Next-Generation Firewall にインポートし、ポリシーを適用することができます。

EDL エントリーにポリシーを適用するため、ポリシールールまたはプロファイルからリストを参照します。EDL エントリーが変更されたときに、ファイアウォールは設定された間隔でリストを動的にインポートするため、ファイアウォールでの設定変更やコミットを必要とせずにポリシーを適用できます。この統合では、承認済みの Palo Alto Networks Next-Generation Firewallによって、設定された取得間隔で取得される EDL エントリを含むテーブルを Now Platform に作成しています。

この統合には次の機能が含まれています。

- 複数の EDL を作成して、さまざまなファイアウォール拒否または許可ポリシーに適用できる柔軟性
- ブロックされているサイトのタイプ (フィッシング、マルウェア、許可リストサイト) に関する詳細なレポート
- 観測可能タイプ (URL、ドメイン、IP アドレス) 別の EDL エントリーによる Now Platform セキュリティインシデントのタグ付け
- EDL に有効期間を設定することで、古いエントリーを自動的に失効または削除し、EDL リストのサイズを維持

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- EDL リスト間での EDL エントリーの検索、削除、移行
- 脅威インテリジェンスの結果とエントリーがブロックされた理由の詳細を含む、観測可能なレコードとセキュリティインシデントに EDL エントリーをリンク

統合では、セキュリティインシデントレスポンス 製品の (com.snc.security_incident) および (com.snc.secops.orchestration) プラグインが有効になっている必要があります。

この統合でサポートしているのは、Palo Alto Networks (PAN-OS 8.x) のみです。以前のバージョンはサポートされていません。

この統合は、Kingston、London、Madrid、New York リリースの Now Platform® と互換性があります。

注:
次のトピックには番号が付けられています。インストールと設定をスムーズに行い、期待した結果が得られるように、記載されている順序のとおりにトピックに従ってください。

Palo Alto Networks Next-Generation Firewall の証明書プロファイルの作成

この統合では、Now Platform® サーバーと Palo Alto Networks Next-Generation Firewall サーバーの間のセキュア接続を検証および認証するために証明書プロファイルが必要になります。

必要なロール: Palo Alto Networks Next-Generation Firewall アドミニストレーター。

Palo Alto Networks Next-Generation Firewall は Now Platform® インスタンスに対して認証し、データベーステーブルから EDL エントリーを取得して、対応するファイアウォールポリシールールに組み込みます。この取得には、Now Platform® インスタンスの API ユーザーアカウントロールが必要です。このロールは、Now Platform® API にアクセスするために PAN ファイアウォールアドミニストレーターによって使用されます。

DigiCertificates をダウンロードし、証明書プロファイルを設定する方法については、以下の手順に従ってください。

1. ユースケースに基づいて DigiCert または Entrust CA Gateway 証明書をダウンロードします。詳細については、Now Support ナレッジベース のKB1702083 記事を参照してください。
2. 証明書プロファイルを構成します。詳細については、 Palo Alto Networks のドキュメント を参照してください。

関連情報

『PAN-OS 10.0 Administrator's Guide (PAN-OS 10.0 管理ガイド)』の「Configure a Certificate Profile (証明書プロファイルの設定)」

Palo Alto Networks Next-Generation Firewall のセットアップとインストール

インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールをスムーズに行うために必要です。

始める前に
必要なロール：(admin)

セットアップタスク	説明
必要な Now Platform ロールと セキュリティインシデントレスポンス ロールがアサインされていることを確認します。	以下のロールが必要です。 • システムアドミニストレーター (admin) は、アプリをインストールし、セキュリティインシデントアドミン (sn_si.admin) ロールをアサインします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	• セキュリティインシデントアドミン (sn_si.admin) は、設定を監督し、EDL を作成、アクティブ化、削除します。このロールは、sn_si.analyst ロールもアサインします。 • (admin) は Now Platform API アカウントロール (sn_sec_panfw.api_account_access) をアサインします。このロールは、ファイアウォールが Now Platform から EDL を取得できるように、Palo Alto Networks での認証に必要な認証情報を入力するためにのみ使用されます。 • (sn_si.analyst)、または Security Operations Center (SOC) アナリストは、EDL エントリーを作成し、セキュリティインシデントに対処します。
Palo Alto Networks Next-Generation Firewall バージョン OS 9.x、または 10.x を使用していることを確認します。	この統合は Palo Alto Networks Next-Generation Firewall OS 9.0 以降のみをサポートしています。
Palo Alto Networks ドキュメントで推奨されているように、Palo Alto Networks で EDL プロファイル、セキュリティポリシールール、および証明書プロファイルを設定します。	Paloalto Networks ドキュメント Web サイト の Palo Alto Networks ドキュメント全般と要件を参照してください。
DigiCert ルート機関証明書をダウンロードして構成したことを確認します。	この統合では、Now Platform サーバーと Palo Alto Networks Next-Generation Firewall サーバーの間のセキュア接続を検証および認証するためにこの証明書が必要になります。証明書のセットアップの詳細については、『PAN-OS 10.0 Administrator's Guide (PAN-OS 10.0 管理ガイド)』の「Configure a Certificate Profile (証明書プロファイルの設定)」を参照してください。ダウンロードについては、「Palo Alto Networks Next-Generation Firewall の証明書プロファイルの作成 と DigiCert の信頼できるルート機関の証明書」を参照してください。
統合用のアプリケーションをインストールする前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	Madrid 以降のリリースの要件 Madrid リリース以降のファミリリリースでは、セキュリティインシデントレスポンス Dependency プラグイン (com.snc.si_dep) が必要です。このプラグインは、セキュリティインシデントレスポンス 製品をサポートするために必要なすべての依存関係を自動的にインストールします。統合に必要な他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。 **1.** セキュリティインシデントレスポンス **2.** Security Integration Framework **3.** Security Support Common **4.** セキュリティサポートオーケストレーション 統合のための Now Platform インスタンスのセットアップの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。
組織にメール削除用の Now Platform の変更管理および承認プロセスがある場合は、メールの送受信機能が有効になっていることを確認します。	Now Platform インスタンスでメールの送受信機能が有効になっていることを確認するには、メールプロパティ > アドミニストレーション > メールプロパティ. [送信メール設定] で、[メール送信] と [メール受信] が選択されていることを確認します。

手順

統合用のアプリケーションをインストールしていない場合は、「セキュリティオペレーション 統合のインストール」を参照し、手順に従ってインストールしてください。

Palo Alto Networks Next-Generation Firewall の API アカウントロールの作成

この統合には、Now Platform インスタンスに API アカウントロールが必要です。このアカウントに関連付けられたユーザー名とパスワードは Now Platform で作成され、Palo Alto Networks に入力されるため、Palo Alto Networks Next-Generation Firewall は EDL エントリーを取得するときに Now Platform で認証されます。

始める前に
必要なロール：admin

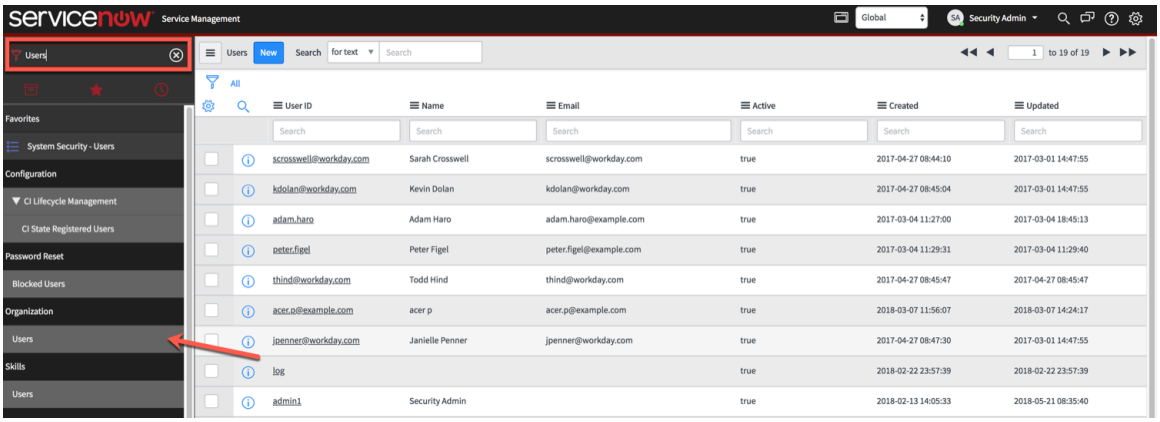
このタスクについて
Now Platform アドミニストレーターが API アカウントロール (sn_sec_panfw.api_account_access) を作成します。このアカウントは、ファイアウォールが Now Platform から EDL を取得できるように、Palo Alto Networks の認証に必要な認証情報を入力するためだけに使用されます。このアカウントは、Now Platform インスタンス内の独立した一意の API ユーザーアカウントであり、Palo Alto Networks Next-Generation Firewall アドミニストレーターにアサインされます。

自動翻訳

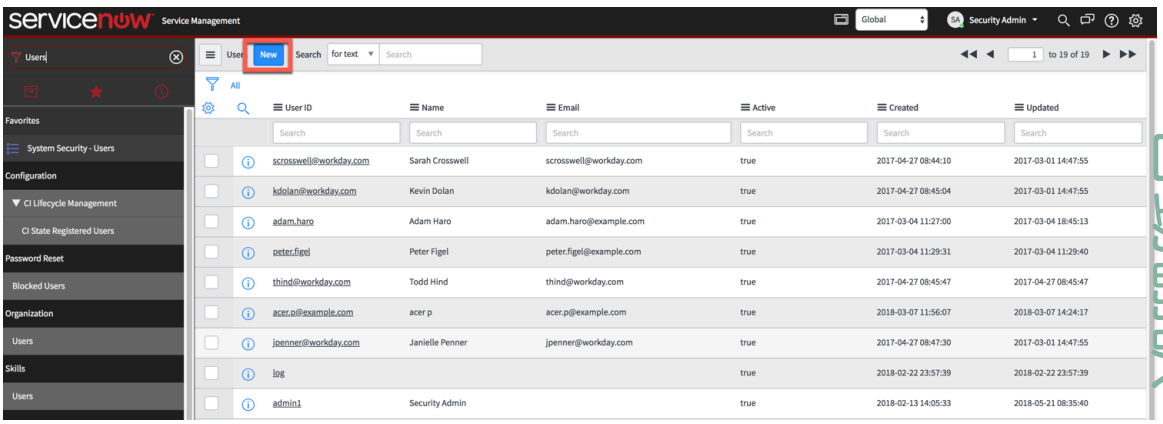
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 組織 > ユーザー.
2. [ユーザー] モジュールをクリックします。



3. 表示される [ユーザー] リストで、[新規] をクリックします。



新しいユーザーフォームが表示されます。

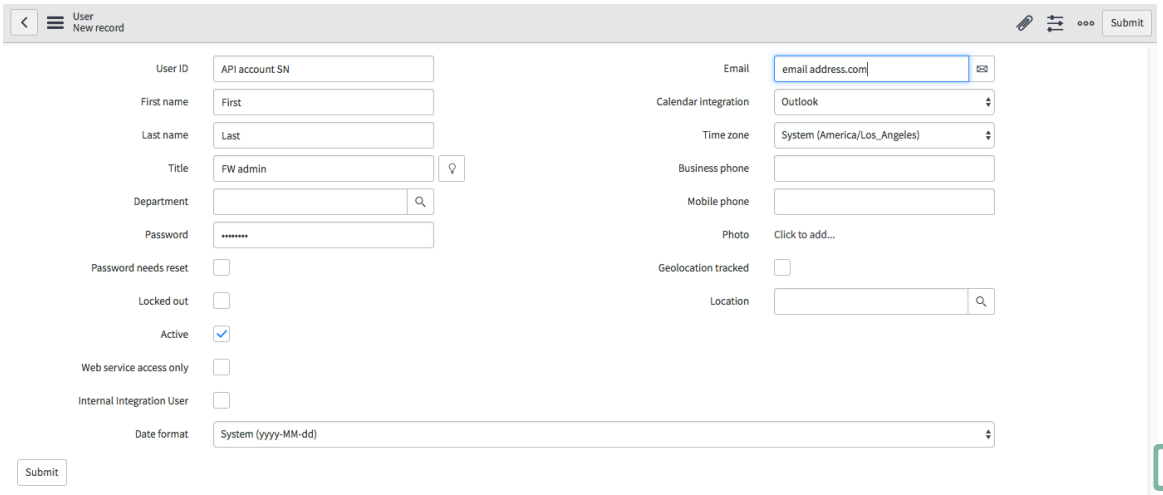
4. フォームに入力します。

> **注:**
> 次の表と図に示すユーザー ID、タイトル、メールアドレスの値は、値の例です。

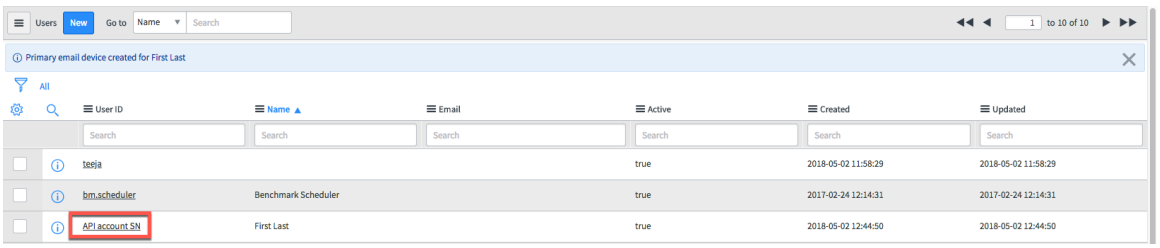
フィールド	説明
ユーザー ID	Now Platform® インスタンスのロールの一意のユーザー ID。このユーザー ID は、Palo Alto Networks サイトの [外部動的リスト (External Dynamic Lists)] ダイアログの [クライアント認証 **(Client Authentication)**] セクションの [ユーザー名 **(Username)**] フィールドに入力されます。例：API account SN。
名	アサインする人物
姓	アサインする人物
タイトル	役職 (FW admin など)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
パスワード	このロール用に作成した一意のパスワード。このパスワードは、Palo Alto Networks サイトの [外部動的リスト (External Dynamic Lists)] ダイアログの [クライアント認証 **(Client Authentication)**] セクションの [パスワード **(Password)**] フィールドに入力されます。
メール	一意のメールアドレス

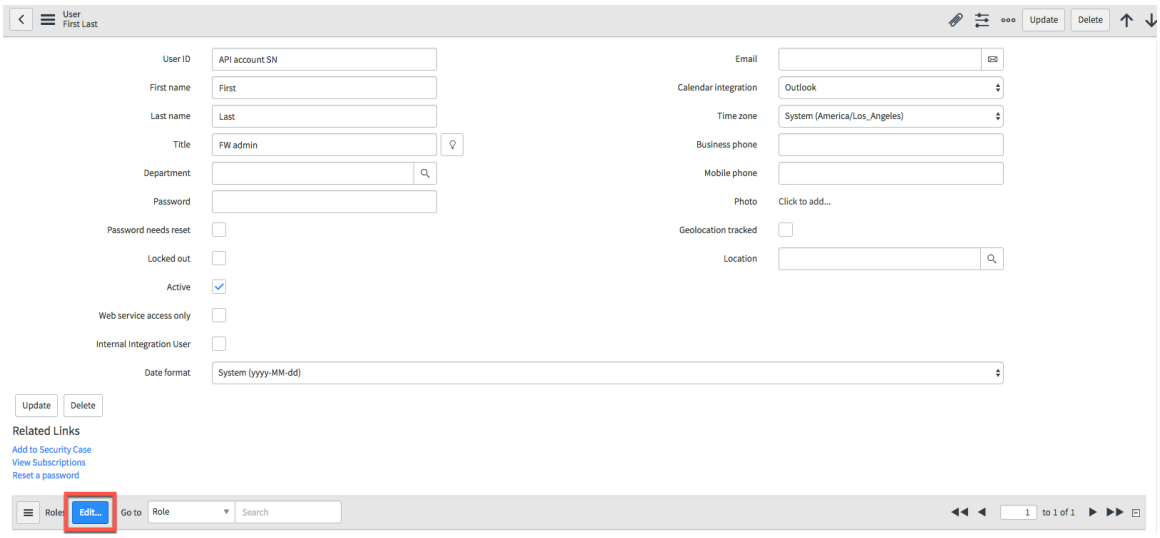


5. **[Submit]** をクリックします。
   送信後、ロールをアサインできます。
6. [ユーザー **ID]** 列の [ユーザー] リストで、入力したユーザー ID の名前 (例：API account SN) をクリックします。

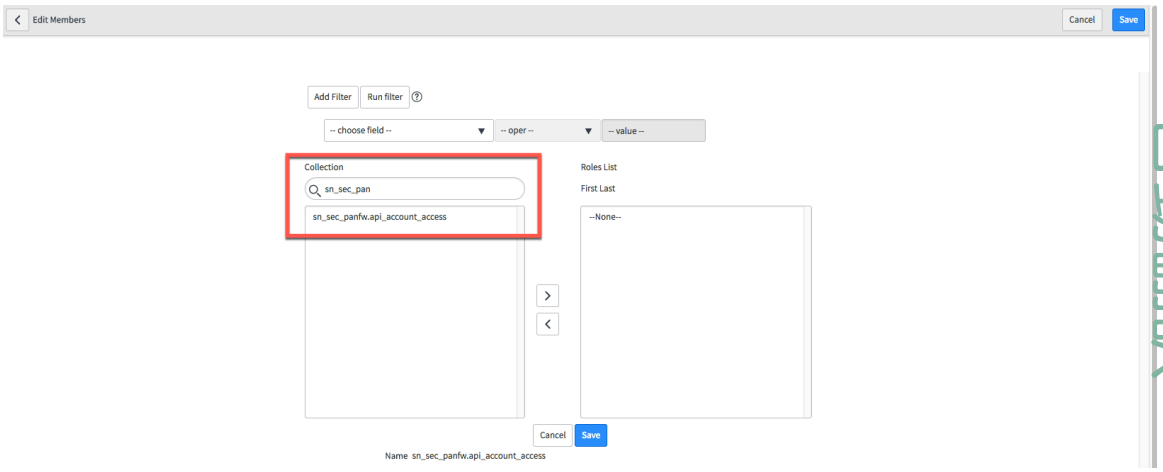


7. [ロール] セクションのオープンレコードで、[編集] をクリックします。

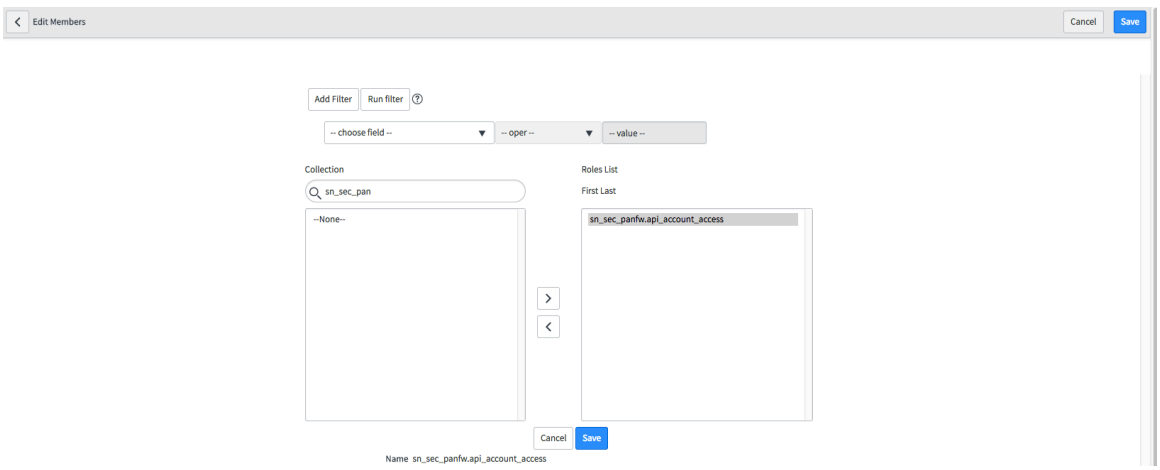
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



8. 表示される [メンバーの編集] フォームで、[コレクション] フィールドに「sn_sec_panfw.api_account_access」と入力します。
[コレクション] フィールドの下の列にロールが表示されます。



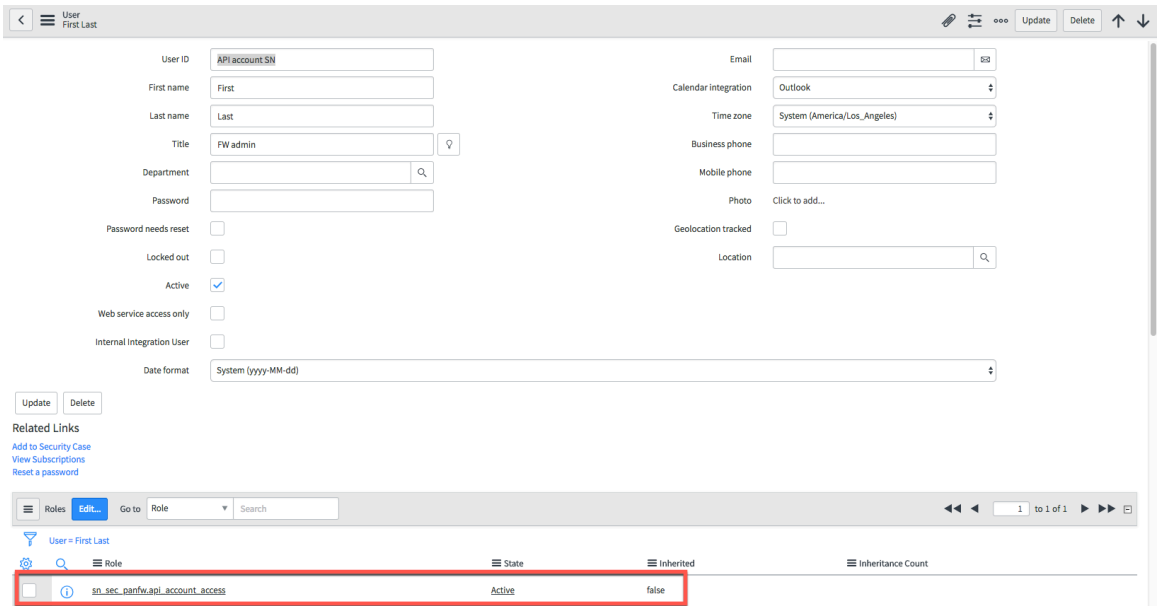
9. [コレクション] 列で、[sn_sec_panfw.api_account_access] を選択して、[ロールリスト **(Roles List)]** に移動します。



10. [保存] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

11. [ユーザー] に移動し、リストの [ユーザー] 列で、ロールに作成した ID 名 (API account SN) をクリックします。



ユーザーレコードが表示されます。このレコードで、ユーザーアカウントがアサインされていることを確認できます。[ステータス] はアクティブです。ロールは継承されていません。

サポートされている **Palo Alto Networks Next-Generation Firewall** の外部動的リスト **(Supported External Dynamic Lists for Palo Alto Networks Next-Generation Firewall)**

ServiceNow Palo Alto Networks Next-Generation Firewall 統合は、IP、URL、およびドメイン観測事象に対応する外部動的リスト (EDL) をサポートしています。

サポートされる **EDL** と観測事象タイプ

外部動的リストは、外部 *Web* サーバーでホストされるテキストファイルです。この統合では、Now Platform インスタンスでホストされます。そして、Palo Alto Networks Next-Generation Firewall はリストに含まれているオブジェクト (IP アドレス、URL、ドメイン) をインポートし、ポリシーを適用できます。EDL エントリーにポリシーを適用するため、ポリシールールまたはプロファイルからリストを参照します。

この統合は、次の 3 つのタイプの EDL をサポートしています。

- IP (単一の IP アドレスと複数のアドレスの CIDR ブロック (範囲) が含まれます)
- URL
- ドメイン

次の表に、この統合でサポートされている観測事象の説明と各タイプの形式の例を示します。

サポートされる観測事象と形式の例

観測事象	形式の例	説明
IP アドレス	• 95.153.103.54 (IPv4) • (IPv6) : 2001:00B8:130F:FE03:0000:09C0:080F:130B	単一の個別のインターフェイスアドレスを表します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サポートされる観測事象と形式の例 (続く)

観測事象	形式の例	説明
		統合は、IPv4、IPv6、および CIDR 形式をサポートしています。 IP アドレス観測事象のサポートには、CIDR (クラスレスドメイン間ルーティング) 範囲が含まれます (例：95.153.100.0/22)。 注：CIDR 範囲の一部としてすでにブロックしている EDL に単一の IP アドレスを添付しようとすると、エラーメッセージが表示されます。たとえば、単一のアドレス 95.153.103.54 は、95.153.100.0/22 (95.153.100.0-95.153.103.255) で表される CIDR 範囲の一部です。
URL	• www.example.com • www.example.com/article.html • example.com • *.example.com	ワイルドカードがサポートされています。Now Platform は、Palo Alto Networks EDL 形式の要件に準拠するように URL エントリーを再フォーマットします。
ドメイン	• www.example.com • example.com • mail.example.com	ワイルドカードはサポートされていません。

書式設定のガイドラインと EDL の詳細については、 Palo Alto Networks Web サイトの『PAN-OS 10.0 Administrator's Guide (PAN-OS 10.0 管理ガイド)』の「Formatting Guidelines for an External Dynamic List (外部動的リストのフォーマットに関するガイドライン)」を参照してください。

Palo Alto ネットワーク次世代ファイアウォールの EDL 作成

Now Platform インスタンスに外部動的リスト (EDL) を作成します。承認されてアクティブ化されると、Now Platform セキュリティインシデントレスポンス (SIR) インシデントで悪意があると判断された観測事象から EDL のエントリーを作成し、それらをブロックするための承認を要求できます。

始める前に

必要なロール：sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
ファイアウォールがリストに含まれているオブジェクト (IP アドレス、URL、ドメイン) をインポートできるように、Now Platform インスタンスに EDL を作成し、ポリシーを適用します。EDL エントリーにポリシーを適用するため、ポリシールールまたはプロファイルからリストを参照します。

次のセクションの図は、[システムの設定] で [タブ付きフォーム] をオフにした状態で示されています。 タブ付きフォームの選択とクリアの詳細については、Configuring the form layout の「タブ付きフォームの表示」を参照してください。

手順

1. アプリケーションのインストールが完了したら、次に移動します: 統合 > 統合設定.
2. Palo Alto Networks Next-Generation Firewall タイルを探して、[構成] をクリックします。

3. [新しい **EDL** リストの作成 **(Create new EDL List)]** をクリックします。

4. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[Palo Alto Networks 次世代ファイアウォール外部動的リスト **(Palo Alto Networks Firewall External Dynamic List)]** フォーム

フィールド	説明
名前	Palo Alto Networks ファイアウォール動的リスト名。 このフィールドに観測事象タイプ (URL、IP、ドメイン) を含めて、セキュリティアナリストが名前で EDL の目的を簡単に認識できるようにします。また、これらの EDL オブジェクトがどのようなファイアウォールポリシーにマッピングされるのかを名前で明確に示す必要もあります。EDL 名の例としては、 送信マルウェア IP、 送信フィッシング URL などが挙げられます。
アクティブ	デフォルトではこのチェックボックスはオフになっており、EDL が非アクティブであることを示します。 EDL が非アクティブの場合、追加のエントリーを受け取ることができません。 チェックボックスをオンにすると、EDL が有効になり、EDL エントリーに使用できるようになります。
タグを表示	このチェックボックスはデフォルトでオンになっており、観測事象が EDL でブロックされた場合に、観測事象と関連するセキュリティインシデントレコードに自動的にタグが付きます。オンにすると、[タグタイプ] フィールドと [観測事象の EDL タグ (EDL tag for observables)] フィールドをフォームで使用できるようになります。 **注:** タグ名は、デフォルトでは、[名前] フィールドに入力した値に、*EDL-* プリフィックスを付けたものになります (例：EDL-マルウェア送信 IP)。タグの名前と色は変更できます。「(オプション) Palo Alto Networks Next-Generation Firewall のセキュリティタグ名の編集」を参照してください。EDL が保存されると、[観測事象の EDL タグ (EDL tag for observables)] フィールドにタグ名が表示されます。 このチェックボックスをオフにすると、タグが作成されず、[タグタイプ] および [観測事象の EDL タグ (EDL tag for observables)] フィールドをフォームで使用できなくなります。

自動翻訳

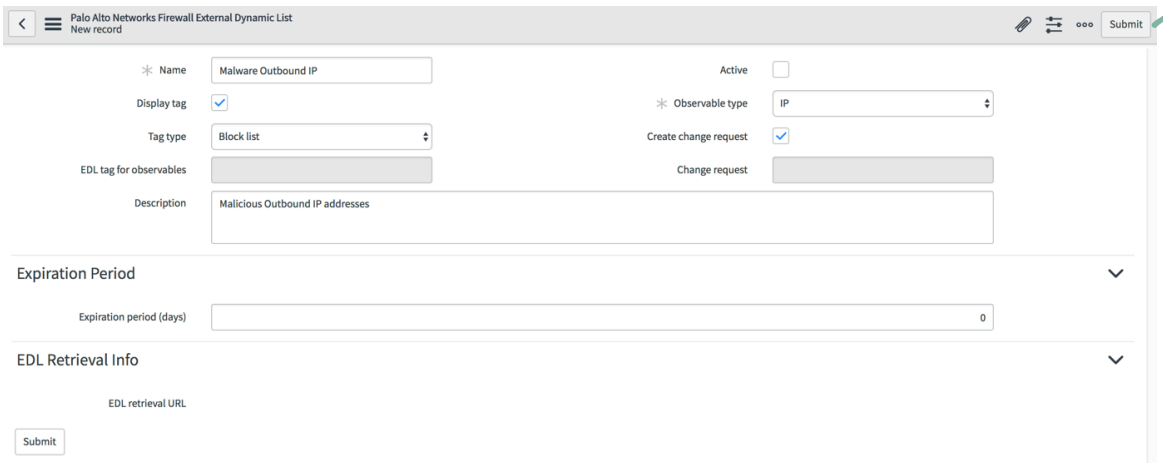
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
観測事象タイプ	この EDL が受け付ける観測事象タイプ (IP (CIDR を含む)、URL、またはドメイン) を選択します。
タグタイプ	選択リストから選択可能なタグ。 ブロックリストは、Palo Alto Networks Next-Generation Firewall にブロックしてほしい観測事象のリストです。 許可リストは、 Palo Alto Networks Next-Generation Firewall に許可してほしい観測事象のリストです。 デフォルトでは、ブロックリストのタグの色は黒で、許可リストのタグの色はグレーです。色は変更できます。「(オプション) Palo Alto Networks Next-Generation Firewall のセキュリティタグ名の編集」を参照してください。
変更要求の作成	このチェックボックスはデフォルトでオンになっており、Now Platform インスタンスで変更要求と変更タスクを自動的に作成し、EDL レコードに添付します。 変更要求は、Palo Alto Networks Next-Generation Firewall サーバーで EDL リスト取得 URL を設定するために使用されます。 ファイアウォールアドミニストレーターがファイアウォールポリシーまたはルールの変更に Now Platform も使用している場合は、このオプションをお勧めします。要求を作成して、要求がクローズされると、EDL リストは自動的に有効になります。 Palo Alto Networks の設定が完了したことの通知をファイアウォールアドミンからメールで受け取った後に、EDL を手動でアクティブ化する場合は、チェックボックスをオフにします。 [変更要求の作成] チェックボックスをオフにすると、[変更の要求] フィールドは使用できなくなります。
観測事象の **EDL** タグ	このフィールドは、[タグを表示] チェックボックスがオンになっている場合にのみ表示されます。EDL が保存されると、このフィールドに [名前] フィールドのデフォルト値が自動的に入力されます。 デフォルトのタグ名と色の変更の詳細については、「(オプション) Palo Alto Networks Next-Generation Firewall のセキュリティタグ名の編集」を参照してください。

自動翻訳

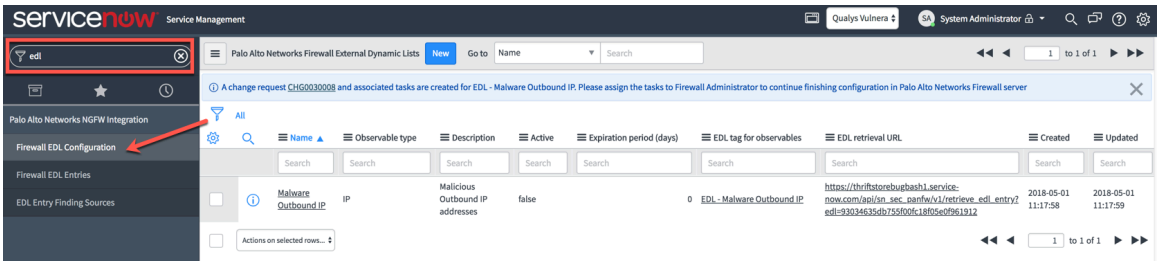
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
変更要求	[変更要求の作成] チェックボックスをオンにすると、EDL が保存されたときに、Now Platform インスタンスに変更要求番号が表示されます。 [変更要求の作成] チェックボックスをオフにすると、このフィールドは表示されません。
説明	Palo Alto Networks ファイアウォール動的リストの説明。名前には通常、この EDL にあると予想されるサイトと観測事象のタイプが含まれており、このフィールドを使用して詳細を確認できます。
有効期間 (日数)	EDL の有効期間。 0 (デフォルト) は、EDL エントリーが無期限であることを示します。 この値を変更すると、このエントリーは入力した日数の間有効になります。入力できる最小値は 1 で、最大値はありません。 たとえば、5 月 1 日の午後 2 時 1 分に 30 日と入力すると、EDL は 5 月 31 日の午後 2 時 1 分に有効期限切れになります。 この EDL のすべてのエントリーは、個々のエントリー単位で値を上書きしない限り、デフォルトでこの値を継承します。

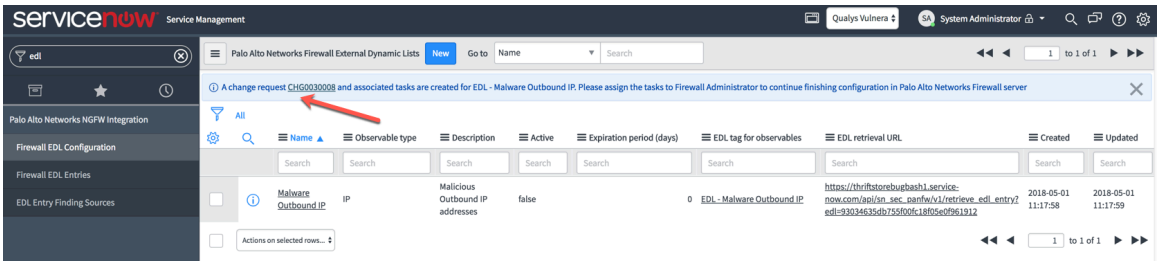


5. [**Submit** (送信)] を選択します。
6. [Palo Alto Networks ファイアウォール外部動的リスト] リストが表示されない場合は、 **Palo Alto Networks NGFW** 統合 > ファイアウォール **EDL** 構成 をクリックし、[ファイアウォール **EDL** 構成] をクリックします。

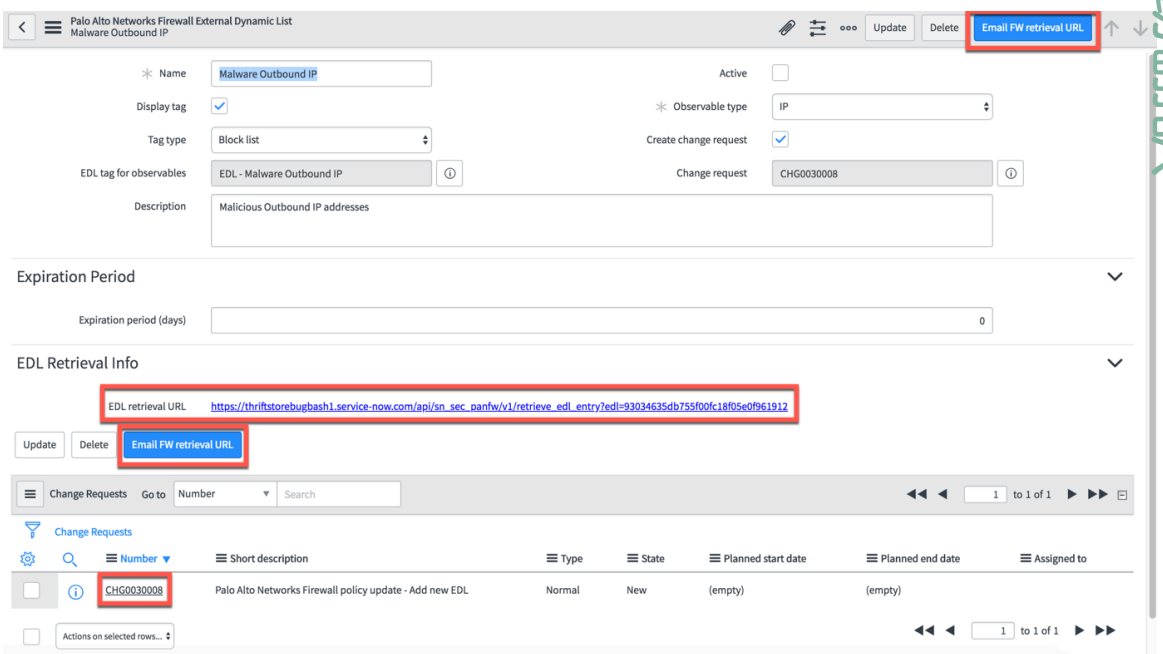
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



新しい EDL が表示されます。EDL ステータスはまだ非アクティブ (false) です。これは、EDL がエントリーを受け入れることができないことを意味します。[変更要求の作成] が設定されている場合は、Now Platform インスタンスに変更の要求とタスクが作成されたことを示すメッセージが表示されます。



7. [名前] 列でアイテムをクリックしてレコードを開きます。
EDL レコードが表示されます。この例では、マルウェア送信 IP EDL を示しています。次のフィールド、オプション、リンクが送信後に新しいレコードに表示されます。詳細は次の表を参照してください。



EDL レコード上の取得 URL と変更要求リンク

オプション	説明
メール **FW** 取得 **URL**	Palo Alto Networks ファイアウォールアドミニストレーターに、設定のための EDL リンクが使用可能であることをメールで通知します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
EDL 取得 URL	この URL は、Palo Alto Networks Web サイトの [リストを作成 **(Create List)]** タブの [外部動的リスト認証 (External Dynamic Lists authentication)] ダイアログボックスの [ソース] フィールドに配置されます。 Palo Alto Networks ファイアウォールアドミニストレーターが Palo Alto Networks ファイアウォールの設定に使用する URL リンクが自動的に生成され、表示されます。 **注:** [システムの設定] を [タブ付きフォーム] に設定している場合、このリンクはレコード下部の **[EDL** 取得情報] タブに表示されます。
Now Platform 変更要求	設定時に変更要求レコードへのリンクが [変更の要求] セクションに表示され、要求番号が [変更の要求] フィールドに表示されます。
更新	データを変更し、編集可能なフィールドを更新します。
削除	レコードを削除します。

8. 必要に応じて、さらに EDL を作成して追加します。
   EDL は [Palo Alto Networks 外部動的リスト] リストに表示されます。

次のタスク
手動で、または Now Platform 変更要求を使用して、EDL をアクティブ化します。

Palo Alto Networks® Next-Generation Firewall の EDL をアクティブ化する

Now Platform™ に外部動的リスト (EDL) が作成され、URL が利用可能になったら、Palo Alto Networks ファイアウォールアドミニストレーターが Palo Alto Networks Next-Generation Firewall で EDL を設定します。取得 URL は、Palo Alto Networks ファイアウォールアドミニストレーターが Palo Alto Networks Next-Generation Firewall サーバーで EDL を設定するために使用します。EDL エントリーを受け入れるには、Palo Alto Networks で EDL を設定し、Now Platform™ でアクティブ化する必要があります。

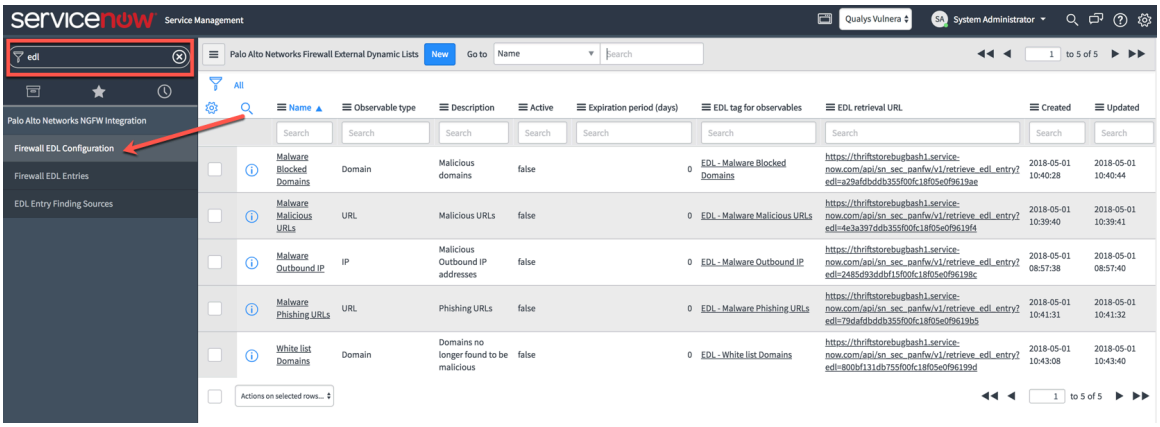
始める前に
必要なロール：sn_si.admin

このタスクについて
EDL が設定された後、セキュリティインシデントアドミニストレーターとして、EDL を手動でアクティブ化するか、Now Platform™ 変更要求の完了時に EDL を自動的にアクティブ化することができます。EDL は、EDL エントリーを受け入れる前に承認され、非アクティブ状況からアクティブ状況に移行する必要があります。

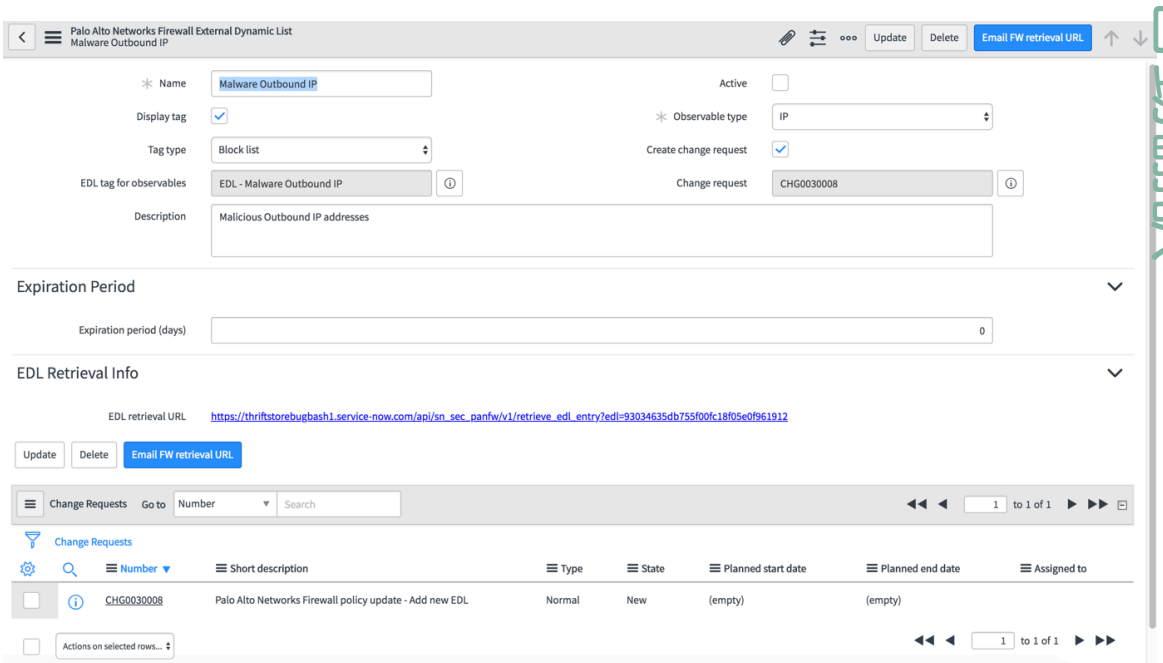
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > **Palo Alto Networks NGFW** 統合 > ファイアウォール **EDL** 構成 をクリックし、 ファイアウォール **EDL** 構成 モジュールを選択します。



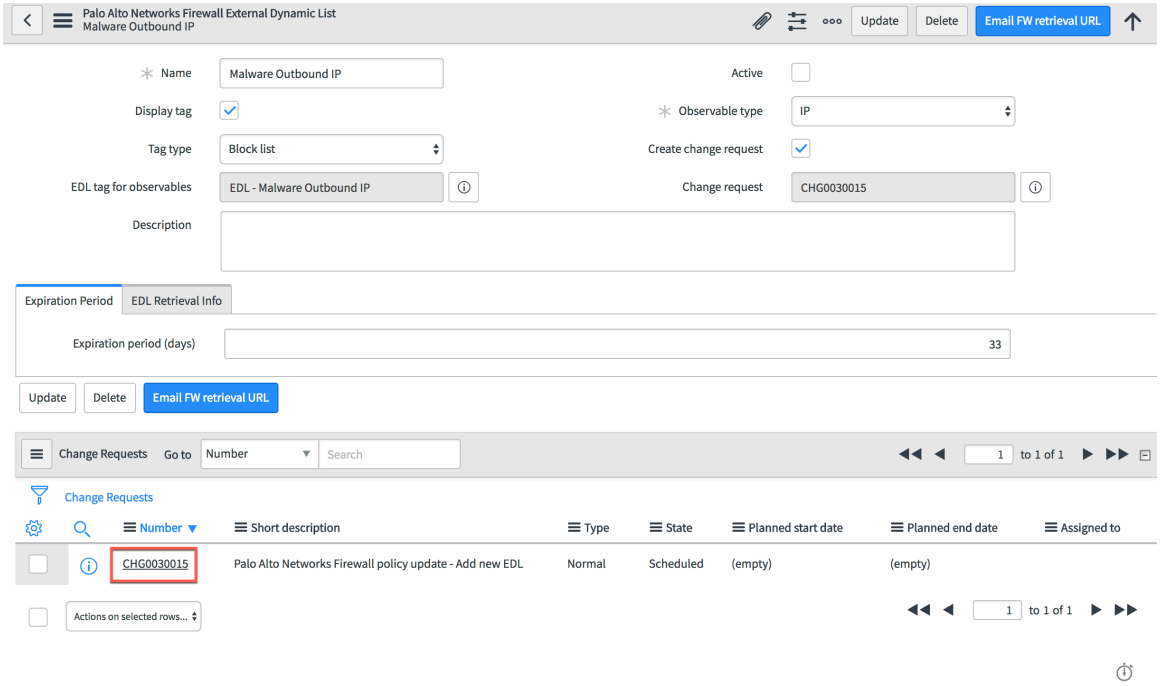
2. 表示される [Palo Alto Networks ファイアウォール動的リスト (Palo Alto Networks Firewall Dynamic Lists)] リストで、[名前] 列で新しい EDL を選択します。
3. 表示されるレコードで、[メール **FW** 取得 **URL]** ボタン、アクティブな [EDL 取得 URL] リンク、そして設定してある場合は、[変更の要求] セクションの Now Platform　変更要求を確認します。[アクティブ] チェックボックスがオフになっていることを確認します。



> **注:**
> システムの設定で [タブ付きフォーム] がオフになっていると、前の図に示したように EDL 取得 URL が **[EDL** 取得情報] セクションに表示されます。

次の図では、システムの設定で [タブ付きフォーム] がオンになっているため、**[EDL** 取得情報] がタブとして表示されています。**[EDL** 取得情報] タブをクリックして、取得 URL を表示します。変更要求へのリンク (**CH0030015**) も表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. 設定を完了し、EDL を非アクティブからアクティブに移行させるには、次のいずれかのオプションを選択して、取得 URL が利用可能であることをファイアウォールアドミニストレーターに通知する必要があります。
   取得 URL が利用可能であることをファイアウォールアドミニストレーターに通知し、Palo Alto Networksで EDL が設定されていることを確認したら、次の手順では、セキュリティインシデントアドミニストレーターとして EDL をアクティブ化します。EDL を手動でアクティブ化するか、設定されている場合は、Now Platform 変更要求フォームを使用して EDL をアクティブ化します。

関連情報

Palo Alto Networks Next-Generation Firewall で EDL を設定する

Palo Alto Networks Next-Generation Firewall の EDL を手動でアクティブ化する

Palo Alto Networks ファイアウォールアドミニストレーターが Now Platformを使用しておらず、Palo Alto Networks Next-Generation Firewall が設定されていることが自分に直接通知されている場合は、外部動的リスト (EDL) を手動でアクティブ化することができます。

始める前に
Palo Alto Networks で、作成した EDL に EDL オブジェクト、ポリシー、ソース URL をアサインします。Palo Alto Networks で EDL を Palo Alto Networks Next-Generation Firewall に設定する方法の詳細については、「Palo Alto Networks Next-Generation Firewall で EDL を設定する」を参照してください。

必要なロール：sn_si.admin

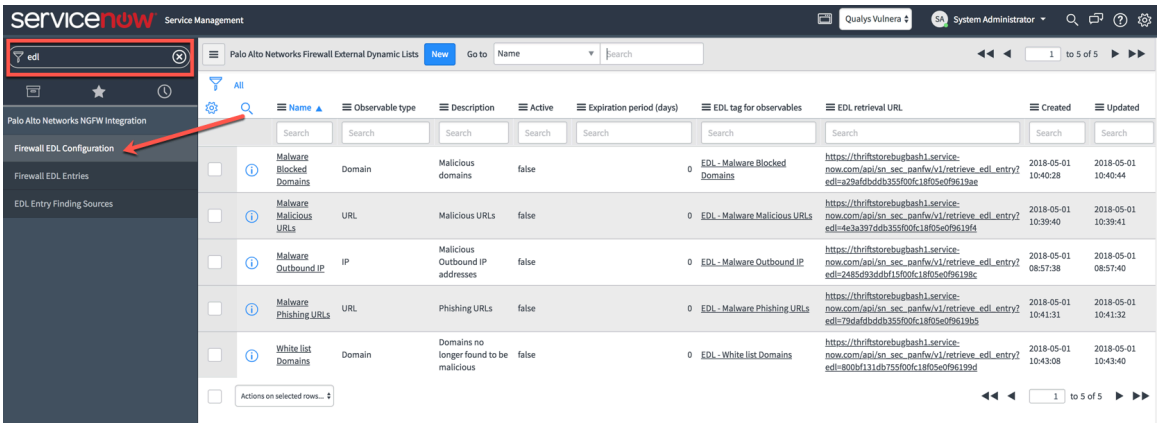
このタスクについて
Now Platform セキュリティインシデントアドミニストレーターは、Palo Alto Networks Next-Generation Firewall で EDL の設定が完了したときに、Palo Alto Networks ファイアウォールアドミンから通知を受け取ります。

自動翻訳

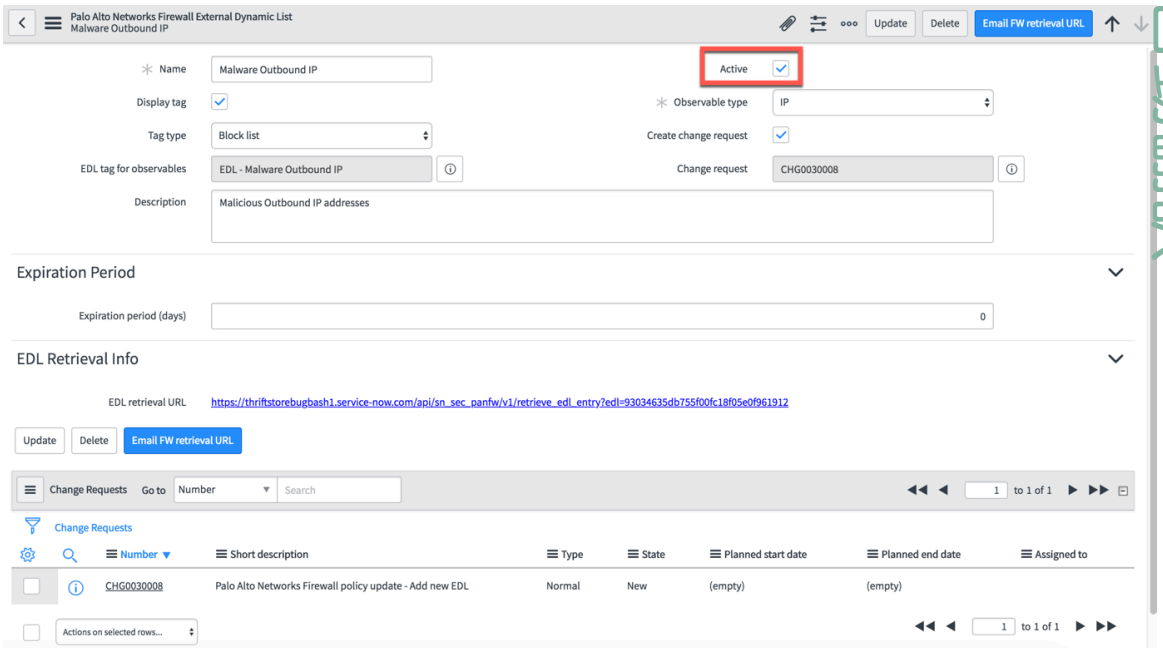
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > **Palo Alto Networks NGFW** 統合 > ファイアウォール **EDL** 構成.



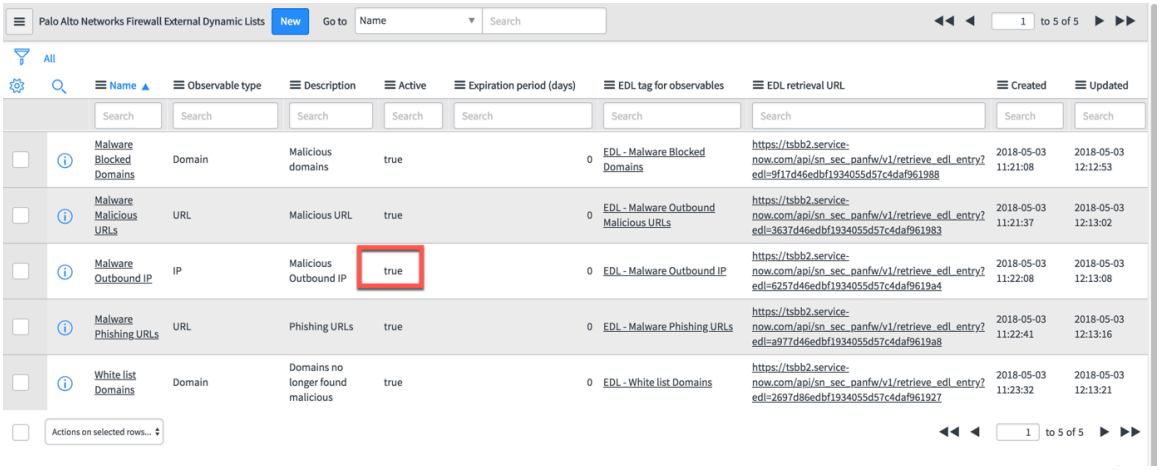
2. [ファイアウォール **EDL** 構成] モジュールを選択します。
3. [Palo Alto Networks ファイアウォール外部動的リスト] リストで、 [名前] 列のアイテムをクリックして開きます。
4. レコードが開いたら、[アクティブ] チェックボックスをオンにします。



5. [更新] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[Palo Alto Networks ファイアウォール外部動的リスト] リストの [アクティブ] 列で、EDL のステータスに true が表示されます。



タスクの結果
EDL が有効になり、EDL エントリーを受信する準備ができました。

次のタスク
セキュリティインシデントまたはブロックリストから EDL エントリーを送信します。

Palo Alto Networks Next-Generation Firewall で EDL を設定する

Palo Alto Networks ファイアウォールアドミニストレーターは、Now Platform から取得 URL が利用可能であると通知を受けると、Palo Alto Networks Next-Generation Firewall に EDL を設定します。EDL は、Palo Alto Networks で設定し、Now Platform でアクティブ化してからでないと、EDL エントリーを受け付けられません。

始める前に
必要なロール：Palo Alto Networks ファイアウォールアドミン

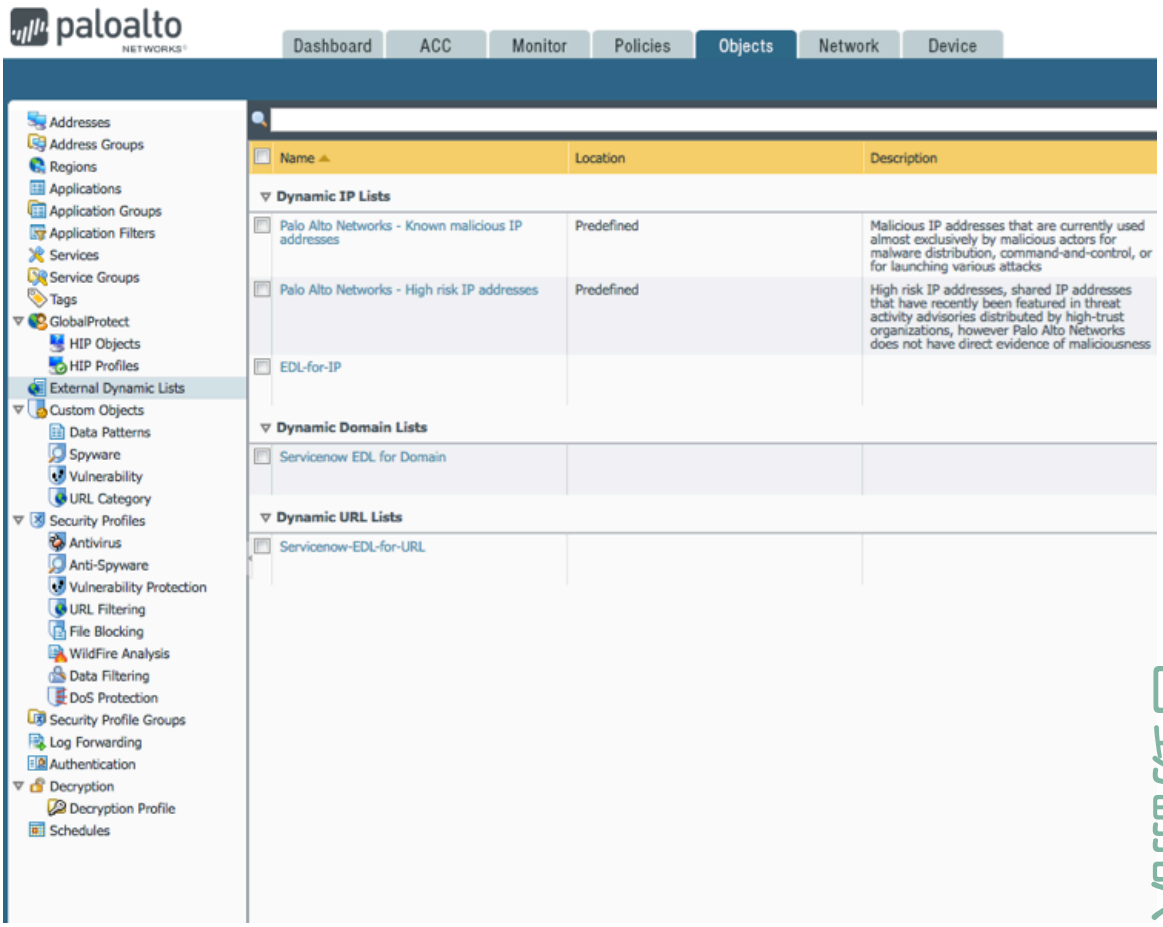
このタスクについて
Palo Alto Networks Next-Generation Firewall アドミニストレーターは、EDL オブジェクトを作成し、ソース (取得) URL とポリシーを EDL にアサインします。これらのタスクは、Now Platform で EDL が有効になる前に Palo Alto Networks で実行されます。

以下のセクションの画像は特権のある専有物であり、許可を得て使用しています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

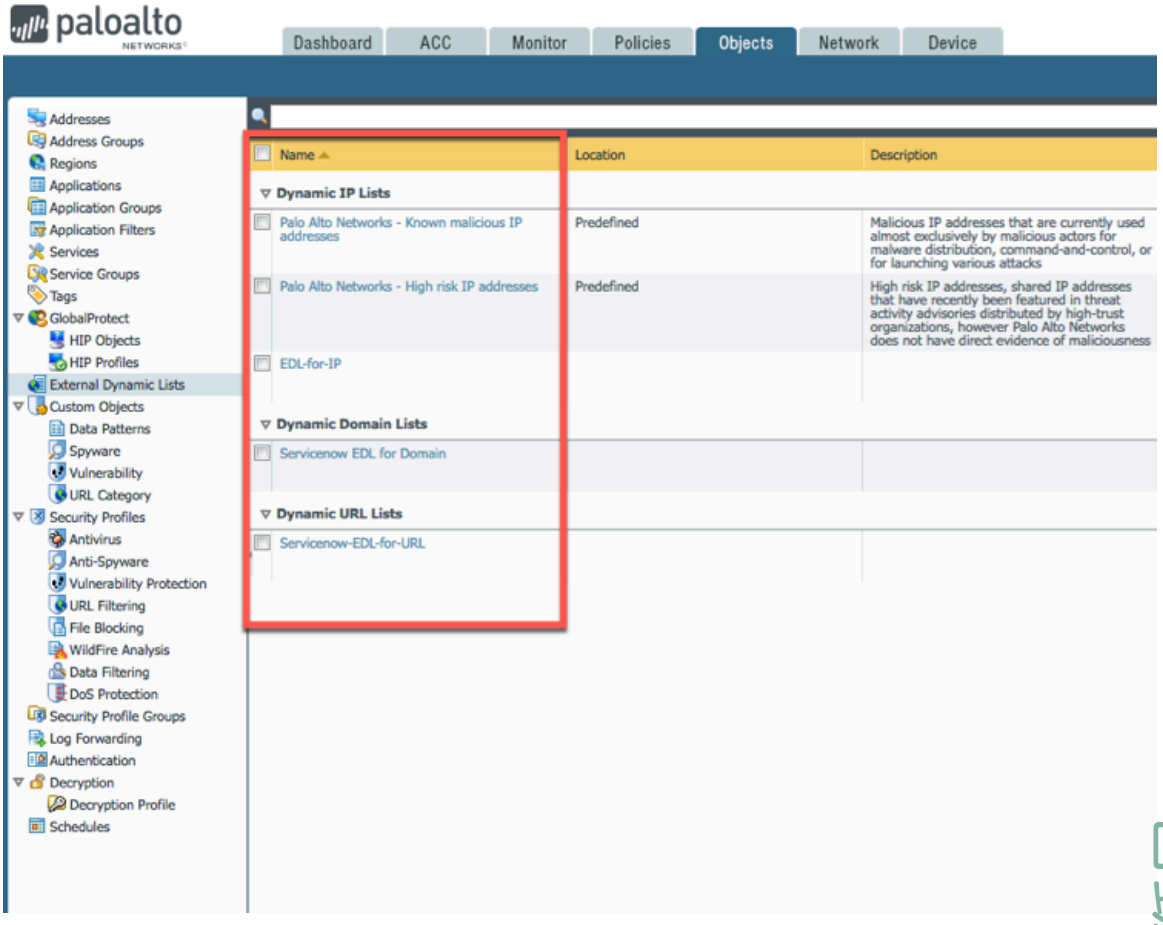
1. ファイアウォールに EDL を設定していない場合は、 外部動的リスト > オブジェクト in Palo Alto Networks.



2. [名前 **(Name)]** 列で、設定する ServiceNow EDL をリストから選択します。たとえば、**URL** 用の **ServiceNow EDL (ServiceNow EDL for URL)** です。

自動翻訳

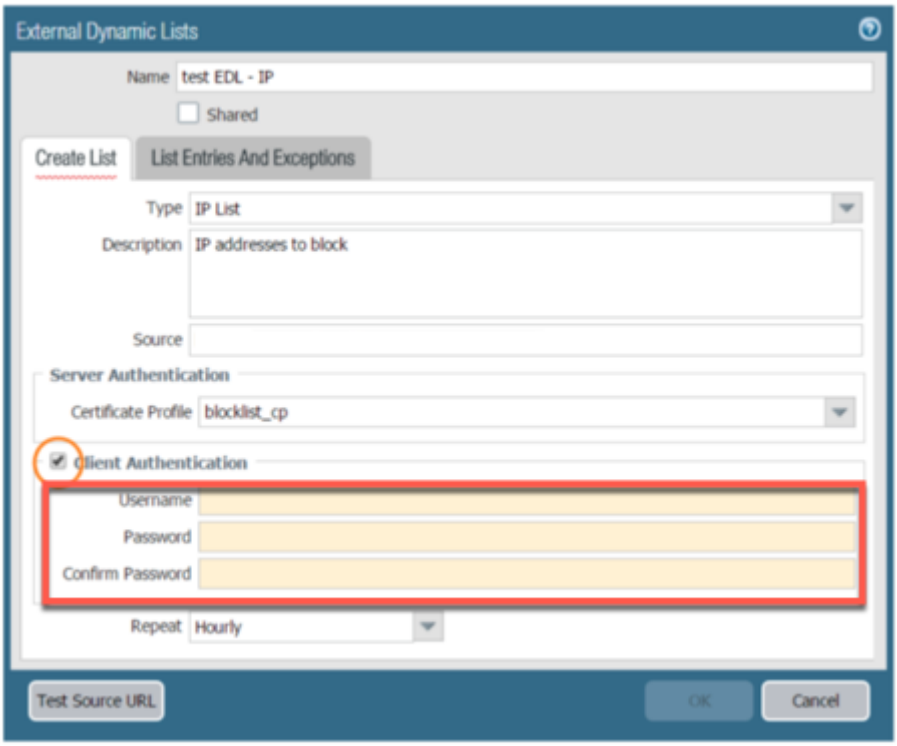
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



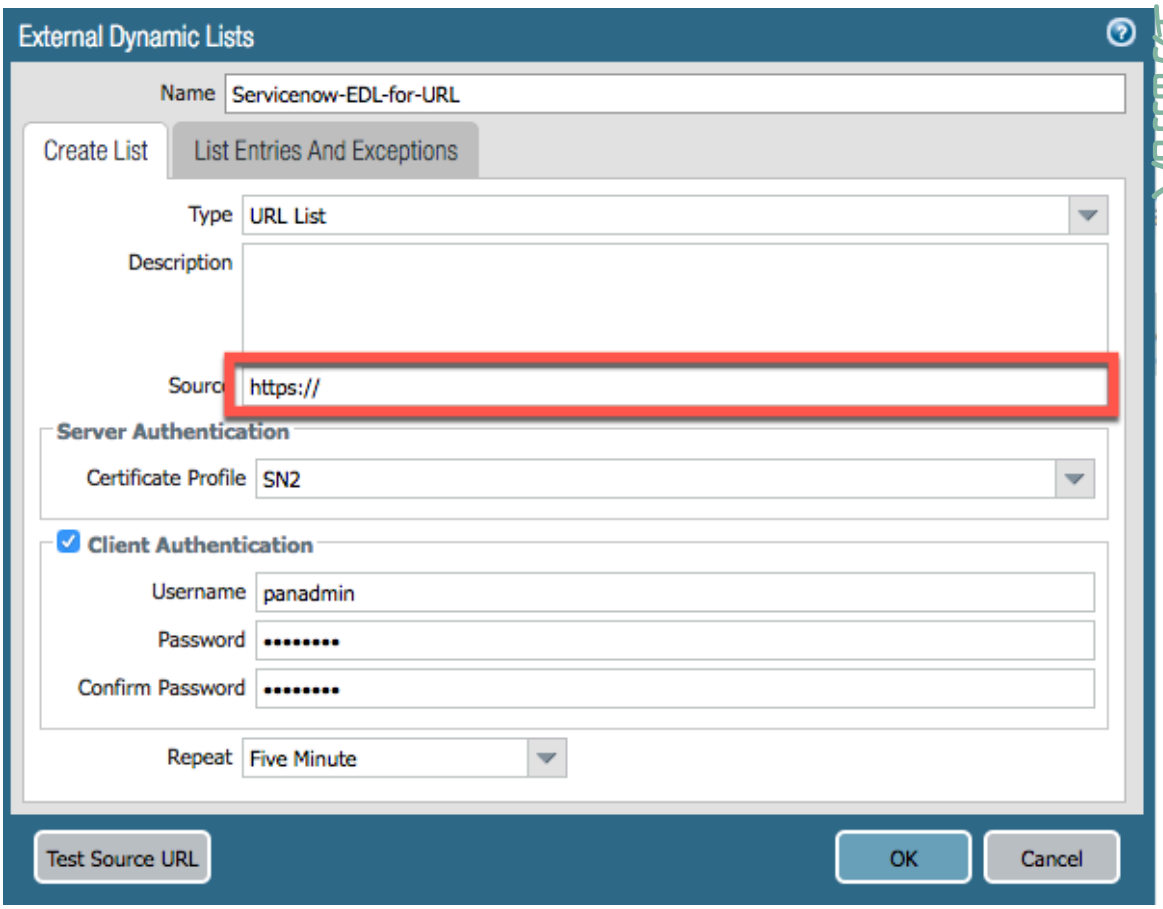
3. [外部動的リスト (External Dynamic Lists)] ダイアログボックスで、 ユーザー名とパスワードを入力し、Now Platform　の認証を行います。
この認証情報は、ServiceNow インスタンスで、API アカウントロール (sn_sec_panfw.api_account_access) のために作成したユーザー名とパスワードです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [ソース (Source)] フィールドに、ServiceNow インスタンスの EDL リストで生成された URL を入力します。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. 選択リストから「SN2」などの証明書プロファイルを選択します。
6. [OK] をクリックします。

変更要求を使用した Palo Alto Networks Next-Generation Firewall の EDL のアクティブ化

設定されている場合は、ServiceNow 変更要求フォームを使用して、外部動的リスト (EDL) がアクティブ化されます。ファイアウォールアドミニストレーターがファイアウォールポリシーまたはルールの変更に Now Platform も使用している場合は、このオプションをお勧めします。Now Platform 変更要求がクローズされると、EDL は自動的に有効になり、EDL エントリーを受け取る準備ができます。

始める前に

注:
次のセクションの図は、[システムの設定] で [タブ付きフォーム] をオンにした状態で示されています。 タブ付きフォームのオン/オフの詳細については、ServiceNow 製品ドキュメント Web サイト の「Display tabbed forms in Configuring the form layout (フォームレイアウトを設定する際のタブ付きフォームの表示)」セクションを参照してください。

必要なロール：変更要求および変更タスクを承認するための sn_si.admin

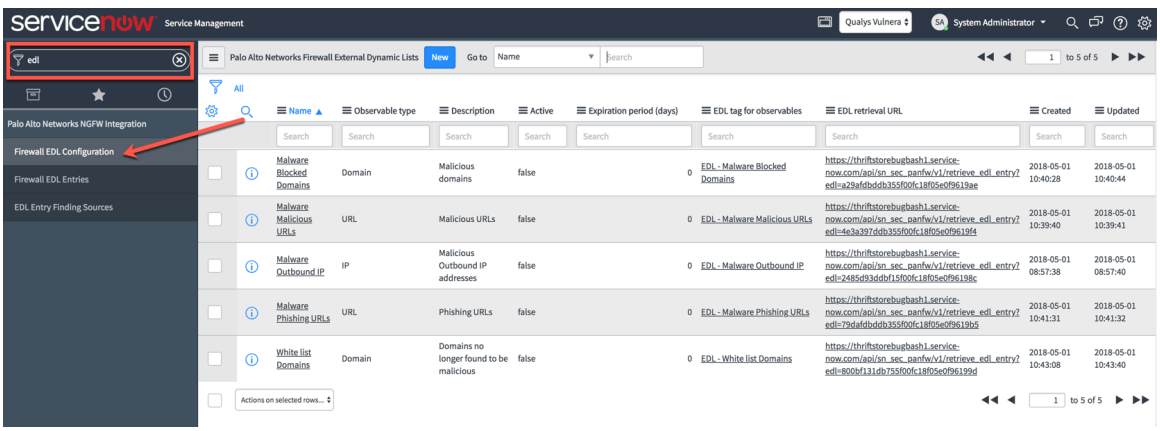
Palo Alto Networks で構成タスクを完了するための Palo Alto Networks ファイアウォールアドミン

このタスクについて

設定されている場合は、Now Platform の変更要求を監視し、Palo Alto Networks Next-Generation Firewall の設定に必要なタスクをアサインします。これらのタスクが完了したら、Now Platform の変更要求をクローズして EDL を自動的にアクティブ化します。

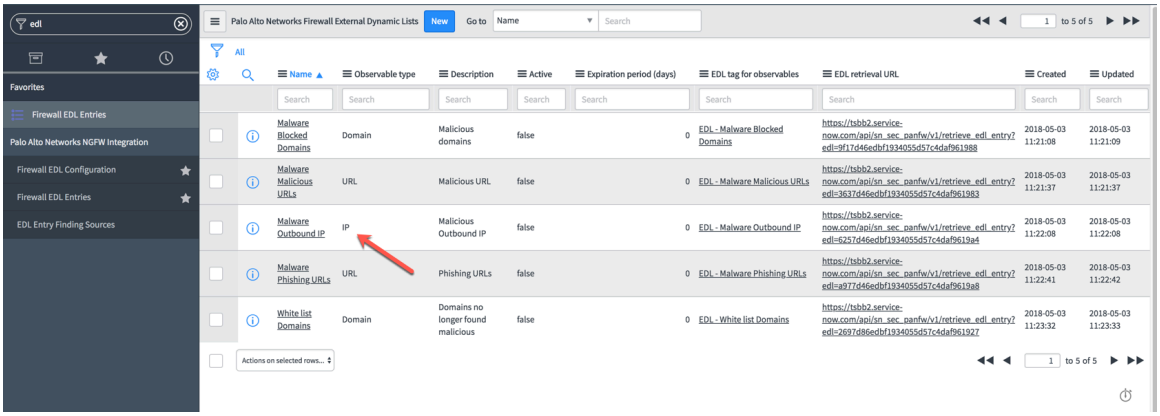
手順

1. 次のように移動する。 **All** (すべて) > **Palo Alto Networks NGFW** 統合 > ファイアウォール **EDL** 構成.

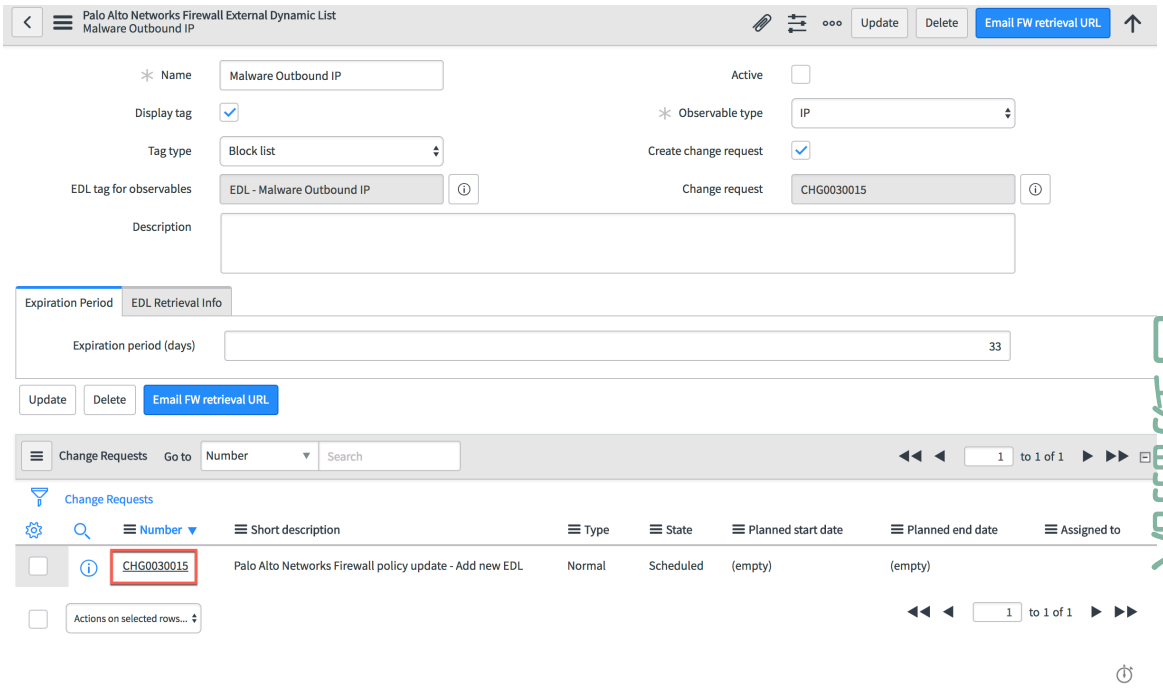


2. EDL モジュールを選択し、[名前] 列で EDL をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

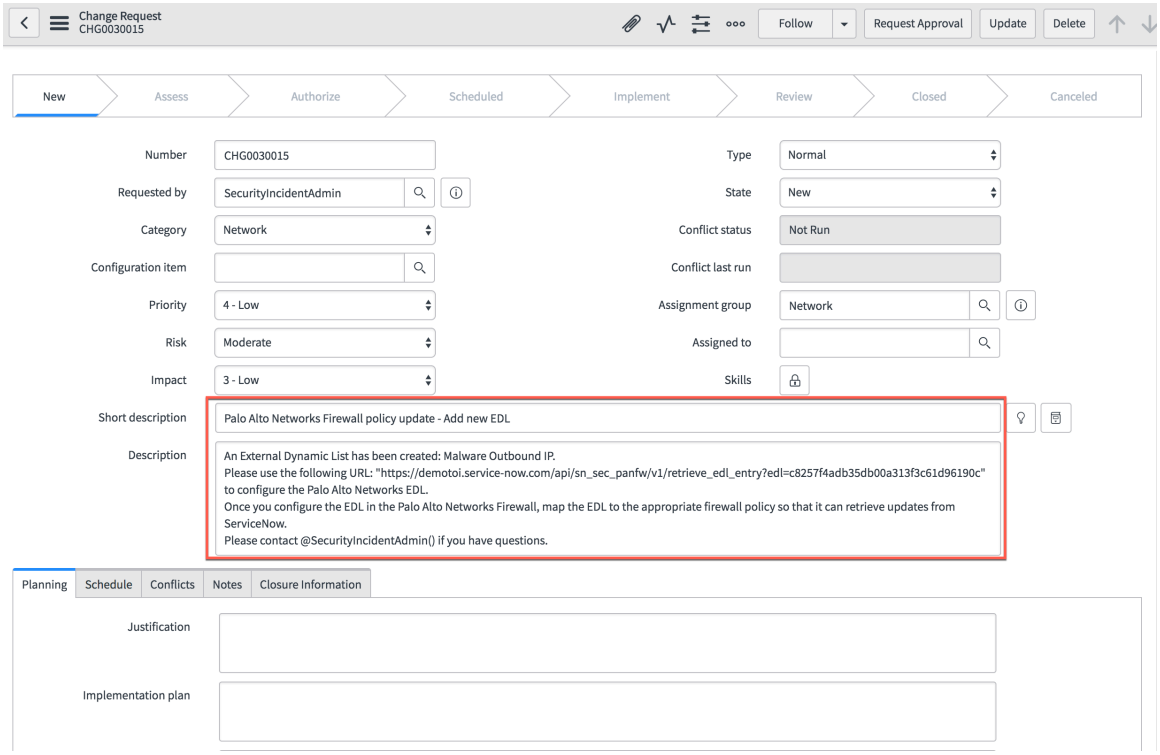


3. EDL レコードが開くので、[変更の要求] 関連リストの変更要求番号をクリックします。

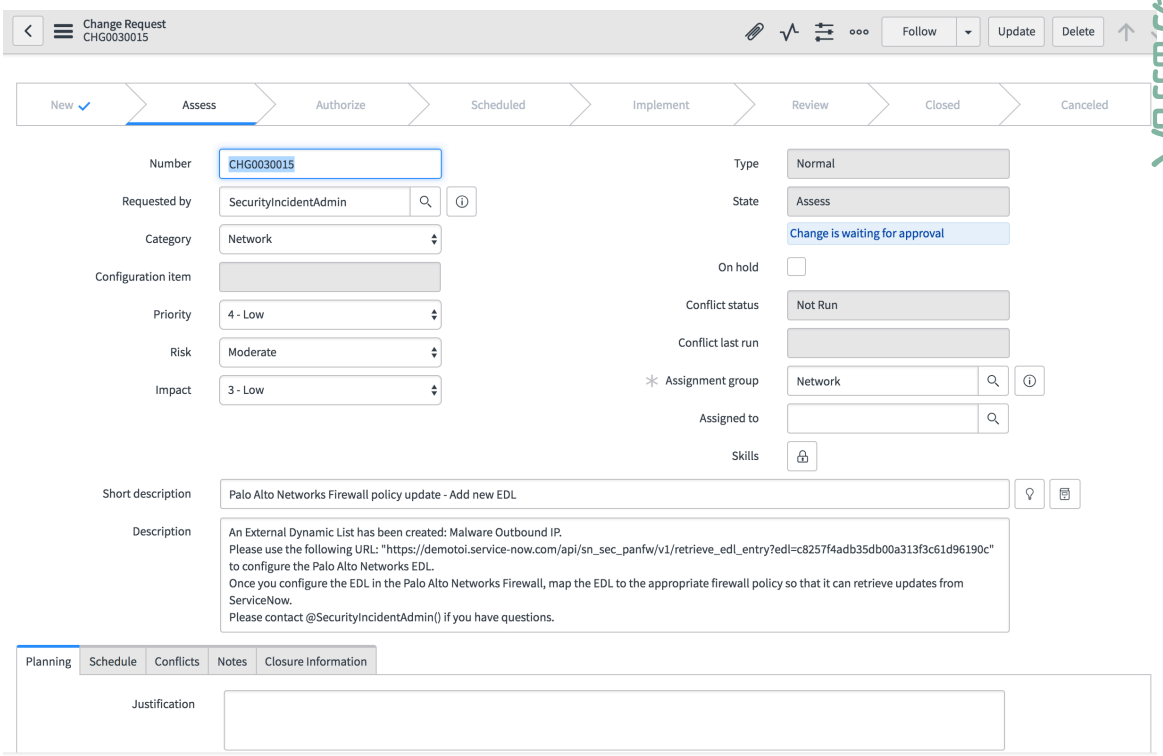


変更要求レコードが表示されます。[説明] フィールドには、Palo Alto Networks EDL の設定に使用する取得 URL が表示されます。EDL から適切な Palo Alto Networks Next-Generation Firewall ポリシーへのマッピングに関する詳細も含まれています。[簡単な説明] フィールドのコメントは、新しい EDL を追加する要求があることを示しています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. レコードの右上隅にある [承認要求] をクリックします。
[ステータス (State)] が [評価] に変わり、変更要求が承認待ちであることを示すメッセージが表示されます。

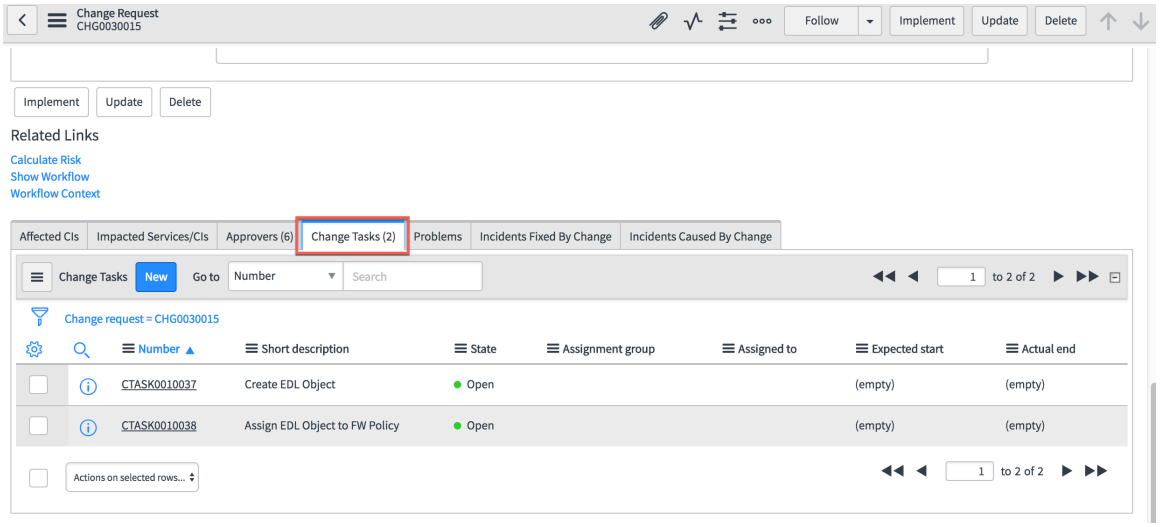


5. 変更要求を完了して EDL をアクティブ化するには、手順に従ってタスクをアサインし、変更要求をクローズします。

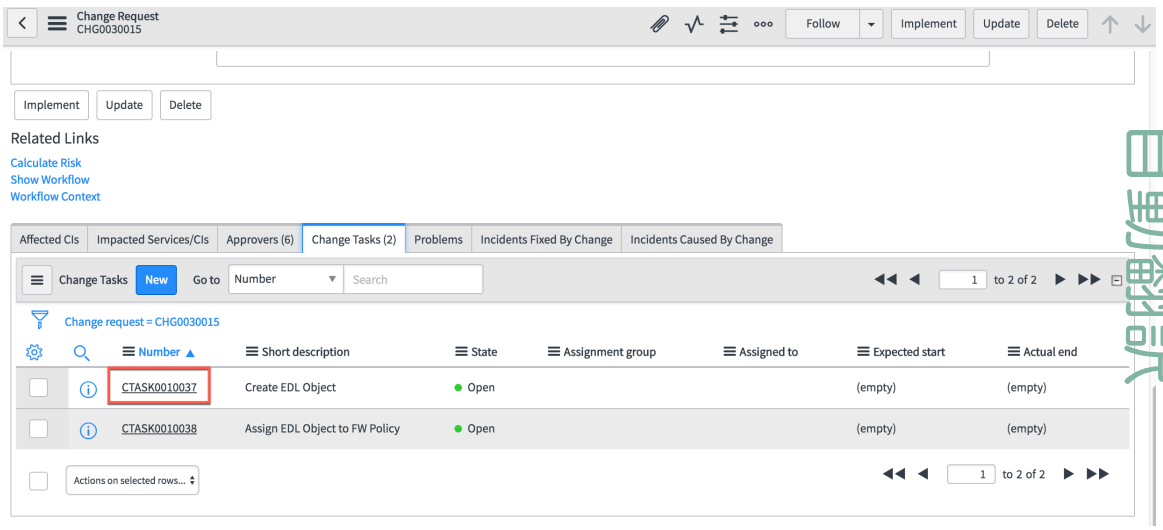
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. 表示されていない場合は、変更要求を開き、[変更タスク] タブを選択します。



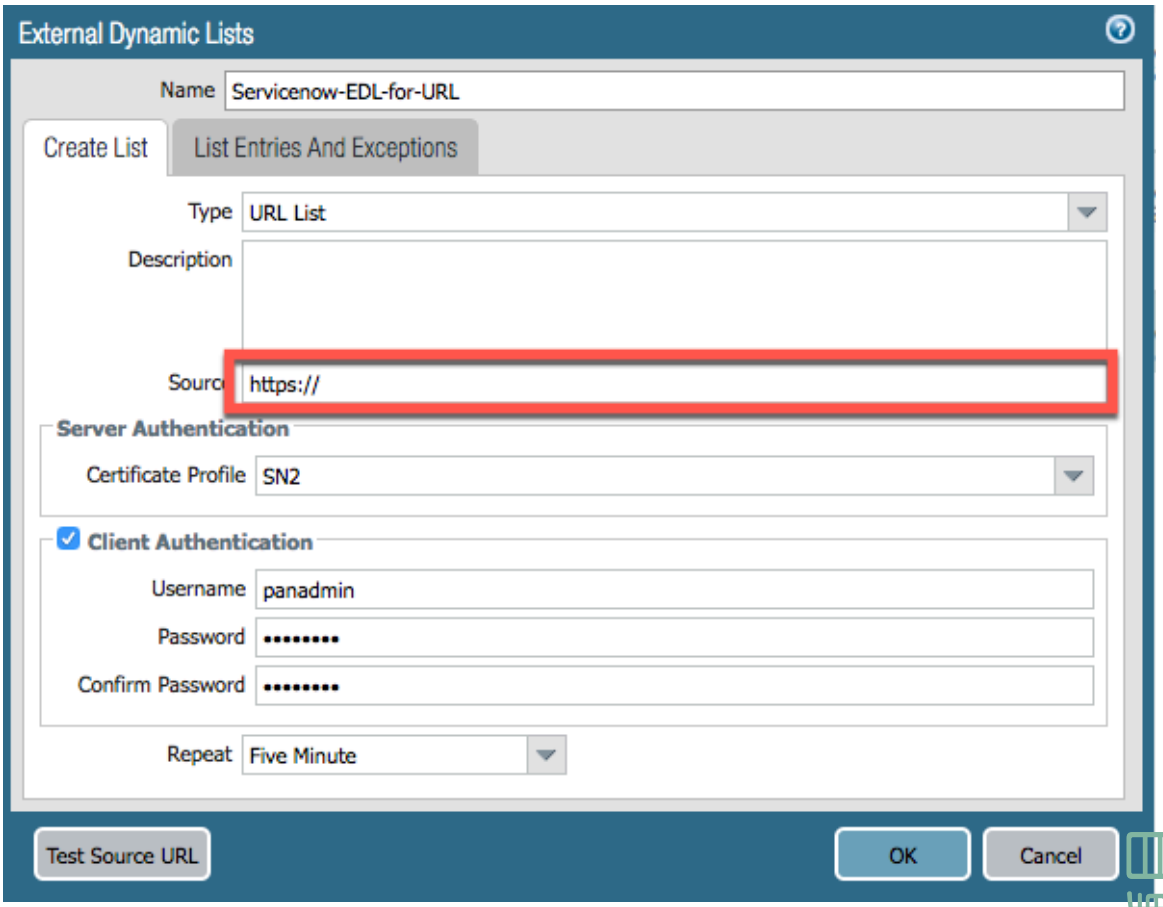
b. EDL オブジェクトの作成に関連付けられているタスクをクリックして開きます。



c. レコードが表示されるので、Palo Alto Networks ファイアウォールアドミニストレーターにタスクをアサインし、[更新] をクリックします。
ファイアウォールアドミニストレーターは通知を受け取り、Palo Alto Networks Next-Generation Firewallに EDL オブジェクトを作成します。

EDL オブジェクトを作成するために、 Now Platform 取得 URL が次の Palo Alto Networks にコピーされます 外部動的リスト > リストを作成 > ソース.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

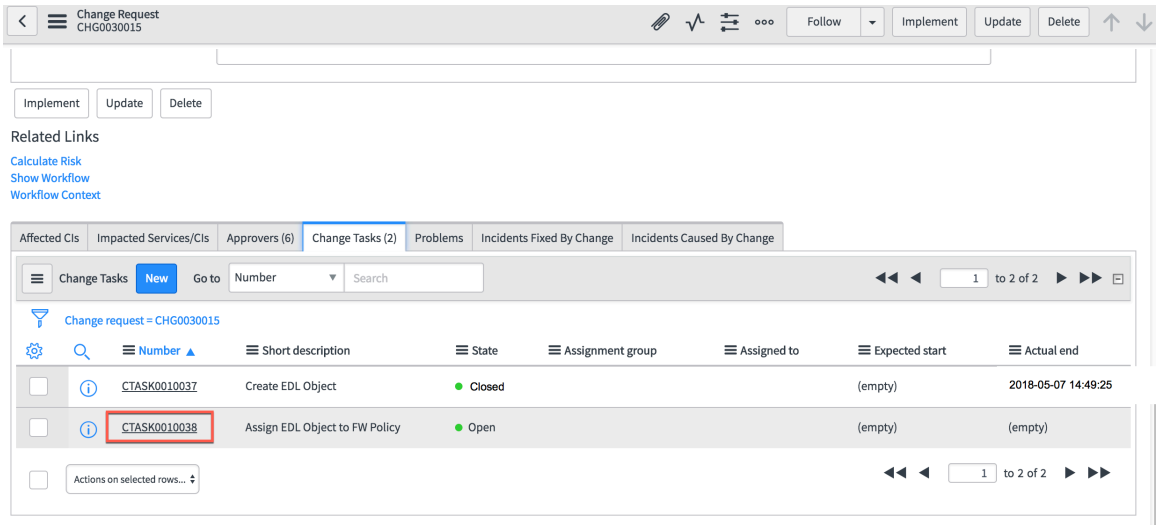


画像は特権のある専有物です。許可を得て使用しています。

d. Palo Alto Networksで EDL オブジェクトが作成されたことを確認したら、Now Platformで EDL オブジェクトの作成に関連付けられている変更要求に移動し、[タスクをクローズ] をクリックします。

この例のタスクレコードでは、このタスクに対して CTASK0010037 がクローズされました。

e. [変更タスク] タブに移動し、ファイアウォールポリシーを EDL オブジェクトに割り当てるためのタスクをクリックします。

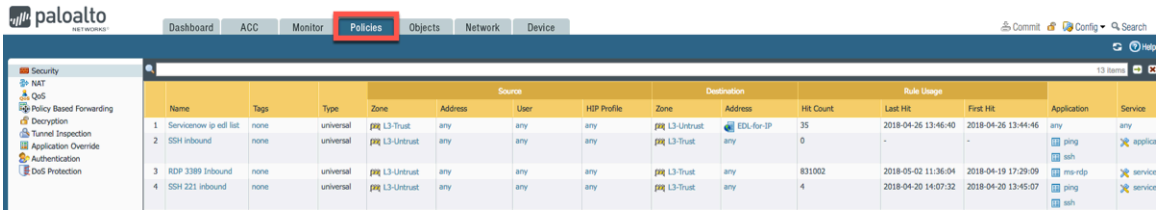


CTASK0010037 のステータスは [クローズ済み (Closed)] です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

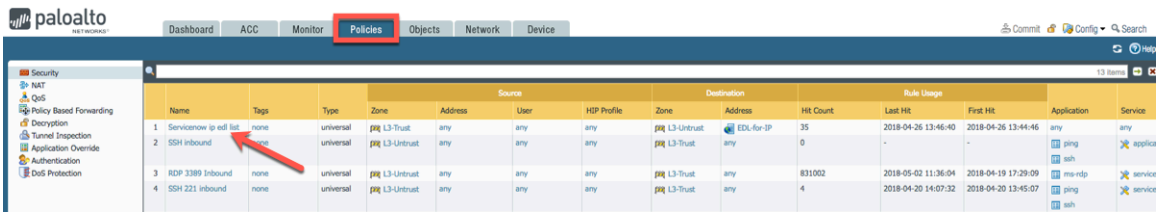
f. レコードを開き、次のタスクをアサインします。

タスクのアサイン後、ファイアウォールアドミニストレーターは、Palo Alto Networksで [ポリシー **(Policies)]** タブに移動してポリシーをアサインします。



画像は特権のある専有物です。許可を得て使用しています。

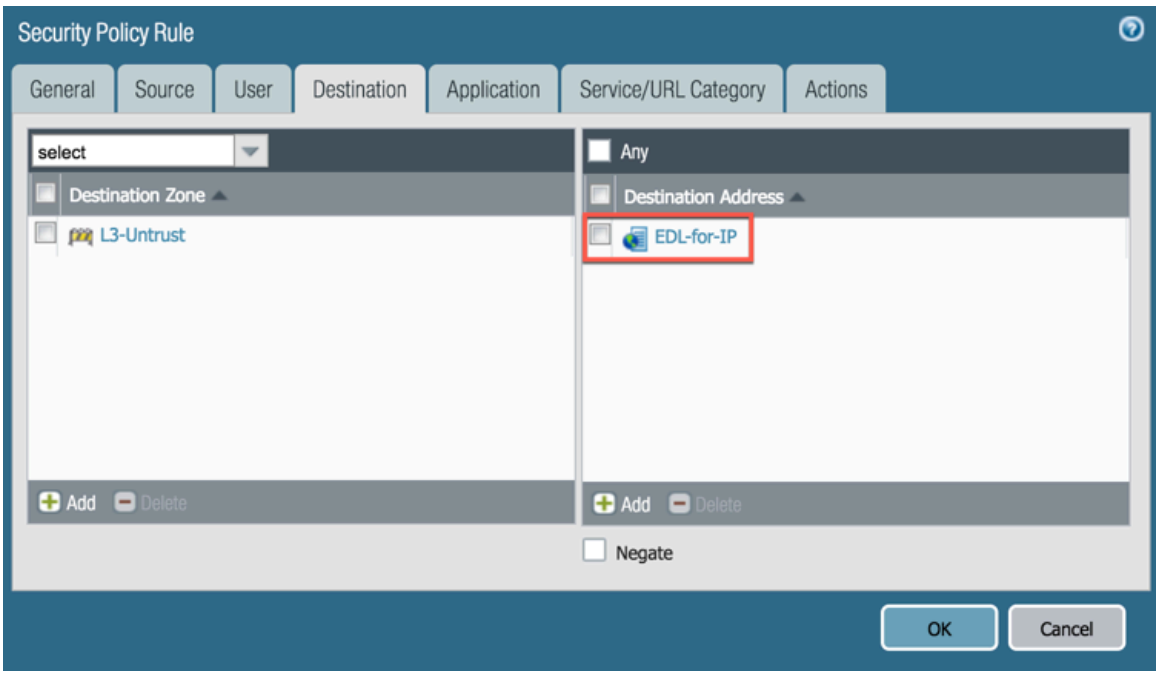
g. [名前 **(Name)]** 列で、EDL を追加したいセキュリティポリシールールを見つけてクリックします (例： **ServiceNow ip edl list**)。



画像は特権のある専有物です。許可を得て使用しています。

h. [Security Policy Rule (セキュリティポリシールール)] ダイアログボックスで、[宛先 **(Destination)]** タブを選択して [宛先アドレス **(Destination Address)]** フィールドに EDL を追加します。

i. 利用可能なすべての EDL を表示するには、 [追加 **(Add)]** アイコンをクリックします。



画像は特権のある専有物です。許可を得て使用しています。

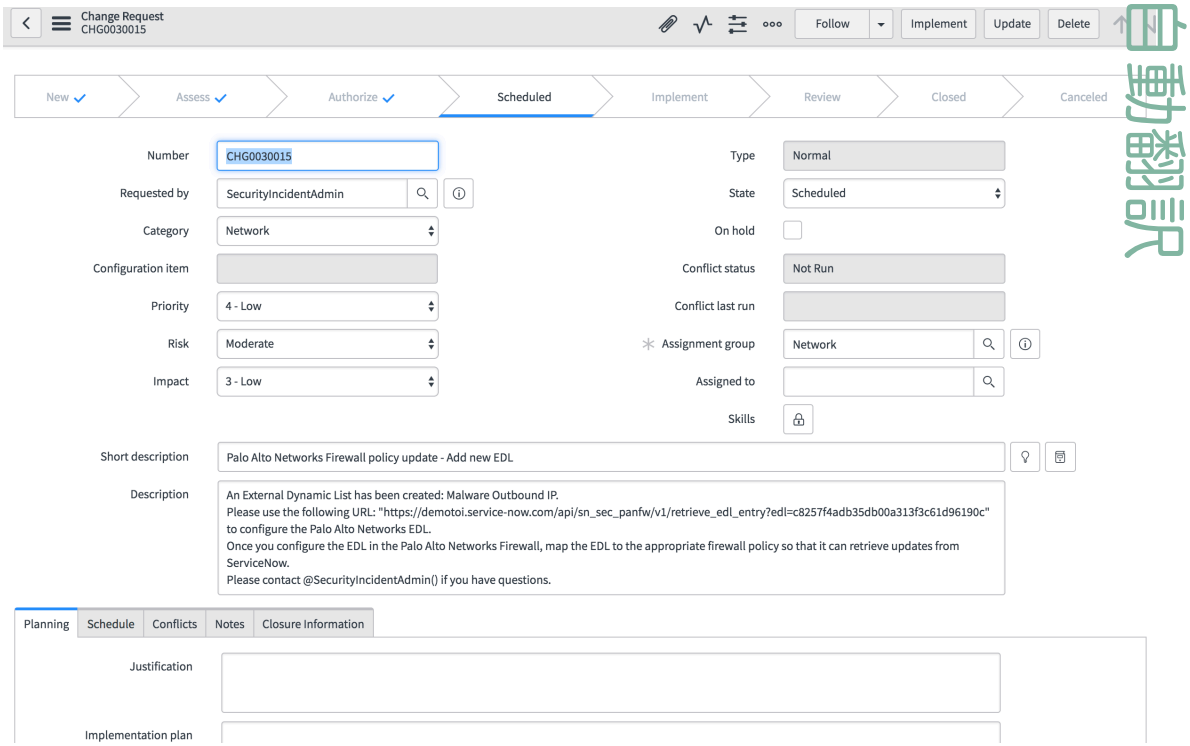
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

j. **[OK]** をクリックします。

k. Now Platformで EDL オブジェクトがセキュリティポリシーに割り当てられたことを確認したら、変更要求に移動し、EDL オブジェクトの割り当てに関連付けられているタスクを開いて、[タスクをクローズ] をクリックします。
タスクが両方ともクローズされれば、次は変更要求を承認できます。

l. 変更要求レコードで [承認者] 関連リストをクリックし、[ステータス **(State)]** 列のアイテムを選択して、EDL の作成に使用する要求を開きます。

m. 承認要求フォームが開くので、[承認] をクリックします。
変更要求状況が [予約済み] に移行されます。

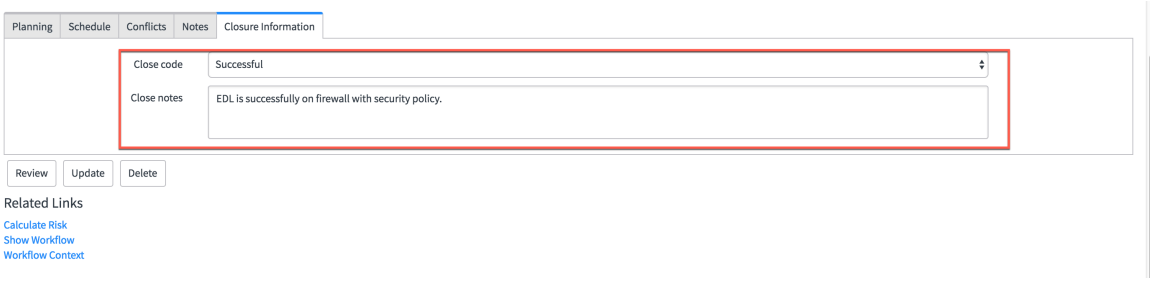


n. [実装] をクリックします。

o. [クローズ情報] 関連タブをクリックし、メモを入力して要求をクローズします。

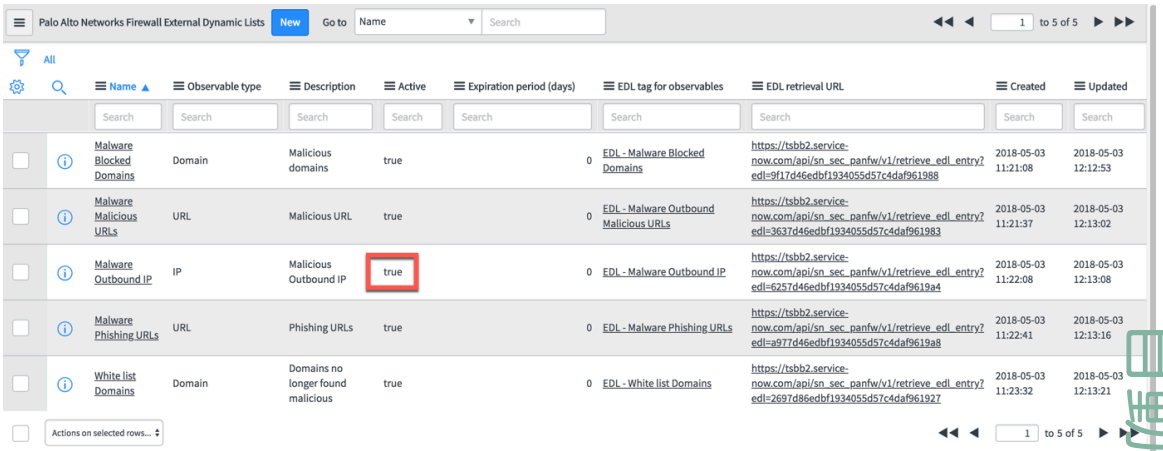
変更要求をクローズするには、このフィールドに入力する必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

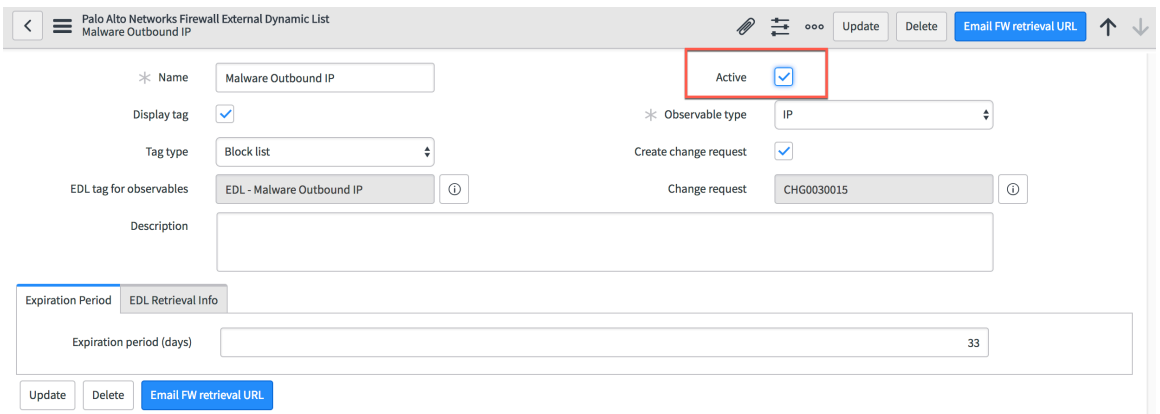


変更要求がクローズすると、EDL は自動的に有効になります。EDL がアクティブになっていることを確認していない場合は、 **Palo Alto Networks NGFW** 統合 > ファイアウォール **EDL** 構成.

リストの [アクティブ] 列で、EDL のステータスが (true) であることを確認します。



[名前] 列で EDL 名をクリックし、開いているレコードで、[アクティブ] チェックボックスもオンになっていることを確認します。



これで EDL は EDL エントリーを受け入れることができます。

次のタスク
セキュリティインシデントまたはブロックリストから EDL エントリーを送信します。

Palo Alto Networks Next-Generation Firewall のセキュリティインシデントレコードから **EDL** エントリーを送信する

セキュリティインシデントレコードに添付された観測事象は、承認のために外部動的リスト (EDL) エントリーとして EDL に送信されます。EDL エントリーの承認プロセスは、事前設定済みのワーク

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

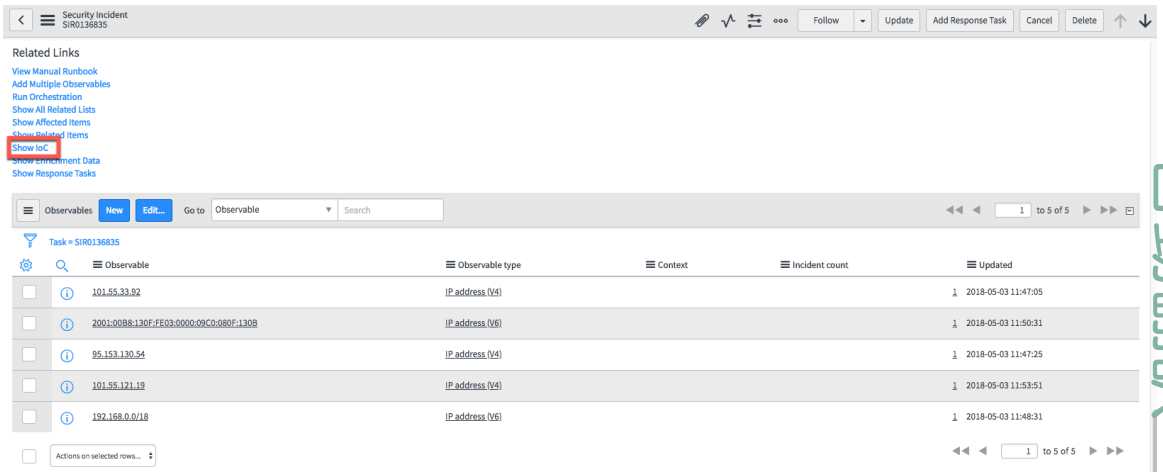
フローの一部です。ファイアウォールは、EDL リストに含まれている EDL エントリー (IP アドレス、URL、ドメイン) をインポートし、ポリシーを適用します。

始める前に
必要なロール：EDL エントリーを送信するための sn_si.analyst。EDL エントリーの承認：承認は、デフォルトで sn_si.admin にアサインされますが、この権限は組織の必要に応じて割り当てることができます。

このタスクについて
sn_si.analyst ロールを持つユーザーは、セキュリティインシデントレコードに添付された観測事象のブロックを要求することで、EDL エントリーを送信します。送信後、ステータスが [処理待ち (Pending)] の EDL エントリーが生成され、承認のために送信されます。次の例は、URL 観測事象のブロック要求を示しています。

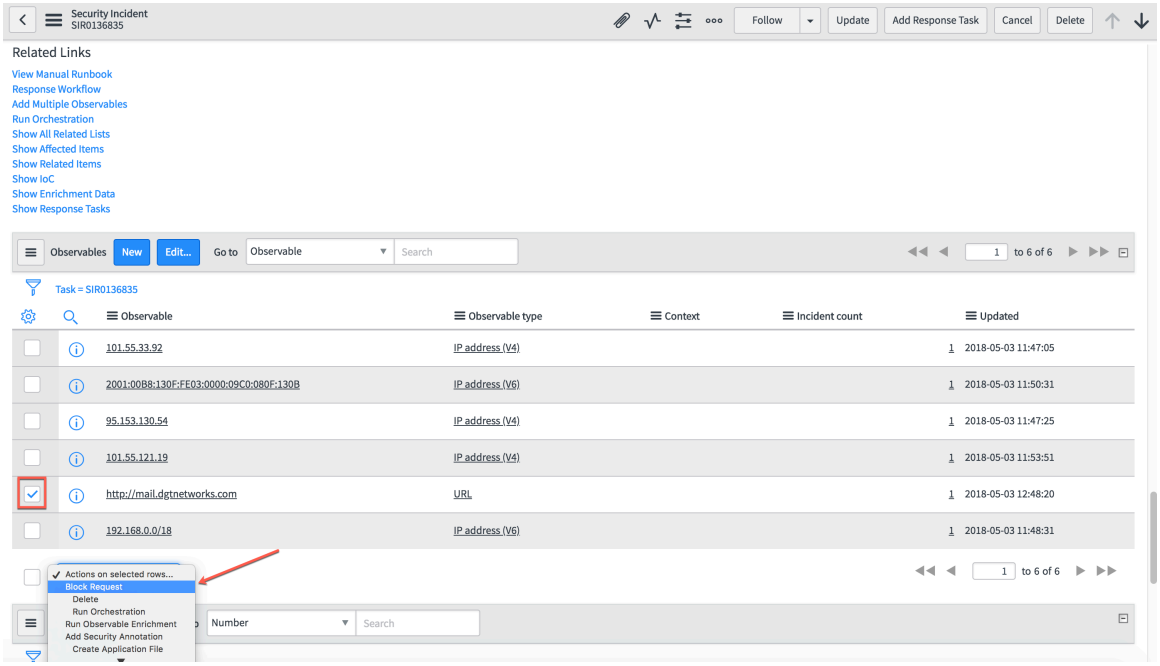
手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデント > すべてのインシデントを表示をクリックし、セキュリティインシデントレコードをクリックして開きます。
2. **[IoC** を表示] 関連リンクをクリックします。



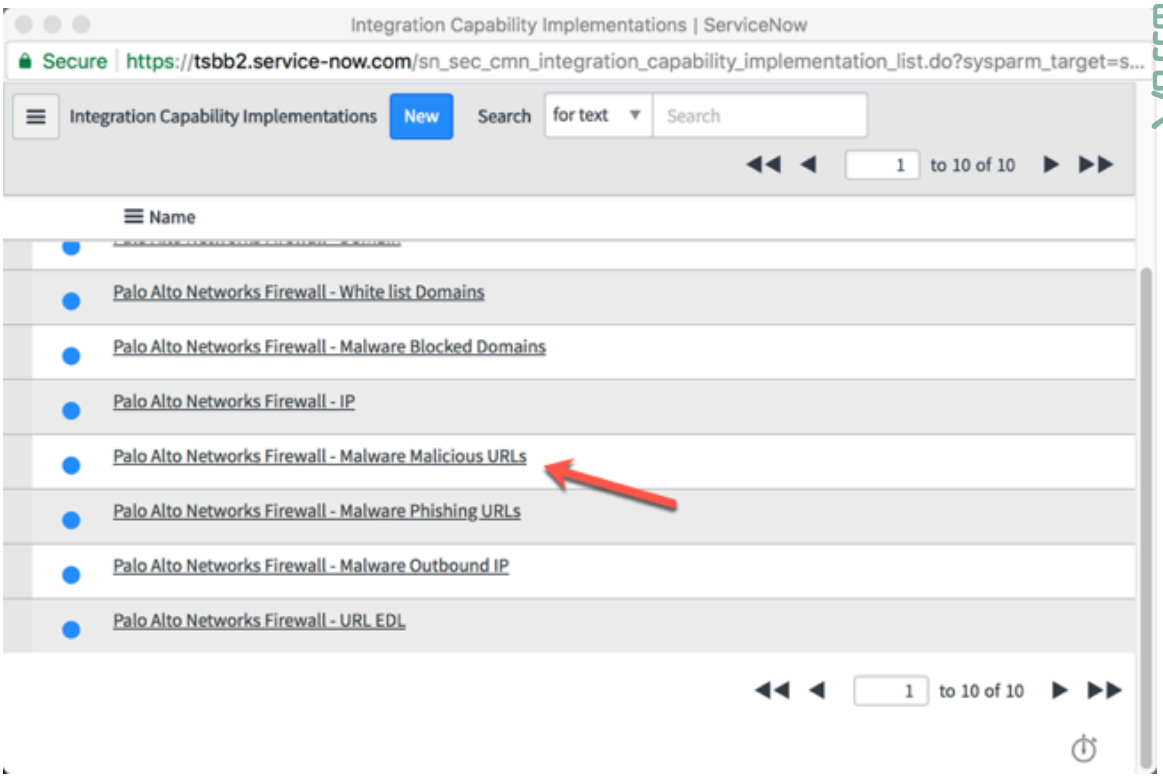
3. [観測事象 (Observables)] 関連リストでブロックする観測事象を選択し、[選択した行のアクション] リストから [ブロック要求] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. 表示されるダイアログボックスで、検索アイコン (🔍) をクリックします。
5. 表示されるリストで、このエントリーを添付する EDL を選択します。

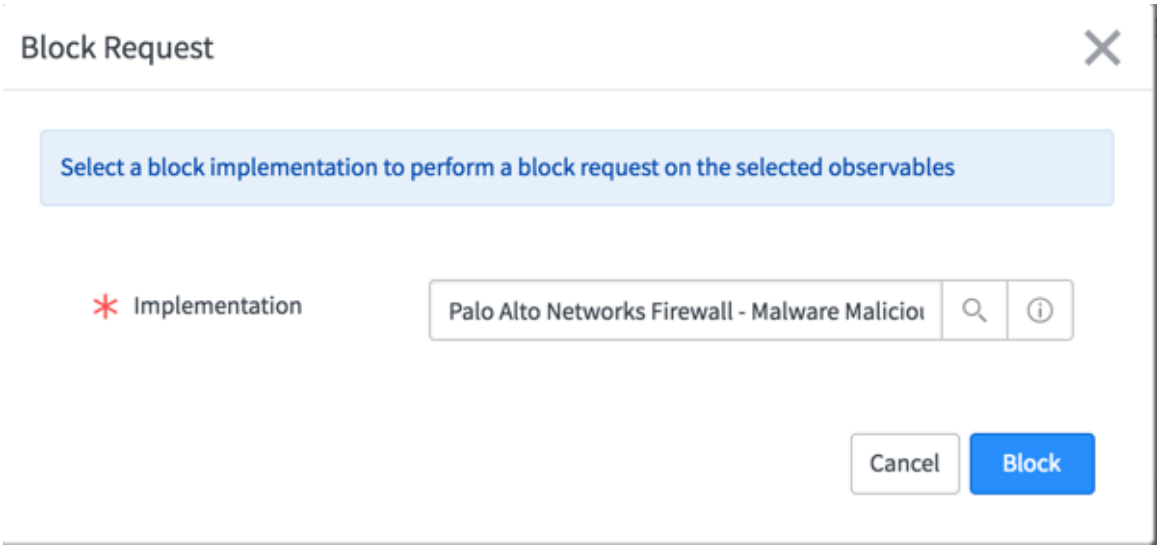
> **注:**
> この例では、エントリーの観測事象タイプ (URL) が EDL の観測事象タイプ (URL) と一致している必要があります。



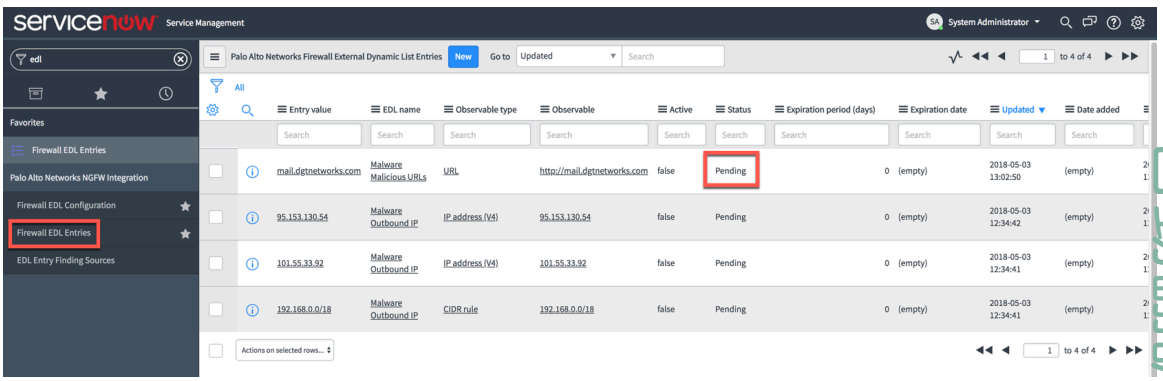
6. [ブロック要求] ダイアログボックスで EDL 名が [実装] フィールドに表示されている状態で、[ブロック] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

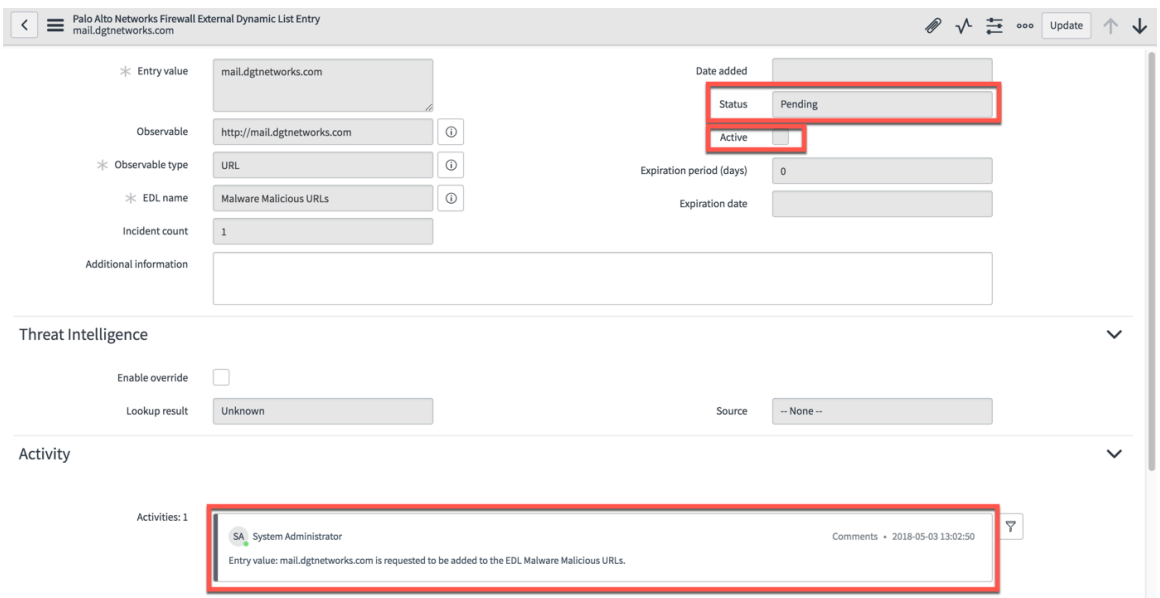


7. 次のように移動する。 **Palo Alto Networks NGFW** 統合 > ファイアウォール **EDL** エントリー をクリックし、[ファイアウォール **EDL** エントリー] をクリックします。



8. [Palo Alto Networks ファイアウォール外部動的リストエントリー] リストで、[エントリー値] 列の観測事象をクリックしてレコードを開きます。

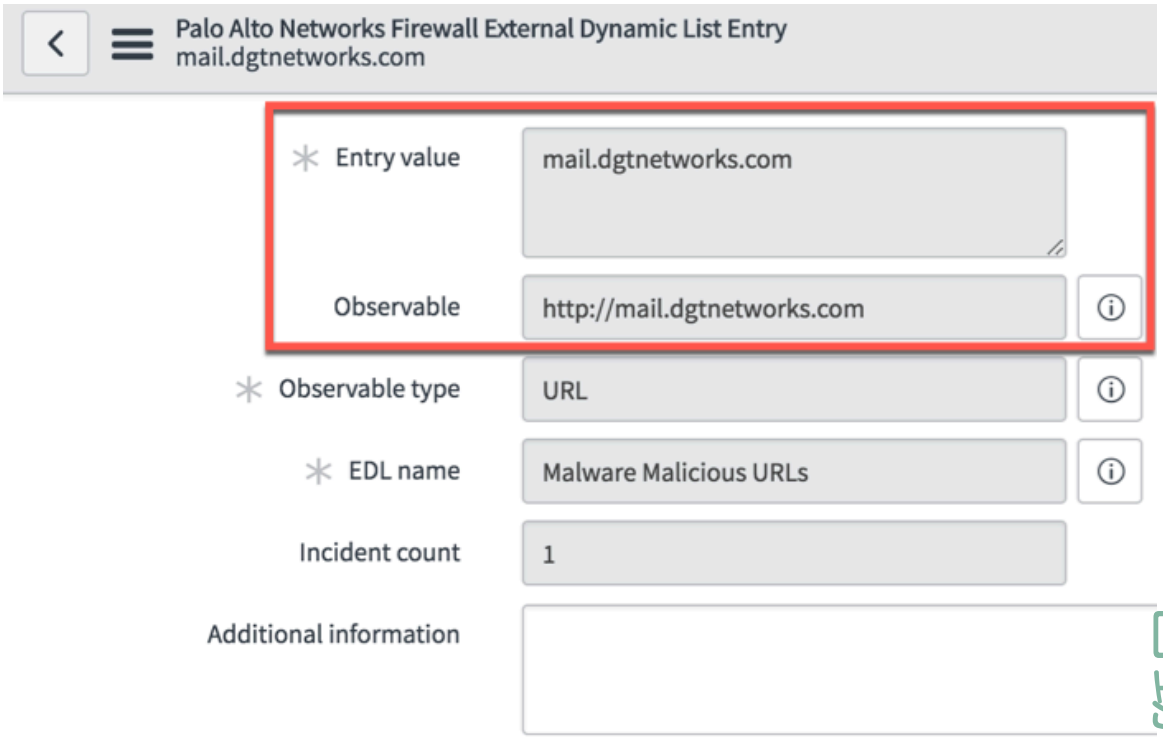
   この例では、**mail.dgtnetworks.com** のレコードが表示されています。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ステータスが [処理待ち] で、 [アクティブ] チェックボックスがオフになり、作業メモに観測事象を追加する要求があることが示されます。この EDL エントリー要求は承認の準備ができています。

[エントリー値] フィールドと [観測事象 (Observable)] フィールドには、URL 観測事象が異なる形式で表示されます。



[観測事象 (Observable)] フィールドの横にあるアイコンは、Now Platform® の [観測事象 (Observable)] テーブルへのリンクです。

[観測事象 (Observable)] フィールドの値 (http://mail.dgtnetworks.com) が [観測事象 (Observable)] テーブルにリンクされ、セキュリティインシデントレスポンス のインシデントトリガーイベントから引き継がれた形式と照合されます。

Now Platform® が、 Palo Alto Networks の EDL URL 形式と互換性があるように EDL エントリーを自動的に修正する場合があります。

この例では、観測事象は http:// プロトコル (http://mail.dgtnetworks.com) で作成され、この形式が [観測事象 (Observable)] フィールドに表示されています。http:// プロトコルは、Palo Alto Networks との互換性を確保し、 取得できるように、Now Platform® によって観測事象から自動的に削除されます。その結果、[エントリー値] フィールドには、mail.dgtnetworks.com と表示されています。

次のタスク
EDL エントリーを承認します。

関連情報

Palo Alto Networks Next-Generation Firewall の EDL エントリーの例外

Palo Alto Networks Next-Generation Firewall のブロックリストから **EDL** エントリーを送信する

悪意があると判断され、特定の Now Platform セキュリティインシデントに関連付けられていない観測事象の場合は、ブロックリストから外部動的リスト (EDL) エントリーを送信します。

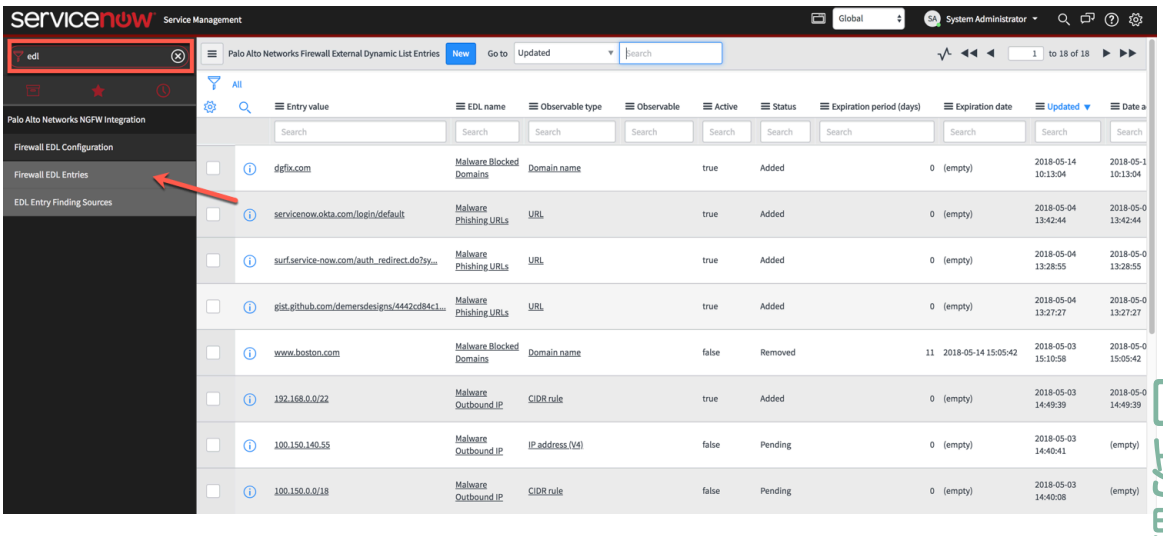
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_si.analyst

このタスクについて
悪意があると判断した観測事象をブロックしたり、悪意がないと判断した観測事象を許可したりしたいときに、その観測事象が特定の Now Platform セキュリティインシデントレコードに関連付けられていない場合は、ブロックリストから EDL エントリーを直接送信します。これらのタイプの EDL エントリーの例として、特定のサイトの URL やドメインが挙げられます。

手順

1. 次のように移動する。 **All** (すべて) > **Palo Alto Networks NGFW** 統合 > ファイアウォール **EDL** エントリー.



2. [ファイアウォール **EDL** エントリー] モジュールをクリックします。
3. [Palo Alto Networks ファイアウォール外部動的リストエントリー] リストで、[新規] をクリックします。
4. 表示される新しいレコードで、[エントリー値] フィールドに、観測事象の値を入力します。
この入力で考えられる結果は 2 つあります。

   フォームの残りのフィールドがすべて自動入力されます。

   一致する観測事象が見つかり、一致する観測事象が存在することを示すメッセージが表示されます。このエントリーを添付する EDL を選択し、[送信] をクリックします。有効期間を設定する前に、このエントリーを添付する EDL を選択します。

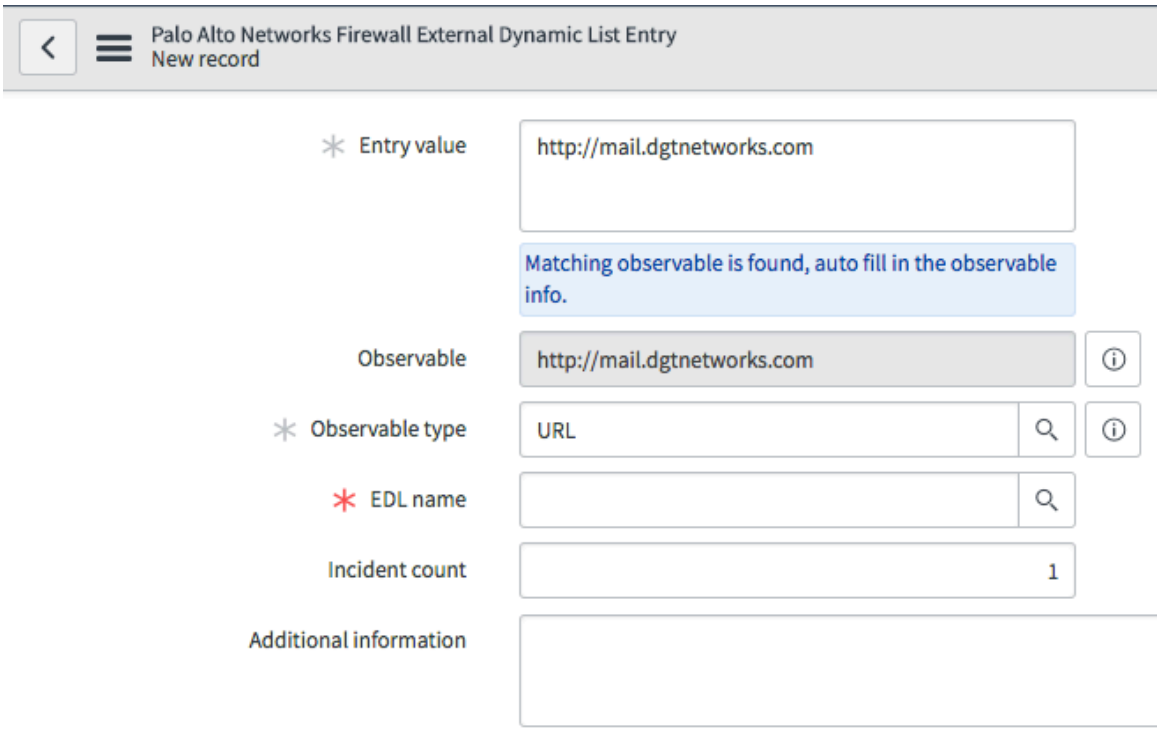
   フォームに入力するように指示するメッセージが表示されます。

   一致する観測事象が見つかりません。フォームに入力する必要があります。完了したら、観測事象を添付する EDL を選択し、[送信] をクリックします。観測事象レコードが作成されます。

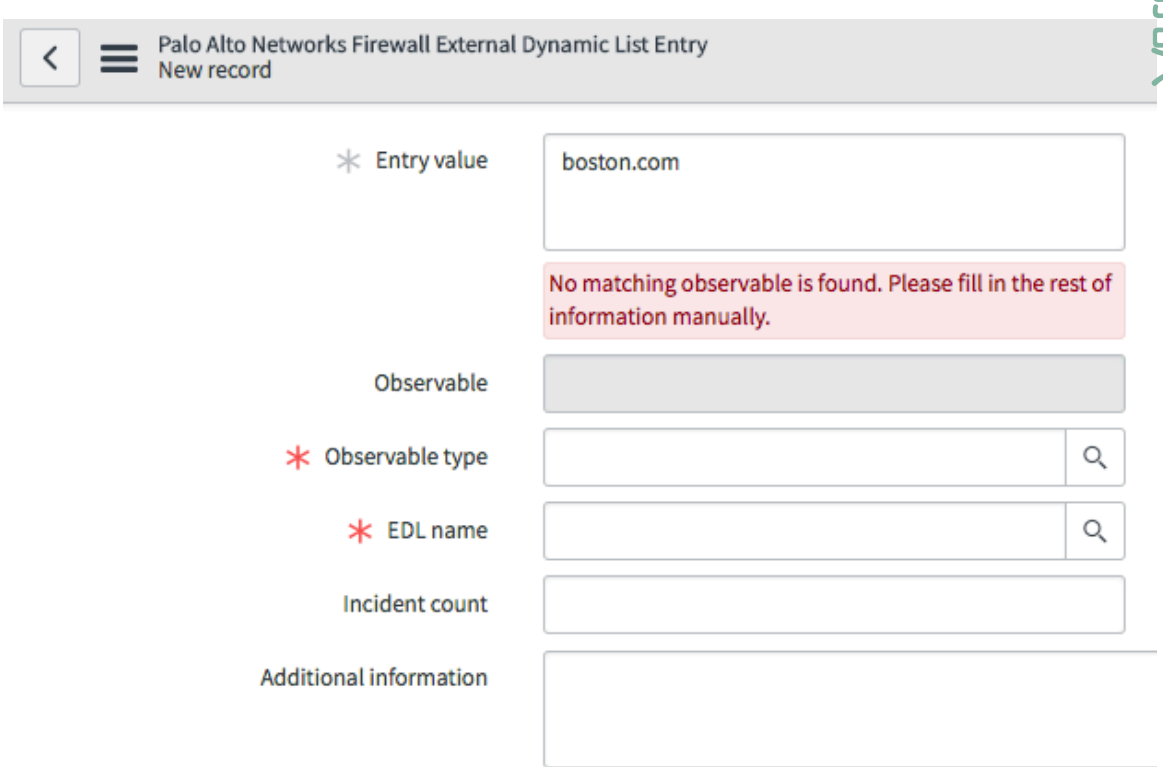
   次の図は、既存のドメイン観測事象の例と、フィールドがどのように自動入力されるかを示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



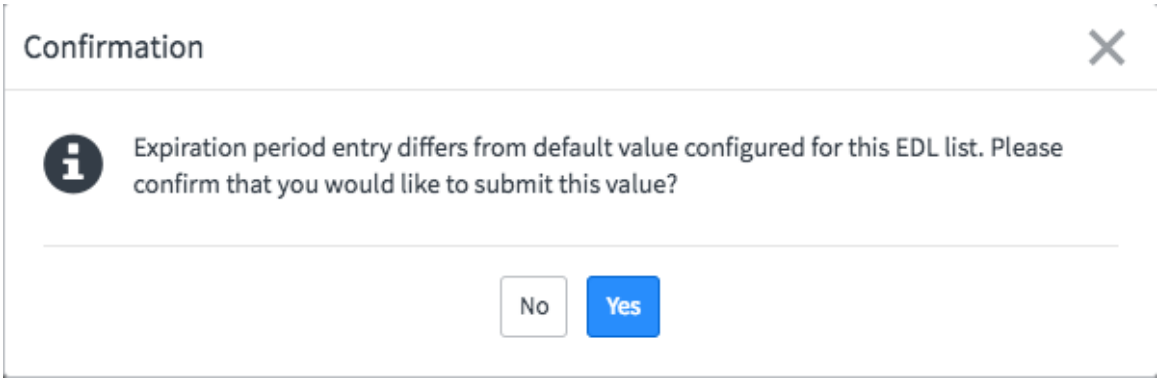
5. 検索アイコンをクリックして、エントリーを添付する EDL を選択します。
6. **[Submit]** をクリックします。
   ワークフローでメール承認が設定されている場合は、承認メール要求が送信されます。
7. 残りの情報を手動で入力するように要求するメッセージが表示された場合は、フィールドに入力します。



自動翻訳

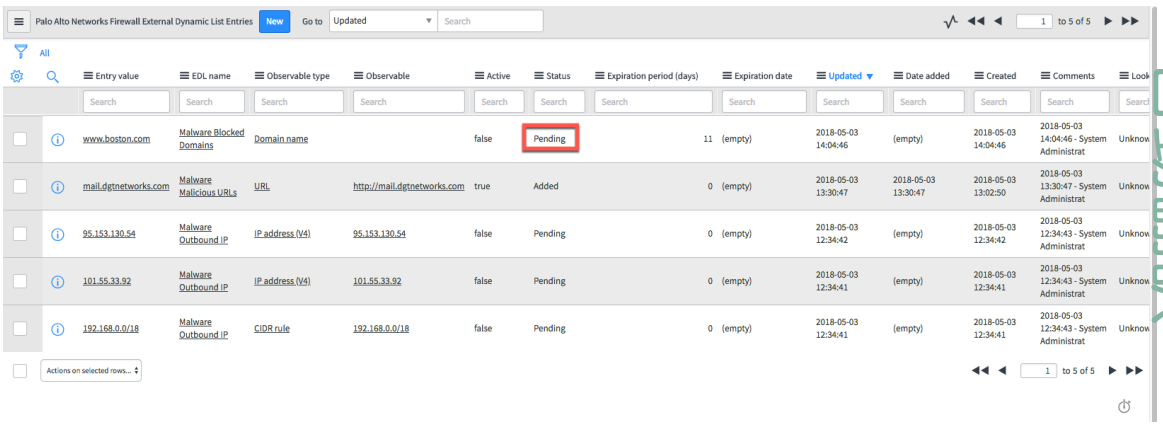
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

8. **[Submit]** をクリックします。
   EDL エントリーのデフォルトの有効期間を変更した場合は、期間が選択した EDL と異なることを示す警告確認ダイアログボックスが表示されます。



9. 有効期間を設定するオプションを 1 つ選択します。

10. 表示されない場合は、**[Palo Alto Networks** ファイアウォール外部動的リストエントリー] リストに移動して、エントリーのステータスが [処理待ち (Pending)] であることを確認します。



これで、エントリーを承認する準備ができました。

次のタスク
EDL エントリーを承認します。

関連情報

Palo Alto Networks Next-Generation Firewall の EDL エントリーの例外

Palo Alto Networks Next-Generation Firewall の EDL エントリーの承認

外部動的リスト (EDL) エントリーの承認プロセスは、事前設定済みのワークフローの一部です。EDL エントリーは、EDL でアクティブ化される前に承認します。EDL エントリーを承認すると、ファイアウォールがそのエントリーを取得し、以降は観測事象がブロックされるようになります。

始める前に
必要なロール：EDL エントリーの承認は、デフォルトで sn_si.admin にアサインされますが、この権限は組織の必要に応じて割り当てることができます。次の例では、Now Platform アドミニストレーターが承認権限を持っています。

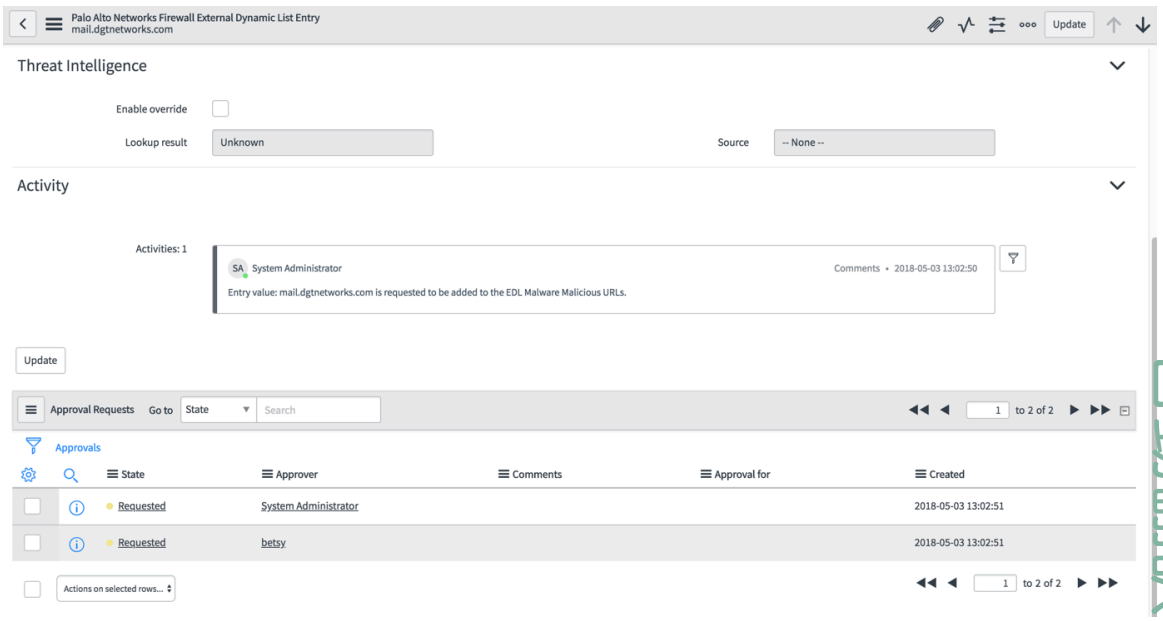
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
承認プロセスが有効になっている場合、EDL エントリーは承認されるまで EDL でアクティブ化または非アクティブ化されません。

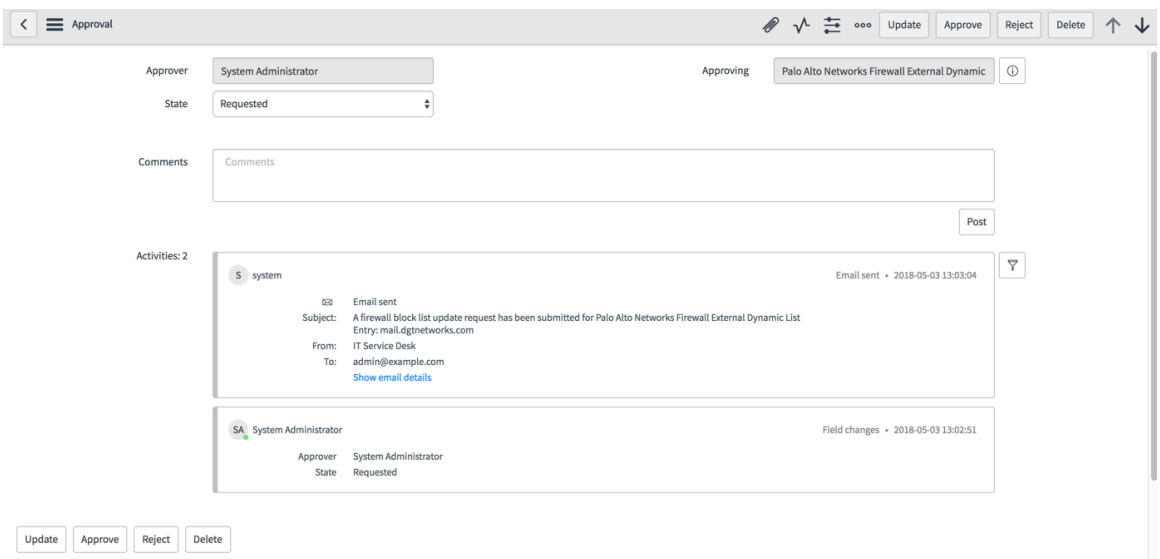
手順

1. 次のように移動する。 **All** (すべて) > **Palo Alto Networks NGFW** 統合 > ファイアウォール **EDL** エントリー をクリックし、EDL レコードを開きます。
2. EDL レコードで、[承認要求] セクションまでスクロールします。

   注:
   [システムの設定] で [タブ付きフォーム] を選択している場合、このセクションはレコードにタブとして表示されます。



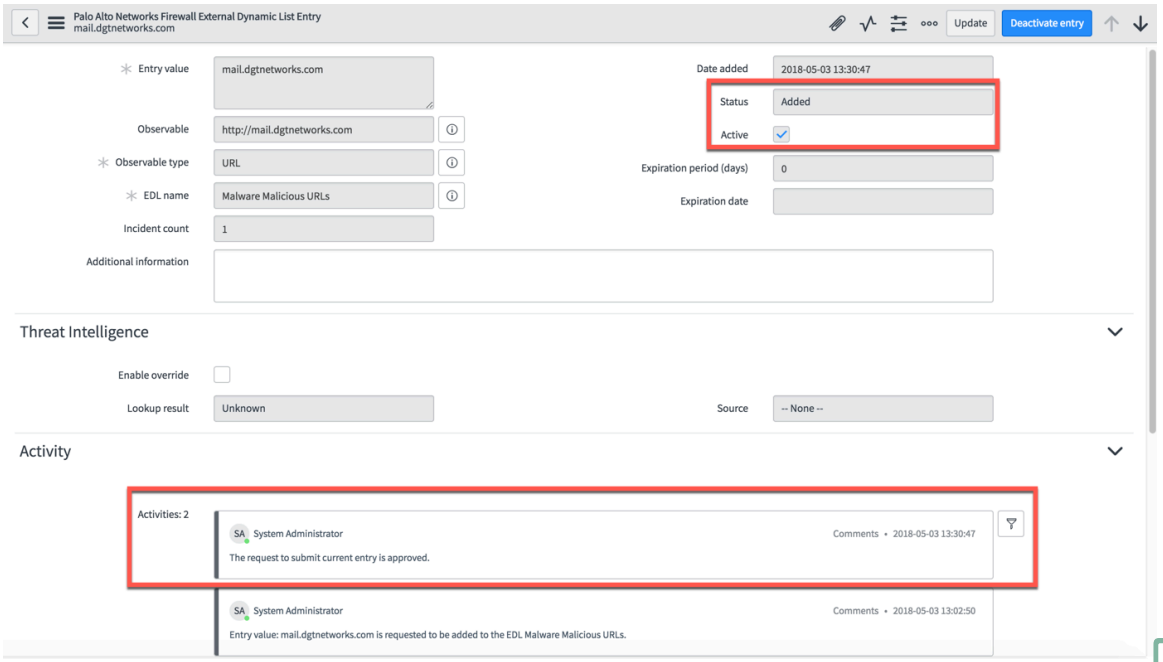
3. [承認要求] で、[ステータス] 列のアイテムをクリックして開きます。
   承認要求が表示されます。



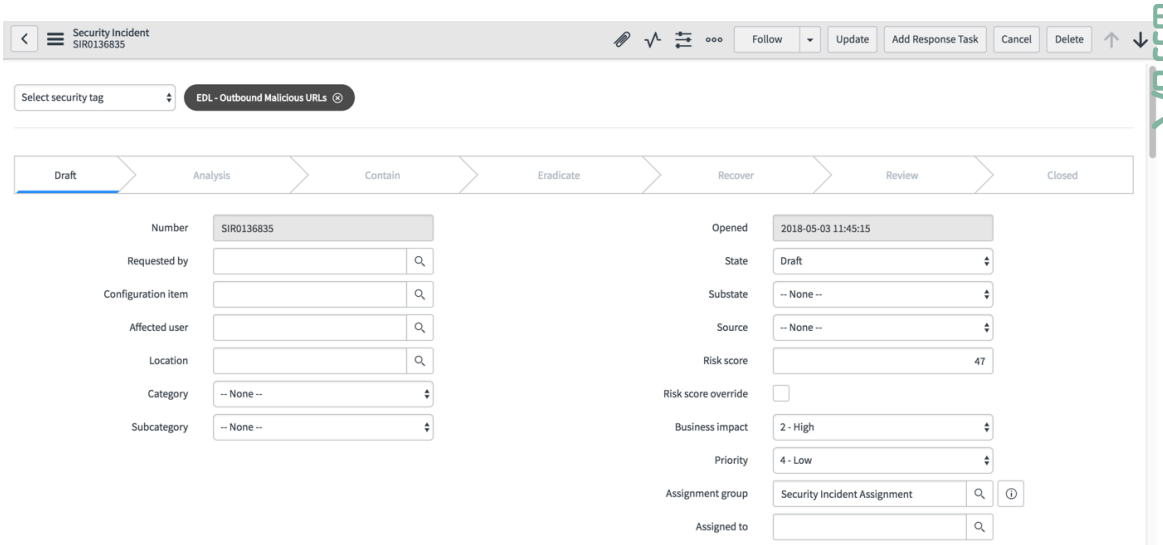
4. EDL エントリーを承認するためのオプションを 1 つ選択してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

EDL エントリーを承認し、エントリーがアクティブになると、Palo Alto Networks Next-Generation Firewall は、次の取得間隔の後に EDL エントリーを取得します。エントリーが取得されると、その時点から観測事象がブロックされます。次の図では、[アクティブ] チェックボックスがオンで、ステータスが [追加] になっており、作業メモに要求が承認されたことが示されています。

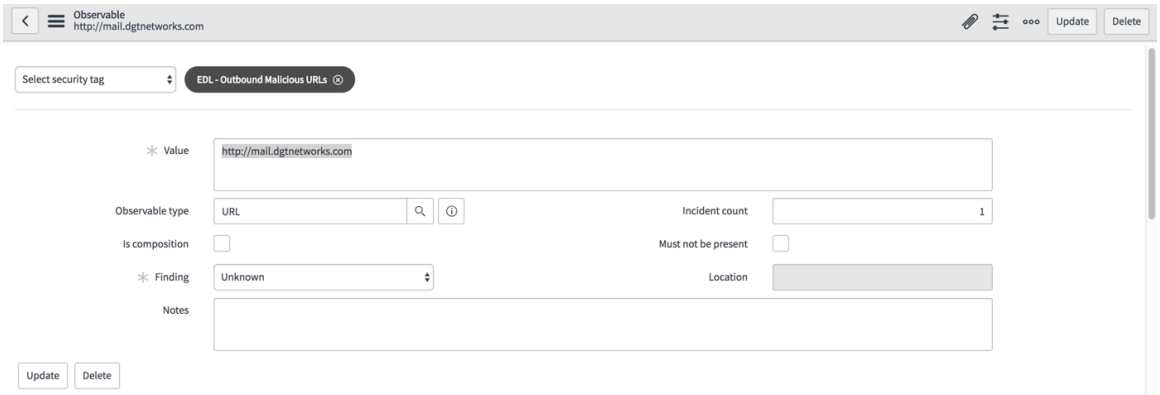


EDL エントリーが承認されてアクティブ化されると、セキュリティインシデントレコードがセキュリティタグでマークされます。タグはレコードの上部に表示されます。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティタグは観測事象レコードにも表示されます。



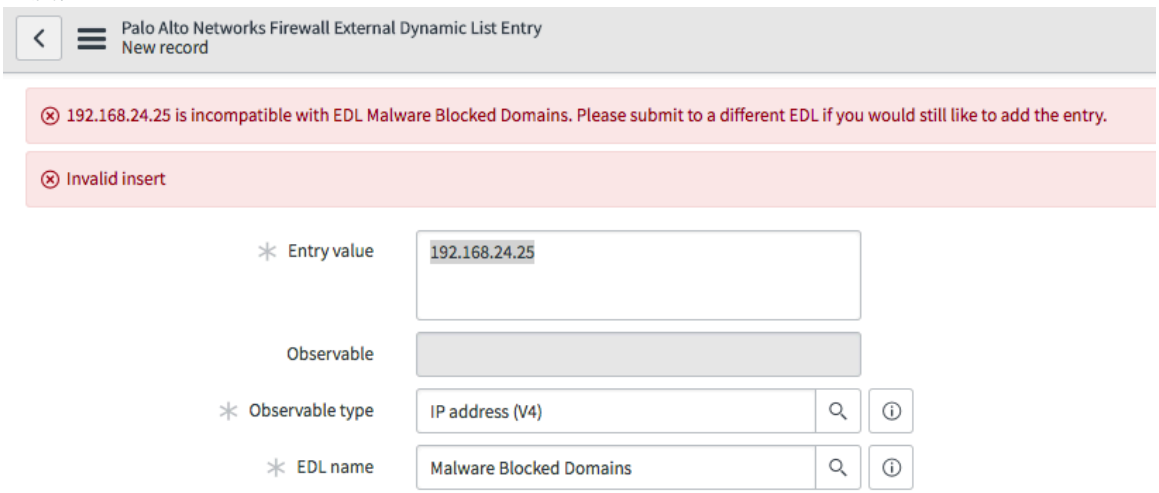
Palo Alto Networks Next-Generation Firewall の EDL エントリーの例外

外部動的リスト (EDL) エントリーの EDL への追加には制限があります。EDL エントリーを EDL に追加しようとしたときに、重複、互換性、または CIDR (クラスレスドメイン間ルーティング) の競合が見つかった場合、エラーの解決に役立つエラーメッセージが表示されます。

互換性の例外

各 EDL は、観測事象タイプに互換性のあるエントリーのみを受け付けます。ドメイン EDL を作成して、IP アドレスの観測事象を添付しようとすると、非互換性エラーメッセージが表示されます。たとえば、次の図に示すように、ドメイン EDL はドメイン観測事象のみを受け付けます。

互換性エラー



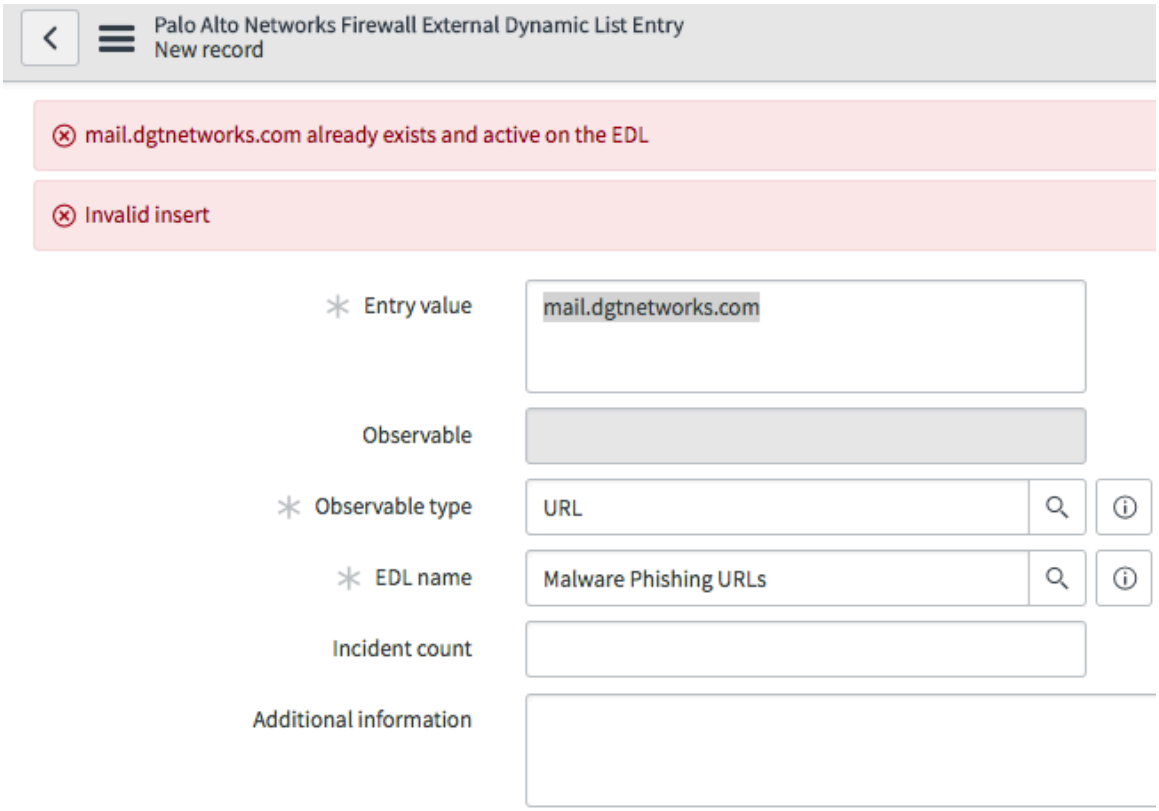
重複の例外

1 つの観測事象を観測事象タイプが同じ複数の EDL でアクティブ化することはできません。ある URL 観測事象がある URL EDL ですでにアクティブ化されている場合、同じ観測事象をフィッシング URL EDL でアクティブ化しようとすると、重複エラーメッセージが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重複エラー



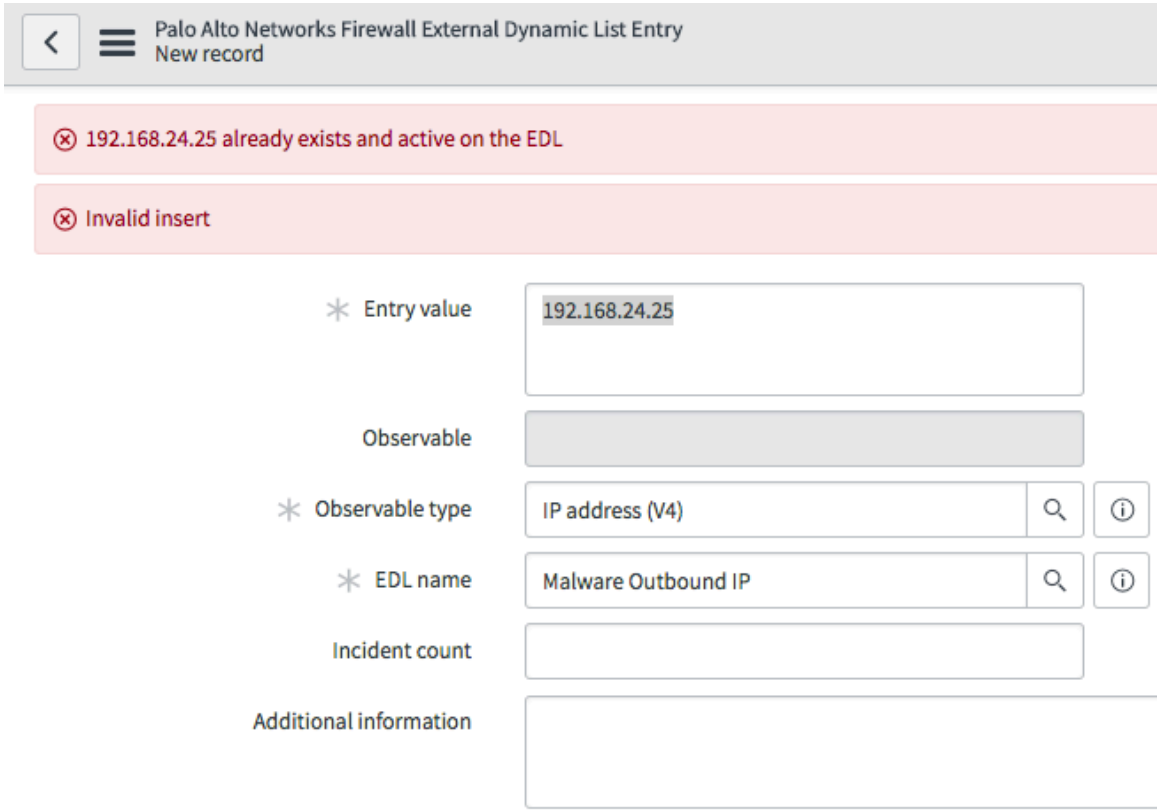
CIDR (クラスレスドメイン間ルーティング) の例外

単一の IP アドレスを EDL に添付しようとしたときに、その IP アドレスがすでに EDL 上にある CIDR 観測事象の一部であった場合は、CIDR 競合エラーが表示されます。このエラーは、単一の IP アドレスが CIDR 観測事象の一部としてすでに EDL に含まれていることを示します。たとえば、192.168.24.25 は CIDR ブロック 192.168.0.0/22 の一部です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CIDR の競合



(オプション) **Palo Alto Networks Next-Generation Firewall** のセキュリティタグ名の編集

外部動的リスト (EDL) レコードの作成時に [タグを表示] チェックボックスがオンになっている場合は、セキュリティタグのタグ名と色を編集できます。セキュリティタグは、すでにブロックされている観測事象を追跡するのに役立ちます。

始める前に
必要なロール：sn_si.admin

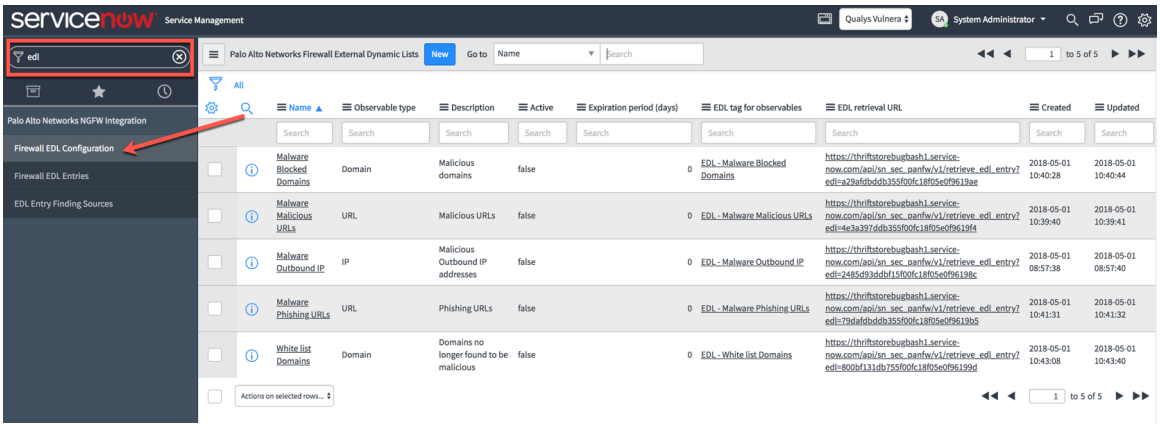
このタスクについて
セキュリティタグは、どのセキュリティインシデントのブロックリストに観測事象があるのかをすばやく識別するのに役立ちます。タグは、観測事象がすでにブロックされているかどうか、または EDL から削除されているかどうかを識別するのにも役立ちます。デフォルトでは、セキュリティタグの色は、ブロックリストエントリーの場合は黒、許可リストエントリーの場合はグレーです。特定のタグをより簡単に認識できるように、タグの名前と色を変更できます。

自動翻訳

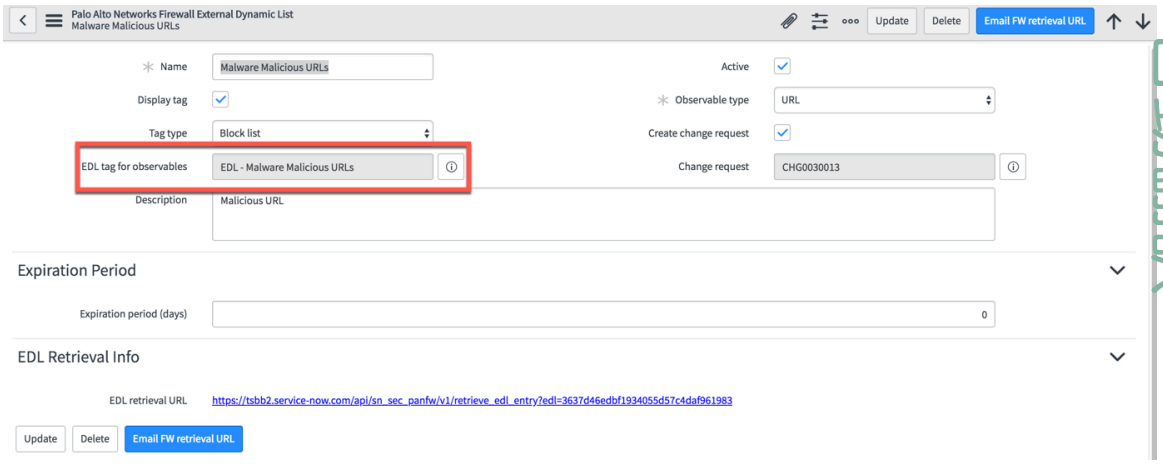
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

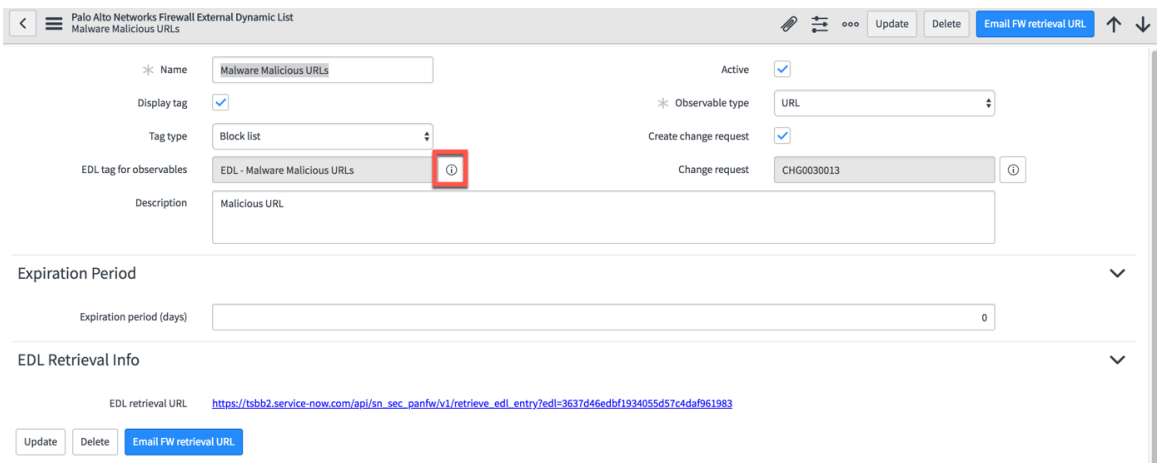
1. 次のように移動する。 **All** (すべて) > **Palo Alto Networks NGFW** 統合 > ファイアウォール **EDL** 構成.



2. [名前] 列でアイテムをクリックしてレコードを開きます。
EDL レコードが表示されます。デフォルトでは、セキュリティタグの名前は、EDL の作成時に [名前] フィールドに入力した値と同じです。デフォルトでは、名前には *EDL* プリフィックスも含まれます (例： EDL – Malware Malicious URLs)。

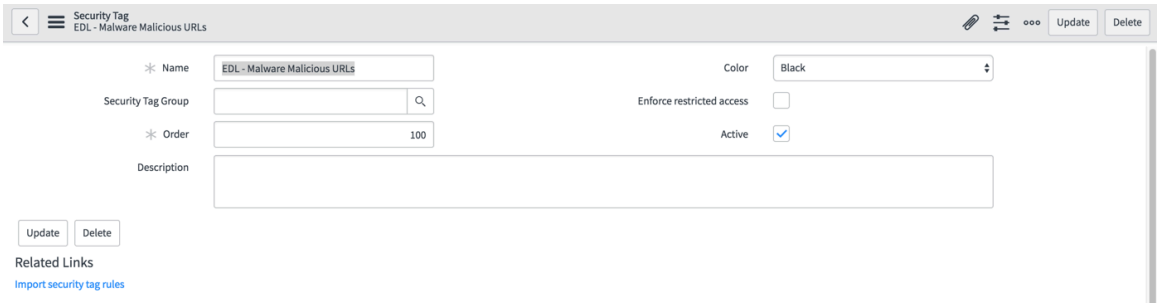


3. [観測事象の **EDL** タグ **(EDL tag for observables)]** の横の情報アイコン ( ) をクリックしてから、[レコードを開く] をクリックします。

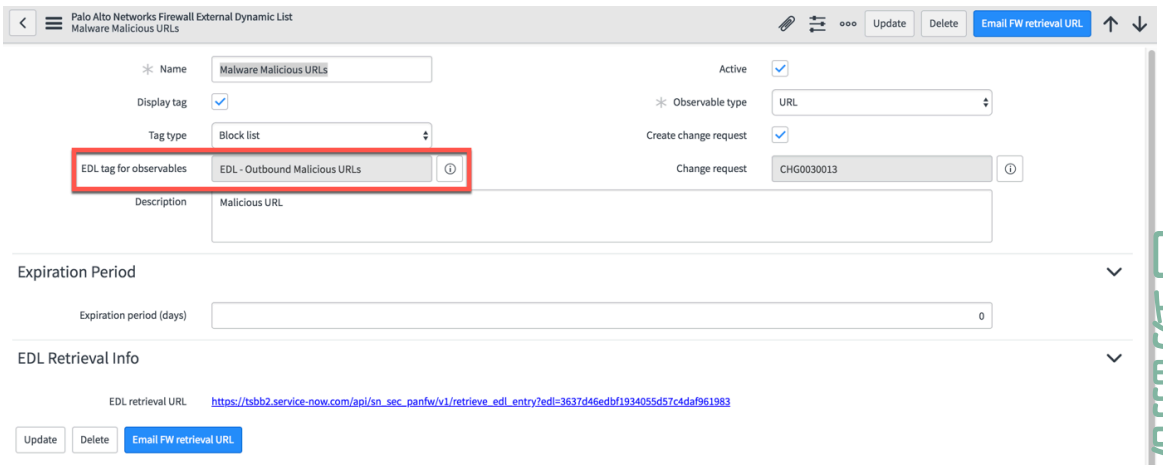


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

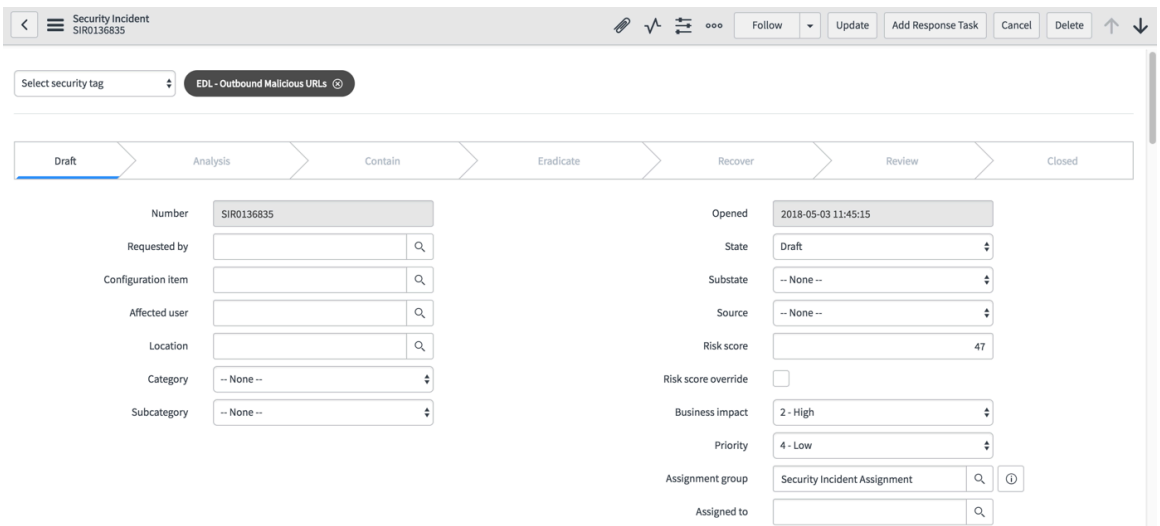
[セキュリティタグ] フォームが表示されます。



4. [名前] フィールドでセキュリティタグ名を変更し、[更新] をクリックします。
変更したタグ名で更新された EDL レコードが表示されます。次の例では、タグ名に Outbound (送信) が追加されています。新しいタグ名の EDL プリフィックスはそのまま残して、タグが Palo Alto Networks Next-Generation Firewall 統合に関連付けられていることを識別できるようにします。



EDL に観測事象が追加されるたびに、セキュリティインシデントレコードと観測事象レコードに、各観測事象タイプ (IP、URL、ドメイン) のセキュリティタグが表示されます。



観測事象がすでに EDL に追加されていて、この観測事象のセキュリティインシデントにセキュリティタグが表示されている場合、その後に作成されるセキュリティインシデントレコードにも

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

EDL セキュリティタグが自動的に表示されます。この重複は、観測事象がすでにブロックリストにあることを示しています。この観測事象を追加して再度ブロックする必要はありません。

観測事象のブロックが解除されると、セキュリティインシデントレコードまたは観測事象レコードにセキュリティタグが表示されなくなります。この場合、セキュリティタグがないことは、観測事象の有効期限を過ぎているか、観測事象が EDL から非アクティブ化されていることを示しています。

Palo Alto Networks Next-Generation Firewall をアンインストール

Now Platform インスタンスから Palo Alto Networks Next-Generation Firewall をアンインストールし、統合から残りすべてを削除する場合は、ServiceNow のドキュメントサイトで、アプリケーションのアンインストール手順を参照してください。

始める前に

必要なロール：システムアドミニストレーター (admin)
ServiceNow 製品ドキュメント Web サイト の「アプリケーションのアンインストール」を参照してください。

PhishTank の統合

PhishTank はコミュニティベースのフィッシング検証システムです。ユーザーがシステムに疑わしい脅威を送信すると、フィッシングの脅威が正当であるかどうかを、システムの他のユーザーが投票によって判定します。Now Platform セキュリティオペレーション 製品と統合すると、アナリストは、脅威インテリジェンスの結果から、フィッシング関連のセキュリティインシデントまたは調査に関する追加のインサイトを得られます。

PhishTank 統合は、潜在的なフィッシングサイトの URL のルックアップを実行します。

ワークフローは、新しい観測事象がセキュリティインシデントに入るとチェックします。観測事象が API 統合によって認識されるタイプである場合、観測事象が評価されます。悪意があると判定された観測事象にタグ付けされます。

PhishTank のインストールと構成

インスタンスで統合を実行する前に、インストールと構成の手順を完了して、PhishTank アプリケーションが Now Platform セキュリティオペレーション と適切に統合されるようにします。

始める前に

インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

セットアップタスク	説明
インスタンスに必要な Now Platform ロールが割り当てられていることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。 • システムアドミニストレーター (admin) は、アプリをインストールし、セキュリティインシデントアドミン (sn_si.admin) ロールをアサインします。 • セキュリティインシデントアドミン (sn_si.admin) は構成を監視し、期待する結果を検証します。このロールは セキュリティオペレーション モジュールにもアクセスできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
API キーを取得します。	API キーやアカウント作成方法については、PhishTank の Web サイト (PhishTank Web サイト) を参照してください。
統合用のアプリケーションをインストールする前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	Madrid 以降のリリースの要件 Madrid リリース以降のファミリリリースでは、セキュリティインシデントレスポンス Dependency プラグイン (com.snc.si_dep) が必要です。このプラグインは、セキュリティインシデントレスポンス 製品をサポートするために必要なすべての依存関係を自動的にインストールします。統合に必要な他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。 次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。 **1.** セキュリティインシデントレスポンス **2.** Security Integration Framework **3.** Security Support Common **4.** セキュリティサポートオーケストレーション 統合のための Now Platform インスタンスのセットアップの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

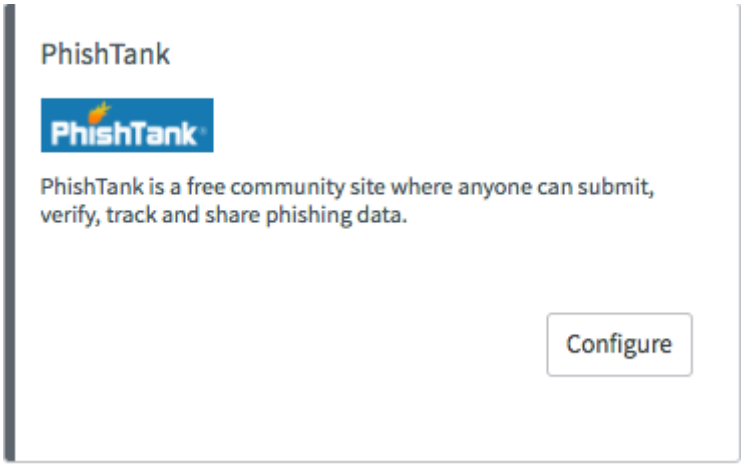
必要なロール：admin

手順

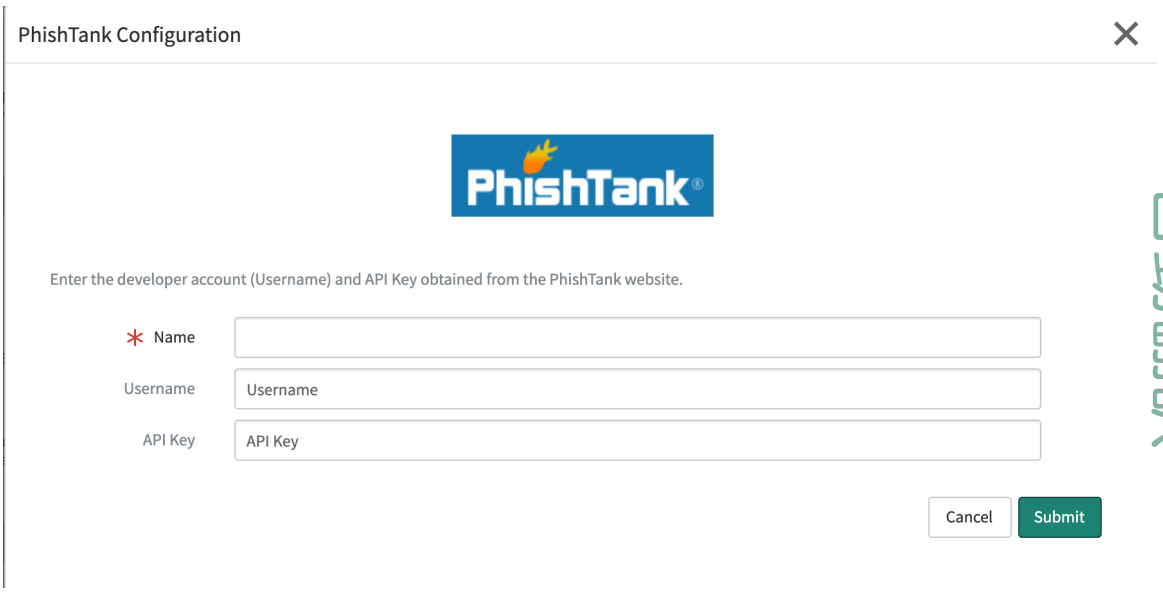
1. 統合用のアプリケーションをインストールしていない場合は、「セキュリティオペレーション 統合のインストール」を参照し、手順に従ってインストールしてください。
2. インストールが完了したら、次に移動します: 統合 > 統合構成 をクリックし、 PhishTank タイルを見つけます。
3. [構成] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. **[PhishTank 構成 (PhishTank Configuration)]** ダイアログボックスで、構成の [名前]、[ユーザー名] (PhishTank で作成された開発者アカウント)、および PhishTank Web サイトから取得した API キーを入力し、 [送信] をクリックします。



5. 正常に構成されていることを確認します。
エラーメッセージが表示されない限り、構成は正常に完了しています。

Trouble?

構成中にエラーメッセージが表示された場合は、 PhishTank API キーが無効である可能性があります。

PhishTank の期待される結果の確認

観測事象は、セキュリティインシデントによって自動的に生成され、アプリケーションによってスキャンされます。ルックアップ結果は、セキュリティインシデントレコードの下部にある [脅威のルックアップ結果] タブに表示されます。

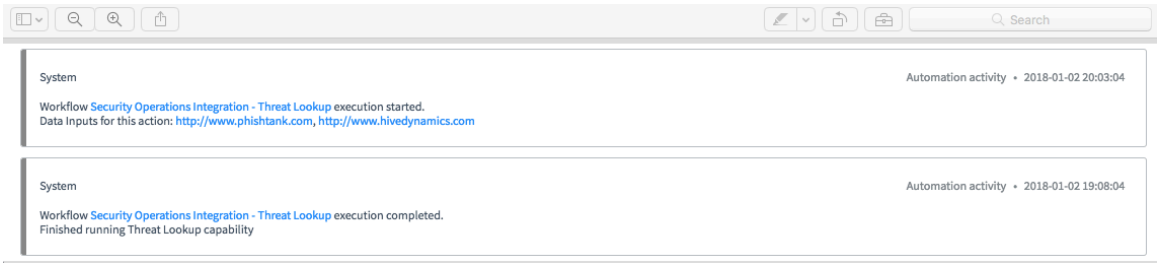
始める前に
必要なロール：sn_si.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 作業しているセキュリティインシデントフォームを開き、ルックアップが正常に実行されたことを確認します。

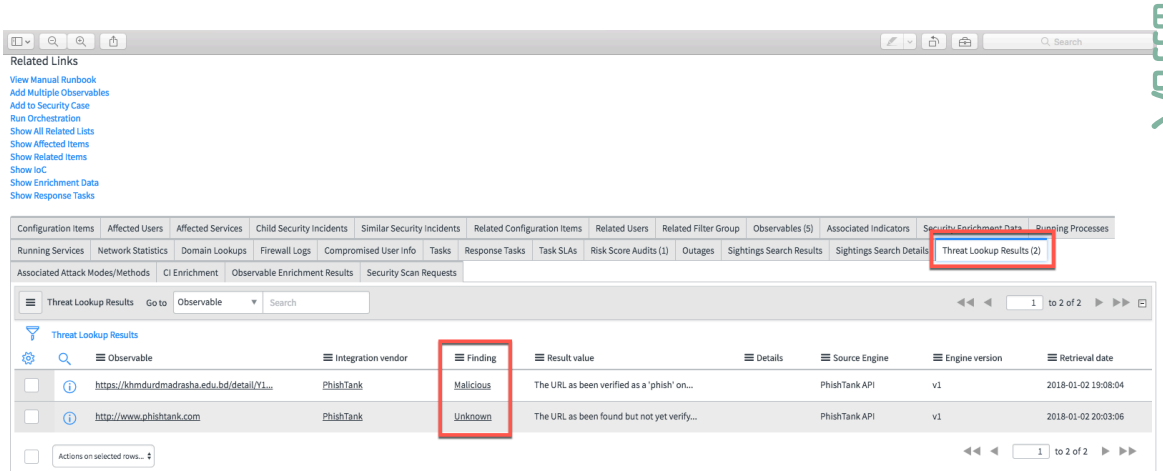


アプリケーションを設定すると、インシデントの作成時にフローが自動的に起動します。ルックアップの実行および完了ステータスは、セキュリティインシデントレコードの作業メモに表示されます。

2. ルックアップが正常に実行されたことを確認できない場合は、作業メモで詳細と対処方法を確認してください。

3. セキュリティインシデントの下部に移動し、[すべての関連リストを表示] 関連リンクをクリックします。

> **注:**
> 次の手順の図は、[システムの設定] で [タブ付きフォーム] 設定をアクティブにした状態で示されています。タブ付きフォームが表示されない場合は、バナーフレームの右上隅にある [設定] 歯車アイコンをクリックします。表示される [システムの設定] ダイアログボックスで [フォーム] をクリックし、[タブ付きフォーム] と [フォームと同時] が選択されていることを確認します。



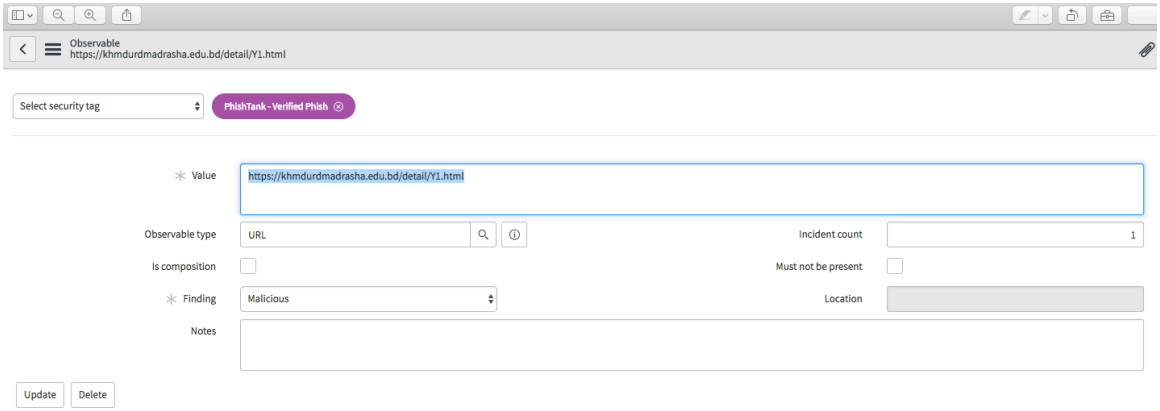
セキュリティインシデントレコードの下部にある [脅威のルックアップの結果] タブにルックアップ結果が表示されます。

悪意があると判断されなかったレコードについては、[結果] 列に [不明] と表示されます。結果で悪意があると判定された場合、 [結果] 列に [悪意がある] と表示されます。

4. [観測事象] 列で観測事象をクリックしてレコードを開き、詳細情報を表示します。

自動翻訳

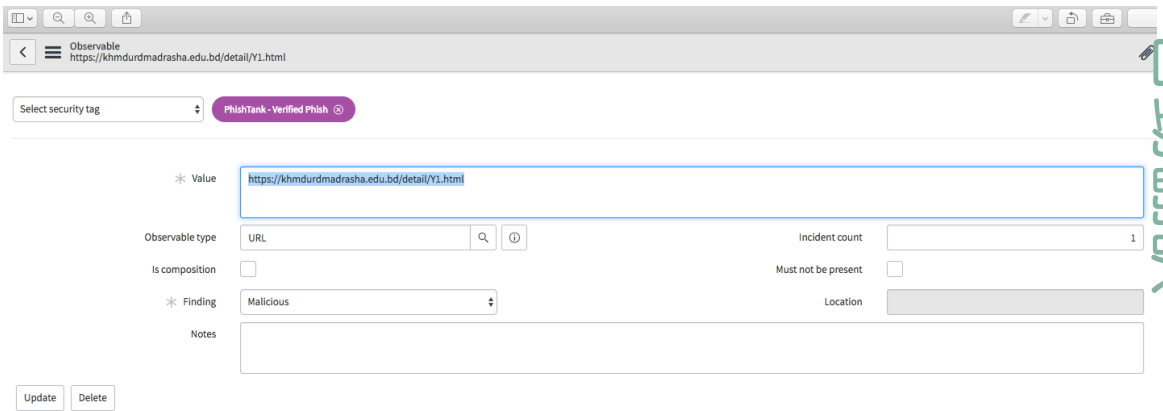
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



観測事象レコードで、ルックアップで悪意があると判定された場合、 [結果] フィールドに [悪意がある] と表示されます。観測事象は、悪意があると判定した 脅威インテリジェンス ソース (この場合は PhishTank アプリケーション) でタグ付けされます。

5. 生データを表示するには、セキュリティインシデントに戻り、観測事象の横の青い情報アイコンをクリックします。

6. 表示されるウィンドウで [レコードを開く] をクリックします。



API によって作成されたリンクと、結果が表示される [結果] フィールド。

Trouble?
[脅威のルックアップの結果] タブに結果が表示されない場合は、観測事象が統合によるルックアップでサポートされているタイプであることを確認します。

(オプション) **PhishTank** の観測事象を手動で添付する

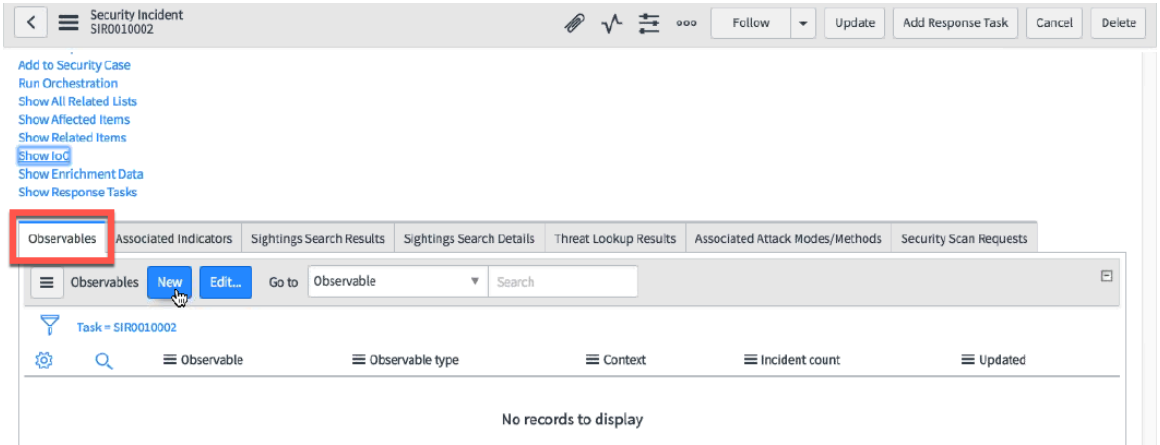
観測事象をセキュリティインシデントに手動で添付することができます。最初のイベントトリガーでセキュリティインシデントに添付されていない観測事象に対して脅威のルックアップを実行する場合は、観測事象を手動で添付します。また、関連する観測事象に関する詳細情報が必要な場合にも、このタスクを実行します。

始める前に
必要なロール：sn_si.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

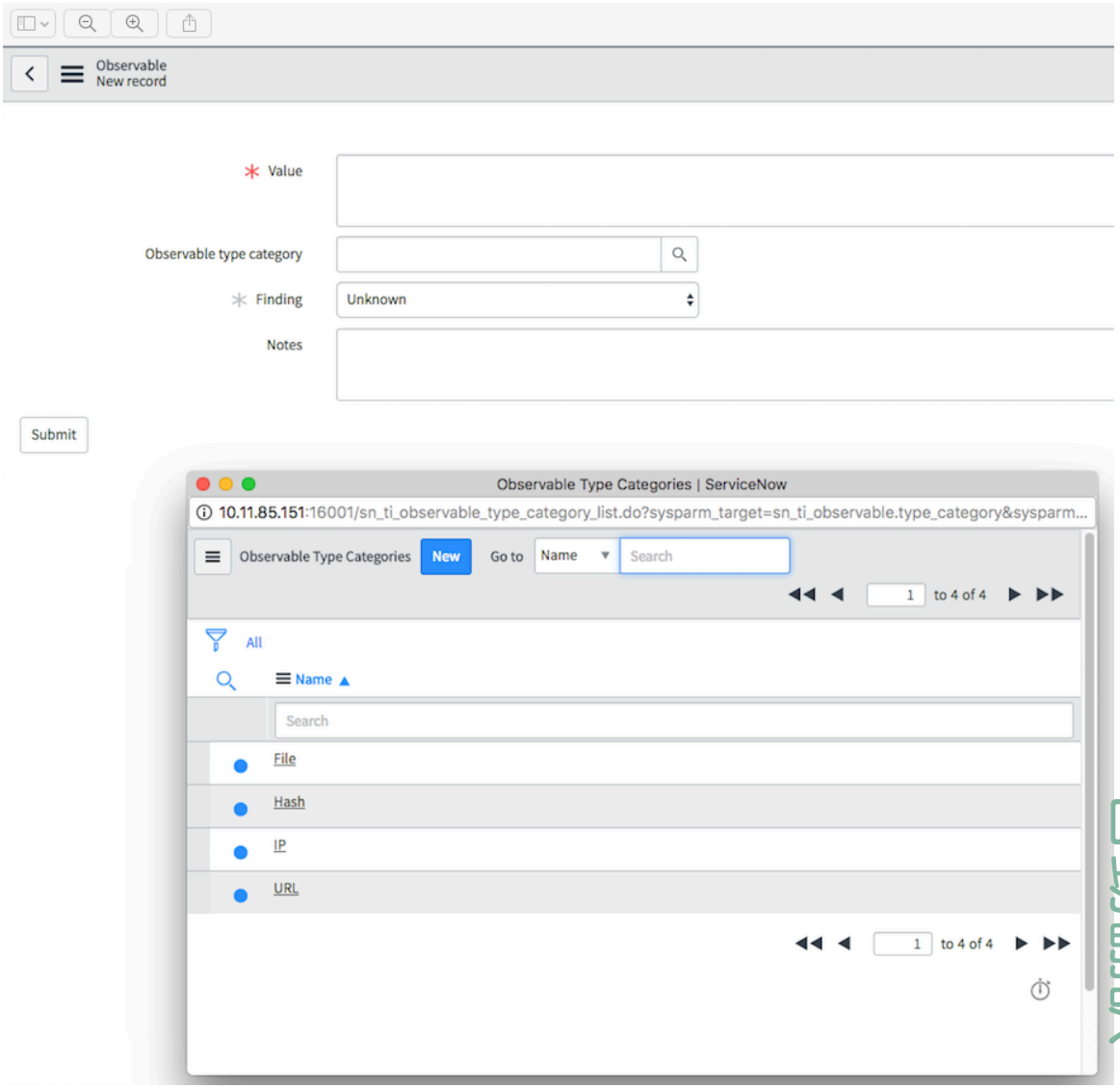
1. オープンセキュリティインシデントに移動します。
2. オープンセキュリティインシデントレコードで、[関連リンク] の **[IoC を表示]** リンクをクリックし、 [観測事象 **(Observables)]** タブを表示します。



3. [新規] をクリックします。
   観測事象フォームが表示されます。
4. [値] フィールドに URL を入力します。
5. 検索アイコンをクリックし、[観測事象タイプカテゴリ] ダイアログボックスで、リストの **[URL]** をクリックしてフィールドに入力します。

自動翻訳

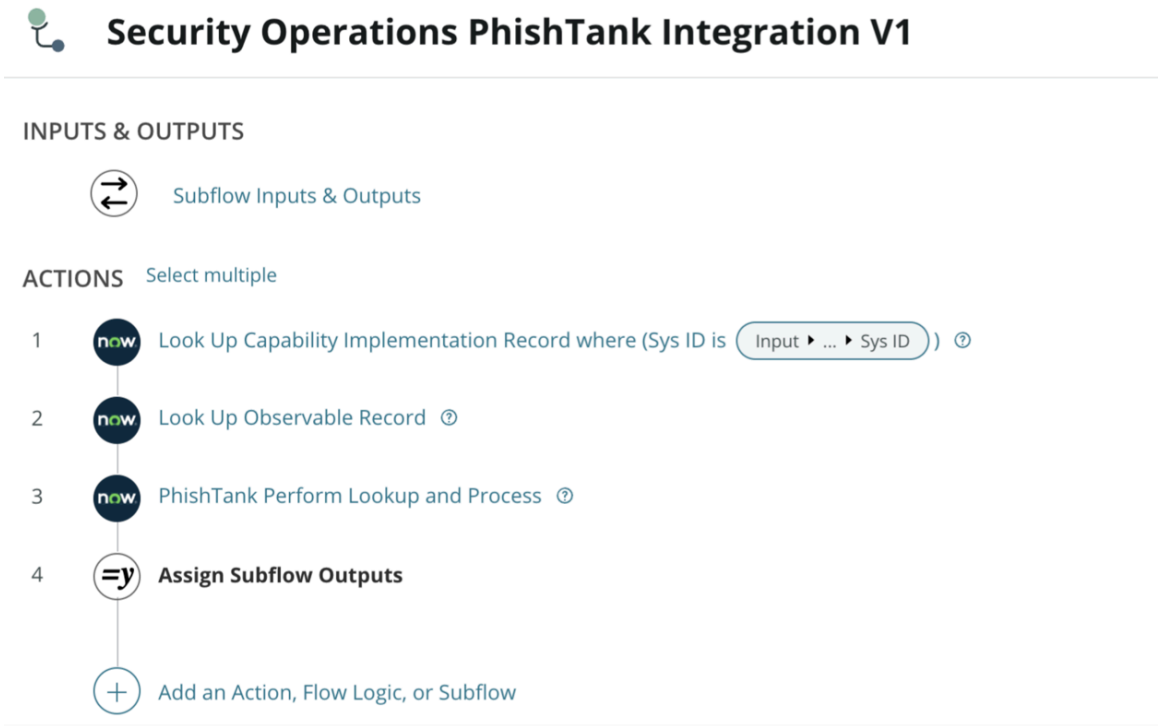
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



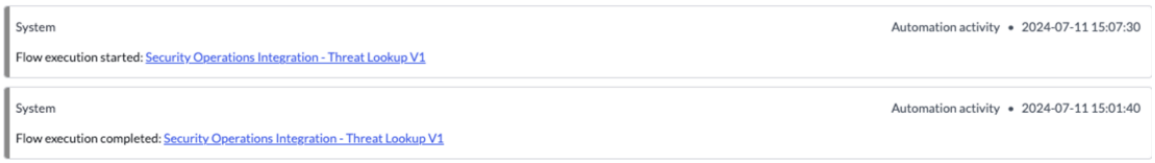
自動翻訳

6. [送信] をクリックします。
   フローが起動し、新しい観測事象がチェックされます。実行および完了ステータスは、[セキュリティインシデント] レコードの作業メモセクションに表示されます。

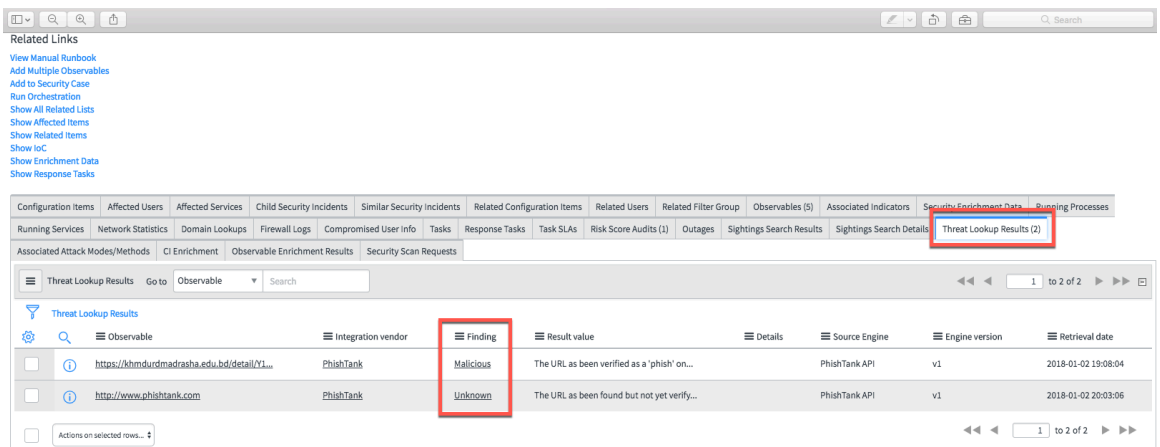
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



7. セキュリティインシデントに移動し、作業メモを確認します。



8. セキュリティインシデントの下部にある [すべての関連リストを表示] 関連リンクをクリックします。
9. [脅威のルックアップの結果] タブをクリックして結果を表示します。



10. [観測事象 **(Observable)**] 列で、観測事象の横にある青色の情報アイコンをクリックして、詳細情報と生データを表示します。

11. 表示されるダイアログボックスで、[レコードを開く] をクリックします。

自動翻訳

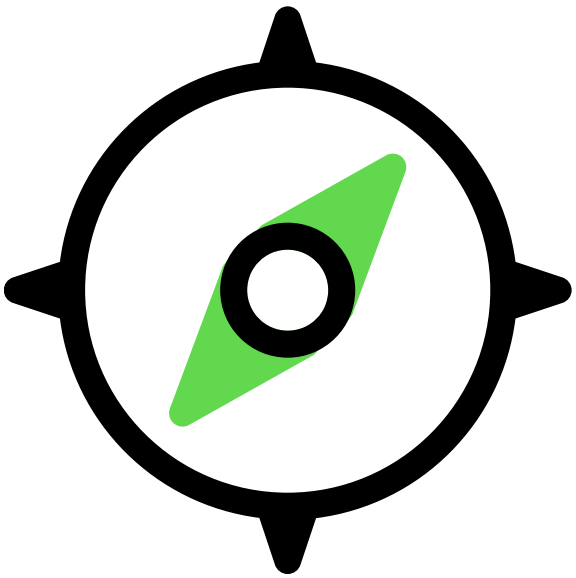
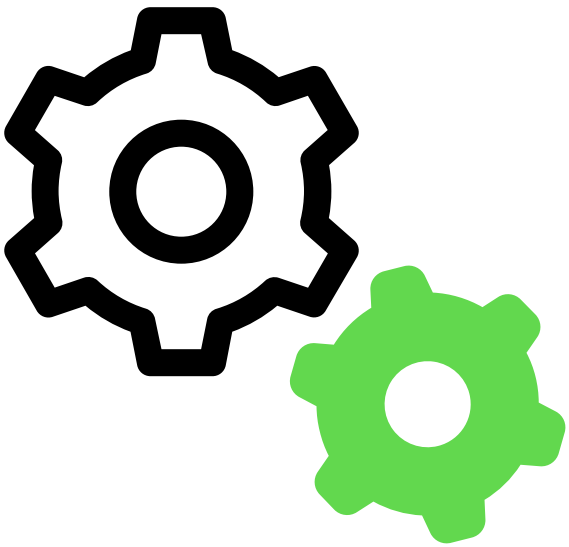
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Trouble?
ルックアップが正常に実行されたことを確認できない場合は、作業メモで詳細と対処方法を確認してください。

セキュリティオペレーション での **Proofpoint** の統合

Proofpointセキュリティオペレーション 統合は、Proofpointからのイベントの取り込みをサポートしています。セキュリティインシデントレスポンス (SIR) は、取り込まれたイベントごとに、アナリストがレビューまたは作業できるインシデントを作成します。

開始するには

探索	構成
	
Proofpoint統合の詳細	SIR ワークスペースの Proofpoint の構成

自動翻訳

の **Proofpoint** 統合の詳細 セキュリティオペレーション

セキュリティインシデントレスポンス (SIR) でイベントプロファイルを設定して、Proofpointからイベントを取り込むことができます。SIR は、取り込まれたイベントごとにインシデントを作成し、アナリストが確認または操作できるようにします。

Proofpointセキュリティオペレーションユーザーの統合

ユーザー

ユーザー	説明
セキュリティアドミン	取り込まれたイベントをフィルタリングするためのイベントプロファイルを作成します。 SIR は、これらの取り込まれたイベントのインシデントを作成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

福利厚生**Proofpoint**のための統合 セキュリティオペレーション

福利厚生**Proofpoint**のための統合 セキュリティオペレーション

ベネフィット	機能	ユーザー
イベントデータをインスタンスにプルし、セキュリティインシデントを作成します。不審または悪意があると見なされたイベントのセキュリティインシデントを 1 つの場所から確認します。	配信されたメール メッセージと許可されたクリックが後で悪意のあるものと見なされた場合、これらのメッセージは従業員によって開封され、操作された可能性があります。これらのメッセージのレビューを追跡するために、統合のメッセージトラフィック用に作成および設定したイベントプロファイルに基づいて、セキュリティインシデントを自動的に作成します。 監査を目的として、ブロックされたメッセージとクリックのセキュリティインシデントの作成を有効にすることもできます。	マネージャー

自動翻訳

次に探索する内容

Proofpointの構成と使用の詳細については、次のトピックを参照してください。

- の Proofpoint 統合の構成 セキュリティオペレーション
- Proofpoint統合設定の確認
- Proofpointアナリティクスダッシュボードの表示

の **Proofpoint** 統合の構成 セキュリティオペレーション

セキュリティオペレーション の Proofpoint 統合の実装を構成します。

構成の概要

1. の Proofpoint 統合のインストールと構成 セキュリティオペレーション.

   統合アプリケーションをダウンロードしてインストールし、アクティブ化します。

2. Proofpoint の統合セキュリティオペレーションのイベントプロファイルの作成.

   イベントプロファイルを作成して、 Proofpoint 製品からインポートするイベントと、インポートされたデータからセキュリティインシデントを作成するために使用する条件を特定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. Proofpoint統合設定の確認

イベントプロファイルを作成するための統合設定を確認します。

の **Proofpoint** 統合のインストールと構成セキュリティオペレーション®

ServiceNowインスタンスのServiceNow Storeから セキュリティオペレーション アプリケーションの Proofpoint 統合をインストールして設定します。

始める前に
必要なロール：sn_si_admin

手順

1. ServiceNow® Store から Proofpoint Integration for the セキュリティオペレーション アプリケーションをダウンロードしてインストールします。
   詳細については、「 ServiceNow Store アプリケーションのインストール 」を参照してください。
2. 次のように移動する。 セキュリティオペレーション > 統合 > 統合設定.
3. [セキュリティオペレーション の Proofpoint 統合] タイルを見つけて、[構成] を選択します。
4. フォームのフィールドに入力します。

Proofpoint 統合構成フォーム

フィールド	説明
名前	Security Operations 構成の Proofpoint 統合の名前。
サービスプリンシパル	Proofpointテナントのユーザー名。
シークレット	Proofpointテナントの ID。

5. [**Submit** (送信)] を選択します。

タスクの結果
構成の検証と送信が正常に完了すると、統合は [セキュリティ統合] ページにタイルとして保存されます。

Proofpoint の統合セキュリティオペレーションのイベントプロファイルの作成

イベントプロファイルを作成して、 Proofpoint 製品からインポートするイベントを特定し、 セキュリティインシデントレスポンス アプリケーションでセキュリティインシデントを作成します。

このタスクについて
イベントプロファイルを作成するには、イベントタイプ、マッピング、およびスケジュール済みインポートを構成します。ページの進捗状況バーにすべてのステップが表示され、現在アクティブな構成が強調表示されます。[続行] または [前へ] ボタンを使用して、それぞれ前後に移動できます。

始める前に
必要なロール：sn_si_admin

手順

1. 次のように移動する。 **All** (すべて) > **Proofpoint** との **SIR** 統合 > **Proofpoint** イベントプロファイル.
   [Proofpoint イベントプロファイル] ページには、既存のイベントプロファイルが一覧表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

2. **[New** (新規)] を選択します。
3. フォームのフィールドに入力します。

   進捗状況バーは [名前] から始まります。

   Proofpoint イベントプロファイル フォーム

フィールド	説明
名前	イベントプロファイルの名前。関連するイベントタイプを含む名前を使用することを検討してください。 ○ ブロックされたクリック ○ 許可されたクリック ○ ブロックされたメッセージ ○ 配信されたメッセージ
ソース	[統合設定] ページで統合用に構成されたソース。
順序	このプロファイルの実行順序。デフォルト値は 100 です。
アクティブ	プロファイルをアクティブ化するためのオプション。
説明	このイベントプロファイルためのオプション説明 。

4. **[Continue** (続行)] をクリックします。
5. 1 つ以上のイベントタイプを [利用可能] 列から [選択済み] 列に移動して選択します。
   利用可能なイベントタイプは、次のとおりです。
   - ブロックされたクリック
   - 許可されたクリック
   - ブロックされたメッセージ
   - 配信されたメッセージ
6. **[Continue** (続行)] をクリックします。

   選択したイベントタイプに関連する構成ステップが進捗状況バーに表示されます。

   ソースフィールドの値は、環境内の標的型攻撃防御 (TAP) データから参照として提供されます。

   ソースフィールドデータとターゲットフィールドのデフォルトマッピングがページに表示されます。基本データはガイドとして含まれていますが、このマッピングは変更できます。

7. オプション: **f(x)** アイコンを選択すると、アプリケーションに含まれるデフォルトの翻訳が表示されます。

   (Optional) これらの翻訳では、値の間にカンマを挿入することで、フィールドの複数の値に対応します。

8. **[Continue** (続行)] をクリックします。
9. [フィルタリングと集計] ページで、次の表のプロパティを構成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィルタリングとアグリゲーションのプロパティ

オプション	説明
メッセージイベントの条件に基づいてフィルター	メッセージイベントに基づいてフィルタリングを有効にするオプション。
メッセージイベントフィルター条件	メッセージイベントフィルター条件。
クリックイベントの条件に基づいてフィルター	クリックイベントに基づいてフィルタリングを有効にするオプション。
クリックイベントフィルター条件	イベントフィルター条件をクリックします。
集計条件	新しいインシデントを作成する代わりに、受信インシデントをオープンセキュリティインシデントに追加できるようにするオプション。
一致する値を持つインシデントフィールド	インシデントを集計に含めるために値を一致させる必要がある セキュリティインシデントレスポンス フィールドを追加します。
新規インシデントの作業メモを記録	作業メモを親 セキュリティインシデントレスポンスに記録できるようにするオプション。
ThreatID リレーションを有効にする	一致する ThreatID を持つすべてのインシデントの集計を有効にするオプション。

10. **[Continue** (続行)] をクリックします。
11. インポートタイプのいずれかを選択し、イベントデータをインポートする頻度を選択します。
12. [完了] を選択します。

タスクの結果
新しく作成されたイベントプロファイル既存のイベントプロファイルとともに一覧表示されます

Proofpoint統合設定の確認

環境のシステムプロパティを変更できるように、Proofpoint統合設定を確認します。

Proofpoint 統合設定フォーム

プロパティ名	説明
restAPI 呼び出しのタイムアウト。 sn_sec_proofpoint.http_timeout	API 呼び出しからデータをフェッチするためのタイムアウト (秒)。 タイプ: 整数 デフォルト値：3000
ロギングレベル - デバッグ、情報、警告、エラー sn_sec_proofpoint.logging_verbosity	情報のタイプの名前を示すアプリケーションのログの詳細度レベル。使用可能な値： • エラー • warn

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Proofpoint 統合設定フォーム (続く)

プロパティ名	説明
	• info • debug デフォルト値：info
単一のインシデントに集計できる Proofpoint イベント数の制限を強制します。 sn_sec_proofpoint.max_aggregations_per_si	1 つのインシデントに集計できる Proofpoint イベントの最大数。 タイプ: 整数 デフォルト値：100
24 時間内に作成できるセキュリティインシデント数の制限を強制します。 sn_sec_proofpoint.max_si_per_day	24 時間に作成できるインシデントの最大数。 タイプ: 整数 デフォルト値：1000
トップクリッカー (VAP) の API 呼び出しで使用する必要がある日数。 sn_sec_proofpoint.default_days	トップクリッカーと VAP についてフェッチするデータの日数。使用可能な値： • 14 • 30 • 90 タイプ: 整数 デフォルト値：90
ブールフラグ。有効にすると、API 呼び出しが行われ、Topclickers の詳細が入力されます。 sn_sec_proofpoint.call_topclickers_api	トップクリッカーデータを有効にしてフェッチするオプション。 タイプ：ブーリアン デフォルト値：True
ブールフラグ。有効にすると、API 呼び出しが行われ、VAP の詳細が入力されます。 sn_sec_proofpoint.call_vap_api	VAP データを有効にしてフェッチするオプション。 タイプ：ブーリアン デフォルト値：False
これは、topClickers、VAP ユーザーに表示するユーザーの最大数を制限することです。 sn_sec_proofpoint.maxresults	トップクリッカーと VAP ユーザーに表示するユーザーの最大数。 タイプ: 整数 デフォルト値：100
Proofpoint イベントのスケジュールされたポーリング中に重複期間を使用して有効/無効にします。	スケジュール済みポーリングが構成されている場合に重複期間を有効にするオプション。 タイプ：ブーリアン

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Proofpoint 統合設定フォーム (続く)

プロパティ名	説明
sn_sec_proofpoint.allow_overlap	デフォルト値：False
重複が有効になっている場合に、ProofpointEvents のスケジュール設定済みポーリング中に使用される重複時間 (分)。 sn_sec_proofpoint.overlap_time	スケジュール済みポーリングが構成されている場合の重複時間 (分)。 タイプ: 整数 デフォルト値：5

Proofpointアナリティクスダッシュボードの表示

Proofpointアナリティクスダッシュボードには、VAP ユーザーと上位クリッカーに関する詳細が表示されます。

このタスクについて

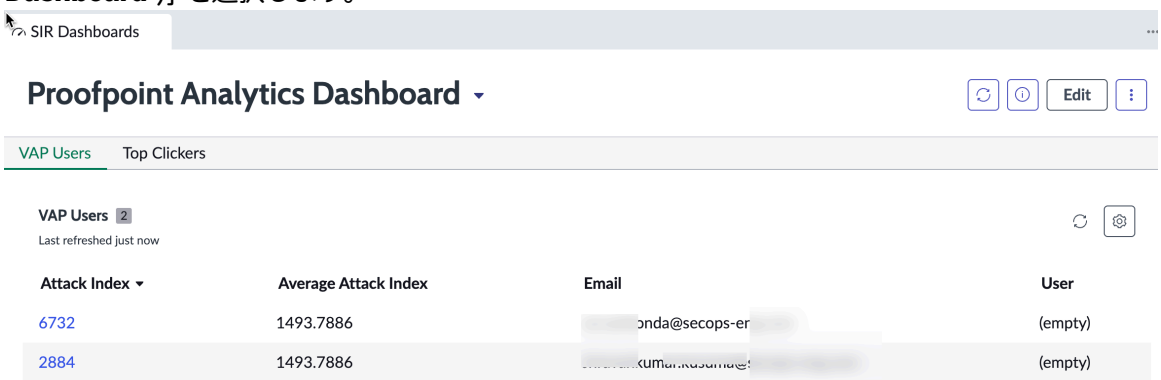
Users 主にセキュリティ攻撃の標的は、 VAPユーザーと見なされます。疑わしいリンクやフィッシングリンク頻繁にクリック するEmployeは、 トップクリッカーと見なされます。

始める前に

必要なロール：sn_si_admin

手順

1. 次のように移動する。 **All** (すべて) > ワークスペース > セキュリティインシデントレスポンスワークスペース.
2. **[SIR** ダッシュボード] を選択します。
3. ドロップダウンリストから [**Proofpoint** アナリティクスダッシュボード **(Proofpoint Analytics Dashboard**)] を選択します。



4. VAP ユーザーに関する情報を表示します。
   a. **[VAP** ユーザー] タブを選択して、VAP ユーザーのリストを表示します。
   b. ユーザー名を選択して、VAP ユーザーの詳細を表示します。
5. 上位クリッカーに関する情報を表示します。
   a. [トップクリッカー] タブを選択して、上位クリッカーのリストを表示します。
   b. トップクリッカーの詳細を表示するには、 ユーザー名を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Reverse Whois の統合

Reverse Whois は、個人または組織によって登録されたドメイン名の検索を実行するサービスです。

セキュリティインシデントに添付する観測事象の検索用語を使用して、ドメインルックアップを実行します。Reverse Whois API は、入力された検索用語に基づいてドメインレコードを検索し、それらの用語に対応するすべてのレコードを返します。

アナリストは、セキュリティインシデント調査のために Whois 統合と併せてこの統合を使用することがあります。Whois 統合は、Reverse Whois 統合からのドメインルックアップに基づいて追加の拡張情報を提供します。

Reverse Whois のインストールと構成

インスタンスで統合を実行する前に、インストールと構成の手順を完了して、Reverse Whois アプリケーションが セキュリティオペレーション 製品と適切に統合されるようにします。

始める前に

インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

セットアップタスク	説明
必要な ServiceNow ロールがアサインされていることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。 • システムアドミニストレーター (admin) は、アプリをインストールし、セキュリティインシデントアドミン (sn_si.admin) ロールをアサインします。 • セキュリティインシデントアドミン (sn_si.admin) は構成を監視します。セキュリティインシデントアドミニストレーターは、セキュリティインシデントアナリスト (sn_si.analyst) ロールのアサインも行います。 • セキュリティインシデントアナリスト (sn_si.analyst) は、Reverse Whois でドメインルックアップを実行し、セキュリティインシデントを処理します。
API キーを取得します。	API キーやアカウント作成方法については、WhoisXML API の Web サイト を参照してください。設定するには、API キーを入力する必要があります。
統合用のアプリケーションをインストールする前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	Madrid 以降のリリースの要件 Madrid リリース以降のファミリリリースでは、セキュリティインシデントレスポンス Dependency プラグイン (com.snc.si_dep) が必要です。このプラグインは、セキュリティインシデントレスポンス 製品をサポートするために必要なすべての依存関係を自動的にインストールします。統合に必要な他の セキュリティオペレーション アプリケーションをインストー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	ルしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。 次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。 **1.** セキュリティインシデントレスポンス **2.** Security Integration Framework **3.** Security Support Common **4.** セキュリティサポートオーケストレーション 統合のための Now Platform インスタンスのセットアップの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

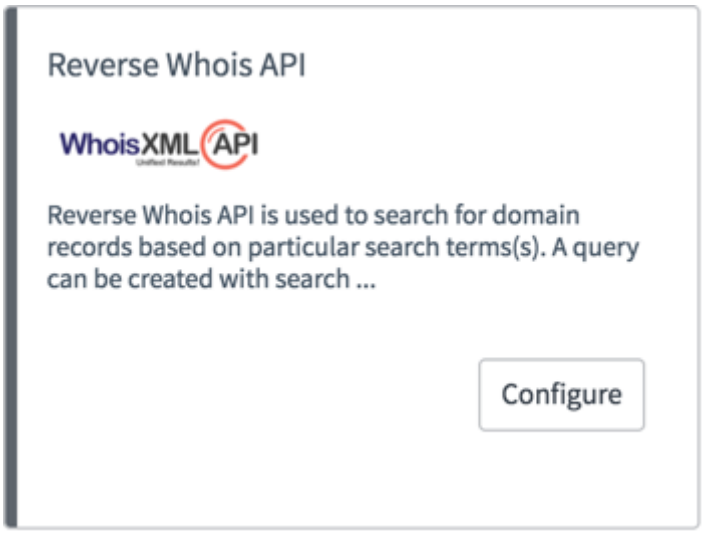
必要なロール：admin

手順

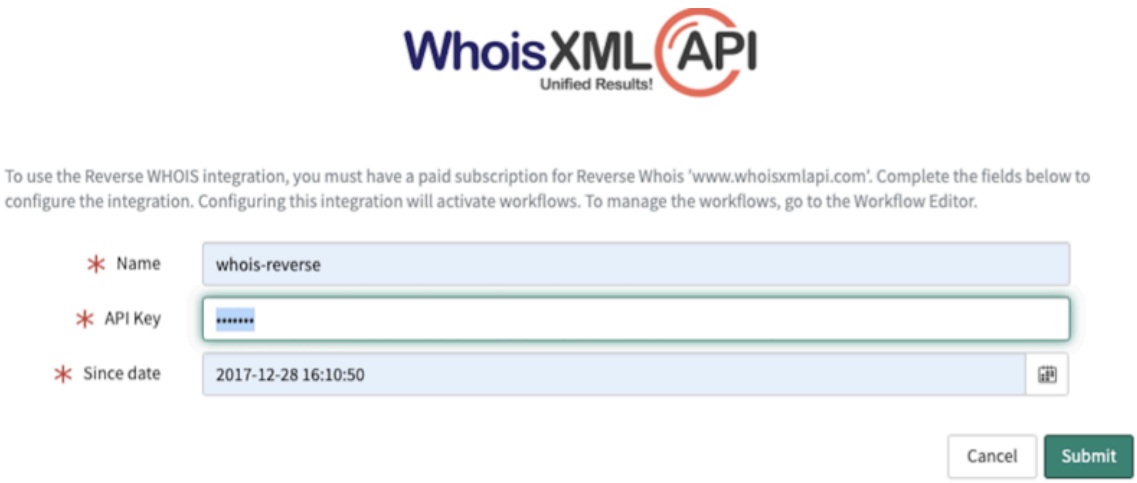
1. Reverse Whois アプリケーションをすでにインストールして設定している場合は、次の手順に従います。
   a. 既存の構成を削除します。
   b. 取得した API キーを使用して、新しい構成をインストールして作成します。
2. 統合用のアプリケーションをインストールしていない場合は、「セキュリティオペレーション 統合のインストール」を参照し、手順に従ってインストールしてください。
3. インストールが完了したら、次に移動します: 統合 > 統合構成 をクリックし、[Reverse Whois API] タイルを見つけます。
4. [構成] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



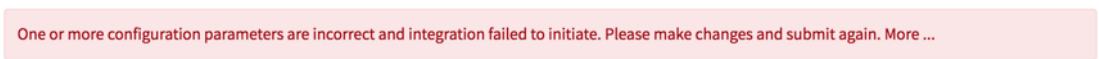
5. **[Reverse Whois API** 構成 **(Reverse Whois API Configuration)]** ダイアログボックスで、Whois XML API Web サイトから取得した API キーを入力します。
6. 次の表からオプションを 1 つ選択し、検索用語のドメインルックアップをフィルタリングします。
   これらの構成設定は、変更してすべての Reverse Whois API 検索に適用するまで保存されます。



7. **[Submit]** をクリックします。
   エラーメッセージが表示されない限り、構成は正常に完了しています。

Trouble?
エラーメッセージが表示される場合は、API キーが無効である可能性があります。

エラーメッセージ



(オプション) **Whois** のインストールと設定

Whois プラグインをインストールすると、Reverse Whois API からのドメインルックアップに関する追加の拡張情報を得られます。このルックアップは、登録日、登録機関の名前、登録国など、ドメインに関する追加の拡張データを提供します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

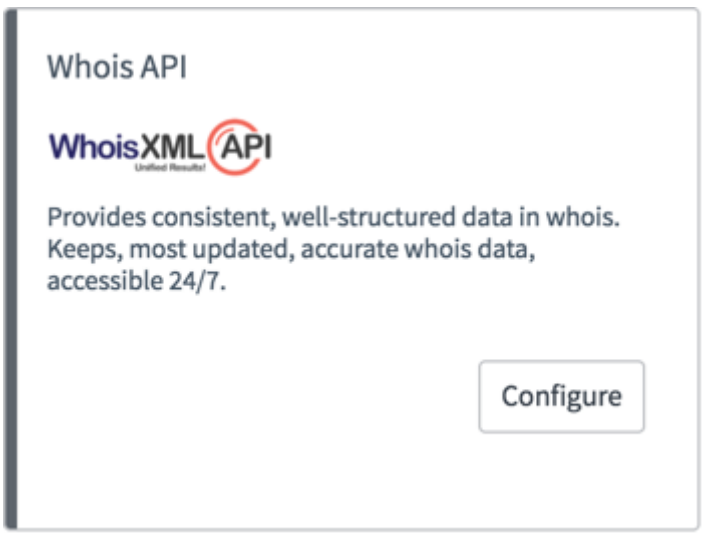
始める前に

1. ServiceNow Store の Whois アプリケーションのエンタイトルメントをまだ要求していない場合は、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」を参照してください。
2. 製品 Web サイト (WHOIS API Web サイト) から Whois API キーの認証情報を取得します。

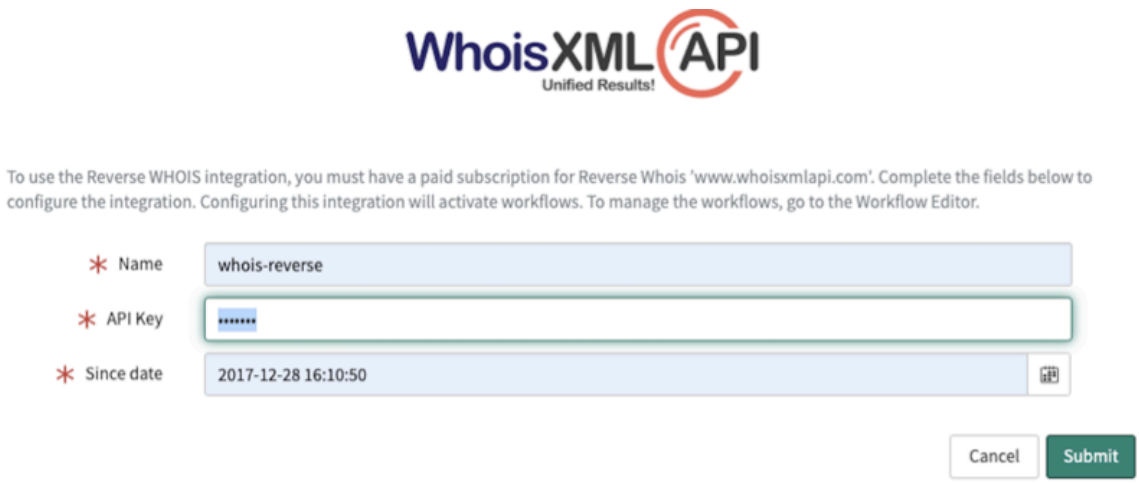
必要なロール：admin

手順

1. アプリケーションをまだインストールしていない場合は、「セキュリティオペレーション 統合のインストール」を参照し、手順に従ってインストールしてください。
2. インストールが完了したら、次に移動します: 統合 > 統合構成 をクリックし、[Whois API] タイルを見つけます。
3. [構成] をクリックします。



4. **[Whois API 構成 (Whois API Configuration)]** ダイアログボックスで、製品 Web サイトから取得した API キーを入力します。



5. **[Submit]** をクリックします。
エラーメッセージが表示されない限り、構成は正常に完了しています。これで、Reverse Whois 統合から返されたドメインに対して拡張ルックアップを実行できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Trouble?
エラーメッセージが表示される場合は、API キーが無効である可能性があります。

トラブルシューティング

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

Reverse Whois のルックアップの開始

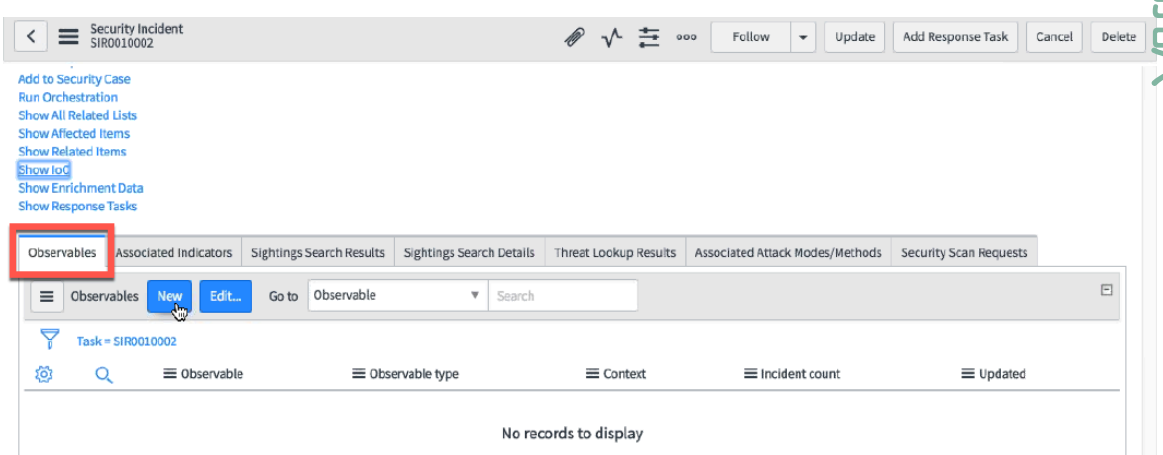
セキュリティインシデントレコードに手動で添付する観測事象の検索用語を使用して、ドメインルックアップを開始します。

始める前に
必要なロール：sn_si.analyst

手順

1. 開いていない場合は、次に移動します: セキュリティインシデント > インシデント > すべてのインシデントを表示 をクリックし、目的のセキュリティインシデントを開きます。
2. レコードの下部の **[IoC** を表示] 関連リンクをクリックして、[観測事象 (Observables)] タブを表示します。

   注:
   次の手順の図は、[システムの設定] で [タブ付きフォーム] 設定をアクティブにした状態で示されています。セキュリティインシデントにタブが表示されない場合は、バナーフレームの右上隅で、[設定] 歯車アイコンをクリックします。表示される [システムの設定] ダイアログボックスで [フォーム] をクリックし、[タブ付きフォーム] と [フォームと同時] が選択されていることを確認します。



3. [観測事象 (Observables)] タブで、[新規] をクリックします。
4. フィールドに入力します。

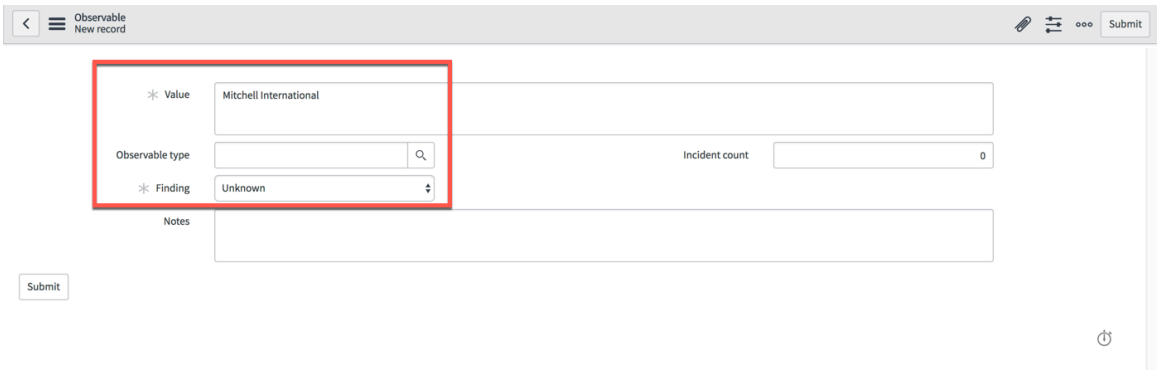
新規レコードの必須フィールド

フィールド	説明
値	ドメインの一意の検索用語
観測事象タイプ	このフィールドは自動的にクリアされます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
結果	このフィールドは自動的に [不明] に設定されます。



5. [送信] をクリックします。
   セキュリティインシデントレコードに戻り、フローがルックアップを開始します。

次のタスク
セキュリティインシデントでルックアップの結果を確認します。「Reverse Whois の期待される結果の確認」を参照してください。

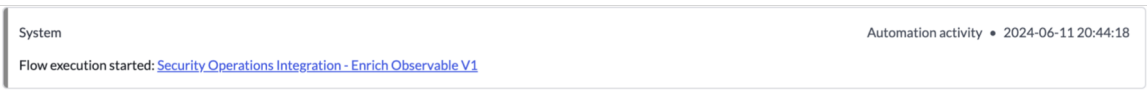
Reverse Whois の期待される結果の確認

エンリッチメント結果は、セキュリティインシデントレコードの下部にある **[ReverseWhois ドメイン (ReverseWhois Domains)]** タブに表示されます。ルックアップ結果を見つけて、ルックアップが正常に実行されたことを確認します。

始める前に
必要なロール：sn_si.analyst

手順

1. まだ開いていない場合は、次に移動します: セキュリティインシデント > インシデント > すべてのインシデントを表示 をクリックし、目的のセキュリティインシデントを見つけます。



   アプリケーションが構成された後、観測事象を添付すると、フローが自動的に起動します。セキュリティインシデントレコードの作業メモには、ルックアップの実行および完了ステータスが表示されます。

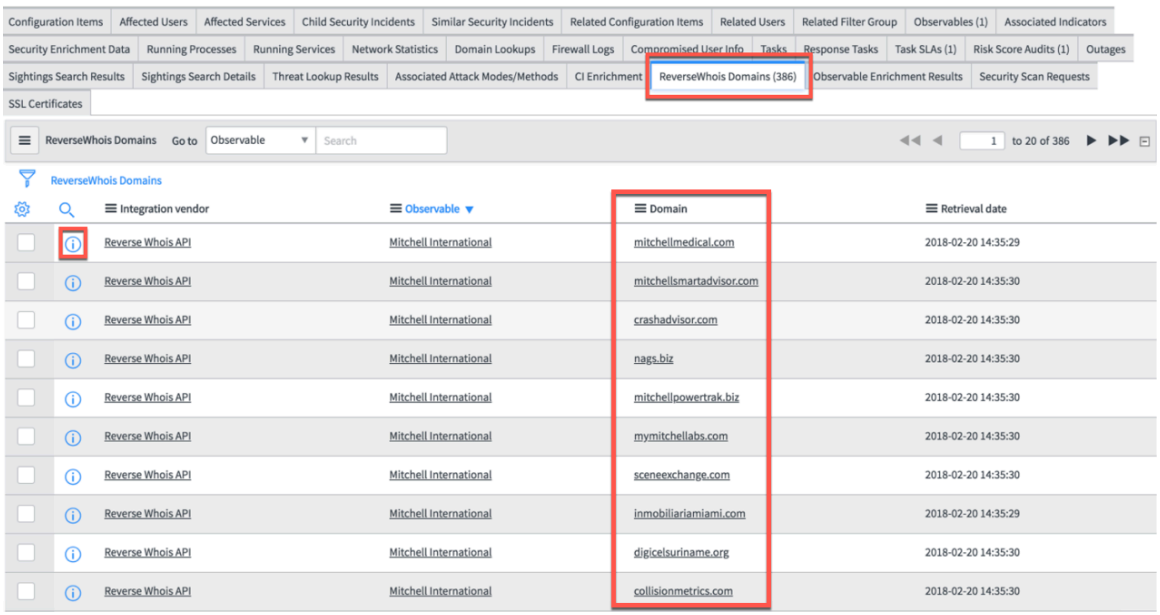
2. ルックアップが正常に実行されたことが確認できない場合は、処理方法の詳細について作業メモを確認してください。

3. セキュリティインシデントの下部に移動し、[すべての関連リストを表示] 関連リンクをクリックします。

自動翻訳

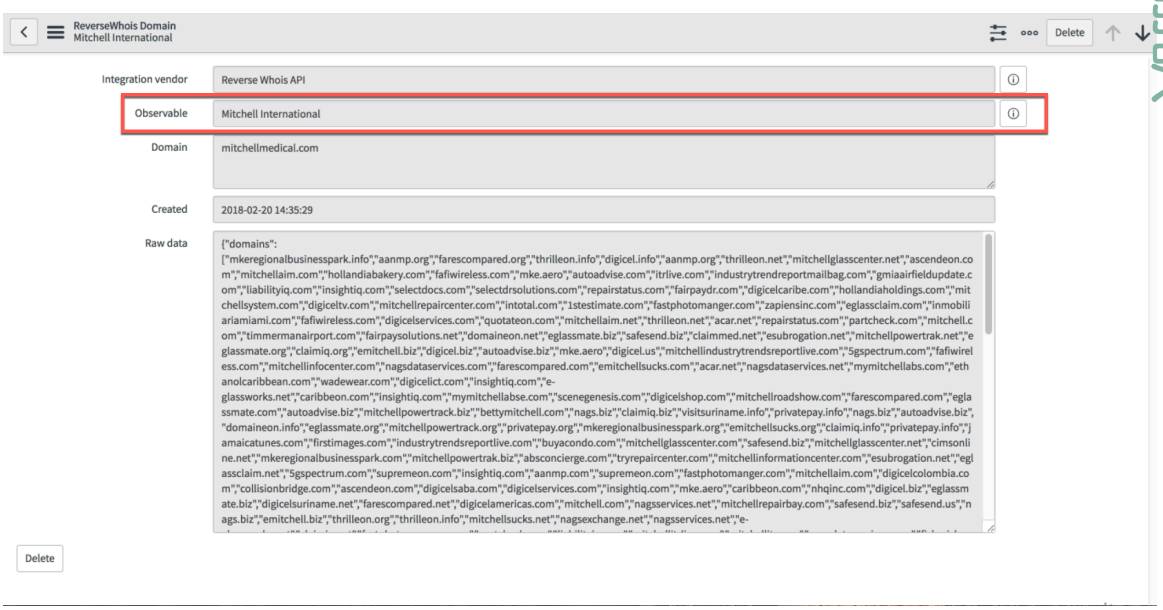
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
次の図に示すフィルタリング済みのルックアップ結果では、 Reverse Whois API 構成タイルの構成設定が、[開始日] フィールドに「**1991-06-01**」と入力された状態で保存されています。



エンリッチメント結果は、**[ReverseWhois ドメイン (ReverseWhois Domains)]** タブに表示されます。この観測事象のアクティブなドメインが [ドメイン] 列に表示されます。

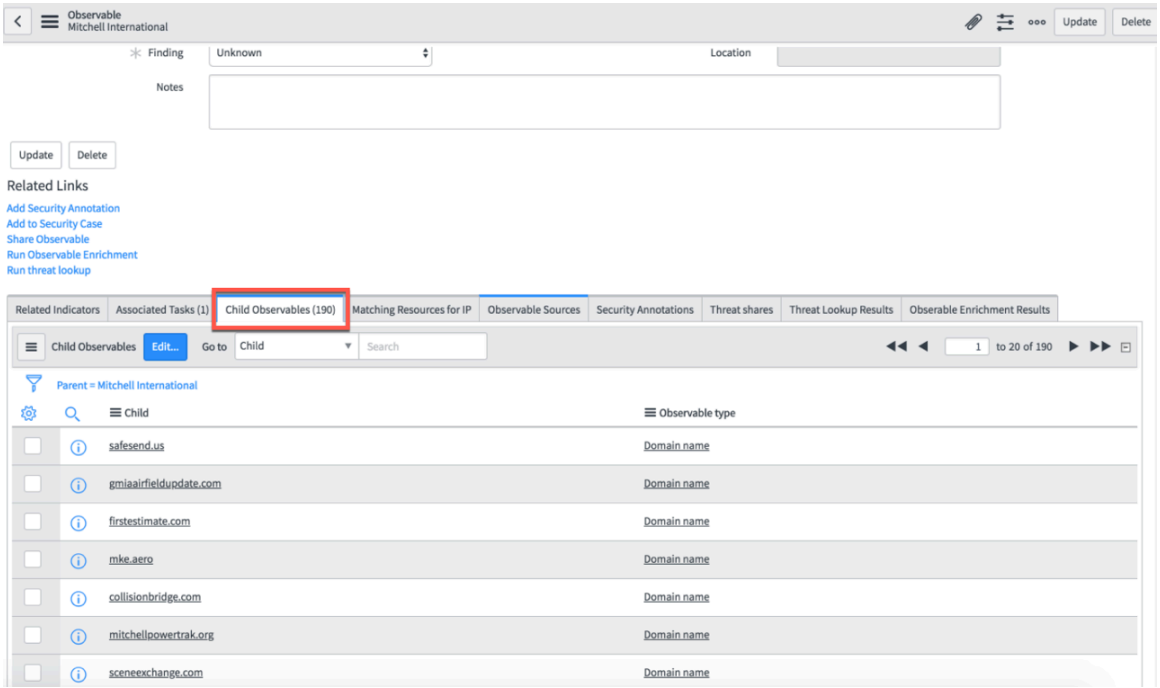
4. アイテムの横の青い情報アイコンをクリックし、表示されるダイアログボックスで [レコードを開く] をクリックします。



レコードは、生データを含む拡張の詳細とともに表示されます。

5. セキュリティインシデントに戻り、**[ReverseWhois ドメイン (ReverseWhois Domains)]** タブを選択した状態で [観測事象 **(Observable)]** 列の観測事象をクリックしてレコードを開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[観測事象 (Observable)] レコードの [子観測事象] タブに、子観測事象が表示されます。子観測事象は、Reverse Whois アプリケーションがドメインを返した場合のみ生成されます。

Trouble?
ルックアップが正常に完了しない場合は、入力した検索用語が統合によってサポートされていることを確認してください。詳細については、作業メモを確認してください。

次のタスク
さらにドメインルックアップの結果の拡張データが必要な場合は、 Whois 統合を実行して、Reverse Whois 統合から返された子観測事象に対して拡張ルックアップを実行することができます。子観測事象に関するこの拡張データには、登録日、登録機関の名前、登録国など関する情報が含まれています。

(オプション) **Whois** の拡張ルックアップを実行し、結果が期待どおりかどうかを確認する

Whois 統合を実行して、Reverse Whois 統合から返されたドメインで拡張ルックアップを実行します。

始める前に
Reverse Whois および Whois プラグインがインストールおよび設定されていることを確認します。次の手順は、必ず、Reverse Whois プラグインを使用してドメインルックアップを正常に実行してから実行してください。

必要なロール：sn_si.analyst

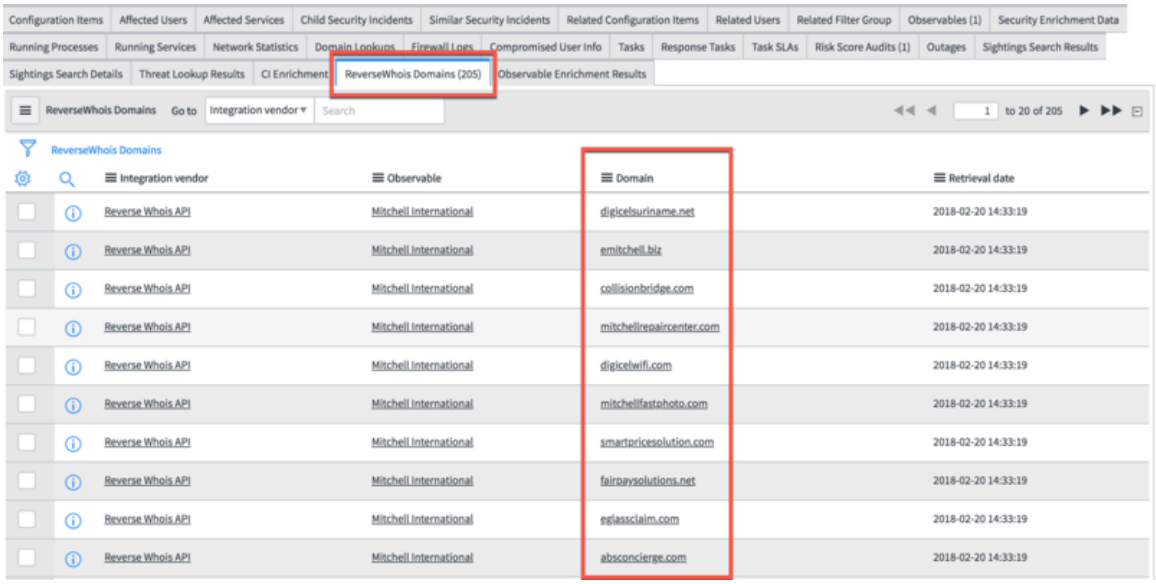
このタスクについて
結果は、[観測事象 (Observable)] レコードの [観測事象の拡張結果] タブに表示されます。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデント > すべてのインシデントを表示 をクリックし、ドメインルックアップを正常に実行した、操作しているセキュリティインシデントを見つけます。
2. レコードを開き、[すべての関連リストを表示] 関連リンクをクリックします。

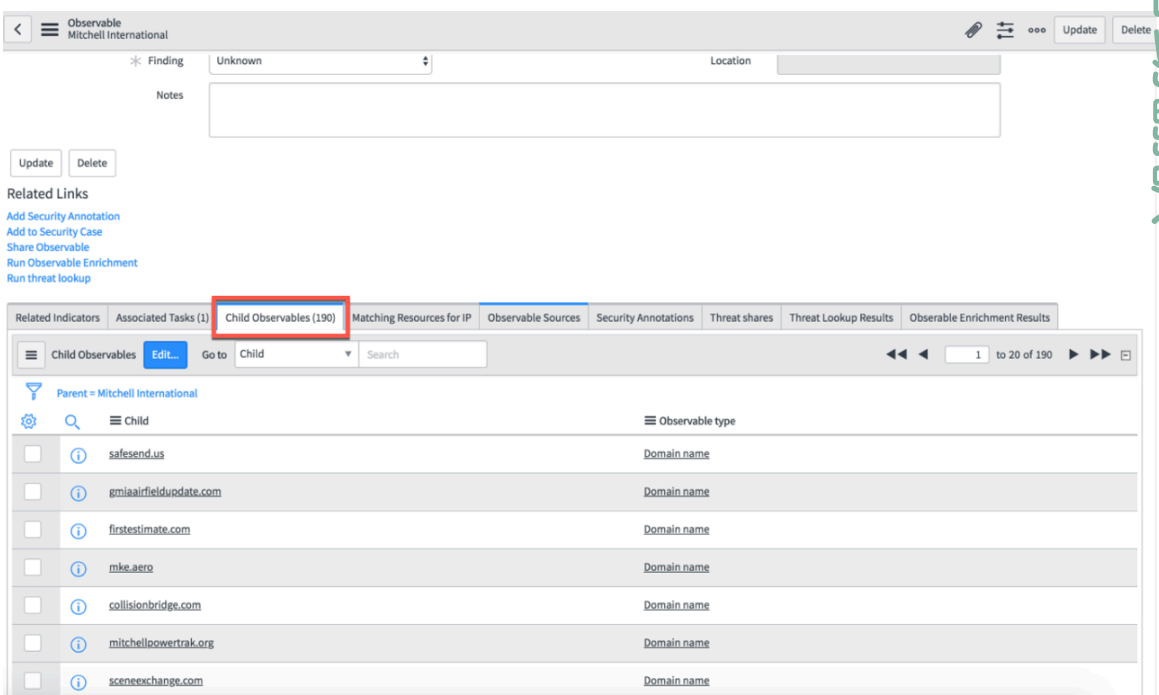
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. レコードの下部にある **[ReverseWhois ドメイン (ReverseWhois Domains)]** タブを選択します。



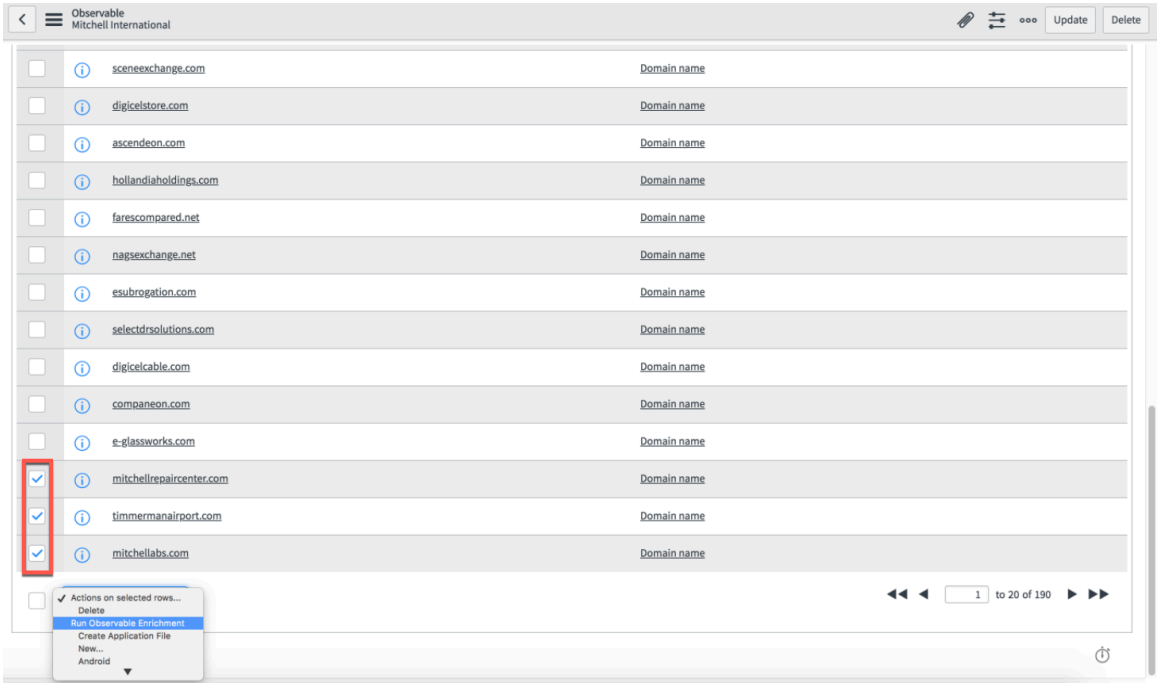
[ドメイン] 列に、返されたドメインのリストが表示されます。

4. [観測事象 **(Observable)]** 列で、観測事象をクリックします。
[子観測事象] タブに、子観測事象が表示されます。子観測事象は、Reverse Whois アプリケーションによる観測事象の最初のスキャンでドメインが返された場合にのみ生成されます。



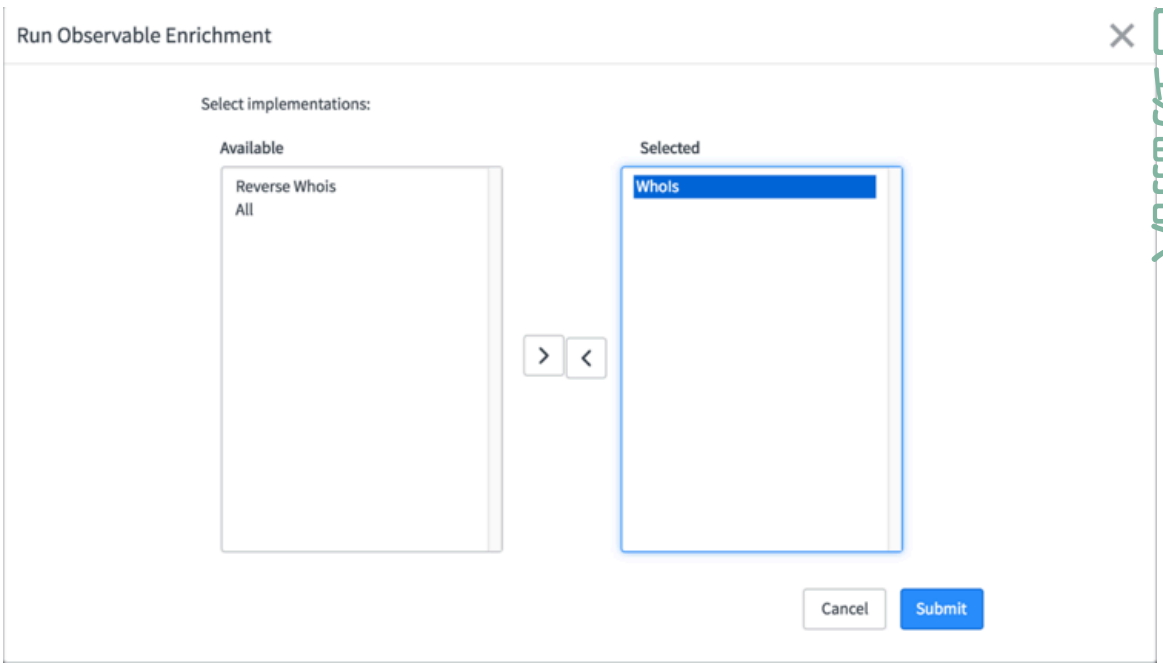
5. 観測事象の拡張を実行する子観測事象を選択し、[選択した行でアクションを実行 **(Action on selected rows)]** 選択リストで [観測事象の拡張を実行]を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[観測事象の拡張を実行] ダイアログボックスが表示されます。

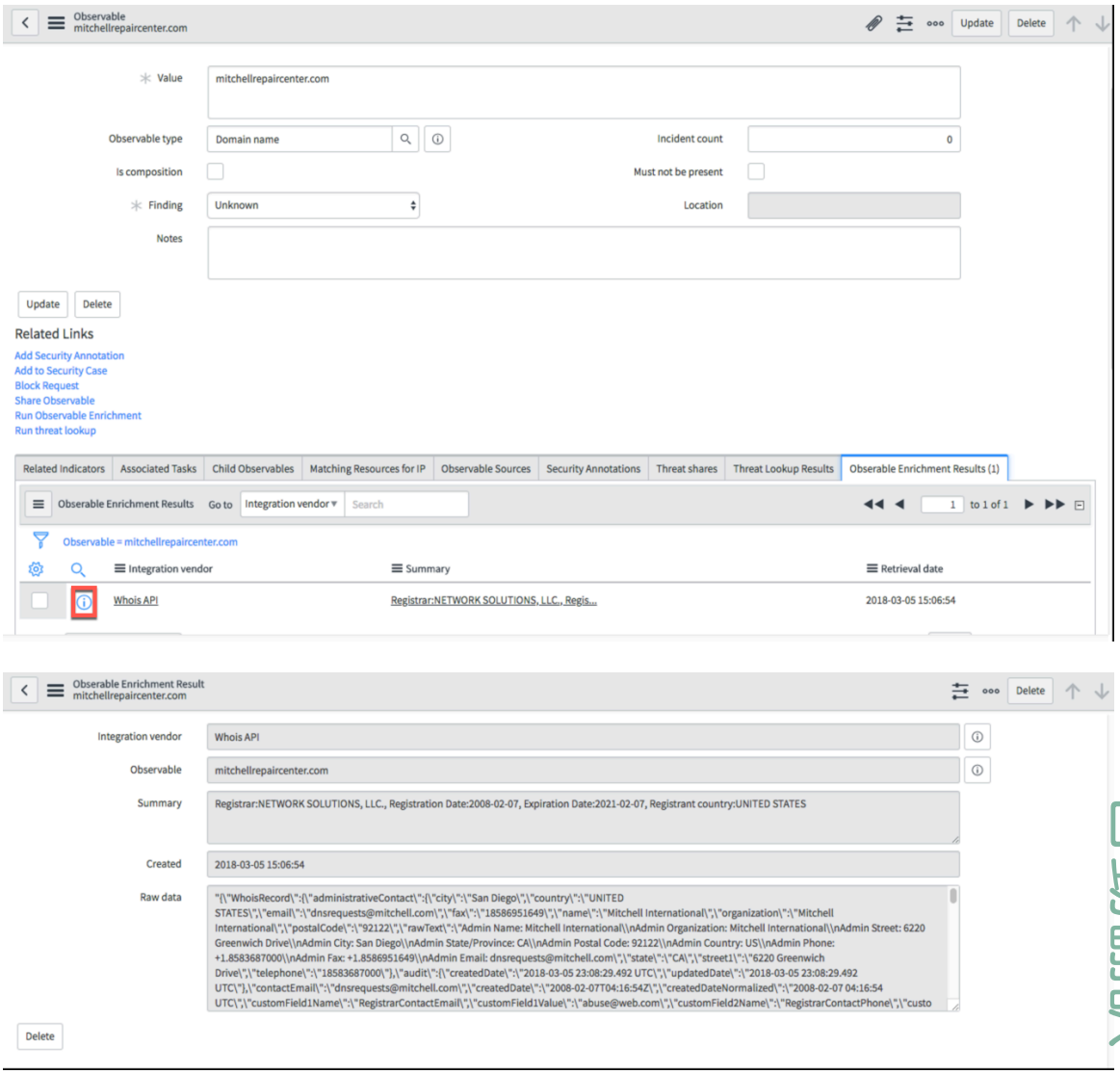
6. Whois 統合を [利用可能] から [選択済み] に移動し、[送信] をクリックします。



結果は、観測事象レコードの [観測事象の拡張結果] タブに表示されます。

7. 青い情報アイコンをクリックし、表示されるダイアログボックスで [レコードを開く] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



登録日、登録機関の名前、登録国など、元のドメインのルックアップに関連する詳細情報と生データが表示されます。

Trouble?
子観測事象またはエンリッチメント結果が見つからない場合は、Reverse Whois 統合が正常に実行され、ドメインが返されていることを確認します。また、詳細についてはレコードの作業メモも参照してください。

関連情報

Reverse Whois のインストールと構成

Reverse Whois の期待される結果の確認

RISKIQ および WHOISIQ の統合

RISKIQ および WHOISIQ® の API を Now Platform セキュリティオペレーション 製品と統合することで、セキュリティアナリストは Web サイトの妥当性に関する追加の拡張データとインサイトを得ることができます。

RISKIQ SSL 証明書 API は、SSL 証明書のルックアップを実行します。ルックアップには、発行元の認証局、証明書を要求する組織、証明書の発行先のエンティティ、およびドメインが含まれます。セキュリティインシデントが作成されると、SSL 証明書のルックアップが自動的に実行されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

RISKIQ WHOISIQ API は、ドメイン、メール、ネームサーバー、組織、住所、電話番号など、その他の観測事象タイプのルックアップを実行します。セキュリティインシデントが作成されると、URL およびドメイン観測事象が自動的に拡張されます。

統合には セキュリティインシデントレスポンス および 脅威インテリジェンス 製品が必要です。

RISKIQ および RISKIQ WHOISIQ でサポートされている観測事象

RISKIQ API は、観測事象として、IP アドレス、ファイルハッシュ、証明書のシリアル番号、ドメイン、および URL の自動 SSL 証明書ルックアップをサポートしています。URL およびドメイン観測事象は、WHOISIQ API で自動的に拡張されます。WHOISIQ API で他のタイプの観測事象を拡張するには、観測事象を作成し、[観測事象 (Observable)] テーブルから手動でルックアップを実行します。

サポートされている観測事象

次の表に、この統合で使用される API のタイプと、各 API がサポートする観測事象を示します。この表は、セキュリティインシデントの作成時にルックアップが自動的に発生するか、[観測事象 (Observable)] テーブルからルックアップを手動で実行するかも示しています。

サポートされている観測事象とルックアップ

API	サポートされている観測事象	ルックアップ (自動または手動)
RISKIQ SSL 証明書 API	• IP アドレス • ファイルハッシュ (証明書のサムプリント)。ファイルハッシュの例については、次の図を参照してください。 • 証明書シリアル番号またはシリアル番号。この文字列はエンティティの一意の ID です。証明書シリアル番号の例については、次の図を参照してください。 • ドメイン (www.site.com または site.com) • URL **注:** 自動スキャンは、https:// プロトコルを使用して URL 形式で実行されます (例：https://example.com/index.html)。	インシデント作成時に自動ルックアップ。 結果は、セキュリティインシデントレコードの **[SSL** 証明書] タブに表示されます。
RISKIQ WHOISIQ API	• ドメイン • URL	インシデント作成時に自動ルックアップ。 結果は、セキュリティインシデントレコードの [観測事象の拡張結果] タブに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サポートされている観測事象とルックアップ (続く)

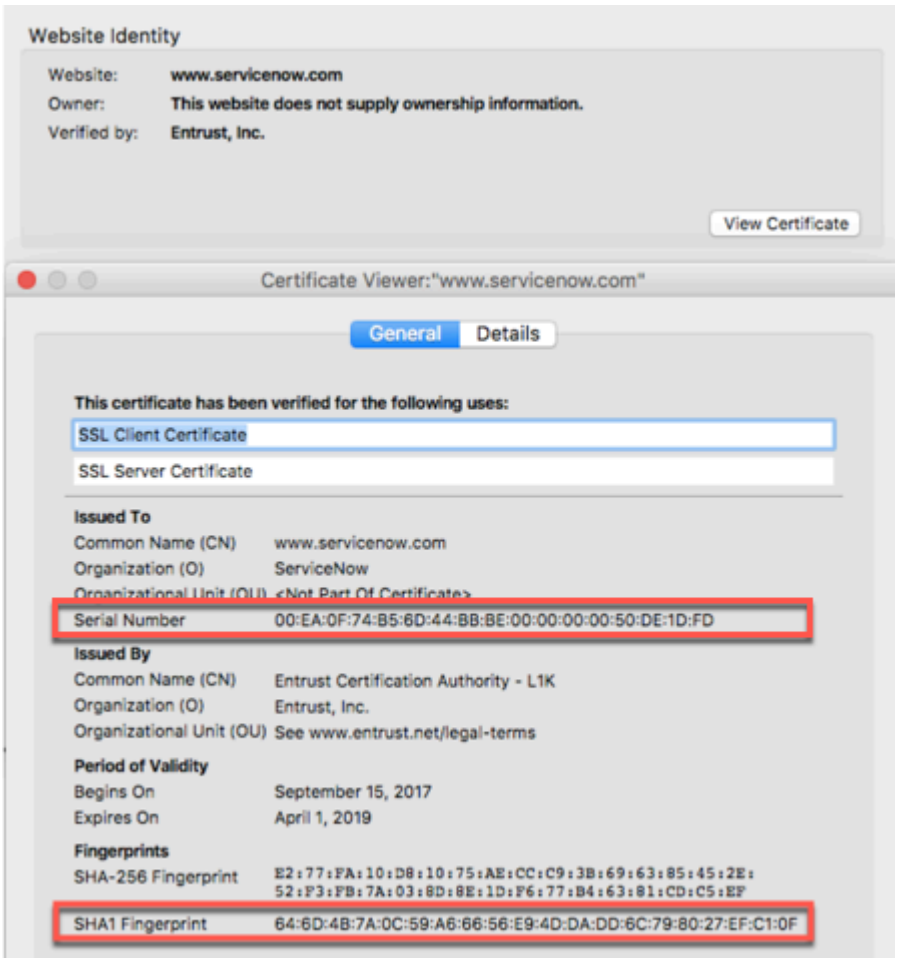
API	サポートされている観測事象	ルックアップ (自動または手動)
RISKIQ WHOISIQ API	• メールアドレス • 組織名 • 電話番号 • 郵送先	[観測事象 (Observables)] テーブルから手動でルックアップを実行します。 結果は、[観測事象 (Observable)] レコードの [観測事象の拡張結果] タブに表示されます。

ファイルハッシュと証明書シリアル番号の例

この図は、この統合の SSL 証明書ルックアップに使用されるファイルハッシュと証明書のシリアル番号の観測事象の例を示しています。ファイルハッシュとは、SHA-1 フィンガープリントを指しています。Now Platform インスタンスでは、この値はコロンの区切りなしで表示されます。
例：646D4B7A0C59A66656E94DDADD6C798027EFC10F。

証明書のシリアル番号観測事象とは、エンティティの一意の ID またはシリアル番号を指しています。この値もコロンの区切りなしで表示されます。
例：00EA0F74B56D44BBBE0000000050DE1DFD。

ファイルハッシュと証明書シリアル番号



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

RISKIQ と WHOISIQ のインストールと構成

インスタンスで統合を実行する前に、インストールと構成の手順を完了して、RISKIQ および WHOISIQ アプリケーションが Now Platform セキュリティオペレーション と適切に統合されるようにします。

始める前に

必要なロール：admin、RISKIQ admin、WHOISIQ admin

インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

セットアップタスク	説明
必要なロールがアサインされていることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。 • システムアドミニストレーター (admin) は、アプリをインストールし、セキュリティインシデントアドミン (sn_si.admin) ロールをアサインします。 • セキュリティインシデントアドミン (sn_si.admin) は構成を監視し、期待される結果を検証します。このロールは セキュリティオペレーション モジュールにもアクセスでき、セキュリティインシデントアナリスト (sn_si.analyst) ロールをアサインします。 • セキュリティインシデントアナリスト (sn_si.analyst) は、セキュリティインシデントレコードを操作します。
ユーザー名と API キーを取得します。	API キーやアカウント作成方法については、RISKIQ の Web サイト にアクセスしてください。構成には API キーを入力する必要があります。
統合用のアプリケーションをインストールする前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	Madrid 以降のリリースの要件 Madrid リリース以降のファミリリリースでは、セキュリティインシデントレスポンス Dependency プラグイン (com.snc.si_dep) が必要です。このプラグインは、セキュリティインシデントレスポンス 製品をサポートするために必要なすべての依存関係を自動的にインストールします。統合に必要な他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。 次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。

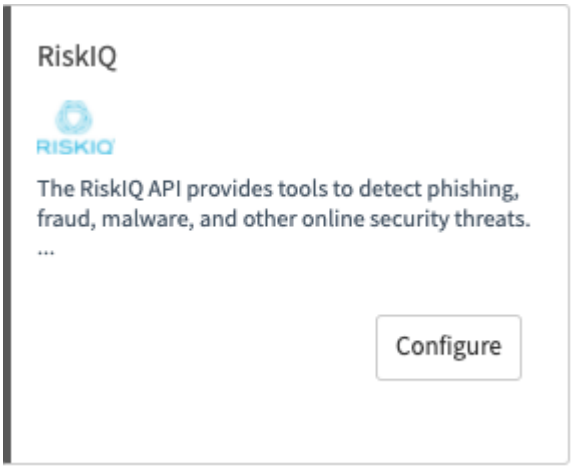
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	1. セキュリティインシデントレスポンス **2.** Security Integration Framework **3.** Security Support Common **4.** セキュリティサポートオーケストレーション 統合のための Now Platform インスタンスのセットアップの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

手順

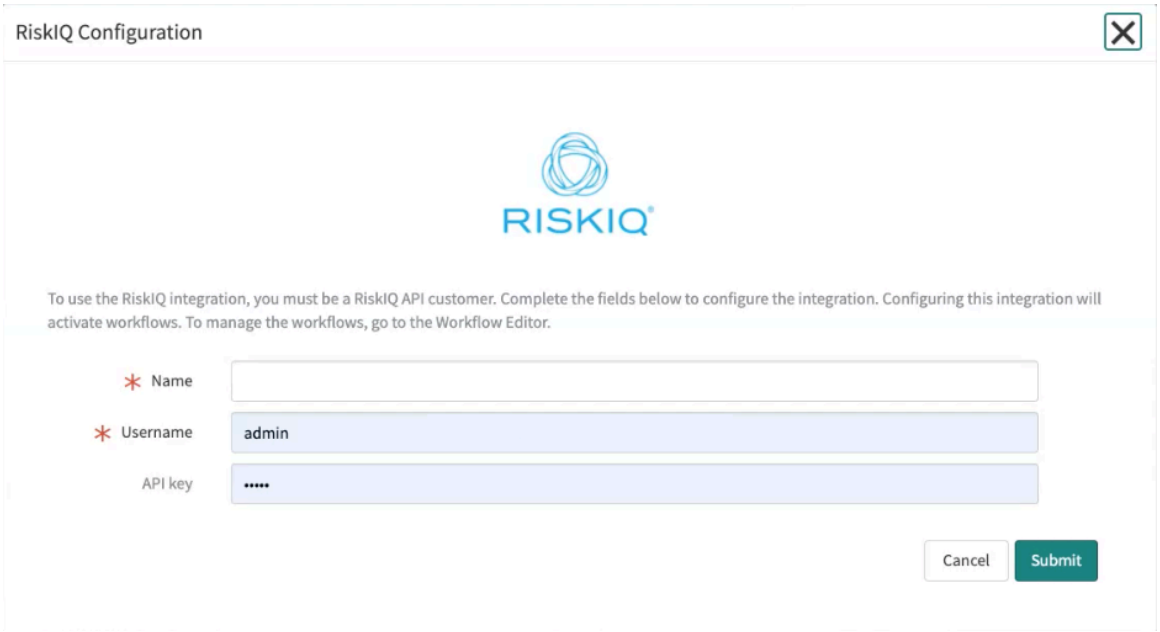
1. 統合用のアプリケーションをインストールしていない場合は、「セキュリティオペレーション 統合のインストール」を参照し、手順に従ってインストールしてください。
2. インストールが完了したら、次に移動します: セキュリティオペレーション > 統合 > 統合構成 API タイルを見つけます。
3. [構成] をクリックします。



4. 表示される [RiskIQ 設定 (RiskIQ Configuration)] ダイアログボックスで、ユーザー名と **API** キーを入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. **[Submit]** をクリックします。
6. 正常に構成されていることを確認します。
   構成が正常に完了すると、統合タイルを含む [セキュリティ統合] ページが表示されます。

Trouble?
エラーメッセージが表示される場合は、ユーザー名または API キーが無効である可能性があります。ユーザー名と API キーが正しいことを確認します。

トラブルシューティング

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

RISKIQ SSL 証明書ルックアップの期待する結果を確認する

セキュリティインシデントによって URL、ドメイン、IP アドレス、証明書ファイルハッシュ (SHA-1 フィンガープリント)、および証明書シリアル番号が生成される場合、セキュリティインシデントアナリストは、SSL 証明書ルックアップ結果を使用して、サイトに信頼できる公開認証局 (CA) が発行した証明書があるかどうかを確認します。

始める前に
必要なロール：sn_si.analyst

このタスクについて
サポートされている観測事象について、Now Platform は URL、ドメイン、IP アドレス、証明書ファイルハッシュ (SHA-1 フィンガープリント)、および証明書シリアル番号の最新の発生をスキャンします。スキャンから得られる可能性のある結果は次のとおりです。

完全一致が見つかった

SSL 証明書の有効な発行者がセキュリティインシデントレコードにリストされています。

証明書の結果が見つからなかった

セキュリティインシデントレコードに結果がリストされていません。

自己署名証明書または内部で生成された証明書で完全一致が見つかった

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

内部で生成された SSL 証明書の結果は、セキュリティインシデントレコードに表示されます。

プライマリ SSL 証明書で完全一致が見つからなかった

ルックアップ値が複数のエントリーを返し、プライマリ証明書を識別できません。セキュリティインシデントレコードにサマリーメッセージが表示されます。

手順

1. 観測事象を表示してルックアップ結果を確認するには、操作しているセキュリティインシデントレコードを開き、作業メモを見つけます。

Example
この統合で考えられるルックアップ結果の例を示すために、次の観測事象を含むセキュリティインシデントが生成されたとします。

- community.servicenow.com
- invalidsubdomain.servicenow.com
- mail.dgnetworks.com
- servicenow.com

観測事象とルックアップ結果の場所

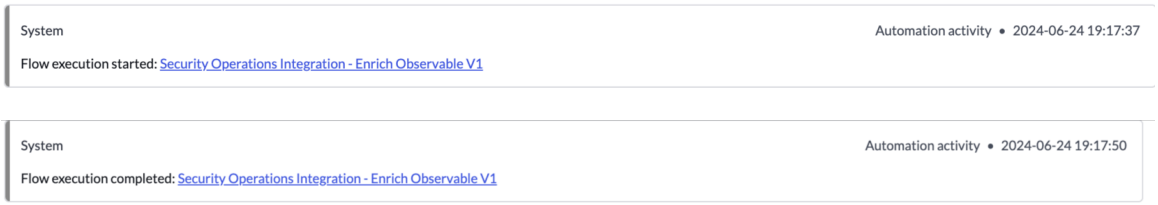
観測事象 (例)	スキャン結果	説明と場所
community.servicenow.com	SHA1 ハッシュを含む証明書が見つかりました。	完全に一致するものが見つかり、SSL 証明書の有効な発行者がリストされます。完全一致の結果が、セキュリティインシデントレコードの **[SSL** 証明書] タブに表示されます。
invalidsubdomain.servicenow.com	証明書が見つかりませんでした。	証明書の結果が見つからなかったことを示すサマリーが、セキュリティインシデントレコードの [観測事象の拡張結果] タブに表示されます。
mail.dgnetworks.com	SHA1 ハッシュを含む証明書が見つかりました。	自己署名証明書または内部で生成された証明書で完全一致がリストされます。結果が、セキュリティインシデントレコードの **[SSL** 証明書] タブに表示されます。
servicenow.com	検索により 138 個の証明書が返されましたが、1 つのプライマリ証明書を特定できませんでした。	ルックアップ値が複数の証明書を返すため、プライマリ SSL 証明書で完全一致が見つかりませんでした。プライマリ証明書が見つからなかったことを示すサマリーが、セキュリティインシデントレコードの [観測事象の拡張結果] タブに表示されます。

アプリケーションが構成されると、フローが自動的に起動します。ルックアップステータスと観測事象が作業メモに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. ルックアップが正常に実行されたことを確認します。



Trouble?
期待する結果が表示されない場合は、統合の SSL 証明書ルックアップで観測事象がサポートされていることを確認してください。

関連情報

RISKIQ および RISKIQ WHOISIQ でサポートされている観測事象

完全一致を返す **RISKIQ** の **SSL** 証明書ルックアップ

RISKIQ SSL 証明書ルックアップの完全一致の結果は、セキュリティインシデントレコードの **[SSL** 証明書] タブに表示されます。完全一致は有効な認証局名を提供します。この認証局名はセキュリティインシデントアナリストが Web サイトの妥当性を判断するのに役立ちます。

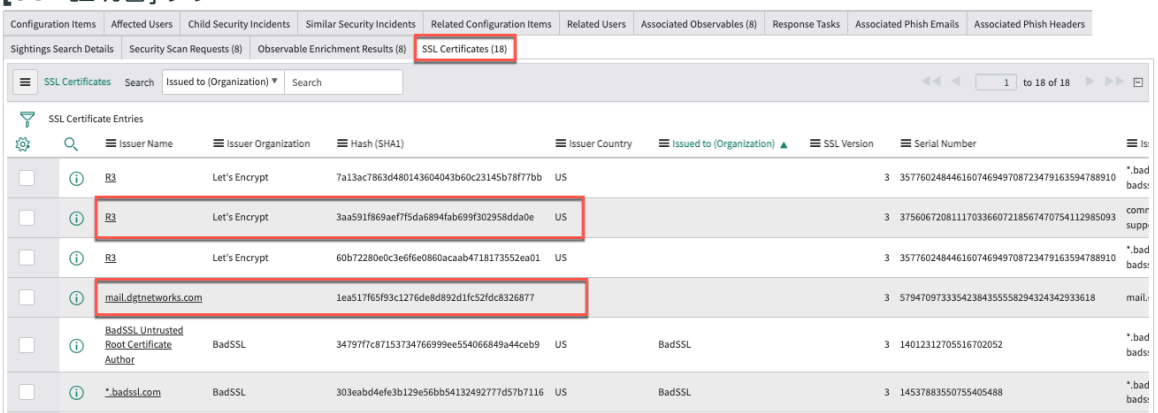
Example: 有効な **SSL** 証明書の完全一致

次の例は、ルックアップ結果の完全一致からの SSL 証明書の有効な発行者を示しています。手順に従って結果と生データを表示します。

> **注:**
> 次の例の図は、[システムの設定] で [タブ付きフォーム] 設定を有効にした状態で示されています。画面が以下の図と一致しない場合は、手順に従ってタブ付きフォームを設定します。
>
> 1. バナーフレームの右上隅にある [設定] アイコンをクリックします。
> 2. 表示される [システムの設定] ダイアログボックスで [フォーム] をクリックし、[タブ付きフォーム] と [フォームと同時] が選択されていることを確認します。

1. セキュリティインシデントレコードで、**[SSL** 証明書] タブをクリックします。

[SSL 証明書] タブ



証明書の発行者の名前、発行者の組織、および証明書の発行先 (組織) に関する情報が他のデータとともに表示されます。

[発行者名] 列に 18 アイテムが表示されています。2 番目のアイテム (R3) は、[発行組織] 列に有効な認証局名 (Let's Encrypt) が表示されています。

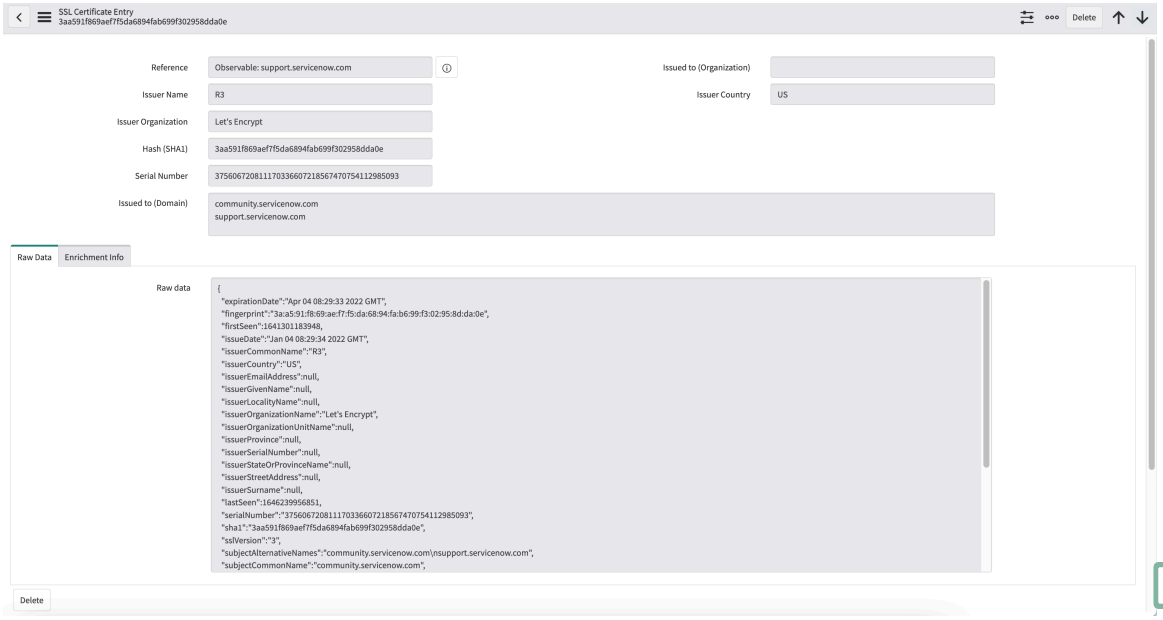
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

2 番目のアイテム (mail.dgtnetworks.com) では、[発行組織] 列と [発行先] 列に情報が表示されていません。

2. [発行者名] 列の 2 番目のアイテム (**R3**) をクリックして、エントリーレコードを開きます。または、アイテムの横の情報アイコンをクリックしてから、[レコードを開く] をクリックします。
3. [生データ] タブを選択します。

[生データ] タブ



SSL 証明書エントリーレコードでは、[エンティティ名] 列の下の [生データ] タブに、観測事象とその他のデータが表示されます。

[カテゴリ] 列の [件名] と [発行者] は、[エンティティ名] 列の認識可能なエンティティに対応しています。この証明書の発行者は、有効であり、信頼できる公的認証局からのものである可能性が高いです。また、[件名] と [発行者] は異なるエンティティであることに注意してください。これらの個別のエンティティは、証明書が、内部で署名された不明な認証局からの証明書ではないことを示します。

Example: 自己署名 **SSL** 証明書の完全一致

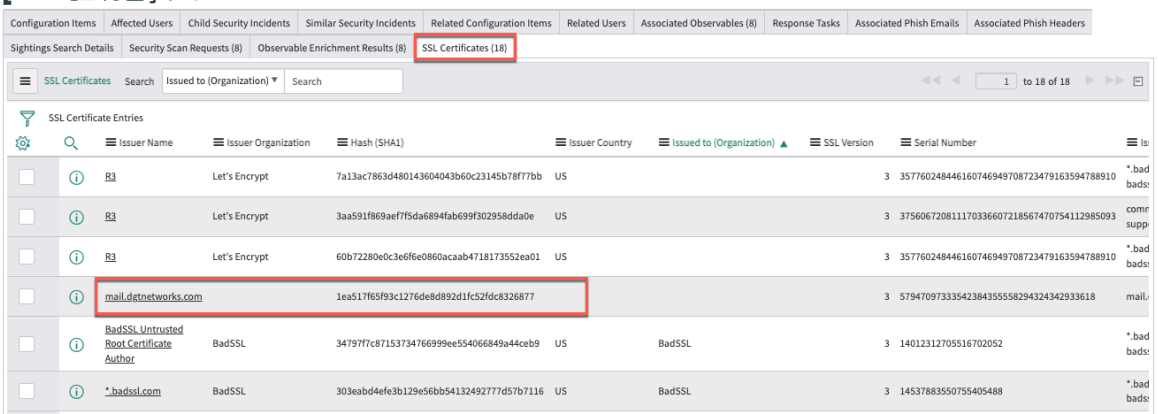
次の例は、自己署名 SSL 証明書のルックアップ結果を示しています。手順に従って結果と生データを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

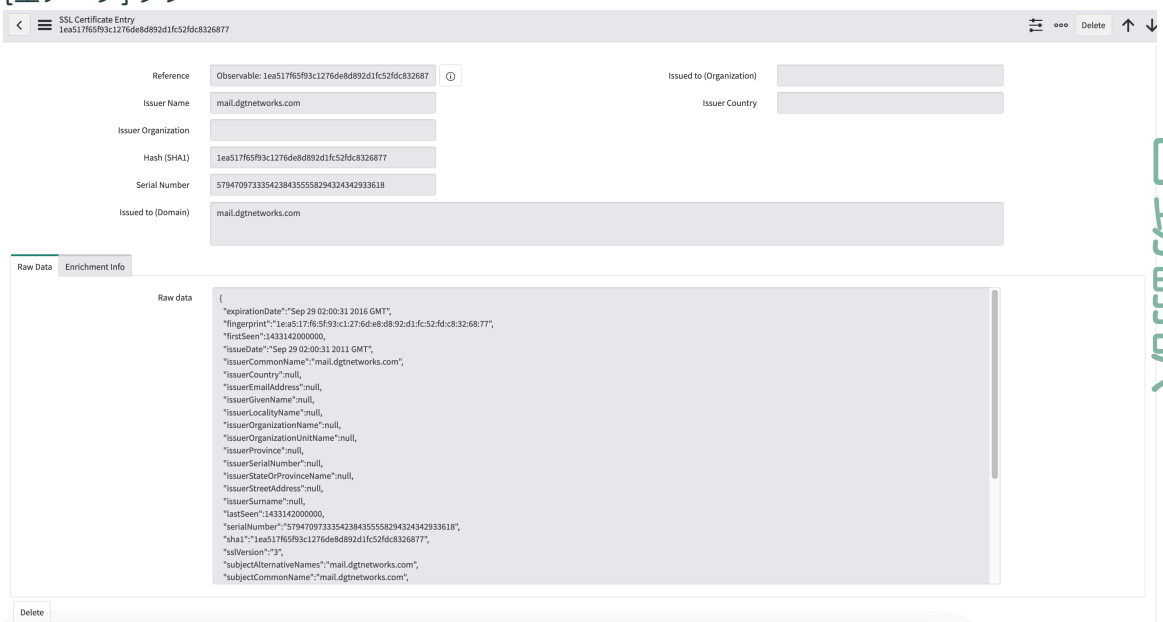
1. セキュリティインシデントレコードに戻ります。[発行者名] 列で、他のアイテム (**mail.dgtnetworks.com**) をクリックします。

[SSL 証明書] タブ



2. 開いたレコードで、[生データ] タブを選択します。

[生データ] タブ



[カテゴリ] 列は、[発行者] (mail.dgtnetworks.com および dgtsbs.DGTNetworks.local) が信頼できる公開認証局ではないことを示しています。また、[発行者] と [件名] は同じエンティティ (dgtsbs.DGTNetworks.local) であり、それぞれに観測事象の名前 (dgtsbs) が含まれています。この証明書は自己署名証明書である可能性があります。自己署名証明書は、既知の認証局によって発行されていないため、さらなる調査が必要です。

複数の証明書を返す、または証明書を返さない **RISKIQ SSL** 証明書のルックアップ

セキュリティインシデントアナリストは、複数の SSL 証明書を返す結果を利用して、サイトが共通の認識可能なエンティティの一部であるかどうかを判断できます。SSL 証明書がない場合は、あいまいまたは不審な名前のサイトに信頼できる証明書がないことを示している可能性があります。SSL 証明書を返さない、または複数の SSL 証明書を返す観測事象のルックアップ結果は、セキュリティインシデントレコードの [観測事象の拡張結果] タブに表示されます。

自動翻訳

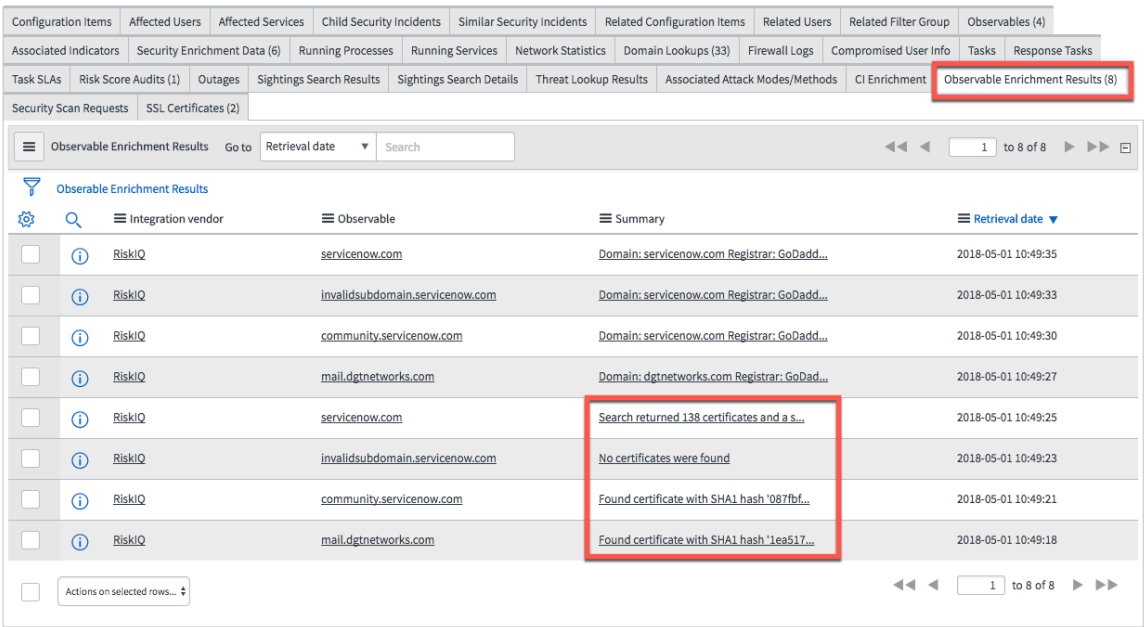
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Example: SSL 証明書がない、または複数の SSL 証明書を返す結果

SSL 証明書を返さない、または複数の証明書を返す観測事象の結果を表示するには、次の手順に従います。

1. セキュリティインシデントレコードで、[観測事象の拡張結果] タブをクリックします。

[観測事象の拡張結果] タブ



RISKIQ および WHOISIQ ルックアップの観測事象の拡張結果が表示されます。

[観測事象 **(Observable)**] 列の、servicenow.com は、[サマリー] 列の「検索で 138 件の証明書が返されました (Search returned 138 certificates)」メッセージに対応します。同様に、invalidsubdomain.servicenow.com は、[サマリー] 列の「証明書が見つかりませんでした」に対応します。これらのサマリーはそれぞれ、複数の SSL 証明書が見つかったこと、完全一致する SSL 証明書が見つからなかったこと示しています。

2. [観測事象 **(Observable)**] 列で、**servicenow.com** をクリックします。

複数の **SSL** 証明書

レコードに表示されるサマリーメッセージは、servicenow.com に一致する複数の SSL 証明書が返され、プライマリ SSL 証明書を特定できなかったことを示しています。このメッセージは、servicenow.com のような一般的なドメイン名を含むルックアップで返されることがよくあります。

一般的なドメインに関する詳細情報が必要な場合は、RISKIQ API を使用して直接検索を実行できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. [観測事象の拡張結果] タブに戻り、[観測事象 **(Observable)]** 列で、**invalidsubdomain.servicenow.com** をクリックします。

SSL 証明書なし

注:

- 現在の観測事象の SSL 証明書が見つからない場合は、[サマリー] フィールドに「証明書が見つかりませんでした」というメッセージが表示されます。
- 現在の観測事象のアクティブな SSL 証明書が見つからない場合は、[サマリー] フィールドに「アクティブな証明書が見つかりませんでした」というメッセージが表示されます。

WHOISIQ URL ルックアップの期待する結果を確認する

セキュリティインシデントによって URL またはドメインの観測事象が生成されると、セキュリティインシデントの作成時に WHOISIQ API が自動的に観測事象の拡張を実行します。ルックアップの結果は、セキュリティインシデントレコードの [観測事象の拡張結果] および **[SSL** 証明書] タブに表示されます。

始める前に

注:
次の手順の図は、[システムの設定] で [タブ付きフォーム] 設定をアクティブにした状態で示されています。

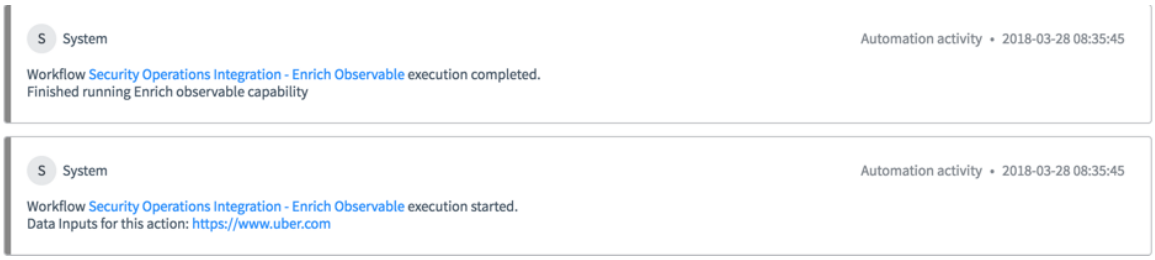
必要なロール：sn_si.analyst

このタスクについて

観測事象の拡張結果は、セキュリティインシデントレコードの下部にある [観測事象の拡張結果] タブに表示されます。サポートされている観測事象については、SSL 証明書の検索も実行され、結果が **[SSL** 証明書] タブに表示されます。

手順

1. 操作しているセキュリティインシデントレコードを開き、作業メモでルックアップが正常に実行されたことを確認します。

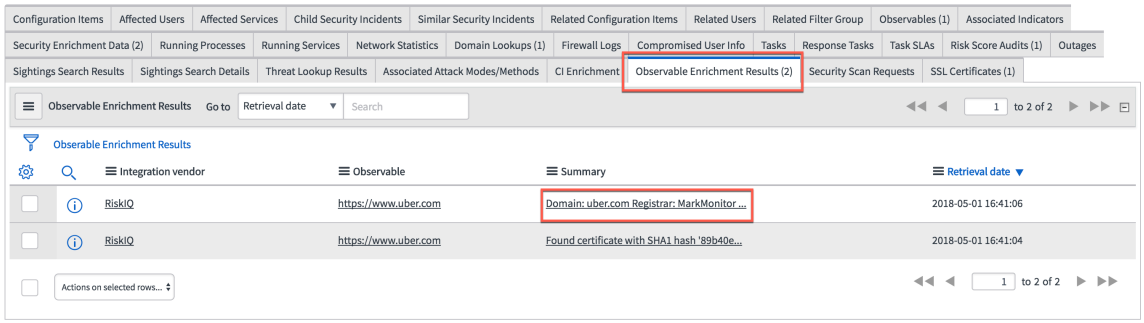


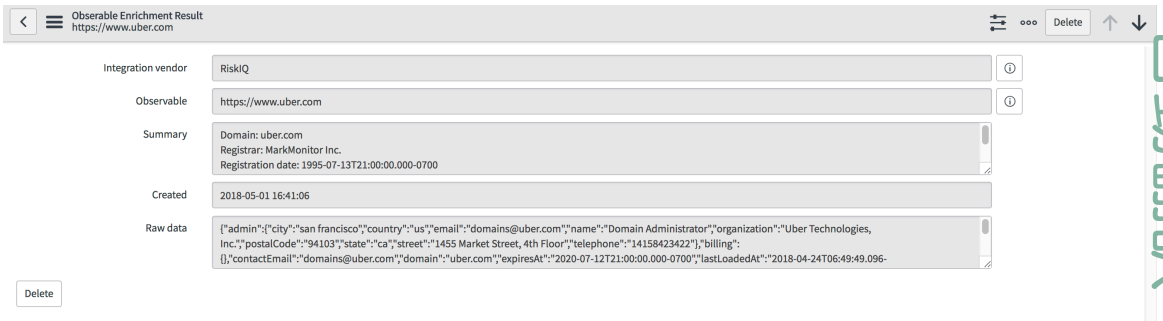
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーションが構成されると、インシデントの作成時にフローが自動的に起動します。ルックアップの実行および完了ステータスは、セキュリティインシデントレコードの作業メモに表示されます。

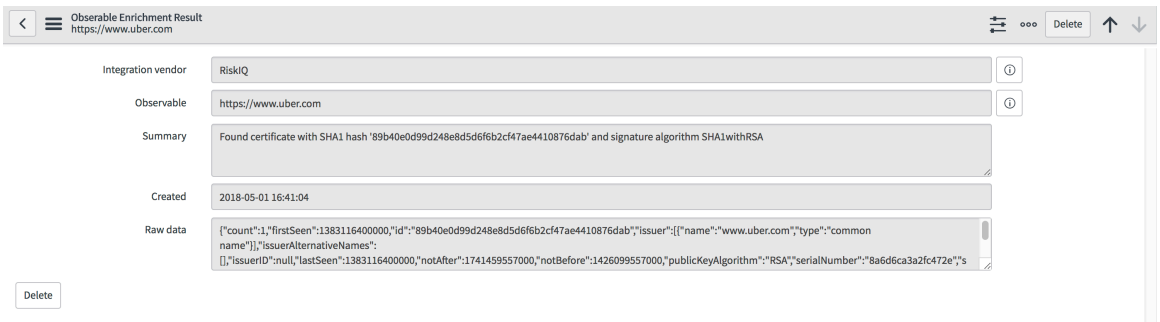
2. ルックアップが正常に実行されたことが確認できない場合は、処理方法の詳細について作業メモを確認してください。
3. オープンセキュリティインシデントで、[すべての関連リストを表示] 関連リンクをクリックします。
4. [観測事象の拡張結果] タブをクリックして選択します。
5. [サマリー] 列で、最初のアイテム [ドメイン：**uber.com** レジストラ：**Markmonitor... (Domain: uber.com Registrar: Markmonitor...)]** をクリックします。





表示されるレコードには、ドメインに関する情報が含まれています。

6. [観測事象の拡張結果] タブに戻り、[サマリー] 列で 2 番目のアイテム **[SHA1** ハッシュを含む証明書が見つかりました... **(Found certificate with SHA1 hash...)]** をクリックします。

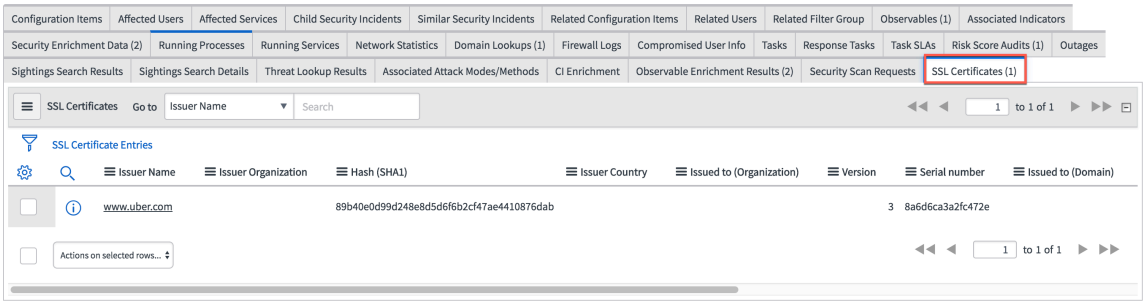


このレコードは、ファイルハッシュを含む SSL 証明書が見つかったことを示します。

7. セキュリティインシデントレコードに戻り、**[SSL** 証明書] タブをクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



ファイルハッシュの SSL 証明書の結果もここに表示されます。

Trouble?
期待する結果を表示できない場合は、作業メモを確認してください。また、観測事象が統合によるルックアップでサポートされていることを確認します。

関連情報

RISKIQ および RISKIQ WHOISIQ でサポートされている観測事象

手動 **WHOISIQ** ルックアップ用の観測事象を作成する

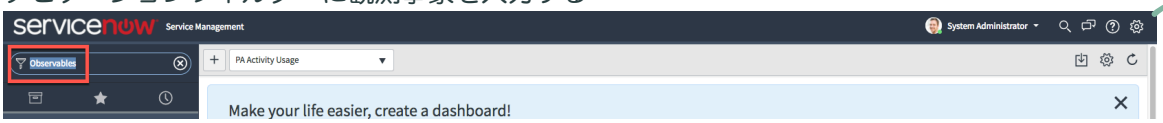
セキュリティインシデントアナリストは、WHOISIQ API による観測事象の拡張からの情報を使用して、組織のメールアドレス、名前、および電話番号の詳細を確認します。

始める前に
必要なロール：sn_si.analyst

手順

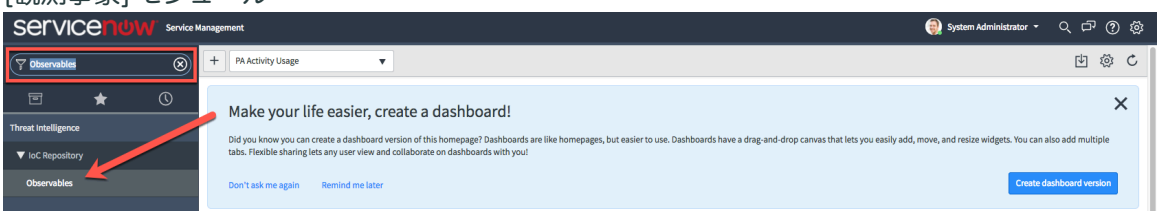
1. 次のように移動する。 **All** (すべて) > **IoC** リポジトリ > 観察事項.

ナビゲーションフィルターに観測事象を入力する



ナビゲーションパネルの下に [観測事象] モジュールが表示されます。

[観測事象] モジュール

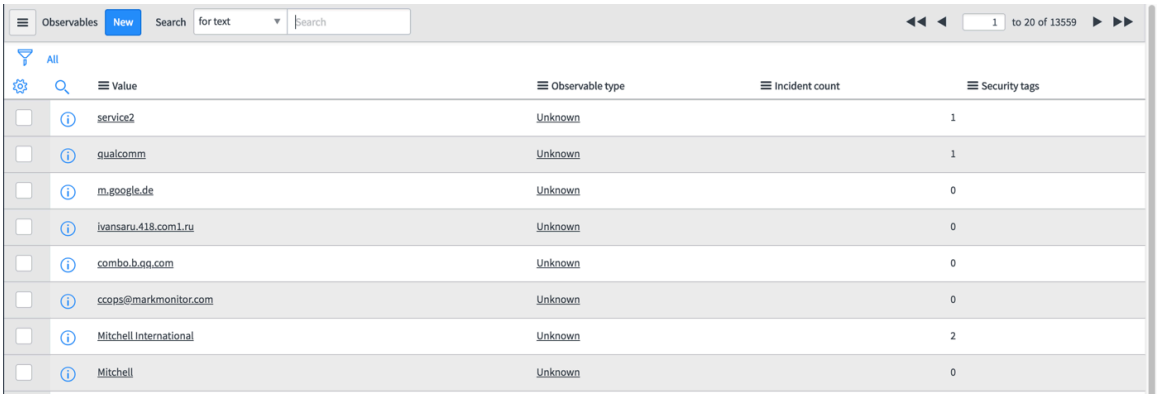


2. [観測事象] モジュールをクリックして、[観測事象] リストを表示します。

自動翻訳

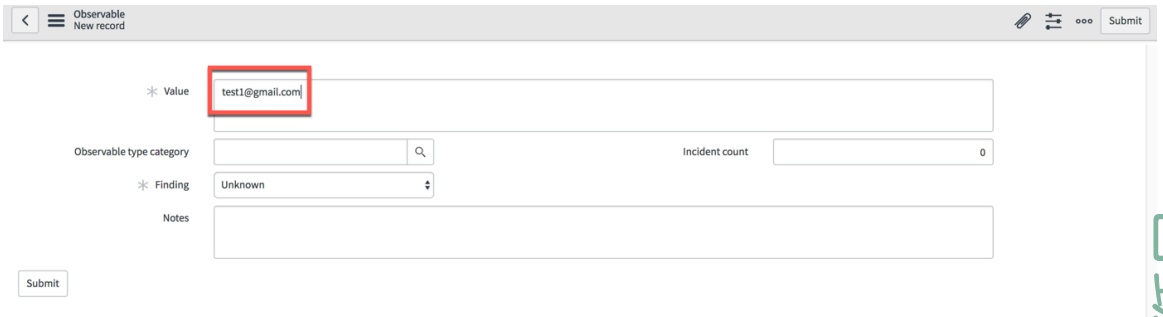
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[観測事象] リスト



3. [新規] をクリックして、新しい観測事象を作成します。
4. [観測事象] フォームのフィールドに入力します。

新しい観測事象を作成する



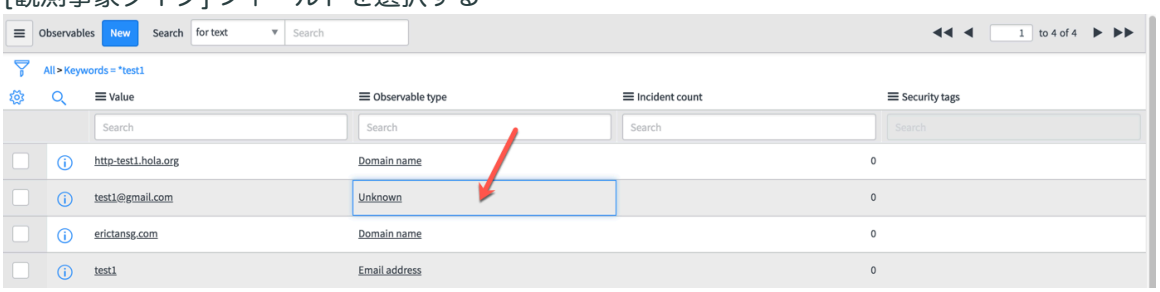
5. **[Submit]** をクリックします。
   [観測事象] リストに戻ります。[値] 列に新しい観測事象が表示されます。

   注:
   表示されているリストの一部で観測事象を見つけることができない場合は、検索機能を使用して見つけます。

6. [観測事象タイプ] フィールドを編集して、観測事象に合わせてタイプを [不明] から [メールアドレス] に変更します。

   a. [観測事象タイプ] 列で、[不明] のテキストの右側をシングルクリックして選択します。

[観測事象タイプ] フィールドを選択する



選択したフィールドが青色で囲まれます。

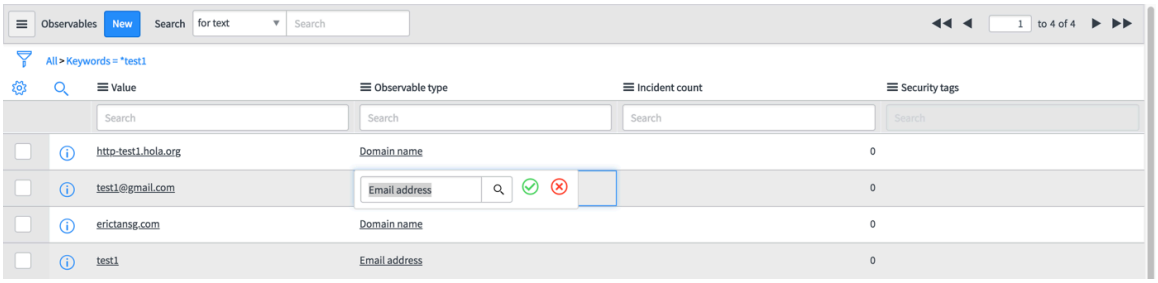
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

b. 青色で囲まれたフィールドで、ハイライト表示されたフィールド内の任意の場所をダブルクリックしてエディターを開きます。

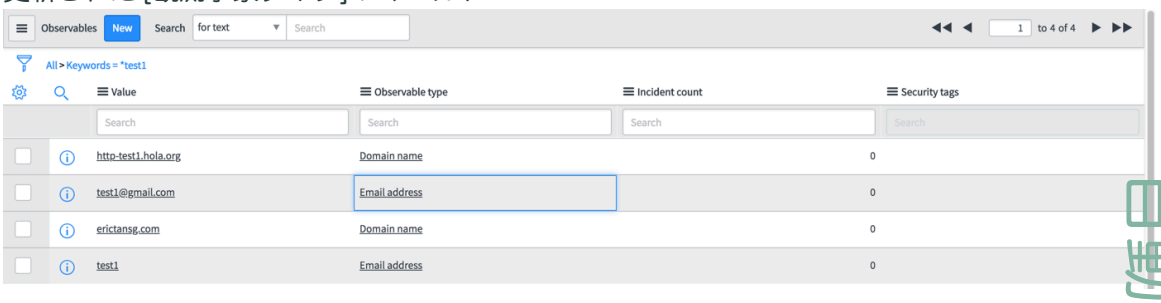
c. 表示されるフィールドに観測事象タイプ (メールアドレス) を入力し、緑色のチェックマークをクリックして値を保存します。

[観測事象タイプ] フィールドを編集する



リストの [観測事象タイプ] 列に、新しい観測事象の [メールアドレス] が表示されます。

更新された [観測事象タイプ] フィールド



次のタスク

ルックアップ用に観測事象を作成および編集した場合は、WHOISIQ API を使用して観測事象レコードから観測事象の拡張ルックアップを実行します。

手動 **WHOISIQ** ルックアップの期待する結果を確認する

セキュリティインシデントが自動的に生成されない場合は、観測事象に対して手動ルックアップを実行します。メールアドレス、組織名、電話番号、または住所に対して WHOISIQ API を使用して観測事象を拡張するには、[観測事象] テーブルから手動でルックアップを開始します。

始める前に

必要なロール：sn_si.analyst

このタスクについて

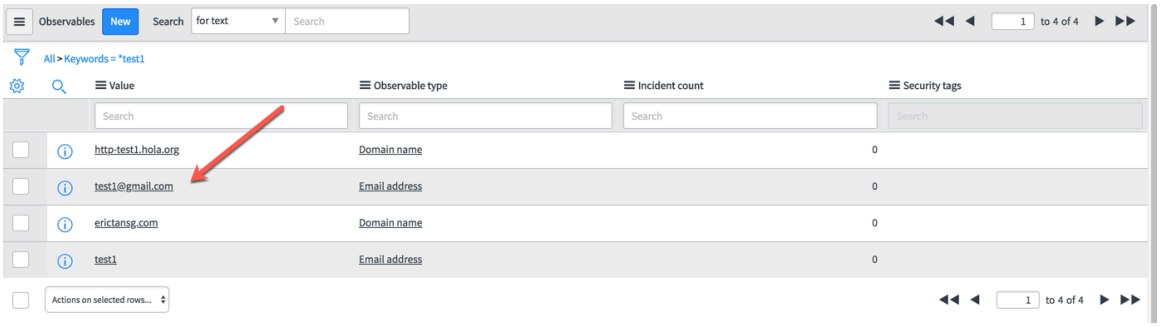
WHOISIQ API を使用して手動ルックアップ用の観測事象を作成します。観測事象を作成および編集する方法の詳細については、「手動 WHOISIQ ルックアップ用の観測事象を作成する」を参照してください。

手順

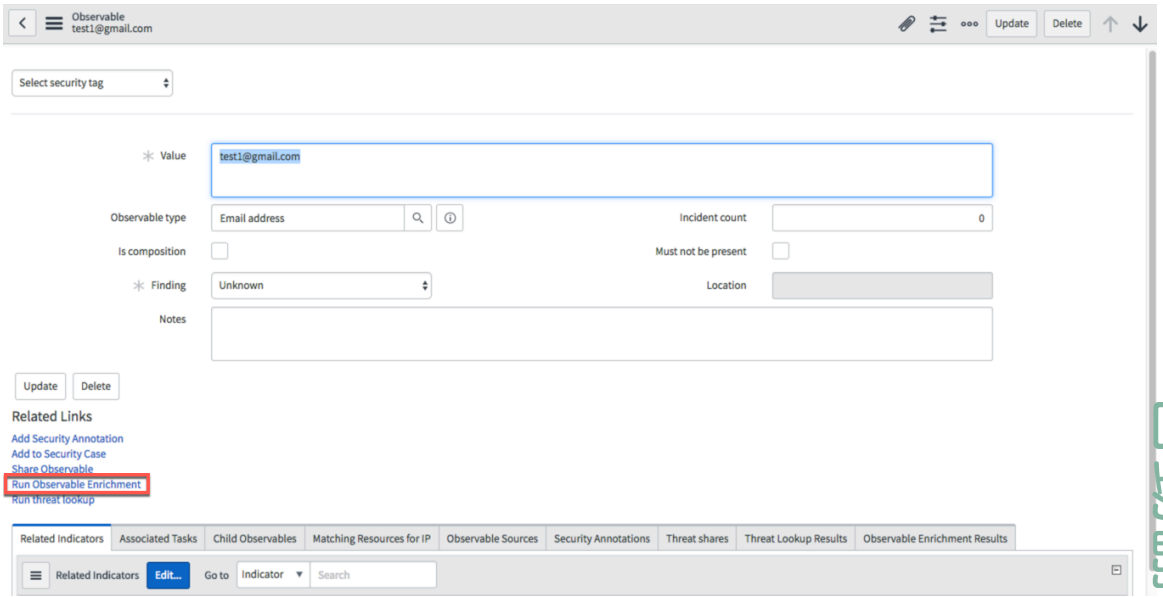
1. 次のように移動する。 **All** (すべて) > **IoC** リポジトリ > 観察事項 をクリックし、操作しているリストで観測事象を見つけます。
2. [値] 列の観測事象をクリックしてレコードを開きます。

自動翻訳

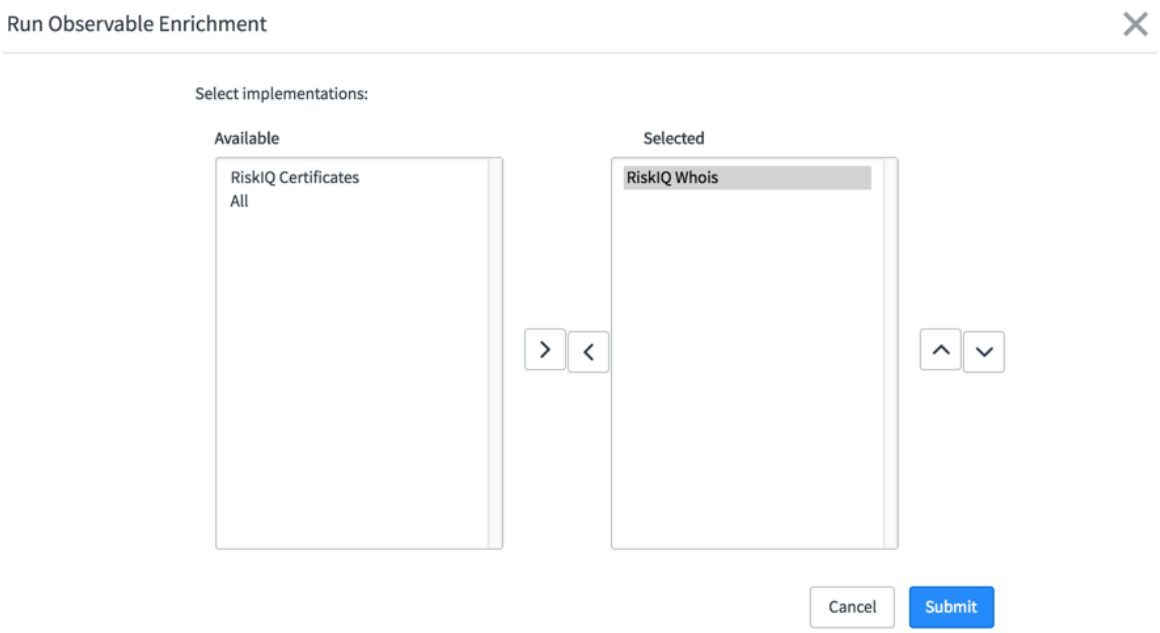
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. [観測事象の拡張を実行] 関連リンクをクリックしてルックアップを実行します。



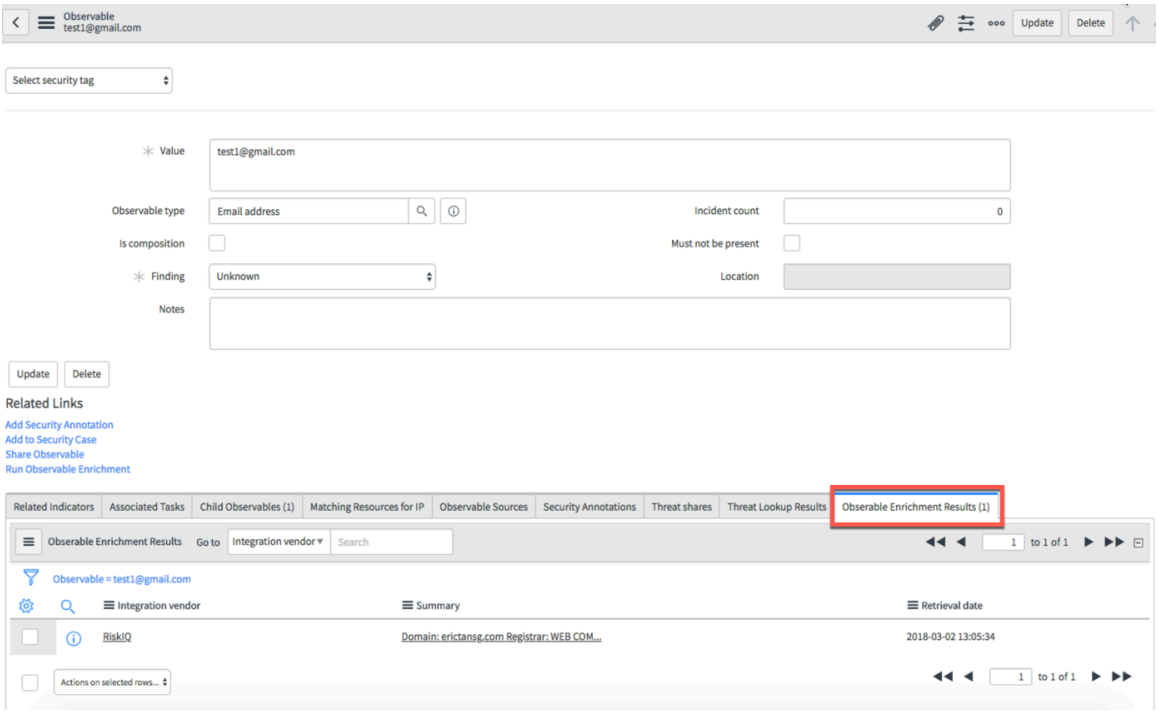
4. [観測事象の拡張を実行] ウィンドウで、**[RiskIQ Whois]** を [選択済み] リストに移動します。



5. [Submit] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ルックアップ結果は、観測事象レコードの [観測事象の拡張結果] タブに表示されます。



Trouble?
観測事象に対して結果が返されない場合は、[サマリー] 列にメッセージが表示されます。結果が表示されない場合は、観測事象が API でサポートされていることを確認してください。

関連情報

RISKIQ および RISKIQ WHOISIQ でサポートされている観測事象

Shodan の統合

Shodan は、世界中の接続されたデバイスからのサービスバナー情報を分析する検索エンジンです。サービスバナーには、ホスト名、デバイスタイプ、オペレーティングシステム、地理的な場所、接続されている ISP などのコンピューターシステムに関する情報が含まれています。Now Platform セキュリティオペレーション 製品と統合すると、このサービスバナー情報は、セキュリティインシデントまたは調査のための追加の拡張データとインサイトをアナリストに提供します。

統合には セキュリティインシデントレスポンス および 脅威インテリジェンス プラグインが必要です。

Shodan 統合は、次の観測事象で拡張を実行します。

- IP アドレス
- URL

アプリケーションは 5 分ごとに新しい観測事象をチェックします。観測事象が Shodan 統合で認識されるタイプであれば、拡張できます。

Shodan のインストールと構成

インスタンスで統合を実行する前に、インストールと構成の手順を完了して、Shodan アプリケーションが Now Platform セキュリティオペレーション と適切に統合されるようにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

セットアップタスク	説明
インスタンスに必要な Now Platform ロールが割り当てられていることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。 • システムアドミニストレーター (admin) は、アプリをインストールし、セキュリティインシデントアドミン (sn_si.admin) ロールをアサインします。 • セキュリティインシデントアドミン (sn_si.admin) は構成を監視し、期待する結果を検証します。このロールは セキュリティオペレーション モジュールにもアクセスできます。
Shodan API キーを取得します。	アカウントを作成し、Shodan Web サイト (Shodan Web サイト) から API キーを取得します。
統合用のアプリケーションをインストールする前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	Madrid リリース以降のファミリリリースでは、セキュリティインシデントレスポンス Dependency プラグイン (com.snc.si_dep) が必要です。このプラグインは、セキュリティインシデントレスポンス 製品をサポートするために必要なすべての依存関係を自動的にインストールします。統合に必要な他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。 次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。 **1.** セキュリティインシデントレスポンス **2.** Security Integration Framework **3.** Security Support Common **4.** セキュリティサポートオーケストレーション 統合のための Now Platform インスタンスのセットアップの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

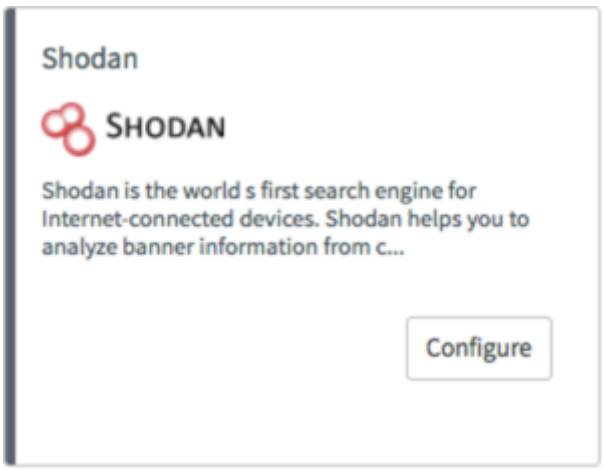
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

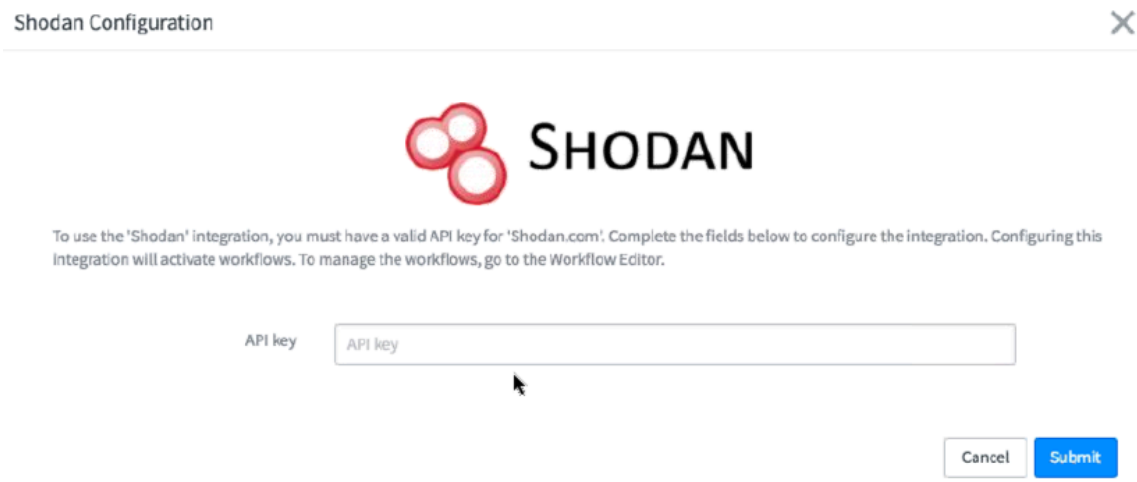
必要なロール：admin

手順

1. 統合用のアプリケーションをインストールしていない場合は、「セキュリティオペレーション 統合のインストール」を参照し、手順に従ってインストールしてください。
2. インストールが完了したら、次に移動します: 統合 > 統合構成 をクリックし、 Shodan タイルを見つけます。



3. [構成] をクリックします。
4. **[Shodan 構成 (Shodan Configuration)]** ダイアログボックスで、Shodan Web サイトから取得した API キーを入力し、[送信] をクリックします。



5. 正常に構成されていることを確認します。
エラーメッセージが表示されない限り、構成は正常に完了しています。

Trouble?

構成中にエラーメッセージが表示された場合は、 Shodan API キーが無効である可能性があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Shodan の期待される結果の確認

観測事象は、セキュリティインシデントによって自動的に生成され、アプリケーションによってスキャンされます。拡張結果は、[観測事象の拡張結果] タブと [ネットワークバナー] タブに表示されます。

始める前に
必要なロール：sn_si.analyst

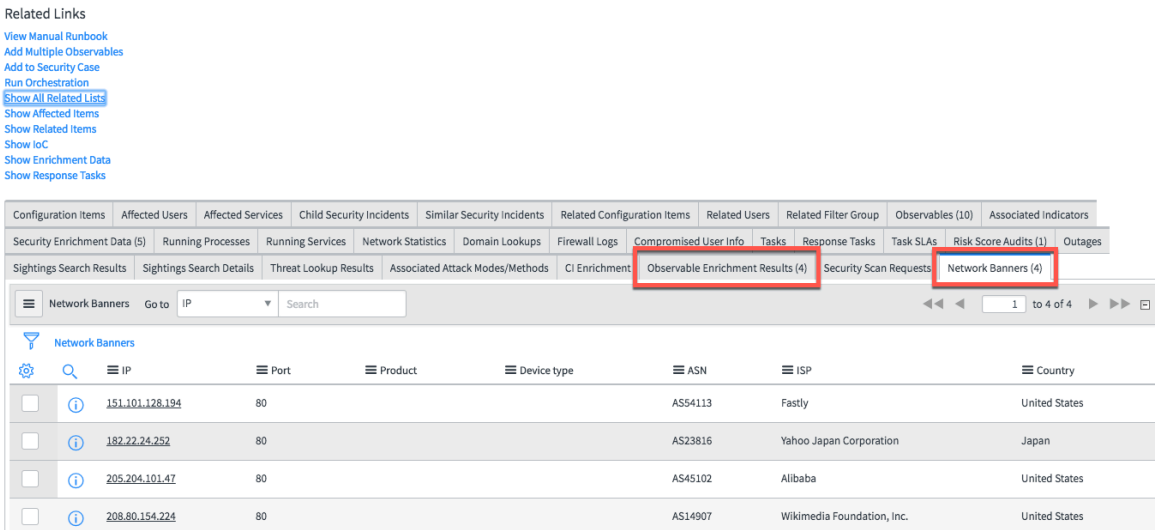
手順

1. 操作しているセキュリティインシデントを開き、ルックアップが正常に実行されたことを確認します。

アプリケーションが構成されると、インシデントの作成時にワークフローが自動的に起動します。ルックアップの実行および完了ステータスは、セキュリティインシデントの作業メモに表示されます。

2. ルックアップが正常に実行されたことを確認できない場合は、作業メモで詳細と対処方法を確認してください。
3. セキュリティインシデントの下部に移動し、[関連リンク] の [すべての関連リストを表示] リンクをクリックします。

> **注:**
> 次の手順の図は、[システムの設定] で [タブ付きフォーム] 設定をアクティブにした状態で示されています。タブ付きフォームが表示されない場合は、バナーフレームの右上隅にある [設定] 歯車アイコンをクリックします。表示される [システムの設定] ダイアログボックスで [フォーム] をクリックし、[タブ付きフォーム] と [フォームと同時] が選択されていることを確認します。



結果は、セキュリティインシデントの下部にある [観測事象の拡張結果] タブと [ネットワークバナー] タブに表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

4. [ネットワークバナー] タブを選択した状態で、観測事象の横にある青色の情報アイコンをクリックします。

5. 表示されるダイアログボックスで、[レコードを開く] をクリックして生データと詳細を表示します。

Trouble?
[観測事象の拡張結果] タブと [ネットワークバナー] タブの下に結果が表示されない場合は、観測事象が統合によるルックアップでサポートされているタイプであることを確認します。

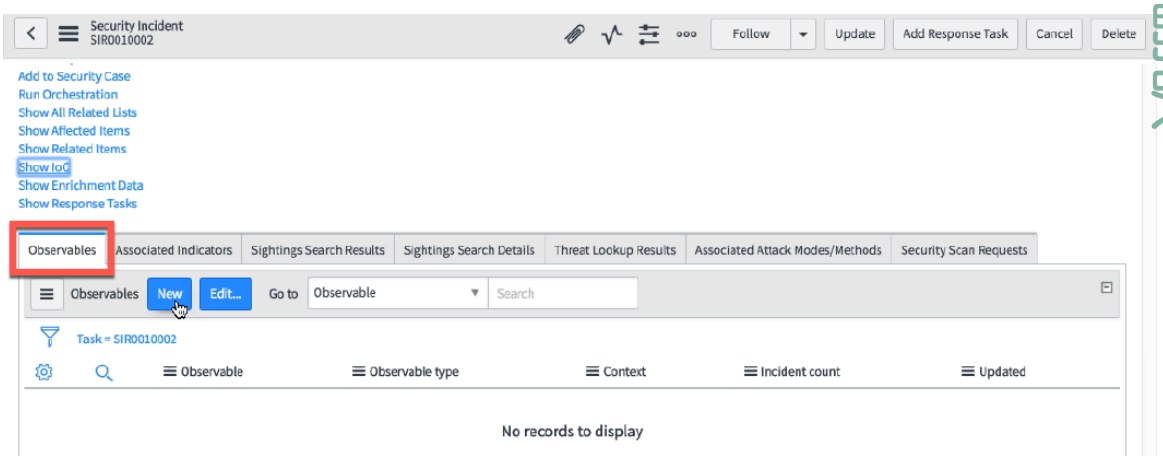
(オプション) **Shodan** の観測事象を手動で添付する

観測事象をセキュリティインシデントに手動で添付することができます。最初のイベントトリガーでセキュリティインシデントに添付されていない観測事象に対して脅威のルックアップを実行する場合は、観測事象を手動で添付します。また、関連する観測事象に関する詳細情報が必要な場合にも、このタスクを実行します。

始める前に
必要なロール：sn_si.analyst

手順

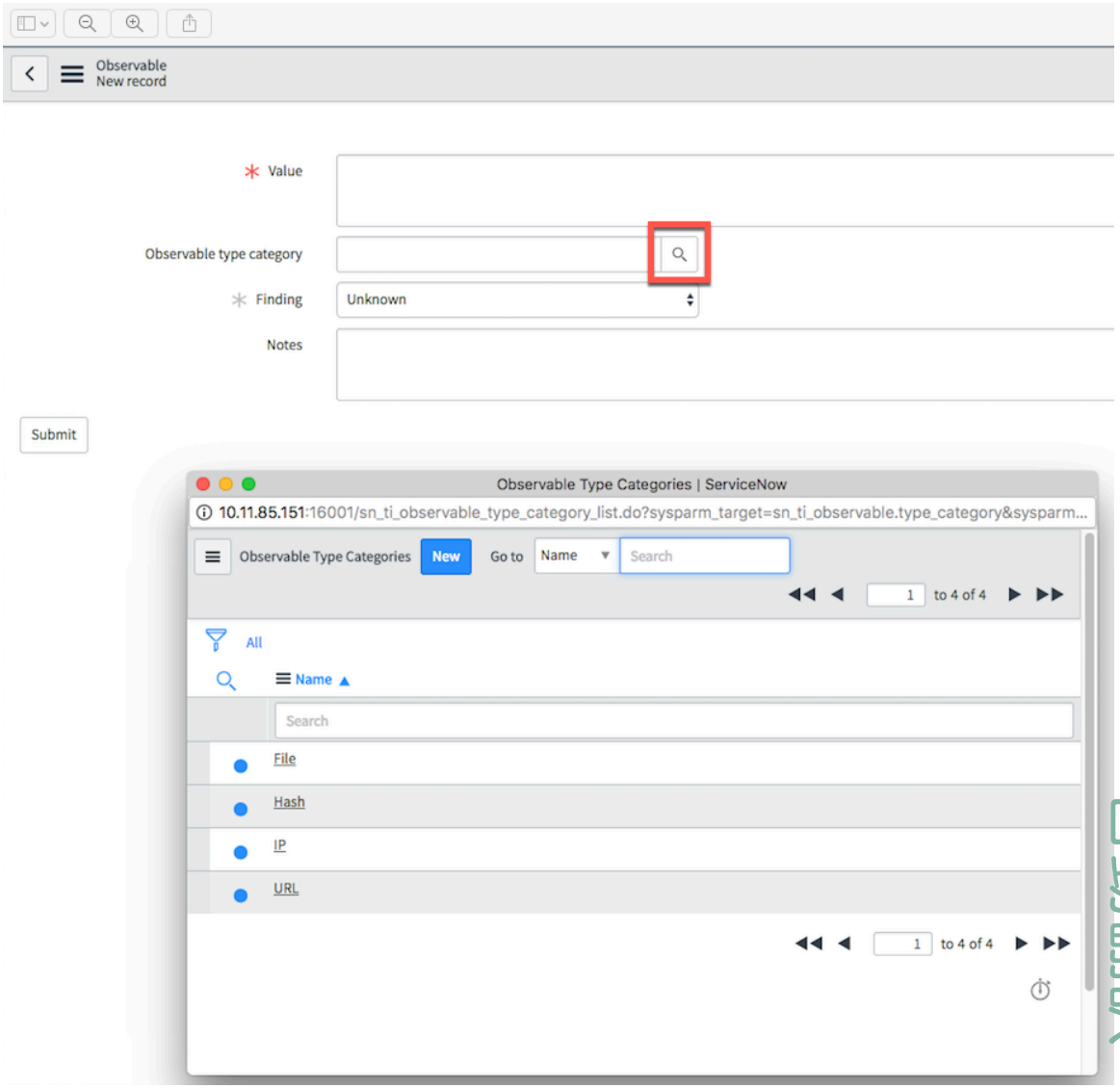
1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデント > すべてのインシデントを表示 をクリックし、観測事象を添付するセキュリティインシデントを開きます。
2. レコードの下部で、[関連リンク] の **[IoC** を表示] リンクをクリックします。



3. [観測事象 **(Observables)]** タブで、[新規] をクリックします。
観測事象フォームが表示されます。
4. [値] フィールドに観測事象 (IP アドレスまたは URL) を入力します。
5. 検索アイコンをクリックし、[観測事象タイプカテゴリ] ダイアログボックスからリストで目的の観測事象タイプをクリックしてフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

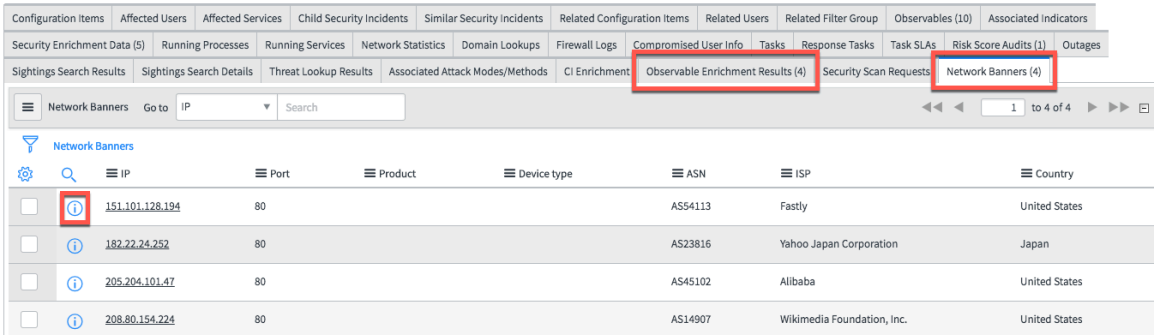


6. **[Submit]** をクリックします。
   ワークフローが起動し、新しい観測事象がチェックされます。実行および完了ステータスは、[セキュリティインシデント] レコードの作業メモセクションに表示されます。
7. セキュリティインシデントに移動し、作業メモを確認します。

8. レコードの下部で、[すべての関連リストを表示] 関連リンクをクリックします。
9. [観測事象のエンリッチメント結果] タブまたは [ネットワークバナー] タブをクリックして結果を表示し、観測事象の横にある青色の情報アイコンをクリックすると、特定のアイテムの詳細が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



10. 表示されるダイアログで、[レコードを開く] をクリックして生データと詳細を表示します。
11. オプション: 検索アイコンの近くにある青色の設定アイコンをクリックして、列の出力と順序をカスタマイズします。
12. [リストの列をカスタマイズ] で利用可能な設定を選択し、[選択済み] 列に移動して、**[OK]** をクリックします。

Trouble?
ルックアップが正常に実行されたことを確認できない場合は、作業メモで詳細と対処方法を確認してください。

Secureworks CTP チケット取り込み統合

Secureworks Counter Threat Platform チケット取り込み統合により、Secureworks CTP チケットを自動的にフェッチして、セキュリティインシデントに変換し、自動応答アクションを実行することができます。

この統合の主な機能には次が含まれます。

- 事前定義されたスケジュールに基づく、選択されたチケット (添付ファイルを含む) の自動取り込み。
- チケットフィールドとイベントフィールドの セキュリティインシデントレスポンス フィールドへのマッピング。
- チケットフィールドにマッピングされたセキュリティインシデントのプレビュー。
- チケットのフィルタリングと集計。
- チケットに関連付けられたイベントのオンデマンド取得。
- チケットの重要な更新の定期的な追跡。
- SIR インシデント状況に基づくチケットの更新とクローズの自動化。
- マスターチケットの更新。
- Secureworks 作業ログと セキュリティインシデントレスポンス 作業メモの同期。

Secureworks CTP チケット取り込み統合での Now Platform インスタンスの設定

次のセクションでは、ServiceNow Store からアプリケーションをインストールする前に Now Platform インスタンスで完了する必要があるセットアップタスクを示します。

始める前に
必要なロール：sn_si.admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
スムーズなインストールと構成を行うために、 アプリケーションをダウンロードしてインストールする前に、次のテーブルを参照して、リストされたすべてのタスクを完了していることを確認してください。

セットアップタスク	説明
必要な Now Platform ロールと セキュリティインシデントレスポンス ロールがアサインされていることを確認します。	Now Platform インスタンスで統合をインストール、セットアップ、および使用するには、次のロールが必要です。 • Now Platform アドミン (admin) ロールを持つユーザーが ServiceNow Store からアプリケーションをインストールし、SIR アドミン (sn_si.admin) ロールをアサインします。 • sn_si.admin ロールを持つユーザーは、Now Platform で次のタスクを監督します。 ○ プロファイルに名前を付け、作成し、編集します。 ○ Secureworks CTP チケットフィールドを選択して、セキュリティインシデントフィールドにマッピングします。 ○ 構成を確定する前に、正確性を確認するためにセキュリティインシデントの詳細をプレビューします。 ○ 進行中のチケットの取り込みをスケジュールします。 ○ SIR SIRインシデントが作成されてクローズされたときに、チケットの更新を有効にします。 ○ セキュリティインシデントアナリスト (sn_si.analyst) ロールをアサインします。 ○ sn_si.analyst を持つユーザーは、セキュリティインシデントを処理します。 ロールとユーザーへのロールのアサインの詳細については、「Managing roles」を参照してください。
次のバージョンを使用していることを確認します。 • Secureworks Ticket API 4.0 • Secureworks Event API 1.0 • Secureworks Enrichment API 1.0	Secureworks CTP ポータルへのアクセス権がある場合は、この統合に必要な API にアクセスできます。API に必要なその他の特別なセットアップはありません。
統合用のアプリケーションをインストールする前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	1. セキュリティインシデントレスポンス 2. セキュリティオペレーション のイベントとアラートの取り込み (SIEM 統合に必要)：このアプリケーションでは次のものが必要です。 ○ com.glide.hub.integration.runtime => ServiceNow 統合ハブランタイム ○ com.glide.hub.action_step.rest => ServiceNow 統合ハブアクションステップ - REST **注:** Integration Hub コンポーネントは、イベントおよびアラートの取り込みプラグインとともにインストールされます。これらがインストールされていない場合は、 カスタマーサポートに連絡してください。 セキュリティオペレーション コアアプリケーションのインストールの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

Secureworks CTP チケット取り込み統合用の **ServiceNow** アプリケーションのインストールと設定

Now Platform インスタンスで統合を実行する前に、これらのインストールと構成のステップを完了して、Now Platform インスタンスでアプリケーションが セキュリティインシデントレスポンス と セキュリティオペレーション 製品と適切に統合されるようにします。

始める前に
必要なロール：sn_si.admin

手順

1. ServiceNow Store から統合用の Secureworks CTP チケットアプリケーションをインストールしていない場合は、「セキュリティオペレーション 統合のインストール」を参照し、ステップに従ってインストールします。
2. アプリケーションのインストールが完了したら、 統合 > 統合構成 をクリックし、[Secureworks CTP チケット取り込み統合] タイルを見つけます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

の設定

3. アプリケーションを設定するには、[新規] をクリックします。
4. または、[構成] ボタンがタイルに表示されている場合は、そのボタンをクリックして既存の構成を編集します。
5. 表示されるダイアログで、フィールドに入力します。

6. **[Submit]** をクリックします。
   検証と送信が正常に完了すると、各構成は [セキュリティ統合] ページにタイルとして保存されます。

タスクの結果

保存された構成タイルが [セキュリティ統合] ページに表示されない場合。ページの右上隅にある [構成を表示] 選択リストで [はい] をクリックします。

Secureworks CTP チケット取り込み統合用のプロファイルの作成

Now Platform インスタンスにプロファイルを作成し、取り込む必要があるチケットと、セキュリティインシデントの作成に使用するチケットを指定します。セキュリティインシデントが取り込まれたチケットから作成される前に、チケットのフィールド値が Now Platform セキュリティインシデントのレイアウトに表示されるため、実際のセキュリティインシデントがどのように表示されるかをプレビューできます。

この統合により、インスタンスの セキュリティオペレーション 環境で設定したプロファイルに基づいてチケットを取り込むことができます。すべてのチケットは、最初にプロファイル内の設定されたチケットタイプに対して取り込まれます。取り込まれたチケットをさらにフィルタリングして、セキュリティインシデントを作成するチケットを指定できます。

たとえば、高リスクとして識別されたチケットに対してのみセキュリティインシデントを作成するフィルターを使用できます。プロファイルがアクティブになり、取り込まれたチケットからセキュリティインシデントが作成される前に、個々のフィールド値が、プレビュー用のセキュリティインシデントのレイアウトの対応するフィールドにマッピングされます。

プロファイルのソースの識別

プロファイルの名前とソースを指定します。

始める前に

必要なロール：sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

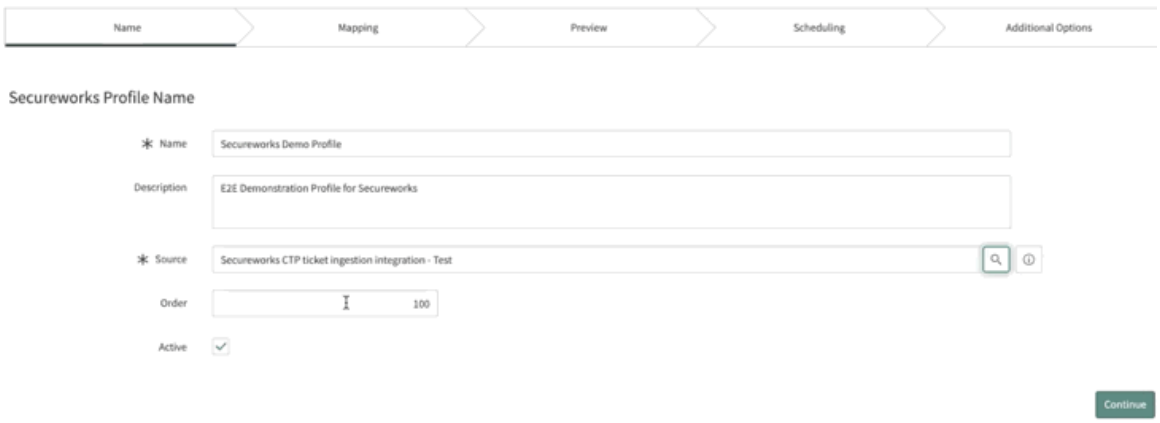
手順

1. Now Platformインスタンスでチケットのプロファイルを作成するには、次に移動します: **Secureworks** チケット取り込み統合 > **Secureworks** プロファイル.
2. [**New**] をクリックします。
3. フィールドに入力します。

   完成したフォームの例が表の後に表示されます。

フィールド	説明
名前	プロファイルの一意の名前。名前が一意でない場合、エラーが表示され、重複するプロファイル名は保存されません。 Now Platform インスタンスのプロファイル名は一意である必要があります。
ソース	データを取り込むソースを選択します。
順序	デフォルトは 100 です。 複数のプロファイルを作成した場合、この値は、2 つ以上のプロファイルが同じトリガー条件を共有する場合の実行時の優先度を示します。順番の値が低いほど、優先度が高くなります。
アクティブ	このオプションはデフォルトでクリアされています。このオプションを無効にすると、プロファイルは非アクティブになります。 **注:** アクティブにする前に、プロファイルのすべてのセクションを完了する必要があります。

次の図は、完成したフォームの例です。



次のタスク
チケットフィールドをマップします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

SecureWorks CTP 統合のためのチケットフィールドのマッピング

チケットフィールドとイベントフィールドをセキュリティインシデントフォームのフィールドにマッピングします。

マッピングステップでは、まずサンプルチケットを取り込み、関連するすべてのチケットフィールドが セキュリティインシデントレスポンス フォームの適切な場所にマッピングされていることを確認してから、プレビューセクションでセキュリティインシデントを可視化する必要があります。

サンプルチケットフィールドのマッピングには、次の手順が含まれます。

- サンプルデータのフェッチと入力：「サンプル Secureworks チケットの取り込み」を参照してください。
- セキュリティインシデントへのチケットフィールドのマッピング：「Secureworks チケットフィールドの セキュリティインシデントレスポンスフィールドへのマッピング」を参照してください。

サンプル Secureworks チケットの取り込み

取り込むサンプルチケットを選択します。

始める前に

必要なロール：sn_si.admin

手順

1. このマッピングフォームが表示されない場合は、進捗状況バーの [マッピング] をクリックします。
2. 最新の 5 つのサンプルチケットをプルするか、マッピングエクスペリエンスに使用する特定のチケットに一意のチケット ID を指定できます。
   [取り込み設定] 選択リストから、次のいずれかを選択します。
   - 最新のチケットを取得：最新の 5 つのチケットが取得されます。
   - チケット ID に基づいてチケットを選択：取得するチケットのチケット ID を指定します。最大 5 つのチケット ID をカンマで区切って指定できます。
3. [サンプルデータをフェッチ] をクリックして、Secureworks CTP サーバーから最新のサンプルチケットデータをプルします。
   サンプルチケットのプルには少し時間がかかる場合があります。トランザクションが機能していることを示すメッセージが画面の上部に表示されます。取得されたチケットは個々のタブとして表示されます。チケットデータを表示するには、タブをクリックします。各チケットについて、チケットのフィールドとその値、およびチケットをトリガーした貢献イベントの詳細を表示できます。

   注:
   過去 7 日間に発生した貢献イベントの詳細のみが表示されます。7 日より古いイベントは表示されません。

次のタスク

サンプルデータをフェッチした後の次のステップでは、チケットフィールドをセキュリティインシデントにマップします。

Secureworks チケットフィールドの セキュリティインシデントレスポンスフィールドへのマッピング

個々のチケットフィールドまたはイベントフィールドを Now Platform SIR セキュリティインシデントのフィールドにマッピングします。

自動翻訳

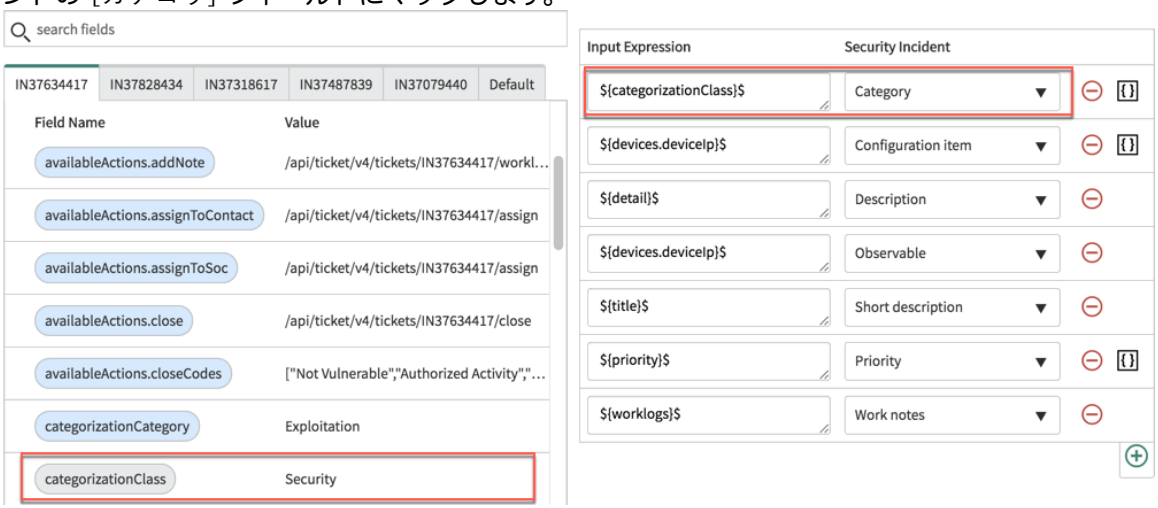
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チケットフィールドのマッピング

sn_si.admin ロールを持つユーザーとして、左側の [サンプルチケット] セクションからフィールドを使用し、**[SIR** インシデントフィールドマッピング] 列の [セキュリティインシデント] フィールドにマップします。左側からチケットフィールドまたはイベントフィールドをドラッグして、右側の [SIR インシデントマッピング] セクションにドロップして、マッピング構成を編集します。右側のマッピングで、[受信チケット] フィールドを [送信セキュリティインシデント] フィールドに関連付けることができます。

1. フォームの左側からフォームの右側のセキュリティインシデントのフィールドにフィールド値をマッピングするには、フォームの左側で青色のフィールド名をクリックしたままにします。
2. [入力式] 列にフィールド名を手動で入力するか、フィールド名をドラッグアンドドロップできます。たとえば、description を [セキュリティインシデント] 列のフィールド名の横にある [入力式] 列のフィールドにドロップします。

   フィールド値が [入力式] 列に表示されます。次の画像で、categoryClass をセキュリティインシデントの [カテゴリ] フィールドにマップします。



> **注:**
> [入力式] セクションに手動でイベントフィールド名を入力する場合は、マップされるフィールドの名前の前に *${Event:eventfield}$* というプリフィックスを追加する必要があります。

マッピングプロセスでチケットフィールドまたはイベントフィールドが見落とされたり、重複したりしないようにするために、フィールドは色分けされています。マップされていない残りのフィールドはすべて青で表示されるのに対し、すでにマップされたフィールドはグレー表示されるため、チケットフィールドの色分けは、マップされたチケット値の追跡に役立ちます。色分けすることで、セキュリティインシデントに追加されたフィールド値、およびマップされていない残りの重要なチケット情報を視覚的に把握できます。

左側のライトブルーのフィールドは、チケットフィールドがまだ未選択で、セキュリティインシデントにマップされていないことを示します。受信チケットフィールドまたは受信イベントフィールドをセキュリティインシデントの 1 つ以上のフィールドに関連付けることができます。灰色のフィールドは、フィールドが選択され、セキュリティインシデントのフィールドにマッピングされていることを示します。この色分けは、マッピングを追跡するのに役立ちます。

3. フォームの右側のセキュリティインシデントで表示されるデフォルトフィールドにフィールドを追加するには、次のステップを実行します。

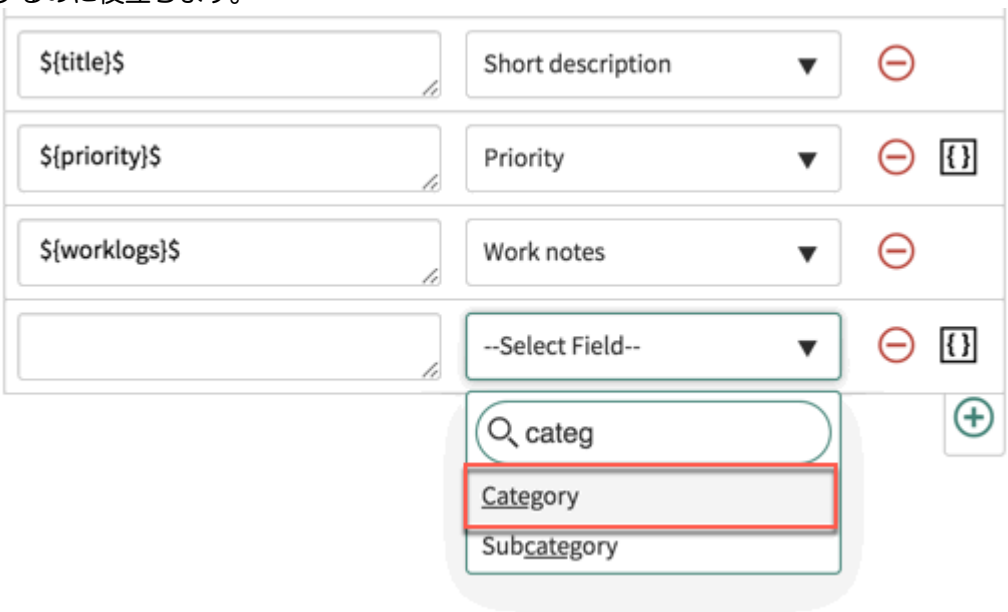
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. グリッドの下部にある [SIR インシデントフィールドマッピング] セクションのフォームの右側で、プラス (+) アイコンをクリックします。新しいフィールドが表示されます。

b. [セキュリティインシデント] 列で表示されている選択リストを展開し、フィールドを選択します。

新しいフィールドの展開された選択リストでは、一部のフィールドが網掛けされています。次の図では、セキュリティインシデントにマッピングされているため、カテゴリのバックグランドがグレーになっています。フォームの左側のチケットフィールドの色分け同様、セキュリティインシデントフィールドのこの色分けも、すでにマップされた SIR インシデントフィールドを追跡するのに役立ちます。



注:
同じセキュリティインシデントに複数の観測事象を表示できるため、[観測事象] フィールドを異なる値で複数回マップできます。同様に、[構成アイテム] フィールドと [作業メモ] フィールドは複数の値をサポートします。複数の値をサポートできないフィールドに 2 つの値をマッピングしようとすると、インシデントをプレビューするときに、フィールドに値がないことを示すエラーメッセージが表示されます。同様に、セキュリティインシデントのフィールドに複数のオプションを選択できる選択リストがあり、選択リストに表示されていないフィールドにオプションをマップしようとすると、そのフィールドはセキュリティインシデントに入力されません。

c. または、新しい行の [検索] フィールドに値を入力します。

d. フォームの左側でチケットフィールドを選択し、右側の適切なセキュリティインシデントフィールドにドラッグアンドドロップします。

4. [SIR インシデントフィールドマッピング] セクションのフィールド名の横にある - アイコンを使用してフィールドを削除します。

5. フィールドの値をマッピングに追加するか、削除して、マッピングを続行します。

フォーマットフィールド変換

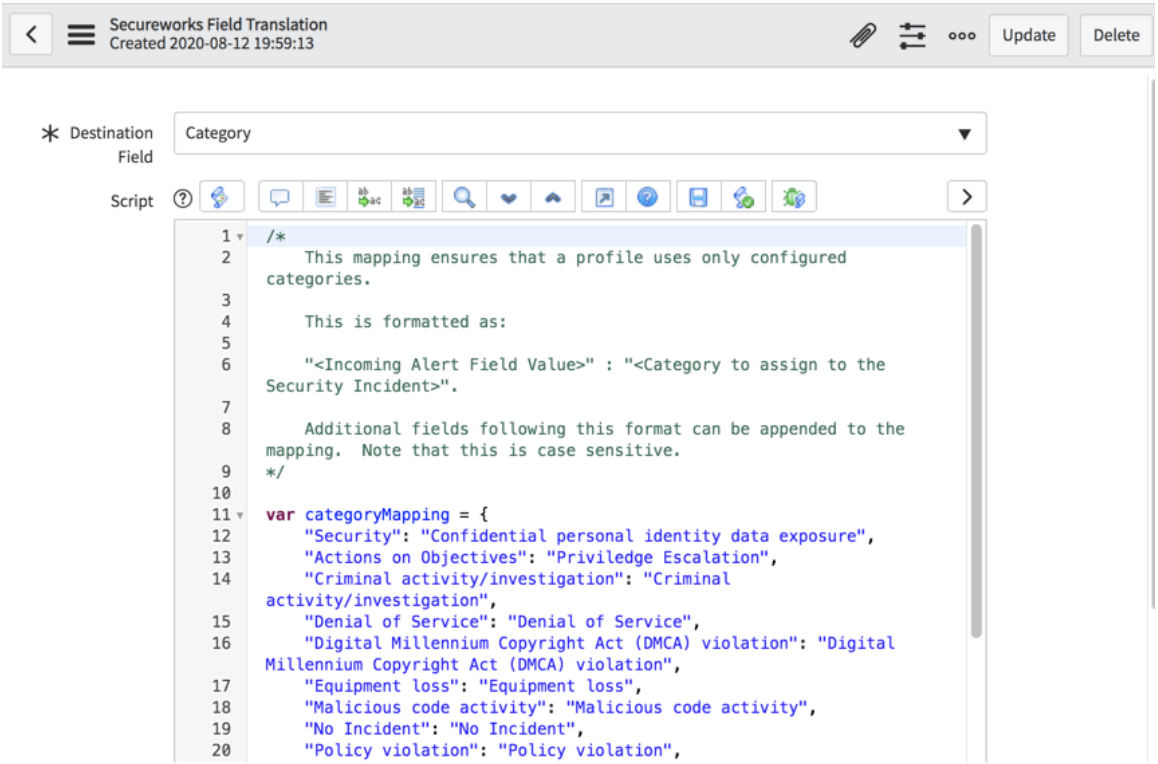
特定の場合、チケットフィールドは SIR セキュリティインシデントのフィールドに直接変換されないことがあります。これらの値については、マッピングステップでスクリプトエディターを使用してセキュリティインシデントのフィールド値をフォーマットできます。類似しているが同一ではない値をフォーマットする場合は、スクリプトエディターを使用します。たとえば、スクリプトエディターを使用すると、 [マルウェアアラート] と [ウイルス感染]のカテゴリ値でソースカテゴリのフィールド値が異なる可能性がありますが、フォーマットフィールド変換機能を使用して、SIR セキュリティイ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ンシデントの [カテゴリ] フィールドで両方の値を一般的な悪意のあるコードアクティビティに変換することができます。

スクリプトエディターを使用するには、[カテゴリ] フィールドの横にある {} アイコンをクリックします。スクリプトエディターが表示されます。



スクリプトへの変更を入力し、[更新] をクリックして変更を保存し、 [マッピング] ページに戻ります。

インシデント生成条件

マッピングセクションが完了すると、フィルター条件を設定して、セキュリティインシデントを作成するチケットとフィルタリングで除外されるチケット (低優先度の違反など) を指定できます。インシデント生成条件ビルダーで同じフィールド値を使用して、セキュリティインシデントを作成する際に受信チケットを満たす必要がある追加の条件を定義することができます。インシデント生成条件を設定するには、次のステップを実行します。

1. フォームの [インシデント生成条件] セクションまでスクロールし、[条件に基づいてフィルター] チェックボックスをオンにして、オプションを有効にします。

   フィルター条件ビルダーが表示されます。これらのフィルターを使用して、フィールドで説明されている特定の条件に一致するセキュリティインシデントを作成します。

   フィルター条件ビルダーの最初のフィールドの選択リストオプションは、取り込まれたチケットの [サンプルチケットの取り込み] セクションに表示されるフィールドと一致します。これらのフィールドは動的で、取り込むチケットに応じて変更されます。入力する条件は大文字と小文字が区別され、Secureworks CTP チケットの値と正確に一致する必要があります。フィルターフィールドに入力する値が不明な場合、Secureworks CTP コンソールに戻り、キーワードについてチケットを確認することができます。

   注:
   worklogs、*devices*、*attachments*、*watchers*、*availableactions*、*closeCodes* の各チケットフィールドには複数の値を設定できます (値はアレイに格納されます)。フィルター条件は文字列のみ取得できるため、これらのフィールドに包含フィルター条件を使用して、データが正確にフィルタリングされるようにする必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. 条件ビルダーの選択リストとフィールドを使用して、最初の行のフィルターを設定します。
3. 条件を追加するには、フィールドの右側にある [**AND**] または [**OR**] をクリックします。
   - [**AND**] を選択した場合は、すべての条件に一致する必要があります。
   - **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。
4. (オプション) 2 番目の行で、2 番目のフィルター条件を設定します。

この種のインシデント生成条件フィルタリングで、チケットを絞り込み、基本的なルールまたはフィルターを変更することなく、作成する不要なセキュリティインシデントの数を制限することができます。追加のフィルタリング条件を設定する場合、すべての条件に一致するチケットのみがセキュリティインシデントにマップされます。

類似のチケットを処理して重複インシデントを防止するチケット集計基準

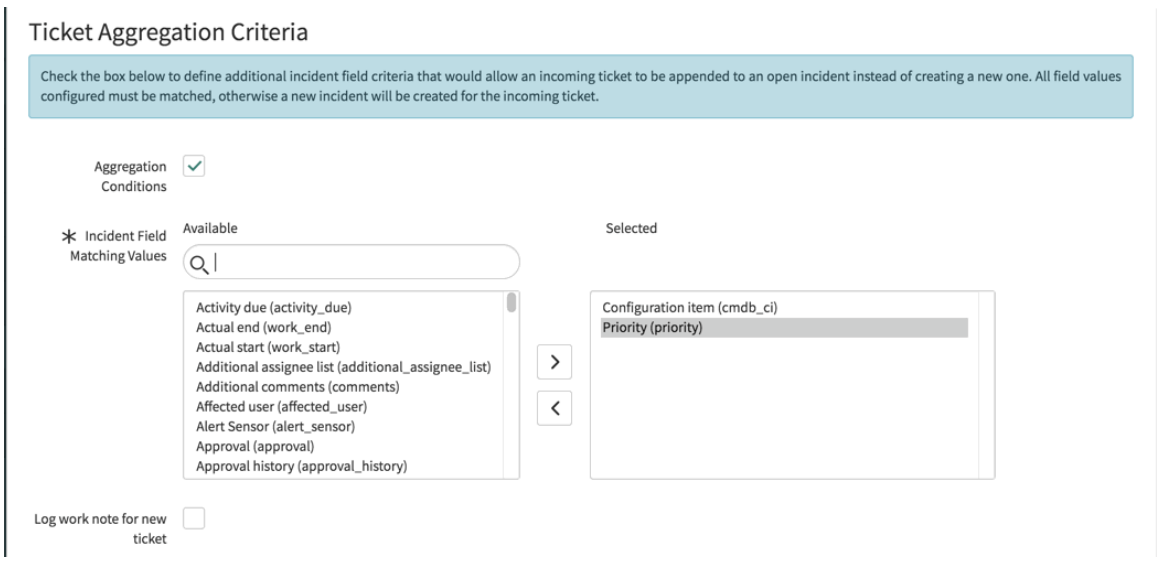
類似の重複する可能性があるインシデントを作成するのではなく、既存の SIR セキュリティインシデントに受信チケットを集計する追加のチケット違反集計基準を定義します。この追加の集計機能では、各プロファイルのフィールド一致値基準を使用して、関連するすべてのチケットデータを単一のセキュリティインシデントに配置することで、アクティブな重複するセキュリティインシデントの数を減らすことができます。基準を設定するには、以下のステップを実行します。

1. フォームで [チケット集計基準] セクションにスクロールして、[集計条件] チェックボックスをオンにして、このオプションを有効にします。

   [値が一致するインシデントフィールド] 列が表示されます。これらのフィールド名は、SIR セキュリティインシデントで構成されたカスタムフィールドを含むセキュリティインシデントのフィールドです。

2. [利用可能] リストから、Now Platform の既存のセキュリティインシデントで照合するフィールド値を選択し、[選択済み] リストに移動させます。

   この受信チケットを既存のセキュリティインシデントに追加するには、選択するすべてのフィールド値が一致する必要があります。これには、複数のチケットフィールド値がマッピングされている可能性がある [観測事象] や [構成アイテム] などのフィールドが含まれます。すべての値が一致している必要があります。値のサブセットのみが一致した場合、チケット集計条件は満たされず、新しいセキュリティインシデントが作成されます。複数値フィールドのマッピングについては、以下のスクリーンショットを参照してください。



新しいチケットが、マッピングステップの集計フィールド条件で選択されたすべての値と一致する場合、新しいチケットは、同じフィールド値を持つ最新のオープンセキュリティインシデントに自

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

動的に追加されます。セキュリティインシデントを扱う sn_si.analyst ロールを持つユーザーは、セキュリティインシデントの関連リストで、追加されたすべての集計チケットを表示できます。このリストには、関連するタイムスタンプと集計されたフィールド値の詳細が表示されます。この情報は、これらのチケットが既存のセキュリティインシデントに集計される理由を理解するのに役立ちます。このタブがセキュリティインシデントで表示されない場合は、[関連リンク] の下のレコードの左側にスクロールし、[すべての関連リストを表示] リンクをクリックします。

> **注:**
> [Secureworks 集計チケット] 関連リストは、ベースシステムでは使用できません。[関連リスト] のレイアウトを設定し、他の関連リストに明示的に含める必要があります。

3. セキュリティインシデントで最近追加された新しいチケットの作業メモを記録するには、このチェックボックスをオンにしてこのオプションを有効にします。作業メモには、新しいチケットが追加され、チケットの詳細へのリンク、およびマッピングセクションの作業メモフィールドに追加されたその他の詳細が記録されます。

   Secureworks CTP チケットからセキュリティインシデントのフィールドに値が正常にマッピングされました。また、インシデント生成フィルタリング基準を使用してセキュリティインシデントの作成を制限する追加条件も構成しました。また、チケットフィールド値が構成された集計基準に一致する場合は、追加されたチケットが既存のセキュリティインシデントに集計されました。

4. [続行] をクリックして、プロファイル設定を続行します。次のステップでは、SIR セキュリティインシデントにマッピングしたフィールドをプレビューします。

セキュリティインシデントでのマップされた値のプレビュー

マッピングステップを完了したら、SIR セキュリティインシデントでマッピングした値をプレビューします。このプレビューステップでは、セキュリティインシデントに表示するすべてのチケットフィールドがマッピングされていることを確認できます。

始める前に
必要なロール：sn_si.admin

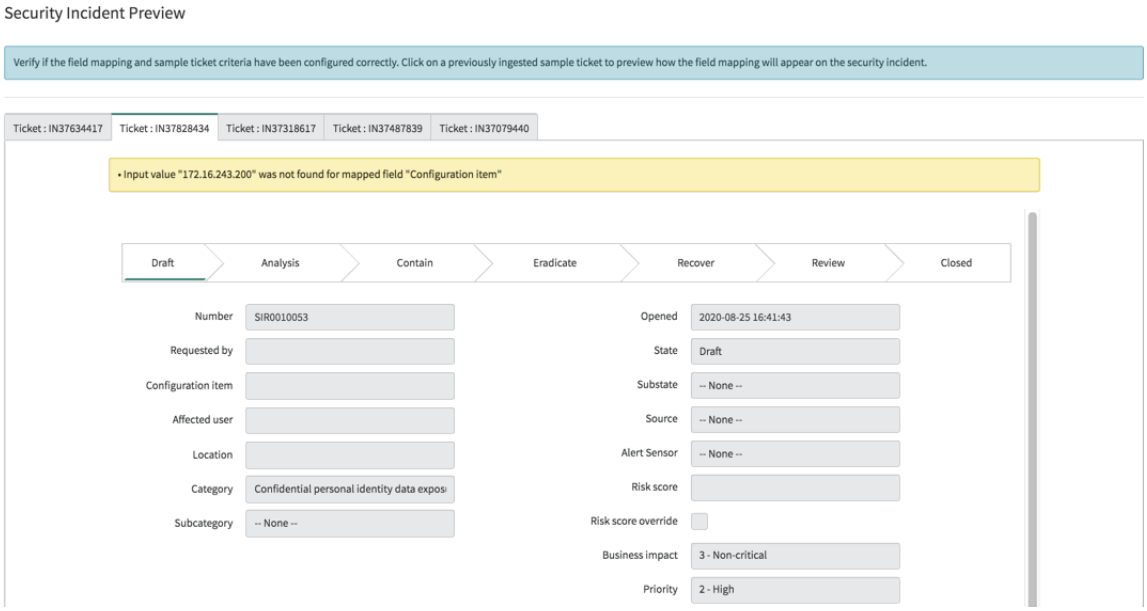
このタスクについて
セキュリティインシデントをプレビューし、必要に応じてマッピングを再編集して、エラーのあるフィールドを修正するか、欠落しているデータを入力します。プレビューが正常に完了しない場合、スケジュール設定ステップに進むことはできません。SIR セキュリティインシデントのプレビューは、セキュリティインシデントレスポンス製品の実際のインシデントとして保存されません。

手順

1. セキュリティインシデントのプレビューが表示されない場合は、進捗状況バーの [プレビュー] をクリックします。
   チケットはタブとして表示されます。
2. タブをクリックしてセキュリティインシデントをプレビューします。
   このビューは読み取り専用であり、このセキュリティインシデントのレコードは保存されません。
3. セキュリティインシデントのチケット値のフィールドマッピングを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



前の画像は、取り込まれたサンプルのマッピングエラーのあるプレビューの例です。

4. このエラーを解決するには、進捗状況バーの [マッピング] をクリックします。
5. マッピングを編集して誤った値を修正するか、欠落しているデータを入力します。
6. マッピングを再度プレビューし、エラーメッセージに記載されているエラーの修正を続行します。

次のタスク

エラーメッセージが表示されず、セキュリティインシデントのフィールドマッピングにも問題はありません。スケジュールを定義します。

Secureworks CTP チケットの取り込みスケジュールの定義

必要に応じて、チケット取得のデフォルトの設定を確認したり、スケジュールを変更したりすることができます。このステップでは、日付範囲とポーリング間隔に基づいてチケットの取得をフィルタリングできます。

始める前に

必要なロール：sn_si.admin

このタスクについて

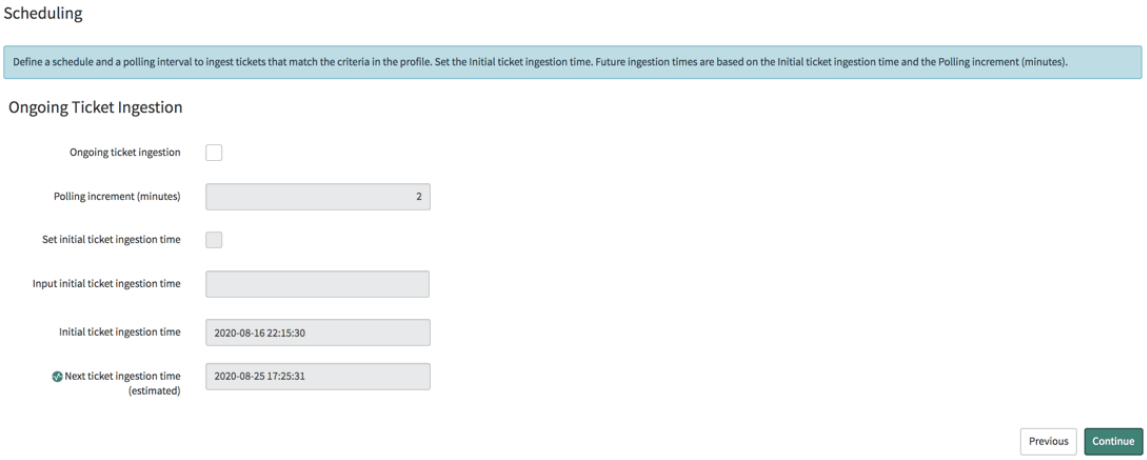
また、チケットプロファイル構成に一致する将来のチケットをポーリングする頻度も選択します。ポーリング間隔をプロファイルごとに設定します。スケジュールするときは、インシデントの緊急度とシステム負荷のバランスを取るように計画してください。1 分間のデフォルト値が任意のプロファイルに設定されますが、インシデントの緊急度とシステムの予想される負荷に基づいて変更できます。

手順

1. 進捗状況バーに [スケジュール] ページが表示されない場合は、[スケジュール] を選択します。
2. Secureworks CTP ポータルからチケットをプルする方法とタイミングをスケジュールするものを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. [続行] をクリックして、[他のオプション] ページに移動します。

SIR インシデント状況に基づくチケットの更新とクローズの自動化

Secureworks CTP チケットには、チケットからセキュリティインシデントを作成する機能と、セキュリティインシデント番号、アサイン先グループ、セキュリティインシデント URL などの関連するインシデントの詳細を使用して、セキュリティインシデントが作成および/またはクローズされるとチケットを更新する機能を許可する双方向インターフェイスがあります。

始める前に
必要なロール：sn_si.admin

手順

1. 進捗状況バーに [その他のオプション] ページが表示されない場合は、[その他のオプション] を選択します。
2. セキュリティインシデントが作成されたときにチケットを更新するための構成を完了します。

3. [完了] をクリックして構成を完了し、プロファイルを [待機中] ステータスに移行します。
確認ダイアログが表示されます。プロファイルが正常に設定されました。このプロファイルをアクティブ化して、スケジューリングに基づいて Secureworks CTP ポータルからチケットをプルします。

オプション：Secureworks CTP プロファイルのコピー

新しいプロファイルを作成する代わりに、既存のプロファイルとその関連設定をコピーします。複数のプロファイルを作成していて、既存のプロファイルの設定を再利用する場合は、時間を節約するためにプロファイルをコピーすることをお勧めします。

始める前に
必要なロール：sn_si.admin

このタスクについて
sn_si.admin ロールを持つユーザーがプロファイルをコピーすると、プロファイルの重複を避けるためにプロファイル名が最初に変更されます。また、コピーされたプロファイルは無効 (false) であるため、構成が完了する前に誤って有効になることはありません。既にプレビューおよび検証したセキュリティインシデントのプロファイルをコピーし、既存のマップを使用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > **Secureworks** チケット取り込み統合 > **Secureworks** プロファイル.
2. 表示される [Secureworks プロファイル] リストでコピーするプロファイルを選択し、[選択した行のアクション] 選択リストから [コピー] をクリックします。
   プロファイルがコピーされ、リストに表示されます。コピーには、マッピングとスケジュール設定を含む元のプロファイルのすべての設定が含まれます。プロファイルの名前に「copy」が含まれています。元のプロファイルは有効ですが (true)、この時点でコピーは無効になります (false)。必要に応じて、コピーしたプロファイルの値を編集して名前を変更し、構成設定を新しいプロファイルに適用することもできます。

   既存のプロファイルから新しいプロファイルに設定が正常にコピーされました。プロファイルをアクティブ化する必要があるため、[アクティブ] 列のステータスが false に設定されていることに注意してください。

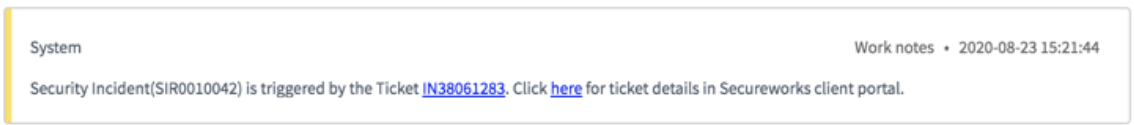
次のタスク
構成ステップが完了すると、新しいプロファイルをアクティブ (有効) にするように求められます。

チケット取り込み後の セキュリティインシデントレスポンスフォーム

Secureworks CTP チケットが取り込まれると、セキュリティインシデントが作成され、そのセキュリティインシデントレコードに対応する更新が実行されます。

作業メモ

セキュリティインシデントをトリガーしたチケットの詳細を含む作業メモが投稿されます。



チケットのリンクをクリックして、タスクレコードに対する内部 Secureworks チケットに移動します。[ここをクリック] ハイパーリンクをクリックすると、チケットの詳細を表示できる Secureworks CTP ダッシュボードに移動します。

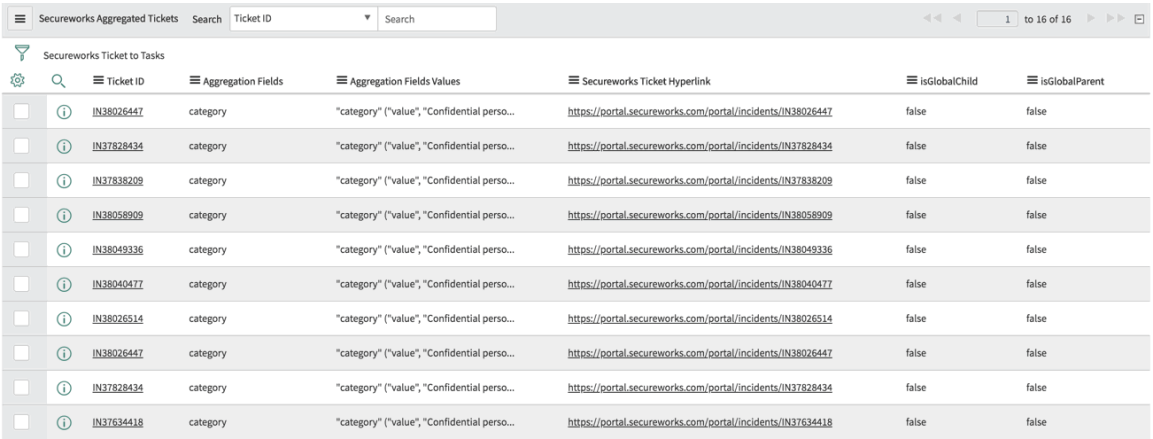
「プロファイルの作成：マッピング」ページで説明されているように、チケット集計基準で [新規チケットの作業メモを記録] オプションを選択した場合、チケットが集計されると作業メモが投稿されます。

集計チケット

クリックします 関連リスト > **Secureworks** 集計チケット をクリックして、セキュリティインシデントに集計されたチケットを表示します。Secureworks CTP ダッシュボードでチケットを表示するには、チケットのハイパーリンクをクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

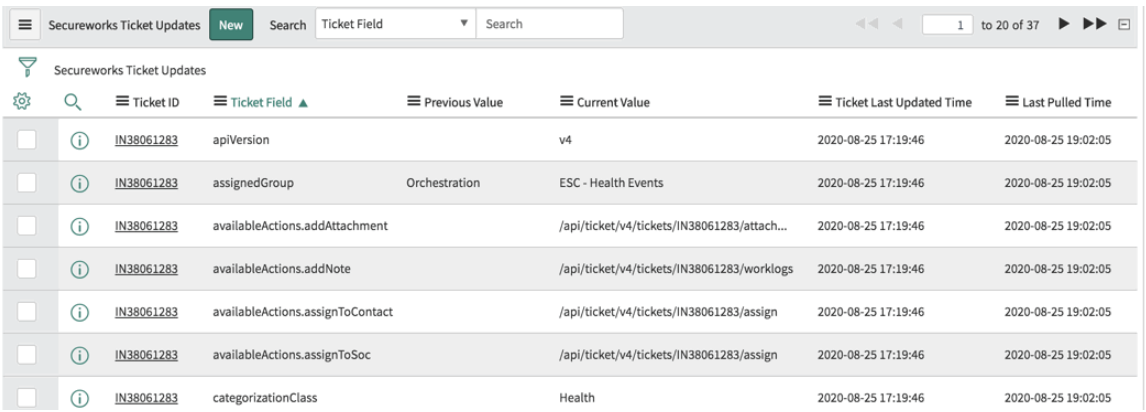


セキュリティインシデントの作成：リストからチケットを選択し、[アクション] メニューをクリックして、[セキュリティインシデントの作成] をクリックします。このオプションで、チケットの新しいセキュリティインシデントを作成できます。このチケットは親セキュリティインシデントからは集計されません。

チケットレコードの削除：リストからチケットを選択し、[アクション] メニューをクリックして、[削除] をクリックします。このオプションで、チケットレコードを削除できます。

Secureworks チケットの更新

これにより標準チケットフィールドが表示され、ポーリング間隔ごとにチケットの変更が追跡されます。Secureworks CTP ダッシュボードに移動せずにチケットの更新が直接表示されるため便利です。値の変更は [前の値] フィールドと [現在の値] フィールドに表示されます。

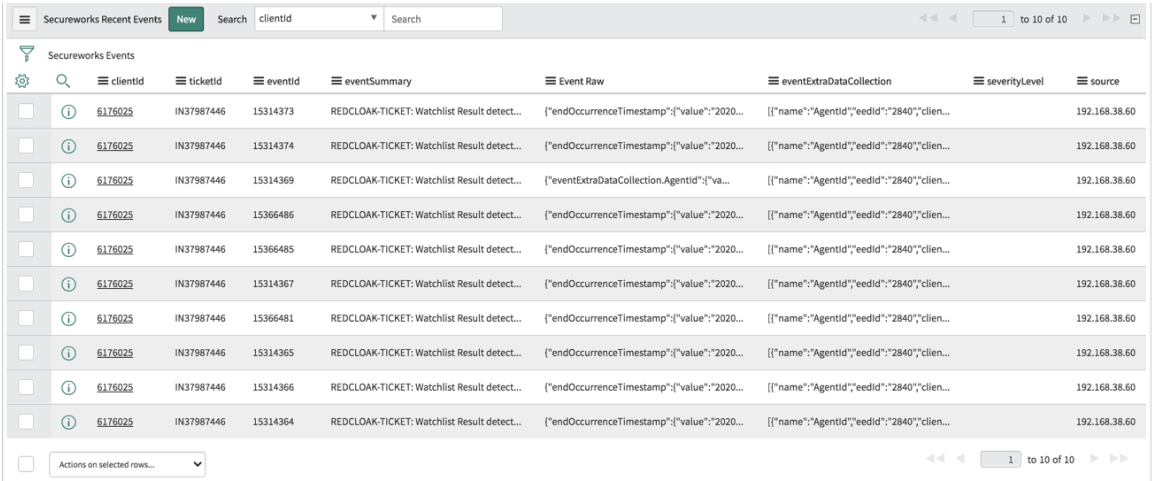


Secureworks の最新のイベント

[関連リンク] の [最新の **Secureworks** イベントをフェッチ] オプションをクリックして、最新の Secureworks イベントを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



デフォルトでは、最大 50 件のイベントが表示されます。このデフォルト設定は Secureworks 統合設定で変更できます。

Secureworks チケットと対応するセキュリティインシデントの表示

インポートされた Secureworks CTP チケットは、[チケットインポート] テーブルに最初に保存されます。フィルター条件が適用される前にインポートされたすべての Secureworks CTP チケットが表示されます。

始める前に
必要なロール：sn_si.admin

手順

1. 次のように移動する。 **All** (すべて) > **Secureworks** チケット取り込み統合 > 安全なチケットのインポート.
2. チケットが集計される前またはフィルター条件が適用される前にインポートされたすべての Secureworks CTP チケットが表示されます。
3. チケット ID をクリックすると、生のチケットデータが表示されます。
4. 次のように移動する。 **Secureworks** チケットの取り込み > タスクに対する **Secureworks** チケット.
   Secureworks CTP チケットとそれに対応するセキュリティインシデントが表示されます。

Secureworks CTP マスターチケットクローズ通知

Secureworks CTP マスターチケットで作成されたセキュリティインシデントをクローズする前に、マスターチケットに関連付けられているすべての子チケットがクローズされていることを確認する必要があります。

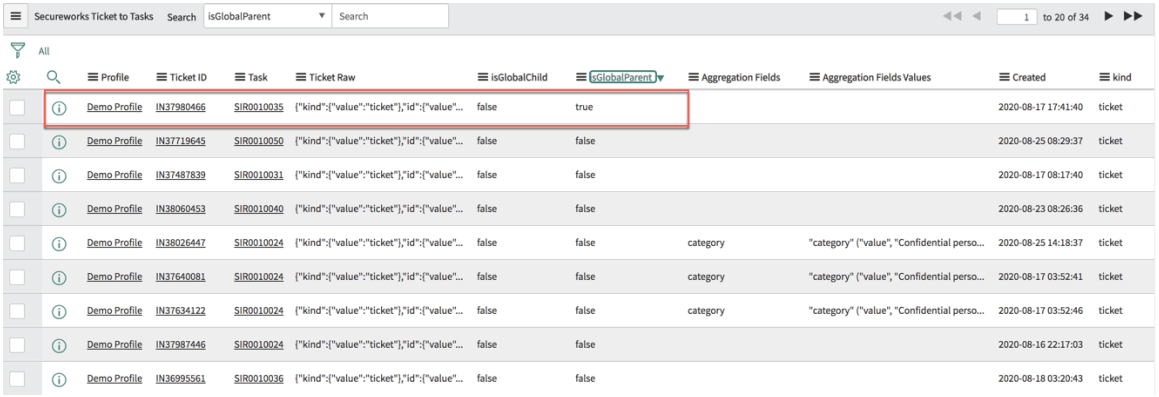
始める前に
必要なロール：sn_si.admin

手順

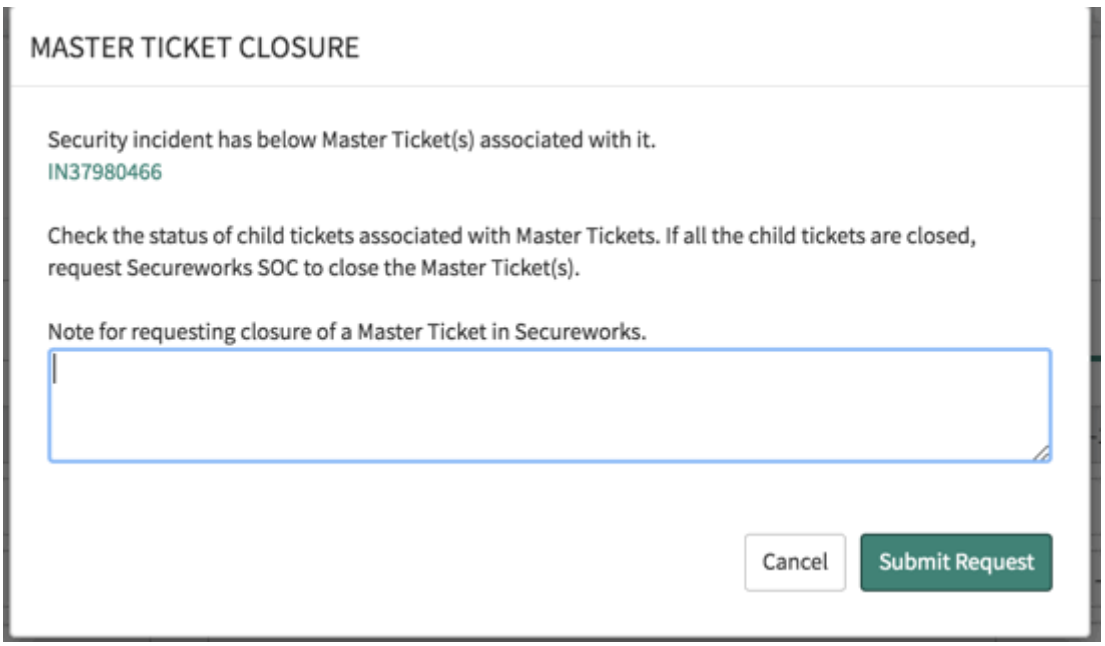
1. 次のように移動する。 **All** (すべて) > **Secureworks** チケットの取り込み > タスクに対する **Secureworks** チケット.
   Secureworks CTP チケットとそれに対応するセキュリティインシデントが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



2. **[isGlobalParent]** フィールドが **true** に設定されているセキュリティインシデントをクリックします。
3. セキュリティインシデントの [ステータス] を [クローズ済み] に変更し、クローズコードを指定して [保存] をクリックします。
   次のダイアログボックスが表示されます。



   このセキュリティインシデントは Secureworks マスターチケットに関連付けられています。マスターチケットには、1 つ以上の子チケットを関連付けることができます。マスターチケットをクローズする前に、そのマスターチケットに関連付けられているすべての子チケットがクローズされていることを確認する必要があります。

4. Secureworks でマスターチケットのクローズを要求するメモを追加し、[要求を送信] をクリックします。
   マスターチケットが Secureworks SOC チームに再割り当てされました。
5. 要求が送信されたら、セキュリティインシデントをクローズできます。
6. 次のように移動する。 アプリケーション > モジュール.

Secureworks CTP 統合設定

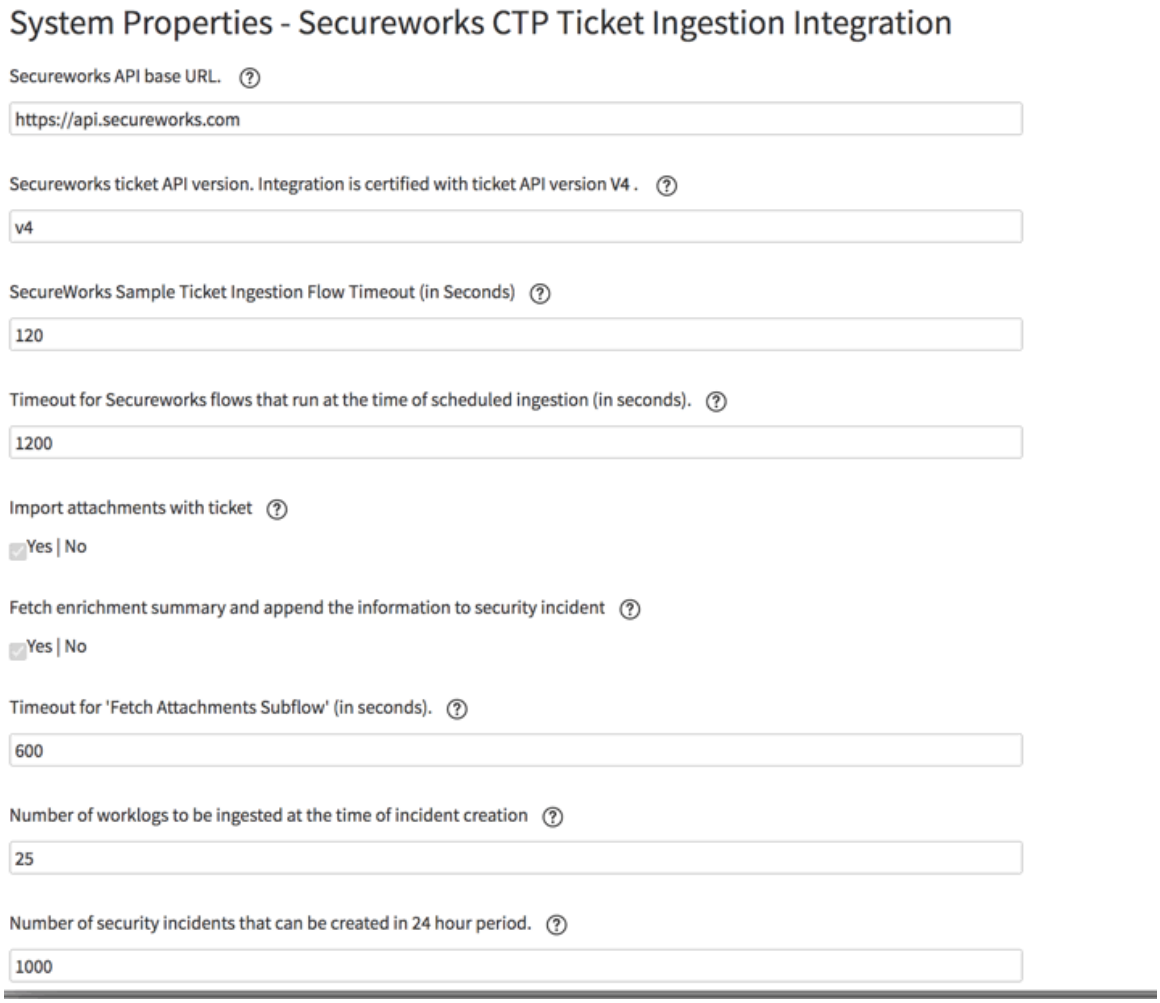
このオプションを使用して、Secureworks CTP チケット取り込み統合のデフォルトのシステムプロパティを変更します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

システムプロパティを変更するには、 *sn_si.admin* ロールを持つユーザーとしてログインし、次の場所に移動します。 **Secureworks** チケット取り込み統合 > **Secureworks** 統合設定.

デフォルトの構成設定が表示されます。必要に応じて、これらの設定を変更できます。



変更した統合設定は、プロファイルで定義されている次のポーリング間隔で適用されます。

セキュリティインシデントレスポンスと **Zscaler** の統合

セキュリティインシデントレスポンスと Zscaler の統合 製品を使用して、Zscaler Internet Access サーバー (ZIA) ログを Now Platform に接続できます。この統合により、ダッシュボードの表示、カスタムアラートの作成、セキュリティインシデントの調査が可能になります。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

概要

Zscaler インターネットおよび Web ゲートウェイ製品はクラウドから提供されます。エンタープライズセキュリティ環境の重要なデータポイントとインサイトを提供します。セキュリティインシデントレスポンスと Zscaler の統合 は Zscaler Internet Access 製品を Now Platform インスタンスに接続します。Now Platform で Zscaler 製品を使用することで、組織のインターネット使用状況をより詳細に把握できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

統合の主な機能

この統合の主な機能は次のとおりです。

- Zscaler 製品で管理される、グローバル脅威ライブラリに対する観測事象の評判のルックアップ。

  注:
  Zscaler グローバル脅威ライブラリは、傾向、発信国、ターゲット宛先、ボリューム、およびさまざまな脅威カテゴリ別に脅威をリストします。このグローバル脅威ライブラリを使用すると、グローバルな脅威ランドスケープに対して観測事象を調査できます。

- Zscaler 製品のブロックリストまたは許可リスト内の観測事象のメンテナンス。
- MD5 ハッシュの Zscaler 製品からサンドボックスレポートをフェッチしてレビューする機能。Zscaler 製品のクラウドサンドボックス機能は、仮想環境でファイルを実行して分析し、悪意のある動作を検出します。
- ユーザーが不明な悪意のあるファイルをダウンロードしたときに Zscaler 製品で生成される、患者 0 イベントからのセキュリティアラート。
- Zscaler 製品で定義されたブロックリストまたは許可リストとして機能する複数の URL カテゴリリスト。
- 観測事象が追加される URL カテゴリを識別するためにタグ付けできる Now Platform セキュリティインシデント。
- 古いエントリーを自動で期限切れまたは削除して URL カテゴリリストエントリーのサイズを維持する有効期限。
- URL カテゴリリストから観測事象を追加したり、削除したりするための承認ワークフロー。
- 脅威インテリジェンスの結果とエントリーがブロックされている理由の詳細を含む、観測事象レコードとセキュリティインシデントにリンクできる URL カテゴリエントリー。

この統合の詳細

ドキュメント識別子	ドキュメントタイトル
Zscaler 製品ドキュメント Web サイト	ZScaler 製品ドキュメント Web サイト
ServiceNow 製品ドキュメント Web サイト	ServiceNow 製品ドキュメント Web サイト

セキュリティインシデントレスポンスと **Zscaler** の統合 の開始

Zscaler Internet Access 製品をアクティブ化して、Now Platform インスタンスおよび セキュリティインシデントレスポンス 製品と連動するように設定できます。

チェックリスト

セットアップタスク	説明
必要な Now Platform および セキュリティインシデントレスポンス ロールをアサインして確認します。	予想される結果の構成と検証には、次のロールが必要です。 • admin ロールは、ServiceNow Store から統合をインストールし、sn_si.admin ロールをアサインします。 • 次のタスクを実行するには、sn_si.admin ロールが必要です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト (続く)

セットアップタスク	説明
	○ 統合を構成します。 ○ URL カテゴリリストを作成、アクティブ化、および削除します。 ○ sn_si.analyst ロールをアサインします。 • sn_si.analyst ロールは、エントリーを作成し、セキュリティインシデントを処理します。
この統合を構成する前に、ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	ServiceNow 統合ハブ Enterprise Pack Installer [com.glide.hub.integrations.enterprise] プラグインが必要です。 セキュリティインシデントレスポンス プラグイン (com.snc.security_incident) が必要です。このプラグインは、セキュリティインシデントレスポンス 製品のすべての依存関係を自動的にインストールします。統合のために他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。 次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。 **1.** セキュリティインシデントレスポンス 依存関係 (com.snc.si_dep) **2.** Security Integration Framework **3.** Security Support Common **4.** セキュリティサポートオーケストレーション **5.** 脅威インテリジェンス Support Common **6.** トラステッドセキュリティサークル **7.** セキュリティオペレーション セットアップアシスタント **8.** セキュリティインシデントレスポンス
Zscaler のバージョンを確認します。	• この統合は Zscaler Internet Access バージョン 1.0 以降でサポートされています。 • この統合は、次の Zscaler バージョンでテストされています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト (続く)

セットアップタスク	説明
	○ Zscaler Client Connector for Windows - 3.0 ○ Zscaler Client Connector for macOS - 3.0 ○ Zscaler Client Connector for Linux - Beta ○ Zscaler Cloud Connector - 6.1
必要な Zscaler 権限があり、設定していることを確認します へのアクセス Zscaler Internet Access API 一覧.	• Zscaler Internet Access のアドミン認証情報が必要です。 • 有効なクラウドサービス API サブスクリプションが必要です。Zscaler サポートがキーを提供する必要があります。 • Zscaler Internet Access アドミン認証情報 (ユーザー名とパスワード) が必要です。API 認証は、API キーと Zscaler Internet Access アドミンの認証情報の組み合わせに基づいています。 **注:** Zscaler Internet Access API キーの管理方法の詳細については、Zscaler のドキュメント を参照してください。

自動翻訳

Zscaler Internet Access API へのアクセスの設定

Now Platform インスタンスと Zscaler サーバー間のセキュア接続を認証するために、Zscaler Internet Access サーバーへのアクセスを設定します。

始める前に
必要なロール：Zscaler Internet Access admin

このタスクについて
Zscaler で組織のクラウドサービスの API サブスクリプションが有効になると、[Zscaler Internet Access API キー管理] ページでベース URL を使用して API サブスクリプションを利用できます。組織で使用できる API キーまたはトークンは 1 つだけです。新しいキーまたはトークンを追加する前に、既存のキーまたはトークンを削除します。

API のベース URL は `${Cloud_Name}/api/v1` です。組織にプロビジョニングされた Zscaler クラウド名を確認し、それを使用してベース URL の `{Cloud_Name}` を置き換えます。ベース URL の例を次に示します。

- example.zscalerbeta.net
- example.zscalerone.net
- example.zscalertwo.net
- example.zscaler.net
- example.zscloud.net

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
Zscaler Internet Access 管理ポータルの詳細については、Zscaler API キー管理に関するドキュメント と Zscaler ポータルのドキュメント を参照してください。

手順

1. アドミニストレーターとして Zscaler Internet Access 管理ポータルにログインします。
2. 次のように移動する。 アドミニストレーション > **API** キー管理.
3. **[API** キーを追加] をクリックします。
   [API キーを追加] オプションが表示されない場合は、既存のキーを削除します。
   新しい API キーがすぐに有効になり、タブに表示されます。

タスクの結果
Now Platform インスタンスから Zscaler へのアクセスを設定するためのベース URL と API キーを取得しました。

セキュリティインシデントレスポンスと **Zscaler** の統合 のインストールと構成

Now Platform インスタンスで統合を使用して開始するには、ServiceNow Store から セキュリティインシデントレスポンスと Zscaler の統合 Internet Access 製品をインストールして設定します。

始める前に
必要なロール：sn_si.admin

手順

1. ServiceNow Store から セキュリティインシデントレスポンスと Zscaler の統合 製品をダウンロードして、インストールします。
2. 次のように移動する。 セキュリティオペレーション > 統合 > 統合設定.
3. セキュリティインシデントレスポンスと Zscaler の統合タイルを検索し、 構成 > 新しい構成を作成.
4. フォームのフィールドに入力します。

Zscaler 構成フォーム

フィールド	説明
サーバー名	Zscaler サーバー名。例：ZSserver。
アクティブ	プロファイルがアクティブであることを示すインジケーター。
順序	フロー優先度。このフィールドの値は、2 つ以上のプロファイルがトリガー条件を共有する場合にワークフローが実行される順序を示します。 番号が最も小さいフローの優先度が最も高くなります。 操作の順序を設定するには、値を入力します。例：100、200、300、400。 デフォルトは 100 です。

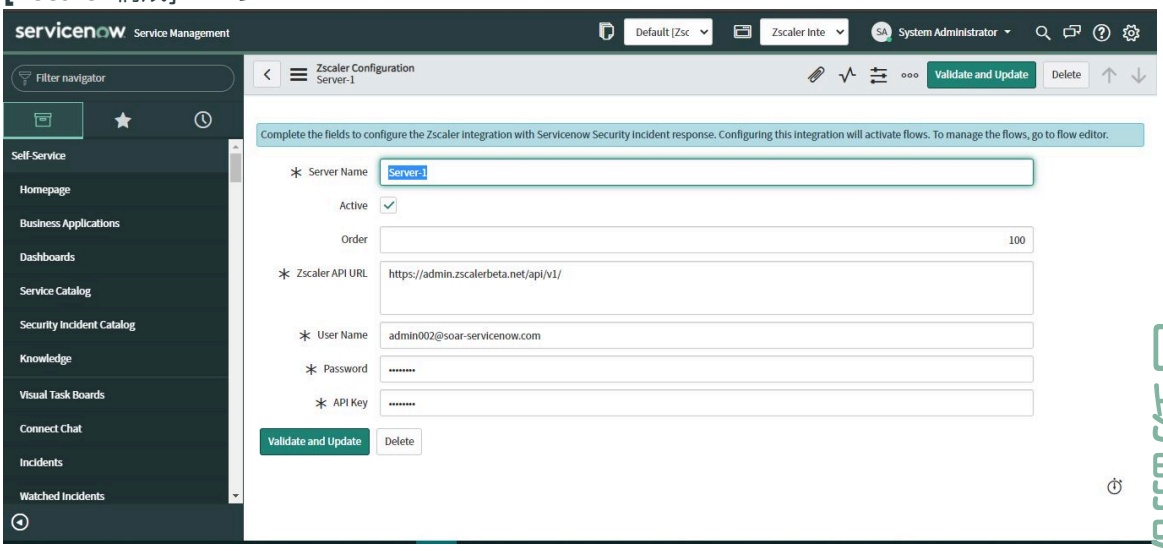
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
Zscaler API URL	Zscaler API をホストするベース URL。例：https://example.zscalerbeta.net
ユーザー名	Zscaler Internet Access アドミンアカウントのユーザー名。
パスワード	Zscaler Internet Access アドミンアカウントのパスワード。
API キー	Zscaler Internet Access 管理ポータルから取得した API キー。

次の例は、[Zscaler 構成] ページを示しています。

[Zscaler 構成] ページ



自動翻訳

5. [検証および更新] をクリックします。

タスクの結果
この構成を検証して保存した後、[Zscaler 構成] ページに戻ります。

Zscaler Internet Access URL カテゴリリストの追加

Zscaler インターネットアクセス製品で利用可能な URL カテゴリを Now Platform インスタンスに追加して、各 URL のアクションを指定し、詳細なフィルタリングとポリシー作成に簡単にアクセスできるようにします。

始める前に
必要なロール：sn_si.admin

このタスクについて
セキュリティインシデントレスポンスと Zscaler の統合 は、コンテンツのフィルタリングに役立つデフォルトの許可リストと拒否リストの URL カテゴリリストを提供します。

Now Platform インスタンスに追加する URL カテゴリは、既に Zscaler Internet Access 環境に存在する必要があります。セキュリティインシデントレスポンスと Zscaler の統合 を使用して Zscaler に URL カテゴリを作成することはできません。

注:
Zscaler 製品の URL カテゴリリストの詳細については、URL カテゴリに関する Zscaler ドキュメント を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > **ZScaler** 統合 > **ZScaler URL** カテゴリリスト.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

[Zscaler URL カテゴリリスト] フォーム

フィールド	説明
ソース	サーバーの名前。URL カテゴリリストからは、以前に構成された Zscaler Internet Access サーバーのみを表示できます。
アクティブ	URL カテゴリリストがアクティブであることを示すインジケーター。
URL カテゴリ	ソースを選択した後に有効になるフィールド。Zscaler に作成された URL カテゴリのリストを表示できます。
有効期間 (日数)	URL カテゴリリストの有効期間。 0 (デフォルト) は、URL カテゴリリストのエントリーが無期限であることを示します。 この値を変更すると、この URL カテゴリに追加された観測事象が、入力した日数の間アクティブになります。入力できる最小値は 1 です。 たとえば、有効期間を 30 日に設定すると、エントリーは 30 日後にカテゴリリストから削除されます。
タグを表示	SIR セキュリティインシデントに表示されるセキュリティタグ。 [タグを表示] オプションを有効にすると、 [観測事象] フィールドの Zscaler タグがフォームで使用可能になります。
変更要求の作成	URL カテゴリリストに添付されているレコードの Now Platform インスタンスの変更要求と変更タスク。 [変更要求の作成] オプションを有効にすると、[変更の要求] フィールドがフォームで使用可能になります。
承認が必要	承認者グループのリスト。要求が送信された後、要求を完了するにはグループからの承認が必要です。 [承認が必要 **(Require Approval)]** オプションを有効にすると、[観測事象を追加する承認者 **(Approvers for adding observables)]** フィールドおよび [観測事象を削除する承認

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	者 **(Approvers for removing observables)]** フィールドがフォームで使用可能になります。 ○ 観測事象を追加する承認者 **(Approvers for adding observables)**：ルックアップを使用して、**[Zscaler URL** カテゴリリスト] ページから観測事象を追加する承認者を選択します。このオプションを使用すると、承認のためにユーザーグループを追加できます。 ○ 観測事象を削除する承認者 **(Approvers for removing observables)**：ルックアップを使用して、**[Zscaler URL** カテゴリリスト] ページから観測事象を削除する承認者を選択します。このオプションを使用すると、承認リストからユーザーグループを削除できます。
説明	Zscaler URL カテゴリリストの説明。このフィールドを使用して、URL カテゴリレコードの詳細を追加します。

4. **[Submit]** をクリックします。
   送信が成功すると、承認グループへのメール通知がトリガーされます。

セキュリティインシデントレコードから **URL** カテゴリリストへの観測事象の送信

要求の許可またはブロックを使用して、セキュリティインシデントレコードに添付された観測事象を設定された URL カテゴリリストに送信します。セキュリティスキャンの許可リストまたはブロックリストに観測事象を追加すると、ユーザーはこれらの URL からコンテンツを確認し、信頼できるコンテンツにアクセスできます。

始める前に
必要なロール：sn_si.analyst

このタスクについて
[関連する観測事象] 関連リストの要求の許可またはブロックアクションを使用して、観測事象エントリーを送信します。観測事象は、ネットワークまたはオペレーティングシステムで検出された、侵入を示す可能性のあるアーティファクトです。以前に構成した URL カテゴリのリストを使用して、送信する観測事象を選択します。要求を送信すると、承認要求が承認グループに送信されます。

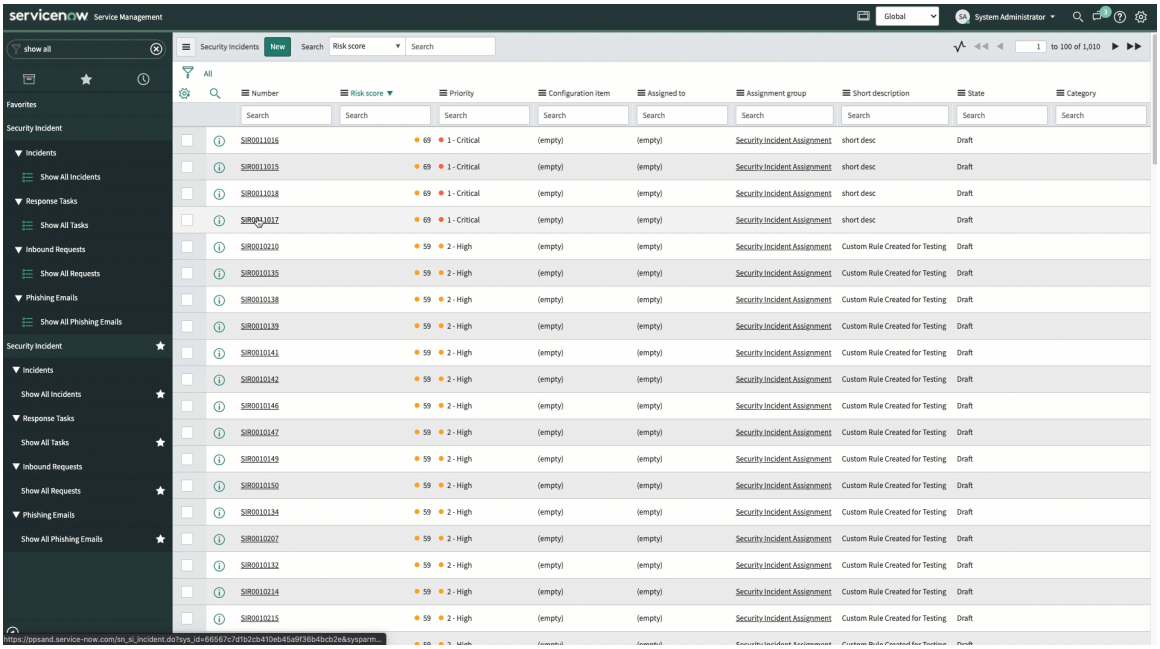
手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデント > すべてのインシデントを表示.
   この例では、セキュリティインシデントと観測事象を選択する方法、および許可リストを追加する方法を示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

許可リストの追加



2. Zscaler の要求の許可またはブロックに関連付けるセキュリティインシデントを選択します。
3. [すべての関連リストを表示] と [関連する観測事象 **(Associated Observables)]** タブをクリックします。
   観測事象が見つからない場合は、[新規] をクリックします。
4. 観測事象を選択し、アクションメニューで [要求を許可/ブロック] をクリックします。
5. [要求を許可/ブロック] ダイアログボックスで、観測事象に対して要求の許可またはブロックを実行するかどうかを選択します。
6. **[Submit]** をクリックします。
7. 作業メモを表示して、送信のステータスとセキュリティタグを確認します。
   [作業メモ] のリンクをクリックして、ステータスの詳細を表示するか、ワークフロースタジオ の詳細を分析します。セキュリティタグは、応答レコードのメタデータであり、特定のタイプのセキュリティコンテンツにアクセスする必要があるユーザーを定義します。
8. 選択した観測事象のステータスを表示するには、次に移動します: **Zscaler** 統合 > **Zscaler URL** カテゴリリストエントリー.
9. [Zscaler URL カテゴリリストエントリー] ページで、観測事象をクリックしてレコードを表示します。

URL カテゴリリストへの観測事象の承認

観測事象エントリーが適切な許可リストまたは拒否リストに含まれるように、URL カテゴリリストに追加された観測事象を承認します。

始める前に

必要なロール：sn_si.analyst

手順

1. 次のように移動する。 **All** (すべて) > **Zscaler** 統合 > **Zscaler** 承認.
2. 承認するレコードを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [承認] をクリックします。
   承認者グループは、承認要求のメール通知を受け取ります。承認者がメールの [承認/却下] リンクをクリックすると、ステータスが [承認済み] に変わります。

セキュリティインシデントの **Zscaler URL** カテゴリリストへの送信

特定の Now Platform セキュリティインシデントレコードに関連付けられていない観測事象のエントリーを直接送信し、観測事象エントリーが適切な許可リストまたは拒否リストに含まれるようにします。

始める前に
必要なロール：sn_si.admin

このタスクについて
観測事象レコードから URL カテゴリリストに観測事象を直接追加することもできます。

手順

1. 次のように移動する。 **All** (すべて) > **Zscaler** 統合 > **Zscaler URL** カテゴリリストエントリー.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

[Zscaler URL カテゴリリストエントリー] フォーム

フィールド	説明
エントリー値	観測事象の名前。 一致する観測事象が見つかった場合、フォームの残りの部分は自動的に入力されます。 一致する観測事象が見つからない場合、残りの情報は手動で入力する必要があります。
観測事象	観測事象に関連付けられている値 (IP アドレスやハッシュなど)。
観測事象タイプ	IP アドレスやファイルハッシュなどの観測事象の分類。
URL カテゴリリスト	URL カテゴリ。たとえば、組織が Office 365 サービスに example.com を使用している場合、Zscaler は example.com を Professional Services および Office 365 として分類します。
ソース	サーバーの名前。URL カテゴリリストからは、以前に構成された Zscaler サーバーのみを表示できます。
インシデント数	この観測事象が表示されるインシデントの数。この値は、観測事象が手動またはワークフローによって別のインシデントに追加されると自動的に更新されます。
アクティブ	URL カテゴリリストがアクティブであることを示すインジケーター。
ステータス	観測事象が承認済みか却下されたステータス。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
有効期間 (日数)	URL カテゴリリストの有効期間。 0 (デフォルト) は、URL カテゴリリストのエントリーが無期限であることを示します。 この値を変更すると、この URL カテゴリに追加された観測事象が、入力した日数の間アクティブになります。入力できる最小値は 1 です。 たとえば、有効期間を 30 日に設定すると、エントリーは 30 日後にカテゴリリストから削除されます。 **注:** URL カテゴリリストエントリーのデフォルトの有効期間を変更すると、選択した URL カテゴリリストで設定されている期間とは異なるという警告が表示されます。
追加情報	観測事象に関する詳細を追加できるフィールド。

4. **[Submit]** をクリックします。

Zscaler グローバル脅威ライブラリを使用した脅威のルックアップの実行

Zscaler Internet Access 製品のグローバル脅威ライブラリを使用して、観測事象に対して脅威のルックアップを実行します。Zscaler は、観測事象タイプの IP、URL、およびドメインに対するルックアップをサポートしています。

始める前に
必要なロール：sn_si.admin

このタスクについて
脅威インテリジェンスルックアップを 1 つ以上の観測事象で実行し、既知のセキュリティ上の脅威に関連するかどうかを判断します。観測事象が初めてセキュリティインシデントに関連付けられると、Now Platform 内のすべてのアクティブな脅威のルックアップ実装で自動脅威ルックアップが実行されます。[脅威ルックアップの結果 (Threat Look Up Results)] 関連リストに対して結果を表示できます。

デフォルトでは、Zscaler Internet Access 製品のグローバル脅威ライブラリに対して脅威ルックアップを実行するために、最小順序の構成が選択されます。脅威ルックアップを手動で実行することもできます。

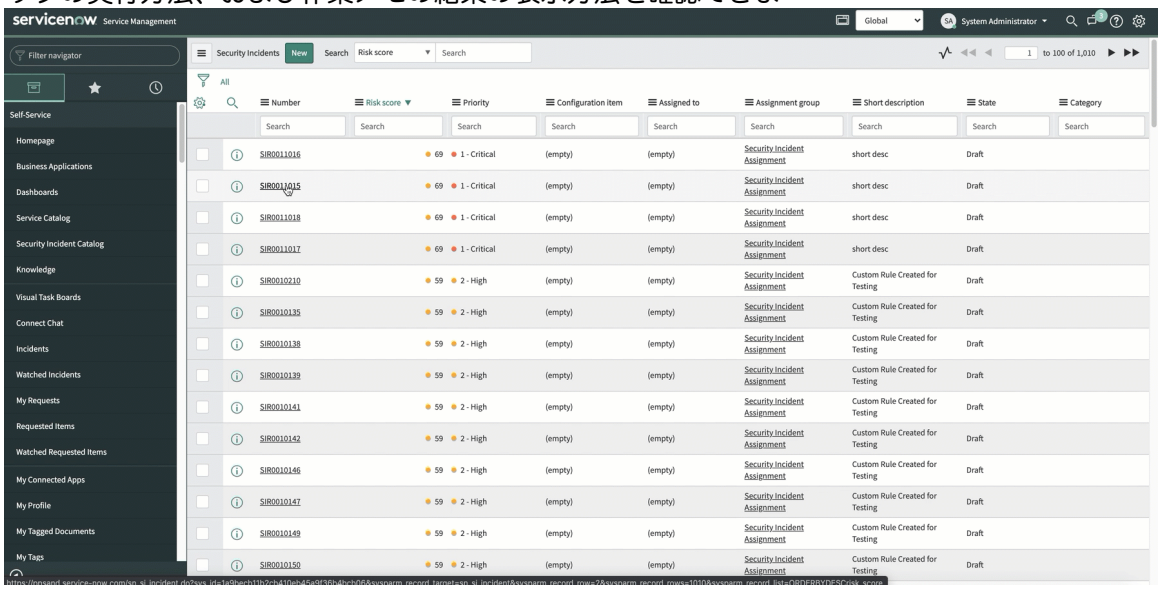
手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデント > すべてのインシデントを表示.
2. 脅威ルックアップを実行するセキュリティインシデントを選択します。
3. [すべての関連リストを表示] と [関連する観測事象 **(Associated Observables)]** タブをクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. 観測事象を選択し、 [アクション] メニューから [脅威のルックアップを実行] をクリックします。
この例では、セキュリティインシデントと観測事象の選択方法、脅威ルックアップの実行方法、および作業メモの結果の表示方法を確認できます。



タスクの結果
脅威のルックアップを開始した後、 作業メモを表示して送信のステータスを確認できます。

Zscaler サンドボックス分析への送信

Zscaler Internet Access 製品のサンドボックスサービスを使用して、仮想環境でファイルを分析し、悪意のある動作を検出します。

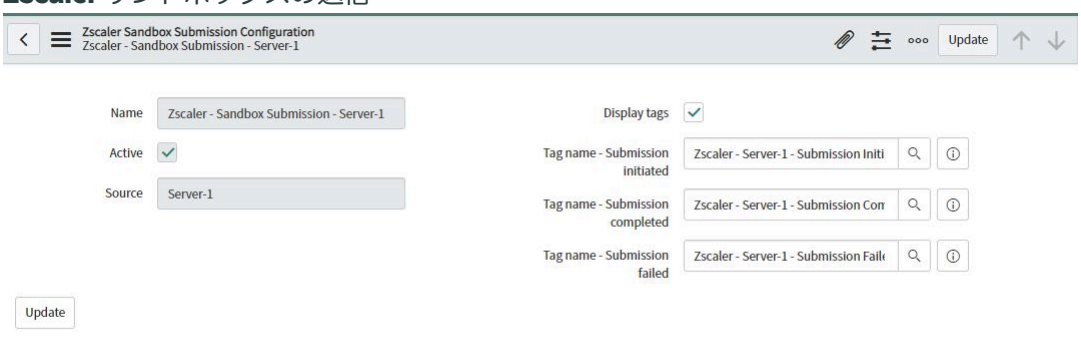
始める前に
必要なロール：sn_si.admin

このタスクについて
Zscaler 構成を作成すると、Zscaler サンドボックス送信がデフォルトで Zscaler サンドボックス構成モジュールに作成されます。

名前フィールドとソースフィールドは自動入力され、構成はデフォルトで有効になります。表示タグとアクティブなオプションのみを編集できます。Zscaler Internet Access 製品を使用すると、MD5 ハッシュタイプの観測事象のサンドボックスレポートのみをフェッチできます。

MD5 ハッシュに関連付けられているファイルの分析が完了し、対応するレポートが Zscaler サンドボックスに格納されます。送信した MD5 ハッシュのレポートが Zscaler にない場合は、エラーメッセージが表示されます。

Zscaler サンドボックスの送信



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデント > すべてのインシデントを表示.
2. サンドボックス分析を実行するセキュリティインシデントを選択します。
3. [すべての関連リストを表示] と [関連する観測事象 **(Associated Observables)]** タブをクリックします。
4. MD5 ハッシュタイプの観測事象を選択し、 [アクション] メニューから [サンドボックスに送信] を選択します。
   既存の MD5 ハッシュタイプの観測事象が見つからない場合は、MD5 ハッシュタイプの観測事象を作成します。
5. [ファイル送信] ダイアログボックスで、 [送信構成] の **[Zscaler -** サンドボックス送信 **-** サーバー] オプションを選択し、[サンドボックスに送信] をクリックします。
   サンドボックス送信を開始した後、 作業メモを表示して送信のステータスを確認できます。タグもセキュリティインシデントに追加されます。
6. 作業メモで、[サンドボックスの送信結果] の投稿のリンクをクリックします。

タスクの結果
[すべての関連リストを表示] と [サンドボックスの送信結果] タブから結果を表示することもできます。

患者 **0** イベントに関するメールアラートの設定

悪意のあるファイルからネットワークを保護できるように、患者 0 イベントなど、悪意がある可能性のある不明なファイルを特定してスキャンするように Zscaler Internet Access 製品を設定します。

始める前に
必要なロール：sn_si.admin、Zscaler Internet Access admin

このタスクについて
患者 0 は、ダウンロードは許可されているが、悪意のある不明なファイルが含まれているアラートクラスです。患者 0 イベントは重大として分類されます。患者 0 イベントのメールアラートを定期的に受信するように Now Platform を設定できます。

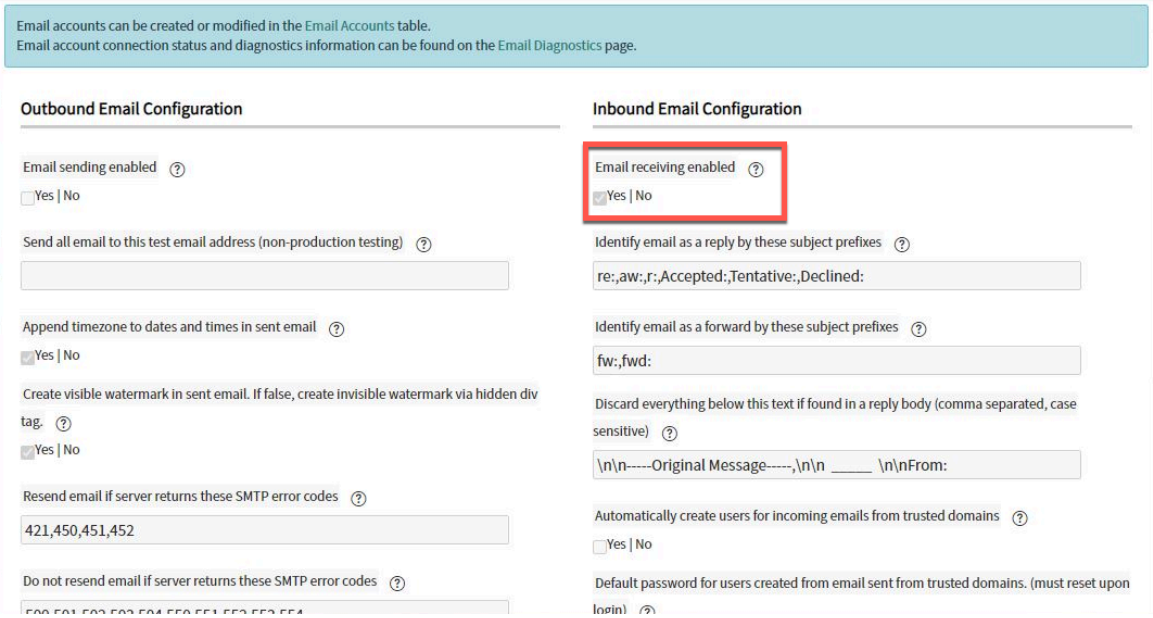
手順

1. 次のように移動する。 **All** (すべて) > システムメールボックス > アドミニストレーション > メールプロパティ.
2. [受信メール構成] セクションで [メール受信の有効化] オプションを選択します。

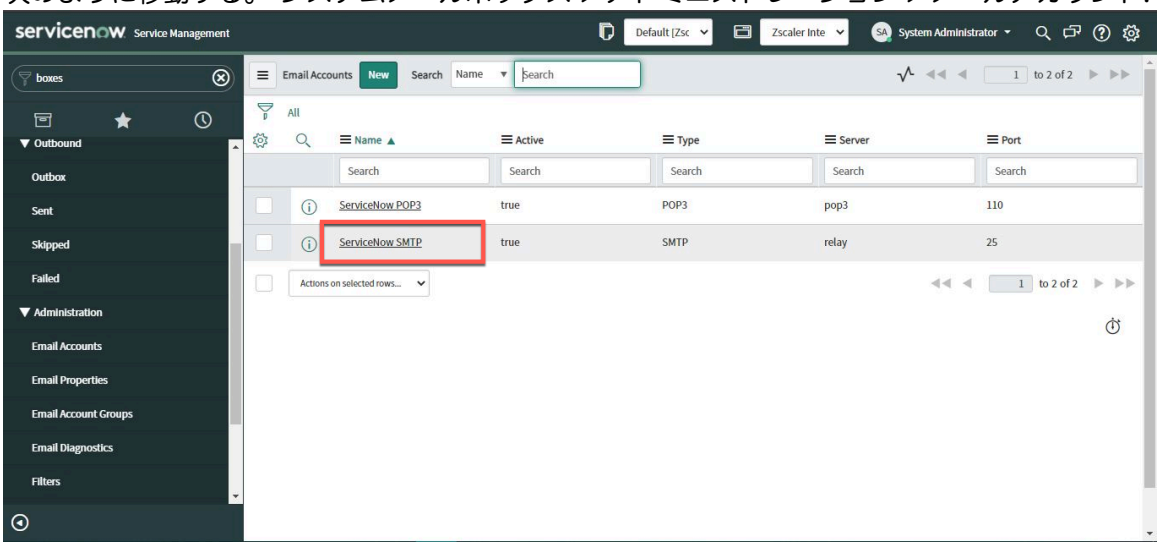
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

受信メールの設定



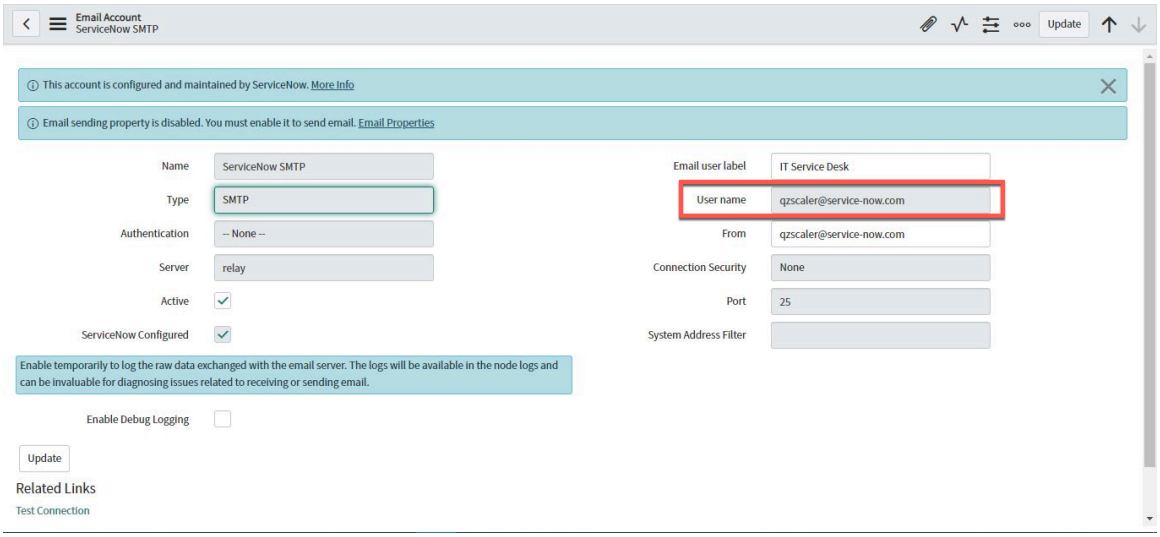
3. **[Save** (保存)] をクリックします。
4. 次のように移動する。 システムメールボックス > アドミニストレーション > メールアカウント.



5. **ServiceNow SMTP** メールアカウントを選択します。
   ユーザー名をメモします。ここで識別されるユーザー名は、Zscaler で患者 0 のアラートの設定に使用する Now Platform メールアドレスです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Now Platform SMTP アカウントのユーザー名



6. Zscaler Internet Access 管理ポータルにログインします。

   注:
   Zscaler Internet Access 管理ポータルの詳細については、Zscaler のドキュメント を参照してください。

7. 次のように移動する。 アドミニストレーション > アラート > アラートを公開.
8. [アラートサブスクリプションを追加] をクリックします。
9. フォームのフィールドに入力します。

   [アラートサブスクリプションを追加] フォーム

フィールド	説明
メール	Now Platform SMTP アカウントのメールアドレス。
説明	患者 0 のアラートに関する詳細を追加するためのフィールド。

10. [保存] をクリックします。

ServiceNow セキュリティオペレーション **Add-On for Splunk** の概要

ServiceNow セキュリティオペレーション Add-On for Splunk を使用すると、Splunk ソフトウェアアドミニストレーターは Now Platform でデータを収集し、インシデントとイベントを作成できます。

アドオンは Splunkbase からインストールされます。

重要:
Splunk はマネージドサービスプロバイダー (MSP) 環境でもサポートされています。

Splunk Integration のセットアップ

ServiceNow セキュリティオペレーション Add-On for Splunk のセットアップ手順には、Splunk へのアドオンファイルのダウンロード、アドオンのインストール、セキュリティインシデントとセキュリティイベントが作成される ServiceNow インスタンスのセットアップが含まれます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

必要なロール

Splunk Integration のセットアップ手順を実行する前に、ServiceNow インスタンスの sn_si.integration_user ロールと sn_si.analyst ロールを持つ統合ユーザーを定義してください。また、インポートを実行するには、セキュリティテーブルの読み取りと書き込み権限を取得するための import_transformer ロールが必要です。sn_si.integration_user ロールは、ロールの import_transformer 部分で定義する必要があります。

ServiceNow SecOps アプリケーションのダウンロード

ServiceNow と Splunk の統合を設定する最初のステップでは、Splunkbase から ServiceNow セキュリティオペレーション アプリケーションをダウンロードします。

始める前に
必要なロール：admin

手順

1. Splunkbase を開きます。
2. ServiceNow Security Operations Integration を検索します。
3. アプリケーションをダウンロードします。

ServiceNow Security Operations Add-on for Splunk のインストール

ServiceNow Security Operations add-on for Splunk をインストールして、Splunk を ServiceNow にリンクします。

始める前に
必要なロール：admin

手順

1. [Splunk] を開きます。
2. [アプリ] ギアアイコンまたは [アプリケーションを管理] ショートカットメニューアイテムをクリックします。
3. [ファイルからアプリをインストール **(Install app from file)**] クリックします。
4. [ファイルを選択] をクリックし、[sn_sec_ops.spl] を選択して、[アップロード] をクリックします。
5. プロンプトが表示されたら、Splunk を再起動します。
   ServiceNow セキュリティオペレーション Add-On for Splunk がインストールされ、設定する準備が整いました。

インシデントまたはイベントが作成されるインスタンスの設定または変更

新しいセキュリティインシデントとセキュリティイベントが作成される ServiceNow インスタンスを設定または変更するには、アプリケーションリストの [セットアップ] アクションを使用します。

始める前に
必要なロール：sn_si.admin

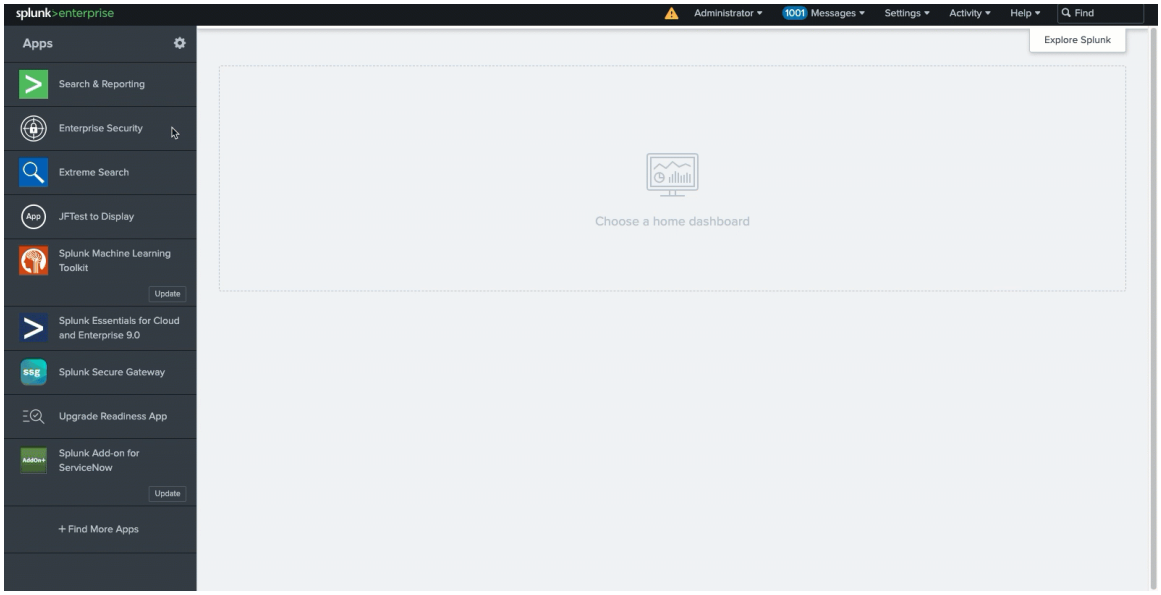
手順

1. **Splunk** を開きます。
2. [アプリ] ギアアイコンまたは [アプリケーションを管理] ショートカットメニューアイテムをクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. アプリケーションのリストで、フィルターを使用して **ServiceNow** アプリを検索します。
4. **ServiceNow Security Operations Integrations** を探し、対応する [セットアップ] アクションをクリックします。
5. フォームのフィールドに入力します。

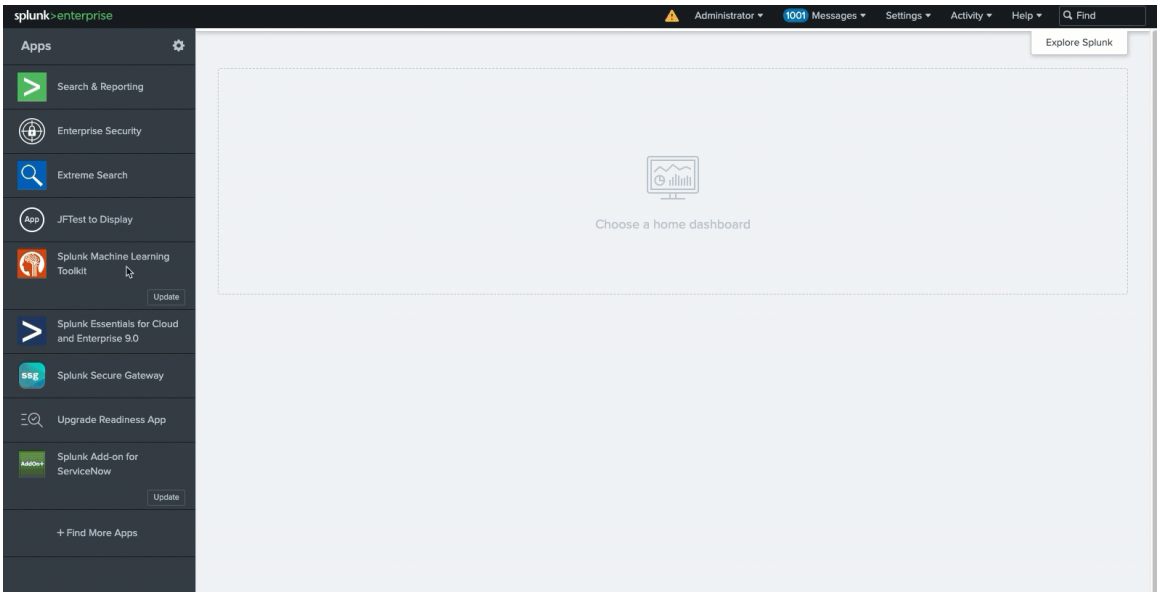


6. [保存] をクリックします。
7. または、「**ServiceNow Event Ingestion Integration**」を探し、対応する [セットアップ] アクションをクリックします。

   ServiceNow Event Ingestion Integration は、3 つの異なるタブで構成されています。
   - **Splunk** プライマリ：デフォルトまたはプライマリの Splunk 構成。
   - **Splunk** セカンダリ：(オプション) バックアップまたは 2 番目の Splunk 構成。
   - ログレベル：統合で生成されたレポートログのレベル (情報のタイプの名前)。
8. **[Splunk** プライマリ] タブを選択します。
9. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



10. オプション: **[Splunk** セカンダリ] タブを選択します。
11. オプション: フォームのフィールドに入力します。
12. [ログレベル] タブを選択します。
13. フォームのフィールドに入力します。
14. [保存] をクリックします。
    検証が正常に完了すると、各構成を含む [セキュリティ統合] ページが表示されます。次の図に示すように、有効な各構成タイルに [更新] および [削除] ボタンが表示されます。

    > **注:**
    > ベーシック認証または OAuth 2.0 認証のいずれかのみを使用する必要があります。いずれかの認証を有効にし、対応する認証の詳細を入力します。両方を有効にすると、エラーが表示されます。

    検証と送信が正常に完了すると、各 [イベントの取り込み] の Splunk サーバー構成は [セキュリティ統合] ページにタイルとして保存されます。保存された構成タイルが右上隅にある [セキュリティ統合] ページに表示されていない場合、[構成を表示] リストから [はい] をクリックします。

ServiceNow インスタンスでのアプリケーションレジストリの設定

OAuth 認証を使用するには、アプリケーションをインスタンスに登録します。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > システム **OAuth** > アプリケーションレジストリー.
2. [**New**] をクリックします。
3. [外部クライアント用の **OAuth API** エンドポイントを作成 **(Create an OAuth API endpoint for external clients)]** をクリックします。
4. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. フォームヘッダーを右クリックし、[保存] をクリックします。
6. **[Submit]** をクリックします。

手動検索コマンド

手動検索コマンドは、任意の [検索] ウィンドウから入力します。セキュリティインシデントまたはセキュリティイベントを作成できます。コマンドの後に、目的のレコードを作成するために使用されるフィールド名と値のペアがあります。

セキュリティイベント

snsecevent セキュリティイベントコマンドは、セキュリティ分類を使用して、ServiceNow にイベントを作成します。

これらのイベントは単独でレビューすることも、ServiceNow 内のアラートルールまたは手動アクションでイベントまたはイベントのコレクションをセキュリティインシデントに変換することもできます。

イベントがセキュリティインシデントになり、各パラメーターがイベントに送信される場合、このデータは次のようにセキュリティインシデントを入力するために使用されます。

セキュリティイベント

パラメーター名	必須	使用	セキュリティインシデントでの使用
node	はい	ノードは、イベントのサーバーまたは構成アイテムを表します。このノードは ServiceNow 内の既存の CI にマッピングされることが理想的です。	セキュリティインシデントでの使用
type	はい	イベントのカテゴリ。	簡単な説明
resource	はい	構成アイテム。	簡単な説明

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティイベント (続く)

パラメーター名	必須	使用	セキュリティインシデントでの使用
source	いいえ	このデータの作成元。デフォルトでは、Splunk サーバーがデータを生成します。	アクティビティログ
external_url	いいえ	このイベントに関する Splunk データに戻るために ServiceNow で使用するドリルダウン URL。デフォルトでは、この URL にはアラートの結果リンク、またはデフォルトの Splunk 検索ページへのリンクが含まれています。	[セキュリティインシデント] フォームの [ドリルダウン] ボタンを使用してアクセスする外部 URL
time_of_event	いいえ	イベントが Splunk に記録された時間。	該当なし
他のすべての値 (例ではカテゴリ、サブカテゴリ)	いいえ	イベントの情報フィールドに含まれていないフィールド。セキュリティインシデントが作成された場合は、それが使用されます。	フィールドが存在し、入力されていない場合、セキュリティインシデントはその値を使用します。たとえば、イベントを通過するカテゴリは、新しいセキュリティインシデントのカテゴリになります。この名前のフィールドが存在しない場合、値はアクティビティログに配置されます。

自動翻訳

セキュリティインシデント

snsecincident セキュリティインシデントコマンドは、ServiceNow インスタンスにセキュリティインシデントを作成します。

セキュリティインシデント

パラメーター	必須	使用
short_description	はい	インシデントの簡単な 1 行の説明。
category	いいえ	セキュリティインシデントのカテゴリ。このカテゴリが存在しない場合は作成されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデント (続く)

パラメーター	必須	使用
subcategory	いいえ	サブカテゴリ。このサブカテゴリが存在しない場合は作成されます。
cmdb_ci	いいえ	セキュリティインシデントの構成アイテム。このアイテムは ServiceNow 内の既存の CI にマップされることが理想的です。
description	いいえ	インシデントのより詳細な説明。

多数の有用な列があり、セキュリティインシデント変換マップ内の任意の列を使用できます。セキュリティインシデントに新しい列が追加された場合、変換マップ内にある限りその列は使用されます。役立つ列には、location、priority、assignment_group、assigned_to、affected_user、attack_vector、watch_list などがあります。

Splunk イベントアクション

Splunk ログを確認するときに、イベントアクションを使用して、ログ内の任意のアイテムからセキュリティイベントとセキュリティインシデントを迅速に作成できます。

これらのアクションのいずれかをクリックすると、ログエントリーのデータが取り込まれた手動検索コマンドが作成され、新しいレコードが生成するために実行されます。

これらのアクションは、正規化されたデータにフィールドを追加するように簡単に構成できます。Splunk 内で、 設定 > フィールド > ワークフローアクションの場合、手動検索フィールドを使用して、これらのアクションのいずれかを選択して編集できます。

アクションが表示される場所とフィールドを選択し、検索コマンドを含む検索文字列を変更してレコードを作成できます。

単一レコードの **Splunk** アラート

アラート内では、アラートが発生したときに作成するセキュリティイベントまたはセキュリティインシデントを指定できます。

アラートを開くか作成し、アクションを編集するときに、レコードのタイプを選択して、アラートダイアログボックスに入力します。

複数レコードのカスタムフィールド **Splunk** アラート

複数レコードアラート ([複数の **ServiceNow** セキュリティインシデントを作成 **(Create Multiple ServiceNow Security Incidents)]** および [複数の **ServiceNow** セキュリティイベントを作成 **(Create Multiple ServiceNow Security Events)]** トリガーアクションを使用して定義) では、サポートされているフィールドのセットを使用してレコードを自動的に作成できます。

これらは、デフォルト値が指定されている点で他のアラートアクションとは異なる動作をします。ただし、ほとんどのデータはそのアラートの検索結果から取得されます。

注:
以前のバージョンのアドオンとこのドキュメントでは、スクリプト化されたアラートがサポートされていました。この機能は廃止され、次の手順に置き換えられました。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

複数レコードのカスタムフィールド **Splunk** アラートの作成

カスタムフィールドを使用して複数レコードの Splunk アラートを作成するには、入力する ServiceNow 列に一致するように設計された検索をビルドする必要があります。

始める前に
必要なロール：sn_si.admin

手順

1. [検索] に移動します。
2. [検索] ボックスで、レコードデータを生成する検索を作成します。
   推奨される検索条件については、例を参照してください。
3. [名前を付けて保存] をクリックし、[アラート] を選択します。
4. 必要に応じて、名前、権限、およびスケジュールを設定します。
5. [アクションの追加] をクリックします。
6. 次のいずれかを選択します。
   - 検索の結果ごとに 1 つのイベントを作成するには、[複数の **ServiceNow** セキュリティイベントを作成 **(Create Multiple ServiceNow Security Events)]** を選択します。
   - 検索の結果ごとに 1 つのインシデントを作成するには、[複数の **ServiceNow** セキュリティインシデントを作成 **(Create Multiple ServiceNow Security Incidents)]** を選択します。
7. 必要に応じてデフォルトを設定します。
   検索結果のフィールドが空白であるか存在しない場合は、デフォルトが使用されます。結果に値がある場合、デフォルトは上書きされます。

複数レコードのカスタムフィールド **Splunk** アラートの例

カスタムフィールドを含む複数のレコード Splunk アラートを作成する場合は、アラートデータを生成するための検索条件を定義する必要があります。セキュリティインシデントとセキュリティイベントの検索条件の例を示します。

セキュリティインシデントの検索

セキュリティインシデントの場合、この条件は [セキュリティインシデント] テーブルの列に入力する検索をビルドします。

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval contact_type="Monitoring" |
eval cmdb_ci=host |
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

セキュリティイベントの検索

セキュリティイベントの場合、同じ検索ですが、代わりに [イベント] フィールドに入力されます。このイベントはセキュリティインシデントに変わり、イベントに存在しないフィールドが入力された場合は、セキュリティインシデントに転送されます。それ以外の場合は、イベントとアラートの追加情報フィールドに残ります。

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval type="Monitoring" |
eval node=host |
eval source=source
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

注:
使用する検索条件によって、検索で見つかった数のレコードが追加されます。5 または 10,000,000,000 件のレコードを追加できます。したがって、これはデータの一括転送に推奨される方法ではありません。このメソッドの目的は、REST コールごとに 1 つのレコードを ServiceNow インスタンスに追加することです。

Splunk エラーレポート

ServiceNow インスタンスで接続の問題が発生するたびに、問題を説明するエラーが Splunk に記録されます。

エラーメッセージは、ソースタイプが **servicenow** の新しいインデックス名 **servicenow** に格納されます。

エラーログを検索するには、検索で **servicenow** インデックスを指定していることを確認してください。新しい **servicenow** インデックスをデフォルトの検索インデックスに追加する方法については、最新の Splunk に関するドキュメントを参照してください。

ServiceNow による セキュリティオペレーション 向け Splunk Enterprise Event Ingestion 統合

Splunk Enterprise イベントとアラートのデータを セキュリティインシデントレスポンス (SIR) 製品に統合すると、セキュリティインシデントアナリストはセキュリティログと関連イベントデータを収集して処理できます。

概要

データはリアルタイムで収集され、アナリストが潜在的なサイバー脅威を特定して報告するために使用されます。収集されたセキュリティイベントは、この統合で自動的に取り込まれるトリガーされたアラートに処理できます。また、個々のセキュリティイベントを Splunk Enterprise 検索およびレポートインターフェイスから Now Platform の セキュリティインシデントレスポンス 製品にオンデマンドで手動転送して、セキュリティインシデントを作成することもできます。検索ヘッドクラスター構成を使用して、Splunk Enterprise 検索から注目イベントを取得できます。これは、クラスターの一部である検索ヘッドの URL と API ポートを使用して行います。

この統合により、セキュリティオペレーションセンター (SOC) アナリストはイベントと関連アラートデータを表示できます。このデータは、Now Platform セキュリティインシデントレスポンス (SIR) セキュリティインシデントに統合して、さらに調査および修復できます。Splunk の進行中の取り込まれたアラートと転送されたイベントのプロファイルが Now Platform のインスタンスに作成されます。これらのプロファイルは、SIR セキュリティインシデントでのさまざまな Splunk アラートとイベントフィールドの表示方法をカスタマイズします。顧客固有のニーズに合わせて編集および拡張できる、アラートフィールドのデフォルトマッピングが提供されます。

主な機能

この統合の主な機能は次のとおりです。

- 複数のアラート取り込みプロファイルを作成して、フィッシングやマルウェアなどの特定のタイプの脅威に対して SIR セキュリティインシデントを作成します。
- Splunk コンソールからオンデマンドイベント転送用の複数のイベントプロファイルを作成して、SIR セキュリティインシデントを作成します。
- 関連付けられている SIR セキュリティインシデントフィールドに Splunk アラートフィールド値とイベントフィールド値のマッピングをドラッグアンドドロップします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- プロファイル構成を検証するためのサンプルアラートまたはイベントに基いて、SIR セキュリティインシデントレイアウトをプレビューします。
- 履歴アラームと、構成可能な間隔で進行中の将来のアラームを取り込みます。
- 一致するフィールド値に基づいて既存の SIR セキュリティインシデントにイベントまたはアラートを集計し、重複するセキュリティインシデントを回避します。

サポートされている **Now Platform** のバージョン

com.snc.si_dep プラグインが必要です。このプラグインは、セキュリティインシデントレスポンス製品をサポートするために必要なすべての依存関係を自動的にインストールします。他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。

次の セキュリティオペレーション アプリケーションを、ServiceNow Store からインストールしてアクティブ化する必要があります。スムーズにインストールできるように、アプリケーションを次のリストの順番で、一度に 1 つずつインストールしてアクティブ化します。

1. Security Integration Framework
2. Security Support Common
3. セキュリティサポートオーケストレーション
4. セキュリティインシデントレスポンス

セキュリティオペレーション コアアプリケーションのインストールの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

ServiceNow アドオン

ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise は、Splunk Enterprise コンソールから Now Platform インスタンスに手動でイベントを転送する場合にのみ必要です。この ServiceNow アドオンは splunkbase で入手できます。

この ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise アプリケーションは、統合でサポートされている自動アラートの取り込みには必要ありません。

サポートされている **Splunk** バージョン

この統合は Splunk Enterprise バージョン 6.0 以降でサポートされています。統合は、Splunk Enterprise クラウドサービスもサポートしています。

MID サーバー

Splunk サーバーが企業ネットワーク内に展開されている場合、この統合では、Now Platform® インスタンスにインストールされ、構成された MID サーバーを Splunk サービスに接続する必要があります。Splunk Cloud サービスを使用している場合、MID サーバーは必要ありません。MID サーバーの詳細については、「MID サーバー」を参照してください。

統合アーキテクチャとシステム接続

重要な用語や外部システム接続の詳細など、統合のアーキテクチャの詳細については、「Splunk Enterprise Event Ingestion 統合の統合アーキテクチャと外部システム接続」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト

これらのトピックの印刷可能なチェックリストについては、「Splunk Enterprise Security 注目イベントの取り込み統合用チェックリスト」を参照してください。このリストを使用して、進捗を監視しながら、統合のタスクを進めることができます。

次のトピックで使用する画像は、Now Platform の Kingston リリース用に生成されたものです。San Diego のユーザーインターフェイスについては、「Manage security threats using the Security Analyst Workspace (Security Analyst Workspace を使用したセキュリティ脅威の管理)」を参照してください。

次のトピックには番号が付けられています。アプリケーションのインストールと設定をスムーズに行えるように、以下のトピックを記載されている順に実行してください。

Splunk Enterprise Event Ingestion 統合での Now Platform® インスタンスの設定

次のセクションでは、ServiceNow Store からアプリケーションをインストールする前に Now Platform® インスタンスで完了する必要があるセットアップタスクを示します。

始める前に
必要なロール：admin

このタスクについて
スムーズなインストールと構成を行うために、 アプリケーションをダウンロードしてインストールする前に、次のテーブルを参照して、リストされたすべてのタスクを完了していることを確認してください。

手順

1. 必要な Now Platform® およびセキュリティインシデントレスポンス (SIR) のロールがアサインされていることを確認します。

   Now Platform® インスタンスで統合をインストール、セットアップ、および使用するには、次のロールが必要です。

   - Now Platform® アドミン (admin) ロールを持つユーザーが ServiceNow Store からアプリケーションをインストールし、セキュリティインシデントアドミン (sn_si.admin) ロールをアサインします。
   - この統合のために Splunk Enterprise から手動でイベントを転送する場合は、Now Platform® admin ロールを持つユーザーが Now Platform® で (sn_sec_splunk_v2.api_account_access) ロールを持つユーザーをアサインします。このロールは、Splunk Enterprise アドミンロールを持つユーザーが、この統合の手動イベント転送に必要な Now Platform® の API にアクセスすることを許可します。

     Splunk Enterprise から Now Platform® インスタンスに自動的にアラートを取り込む場合、統合に (sn_sec_splunk_v2.api_account_access) ロールは必要ありません。
   - sn_si.admin ロールを持つユーザーは、Now Platform® で次のタスクを監督します。
     - アラートとイベントプロファイルに名前を付け、作成し、編集します。
     - アラートとイベントから値を選択し、Now Platform® セキュリティインシデントにマップします。
     - 構成を確定する前に、正確性を確認するためにセキュリティインシデントの詳細をプレビューします。
     - 進行中のアラートの取り込みをスケジュールします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- セキュリティインシデントアナリスト (sn_si.analyst) ロールをアサインします。
- sn_si.analyst を持つユーザーは、セキュリティインシデントを処理します。

ロールとユーザーへのロールのアサインの詳細については、「Managing roles」を参照してください。

2. Splunk API のバージョン 6.0 以降を使用していることを確認します。

   Splunk Enterprise コンソールへのアクセス権がある場合は、この統合に必要な API にアクセスできます。API に必要なその他の特別なセットアップはありません。

3. MID サーバーがインストールおよび設定されていることを確認します。

   Splunk サーバーが企業ネットワーク内に展開されている場合、Now Platform® インスタンスの MID サーバーを Splunk サービスに接続する必要があります。MID サーバーの詳細については、「MID サーバー」を参照してください。

   Splunk Cloud サービスを使用している場合、MID サーバーは必要ありません。

4. 統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。

   セキュリティインシデントレスポンス Dependency プラグイン (com.snc.si_dep) が必要です。このプラグインは、セキュリティインシデントレスポンス 製品をサポートするために必要なすべての依存関係を自動的にインストールします。統合に必要な他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。

   次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。

   a. セキュリティインシデントレスポンス
   b. Security Integration Framework
   c. Security Support Common
   d. セキュリティサポートオーケストレーション

   セキュリティオペレーション コアアプリケーションのインストールの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

次のタスク

統合のために Now Platform® インスタンスが正常に設定されました。次のステップでは、統合のために ServiceNow Store から Splunk Enterprise Event Ingestion アプリケーションをインストールします。詳細については、「Splunk Enterprise Event Ingestion 統合用の ServiceNow アプリケーションのインストールと設定」を参照してください。

取り込み用に Splunk Enterprise コンソールに検索を保存していない場合、または Splunk Enterprise コンソールと Now Platform® インスタンスの セキュリティオペレーション 製品でこの統合の初期設定を同時に実行している場合は、詳細について「Splunk Enterprise Event Ingestion 統合での Splunk Enterprise コンソールへの検索の保存」を参照してください。

統合のために Splunk Enterprise コンソールから手動でオンデマンドでイベントをエクスポートする場合、詳細については「Splunk Enterprise イベントの取り込み統合での手動イベント取り込み用の Splunk 環境設定」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

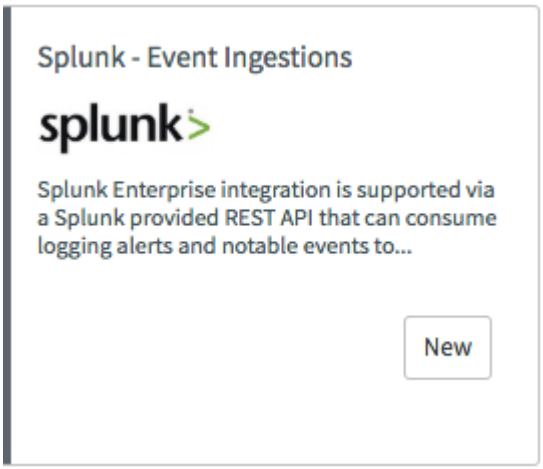
Splunk Enterprise Event Ingestion 統合用の ServiceNow アプリケーションのインストールと設定

Now Platform インスタンスで統合を実行する前に、これらのインストールと構成のステップを完了して、Now Platform インスタンスでアプリケーションが セキュリティインシデントレスポンスと セキュリティオペレーション 製品と適切に統合されるようにします。

始める前に
必要なロール：admin

手順

1. ServiceNow Store から統合用の Splunk Enterprise Event Ingestion アプリケーションをインストールしていない場合は、「セキュリティオペレーション 統合のインストール」を参照し、ステップに従ってインストールしてください。
2. アプリケーションのインストールが完了したら、 統合 > 統合構成 をクリックし、[Splunk イベントの取り込み] タイルを見つけます。
3. アプリケーションを設定するには、[新規] をクリックします。

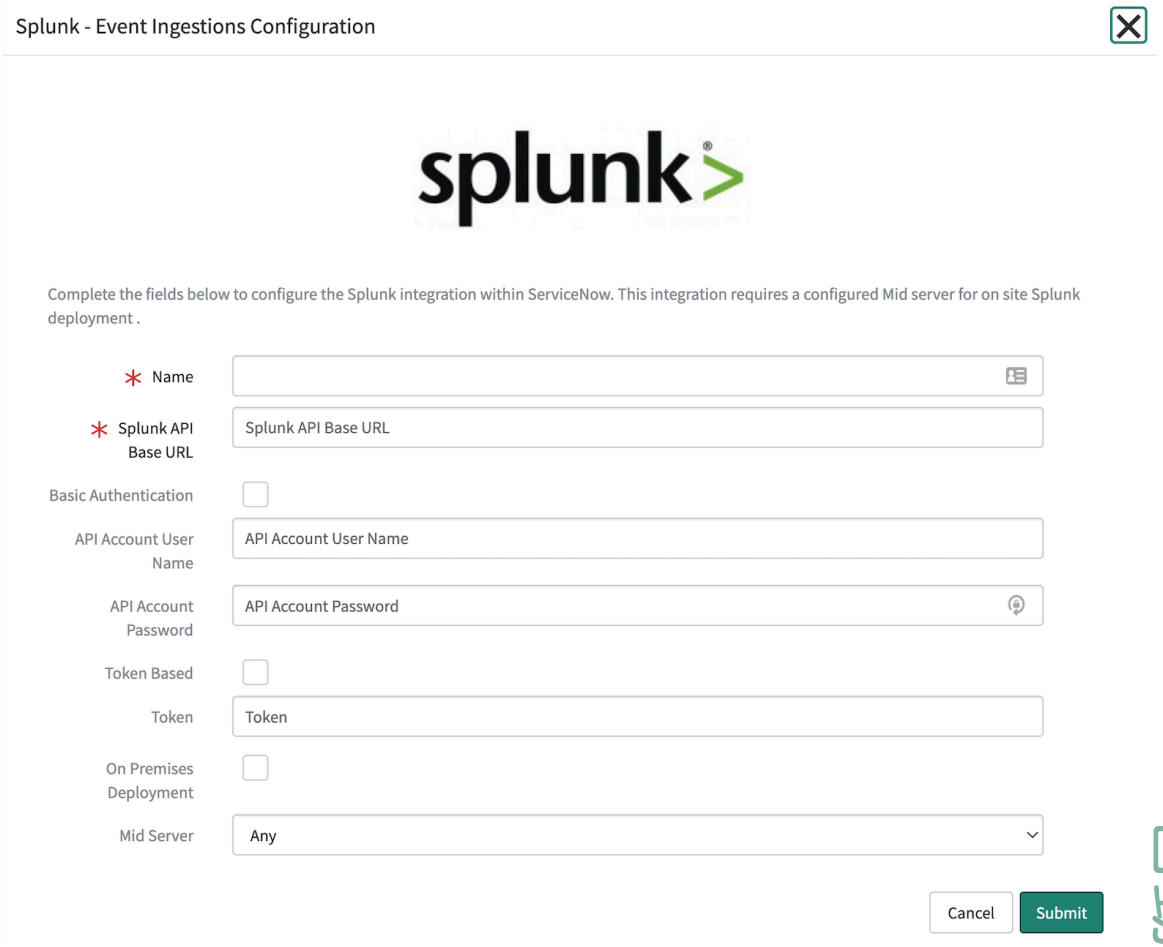


4. または、[構成] ボタンがタイルに表示されている場合は、そのボタンをクリックして既存の構成を編集します。
5. 表示される [イベントの取り込み構成] ダイアログで、フィールドに入力します。

   次の図は、MID サーバーを使用したオンプレミスバージョンの Splunk Enterprise 構成用の完成したフォームの例です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



Splunk Enterprise コンソールから取り込む各 Splunk Enterprise アラートには、Now Platform インスタンス内に一意のイベントプロファイルが必要です。ただし、[イベントの取り込み構成] フォームで構成したソースは、各プロファイルが一意の Splunk トリガーアラートを取り込む限り、複数の Now Platform プロファイルで再利用できます。

6. **[Submit]** をクリックします。
検証が正常に完了すると、各構成を含む [セキュリティ統合] ページが表示されます。次の図に示すように、有効な各構成タイルに [構成] および [削除] ボタンが表示されます。

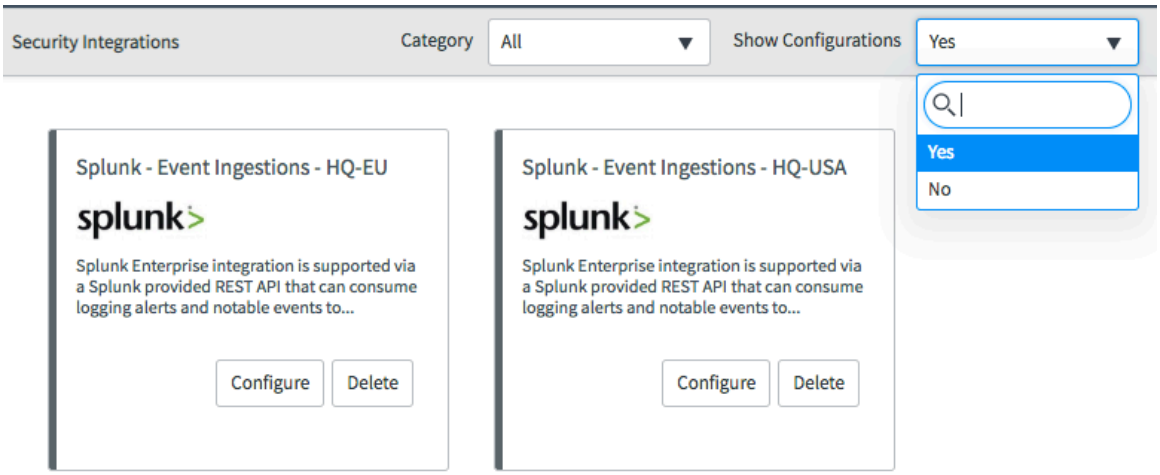
> **注:**
> ベーシック認証またはトークンベースの認証のいずれかを使用する必要があります。いずれかの認証を有効にし、対応する認証の詳細を入力します。両方を有効にすると、エラーが表示されます。

検証と送信が正常に完了すると、各 [イベントの取り込み] の Splunk サーバー構成は [セキュリティ統合] ページにタイルとして保存されます。保存された構成タイルが右上隅にある [セキュリ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ティ統合] ページに表示されていない場合、[構成を表示] 選択リストから [はい] をクリックします。



Trouble?

[送信] をクリックした後にエラーメッセージが表示された場合は、情報を再度入力し、[送信] をクリックします。

次のタスク
アプリケーションのインストールと設定が正常に完了しました。次のステップは、イベントプロファイルの作成です。

Splunk Enterprise イベントの取り込み設定の構成

Splunk Enterprise イベントの取り込み設定を使用して、事前設定された構成とその値を要件に従って変更します。

始める前に
必要なロール：sn_si.admin

手順

1. 次のように移動する。 **All** (すべて) > **Splunk Integration** > **Splunk Integration** 設定.
2. フォームの各フィールドに入力します。

Splunk Integration 設定

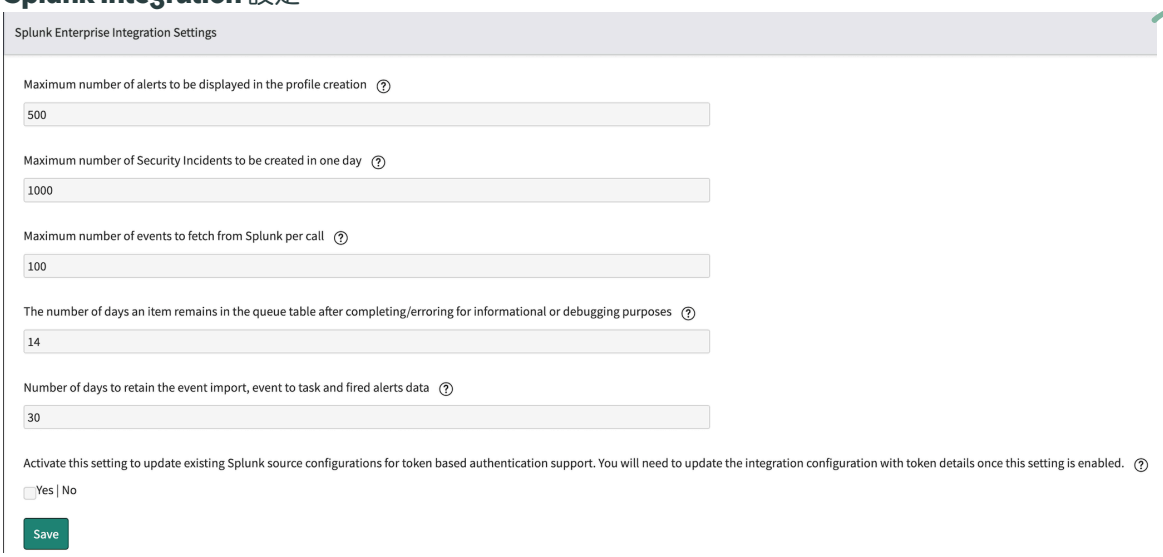
フィールド	説明
プロファイル作成時に表示されるアラートの最大数	イベントプロファイルの作成時に表示するアラートの最大数を定義するオプション。 デフォルト値は 500 に設定されています。
1 日に作成されるセキュリティインシデントの最大数	1 日に作成できるセキュリティインシデントの最大数を定義するオプション。 デフォルト値は 1000 に設定されています。
呼び出しごとに Splunk からフェッチするイベントの最大数	呼び出しごとに Splunk から取得するイベントの最大数を定義するオプション。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	デフォルト値は 100 に設定されています。
情報提供またはデバッグの目的で、完了/エラー発生後にアイテムがキューテーブルに保持される日数	情報提供またはデバッグの目的で、完了またはエラー発生後にアイテムがキューテーブルに保持される日数を定義するオプション。 デフォルト値は 14 に設定されています。
イベントインポート、タスクに対するイベント、および発生したアラートデータを保持する日数	イベントインポート、タスクに対するイベント、および発生したアラートデータを保持する日数を決定するオプション。 デフォルト値は 30 に設定されています。
トークンベースの認証をサポートする既存の Splunk ソース構成を更新するには、この設定をアクティブ化します。この設定を有効にしたら、トークンの詳細を使用して統合構成を更新する必要があります。	既存のバージョンからトークンベースの認証をサポートする既存の Splunk ソース構成を更新するオプション。 **注:** 新しいバージョンにアップグレードすると、トークンフィールドは使用できなくなります。トークンベースの認証を取得するには、この設定を有効にし、その後、トークンの詳細を使用して統合構成を更新する必要があります。 デフォルト値は [いいえ] に設定されています。

Splunk Integration 設定



3. [保存] をクリックします。

Splunk Enterprise Event Ingestion 統合でのイベントプロファイルの作成と名前の設定

Now Platform インスタンスにイベントプロファイルを作成し、セキュリティインシデントを作成する Splunk アラートを指定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_si.admin

このタスクについて
Now Platform セキュリティインシデントレスポンス(SIR) セキュリティインシデントが取り込まれたアラートから作成される前に、アラートのフィールド値が Now Platform セキュリティインシデントのレイアウトに表示されるため、実際のセキュリティインシデントがどのように表示されるかをプレビューできます。

利用可能な API を使用する統合の観点から、Splunk イベントは個別のイベントとして個別に手動で転送されるか、Now Platform インスタンスの セキュリティオペレーション 環境に自動的に取り込まれるトリガーされたアラートに結合されます。統合ワークフローでは、不正なアクセス試行やマルウェアなどのさまざまなタイプのアラートを取り込めます。

これらのアラートは、インスタンスの セキュリティオペレーション 環境で設定したプロファイルに基づいて取り込まれます。すべてのアラートは、最初にプロファイル内の設定されたアラートタイプに対して取り込まれます。取り込まれたアラートをさらにフィルタリングして、セキュリティインシデントを作成するアラートを指定できます。たとえば、高リスクとして識別されたアラートに対してのみセキュリティインシデントを作成するフィルターを使用できます。プロファイルが有効になり、取り込まれたアラートからセキュリティインシデントが作成される前に、フィルタリングされたアラートの個々のフィールド値が、プレビュー用のセキュリティインシデントのレイアウトの対応するフィールドにマッピングされます。

Now Platform インスタンス内のイベントプロファイルのアラート名は一意である必要があり、常に 1 つのアクティブなイベントプロファイルにのみマッピングできます。これらは、統合のセットアップの一部として Splunk サービスで構成したトリガーアラート名です。Splunk Enterprise 環境でアラートを設定する方法の詳細については、「Splunk Enterprise Event Ingestion 統合での Splunk Enterprise コンソールへの検索の保存」を参照してください。

Now Platform は、統合のワークフローを使用して特定のアラートを取り込みます。Splunk Enterprise コンソールの選択基準を満たすすべてのアラートが、最初に Now Platform インスタンスに取り込まれます。

Now Platform のプロファイルは、Splunk Enterprise コンソールの Splunk アラートをカプセル化したものです。プロファイルとともに取り込まれたアラートと Splunk Enterprise コンソールへの接続は 1 対 1 の関係 (1 つの接続に対して 1 つのアラート) です。Splunk Enterprise コンソールにはサーチヘッドへの単一の https 接続があります。単一のサーチヘッドから複数のアラートを取得できます。Splunk Enterprise コンソールで複数のサーチヘッドに接続する場合は、これらのアラートを取り込むために Now Platform インスタンスに複数のプロファイルを作成する必要があります。

スケジュール済みアラートの取り込みのためにプロファイルを作成するステップ

手順

1. アラートのイベントプロファイルを作成するには、 Now Platform インスタンスで **Splunk Integration** > **Splunk** イベントプロファイル.
2. [Splunk イベントプロファイル] フォームが表示されない場合は、進捗状況バーの [名前] をクリックします。
3. [新規] をクリックします。
4. フィールドに入力します。

   完成したフォームの例が表の後に表示されます。

自動翻訳

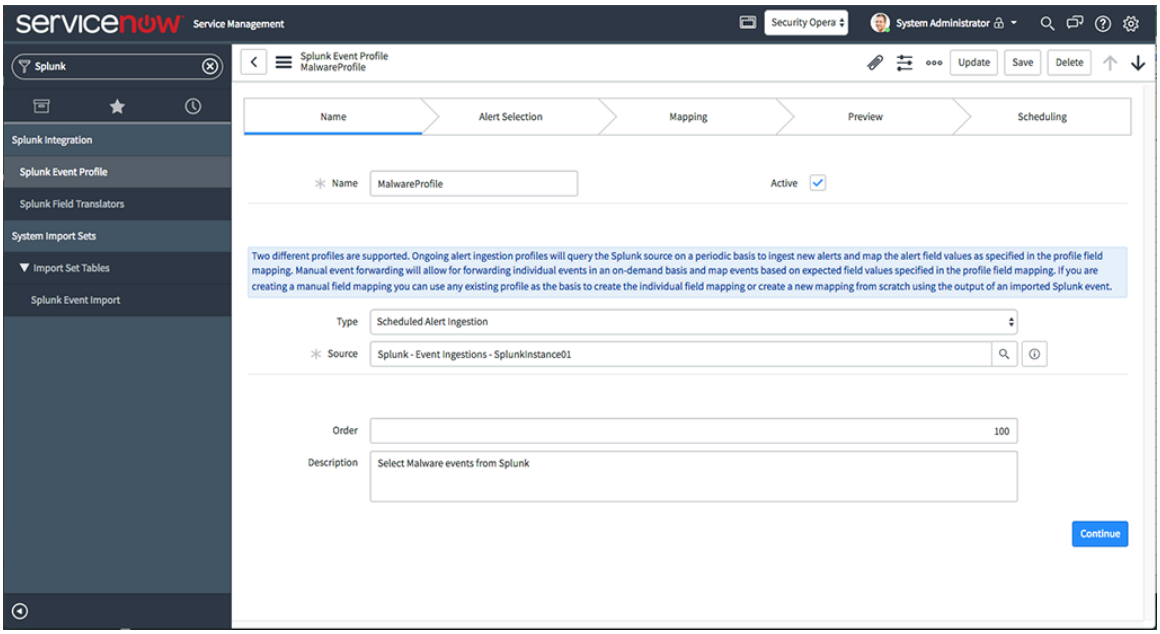
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
名前	プロファイルの一意の名前。名前が一意でない場合、重複するプロファイル名は保存されません。 Now Platform インスタンスのプロファイル名は一意である必要があります。
アクティブ	デフォルトでは、このチェックボックスはクリアされます。 [アクティブ] オプションは無効になり、すべてのプロファイル設定ステップを完了して [完了] をクリックするまで選択できません。
タイプ	選択リストからプロファイルタイプを選択します。 ○ スケジュール済みアラートの取り込み - このタイプのプロファイルは、設定したスケジュールで取り込まれるトリガーアラートをサポートします。フィールドに入力し、[続行] をクリックして、プロファイルのアラート選択ステップに進みます。 ○ 手動イベント転送 - このタイプのプロファイルは、オンデマンドで Splunk Enterprise コンソールから手動で転送される個々のイベントをサポートします。これらのタイプのプロファイルのフォームに入力するには、次のステップを参照してください。
ソースタイプ	アラートを取り込むために構成された Splunk サーバーまたは検索終了。複数の Splunk サーバーが構成されている場合は、プロファイルに取り込む予定のアラートタイプに適したサーバーを選択します。値を入力する必要があります。
順序	デフォルトは 100 です。この設定はデフォルトのままにします。 複数のプロファイルを作成した場合、この値は、2 つ以上のプロファイルが同じトリガー条件を共有する場合の実行時の優先度を示します。プロファイル内の番号が最も小さいワークフローの優先度が最も高くなります。
(オプション) 説明	このプロファイルを他のプロファイルと区別するためのテキスト。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図は、スケジュール済みアラートの完成したフォームの例です。



5. スケジュール済みアラートがあるプロファイルの場合は、プロファイル構成を続行するオプションを 1 つ選択します。
   手動イベント転送用のプロファイルの作成ステップ
6. 手動イベント転送をサポートするプロファイルを作成するには、次のステップを実行します。

   Splunk Enterprise コンソールからオンデマンドで転送するイベントの場合、既存のプロファイルに基づいて個々のフィールドマッピングを行うことができます。または、エクスポートされた添付ファイルデータの新しいマッピンググリッドを作成することもできます。手動で転送するイベントは、イベントプロファイルでスケジュールされません。

   a. まだ選択されていない場合は、[タイプ] フィールドの選択リストで [手動イベント転送] を選択します。

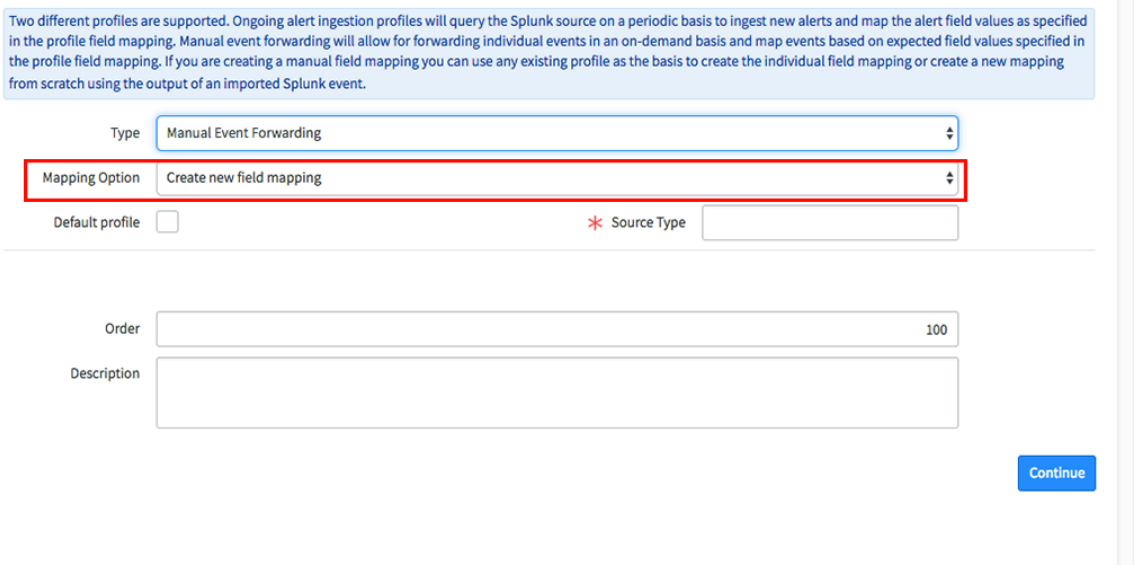
   b. 表示される [マッピングオプション] フィールドで、選択リストからマッピングオプションを 1 つ選択して続行します。

      [マッピングオプション] 選択リストで利用可能なマッピングオプションの詳細については、次の図とテーブルを参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

新しいフィールドマッピングオプションの作成



新しいフィールドマッピングオプションの作成

オプションまたはフィールド	説明
新しいフィールドマッピングオプションの作成	イベントの新しいフィールドマッピング。 作成しているプロファイルに類似した既存のフィールドマッピングがない場合は、このオプションを選択して新しいマップを作成します。
デフォルトプロファイル	すべての Splunk イベントのデフォルトのイベント転送プロファイル。デフォルトはクリア (無効化) されています。 このオプションを有効にすると、このプロファイルが手動イベント転送のデフォルトプロファイルになります。このプロファイルはアクティブで、SIR セキュリティインシデントへのすべての Splunk イベントフィールドマッピングで使用される唯一のプロファイルです。1 つのプロファイルがすべての転送イベントに適合します。 デフォルトのプロファイルオプションが有効になっている場合、 [ソース] フィールドは使用できません。
ソースタイプ	Splunk サーバー。 デフォルトのプロファイルオプションが有効になっている場合、このフィールドは使用できません。 利用可能な場合、 [ソースタイプ] オプションでは、Splunk ソース タイプに基づいてセ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプションまたはフィールド	説明
	キュリティインシデントフィールドに一意のイベントフィールドをマッピングできます。 エンドポイント検出イベントとは異なる方法でファイアウォールログイベントを管理する必要があり、それらのイベントの Splunk ソースタイプが異なる場合は、ソースタイプに基づいて異なるイベントプロファイルを作成して、この要件を満たすことができます。
順序	デフォルトは 100 です。この設定はデフォルトのままにします。 多数のプロファイルを作成した場合、この値は、2 つ以上のプロファイルがトリガー条件を共有する場合の実行時の優先度を示します。プロファイル内の番号が最も小さいワークフローの優先度が最も高くなります。
(オプション) 説明	このプロファイルを他のプロファイルと区別するためのテキスト。

新しいフィールドマッピングがあるプロファイルの場合は、[ソースタイプ] フィールドに値を入力したことを確認してから、[続行] をクリックして構成のマッピングステップに進みます。

既存のフィールドマッピングがあるプロファイルの詳細については、次の図とテーブルを参照してください。

フィールドマッピングオプションの既存のプロファイルの選択

フィールドマッピングオプションの既存のプロファイルの選択

オプションまたはフィールド	説明
フィールドマッピングの既存のプロファイルを選択	イベントの既存のフィールドマッピング。 [プロファイルからコピー] フィールドが表示されます。 このプロファイルの既存のフィールドマッピングをコピーするには、次のステップを実行します。 **i.** 表示される [プロファイルからコピー] フィールドの左側にある検索アイコンをクリックします。 **ii.** 表示される [Splunk イベントプロファイル] リストで、コピーするマップが含まれるプロファイル名をクリックします。 プロファイル名が [プロファイルからコピー] フィールドに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプションまたはフィールド	説明
デフォルトプロファイル	すべての Splunk イベントのデフォルトのイベント転送プロファイル。デフォルトはクリア (無効化) されています。 このオプションを有効にすると、このプロファイルが手動イベント転送のデフォルトプロファイルになります。このプロファイルはアクティブな唯一のプロファイルです。SIR セキュリティインシデントへの Splunk イベントフィールドのマッピングごとに使用されます。1 つのプロファイルがすべての転送イベントに適合します。 デフォルトのプロファイルオプションが有効になっている場合、 [ソース] フィールドは使用できません。
ソースタイプ	Splunk サーバー。 デフォルトのプロファイルオプションが選択されている場合、このフィールドは使用できません。 利用可能な場合、 [ソースタイプ] オプションでは、Splunk ソースタイプに基づいてセキュリティインシデントフィールドに一意のイベントフィールドをマッピングできます。 エンドポイント検出イベントとは異なる方法でファイアウォールログイベントを管理する必要があり、それらのイベントの Splunk ソースタイプが異なる場合は、ソースタイプに基づいて異なるイベントプロファイルを作成して、この要件を満たすことができます。
順序	デフォルトは 100 です。この設定はデフォルトのままにします。 複数のプロファイルを作成した場合、この値は、2 つ以上のプロファイルがトリガー条件を共有する場合の実行時の優先度を示します。プロファイル内の番号が最も小さいワークフローの優先度が最も高くなります。
(オプション) 説明	このプロファイルを他のプロファイルと区別するためのテキスト。

プロファイルの既存のマッピングを選択するフォームの下部で、[完了] をクリックしてプロファイルの構成を完了します。

次のタスク

スケジュール済みアラートと手動イベント転送の両方のプロファイルを作成するステップを正常に完了しました。手動イベント転送のプロファイルの場合は、プロファイルの構成が完了しました。次のステップでは、マッピングステップで添付ファイルデータをロードします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済みアラートのプロファイルの場合、次のステップでは自動取り込みのアラートを選択します。

Splunk Enterprise Event Ingestion 統合でのスケジュール済みアラートの選択

スケジュール済みアラートのプロファイルを作成したら、Now Platform セキュリティインシデントレスポンス セキュリティインシデントにマップするこのプロファイルの Splunk アラートを選択します。

始める前に
必要なロール：sn_si.admin

このタスクについて
Now Platform インスタンスで利用可能なアラートを表示して、マッピングに利用可能なフィールド値を確認します。SIR セキュリティインシデントのフィールドに値をマップする前に、アラートを選択して、基本フォームレイアウトで期待する結果が得られることを確認します。このフォームのリストから選択できるアラートは 1 つだけです。

手順

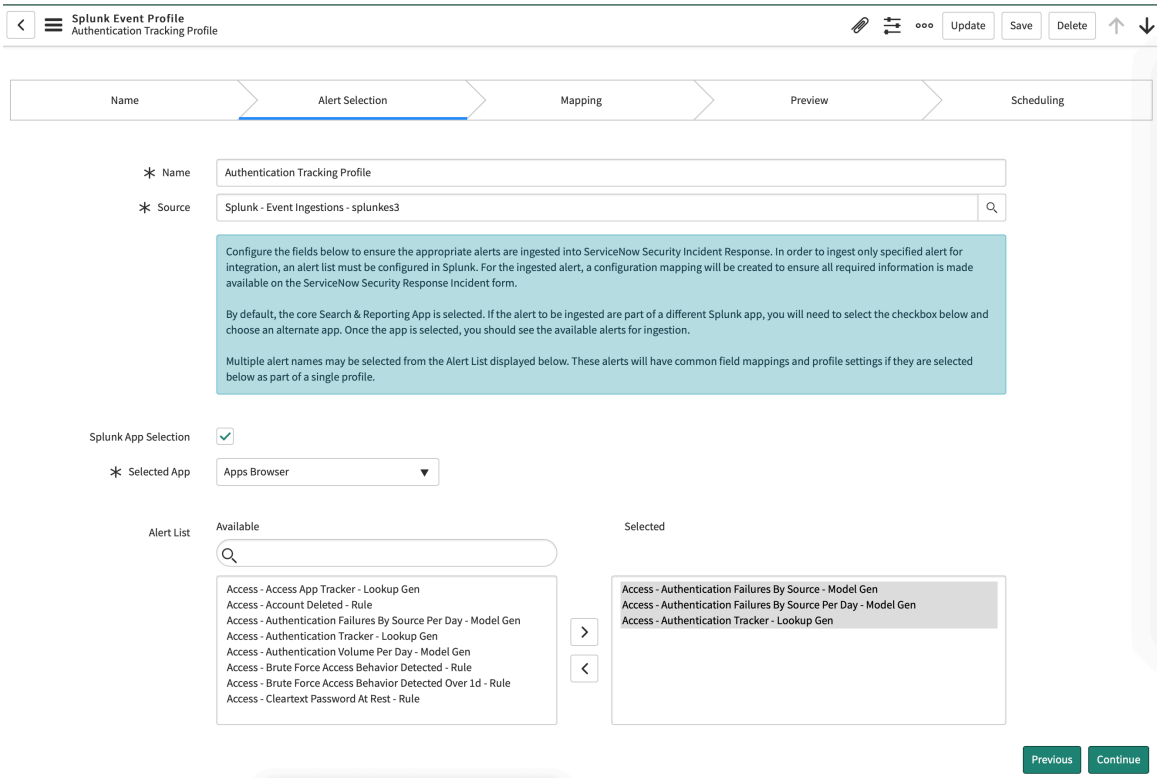
1. [アラートの選択] ページが表示されない場合は、進捗状況バーで選択して表示します。
   デフォルトでは、Search & Reporting コアアプリが選択されています。
2. 取り込むアラートが別の Splunk アプリの一部である場合は、**[Splunk** アプリの選択] を選択し、[選択したアプリ] リストから Splunk アプリを選択します。
3. [アラートリスト] からアラートを選択し、[利用可能] 列から [選択済み] 列に移動します。
   複数のアラートを選択することもできます。アラートが単一のプロファイルの一部として選択されている場合、アラートには共通のフィールドマッピングとプロファイル設定が含まれます。

   このフォームのアラートのリストは、Splunk コンソールのアラートのリストと一致します。このフォームには最大 500 件のアラートが表示されます。[アラート] ページの Splunk コンソールに 500 件を超えるアラートがリストされている場合、Now Platform インスタンスのこのフォームには最初の 500 件のアラートのみが表示されます。

オプション	説明
[アラートリスト] 検索フィールドにテキストを入力します。	検索フィールドの下の列は、入力したテキストに基づいて利用可能なオプションでフィルタリングされます。アラートを選択し、矢印キーを使用して、選択したアラームを [利用可能] から [選択済み] に移動します。
[アラート] リストで、アラートをダブルクリックします。	[選択済み] 列に選択内容が入力されます。
[アラートリスト] で、アラームルールをシングルクリックします。	アラームが選択されます。矢印キーを使用して、選択したアラームを [利用可能] から [選択済み] に移動します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. オプションを 1 つ選択して続行します。

次のタスク
スケジュール済みアラートプロファイルのアラートが正常に選択されました。次のステップでは、アラート値をセキュリティインシデントのフィールドにマップします。

Splunk Enterprise Event Ingestion 統合のアラートとイベントのマッピング

スケジュール済みアラートの取り込みまたは手動イベント転送のソースを特定したら、次のステップでは、個々のイベントフィールドを Now Platform セキュリティインシデントレスポンス (SIR) セキュリティインシデントのフィールドにマッピングします。

概要

マッピング手順では、sn_si.admin ロールを持つユーザーとして、Splunk Enterprise コンソールからサンプルアラートを取り込むか、Splunk Enterprise イベントのイベントデータをエクスポートします。

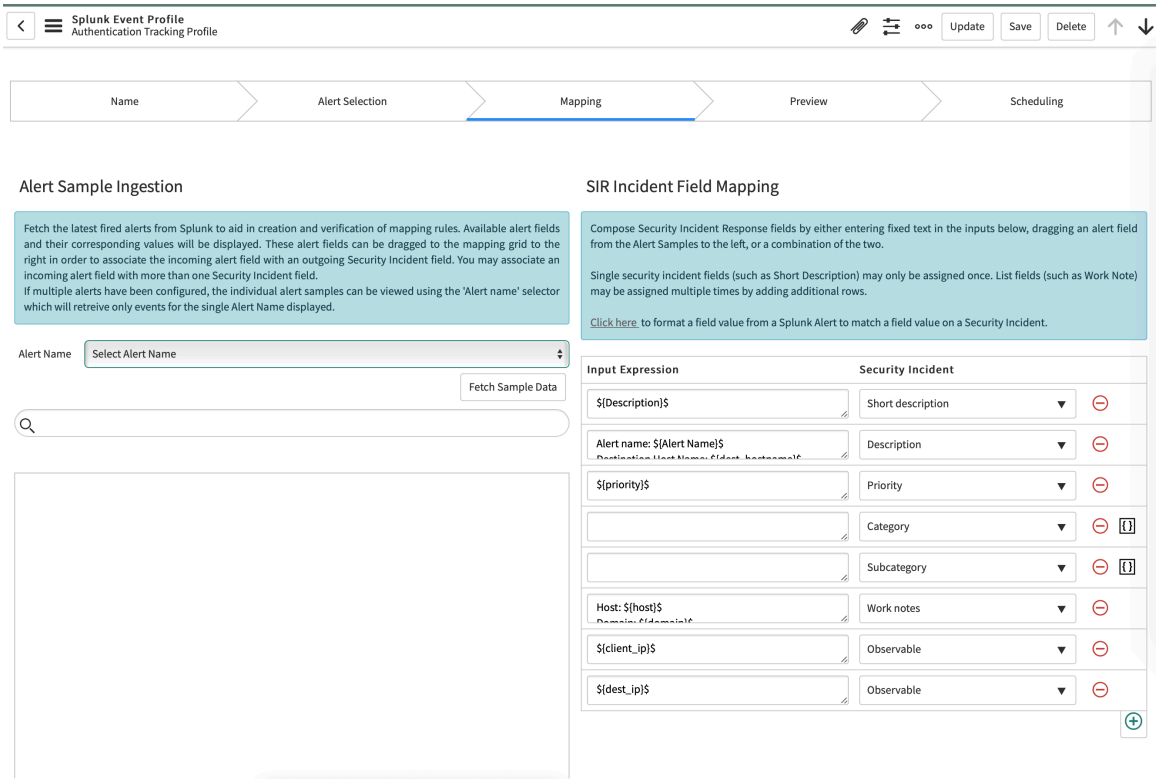
次の図は、イベントプロファイルのタイプごとに提供されるデフォルトのマッピンググリッドの例です。このデフォルトのマッピングは編集できます。この変更により、セキュリティインシデントを入力するフィールドをカスタマイズできます。マッピングステップでは、イベントフィールドの追加または削除が SIR セキュリティインシデントフィールド値にどのように影響するかを視覚化できます。

[アラート名] を選択し、[サンプルデータをフェッチ] をクリックして、サンプルアラートがプロファイルで取り込まれるとフォームの左側に Splunk アラートフィールド値がが入力されます。これらは、SIR セキュリティインシデントフィールドにマップする Splunk アラートフィールドです。

自動翻訳

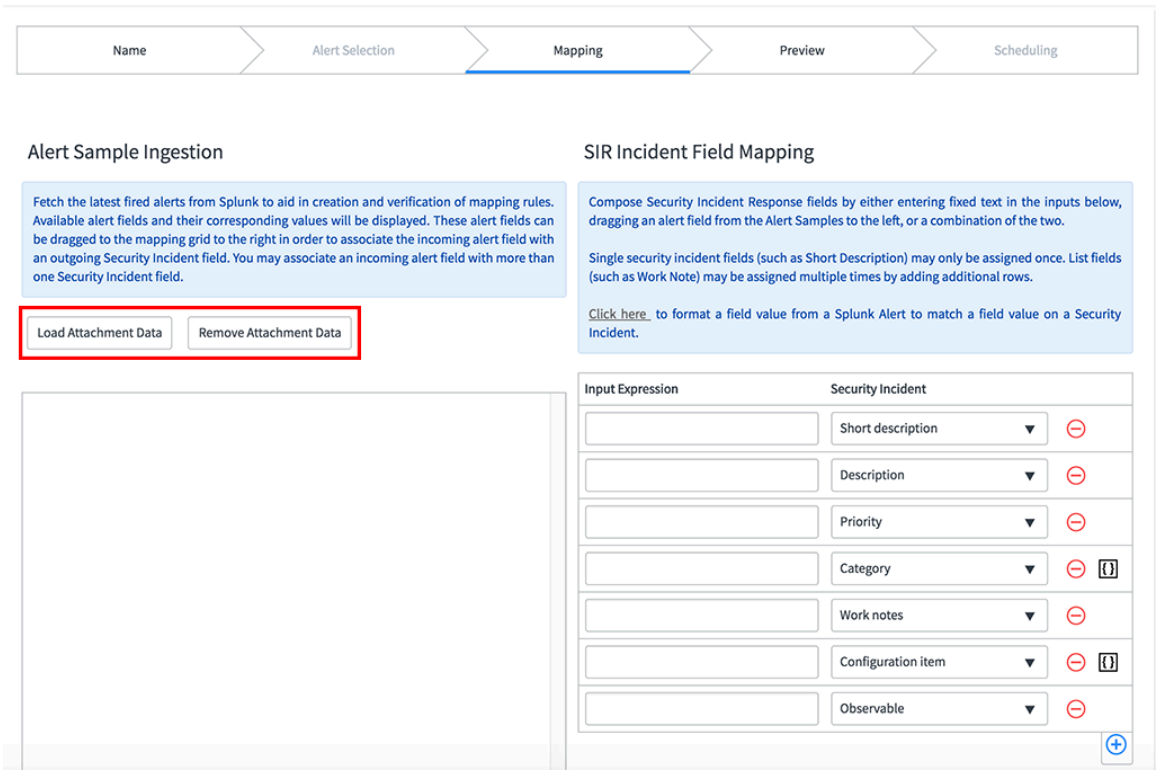
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アラートのデフォルトのマッピングフォーム



クリックして転送されたイベントの添付ファイルデータをロードすると、フォームの左側に Splunk イベントフィールドが入力されます。これらは、SIR セキュリティインシデントフィールドにマップする Splunk データフィールドです。

転送されたイベントのデフォルトのマッピングフォーム



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Splunk コンソールでいくつかのサンプルアラートを確認して、フィールドマッピング構成ステップに取り込むこともできます。このステップは、進捗状況バーで [マッピング] とラベル付けされます。このページが表示されない場合は、進捗状況バーの [マッピング] をクリックします。

Splunk エンタープライズコンソールからのアラートのマッピングとイベントのオンデマンドエクスポートには、次の概念とタスクが含まれます。

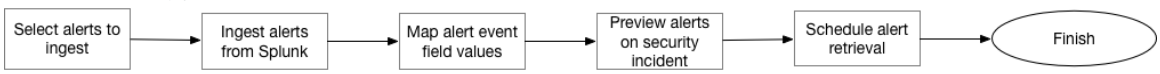
- 自動的に取り込まれたアラートプロファイルのサンプルデータをフェッチします。Splunk Enterprise コンソールで発生したアラートからデータがフェッチ (プル) されると、使用可能なアラートフィールドとそれに対応する値が、マッピングフォームの左側にあるデフォルトのマッピングレイアウトに表示されます。プルしたアラート ID の値を表示するタブが表示されます。フォームの左側にある [アラートサンプルの取り込み] セクションのすべての重要なフィールドが、フォームの右側のグリッドにマッピングされていることを確認します。
- 必要に応じて、手動で転送されたイベントプロファイルのイベントサンプルデータをロードします。これらのイベントのサンプルデータは、Splunk Enterprise コンソールから .xml ファイルにエクスポートされ、Now Platform インスタンスにロードされます。インポートされたデータは、フォームの左側にある [アラートサンプルの取り込み] セクションに表示されます。
- 左側からアラートをドラッグして、右側のマッピンググリッドにドロップし、マッピング構成を編集します。右側のマッピンググリッドで、[受信アラート] フィールドを [送信セキュリティインシデント] フィールドに関連付けることができます。
- フィールドを追加または削除して、マッピンググリッドをカスタマイズします。提供されている色分けを使用して、見落とされているフィールドや重複フィールドを追跡します。
- SIR アプリケーションに取り込むアラートと除外するアラートを指定できるように、フィルター条件を設定します。
- インシデントが重複しないように、既存の SIR セキュリティインシデントに受信アラートを集計する追加のインシデントフィールド基準を定義します。この追加のフィルタリングにより、関連するすべてのセキュリティイベントデータを単一のセキュリティインシデントに配置することで、アクティブな重複するセキュリティインシデントの数を減らすことができます。
- 特定の場合、Splunk Enterprise コンソールは SIR セキュリティインシデントのフィールドに直接変換されないことがあります。これらの値については、マッピングステップでスクリプトエディターを使用してセキュリティインシデントのフィールド値をフォーマットできます。類似しているが同一ではない値をフォーマットする場合は、スクリプトエディターを使用します。たとえば、スクリプトエディターを使用すると、Splunk コンソールの [マルウェアアラート] フィールドと [ウイルス感染] フィールドの値は、どちらも SIR セキュリティインシデントの [カテゴリ] フィールドの [悪意のあるコードアクティビティ] に変換されます。

自動翻訳

スケジュール済みアラートプロファイル

スケジュール済みアラートプロファイルを作成した後の構成のプロセスフローを次の図に示します。

スケジュール済みアラートプロファイルのプロセスフロー

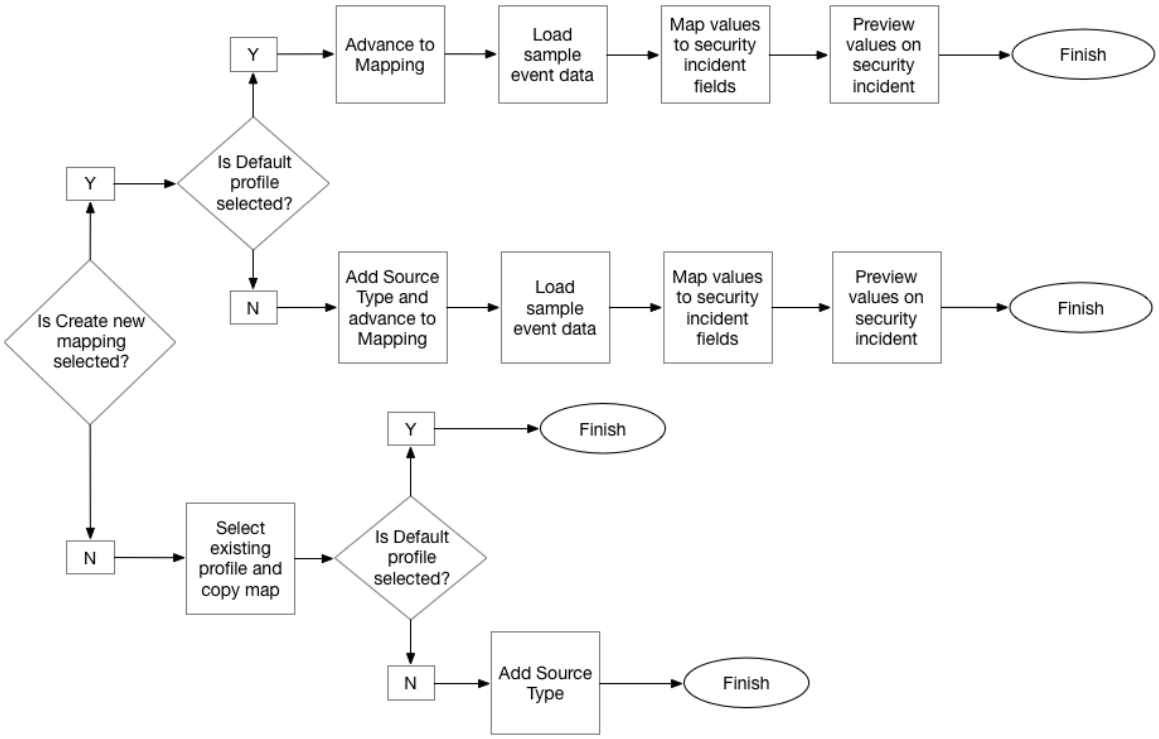


手動イベント転送プロファイル

イベントのプロファイルを作成した後の構成のプロセスフローを次の図に示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

イベントプロファイルのプロセスフロー



次のステップでは、トリガーされたアラートまたはエクスポートデータを取り込み、値を SIR セキュリティインシデントフィールドにマップします。

Splunk Enterprise Event Ingestion 統合でのアラートのマッピング

イベントフィールドマッピングのステップでは、トリガーされたアラートまたはインポートされたイベントデータの個々のイベントフィールドを Now Platform セキュリティインシデントレスポンス (SIR) セキュリティインシデントのフィールドにマップします。

始める前に

必要なロール：sn_si.admin

このタスクについて

デフォルトのセキュリティインシデントフィールドの事前設定されたマッピンググリッドを編集できます。イベントフィールドの色分けは、既にマッピングされているフィールド値を監視するのに役立ちます。このステップは、編集がセキュリティインシデントのフィールドにどのように影響するかを視覚化するのに役立ちます。

フォームの左側にある [アラートサンプルの取り込み] 列から、右側の [SIR インシデントフィールドマッピング] 列のセキュリティインシデントフィールドに最大 5 つのアラートをマッピングします。

フォームの右側にあるマッピンググリッドのフィールドを追加または削除して、カスタムマッピングを作成します。フィールドをカスタマイズすると、SIR セキュリティインシデントのデフォルトのマッピンググリッドに表示されていない Splunk フィールドをマッピングできます。

手順

1. このマッピングフォームが表示されない場合は、進捗状況バーの [マッピング] をクリックします。
2. [アラームサンプルの取り込み] の下にあるスケジュール済みアラートプロファイルの場合、[アラート名] でアラートを選択し、[サンプルデータをフェッチ] をクリックして Splunk Enterprise コンソールから発生したアラートの最新のインスタンスをプルします。

   アラートはタブとして表示されます。最新のアラートを最大 5 件取り込むことができます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

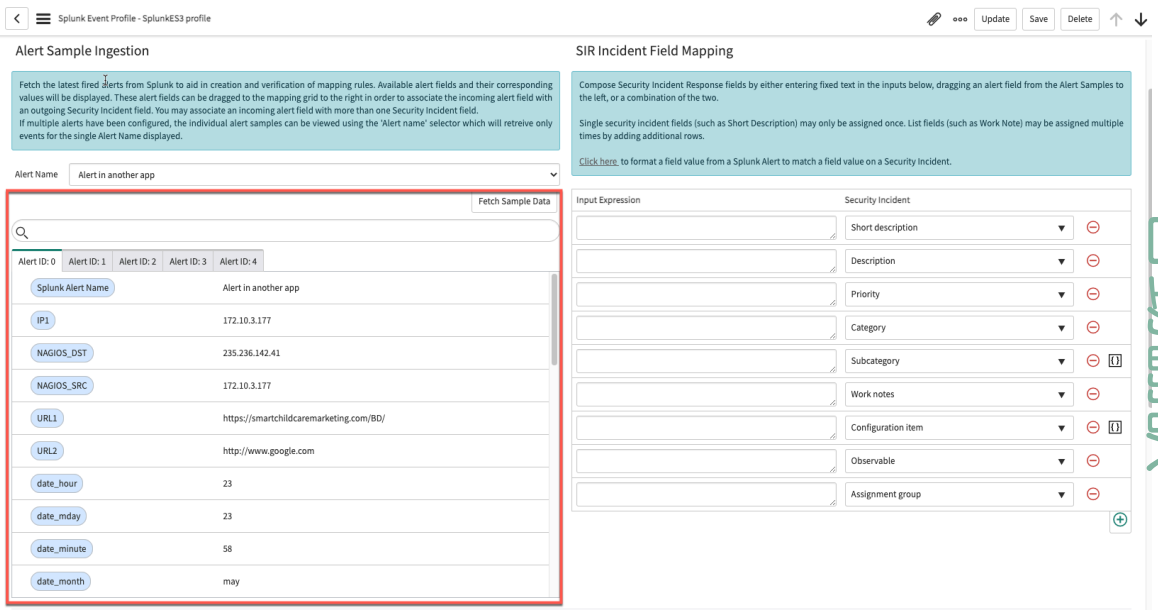
自動翻訳

サンプルイベントのプルには少し時間がかかる場合があります。トランザクションが機能していることを示すメッセージが画面の上部に表示されます。

> **注:**
> 追加のマッピングフィールド **[Splunk** アラート名] が統合によって追加され、Splunk のソースアラートルールまでイベントを追跡できます。これは、複数の Splunk アラートが単一のプロファイルに結合されているシナリオで役立つ可能性があります。

1 つのフィールドに複数の値が含まれている場合、それらの値は解析され、[SIR インシデントフィールドマッピング] セクションの個々のフィールドエントリーにマップされます。たとえば、ソース IP アドレス、資産名、または URL に複数の観測事象フィールドエントリーまたは複数の CI がある場合、それらは解析され、[SIR インシデントフィールドマッピング] セクションの個々のフィールドエントリーにマップされます。

次の図では、プルの完了後に、取り込まれたアラートまたはインポートされたサンプルイベントのフィールド名値のペアがこのフォームの左側に表示されます。これらの値は、フォームの [SIR インシデントフィールドマッピング] 側のセキュリティインシデントフィールドにマッピングする値です。



3. スケジュール済みアラートプロファイルの場合は、ステップ 5 に進んで値をマッピングします。
4. または、Splunk Enterprise コンソールからエクスポートするイベントタイプのプロファイルの場合は、次の手順に従って Now Platform® インスタンスに添付ファイルデータをアップロードします。

   a. まだログインしていない場合は、Splunk Enterprise コンソールにログインします。

   b. [検索] タブに移動し、エクスポートするイベントデータを含む検索の名前を入力します。

      たとえば、「マルウェア」は、この統合のワークフローで転送できるすべてのマルウェアイベントに使用される検索用語です。

   c. イベントを展開し、[フィールド] 列でインポートするフィールドを選択します。

      これらのフィールドは、Now Platform® インスタンスの [マッピング] ページにエクスポートされて表示されるフィールドと値のペアです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

d. Splunk Enterprise コンソールの [検索] ページの右上にある [エクスポート] アイコンをクリックします。

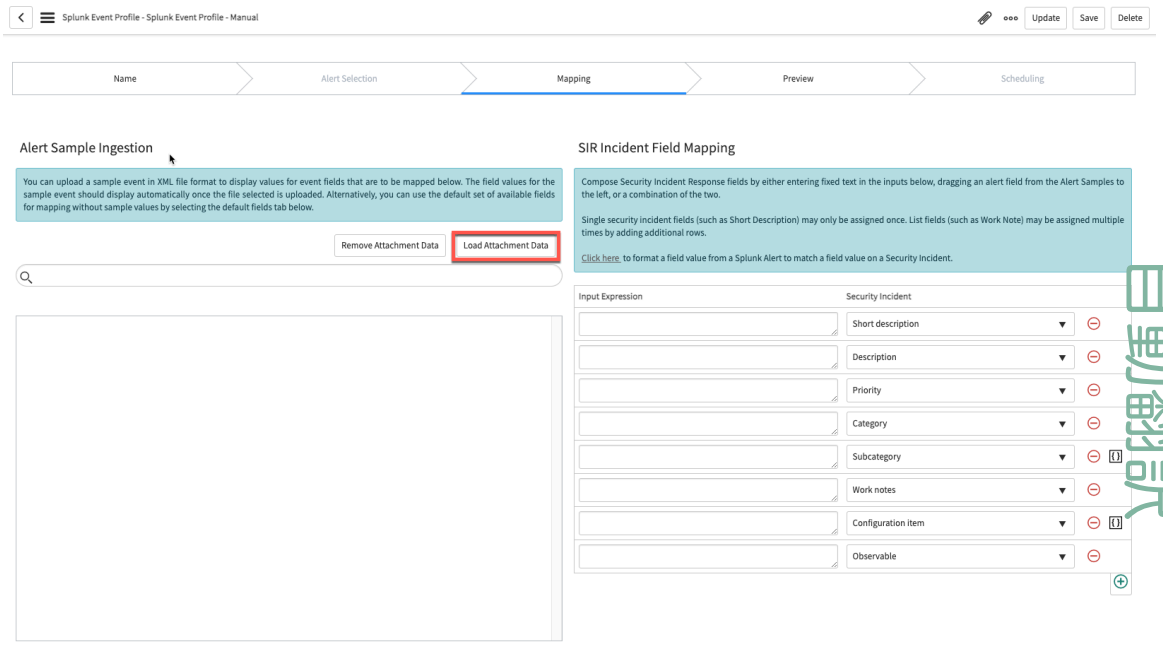
e. 表示されるダイアログの [形式] フィールドのリストで、**[XML** 形式] をクリックします。

f. オプション: 新しいファイル名を入力します。

g. [エクスポート] をクリックします。
ファイルが Now Platform® インスタンスにダウンロードされます。

h. Now Platform® インスタンスに [マッピング] ページが表示されない場合は、進捗状況バーの [マッピング] をクリックします。

i. [アラートサンプルの取り込み] 列で、[添付ファイルデータのロード] をクリックします。



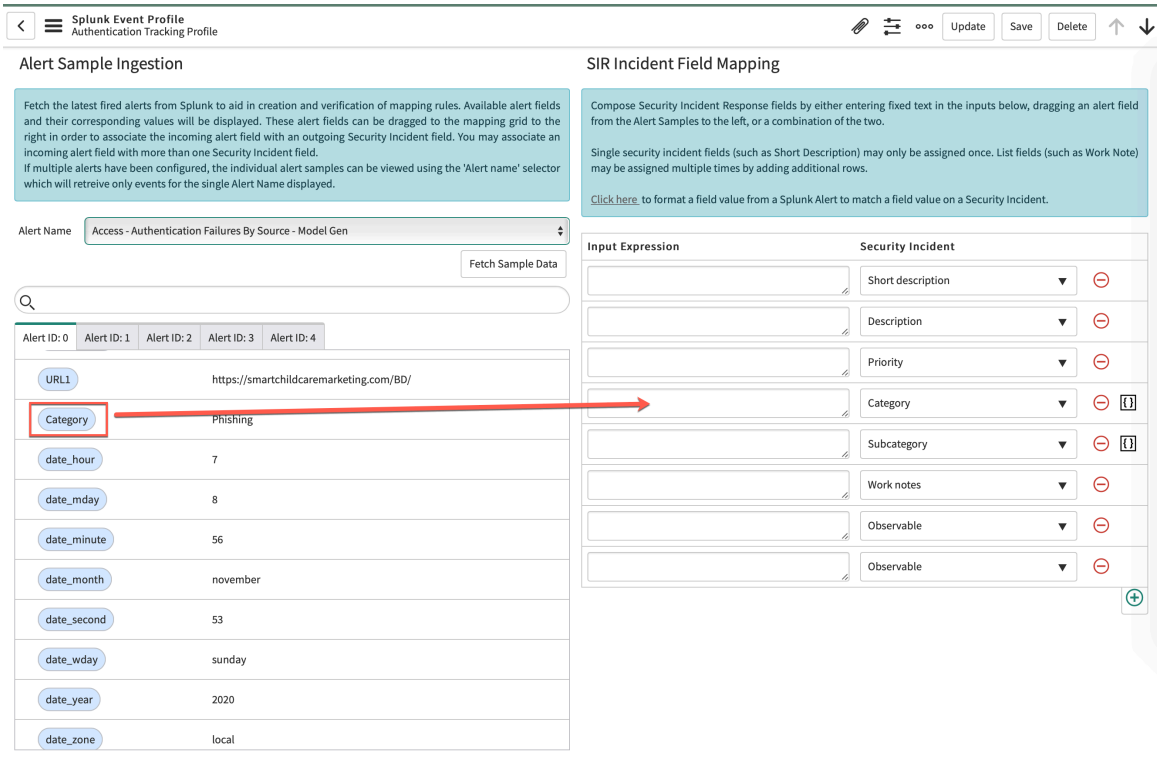
j. 表示されるダイアログで、[ファイルを選択] をクリックし、エクスポートした .xml ファイルに移動して、[開く] をクリックします。
イベントに対してエクスポートしたフィールドの値のペアが、マッピングフォームの左側に表示されます。

次の図では、取り込まれたスケジュール済みアラートのデータペアがこのフォームの左側に表示されています。インポートされたイベントの値のペアもフォームのこちら側に表示されます。これらの値は、フォームの [SIR インシデントフィールドマッピング] 側のセキュリティインシデントフィールドにマッピングするフィールド値です。

5. フォームの左側からフォームの右側のセキュリティインシデントのフィールドにフィールド値をマッピングするには、フォームの左側で青色のフィールド名をクリックしたままにします。

6. フィールド名 (カテゴリなど) をドラッグして、[セキュリティインシデント] 列のフィールド名の横にある [入力式] 列のフィールドにドロップします。

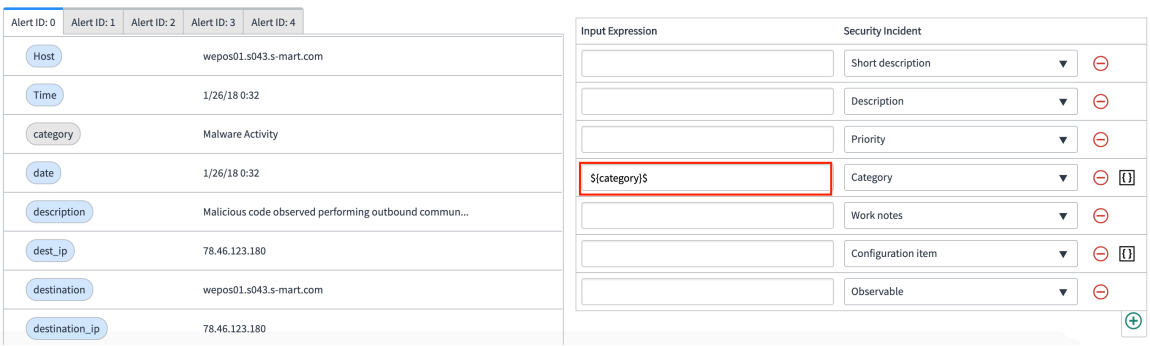
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



フィールド値が [入力式] 列に表示されます。次の画像では、category がセキュリティインシデントの [カテゴリ] フィールドにマップされます。ただし、左側から右側のフィールドまでの任意の値を一致させることができます。プレビューステップで、セキュリティインシデントの値が正しくマッピングされていることを確認します。

マッピングプロセスでイベントが見落とされたり、重複したりしないようにするために、フィールドは色分けされています。左側のライトブルーのフィールドは、フィールドがまだ未選択で、セキュリティインシデントにマップされていないことを示します。受信アラートフィールドをセキュリティインシデントの 1 つ以上のフィールドに関連付けることができます。

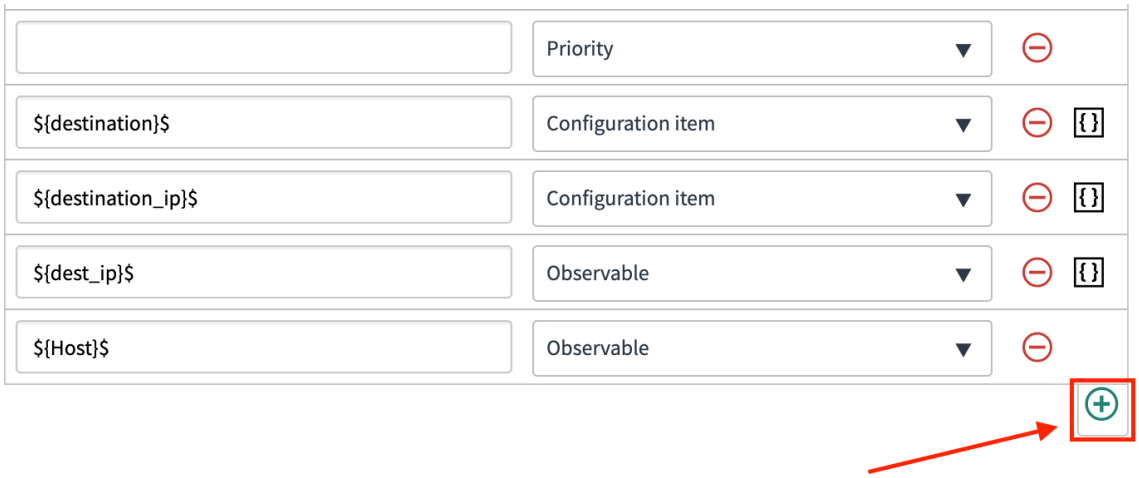
灰色のフィールドは、フィールドが選択され、セキュリティインシデントのフィールドにマッピングされていることを示します。場合によっては、アラートイベントフィールドが 1 回しか割り当てられないことがあるため、この色分けはマッピングの追跡に役立ちます。たとえば、 [簡単な説明] などのフィールドに値を割り当てることができるのは 1 回のみです。ただし、マッピンググリッドに行を追加することで、作業メモなどのリストフィールドを複数回割り当てることができます。



7. フォームの右側のセキュリティインシデントのデフォルトマッピングにフィールドを追加するには、次のステップを実行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

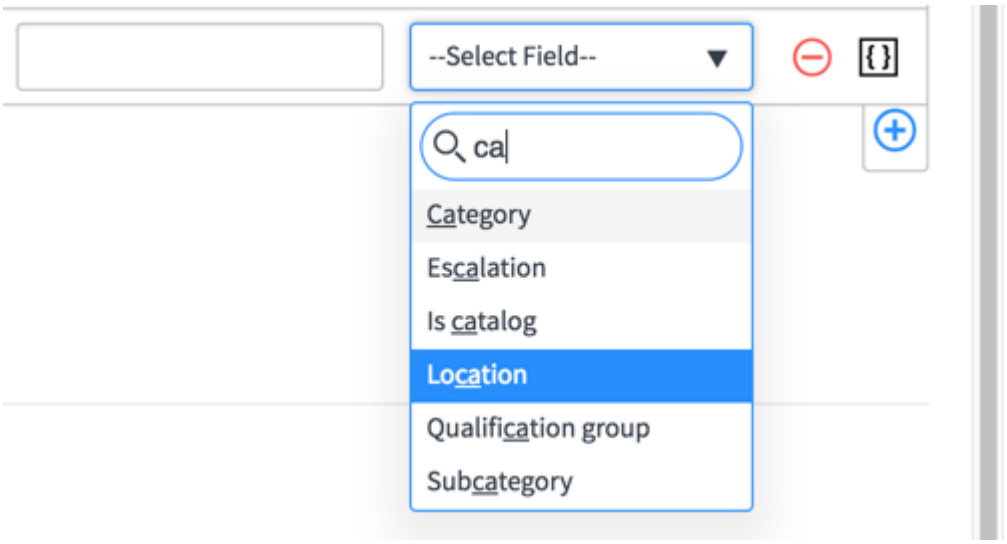
a. フォームの右側の [SIR インシデントフィールドマッピング] セクションで、グリッドの下部にあるプラスアイコンをクリックします。



新しいフィールドが表示されます。

b. [セキュリティインシデント] 列で表示されているリストを展開し、フィールドを選択します。

新しいフィールドの展開されたリストでは、一部のフィールドが網掛けされています。次の図では、セキュリティインシデントにマッピングされているため、カテゴリのバックグランドがグレーになっています。フォームの左側のアラートフィールドの色分け同様、右側のセキュリティインシデントフィールドのこの色分けも、マッピングの追跡に役立ちます。



自動翻訳

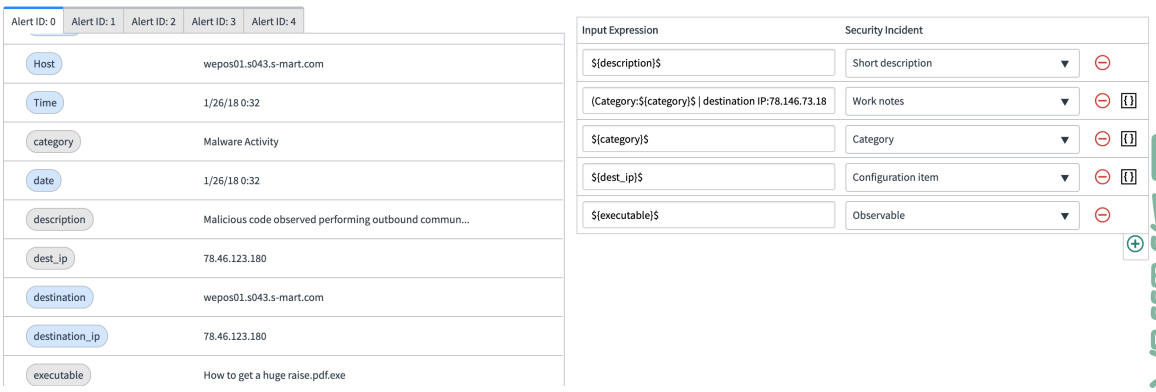
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> 同じセキュリティインシデントに複数の観測事象を表示できるため、[観測事象] フィールドを異なる値で複数回マップできます。同様に、[構成アイテム] フィールドと [作業メモ] フィールドは複数の値をサポートします。複数の値をサポートできないフィールドに 2 つの値をマッピングしようとすると、インシデントをプレビューするときに、フィールドに値がないことを示すエラーメッセージが表示されます。同様に、セキュリティインシデントのフィールドに複数のオプションを選択できるリストがあり、リストに表示されていないフィールドにオプションをマップしようとすると、そのフィールドはセキュリティインシデントに入力されません。

c. または、新しい行の [検索] フィールドに値を入力します。

d. フォームの左側の [入力式] フィールドに入力する [アラート **ID]** を左クリックして選択します。ドラッグ機能を使用して、新しいフィールドの横にマッピングします。

8. フィールドを追加または削除し、値をマップに追加してマッピングを続行します。
次の図は、編集されたマッピンググリッドの例です。右側の下部のフィールドに [作業メモ] フィールドが追加され、複数の値が表示されます。値はスペースと句読点で区切られます (Category:${category} |destination IP:78.146.73.180)。



プレビューでは、これらの値はセキュリティインシデントの [作業メモ] に表示されます。値はグリッドに追加したフィールドの値であり、[作業メモ] フィールドに複数の値がマッピングされているため、値は入力されたとおりに表示されます。この例では、フィールドに入力したスペースと句読点が、セキュリティインシデントのプレビューの作業メモとして [関連アイテム] セクションに表示されます。

次の画像は、前の画像の値がセキュリティインシデントにどのように表示されるかを示した例です。

インシデント生成フィルタリング条件

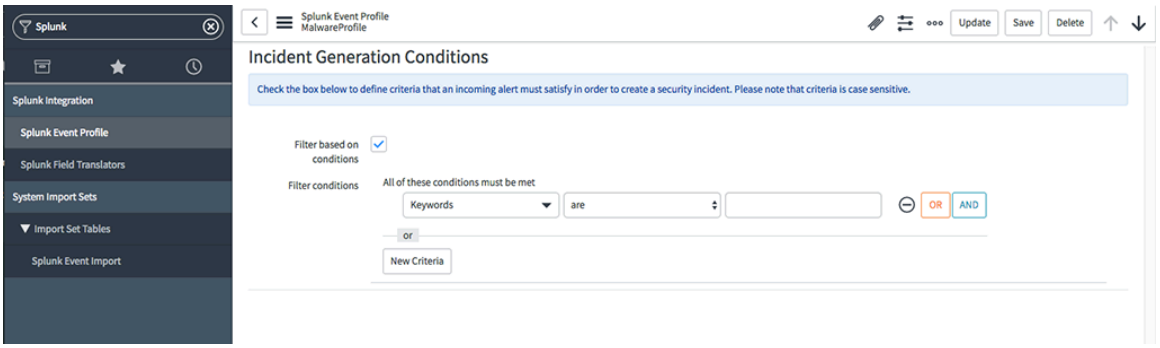
9. オプション: 先行するフィールドレベルマッピングのステップを完了したら、フィルター条件ビルダーで同じフィールド値を使用して、SIR セキュリティインシデントを作成するために受信アラートが満たす必要がある追加の条件を定義できます。
フィルタリング条件を設定するには、次のステップを実行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. フォームの [インシデント生成条件] セクションまでスクロールし、[条件に基づいてフィルター] チェックボックスをオンにして、オプションを有効にします。

(Optional) フィルター条件ビルダーが表示されます。これらのフィルターを使用して、フィールドで説明されている特定の条件に一致するセキュリティインシデントを作成します。

フィルター条件ビルダーの最初のフィールドのリストオプションは、取り込まれたアラートの [アラートサンプルの取り込み] セクションに表示されるフィールドと一致します。これらのフィールドは動的であり、取り込む Splunk アラートまたは手動で転送するイベントに応じて変化します。入力する条件は大文字と小文字が区別され、Splunk Enterprise アラートまたはイベントの値と正確に一致する必要があります。フィルターフィールドに入力する値が不明な場合、Splunk Enterprise コンソールに戻り、アラートとイベントをレビューしてキーワードを確認することができます。

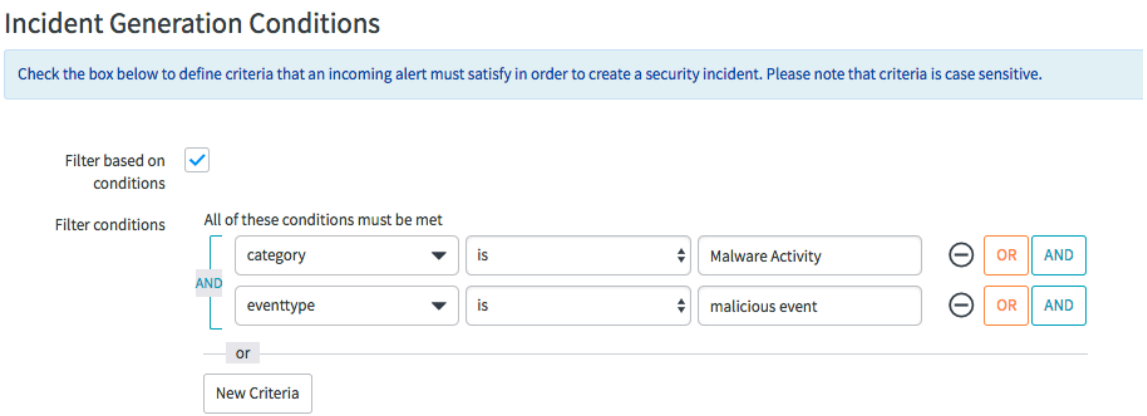


b. 条件ビルダーのリストとフィールドを使用して、最初の行のフィルターを設定します。

c. 条件を追加するには、フィールドの右側にある [**AND**] または [**OR**] をクリックします。[**AND**] を選択した場合は、すべての条件に一致する必要があります。**[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。

d. オプション: 2 行目で、2 番目のフィルター条件を設定します。

(Optional) 次の画像は、セキュリティインシデントが作成される前に一致する必要がある 2 つの条件を含む例です。



(Optional) 入力した両方のフィルタリング条件に一致した場合にのみセキュリティインシデントが作成されるように、トリガー条件を設定しました。

このタイプのフィルタリングは、セキュリティインシデントを分離し、作成するセキュリティインシデントの数を制限するのに役立ちます。追加のフィルター条件を設定すると、Splunk のク

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

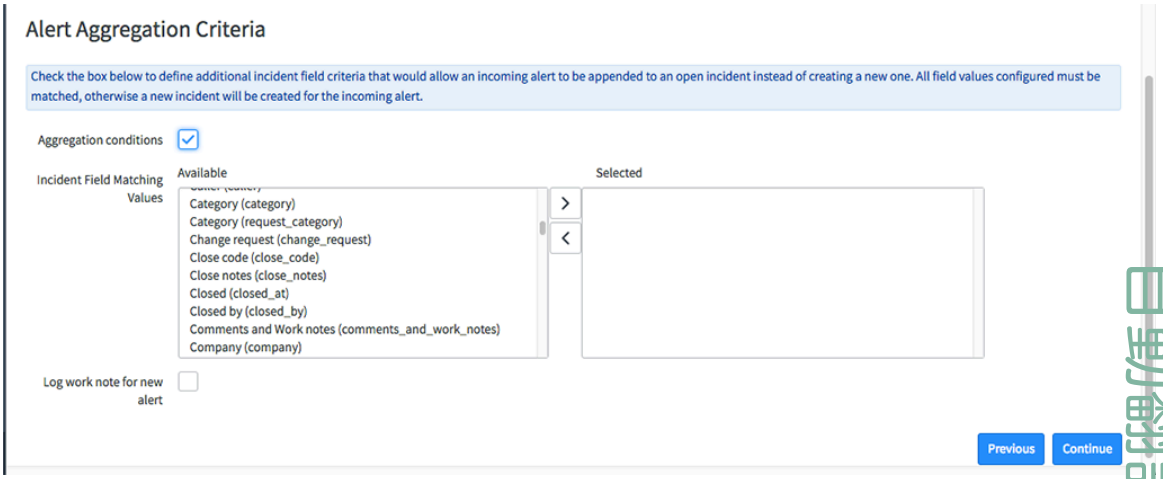
エリまたはトリガーされたアラート構成を変更することなく、必要なアラートのみが取り込まれます。

重複インシデントを防止する集計アラート

10. オプション: 重複セキュリティイベントが作成される可能性がないように、追加のインシデントフィールド条件を定義して、受信アラートをオープンセキュリティインシデント別に集計することができます。
この基準を設定するには、以下のステップを実行します。

    a. フォームで [アラートアグリゲーション基準] セクションにスクロールして、[集計条件] チェックボックスをオンにして、このオプションを有効にします。

    (Optional) [値が一致するインシデントフィールド] 列が表示されます。これらのフィールド名は、SIR セキュリティインシデントで構成されたカスタムフィールドを含むセキュリティインシデントのフィールドです。

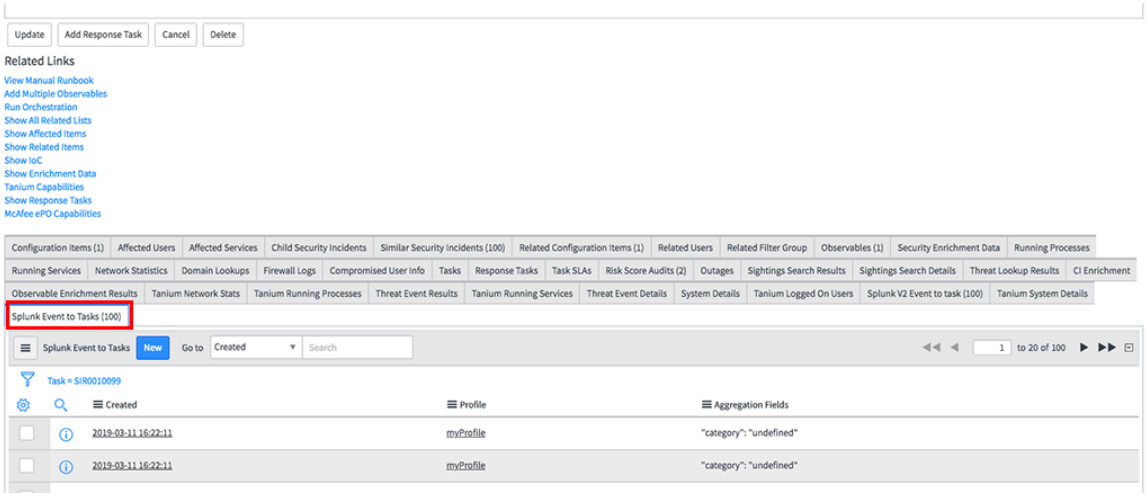


    b. [利用可能] リストから、Now Platform の既存のセキュリティインシデントで照合するフィールド値を選択し、[選択済み] リストに移動させます。

    (Optional) この受信アラートを既存のセキュリティインシデントに追加するには、選択するすべてのフィールド値が一致する必要があります。この基準に使用するセキュリティインシデントのフィールド値を確認するには、次に移動します: インシデント > すべてのインシデントを表示.

    新しいアラートが、マッピングステップの集計フィールド条件で選択されたすべての値と一致する場合、新しいアラートは、同じフィールド値を持つ最新のオープンセキュリティインシデントに自動的に追加されます。セキュリティインシデントを扱う sn_si.analyst ロールを持つユーザーは、セキュリティインシデントの関連リストで、追加されたすべての集計アラートを表示できます。セキュリティインシデントの集計されたアラートはすべて、[タスクに対する Splunk イベント] 関連リストに表示されます。このリストには、関連するタイムスタンプと集計されたフィールド値の詳細が表示されます。この情報は、アラートが既存のセキュリティインシデントに追加される理由を理解するのに役立ちます。このタブが表示されない場合は、 [関連リンク] の下のレコードの左側にスクロールし、[すべての関連リストを表示] リンクをクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



c. オプション: セキュリティインシデントで最近追加された新しいアラートの作業メモを記録するには、このチェックボックスをオンにしてこのオプションを有効にします。
作業メモには、新しいアラートが追加されたことが、アラートの詳細へのリンクとともに記録されます。

Splunk アラートまたはイベントから SIR セキュリティインシデントのフィールドに値を正常にマッピングしました。また、フィルター条件に基づいてセキュリティインシデントの作成を制限する追加条件も設定しました。既存の SIR セキュリティインシデントにアラートまたはイベントも追加しました。

11. オプション: スクリプトエディターを開き、編集を続行します。

(Optional) スクリプトエディターの詳細については、「Splunk Enterprise Event Ingestion 統合でのスクリプトエディターを使用したアラート値のフォーマット」を参照してください。

12. いずれかを選択して、プロファイル構成を続行します。

自動翻訳

次のタスク
次のステップでは、 セキュリティインシデントにマッピングした値をプレビューします。

Splunk Enterprise Event Ingestion 統合でのセキュリティインシデントのプレビュー

マッピングステップを完了したら、Now Platform® セキュリティインシデントレスポンス (SIR) セキュリティインシデントでマッピングした値をプレビューします。このプレビューステップでは、セキュリティインシデントに表示するすべてのアラートフィールドがマッピングされていることを確認できます。

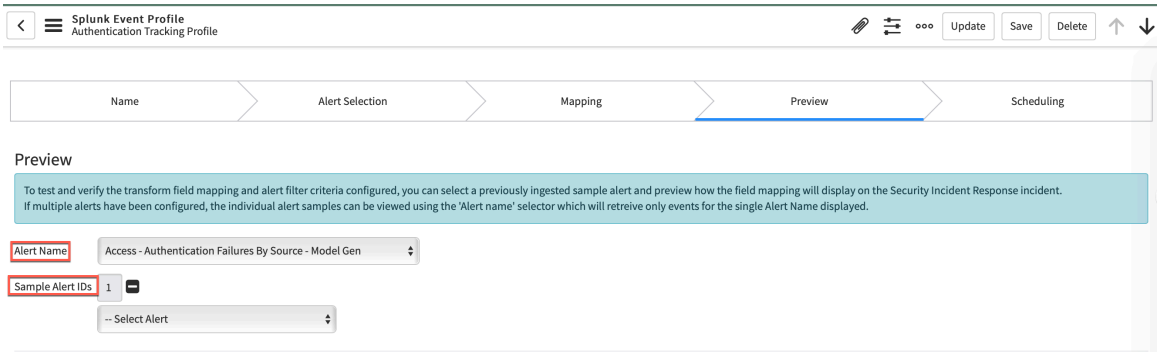
始める前に
必要なロール：sn_si.admin

このタスクについて
セキュリティインシデントをプレビューし、必要に応じてマッピングを再編集して、エラーのあるフィールドを修正するか、欠落しているデータを入力します。プレビューが正常に完了しない場合、スケジュール設定ステップに進むことはできません。SIR セキュリティインシデントのプレビューは、SIR 製品の実際のインシデントとして保存されません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

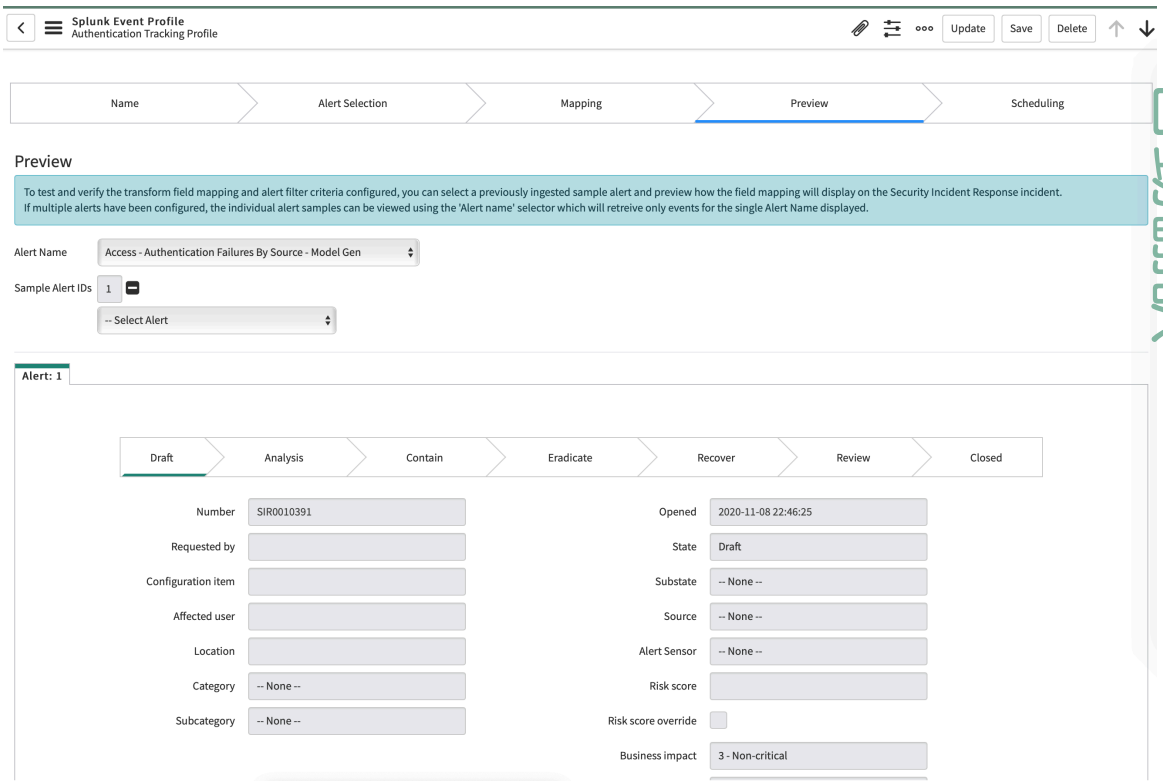
手順

1. セキュリティインシデントのプレビューが表示されない場合は、進捗状況バーの [プレビュー] をクリックします。
2. [アラート名] を選択し、[サンプルアラート **ID**] リストでアイテムを選択します。



セキュリティインシデントが表示されます。フィールドの情報は変更しないでください。このビューは読み取り専用であり、このセキュリティインシデントのレコードは保存されません。

3. セキュリティインシデントのアラート値のフィールドマッピングを確認します。

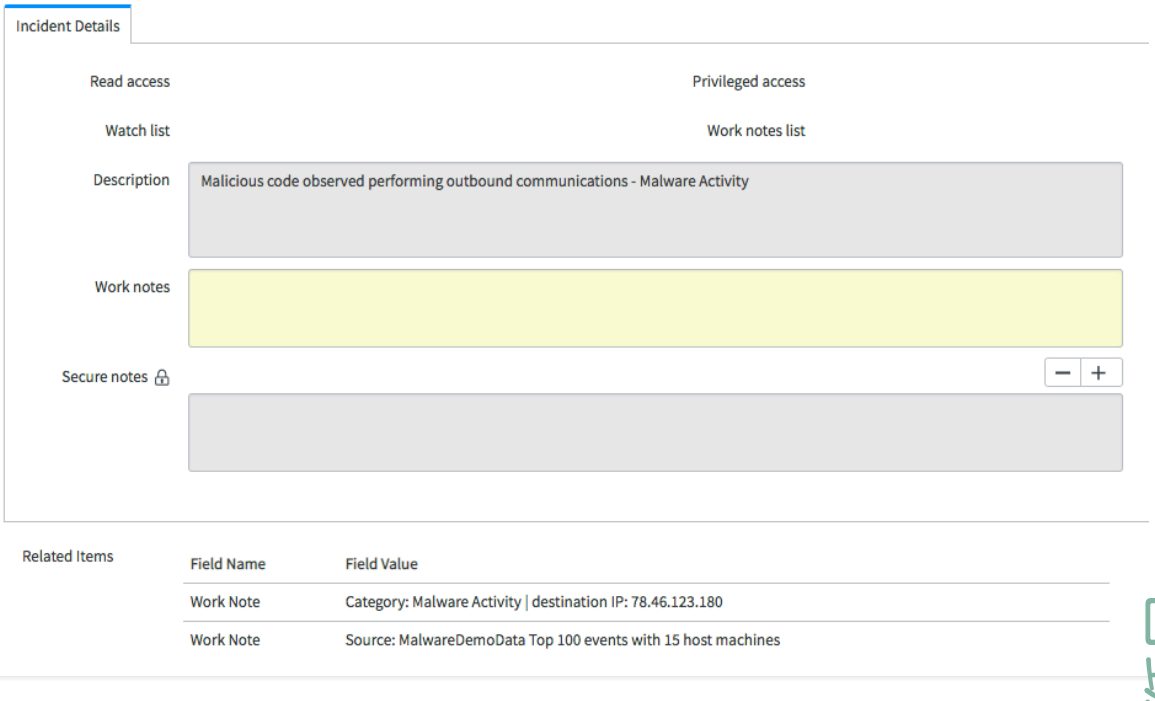


前の画像は、マッピングエラーのあるプレビューの例です。この例では、セキュリティインシデントのフィールドで値が存在しないか、マップした値がサポートされていません。[構成アイテム] フィールドの入力値が見つからなかったことを示すエラーメッセージが表示されます。

4. このエラーを解決するには、進捗状況バーの [マッピング] をクリックします。
5. マッピングを編集して誤った値を修正するか、欠落しているデータを入力します。
6. マッピングを再度プレビューし、エラーメッセージに記載されているエラーの修正を続行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図は、すべてのエラーメッセージが解決された後の SIR セキュリティインシデントの下半分にある [インシデントの詳細] タブの例です。この例では、 [説明] および [作業メモ] フィールドがマッピングされ、これらのフィールドには Splunk Enterprise コンソールからプルされた値のペアが入力されます。最初の [作業メモ] フィールドには値がありません。マッピングステップで、このフィールドはマッピンググリッドで空のままになっていました。値を含む追加の [作業メモ] フィールドが、マッピングステップ中にマッピンググリッドに追加されました。



7. エラーを修正し、フィールドが意図したとおりであることを確認したら、続行するオプションを 1 つ選択します。

次のタスク

エラーメッセージが表示されず、セキュリティインシデントのフィールドマッピングに問題がない場合は、次のステップでは Splunk Enterprise Event Ingestion 統合でのアラートのスケジュールおよび取得 を行います。

Splunk Enterprise Event Ingestion 統合でのアラートのスケジュールおよび取得

自動アラート取り込みプロファイルの場合、このステップはイベントプロファイル構成の最後のステップです。このステップでは、必要に応じて、アラート取得のデフォルトの設定を確認したり、スケジュールを変更したりすることができます。このステップでは、日付範囲に基づいてアラートの取得をフィルタリングできます。

始める前に

必要なロール：sn_si.admin ロール

このタスクについて

次の図に示すように、プロファイル構成の進捗状況バーのすべてのステップを完了すると、手動イベント転送のプロファイルの構成が完了します。Splunk Enterprise コンソールから手動で転送されたイベントにはスケジュールは利用できません。自動アラート取り込みプロファイルの場合、[スケジュール] ステップで履歴アラートを取り込むかどうかを選択できます。また、アラートプロファイル構成に一致する将来のアラートをポーリングする頻度も選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

進捗状況バー

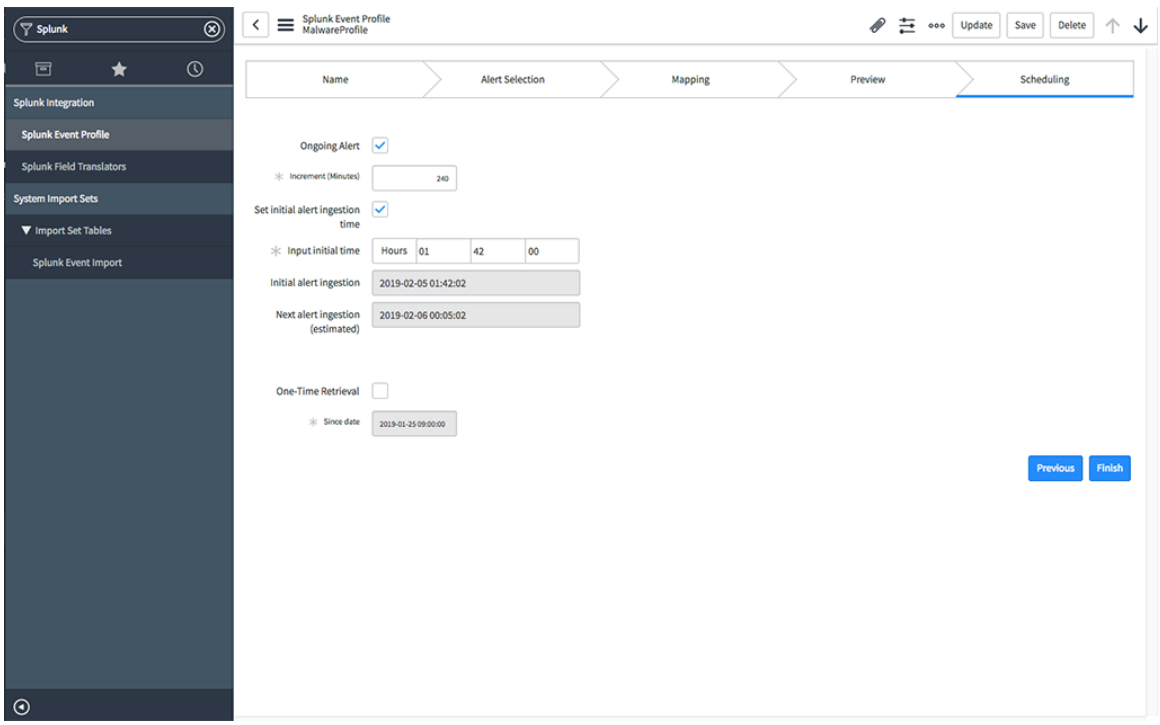
自動アラート取り込みプロファイルの場合は、プロファイルをアクティブ化する前に、スケジュールとアラートの取得を確認して変更します。スケジュール済みアラートプロファイルの場合、このステップはイベントプロファイル構成プロセスの最後のステップです。

ポーリング間隔をプロファイルごとに設定します。Splunk イベントの取り込み統合のパフォーマンスは、ポーリング間隔が異なると影響を受けます。スケジュールするときは、インシデントの緊急度とシステム負荷のバランスを取るように計画してください。5 分間のデフォルト値が任意のプロファイルに設定されますが、インシデントの緊急度とシステムの予想される負荷に基づいて変更できます。

Splunk Enterprise コンソールで、インクリメントまたは特定の時間に基づいてアラートをトリガーするように設定します。この設定を使用すると、Now Platform インスタンスのスケジュールを設定し、Splunk Enterprise コンソールの時間インクリメントを Now Platform インスタンスで設定したスケジューリングと同期させることができます。

手順

1. 進捗状況バーに [スケジュール] ページが表示されない場合は、[スケジュール] を選択します。
2. Splunk Enterprise コンソールからアラートをプルする方法とタイミングをスケジュールするものを選択します。



スケジュールの例として、現地時間の午前 4 時に 1 日 1 回実行される日次 Splunk アラートがある場合、Now Platform インスタンスで対応するアラートプロファイルを現地時間午前 4 時 5 分に実行するように設定して、アラートをすぐにキャプチャし、セキュリティインシデントを作成できます。[初期アラートの取り込み] フィールドに「04 05 00」と入力します。[インクリメント (分)] フィールドに「1440 (24 時間)」と入力して、初期アラートの取り込みから 24 時間後に次のアラートの取り込みをスケジュールします。初期アラートの取り込み時刻と次のアラートの取り込み時刻の両方がフィールドに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. この例の設定を構成するには、次のステップを実行します。

   a. 表示された [スケジュール] ページで、[進行中のアラート] チェックボックスをオンにしてこのオプションを有効にします。

   b. [インクリメント (分)] フィールドに「1440 (24 時間)」と入力します。

   c. [初期アラートの取り込みを選択 **(Select Initial alert ingestion)**] チェックボックスをオンにして [初期アラートの取り込み] と [次のアラートの取り込み] フィールドの編集を有効にします。

   d. [初期アラートの取り込み] フィールドに「04 05 00」と入力します。
   [次のアラートの取り込み (推定)] フィールドに、次のアラートの取り込み時刻が表示されます。

4. [完了] をクリックして、構成を完了します。
   確認ダイアログが表示されます。これで統合のセットアップと構成が正常に完了しました。このプロファイルをアクティブ化して、スケジュールに基づいて Splunk Enterprise コンソールからアラートをプルします。24 時間内に作成できるセキュリティインシデント数は 1,000 件に制限されます。発生したアラートごとに最大 100 件のイベントに制限されます。制限に達すると、後続のイベントは無視されます。

Splunk Enterprise Event Ingestion 統合の統合アーキテクチャと外部システム接続

次のトピックでは、Splunk Enterprise コンソールからのトリガーされたアラートの取り込みをサポートするために開発された統合アーキテクチャについて説明します。この情報は、統合の概念的な操作を高レベルで明確にします。また、ServiceNow Store からアプリケーションをインストールする前に必要なセットアップステップがある理由についても説明します。

この統合で使用される重要な用語

インストールと構成では、次の重要な用語が使用されます。以下の用語の詳細については、ServiceNow の製品ドキュメント Web サイト、Splunk の Web サイト、および Splunk リソース ページのリソースを参照してください。

Now Platform
: エンタープライズ ServiceNow 製品。Now Platform をベースとして、セキュリティインシデントレスポンス (SIR)、IT Service Management (ITSM)、およびその他の製品などの個々のコンポーネントがビルドされています。

ServiceNow Splunkbase アドオン
: 統合の手動イベント転送オプションをサポートする Splunk Enterprise コンソールにインストールされている ServiceNow アプリケーションです。手動イベント転送は、統合のオプション機能です。この ServiceNow Splunkbase アドオンは、統合によって提供される自動アラートの取り込みには必要ありません。

セキュリティインシデントレスポンス (SIR)
: 検出と初期分析から、封じ込め、根絶、復旧、および最終的なインシデントの事後レビューとクローズに至るまで、セキュリティインシデントの進捗状況を追跡する Now Platform アプリケーション。

Splunk Enterprise
: インシデントの分析と管理に使用されるデータを収集する、自動セキュリティインシデントイベント管理 (SIEM) 製品またはクラウドサービスです。このサービスは、このガイドで Splunk コンソールと呼ばれることがあるホスト上にあります。

Splunk アラート

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Splunk で設定して保存し、Splunk Enterprise サービスで設定したパラメーターに基づいて特定のデータをスキャンする検索。Splunk からアラートをプルすると、そのアラートに関連付けられているすべてのイベントもプルされます。

Splunk トリガーアラート

結果を返し、その結果をトリガーされたアラートとしてフラグ付けする、Splunk Enterprise コンソールで構成された検索。トリガーされたアラートは、この統合のために Splunk コンソールから Now Platform インスタンスに取り込まれます。トリガーされたアラートには、1 つ以上の Splunk イベントがあります。

Splunk イベント

Splunk サービスのトリガーされたアラートを生じる 1 つ以上のデータ要素。Now Platform インスタンスから、どの Splunk イベントが Now Platform セキュリティインシデントをトリガーしたかを検索できます。

MID サーバー

このアプリケーションは、Now Platform と外部アプリケーション、データソース、サービスの間の通信やデータの移動を容易にします。このアプリケーションは通常、オンプレミステクノロジーとの統合に必要です。この Splunk Enterprise Event Ingestion 統合のために、MID サーバーは Now Platform と Splunk Enterprise のオンプレミスインスタンス間の通信を支援します。Now Platform インスタンスを Splunk Cloud インスタンスと統合する場合、MID サーバーは必要ありません。

セキュリティインシデントアドミン (sn_si.admin)

このロールを持つユーザーは、Now Platform インスタンス内の SIR 製品との統合の構成を監督します。

セキュリティインシデントアナリスト (sn_si.analyst)

このロールを持つユーザーは、ServiceNow セキュリティインシデントレスポンス 製品でセキュリティインシデントに対応し、分析します。

外部システム接続

イベントプロファイルは、特定の基準に一致する最新のトリガーされたアラートをプルするために、単一の接続用に作成し、名前を付けて構成し、Splunk サービスを呼び出すコンテナです。プロファイルに一致するトリガーされたアラートが Splunk からプルされた後、これらのアラートから Now Platform セキュリティインシデントレスポンス SIR セキュリティインシデントとして表示するものを選択します。Splunk Enterprise アラートフィールドのデフォルトビューが利用可能です。また、ニーズに合わせて SIR セキュリティインシデントのフィールドへのこのアラートフィールドのマッピングを編集します。マッピングをプレビューして、SIR セキュリティインシデントに必要なすべてのアラートフィールド値が入力されていることを確認します。アラートプロファイルの設定を完了するには、アラートの取得をスケジュールしてから、プロファイルをアクティブ化します。Now Platform でプロファイルをアクティブ化すると、履歴アラートと進行中の Splunk アラートを自動的に取り込むことができます。

sn_si.admin ロールを持つユーザーは、新しくトリガーされたアラートが以前に取り込まれたアラートと類似していると判断した場合、新しくトリガーされたアラートを既存の SIR セキュリティインシデントに集計できます。Splunk Enterprise アラートプロファイルで一致するターゲットフィールド値を指定するための基準を設定し、既存のセキュリティインシデントが更新されるタイミングと新しいセキュリティインシデントが作成されるタイミングを定義します。イベントプロファイルで集計機能が有効になっている場合、インポートセットが変換されると、Now Platform インスタンスはターゲットフィールドとソースフィールドに同じ値を持つターゲットテーブルで既存のレコードをチェックします。ターゲットテーブルに一致する値を持つ既存のレコードが見つかった場合、そのレコードが更新されます。一致するレコードが見つからない場合は、ターゲットテーブルに新しいレコードが作成されます。有効な場合、集計オプションは既存のセキュリティインシデントが新しくトリガーされたアラートで更新されるため、複数のセキュリティインシデントが作成されることはありません。集計オプションを使用したレコードの更新に関する詳細については、「結合を使用したレコードの更新」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

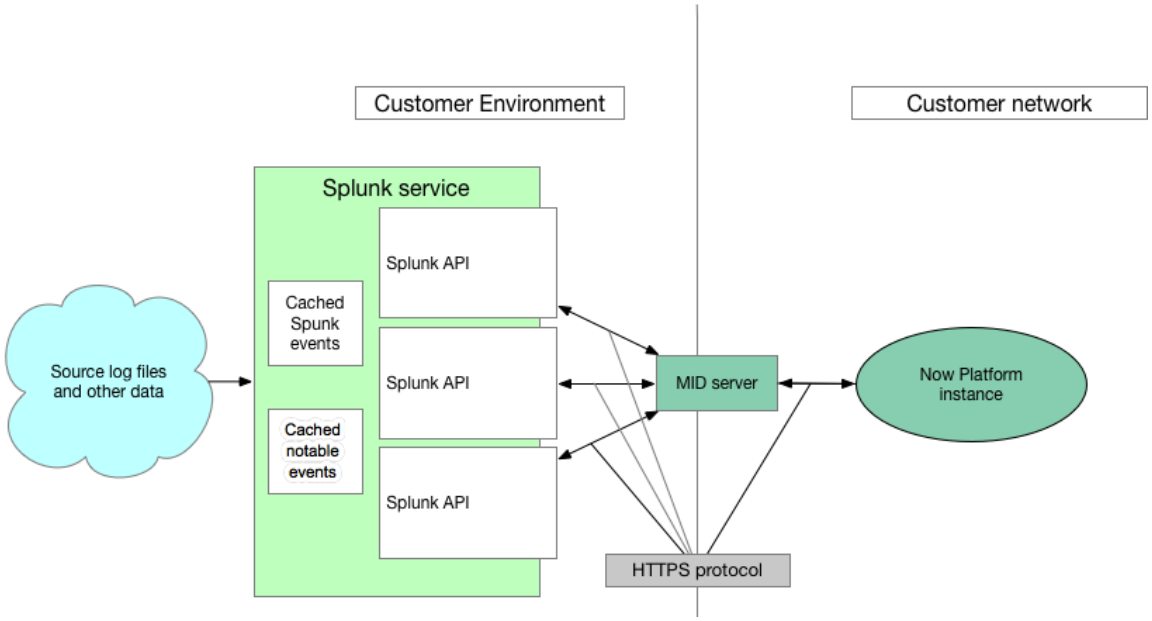
自動翻訳

このアプリケーションは Splunk API サービスを使用して Splunk サービスから情報を取得します。統合が正しく機能するには、MID サーバーからこの環境への送信 HTTPS 接続が必要です。

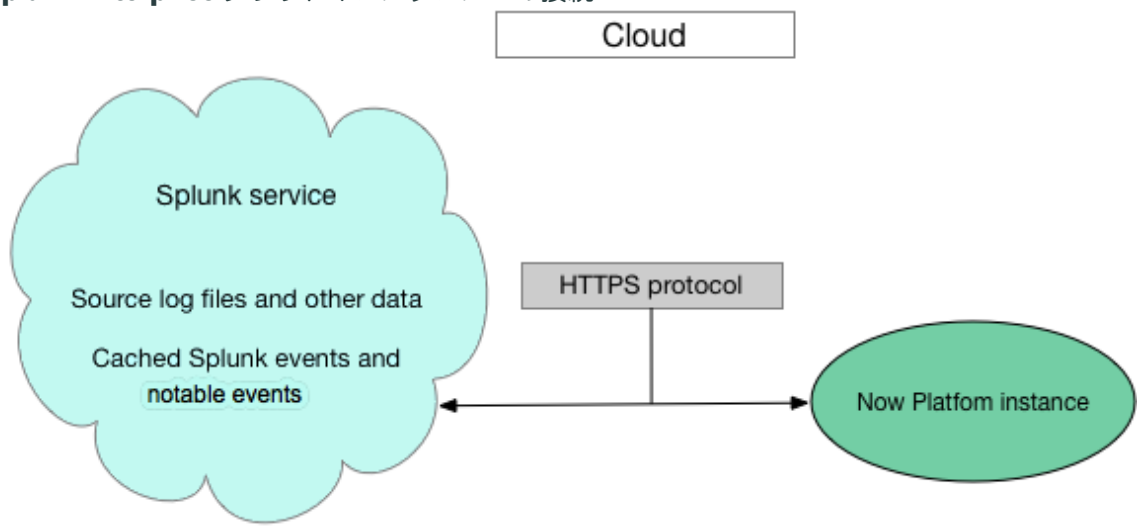
Splunk サービスに接続された後、統合はセキュリティインシデントをトリガーするトリガーされたアラートとイベントのプルと取り込みをサポートします。

基本的なデータフローを次の図に示します。各図では、Now Platform がデータをプル (取り込み) しています。Splunk はスケジュール済みアラートのデータをプッシュしていません。

単一の **MID** サーバー を使用したオンプレミス **Splunk Enterprise** サービスへの接続



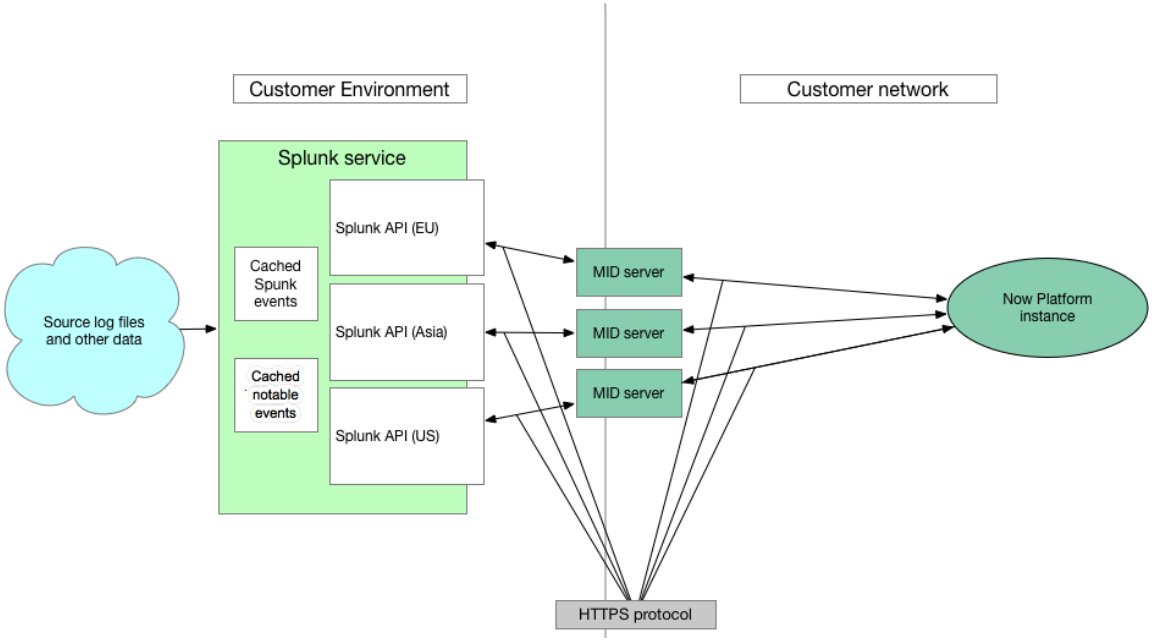
Splunk Enterprise クラウドインスタンスへの接続



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

複数の **MID** サーバーを使用した **Splunk Enterprise** サービスへの複数接続



エクスポート/インポート機能を使用した **Splunk Enterprise Event Ingestion** プロファイルのインスタンス間でのコピー

Splunk Enterprise Event Ingestion プロファイル設定を 1 つの Now Platform インスタンスから別の Now Platform インスタンスにエクスポートおよびインポートできます。

始める前に
必要なロール：sn_si.admin

このタスクについて
この機能により、セキュリティアドミニストレーターは、ある Now Platform インスタンス (非本番など) でテストおよび検証されたプロファイルを、別の Now Platform インスタンス (本番など) にコピーできます。すべての構成設定をやり直す必要はありません。エクスポートおよびインポートされる設定には、プロファイル名、相関ルール、マッピング、フィルター、集計基準、フィールド変換、フェッチされたサンプルデータ、スケジュール、および構成タイルソース情報が含まれます。

注:
手動イベント転送プロファイルタイプをエクスポートすると、サンプルフィールドマッピングに使用される添付ファイルデータはコピーされますが、添付ファイル自体はエクスポートされません。

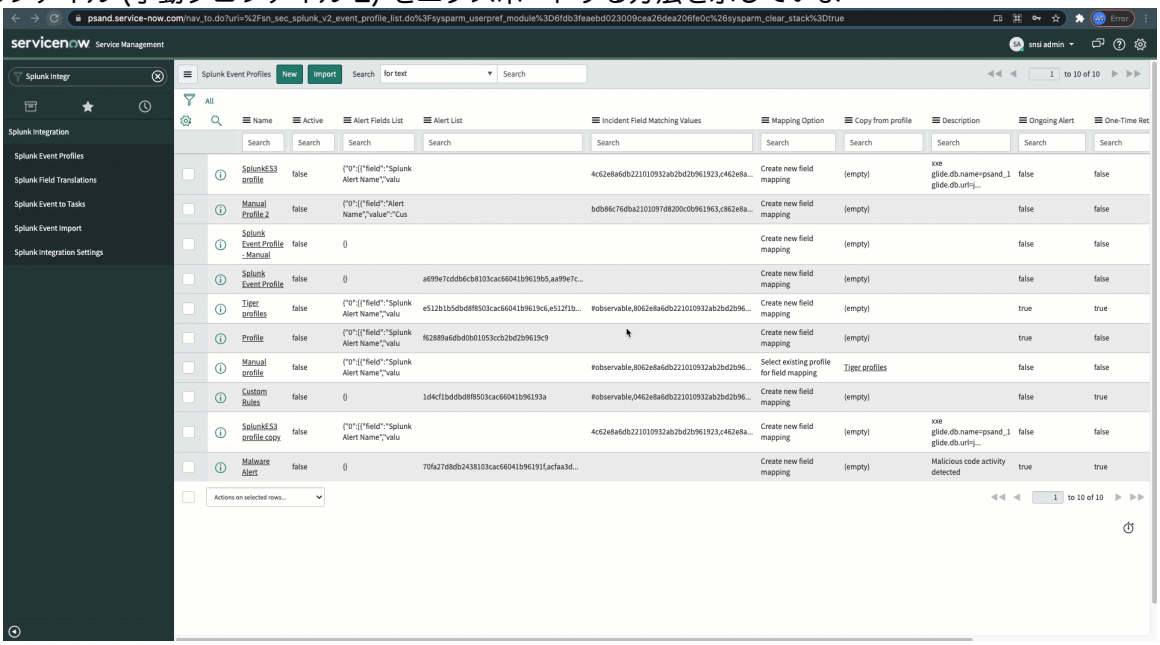
手順

1. 次のように移動する。 **All** (すべて) > **Splunk Integration** > **Splunk** イベントプロファイル.
2. 別の Now Platform インスタンスにエクスポートするプロファイルを選択します。
   エクスポートするプロファイルは複数選択できます。
3. [アクション] メニューから、[エクスポート] をクリックします。
4. エクスポート完了メッセージが表示されたら、[ダウンロード] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図は、Now Platform インスタンス (psand.service-now.com) から Splunk プロファイル (手動プロファイル 2) をエクスポートする方法を示していま



す。

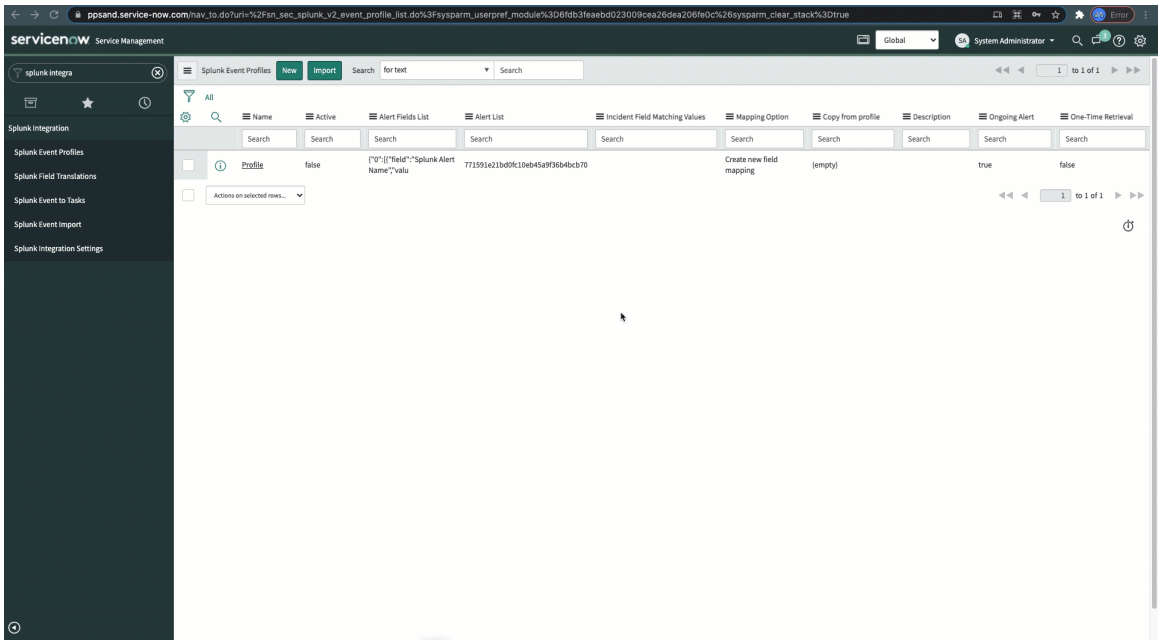
エクスポートされた payload.xml ファイルがコンピューターにダウンロードされます。ファイルには、プロファイル名、相関ルール、マッピング、フィルター、集計基準、フィールド変換、フェッチされたサンプルデータ、スケジュール、および構成タイルソース情報が含まれます。複数のプロファイルを選択してダウンロードすると、同じ payload.xml ファイルに表示されます。

これで、別の Now Platform インスタンスでプロファイルをインポートできます。

5. 次のように移動する。 **Splunk Integration** > **Splunk** イベントプロファイル.
6. [インポート] をクリックします。
7. [ファイルを選択] をクリックし、コンピューターで XML ファイルを選択します。
8. [アップロード] をクリックします。
9. [プロファイルを閉じてリロード] をクリックします。
   次の図は、Now Platform インスタンス (psand.service-now.com) から Splunk プロファイル (手動プロファイル 2) を別の Now Platform インスタンス (ppsand.service-now.com) にインポートする方法を示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



別の Now Platform インスタンスからプロファイルが正常にインポートされました。

エクスポートされたソース (Splunk API アカウントと Splunk サーバー URL) と MID サーバー構成設定が有効で、インポートされた Now Platform インスタンスで使用できることを確認します。必要に応じて Splunk Enterprise Event Ingestion 構成を更新します。

10. オプション: プロファイルをインポートした後、MID サーバーの設定を確認します。
11. オプション: 次のように移動する。 セキュリティオペレーション > 統合設定.
12. オプション: Splunk Enterprise Event Ingestion 構成タイルを選択し、[更新] をクリックします。
13. オプション: ソースおよび MID サーバーの詳細を確認し、必要に応じて更新します。

Splunk Enterprise Event Ingestion 統合でのイベントプロファイルのコピー

新しいプロファイルを作成する代わりに、既存のプロファイルとその関連設定をコピーします。複数のプロファイルを作成していて、既存のプロファイルの設定を再利用する場合は、時間を節約するためにアラームをコピーできます。

始める前に
必要なロール：sn_si.admin

このタスクについて
既存のプロファイルとその関連設定のコピーはオプションです。

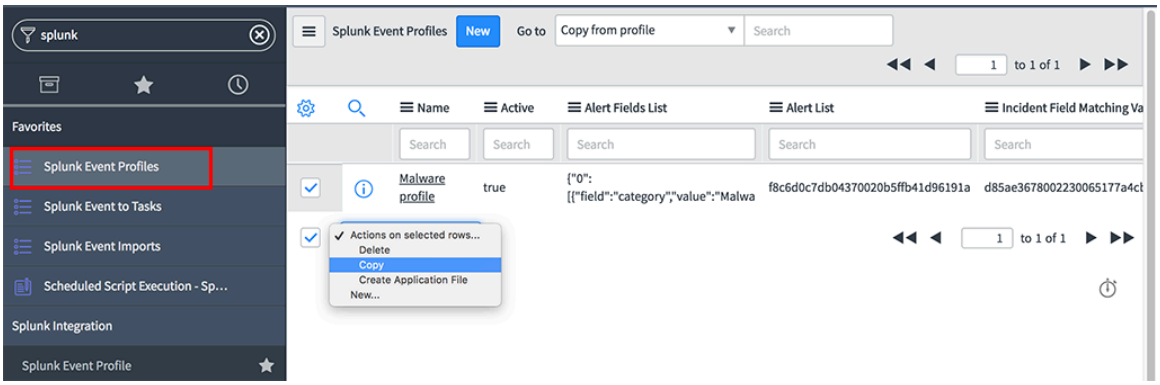
プロファイルをコピーすると、プロファイルの重複を避けるためにプロファイル名が最初に変更されます。また、コピーされたプロファイルは無効 (false) であるため、構成が完了する前に誤って有効になることはありません。既にプレビューおよび検証したセキュリティインシデントのプロファイルをコピーし、既存のマップを使用します。

手順

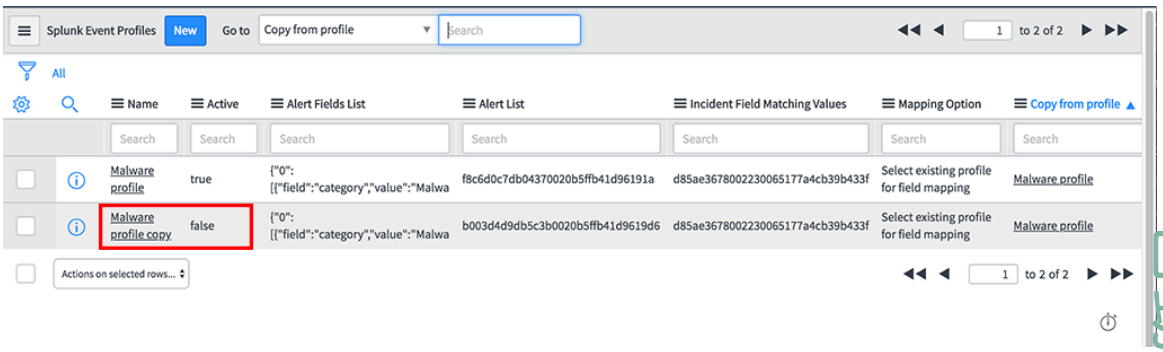
1. 次のように移動する。 **All** (すべて) > **Splunk Integration** > **Splunk** イベントプロファイル.
2. 表示される [Splunk イベントプロファイル] リストでコピーするプロファイルを選択し、選択した行の [アクション] 選択リストで [コピー] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



プロファイルがコピーされ、リストに表示されます。コピーには、マッピングとスケジュール設定を含む元のプロファイルのすべての設定が含まれます。プロファイルの名前に「copy」が含まれています。元のプロファイルは有効ですが (true)、この時点でコピーは無効になります (false)。必要に応じて、コピーしたプロファイルの値を編集して名前を変更し、構成設定を新しいプロファイルに適用することもできます。



既存のプロファイルから新しいプロファイルに設定が正常にコピーされました。

次のタスク
構成ステップが完了すると、新しいプロファイルをアクティブ (有効) にするように求められます。

Splunk Enterprise イベントの取り込み統合での手動イベント取り込み用の **Splunk** 環境設定

この統合のために Splunk Enterprise コンソールから手動でオンデマンドでイベントをエクスポートする場合は、ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise アプリケーションを Splunk Enterprise コンソールまたは Splunk クラウドインスタンスにインストールして設定します。

始める前に
手動イベントの取り込みに必要な splunkbase からのアドオンプラグインをインストールする前に、ServiceNow Store からこの統合用のアプリケーションがインストールされていることを確認してください。ServiceNow Store から統合用のアプリケーションをインストールしていない場合は、「Splunk Enterprise Event Ingestion 統合用の ServiceNow アプリケーションのインストールと設定」を参照し、手順に従ってインストールします。

必要なロール：Now Platform アドミニストレーター (admin)

このタスクについて
ServiceNow Security Operations Event Ingestion Addon のインストールと設定はオプションです。

統合用に Splunk Enterprise コンソールから手動でオンデマンドでイベントをエクスポートする場合は、ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise を Splunk Enterprise コンソールにインストールして設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

この ServiceNow 拡張アドオンは、Now Platform インスタンスにある手動でエクスポートされたイベントからセキュリティインシデントを作成するために必要です。ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise アプリケーションは splunkbase で入手できます。

手動イベント転送の場合は、Splunk Enterprise コンソールで最大 2 つの異なる Now Platform エンドポイント (インスタンス) を特定できます。イベントをエンドポイントに手動で転送して、セキュリティインシデントを作成します。たとえば、ステージング (開発) インスタンスと本番インスタンスの両方を指定できます。個別のインスタンスを指定し、各インスタンスのプライマリおよびセカンダリワークフローに名前を付けることで、さまざまなイベントの転送先を選択できます。

手順

1. ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise をまだインストールしていない場合は、次のステップに従ってインストールして設定します。

   a. splunkbase に移動します。

   b. ServiceNow セキュリティオペレーション Security Operations Event Ingestion Addon for Splunk Enterprise を検索します。

      注:
      ServiceNow セキュリティオペレーション Event Ingestion Addon for Splunk Enterprise を選択していることを確認します。このリストに表示される追加の ServiceNow アドオンがあります。これらのアドオンはさまざまな ServiceNow Splunk 統合用であり、この統合には必要ありません。

   c. アプリケーションをダウンロードします。

   d. Splunk Enterprise アカウントを開きます。

   e. [アプリ] ページで、メニュードロップダウンリストの歯車アイコンまたは [アプリを管理] ショートカットをクリックします。

   f. 表示される [アプリ] ページの左上で、[ファイルからアプリをインストール] をクリックします。

   g. [ファイルを選択] をクリックし、ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise を選択して、[アップロード] をクリックします。

   h. プロンプトが表示されたら、Splunk Enterprise を再起動します。
   ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise が Splunk Enterprise Enterprise コンソールにインストールされます。次のステップでは、アドオンを設定します。

2. アドオンを設定するには、次のステップを実行します。

   a. Splunk Enterprise で、メニュードロップダウンリストの [アプリ] 歯車アイコンまたは [アプリを管理] をクリックします。

   b. 表示されるアプリケーションのリストの [アクション] 列で、ServiceNow セキュリティオペレーション Event Ingestion Addon for Splunk Enterprise の [セットアップ] をクリックします。

自動翻訳

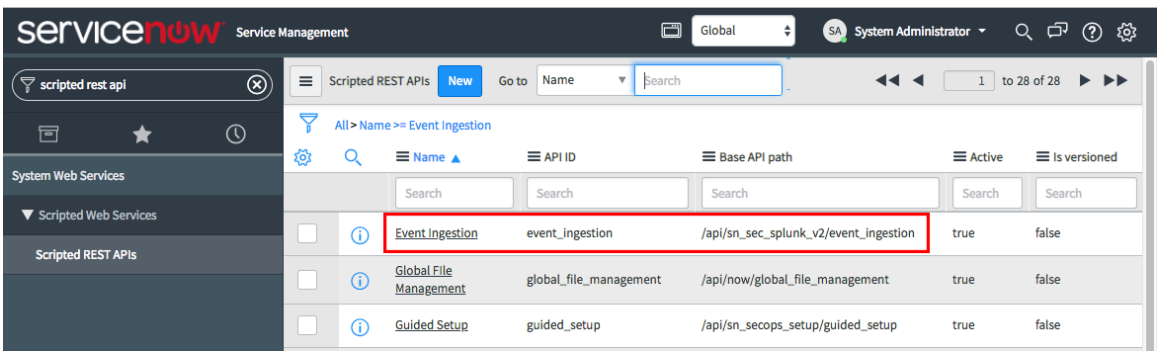
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

c. フォームに記入します。

次の図は、Splunk Enterprise コンソールの完成したフォームの例です。

次の図は、Now Platform のスクリプト済み REST API リストの例です。リストには、Splunk Enterprise コンソールで ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise 拡張機能の設定の一部としてフォームに入力した Now Platform インスタンスのエンドポイント値の場所が表示されます。

Now Platform のスクリプト済み **REST API** リスト



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. Splunk Enterprise コンソールの [セットアップ] フォームで、[保存] をクリックして編集を保存します。

   しばらくすると、Splunk Enterprise コンソールのフォームの左上に、レコードが正常に更新されたことを示すメッセージが表示されます。

   フォームを保存すると、フォームで作成した Now Platform インスタンスの名前 (ワークフローアクションラベル) が、Splunk Enterprise コンソールの検索で選択したイベントの [イベントアクション] 選択リストから使用できるようになります。

次のタスク
Splunk Enterprise コンソールに検索をまだ保存していない場合は、次のステップで Splunk Enterprise コンソールに検索をアラートとして保存します。

Splunk Enterprise Event Ingestion 統合での **Splunk Enterprise** コンソールへの検索の保存

Splunk Enterprise コンソールで検索を保存するための次のステップは、Splunk Enterprise アドミンロールを持つユーザー向けに提供されます。

始める前に
Splunk Enterprise コンソールに既存の保存された検索とトリガーされたアラートがある場合は、この統合でこれらの検索を変更する必要はありません。

Now Platform® セキュリティオペレーション 製品と Splunk イベント通知サービスの統合により、Splunk からイベントとアラートの情報がプルされます。

セキュリティオペレーション 環境にアラートを取り込む前に、Splunk Enterprise コンソールで検索を設定して、アラートとして保存する Splunk Enterprise 内の関連するセキュリティイベントを自動的にプルするようにします。

Splunk Enterprise コンソールで重要なセキュリティイベントが発生したときの通知用に、検索の保存とアラートのトリガーを行っていない場合は、次のステップに従って検索を保存します。

必要なロール：Splunk Enterprise アドミニストレーター

手順

1. Splunk Enterprise アカウントにログインします。
2. [検索] タブをクリックします。
3. 表示される [新規検索] フィールドに、アラートの値 (マルウェアなど) を入力します。
4. 検索に関連するイベントを表示するには、[新規検索] フィールドの右側にある検索アイコンをクリックするか、Enter キーを押します。
   イベントを含む検索結果が表示されます。
5. 検索をアラートとして保存するには、ページの右上にある [名前を付けて保存] 選択リストを展開し、[アラート] を選択します。
6. 表示されるフォームのフィールドに入力します。
7. [保存] をクリックします。
   アラートが保存され、[検索] ページの [アラート] タブに表示されます。
   Splunk サービスは、アラートで設定した条件に一致するイベントをプルします。イベントがキャッシュされると、Now Platform インスタンスで設定したプロファイルからこれらのイベントを要求できます。イベントの取り込みプルは Splunk サービスのキャッシュから行われるため、Now Platform からこの取り込みが行われても Splunk プラットフォームでのパフォーマンスに影響を与えません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のタスク
Splunk Enterprise コンソールで統合に必要なセットアップが正常に完了しました。ServiceNow Store から統合用のアプリケーションをまだインストールしていない場合は、次のステップで統合用のアプリケーションをインストールして設定します。

Splunk Enterprise Event Ingestion 統合でのスクリプトエディターを使用したアラート値のフォーマット

マッピングステップでスクリプトエディターを使用してセキュリティインシデントのフィールド値をフォーマットできます。

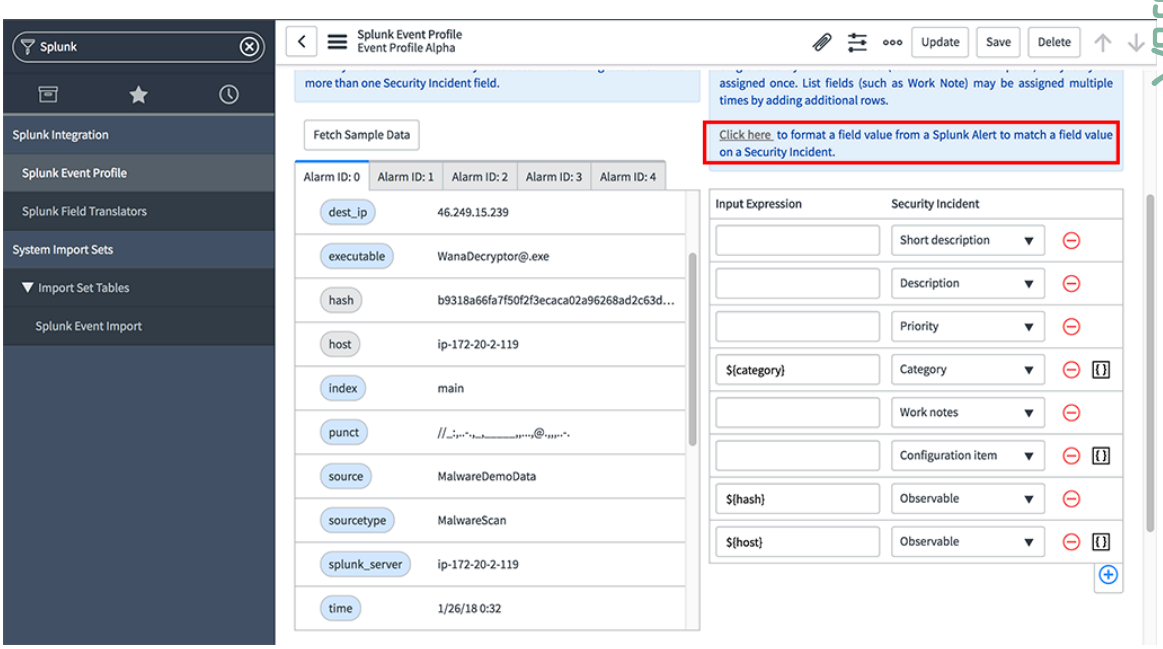
始める前に
プルされたアラート値および手動で入力したアラート値から直接マッピングされたフィールドに加えて、オプションで、マッピングステップでスクリプトエディターを使用してセキュリティインシデントのフィールド値をフォーマットできます。スクリプトエディターは、Splunk アラートの値を変更して、Now Platform セキュリティインシデントレスポンス セキュリティインシデントでサポートされている値が [カテゴリ]、 [構成アイテム (CI)]、および [観測事象] フィールドにマッピングされるように変更します。

必要なロール：sn_si.admin

このタスクについて
場合によっては、Splunk Enterprise アラート値は、SIR インシデントの [カテゴリ]、[構成アイテム (CI)]、および [観測事象] フィールドにマップされ、サポートされません。マッピングされた値を編集することもできます。Splunk Enterprise アラートの値を SIR セキュリティインシデントのこれらのフィールドでサポートされている値に変換する場合は、スクリプトエディターを使用します。

手順

1. [マッピング] フォームを表示した状態で、リンクをクリックしてスクリプトエディターを開きます。



2. 選択リストから、編集する値の宛先フィールドを選択します。
3. または、[SIR インシデントフィールドマッピング] セクションで、フィールドの横にある角かっこアイコン [{}] をクリックして、そのフィールドのスクリプトエディターを開きます。

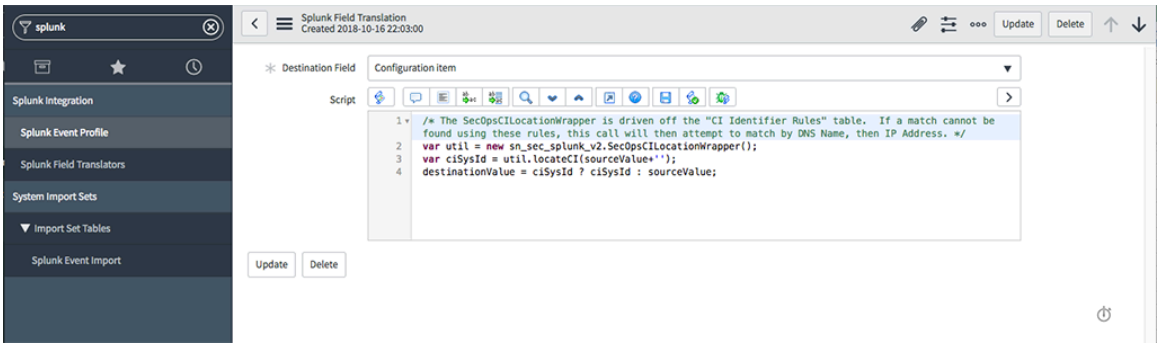
   場合によっては、 [構成アイテム] フィールドにスクリプトインクルードが適している場合があります。たとえば、アラートの場合、構成アイテムの値が一致しない可能性があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

次の図に示すように、[構成アイテム] フィールドの Now Platform CMDB で一致するホスト名が見つからない場合は、IP アドレスが見つかった場合に [構成アイテム] フィールドに入力されるようにルールを編集できます。アラームの値がない場合、セキュリティインシデントのフィールドは null に設定されます。

エディターが開き、[宛先フィールド] にフィールドが表示されます。次の画像は、[構成アイテム] フィールドを [宛先フィールド] に設定したエディターを示しています。



4. スクリプトに変更を入力し、[更新] をクリックして変更を保存します。
   [Splunk フィールド変換] テーブルが表示されます。
5. テーブルを閉じて [マッピング] フォームに戻ります。

Splunk Enterprise Event Ingestion 統合のチェックリスト

このチェックリストを使用して、統合のすべてのタスクをガイドします。次のチェックリストには、セットアップとインストールのタスク、および統合の予想される結果を含むユースケースの例が含まれています。

始める前に

必要なロール：admin

このタスクについて

次のテーブルを使用して、統合のセットアップ、インストール、および構成の進捗状況を追跡します。次のステップに進む前に、ステップのすべてのタスクを完了してください。テーブルの各行にタスクがリストされており、タスクの実行に必要なロールが特定されています。インストールおよび構成ガイドの番号付けされたトピックも参照されます。

必要なロール：ロールは次の各ステップに記載されています。

手順

1. Now Platform アドミンロールを持つユーザーとして、Now Platform インスタンスを設定します。
   - 必要に応じて、sn_si.admin ロールと sn_si.analyst ロールをユーザーにアサインします。
   - Splunk サーバーが企業ネットワーク内に展開されている場合は、MID サーバーをインストールして構成します。
   - ServiceNow セキュリティインシデントレスポンス プラグインが Now Platform のリリースに対して有効になっていることを確認します。
   - Splunk Enterprise コンソールから Now Platform インスタンスに手動でイベントを転送する場合は、Splunk Enterprise エンタープライズアドミン権限を持つユーザーに (sn_sec_splunk_v2.api_account_access) ロールが割り当てられていることを確認します。

   詳細については、「Splunk Enterprise Event Ingestion 統合での Now Platform インスタンスの設定」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

これでセットアップ手順を完了し、統合に期待される結果を検証できました。

2. Now Platform アドミンロールを持つユーザーとして、ServiceNow Store から Splunk Enterprise Event Ingestion アプリケーションをインストールして設定します。
   a. Now Platform インスタンスにアプリケーションがダウンロードされ、インストールされます。
   b. アプリケーションを設定し、Splunk Enterprise コンソールに接続します。

   詳細については、「Splunk Enterprise Event Ingestion 統合用の ServiceNow アプリケーションのインストールと設定」を参照してください。

3. オプション: Splunk Enterprise コンソールから Now Platform インスタンスにイベントを手動でエクスポートする場合は、次のタスクを実行します。
   a. Splunk Enterprise アドミニストレーターは、Splunk Enterprise コンソールで splunkbase から ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise をインストールして設定し、有効にします。
   b. Splunk Enterprise アドミニストレーターとして、まだ設定されていない場合は、Splunk Enterprise コンソールに検索をアラートとして保存します。

      (Optional) 詳細については、「Splunk Enterprise イベントの取り込み統合での手動イベント取り込み用の Splunk 環境設定」と「Splunk Enterprise Event Ingestion 統合での Splunk Enterprise コンソールへの検索の保存」を参照してください。

4. Now Platform sn_si.admin ロールを持つユーザーとして、イベントプロファイルを作成して名前を付けます。

   選択リストからプロファイルタイプを選択します。オプションは、サンプルデータを取り込むために使用するスケジュール済みアラートプロファイル、または Splunk Enterprise コンソールから手動で添付ファイルデータをエクスポートするために使用するイベントプロファイルです。

   - スケジュール済みアラートの場合は、利用可能なアラートを選択します。
   - 手動でエクスポートされたデータのプロファイルの場合は、新しいマップを作成するか、既存のマップをコピーします。

   詳細については、「Splunk Enterprise Event Ingestion 統合でのイベントプロファイルの作成と名前の設定」を参照してください。

5. Now Platform sn_si.admin ロールを持つユーザーとして、取り込まれた値またはエクスポートされた添付ファイルデータを Splunk Enterprise から Now Platform セキュリティインシデントにマップします。
   a. スケジュール済みアラートのサンプルデータをフェッチします。
   b. イベントの添付ファイルデータを Splunk Enterprise から手動でエクスポートします。
   c. デフォルトのマッピング構成を編集します。
   d. 必要に応じて、フィルター条件を追加し、既存のセキュリティインシデントにアラートを追加し、スクリプトエディターを使用します。

   詳細については、「Splunk Enterprise Event Ingestion 統合のアラートとイベントのマッピング」と「Splunk Enterprise Event Ingestion 統合でのアラートのマッピング」を参照してください。

6. Now Platform sn_si.admin ロールを持つユーザーとして、Now Platform セキュリティインシデントに表示される Splunk Enterprise のデータをプレビューします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エラーを修正するか、不足しているデータを追加して、エラーメッセージが表示されないようにします。

詳細については、「Splunk Enterprise Event Ingestion 統合でのセキュリティインシデントのプレビュー」を参照してください。

7. Now Platform sn_si.admin ロールを持つユーザーとして、スケジュール済みアラートを使用してプロファイルのアラート取得をスケジュールします。

詳細については、「Splunk Enterprise Event Ingestion 統合でのアラートのスケジュールおよび取得」を参照してください。

ServiceNow の セキュリティオペレーション 向け **Splunk Enterprise Security** イベントの取り込み統合

セキュリティインシデントレスポンス (SIR) 製品と Splunk Enterprise Security 注目イベント取り込み機能の統合により、セキュリティインシデントアナリストは注目イベントデータ (注目と呼ばれる) を収集して処理できます。

概要

データは設定されたポーリングスケジュールに基づいて継続的に取り込まれ、アナリストが潜在的なサイバー脅威を特定して対応するために使用されます。収集されたセキュリティイベントは、Splunk Enterprise Security の注目イベントに関連付けて、この統合で自動的に取り込むことができます。また、個々の注目イベントを Splunk Enterprise Security インシデントレビューコンソールおよびレポートインターフェイスから Now Platform の セキュリティインシデントレスポンス 製品にオンデマンドで手動転送して、セキュリティインシデントを作成することもできます。

この統合により、セキュリティオペレーションセンター (SOC) アナリストは注目イベントと関連貢献イベントデータを表示できます。このデータは、Now Platform セキュリティインシデントレスポンス (SIR) セキュリティインシデントに統合して、さらに調査および修復できます。プロファイルは、Now Platform インスタンスに作成され、Splunk Enterprise Security の相関検索を介して作成されるさまざまな相関イベントタイプを処理します。これらのプロファイルは、SIR セキュリティインシデントでのさまざまな Splunk イベントフィールドの表示方法をカスタマイズします。

主な機能

この統合の主な機能は次のとおりです。

- 複数の注目イベント取り込みプロファイルを作成して、フィッシング、マルウェア、不正なアクセス試行などの特定のタイプの脅威に対して SIR セキュリティインシデントを作成します。
- Splunk ES インシデントレビューコンソールからオンデマンドイベント転送用の複数のイベントプロファイルを作成して、SIR セキュリティインシデントを作成します。
- 関連付けられている SIR セキュリティインシデントフィールドに Splunk 注目イベントフィールド値のマッピングをドラッグアンドドロップします。
- イベントマッピングの詳細を検証するためのサンプル注目イベントに基いて、SIR セキュリティインシデントレイアウトをプレビューします。
- 構成可能な間隔で、履歴注目イベントと進行中の更新された新しい注目イベントを取り込みます。
- SIR インシデント生成基準を満たさない注目イベント (優先度の低いイベント、まだ特定のステータスに達していないイベントなど) を除外します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 一致するフィールド値に基づいて既存の SIR セキュリティインシデントにイベントまたはアラートを集計し、重複するセキュリティインシデントを回避します。
- 双方向インターフェイスを介して SIR インシデントの作成および/またはクローズ条件に基づいて注目イベントを更新し、Splunk ES 注目イベントの更新を ServiceNow SIR インシデント状況と同期させます。

サポートされている **Now Platform** のバージョン

この統合には com.snc.si_dep プラグインが必要です。このプラグインは、セキュリティインシデントレスポンス 製品をサポートするために必要なすべての依存関係を自動的にインストールします。他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。

次の セキュリティオペレーション アプリケーションを、ServiceNow Store からインストールしてアクティブ化する必要があります。スムーズにインストールできるように、アプリケーションを次のリストの順番で、一度に 1 つずつインストールしてアクティブ化します。

1. Security Integration Framework
2. Security Support Common
3. セキュリティインシデントレスポンス

セキュリティオペレーション コアアプリケーションのインストールの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

ServiceNow アドオン

ServiceNow Security Operations Event Ingestion Addon for Splunk ES は、Splunk Enterprise Security インシデントレビューコンソールから Now Platform インスタンスに手動でイベントを転送する場合にのみ必要です。この ServiceNow アドオンは splunkbase で入手できます。

この ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise アプリケーションは、統合でサポートされている自動アラートの取り込みには必要ありません。

サポートされている **Splunk** バージョン

この統合は、Splunk Enterprise バージョン 8.0.1 および Splunk Enterprise Security アプリケーションバージョン 6.2.1 でテストされています。

MID サーバー

Splunk サーバーが企業ネットワーク内に展開されている場合、この統合では、Now Platform® インスタンスにインストールされ、構成された MID サーバーを Splunk サービスに接続する必要があります。Splunk Cloud サービスを使用している場合、MID サーバーは必要ありません。MID サーバーの詳細については、「MID サーバー」を参照してください。

参照

参照	ドキュメント識別子	ドキュメントタイトル
1	Splunk 製品の Web サイト	Splunk Enterprise Security 製品の Web サイト。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

チェックリスト

これらのトピックの印刷可能なチェックリストについては、「Splunk Enterprise Security 注目イベントの取り込み統合用チェックリスト」を参照してください。このリストを使用して、進捗を監視しながら、統合のタスクを進めることができます。

この統合で使用される重要な用語

このセクションでは、この統合で使用されるいくつかの重要な用語について説明します。

インストールと構成では、次の重要な用語が使用されます。以下の用語の詳細については、ServiceNow の製品ドキュメント Web サイト、Splunk の Web サイト、および Splunk リソース ページのリソースを参照してください。

Now Platform

エンタープライズ ServiceNow 製品。Now Platform をベースとして、セキュリティインシデントレスポンス (SIR)、IT Service Management (ITSM)、およびその他の製品などの個々のコンポーネントがビルドされています。

ServiceNow Splunkbase アドオン

統合の手動イベント転送オプションをサポートする Splunk Enterprise Security コンソールにインストールされている ServiceNow アプリケーションです。手動イベント転送は、統合のオプション機能です。この ServiceNow Splunkbase アドオンは、統合によって提供される Splunk からイベントをプルする自動注目イベントの取り込みには必要ありません。

セキュリティインシデントレスポンス (SIR)

検出と初期分析から、封じ込め、根絶、復旧、および最終的なインシデントの事後レビューとクローズに至るまで、セキュリティインシデントの進捗状況を追跡する Now Platform アプリケーション。

Splunk Enterprise Security

Splunk Enterprise Security は、継続的な監視、インシデント応答、SOC 運用のための組織全体の可視化とセキュリティインテリジェンスを獲得し、エグゼクティブにビジネスリスクに関する窓口を提供するのに役立ちます。Splunk Enterprise Security は有料ライセンスを必要とするプレミアムセキュリティソリューションです。このサービスは、このガイドで Splunk コンソールと呼ばれることがあるホスト上または Splunk クラウドオファリング上にあります。

Splunk Enterprise Security 注目イベント

相関検索でイベントまたはイベントのパターンが識別されると、注目イベントが作成されます。相関検索では、セキュリティデータをフィルタリングし、イベント全体を関連付けて、特定のタイプのインシデント (またはイベントのパターン) を識別して、注目イベントを作成します。

Splunk イベント

Splunk サービスの注目イベントを生じる 1 つ以上のデータ要素。Now Platform インスタンスから、どの Splunk イベントが Now Platform セキュリティインシデントをトリガーしたかを検索できます。

MID サーバー

このアプリケーションは、Now Platform と外部アプリケーション、データソース、サービスの間の通信やデータの移動を容易にします。このアプリケーションは通常、オンプレミステクノロジーとの統合に必要です。この Splunk Enterprise Security イベント取り込み統合のために、MID サーバーは Now Platform と Splunk Enterprise Security のオンプレミスインスタンス間の通信を支援します。Now Platform インスタンスを Splunk Cloud インスタンスと統合する場合、MID サーバーは必要ありません。

セキュリティインシデントアドミン (sn_si.admin)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このロールを持つユーザーは、Now Platform インスタンス内の SIR 製品との統合の構成を監督します。

セキュリティインシデントアナリスト (sn_si.analyst)

このロールを持つユーザーは、ServiceNow セキュリティインシデントレスポンス 製品でセキュリティインシデントに対応し、分析します。

Splunk Enterprise Security 統合での Now Platform® インスタンスの設定

次のセクションでは、ServiceNow Store からアプリケーションをインストールする前に Now Platform® インスタンスで完了する必要があるセットアップタスクを示します。

必要なロール：admin

スムーズなインストールと構成を行うために、 アプリケーションをダウンロードしてインストールする前に、次のテーブルを参照して、リストされたすべてのタスクを完了していることを確認してください。

1. 必要な Now Platform® および セキュリティインシデントレスポンス (SIR) のロールがアサインされていることを確認します。

   Now Platform® インスタンスで統合をインストール、セットアップ、および使用するには、次のロールが必要です。

   - Now Platform® アドミンロール (admin) を持つユーザーが ServiceNow Store からアプリケーションをインストールし、セキュリティインシデントアドミン (sn_si.admin) ロールをアサインします。
   - この統合のために Splunk Enterprise Security から手動で注目イベントを転送する場合は、Now Platform® admin ロールを持つユーザーが Now Platform® で (sn_sec_splunkes.api_account_access) ロールを持つユーザーをアサインします。このロールは、Splunk Enterprise Security アドミンロールを持つユーザーが、この統合の手動イベント転送に必要な Now Platform® の API にアクセスすることを許可します。

     Splunk Enterprise Security から Now Platform® インスタンスに自動的に注目イベントを取り込む場合、統合に (sn_sec_splunkes.api_account_access) ロールは必要ありません。
   - sn_si.admin ロールを持つユーザーは、Now Platform® で次のタスクを監督します。
     - イベントプロファイルに名前を付け、作成し、編集します。
     - Splunk Enterprise Security から値を選択し Now Platform® セキュリティインシデントにマップします。
     - 構成を確定する前に、正確性を確認するためにセキュリティインシデントの詳細をプレビューします。
     - 進行中の注目イベントの取り込みをスケジュールします。
     - SIR インシデントが作成されてクローズされたときに、注目イベントの更新を有効にします。
     - セキュリティインシデントアナリスト (sn_si.analyst) ロールをアサインします。
     - sn_si.analyst を持つユーザーは、セキュリティインシデントを処理します。

   詳細については、「Managing roles」を参照してください。

2. Splunk ユーザーロールをアサインします。

   Splunk ES でセキュリティアナリスト (ess_analyst) ユーザーロールをアサインして、Splunk サーバーで統合関連のすべてのアクティビティを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. Splunk API のバージョン 7.2.6 以降を使用していることを確認します。以前のバージョンはサポートされていません。

   Splunk Enterprise Security コンソールへのアクセス権がある場合は、この統合に必要な API にアクセスできます。API に必要なその他の特別なセットアップはありません。

4. MID サーバーがインストールおよび設定されていることを確認します。

   Splunk サーバーが企業ネットワーク内に展開されている場合、Now Platform® インスタンスの MID サーバー を Splunk サービスに接続する必要があります。詳細については、「MID サーバー」を参照してください。

   Splunk Enterprise Security クラウドサービスを使用している場合、MID サーバー は必要ありません。

5. 統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。

   セキュリティインシデントレスポンス Dependency プラグイン (com.snc.si_dep) が必要です。このプラグインは、セキュリティインシデントレスポンス 製品をサポートするために必要なすべての依存関係を自動的にインストールします。統合に必要な他の セキュリティオペレーション アプリケーションをインストールしてアクティブ化する前に、このプラグインをインストールしてアクティブ化します。

   次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。

   a. セキュリティインシデントレスポンス
   b. Security Integration Framework
   c. Security Support Common

   セキュリティオペレーション コアアプリケーションのインストールの詳細については、「セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

統合のために Now Platform® インスタンスが正常に設定されました。次のステップでは、ServiceNow Store から統合用の Splunk Enterprise Security 注目イベントの取り込みアプリケーションをインストールします。詳細については、「Splunk Enterprise Security 注目イベントの取り込み統合用の ServiceNow アプリケーションのインストールと設定」を参照してください。

統合のために Splunk Enterprise Security コンソールから手動でオンデマンドで注目イベントをエクスポートする場合、詳細については「Splunk Enterprise Security 注目イベントの取り込み統合での手動イベント取り込み用の Splunk 環境設定」を参照してください。

Splunk Enterprise Security 注目イベントの取り込み統合用の **ServiceNow** アプリケーションのインストールと設定

Now Platform® インスタンスで統合を実行する前に、これらのインストールと構成のステップを完了して、Now Platform® インスタンスでアプリケーションが セキュリティインシデントレスポンス と セキュリティオペレーション 製品と適切に統合されるようにします。

始める前に
必要なロール:ess_analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Splunk ES でセキュリティアナリスト (ess_analyst) ユーザーロールをアサインして、Splunk サーバーで統合関連のすべてのアクティビティを実行します。

手順

1. ServiceNow Store から統合用の Splunk Enterprise Security イベントの取り込みアプリケーションをインストールしていない場合は、「セキュリティオペレーション 統合のインストール」を参照し、ステップに従ってインストールしてください。
2. アプリケーションのインストールが完了したら、 統合 > 統合構成 をクリックし、[Splunk イベントの取り込み] タイルを見つけます。
3. アプリケーションを設定するには、[新規] をクリックします。

4. または、[構成] ボタンがタイルに表示されている場合は、そのボタンをクリックして既存の構成を編集します。
5. 表示される [イベントの取り込み構成] ダイアログで、フィールドに入力します。

   次の図は、MID サーバーを使用したオンプレミスバージョンの Splunk Enterprise Security 構成用の完成したフォームの例です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Splunk Enterprise Security インシデントレビューコンソールから取り込む各 Splunk Enterprise Security 注目イベントタイプには、Now Platform インスタンス内に一意のイベントプロファイルが必要です。[イベントの取り込み構成] フォームで構成したソースは、各プロファイルが一意の注目イベントタイプを取り込む限り、複数の Now Platform プロファイルで再利用できます。

6. **[Submit]** をクリックします。
検証が正常に完了すると、各構成を含む [セキュリティ統合] ページが表示されます。次の図に示すように、有効な各構成タイルに [更新] および [削除] ボタンが表示されます。

注:
ベーシック認証またはトークンベースの認証のいずれかを使用する必要があります。両方を有効にすると、次のエラーが発生します。

注:
既存の構成タイルをトークンベースに更新する場合は、Splunk Enterprise 設定モジュールでトークンベースの認証サポート設定の既存の Splunk ソース構成を更新するには、この設定をアクティブ化する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

検証と送信が正常に完了すると、各 [イベントの取り込み] の Splunk サーバー構成は [セキュリティ統合] ページにタイルとして保存されます。保存された構成タイルが右上隅にある [セキュリティ統合] ページに表示されていない場合、[構成を表示] リストから [はい] を選択します。

次のタスク
アプリケーションのインストールと設定が正常に完了しました。次のステップは、イベントプロファイルの作成です。

Splunk Enterprise Security 設定の構成

Splunk Enterprise Security (ES) 設定を使用して、事前設定された構成とその値を要件に従って変更します。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > **Splunk ES** 統合 > **Splunk ES** の設定.
2. フォームの各フィールドに入力します。

Splunk ES の設定

フィールド	説明
単一のインシデントに集計できる注目イベント数の制限を強制します。	単一のインシデントに集計する注目イベント数の制限を強制するオプション。 デフォルト値は 100 に設定されています。
24 時間内に作成できるセキュリティインシデント数の制限を強制します。	24 時間内に作成できるセキュリティインシデント数の制限を強制するオプション。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	デフォルト値は 1000 に設定されています。
Splunk から受信する各フィールドで解析する値の数の制限を強制します。	Splunk から受信する各フィールドで解析する値の数の制限を強制するオプション。 デフォルト値は 1000 に設定されています。
Splunk からプルする相関ルールの数	Splunk から取得する相関ルールの数を定義するオプション。 デフォルト値は 500 に設定されています。
Splunk 検索ジョブの存続時間パラメーター (秒)	Splunk 検索の存続時間パラメーターを秒の形式で定義するオプション。 デフォルト値は 600 に設定されています。
1 回の検索で一括処理する注目タイプの数	1 回の検索で一括処理する注目タイプの合計数を定義するオプション。 デフォルト値は 20 に設定されています。
ServiceNow で Splunk 検索ジョブメタデータを保持する日数	ServiceNow で Splunk 検索ジョブメタデータを保持する日数を定義するオプション。 デフォルト値は 30 に設定されています。
フィールドマッピングで値を分割する区切り文字	フィールドマッピングで値を分割する区切り文字を定義するオプション。 デフォルト値は (,) に設定されています。
Splunk からイベントをフェッチする際に追加する重複時間 (分) (Splunk からのインデックス作成の遅延を解消するため)	Splunk からのインデックス作成の遅延を解消するために、Splunk からイベントを取得する際に追加する重複時間 (分) を定義するオプション。 デフォルト値は 30 に設定されています。
更新された注目イベントをプル	更新された注目イベントを取得するオプション。 デフォルト値は [いいえ] に設定されています。
トークンベースの認証をサポートする既存の Splunk ソース構成を更新するには、この設定をアクティブ化します。この設定を有効にしたら、トークンの詳細を使用して統合構成を更新する必要があります。	既存のバージョンからトークンベースの認証をサポートする既存の Splunk ソース構成を更新するオプション。 **注:** 新しいバージョンにアップグレードすると、トークンフィールドは使用できなくなります。トークンベースの認証を取得するには、この設定を有効にし、その後、トークンの詳細を使用して統合構成を更新する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	デフォルト値は [いいえ] に設定されています。

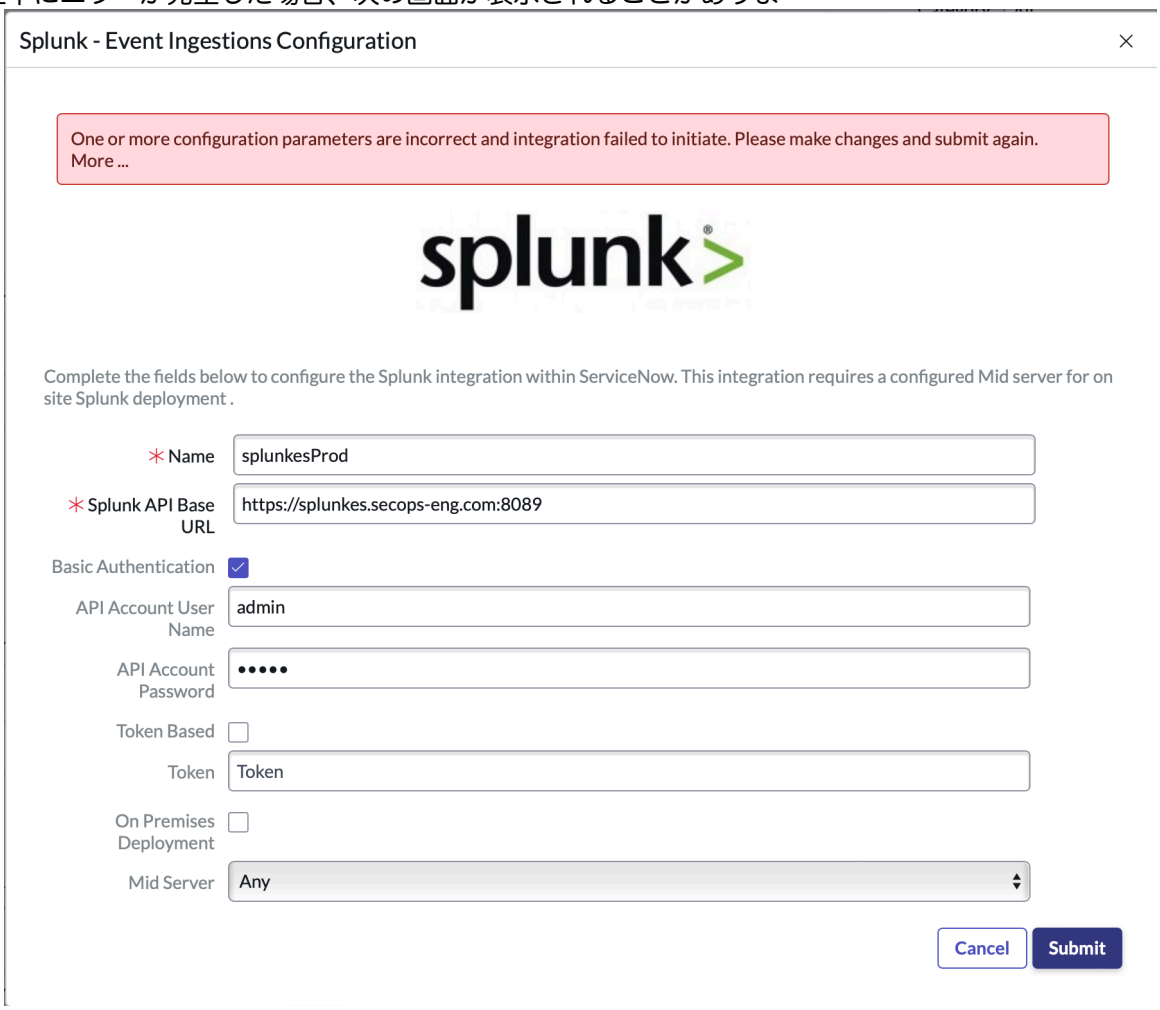
3. [保存] をクリックします。

認証エラー

このセクションでは、一般的な認証エラーとその解決方法について説明します。

証明書の検証に関する問題

認証中にエラーが発生した場合、次の画面が表示されることがありま



す。

API アカウントの認証情報と Splunk のベース URL 情報が正しいことが確認された場合、このエラーはポート 8089 通信の Splunk 証明書に関する問題が原因の可能性があります。ServiceNow インスタンスでは、セキュア接続を確立するために、サーバーのホスト名と一致する共通名を持つ有効な証明書が必要です。詳細については、「証明書」を参照してください。このエラーが表示された場合は、システムログを表示することで、証明書の問題が原因であることを確認できます。

次のようなエラー条件が表示される可能性がありま

す。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

認証を続行するには、ポート 8089 での API アクセス用に提供されている Splunk のデフォルト証明書を置き換える必要があります。SSL 証明書を置き換える方法の詳細については、KB0778285 を参照してください。

Splunk Enterprise Security イベントの取り込み統合でのイベントプロファイルの作成と名前の設定

Now Platform インスタンスにイベントプロファイルを作成し、セキュリティインシデントを作成する Splunk 注目イベントを指定します。

始める前に
必要なロール：sn_si.admin

このタスクについて
Now Platform セキュリティインシデントレスポンス(SIR) セキュリティインシデントが取り込まれた注目イベントから作成される前に、アラートのフィールド値が Now Platform セキュリティインシデントのレイアウトに表示されるため、実際のセキュリティインシデントがどのように作成されるかをプレビューできます。

利用可能な API を使用した統合の観点から、Splunk ES 注目イベントは、個別の注目イベントとして個別に手動で転送されるか、定義されたプロファイルタイプに応じて、Now Platform インスタンスの セキュリティオペレーション 環境に自動的に取り込まれます。

統合ワークフローでは、不正なアクセス試行やマルウェアなどのさまざまなタイプの注目イベントを取り込めます。これらの注目イベントは、インスタンスの セキュリティオペレーション 環境で設定したプロファイルに基づいて取り込まれます。

すべての注目は、プロファイル内の設定された相関検索タイプに対して最初に取り込まれます。取り込まれた注目をさらにフィルタリングして、セキュリティインシデントを作成する注目イベントを指定できます。たとえば、高リスクとして識別された注目イベントに対してのみセキュリティインシデントを作成するフィルターを使用できます。プロファイルがアクティブになり、取り込まれた注目イベントからセキュリティインシデントが作成される前に、注目イベントの個々のフィールド値が、プレビュー用にセキュリティインシデントのレイアウトの対応するフィールドにマッピングされます。

自動翻訳

手順

1. Now Platform インスタンス内のイベントプロファイルの名前は一意である必要があり、常に 1 つのアクティブなイベントプロファイルにのみマッピングできます。
2. Now Platform は、統合のワークフローを使用して特定の注目を取り込みます。
   Splunk ES コンソールの選択基準を満たすすべての注目イベントが、最初に Now Platform インスタンスに取り込まれます。
3. Now Platform のプロファイルは、Splunk ES コンソールの注目イベントをカプセル化したものです。
   プロファイルとともに取り込まれた注目イベントと Splunk ES コンソールへの接続は 1 対 1 の関係 (1 つの接続に対して 1 つの注目イベントタイプ) です。
4. スケジュール済み注目イベントのプロファイルを作成するには、「スケジュール済み注目イベントの取り込み用プロファイルの設定」を参照してください。
5. 手動イベント転送用のプロファイルを作成するには、「手動イベント転送用のプロファイルの設定」を参照してください。

スケジュール済み注目イベントの取り込み用プロファイルの設定

定義されたプロファイルに応じて、Splunk ES の注目イベントが Now Platform インスタンスの セキュリティオペレーション 環境に自動的に取り込まれます。

次の表は、注目イベントのスケジュール済み取り込み用プロファイルを設定するために従う必要があるタスクのリストです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール済み注目イベントの取り込み用プロファイルを設定するステップ

タスク	セクション
イベントプロファイルの作成	「スケジュール済み注目イベントの取り込み用プロファイルの作成」を参照してください。
相関検索名に基づく注目イベントの選択	「Splunk ES イベントの取り込み統合でのプロファイルの相関ルール名に基づいた注目イベントの選択」を参照してください。
注目イベントフィールドのマッピング	「Splunk Enterprise Security 統合での注目イベントフィールドのマッピング」を参照してください。
カスタムマッピングの作成	「Splunk ES 注目イベントのインシデントレビューと貢献イベントの詳細のマッピング作成 (スケジュール済みの取り込み)」を参照してください。
セキュリティインシデントのプレビュー	「Splunk Enterprise Security イベントの取り込み統合のセキュリティインシデントをプレビューする」を参照してください。
新規および更新された注目イベントのスケジュール設定と取得	「Splunk Enterprise Security イベントの取り込み統合での新規および更新された注目イベントのスケジュール設定と取得」を参照してください。
SIR インシデント状況に基づく注目イベントの更新とクローズの自動化	「SIR インシデント状況に基づく注目イベントの更新とクローズの自動化」を参照してください。

スケジュール済み注目イベントの取り込み用プロファイルの作成

注目イベントが自動的に取り込まれるようにプロファイルを設定できます。

始める前に

必要なロール：sn_si.admin

手順

1. Now Platformインスタンスで注目イベントまたは相関ルールタイプのイベントプロファイルを作成するには、 **Splunk Integration** > **Splunk** イベントプロファイル.
2. [Splunk イベントプロファイル] フォームが表示されない場合は、進捗状況バーの [名前] をクリックします。
3. [新規] をクリックします。
4. フィールドに入力します。

   完成したフォームの例が表の後に表示されます。

フィールド	説明
名前	プロファイルの一意の名前。名前が一意でない場合、エラーが表示され、重複するプロファイル名は保存されません。

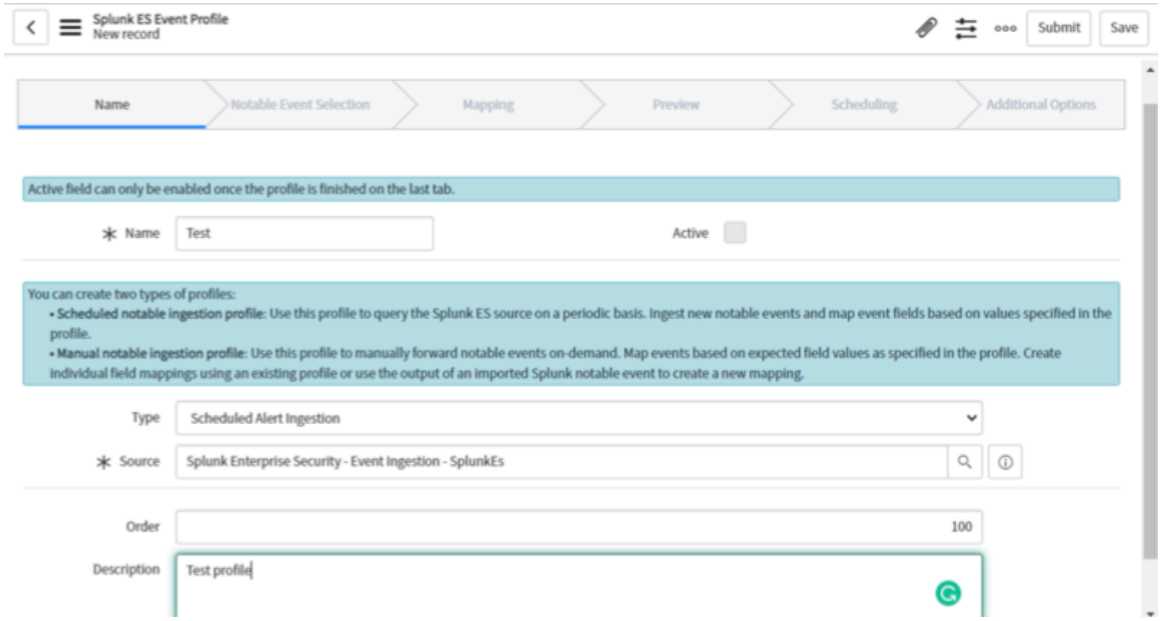
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	Now Platform インスタンスのプロファイル名は一意である必要があります。
アクティブ	デフォルトでは、このチェックボックスはクリアされ、無効にされています。アクティブにする前に、プロファイルのすべてのセクションを完了する必要があります。
タイプ	選択リストからプロファイルタイプを選択します。 ○ スケジュール済みイベントの取り込み：このタイプのプロファイルは、構成されたスケジュールで取り込まれる注目イベントをサポートします。フィールドに入力します。 ○ 手動イベント転送：このタイプのプロファイルは、オンデマンドで Splunk Enterprise Security インシデントレビューコンソールから手動で転送される注目イベントをサポートします。これらのタイプのプロファイルのフォームに入力するには、次のステップを参照してください。
ソース	注目イベントを取り込むために構成した Splunk サーバーまたは検索終了。複数の Splunk サーバーが構成されている場合は、プロファイル用に取り込まれる注目イベントタイプに適したサーバーを選択します。値を入力する必要があります。
順序	デフォルトは 100 です。 複数のプロファイルを作成した場合、この値は、2 つ以上のプロファイルが同じトリガー条件を共有する場合の実行時の優先度を示します。プロファイル内の番号が最も小さいワークフローの優先度が最も高くなります。
(オプション) 説明	このプロファイルを他のプロファイルと区別するための追加テキスト。

次の図は、スケジュール済み注目イベントタイプの完成したフォームの例です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. スケジュール済み注目イベントがあるプロファイルの場合は、プロファイル構成を続行するオプションを 1 つ選択します。

次のタスク
次のステップでは、自動取り込みの対象となる注目イベントを選択します。

Splunk ES イベントの取り込み統合でのプロファイルの相関ルール名に基づいた注目イベントの選択

スケジュール済み注目イベントの取り込み用プロファイルを作成した後、対応する注目イベントを Now Platform セキュリティインシデントレスポンス セキュリティインシデントにマップするために、このプロファイルの Splunk Enterprise Security 相関ルール名を選択します。

始める前に
必要なロール：sn_si.admin

このタスクについて
Now Platform インスタンスで利用可能な相関ルールを表示して、セキュリティインシデントを取り込んで作成する注目イベントタイプを確認します。相関ルールを選択します。このフォームのリストから 1 つ以上の注目イベントを選択できます。

手順

1. [注目イベントの選択] ページが表示されない場合は、進捗状況バーで選択して表示します。
2. [相関ルール] リストから、次のいずれかのオプションを選択して単一の相関ルールまたは複数の相関ルールを選択し、それを [利用可能] 列から [選択済み] 列に移動します。

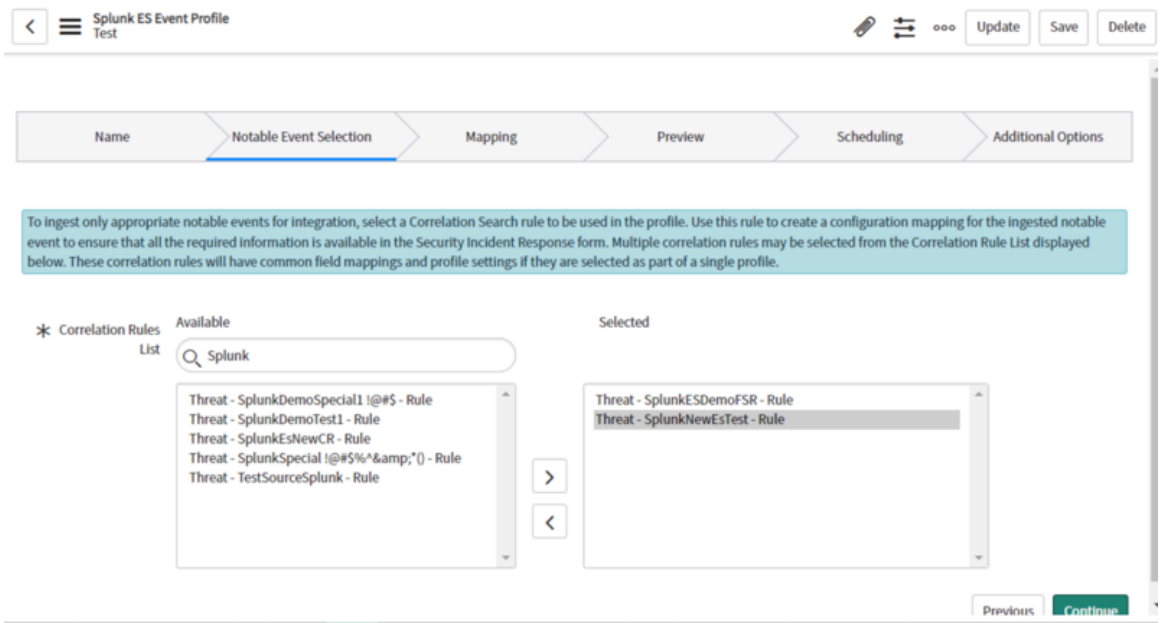
   このフォームの相関ルールのリストは、Splunk ES インシデントレビューコンソールの相関ルールのリストと一致します。このフォームには最大 500 件の相関ルールが表示されます。Splunk ES に 500 件を超える相関ルールがリストされている場合、Now Platform インスタンスのこのフォームには最初の 500 件の注目イベントのみが表示されます。

オプション	説明
[相関ルールリスト] 検索フィールドにテキストを入力します。	検索フィールドの下の列は、入力したテキストに基づいて利用可能なオプションでフィルタリ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

オプション	説明
	ングされます。相関ルールを選択し、矢印キーを使用して、選択したアラームを [利用可能] から [選択済み] に移動します。
[相関ルール] リストで、[相関ルール] をダブルクリックします。	[選択済み] 列に選択内容が入力されます。
[相関ルール] リストで、[相関ルール] をシングルクリックします。	相関ルールが選択されます。矢印キーを使用して、選択した相関ルールを [利用可能] から [選択済み] に移動します。



3. オプションを 1 つ選択して続行します。

次のタスク

スケジュール済み Splunk Enterprise Security プロファイルの相関ルールが正常に選択されました。次のステップでは、注目イベント値を セキュリティインシデントのフィールドにマップします。

Splunk Enterprise Security 統合での注目イベントフィールドのマッピング

プロファイルの特定の相関ルールと注目イベントタイプを特定したら、次のステップでは、個々の注目イベントフィールドを Now Platform セキュリティインシデントレスポンス (SIR) セキュリティインシデントのフィールドにマップします。

概要

マッピングステップでは、選択した相関ルールのサンプルの注目イベントを取り込むことも、手動で転送された注目イベントの注目イベントデータをエクスポートすることもできます。イベントマッピングプロセスは、作成するプロファイルタイプに関係なく同じです。

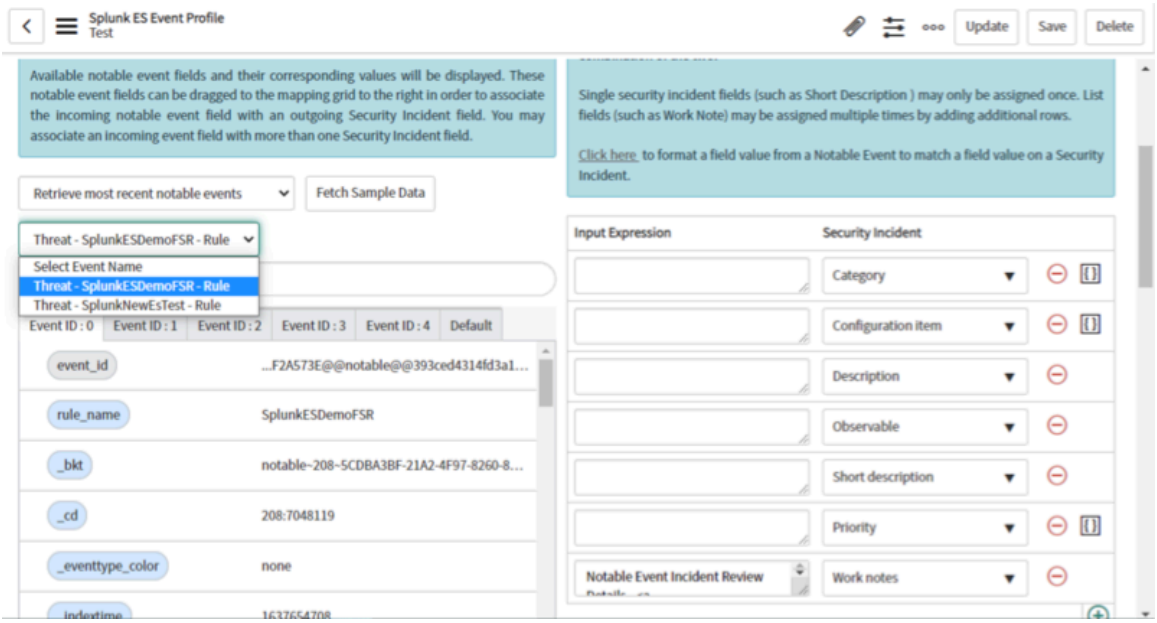
次の図は、イベントプロファイルのタイプごとに提供されるデフォルトのマッピング構成の例です。セキュリティインシデントを入力するフィールドをカスタマイズできます。このマッピングフェーズで、関連するすべての注目イベントフィールドデータが、SIR インシデントフォームの適切な場所にマッピングされていることを確認して、SIR インシデントをプレビューセクションで可視化できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

複数の相関が使用されている場合は、必要なイベントを選択することで注目イベントをフェッチできます。取り込み用に複数のアラートを構成した場合は、[アラート名] を使用してアラートを選択します。

クリックしてデータをフェッチすると、Splunk 注目イベントフィールドの名前と対応する値がフォームの左側に入力されます。これらは、SIR セキュリティインシデントフィールドにマップ可能な Splunk 注目イベントフィールドです。一部のフィールドは、SIR セキュリティインシデントフィールドに複数回マッピングできます。



Splunk コンソールでいくつかのサンプル注目イベントを確認して、フィールドマッピング構成ステップに取り込むこともできます。このステップは、進捗状況バーで [マッピング] とラベル付けされます。このページが表示されない場合は、進捗状況バーの [マッピング] をクリックします。Splunk Enterprise Security から最大 5 つのサンプル注目イベントを取り込んで、注目イベントフィールドのマッピングプロセスを支援できます。選択した相関ルールの最新の 5 つの注目イベントを取り込むか、注目イベント ID に基づいて最大 5 つの特定の注目イベントを取り込むオプションがあります。

注目イベントをマップするために必要なステップの概要を以下に示します。

- スケジュール済み注目イベントのサンプルデータの取り込み：自動的に取り込まれた注目イベントプロファイルに使用されるサンプルデータの場合、サンプルデータが取得されると、使用可能な注目イベントフィールドとそれに対応する値が、マッピングフォームの左側のデフォルトのマッピングレイアウトに表示されます。プルした特定の注目イベント ID の値を表示するタブが表示されます。フォームの左側にある [注目イベントサンプルの取り込み] セクションのすべての重要なフィールドが、フォームの右側の ServiceNow セキュリティインシデントフィールドにマッピングされていることを確認します。
- フィールドマッピング：左側から注目イベントフィールドをドラッグして、右側の [ServiceNow SIR インシデントマッピング] セクションにドロップし、マッピング構成を編集します。右側のマッピングで、[受信注目イベント] フィールドを [送信セキュリティインシデント] フィールドに関連付けることができます。
- マッピングエクスペリエンス：[SIR インシデントフィールドマッピング] セクションの下部にある [+] アイコンを使用してフィールドを追加または削除し、マッピンググリッドをカスタマイズします。提供されている色分け (マップ済みのフィールドはグレー表示、マップされていないフィールドは青) を使用して、見落とされているフィールドや重複フィールドを追跡します。
- インシデント生成条件：マッピングセクションが完了したら、フィルター条件を設定して、どの注目イベントがセキュリティインシデントを作成し、どの注目イベントがフィルタリングで除外

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

されるか (低優先度の違反など) を指定できます。これは、[注目イベントのマッピング (Notable Event Mapping)] セクションの下にある [インシデント生成条件] セクションで行います。

- イベント集計基準：類似の重複する可能性があるインシデントを作成するのではなく、既存の SIR セキュリティインシデントに受信注目イベントを集計する追加のイベント集計基準を定義します。この追加の集計機能では、各プロファイルのフィールド一致値基準を使用して、関連するすべてのセキュリティ注目イベントデータを単一のセキュリティインシデントに配置することで、アクティブな重複するセキュリティインシデントの数を減らすことができます。
- フォーマットフィールド変換：場合によっては、Splunk Enterprise 注目イベントのイベントフィールド値は、SIR セキュリティインシデントのフィールドに直接変換されないことがあります。これらの値については、マッピングステップでスクリプトエディターを使用してセキュリティインシデントのフィールド値をフォーマットできます。類似しているが同一ではない値をフォーマットする場合は、スクリプトエディターを使用します。たとえば、スクリプトエディターを使用すると、 [マルウェアアラート] と [ウイルス感染]のカテゴリ値でソースカテゴリのフィールド値が異なる可能性がありますが、フォーマットフィールド変換機能を使用して、SIR セキュリティインシデントの [カテゴリ] フィールドで両方の値を一般的な悪意のあるコードアクティビティに変換することができます。

次のステップでは、注目イベントを取り込み、値を SIRセキュリティインシデントフィールドにマップします。

Splunk ES 注目イベントのインシデントレビューと貢献イベントの詳細のマッピング作成 (スケジュール済みの取り込み)

注目イベントフィールドマッピングのステップでは、注目イベントから個々のイベントフィールドを (Now Platform セキュリティインシデントレスポンスSIR) セキュリティインシデントのフィールドにマップします。

始める前に

必要なロール：sn_si.admin

このタスクについて

マッピンググリッドは、相関ルールの選択で選択した注目イベントタイプに合わせてカスタマイズできます。マップされていない残りのフィールドはすべて青で表示されるのに対し、すでにマップされたフィールドはグレー表示されるため、イベントフィールドの色分けは、マップされたイベント値の追跡に役立ちます。色分けすることで、セキュリティインシデントに追加されたフィールド値、およびマップされていない残りの重要なイベント情報を視覚的に把握できます。

フォームの左側にある [注目イベントサンプルの取り込み] 列から、右側の [SIR インシデントフィールドマッピング] 列のセキュリティインシデントフィールドに最大 5 つの注目イベントをマッピングします。

フォームの右側にあるマッピンググリッドのフィールドを追加または削除して、カスタムマッピングを作成します。セキュリティインシデントレスポンスフォームに入力する通常重要なフィールドであるデフォルトのフィールドが表示されます。ただし、[+] および [-] ボタンを使用して、これらのフィールドを削除し、追加のフィールドを表示することができます。フォームの右側にあるマッピンググリッドのフィールドを追加または削除して、カスタムマッピングを作成します。フィールドをカスタマイズすると、SIR セキュリティインシデントのデフォルトのマッピンググリッドに表示されていない Splunk フィールドをマッピングできます。

手順

1. このマッピングフォームが表示されない場合は、進捗状況バーの [マッピング] をクリックします。
2. 取り込みがスケジュールされているプロファイルの場合は、 [注目イベントサンプルの取り込み] の下にある [サンプルデータをフェッチ] をクリックして、Splunk Enterprise コンソールから選択した相関ルールに対応する最新のサンプル注目イベントをプルします。

自動翻訳

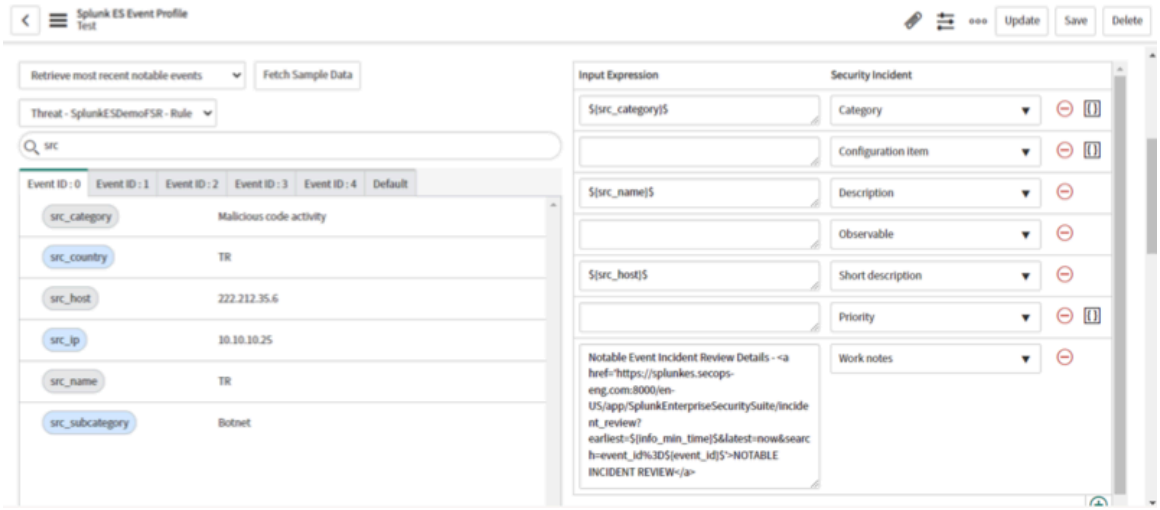
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
最新のサンプル注目イベントをプルするか、注目イベントマッピングエクスペリエンスに使用する特定の注目イベントの一意の注目イベント ID を指定できます。

注目イベントのフィールドと値の結果は、個別のタブとして表示されます。最大 5 つの注目イベントを取り込むことができます。

サンプル注目イベントのプルには少し時間がかかる場合があります。トランザクションが機能していることを示すメッセージが画面の上部に表示されます。

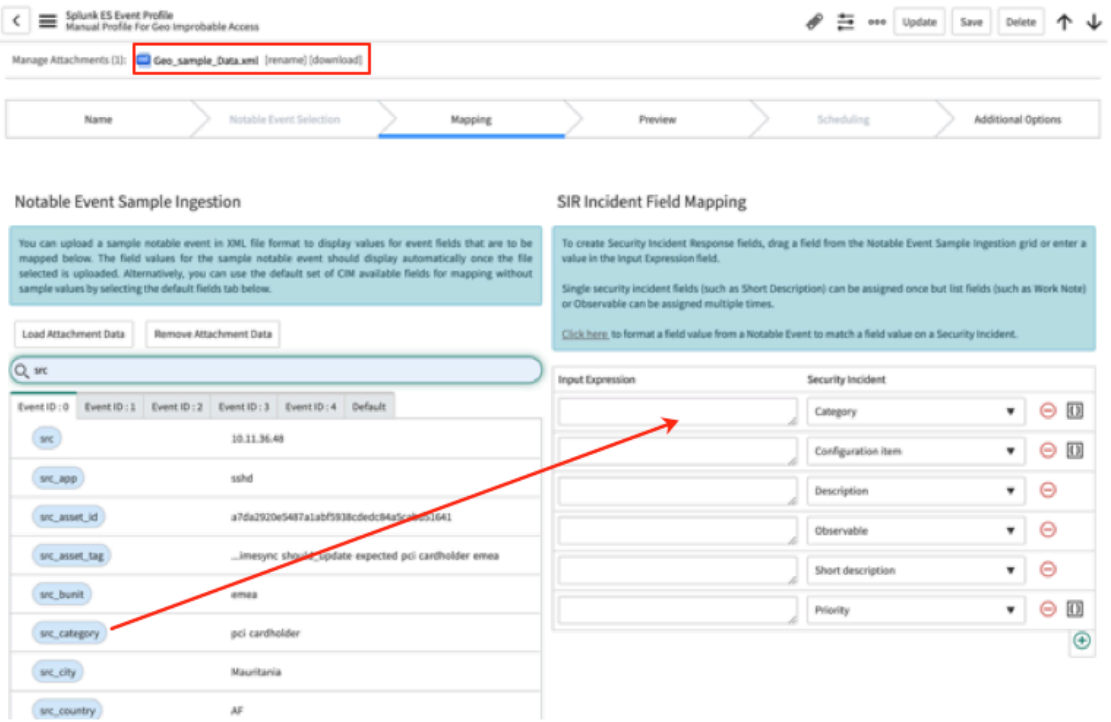
次の図では、取り込みプルの完了後に、取り込まれた注目イベントまたはインポートされたサンプルイベントのフィールド名値のペアがこのフォームの左側に表示されます。これらの値は、フォームの [SIR インシデントフィールドマッピング] 側のセキュリティインシデントフィールドにマッピングする値です。



3. フォームの左側からフォームの右側のセキュリティインシデントのフィールドにフィールド値をマッピングするには、フォームの左側で青色のフィールド名をクリックしたままにします。
4. フィールド名 (src_category など) をドラッグして、[セキュリティインシデント] 列のフィールド名の横にある [入力式] 列のフィールドにドロップします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



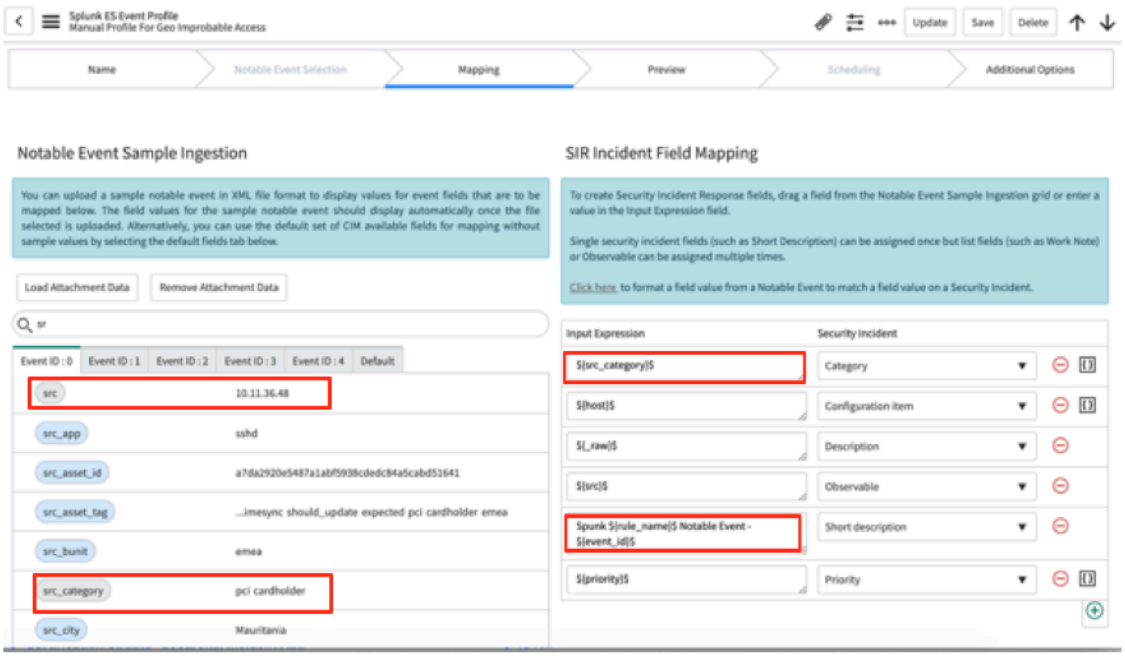
フィールド値が [入力式] 列に表示されます。次の画像で、src_category をセキュリティインシデントの［カテゴリ］フィールドにマップします。ただし、左側から右側のフィールドまでの任意の値を一致させることができます。プレビューステップで、セキュリティインシデントの値が正しくマッピングされていることを確認します。

マッピングプロセスでイベントフィールドが見落とされたり重複したりしないように、フィールドは色分けされています。左側のライトブルーのフィールドは、注目イベントフィールドがまだ未選択で、セキュリティインシデントにマップされていないことを示します。受信注目フィールドをセキュリティインシデントの 1 つ以上のフィールドに関連付けることができます。

灰色のフィールドは、フィールドが選択され、セキュリティインシデントのフィールドにマッピングされていることを示します。この色分けは、マッピングを追跡するのに役立ちます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. フォームの右側のセキュリティインシデントに表示されるデフォルトのフィールドにフィールドを追加するには、次のステップを実行します。

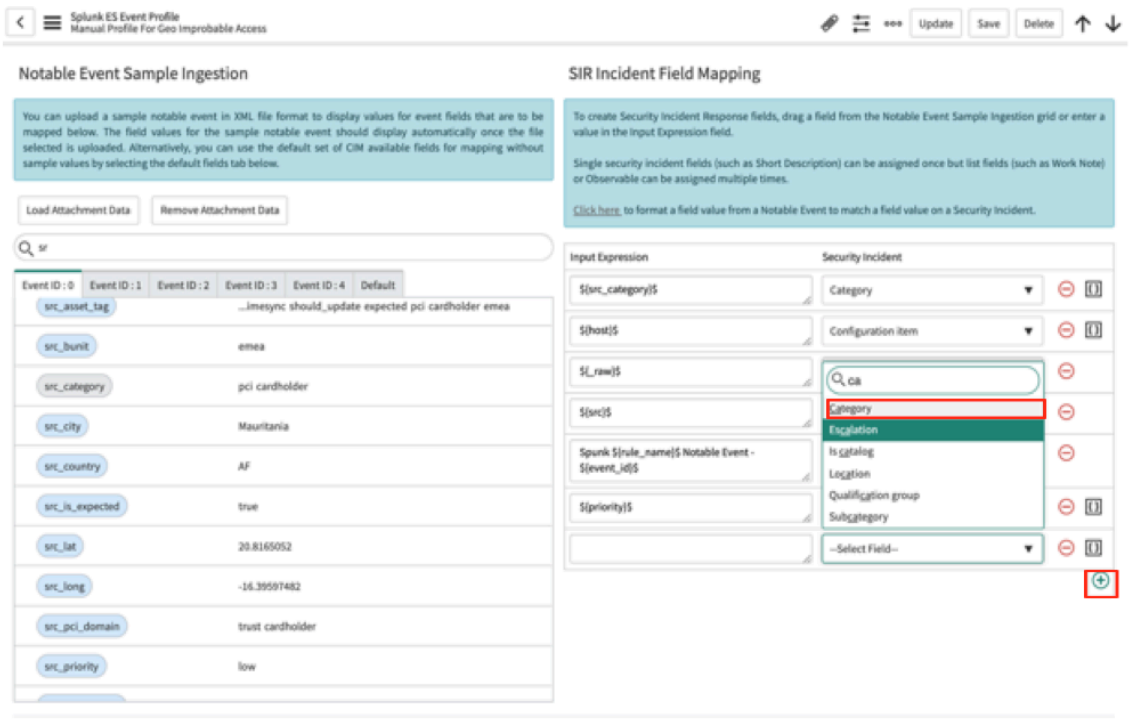
a. フォームの右側の [SIR インシデントフィールドマッピング] セクションで、グリッドの下部にあるプラスアイコンをクリックします。
新しいフィールドが表示されます。

b. [セキュリティインシデント] 列で表示されているリストを展開し、フィールドを選択します。

新しいフィールドの展開されたリストでは、一部のフィールドが網掛けされています。次の図では、セキュリティインシデントにマッピングされているため、カテゴリのバックグランドがグレーになっています。フォームの左側の注目イベントフィールドの色分け同様、セキュリティインシデントフィールドのこの色分けも、すでにマップされた SIR インシデントフィールドを追跡するのに役立ちます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
同じセキュリティインシデントに複数の観測事象を表示できるため、[観測事象] フィールドを異なる値で複数回マップできます。同様に、[構成アイテム] フィールドと [作業メモ] フィールドは複数の値をサポートします。複数の値をサポートできないフィールドに 2 つの値をマッピングしようとすると、インシデントをプレビューするときに、フィールドに値がないことを示すエラーメッセージが表示されます。同様に、セキュリティインシデントのフィールドに複数のオプションを選択できるリストがあり、リストに表示されていないフィールドにオプションをマップしようとすると、そのフィールドはセキュリティインシデントに入力されません。

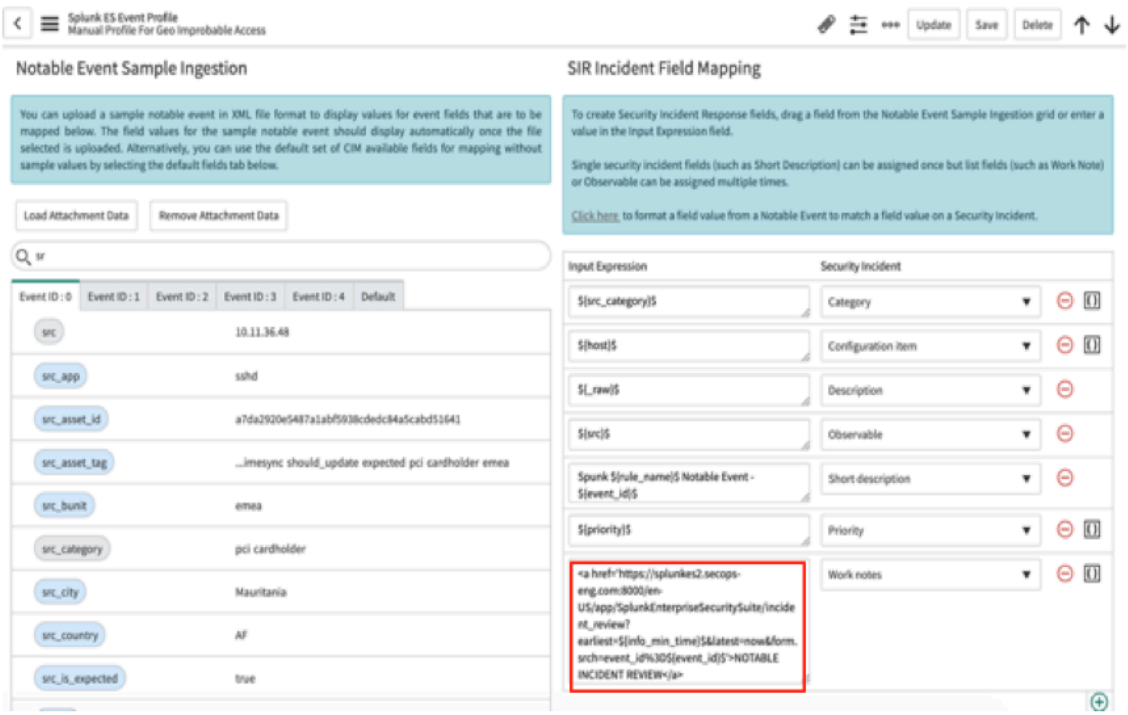
c. または、新しい行の [検索] フィールドに値を入力します。

d. フォームの左側の [入力式] フィールドで [イベント **ID]** を左クリックして選択します。

6. フィールドの値をマッピングに追加するか、削除して、マッピングを続行します。
次の図は、編集されたマッピングの例です。右側の下部のフィールドに [作業メモ] フィールドが追加され、複数の値が表示されます。長いテキスト文字列フィールドの場合、マッピングフィールドを展開して完全な文字列を表示し、以下のスクリーンショットに示すように、[作業メモ] フィールドを追加してフィールドの右下隅をプルすることでサイズを変更できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



警告:
[SIR インシデントフィールドマッピング] セクションの [入力式] フィールドに記載されている URL とポート番号は単なる例であり、初期設定の URL またはポート番号ではないことに注意してください。

プレビューでは、これらの値はセキュリティインシデントの [作業メモ] に表示されます。値は [マッピング] セクションに追加したフィールドの値であり、[作業メモ] フィールドに複数の値がマッピングされているため、値は入力されたとおりに表示されます。この例では、フィールドに入力したスペースと句読点が、セキュリティインシデントのプレビューの作業メモとして [関連アイテム] セクションに表示されます。

次の画像は、前の画像の値がセキュリティインシデントにどのように表示されるかを示した例です。

7. オプション: スクリプトエディターを開き、編集を続行します。

   (Optional) スクリプトエディターの詳細については、「Splunk Enterprise Event Ingestion 統合でのスクリプトエディターを使用したアラート値のフォーマット」を参照してください。

   注目イベントのインシデントレビューおよび貢献イベントのハイパーリンクを含む

   マッピングフィールドに加えて、*sn_si.admin* は、インシデントを処理するセキュリティアナリストが、Splunk Enterprise Security コンソールで注目イベントのインシデントレビューと、ドリルダウン検索の一部である基になる貢献イベントの両方にハイパーリンクできるようにする文字列値をマッピングできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の文字列値には、Splunk Enterprise Security サーバー名と、これらの詳細へのハイパーリンクに使用できる適切な変数が含まれています。

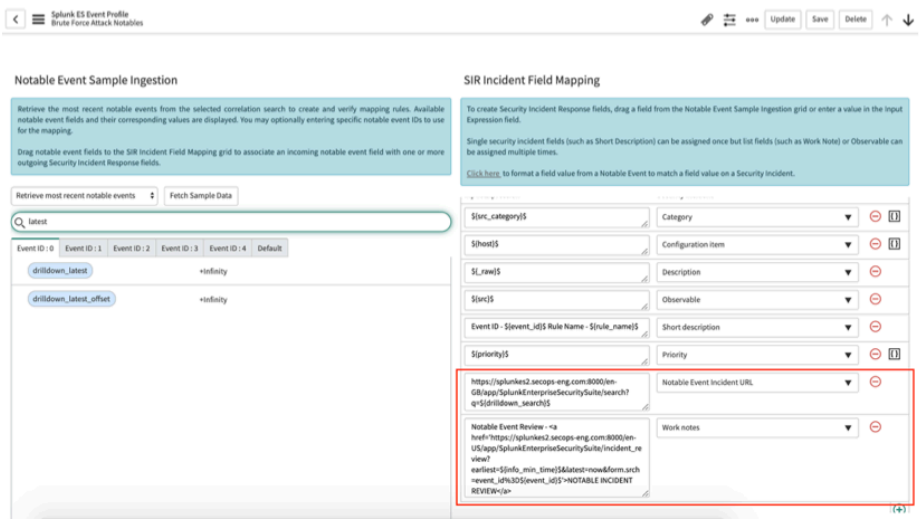
- 注目イベントインシデントレビューへのハイパーリンク：https://splunkes2.secops-eng.com:8000/en-US/app/SplunkEnterpriseSecuritySuite/incident_review?earliest=${info_min_time}$&latest=now&form.srch=event_id%3D${event_id} $

  splunkes2.secops-eng:8000 は Splunk サーバーのソースで、info_min_time と event_id は注目イベントから抽出されたイベントフィールド値です。

- 注目イベント貢献イベント (ドリルダウン検索) へのハイパーリンク：https://splunkes2.secops-eng.com:8000/en-GB/app/SplunkEnterpriseSecuritySuite/search?q=${drilldown_search}$

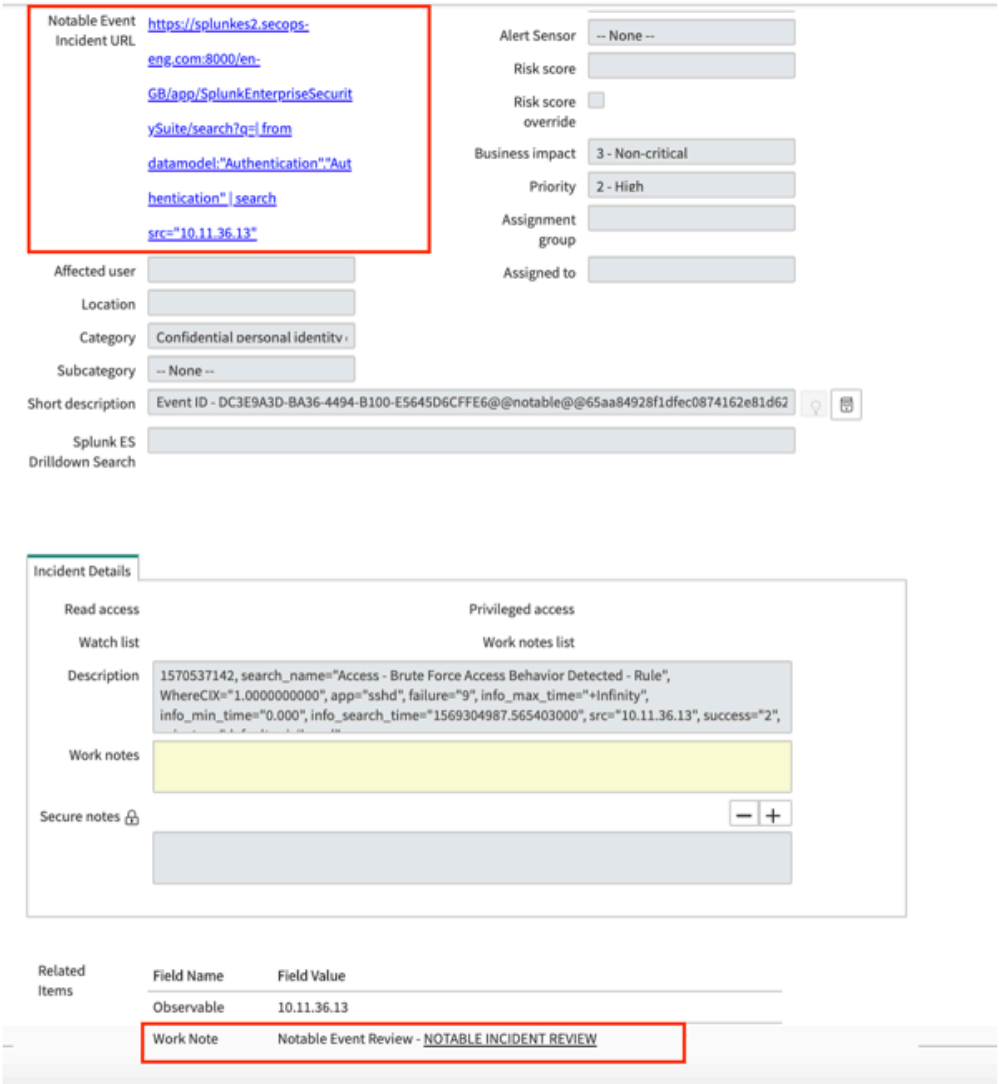
  splunkes2.secops-eng.com:8000 は Splunk サーバーのソースで、drilldown_search は注目イベントから抽出されたイベントフィールド値です。

次の画像は、[作業メモ] フィールドにマッピングされた注目イベントインシデントレビュー URL と、注目イベントインシデント URL と呼ばれるカスタムフィールドにマッピングされた注目イベント貢献イベント (ドリルダウン検索) へのハイパーリンクを示しています。



次の画像は、注目イベントインシデントレビューへのハイパーリンクと貢献イベント URL を含む SIR インシデントプレビューです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



インシデント生成フィルタリング条件

8. オプション: 先行するフィールドマッピングのステップを完了したら、インシデント生成条件ビルダーで同じフィールド値を使用して、SIR セキュリティインシデントを作成するために受信注目イベントが満たす必要がある追加の条件を定義することができます。
インシデント生成条件を設定するには、次のステップを実行します。

   a. フォームの [インシデント生成条件] セクションまでスクロールし、[条件に基づいてフィルター] チェックボックスをオンにして、オプションを有効にします。

      (Optional) フィルター条件ビルダーが表示されます。これらのフィルターを使用して、フィールドで説明されている特定の条件に一致するセキュリティインシデントを作成します。

      フィルター条件ビルダーの最初のフィールドのリストにあるオプションは、取り込まれたイベントの [注目イベントサンプルの取り組み] セクションに表示されるフィールドと一致します。これらのフィールドは動的であり、取り込む Splunk 注目イベントまたは手動で転送された注目

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

イベントサンプルに選択するイベントに応じて変化します。入力する条件は大文字と小文字が区別され、Splunk Enterprise Security 注目イベントの値と正確に一致する必要があります。フィルターフィールドに入力する値が不明な場合、Splunk Enterprise Security コンソールに戻り、注目イベントをレビューしてキーワードを確認することができます。

b. 条件ビルダーのリストとフィールドを使用して、最初の行のフィルターを設定します。

c. 条件を追加するには、フィールドの右側にある [**AND**] または [**OR**] をクリックします。[**AND**] を選択した場合は、すべての条件に一致する必要があります。**[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。

d. オプション: 2 行目で、2 番目のフィルター条件を設定します。

(Optional) 次の画像は、セキュリティインシデントが作成される前に一致する必要がある 2 つの条件を含む例です。

(Optional) 入力した両方のフィルタリング条件に一致した場合にのみセキュリティインシデントが作成されるように、インシデント生成条件を設定しました。

この種のインシデント生成条件フィルタリングで、Splunk で基となる相関検索またはフィルターを変更することなく、セキュリティイベントを絞り込み、作成する不要なセキュリティイン

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

シデントの数を制限することができます。追加のフィルター条件を設定する場合、すべての条件に一致する注目イベントのみがインシデントにマップされます。

> **注:**
> イベントフィールド名に引用符 ("")、ハイフン (')、アンダースコア (-)、アットマーク (@)、またはアンパサンド (@) などの特殊文字が含まれている場合、これらの文字はマッピング変換のために置き換える必要があり、重複イベント名が作成される可能性があります。マッピングは適切に実行できますが、重複するイベント名を持つフィールドを区別するために数値のサフィックスが追加されます。たとえば、最初のイベントフィールドが alerts.alert で、2 番目のイベントフィールドが alerts@alerts の場合、残りの標準的なテキスト文字は同じであるため、これらのフィールドは一意に識別されません。この場合、サフィックスが 2 番目のイベントフィールドに追加され、フィールド名が「alerts@alert(1)」に変更されます。

(Optional) 類似の注目を処理して重複インシデントを防止するイベント集計基準

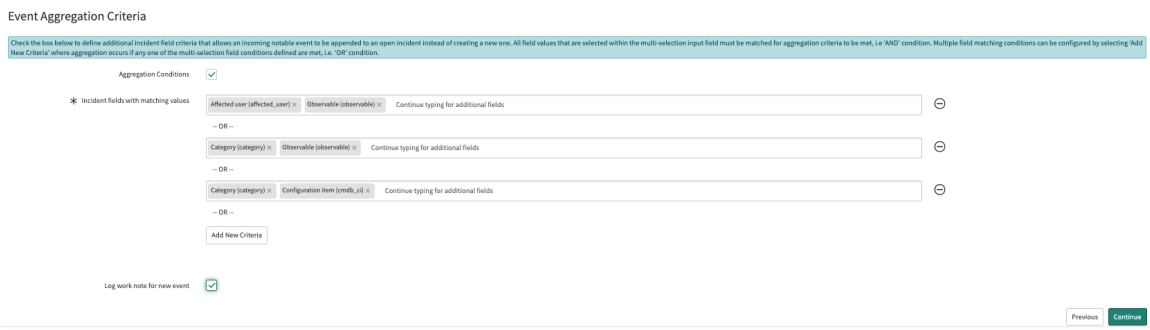
9. オプション: 重複セキュリティイベントが作成されないように、追加のイベント集計条件を定義して、受信注目イベントをオープンセキュリティインシデント別に集計することができます。条件を設定するには、以下のステップを実行します。

   a. フォームで [イベント集計基準] セクションにスクロールし、[集計条件] チェックボックスをオンにして、このオプションを有効にします。

      (Optional) 値が一致するインシデントフィールドが表示されます。これらのフィールド名は、SIR セキュリティインシデントで構成されたカスタムフィールドを含むセキュリティインシデントのフィールドです。

   b. 複数選択入力フィールドから、Now Platform の既存のセキュリティインシデントで照合するフィールド値を選択します。

   c. [新しい基準を追加] を使用して複数のフィールド一致条件を選択します。
      複数選択入力フィールドで選択したすべてのフィールド値は、AND 条件を使用して集計基準と照合されます。[新しい基準を追加] をクリックし、OR 条件を使用して、定義された複数選択フィールド条件のいずれかを満たしている場合に集計が行われるように複数のフィールド一致条件を選択します。

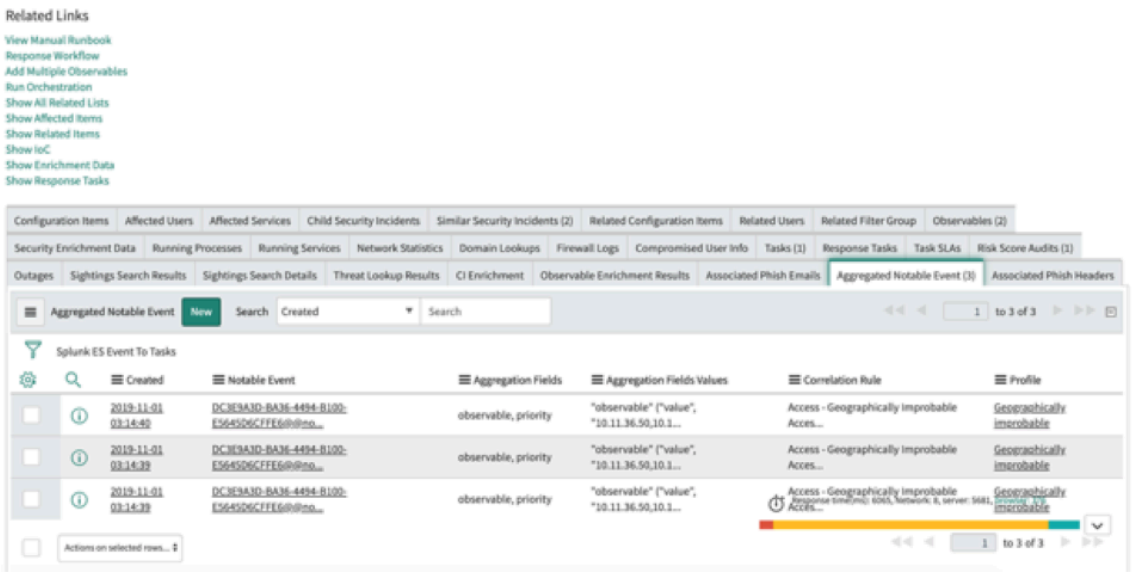


新しい注目イベントが、マッピングステップの集計フィールド条件で選択されたすべての値と一致する場合、新しい注目イベントは、同じフィールド値を持つ最新のオープンセキュリティインシデントに自動的に追加されます。セキュリティインシデントを扱う sn_si.analyst ロールを持つユーザーは、セキュリティインシデントの関連リストで、追加されたすべての集計注目イベントを表示できます。セキュリティインシデントの集計された注目イベントはすべて、[タスクに対する Splunk イベント] 関連リストに表示されます。このリストには、関連するタイムスタンプと集計されたフィールド値の詳細が表示されます。この情報は、これらの注目イベントが既存のセキュリティインシデントに集計される理由を理解するのに役立ちます。このタブが表示さ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

れない場合は、 [関連リンク] の下のレコードの左側にスクロールし、[すべての関連リストを表示] リンクをクリックします。



d. オプション: セキュリティインシデントで最近追加された新しい注目イベントの作業メモを記録するには、このチェックボックスをオンにしてこのオプションを有効にします。
作業メモには、新しい注目が追加され、アラートの詳細へのリンク、およびマッピングセクションの作業メモフィールドに追加された可能性のあるその他の詳細が記録されます。

Splunk注目イベントから SIR セキュリティインシデントのフィールドに値を正常にマッピングしました。また、インシデント生成フィルタリング基準を使用してセキュリティインシデントの作成を制限する追加条件も構成しました。イベントフィールド値が設定された集計基準に一致する場合は、注目イベントを既存の SIR セキュリティインシデントに追加しました。

10. いずれかを選択して、プロファイル構成を続行します。

自動翻訳

次のタスク
次のステップでは、 セキュリティインシデントにマッピングした値をプレビューします。

Splunk Enterprise Security イベントの取り込み統合のセキュリティインシデントをプレビューする

マッピングステップを完了したら、Now Platform® セキュリティインシデントレスポンス (SIR) セキュリティインシデントでマッピングした値をプレビューします。このプレビューステップでは、セキュリティインシデントに表示するすべての注目フィールドがマッピングされていることを確認できます。

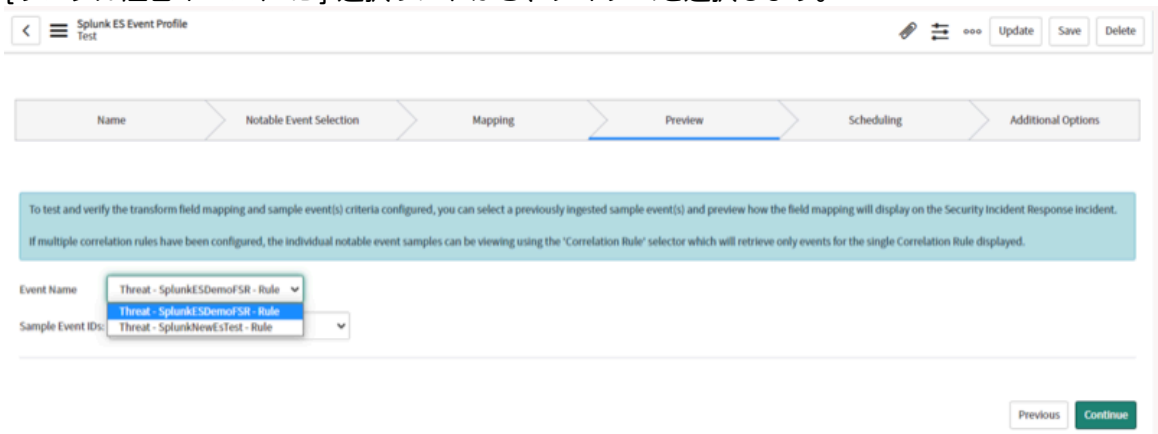
始める前に
必要なロール：sn_si.admin

このタスクについて
セキュリティインシデントをプレビューし、必要に応じてマッピングを再編集して、エラーのあるフィールドを修正するか、欠落しているデータを入力します。プレビューが正常に完了しない場合、スケジュール設定ステップに進むことはできません。SIR セキュリティインシデントのプレビューは、SIR 製品の実際のインシデントとして保存されません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. セキュリティインシデントのプレビューが表示されない場合は、進捗状況バーの [プレビュー] をクリックします。
2. 複数のイベントが使用された場合は、[イベント名] 選択リストからアイテムを選択します。
3. [サンプルの注目イベント ID] 選択リストからイベント ID を選択します。
4. [サンプル注目イベント ID] 選択リストから、アイテムを選択します。



セキュリティインシデントが表示されます。フィールドの情報は変更しないでください。このビューは読み取り専用であり、このセキュリティインシデントのレコードは保存されません。

5. セキュリティインシデントの注目イベント値のフィールドマッピングを確認します。

前の画像は、マッピングエラーのあるプレビューの例です。この例では、注目イベントのフィールド値に、SIR インシデントフォームの参照フィールドの許容値がありません。ServiceNow 顧客管理データベース (CMDB) の [構成アイテム] フィールドの入力値が見つからなかったことを示すエラーメッセージが表示されます。その結果、このマップされたフィールド値は、さらに変更しないと SIR セキュリティインシデントフォームに表示されません。

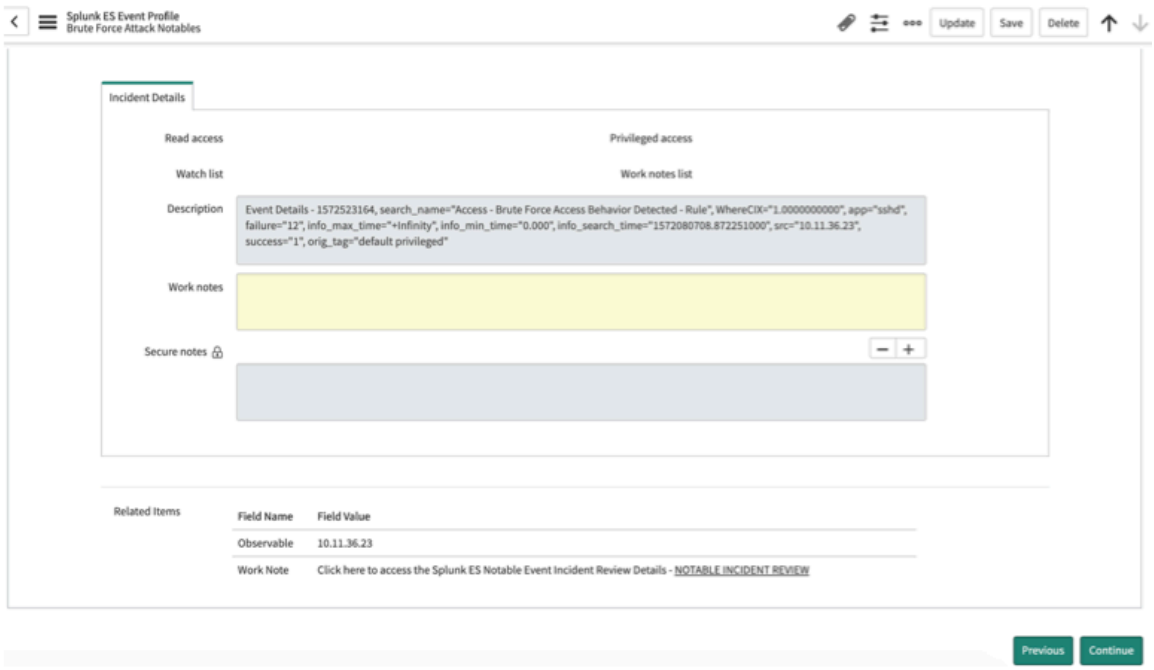
6. このエラーを解決するには、進捗状況バーの [マッピング] をクリックします。
7. マッピングを編集して誤った値を修正するか、欠落しているデータを入力します。
8. マッピングを再度プレビューし、エラーメッセージに記載されているエラーの修正を続行します。

次の図は、すべてのエラーメッセージが解決された後の SIR セキュリティインシデントの下半分にある [インシデントの詳細] タブの例です。この例では、 [説明] および [作業メモ] フィールドがマッピングされ、これらのフィールドには Splunk Enterprise Security 注目イベントサンプルからプルされた値のペアの値が入力されます。最初の [作業メモ] フィールドには値がありません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

マッピングステップで、このフィールドはマッピンググリッドで空のままになっていました。値を含む追加の [作業メモ] フィールドが、マッピングセクションに追加されました。



9. エラーを修正し、フィールドが意図したとおりであることを確認したら、続行するオプションを 1 つ選択します。

次のタスク

エラーメッセージが表示されず、セキュリティインシデントのフィールドマッピングに問題がない場合は、次のステップでは Splunk Enterprise Event Ingestion 統合でのアラートのスケジュールおよび取得 を行います。

Splunk Enterprise Security イベントの取り込み統合での新規および更新された注目イベントのスケジュール設定と取得

自動注目イベントの取り込み用プロファイルの場合、このステップはイベントプロファイル構成で必要です。このステップでは、必要に応じて、注目イベント取得のデフォルトの設定を確認したり、スケジュールを変更したりすることができます。このステップでは、日付範囲を使用して履歴注目イベントを取得することもできます。

始める前に

必要なロール：sn_si.admin

このタスクについて

自動注目イベント取り込み用プロファイルの場合、[スケジュール] ステップで履歴注目イベントを取り込むかどうかを選択できます。また、アラートプロファイル構成に一致する将来の新しい注目イベントと更新された注目イベントをポーリングする頻度も選択します。

自動注目イベント取り込み用プロファイルの場合は、プロファイルをアクティブ化する前に、スケジュールとアラートの取得を確認して変更します。スケジュール済みアラート用プロファイルの場合、このステップはすべてのイベントプロファイル構成プロセスで必要なステップです。

これらのポーリング間隔をプロファイルごとに設定します。Splunk イベントの取り込み統合のパフォーマンスは、ポーリング間隔が異なると影響を受けます。スケジューリングでは、Splunk Enterprise Security サーバーのポーリングのオーバーヘッドを減らすことと、注目イベントが作成または更新されたときにできるだけ早く通知することのバランスを取ることをお勧めします。どのプ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

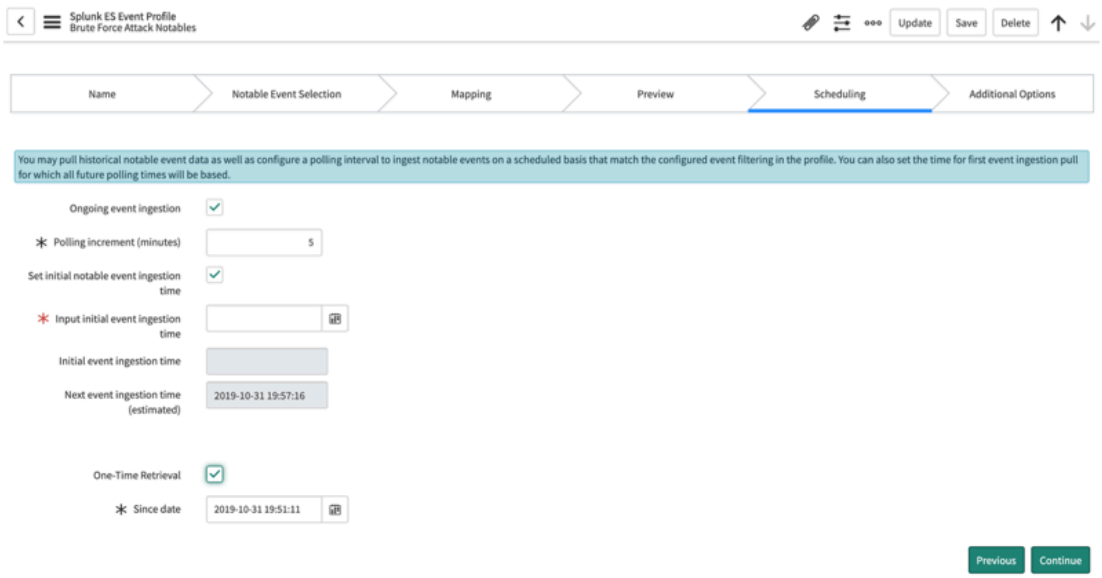
ロファイルにも 5 分のデフォルト値が設定されていますが、必要に応じてこの設定を 1 分に変更することもできます。

新規および更新された注目イベントのプル

ポーリングスケジュールが設定されると、スケジュール済みジョブは、以前にプルされたが、インシデントのフィルター条件を満たしていなかった新規の注目イベントと更新された注目イベントの両方をプルします。これにより、注目イベントが最初に作成されたときに存在しなくても、たとえば調査フェーズ中に更新が発生した後に存在する可能性がある条件に基づいて、インシデントを作成できます。特定の注目イベントに対してインシデントが作成されると、その後の更新は無視されます。これは、注目がアクティブな ServiceNow セキュリティインシデントとして扱われていることが想定されるためです。ただし、以前に取り込まれたが、インシデント生成条件を満たしていない他のすべての注目は引き続きプルされ、アクティブなインシデントの一部になるまでインシデント生成条件と照合されます。

手順

1. 進捗状況バーに [スケジュール] ページが表示されない場合は、[スケジュール] を選択します。
2. Splunk Enterprise Security コンソールから注目イベントをプルする方法とタイミングをスケジュールするものを選択します。



初期注目イベントの取り込み時刻をスケジュールする例として、現地時間の午前 4 時に 1 日 1 回実行される日次 Splunk セキュリティチェックがある場合、Now Platform インスタンスで対応する注目イベントプロファイルを現地時間午前 4 時 5 分に実行するように設定して、セキュリティ障害イベントをすぐにキャプチャし、セキュリティインシデントを作成できます。[初期イベントの取り込み] フィールドに「04 05 00」と入力します。[インクリメント (分)] フィールドに「1440 (24 時間)」と入力して、最初のイベントの取り込みから 24 時間後に次のイベントの取り込みをスケジュールします。初期イベントの取り込み時刻と次のイベントの取り込み時刻の両方がフィールドに表示されます。

3. この例の設定を構成するには、次のステップを実行します。

   a. [スケジュール] ページを表示した状態で、[進行中のイベントの取り込み] チェックボックスをオンにしてこのオプションを有効にします。

   b. [インクリメント (分)] フィールドに「1440 (24 時間)」と入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

c. [初期イベントの取り込みを選択 **(Select Initial event ingestion)]** チェックボックスをオンにして [初期イベントの取り込み] と [次のイベントの取り込み] フィールドの編集を有効にします。

d. [初期イベントの取り込み] フィールドに「04 05 00」と入力します。
[次のイベントの取り込み (推定)] フィールドに、次のイベントの取り込み時刻が表示されます。

4. 次のいずれかをクリックして、プロファイル構成を続行します。

SIR インシデント状況に基づく注目イベントの更新とクローズの自動化

セキュリティインシデントは、Splunk Enterprise Security 統合を使用して双方向インターフェイスで作成した後に作成および更新できます。

始める前に

Splunk Enterprise Security 統合には、セキュリティインシデントを作成し、セキュリティインシデントが作成および/またはクローズされた後に注目イベントを更新できるようにする、双方向のインターフェイスがあります。

関連するインシデントの詳細には、SIR インシデント番号、アサイン先グループ、 SIR インシデント URL が含まれます。このセクションは、Splunk Enterprise Security 注目イベントを更新するオプションの機能を提供するプロファイル構成セットアップの最後の部分です。

必要なロール：sn_si.admin

手順

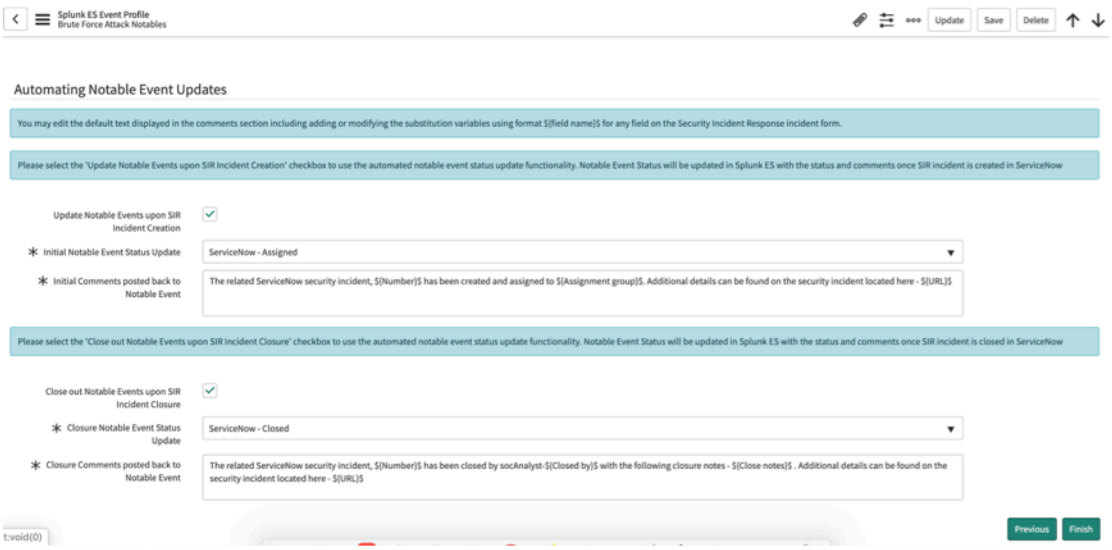
1. 進捗状況バーに [その他のオプション] ページが表示されない場合は、[その他のオプション] を選択します。
2. 以下の手順に従って、セキュリティインシデントの更新に基づいて、注目イベントを更新するための構成を完了します。

3. [完了] をクリックして、構成を完了します。
確認ダイアログが表示されます。これで統合のセットアップと構成が正常に完了しました。このプロファイルをアクティブ化して、スケジュールに基づいて Splunk Enterprise Security コンソールから注目イベントをプルします。24 時間内に作成できるセキュリティインシデント数は 1,000 件に制限されます。発生したアラートごとに最大 100 件の注目イベントに制限されます。制限に達すると、後続の注目イベントは無視されます。

   次の画像は、デフォルト値が入力された [その他のオプション] タブを示しています (

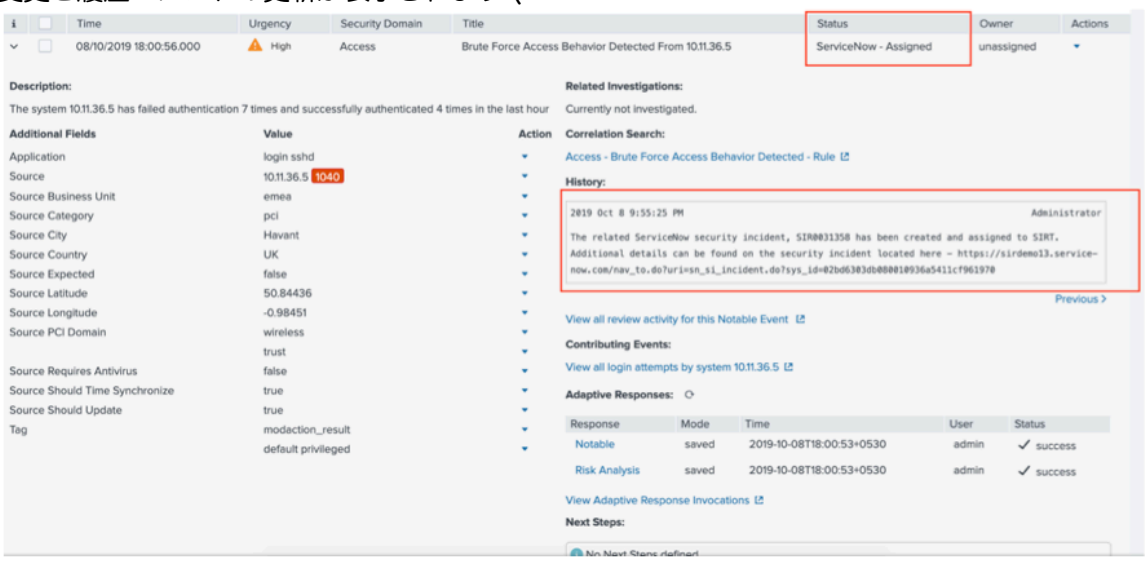
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



)。

[その他のオプション] の構成を有効にすると、注目イベントインシデントレビューでステータスの変更と履歴コメントの更新が表示されます (



)

手動イベント転送用のプロファイルの設定

定義されたプロファイルに応じて、Splunk ES の注目イベントが個別の注目イベントとして Now Platform インスタンスの セキュリティオペレーション 環境に転送されます。

注目イベントの手動転送用のプロファイルを設定するには次のタスクを実行してください。

タスク	セクション
イベントプロファイルの作成	「手動で転送されるイベントのプロファイルの作成」を参照してください。
注目イベントフィールドのマッピング	「Splunk Enterprise Security 統合での注目イベントフィールドのマッピング」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスク	セクション
カスタムマッピングの作成	「Splunk ES 注目イベントのインシデントレビューと貢献イベントの詳細のマッピング作成(手動転送)」を参照してください。
セキュリティインシデントのプレビュー	「Splunk Enterprise Security イベントの取り込み統合のセキュリティインシデントをプレビューする」を参照してください。
手動取り込み用に Splunk 環境を設定	「Splunk Enterprise Security 注目イベントの取り込み統合での手動イベント取り込み用の Splunk 環境設定」を参照してください。
SIR インシデント状況に基づく注目イベントの更新とクローズの自動化	「SIR インシデント状況に基づく注目イベントの更新とクローズの自動化」を参照してください。

手動で転送されるイベントのプロファイルの作成

手動イベント転送用のプロファイルを設定できます。

始める前に

必要なロール：sn_si.admin

手順

手動イベント転送をサポートするプロファイルを作成するには、次のステップを実行します。

Splunk Enterprise Security コンソールからオンデマンドで転送するイベントの場合、既存のプロファイルに基づいて個々のフィールドマッピングを行うことができます。または、エクスポートされた添付ファイルデータの新しいマッピンググリッドを作成することもできます。手動で転送するイベントは、イベントプロファイルでスケジュールされません。

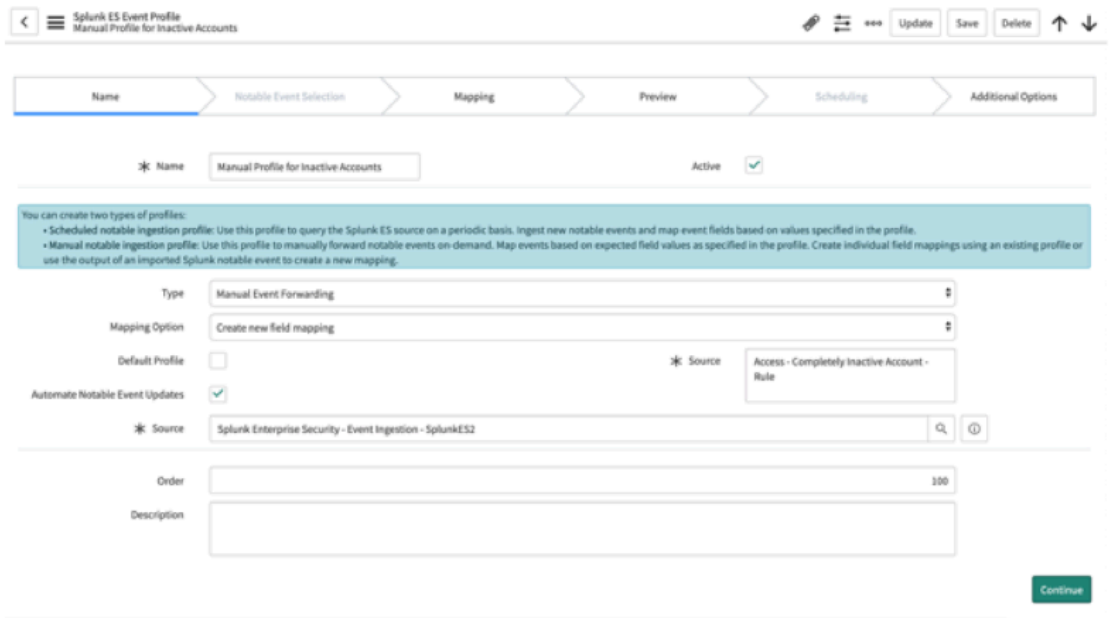
a. まだ選択されていない場合は、[タイプ] フィールドの選択リストで [手動イベント転送] を選択します。

b. 表示される [マッピングオプション] フィールドで、選択リストからマッピングオプションを 1 つ選択して続行します。

[マッピングオプション] 選択リストで利用可能なマッピングオプションの詳細については、次の図とテーブルを参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



新しいフィールドマッピングオプションの作成

オプションまたはフィールド	説明
新しいフィールドマッピングオプションの作成	イベントの新しいフィールドマッピング。 作成しているプロファイルに類似した既存のフィールドマッピングがない場合は、このオプションを選択して新しいマップを作成します。
デフォルトプロファイル	 すべての Splunk イベントのデフォルトのイベント転送プロファイル。デフォルトはクリア (非アクティブ化) されています。 このオプションを有効にすると、このプロファイルが手動イベント転送のデフォルトプロファイルになります。このプロファイルは、手動で転送されたイベントのソースと一致しない場合に使用されます。これは、不明なソースを持つすべてのイベントのデフォルトプロファイルになります。 デフォルトのプロファイルオプションが有効になっている場合、 [ソース] フィールドは使用できません。
ソース (注目イベントフィールド)	これは通常、 総当たり攻撃などの注目をトリガーした相関ルールを定義するフィールドです。 デフォルトのプロファイルオプションが有効になっている場合、このフィールドは使用できません。 利用可能な場合、このフィールドは、通常はイベントタイプごとに異なる Splunk 相関ルールに基づいて、セキュリティインシデントフィー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

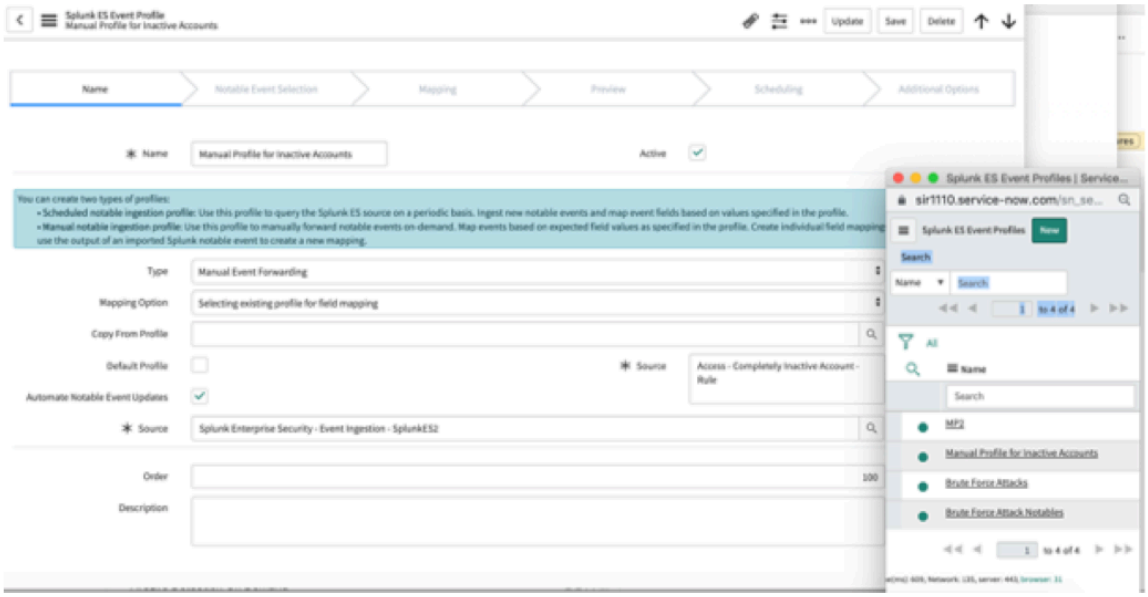
オプションまたはフィールド	説明
	ルドへの一意のイベントフィールドマッピングを許可します。 さまざまな相関ルールを個別に管理する場合は、相関ルールに基づいてさまざまなプロファイルイベントプロファイルを作成して、この要件を満たすことができます。
注目イベントの更新を自動化	SIR インシデントが注目イベントから作成されたとき、および/または SIR インシデントがクローズされたときに、注目イベントステータスを更新してコメントを追加する場合は、このチェックボックスをオンにします。これは、SIR インシデントを作成する最初のトリガー注目イベントと集計イベントの両方で発生します。
ソース (Splunk サーバー)	注目イベントのソースとして構成した Splunk サーバー。複数の Splunk サーバーが構成されている場合は、プロファイル用に更新される注目イベントタイプに適したサーバーを選択します。値を入力する必要があります。
順序	デフォルトは 100 です。この設定はデフォルトのままにします。 多数のプロファイルを作成した場合、この値は、2 つ以上のプロファイルがトリガー条件を共有する場合の実行時の優先度を示します。プロファイル内の番号が最も小さいワークフローの優先度が最も高くなります。
(オプション) 説明	このプロファイルを他のプロファイルと区別するためのテキスト。

新しいフィールドマッピングがあるプロファイルの場合は、[ソースタイプ] フィールドに値を入力したことを確認してから、[続行] をクリックして構成のマッピングステップに進みます。

既存のフィールドマッピングがあるプロファイルの詳細については、次の図とテーブルを参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



フィールドマッピングオプションの既存のプロファイルの選択

オプションまたはフィールド	説明
フィールドマッピングの既存のプロファイルを選択	新しい注目イベントプロファイルの既存のフィールドマッピングを再利用します。[プロファイルからコピー] フィールドが表示されます。 このプロファイルの既存のフィールドマッピングをコピーするには、次のステップを実行します。 **i.** 表示される [プロファイルからコピー] フィールドの左側にある検索アイコンをクリックします。 **ii.** 表示される Splunk ES イベントプロファイルリストで、コピーするマップが含まれるプロファイル名をクリックします。 プロファイル名が [プロファイルからコピー] フィールドに表示されます。
デフォルトプロファイル	一致しないソースのある、すべての Splunk 注目イベントのデフォルトイベント転送プロファイル。デフォルトはクリア (無効化) されています。 このオプションを有効にすると、このプロファイルが手動イベント転送のデフォルトプロファイルになります。 デフォルトのプロファイルオプションが有効になっている場合、 [ソース] フィールドは使用できません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプションまたはフィールド	説明
ソース (注目イベントフィールド)	これは通常、 総当たり攻撃などの注目をトリガーした相関ルールを定義するフィールドです。 デフォルトのプロファイルオプションが有効になっている場合、このフィールドは使用できません。 利用可能な場合、このフィールドは、通常はイベントタイプごとに異なる Splunk 相関ルールに基づいて、セキュリティインシデントフィールドへの一意のイベントフィールドマッピングを許可します。 さまざまな相関ルールを個別に管理する場合は、相関ルールに基づいてさまざまなプロファイルイベントプロファイルを作成して、この要件を満たすことができます。
注目イベントを自動化	セキュリティインシデントが注目イベントから作成されたとき、またはセキュリティインシデントがクローズされたときに、注目イベントステータスを更新してコメントを追加する場合は、このチェックボックスをオンにします。これは、セキュリティインシデントを作成する最初のトリガー注目イベントと集計イベントの両方で発生します。
ソース (Splunk サーバー)	注目イベントのソースとして構成した Splunk サーバーまたは検索終了。複数の Splunk サーバーが構成されている場合は、プロファイル用に更新される注目イベントタイプに適したサーバーを選択します。値を入力する必要があります。
順序	デフォルトは 100 です。この設定はデフォルトのままにします。 複数のプロファイルを作成した場合、この値は、2 つ以上のプロファイルがトリガー条件を共有する場合の実行時の優先度を示します。プロファイル内の番号が最も小さいワークフローの優先度が最も高くなります。
(オプション) 説明	このプロファイルを他のプロファイルと区別するためのテキスト。

プロファイルの既存のマッピングを選択するフォームの下部で、[完了] をクリックしてプロファイルの構成を完了します。

Splunk ES 注目イベントのインシデントレビューと貢献イベントの詳細のマッピング作成 (手動転送)

注目イベントフィールドマッピングのステップでは、注目イベントから個々のイベントフィールドを (Now Platform セキュリティインシデントレスポンスSIR) セキュリティインシデントのフィールドにマップします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_si.admin

このタスクについて
フォームの左側にある [注目イベントサンプルの取り込み] 列から、右側の [SIR インシデントフィールドマッピング] 列のセキュリティインシデントフィールドに最大 5 つの注目イベントをマッピングします。

フォームの右側にあるマッピンググリッドのフィールドを追加または削除して、カスタムマッピングを作成します。SIR インシデントフォームに入力する通常重要なフィールドであるデフォルトフィールドが表示されます。ただし、[+] および [-] ボタンを使用して、これらのフィールドを削除し、追加のフィールドを表示することができます。フォームの右側にあるマッピンググリッドのフィールドを追加または削除して、カスタムマッピングを作成します。フィールドをカスタマイズすると、SIR セキュリティインシデントのデフォルトのマッピンググリッドに表示されていない Splunk フィールドをマッピングできます。

手順

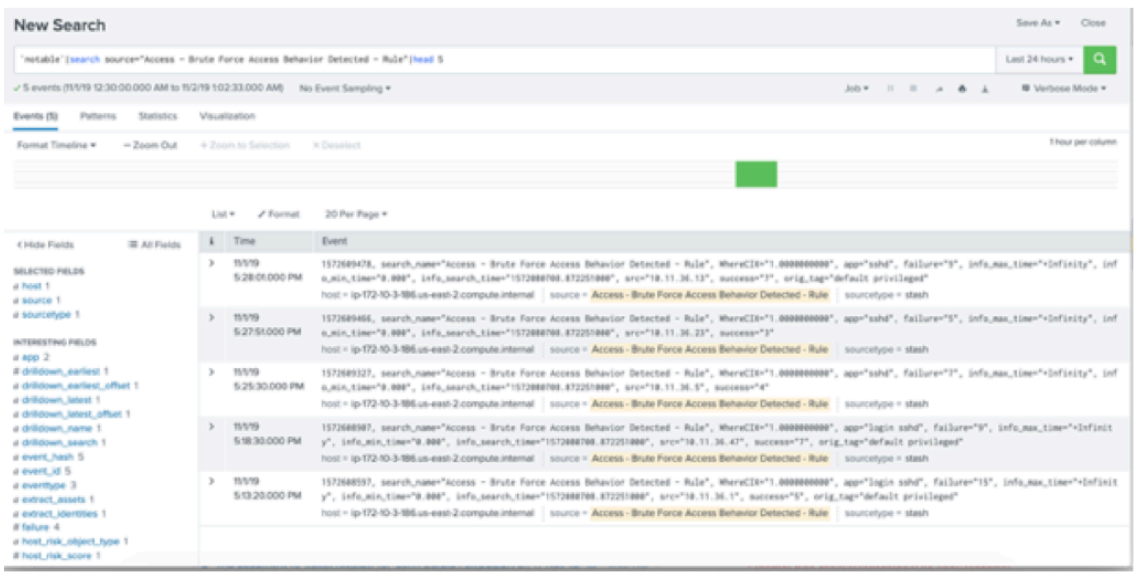
1. このマッピングフォームが表示されない場合は、進捗状況バーの [マッピング] をクリックします。
2. Now Platform® インスタンスに添付ファイルデータをアップロードするには、これらのステップを実行します。

   a. まだログインしていない場合は、Splunk Enterprise コンソールにログインします。

   b. [検索] タブに移動し、エクスポートする注目イベントデータを含む検索の名前を入力します。総当たりアクセス動作相関ルールの注目イベントを取得するための検索形式の例は、「`notable`|search source="Access - Brute Force Access Behavior Detected - Rule」です。

   c. 注目イベントを展開し、[フィールド] 列でインポートするフィールドを選択します。

   これらのフィールドは、Now Platform® インスタンスの [マッピング] ページにエクスポートされて表示されるフィールドと値のペアです。



   d. Splunk Enterprise コンソールの [検索] ページの右上にある [エクスポート] アイコンをクリックします。

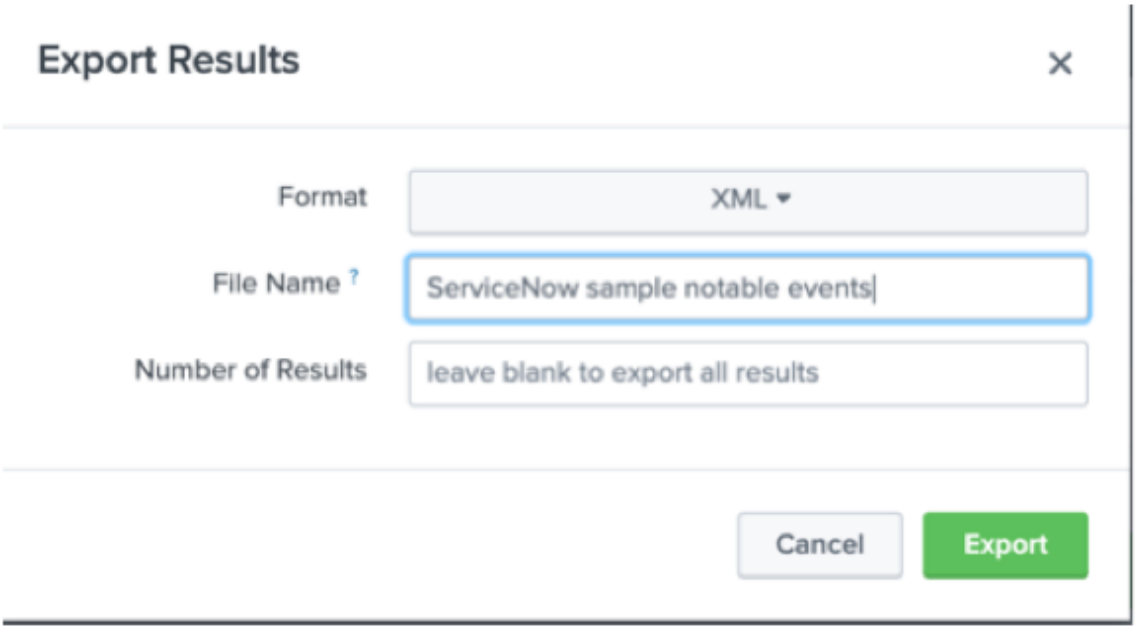
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

e. 表示されるダイアログの [形式] フィールドの選択リストで、**[XML 形式]** をクリックします。

f. オプション: 新しいファイル名を入力します。

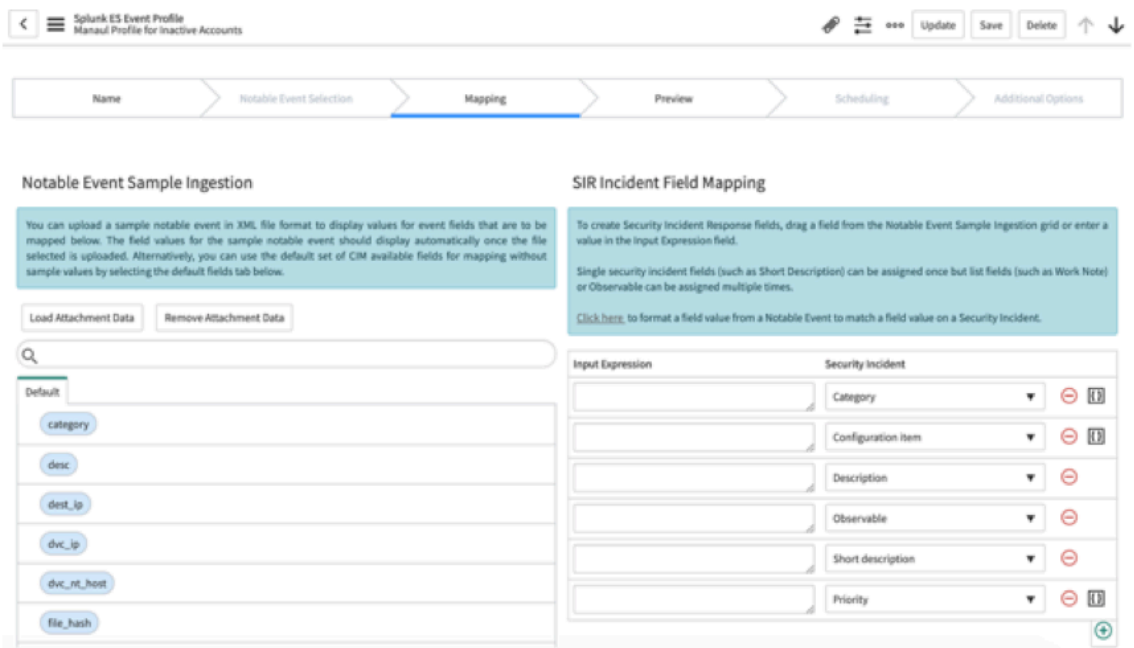
g. [エクスポート] をクリックします。



エクスポートされた Splunk 注目イベントの XML ファイルを Now Platform® インスタンスにアップロードする必要があります。

h. Now Platform® インスタンスに [マッピング] ページが表示されない場合は、進捗状況バーの [マッピング] をクリックします。

i. [注目イベントサンプルの取り込み] 列で、[添付ファイルデータをロード] をクリックします。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

j. 表示されるダイアログで、[ファイルを選択] をクリックし、エクスポートした .xml ファイルに移動して、[開く] をクリックします。
クリックして手動で転送されたイベントの添付ファイルデータをロードすると、フォームの左側に Splunk ES 注目イベントフィールドが入力されます。これらの値は、フォームの [SIR インシデントフィールドマッピング] 側のセキュリティインシデントフィールドにマッピングするフィールド値です。
イベントに対してエクスポートしたフィールドの値のペアが、マッピングフォームの左側に表示されます。

3. Splunk ES 注目イベントのインシデントレビューと貢献イベントの詳細のマッピング作成 (スケジュール済みの取り込み) セクションのステップ 5 ～ 10 に従います。

Splunk Enterprise Security 注目イベントの取り込み統合での手動イベント取り込み用の **Splunk** 環境設定

この統合用に Splunk Enterprise Security コンソールから手動でオンデマンドでイベントをエクスポートする場合は、Splunk Enterprise コンソールまたは Splunk クラウンドインスタンスに ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security アプリケーションをインストールして設定します。

始める前に
Splunk Enterprise コンソールまたは Splunk クラウンドインスタンスへの ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security アプリケーションのインストールと設定はオプションです。

手動イベントの取り込みに必要な splunkbase からのアドオンプラグインをインストールする前に、ServiceNow Store からこの統合用のアプリケーションがインストールされていることを確認してください。ServiceNow Store から統合用のアプリケーションをインストールしていない場合は、「Splunk Enterprise Security 注目イベントの取り込み統合用の ServiceNow アプリケーションのインストールと設定」を参照し、手順に従ってインストールします。

必要なロール：Splunk Enterprise Security アドミニストレーター

このタスクについて
統合用に Splunk Enterprise コンソールから手動でオンデマンドでイベントをエクスポートする場合は、ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security を Splunk Enterprise Security コンソールにインストールして設定します。この ServiceNow 拡張アドオンは、Now Platform インスタンスにある手動でエクスポートされたイベントからセキュリティインシデントを作成するために必要です。ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security アプリケーションは splunkbase で入手できます。

手動イベント転送の場合は、Splunk Enterprise Security コンソールで最大 2 つの異なる Now Platform エンドポイント (インスタンス) を特定できます。イベントをエンドポイントに手動で転送して、セキュリティインシデントを作成します。たとえば、ステージング (開発) インスタンスと本番インスタンスの両方を指定できます。個別のインスタンスを指定し、各インスタンスのプライマリおよびセカンダリワークフローに名前を付けることで、さまざまなイベントの転送先を選択できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security をまだインストールしていない場合は、次のステップに従ってインストールして設定します。

   a. splunkbase に移動します。

   b. ServiceNow セキュリティオペレーション Security Operations Event Ingestion Addon for Splunk Enterprise Security を検索します。

      注:
      ServiceNow セキュリティオペレーション Event Ingestion Addon for Splunk Enterprise Security を選択していることを確認します。このリストに表示される追加の ServiceNow アドオンがあります。これらのアドオンはさまざまな ServiceNow Splunk 統合用であり、この統合には必要ありません。

   c. アプリケーションをダウンロードします。

   d. Splunk Enterprise Security アカウントを開きます。

   e. [アプリ] ページで、メニュードロップダウンリストの歯車アイコンまたは [アプリを管理] ショートカットをクリックします。

   f. 表示される [アプリ] ページの左上で、[ファイルからアプリをインストール] をクリックします。

   g. [ファイルを選択] をクリックし、ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security を選択して、[アップロード] をクリックします。

   h. プロンプトが表示されたら、Splunk Enterprise を再起動します。
   ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security が Splunk Enterprise Security コンソールにインストールされます。次のステップでは、アドオンを設定します。

2. アドオンを設定するには、次のステップを実行します。

   a. Splunk Enterprise Security で、メニュードロップダウンリストの [アプリ] 歯車アイコンまたは [アプリを管理] をクリックします。

   b. 表示されるアプリケーションのリストの [アクション] 列で、ServiceNow セキュリティオペレーション Event Ingestion Addon for Splunk Enterprise Security の [セットアップ] をクリックします。

   c. フォームに記入します。

自動翻訳

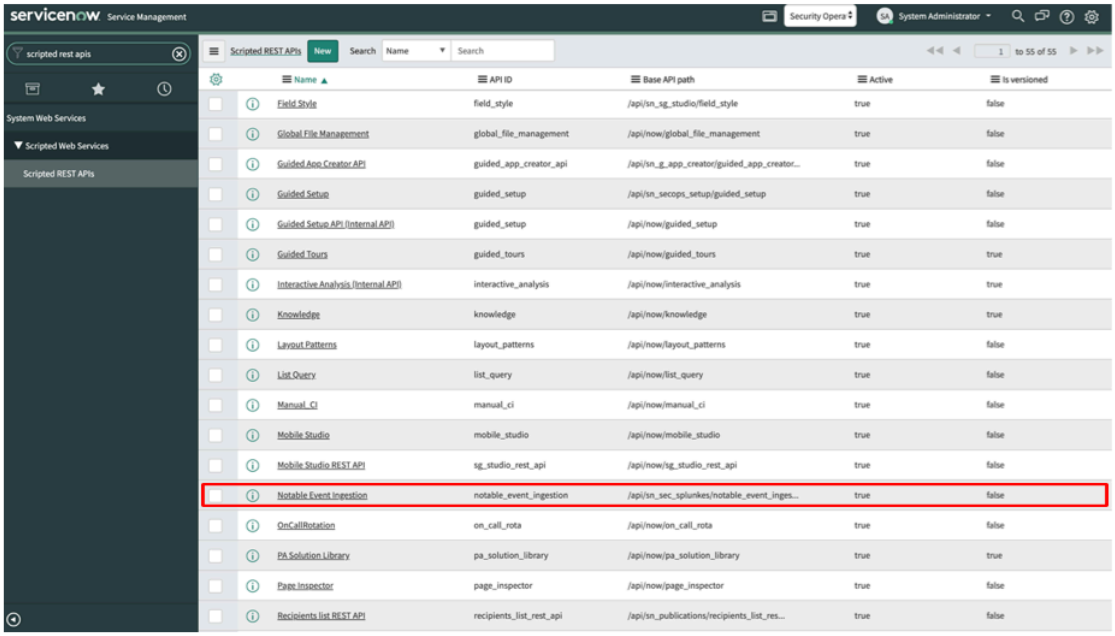
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図は、Splunk Enterprise Security コンソールの完成したフォームの例です。

次の図は、Now Platform のスクリプト済み REST API リストの例です。リストには、Splunk Enterprise Security コンソールで ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security 拡張機能の設定の一部としてフォームに入力した Now Platform インスタンスのエンドポイント値の場所が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. Splunk Enterprise Security コンソールの [セットアップ] フォームで、[保存] をクリックして編集を保存します。

   しばらくすると、Splunk Enterprise Security コンソールのフォームの左上に、レコードが正常に更新されたことを示すメッセージが表示されます。

   フォームを保存すると、フォームで作成した Now Platform インスタンスの名前 (ワークフローアクションラベル) が、Splunk Enterprise Security コンソールの検索で選択したイベントの [イベントアクション] 選択リストから使用できるようになります。

次のタスク
Splunk Enterprise Security コンソールに検索をまだ保存していない場合は、次のステップで Splunk Enterprise Security コンソールに検索をアラートとして保存します。

Splunk Enterprise Security イベントの取り込み統合でのイベントプロファイルのコピー

新しいプロファイルを作成する代わりに、既存のプロファイルとその関連設定をコピーします。複数のプロファイルを作成していて、既存のプロファイルの設定を再利用する場合は、時間を節約するためにアラームプロファイルをコピーすることをお勧めします。

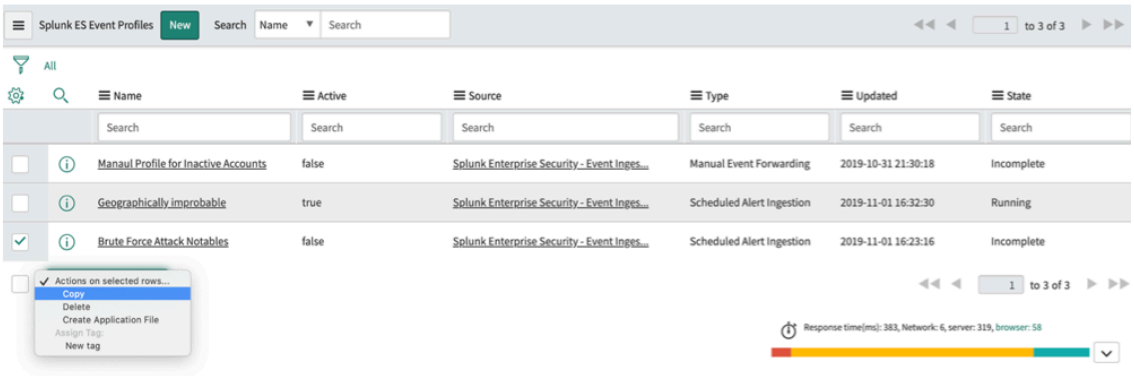
始める前に
必要なロール：sn_si.admin

このタスクについて
プロファイルをコピーすると、プロファイルの重複を避けるためにプロファイル名が最初に変更されます。また、コピーされたプロファイルは無効 (false) であるため、構成が完了する前に誤って有効になることはありません。既にプレビューおよび検証したセキュリティインシデントのプロファイルをコピーし、既存のマップを使用します。

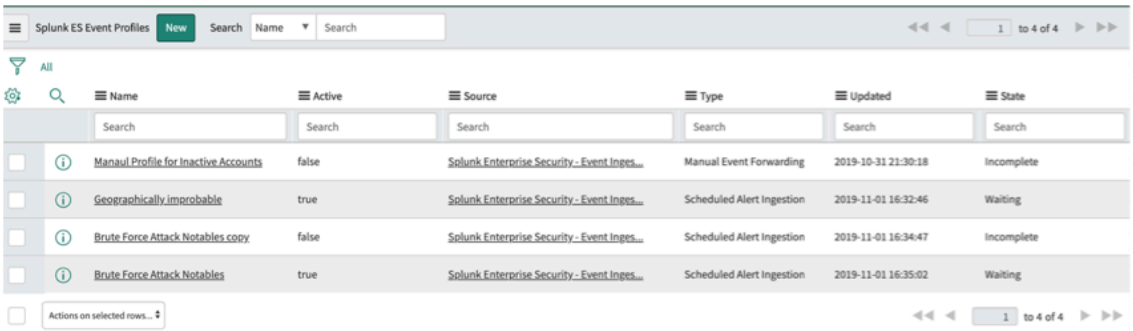
手順

1. 次のように移動する。 **All** (すべて) > **Splunk Integration** > **Splunk** イベントプロファイル.
2. 表示される [Splunk イベントプロファイル] リストでコピーするプロファイルを選択し、選択した行の [アクション] 選択リストで [コピー] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



プロファイルがコピーされ、リストに表示されます。コピーには、マッピングとスケジュール設定を含む元のプロファイルのすべての設定が含まれます。プロファイルの名前に「copy」が含まれています。元のプロファイルは有効 (true) ですが、この時点でコピーは無効 (false) になります。必要に応じて、コピーしたプロファイルの値を編集して名前を変更し、構成設定を新しいプロファイルに適用することもできます。



既存のプロファイルから新しいプロファイルに設定が正常にコピーされました。

次のタスク
構成ステップが完了すると、新しいプロファイルをアクティブ (有効) にするように求められます。

Splunk Enterprise Security イベントの取り込み統合でのスクリプトエディターを使用したアラート値のフォーマット

取り込まれた注目イベント値と手動で入力した値から直接マッピングされたフィールドに加えて、マッピングステップでスクリプトエディターを使用してセキュリティインシデントのフィールド値をフォーマットします。

始める前に
必要なロール：sn_si.admin

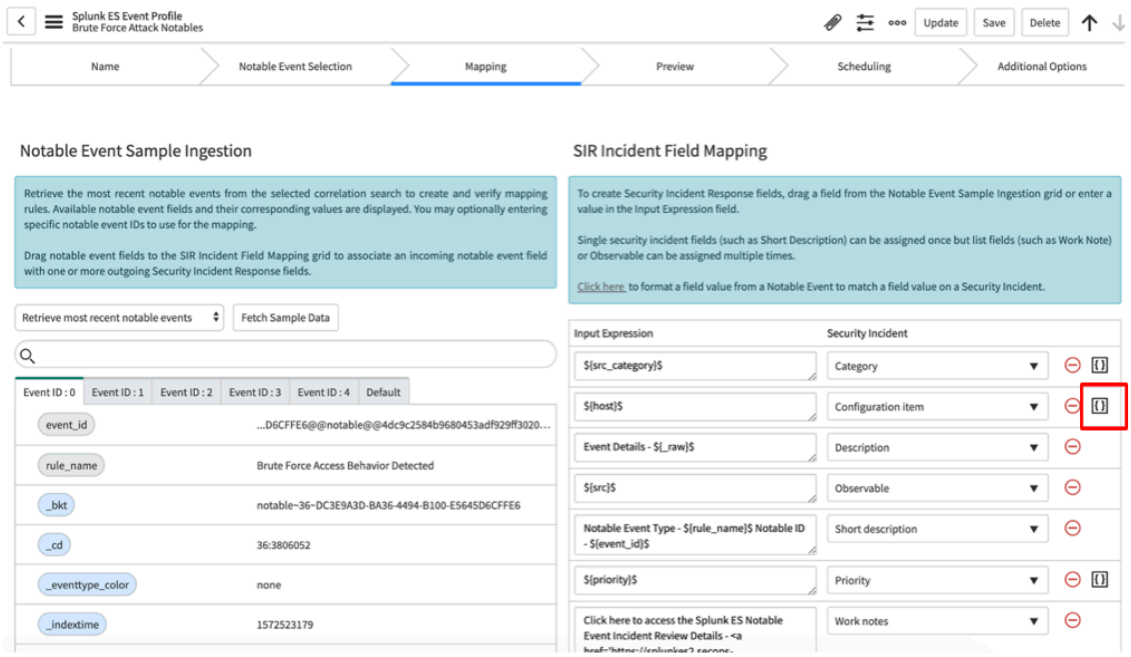
このタスクについて
場合によっては、Splunk Enterprise Security 注目イベント値は、SIR インシデントの [カテゴリ]、[構成アイテム (CI)]、および [観測事象] フィールドにマップされ、サポートされません。マッピングされた値を編集することもできます。Splunk Enterprise Security 注目イベントの値を SIR セキュリティインシデントのこれらのフィールドでサポートされている値に変換する場合は、スクリプトエディターを使用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. [マッピング] フォームを表示した状態で、リンクをクリックしてスクリプトエディターを開きます。

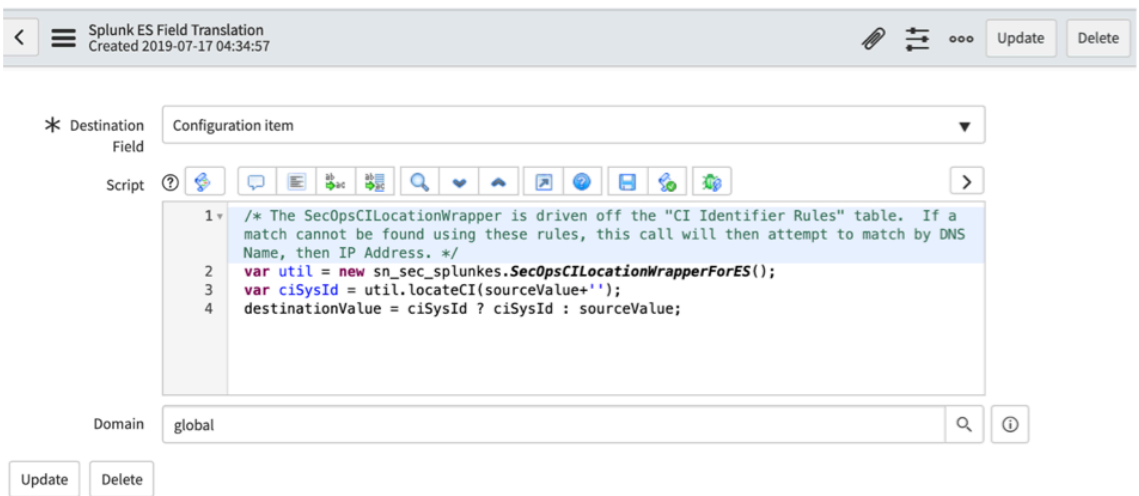


2. 選択リストから、編集する値の宛先フィールドを選択します。
3. または、[SIR インシデントフィールドマッピング] セクションで、フィールドの横にある角かっこアイコン [{}] をクリックして、そのフィールドのスクリプトエディターを開きます。

   場合によっては、 [構成アイテム] フィールドにスクリプトインクルードが適している場合があります。たとえば、注目イベントの場合、構成アイテムの値が一致しない可能性があります。

   次の図に示すように、[構成アイテム] フィールドの Now Platform® CMDB で一致するホスト名が見つからない場合は、IP アドレスが見つかった場合に [構成アイテム] フィールドに入力されるようにルールを編集できます。アラームの値がない場合、セキュリティインシデントのフィールドは null に設定されます。

   エディターが開き、[宛先フィールド] にフィールドが表示されます。次の画像は、[構成アイテム] フィールドを [宛先フィールド] に設定したエディターを示しています。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

4. スクリプトに変更を入力し、[更新] をクリックして変更を保存します。
   [Splunk フィールド変換] テーブルが表示されます。
5. テーブルを閉じて [マッピング] フォームに戻ります。

エクスポート/インポート機能を使用した **Splunk Enterprise Security** プロファイルのインスタンス間でのコピー

Splunk Enterprise Security プロファイル設定を 1 つの Now Platform インスタンスから別の Now Platform インスタンスにエクスポートおよびインポートできます。

始める前に

エクスポートおよびインポートできる設定には、プロファイル名、相関ルール、マッピング、フィルター、集計基準、フィールド変換、フェッチされたサンプルデータ、スケジュール、および構成タイルソース情報が含まれます。

必要なロール：sn_si.admin

このタスクについて

この機能により、セキュリティアドミニストレーターは、ある Now Platform インスタンス (非本番など) でテストおよび検証されたプロファイルを、別の Now Platform インスタンス (本番など) にコピーできます。すべての構成設定をやり直す必要はありません。エクスポートおよびインポートされる設定には、プロファイル名、相関ルール、マッピング、フィルター、集計基準、フィールド変換、フェッチされたサンプルデータ、スケジュール、および構成タイルソース情報が含まれます。

> **注:**
> 手動イベント転送プロファイルタイプをエクスポートすると、サンプルフィールドマッピングに使用される添付ファイルデータはコピーされますが、添付ファイル自体はエクスポートされません。

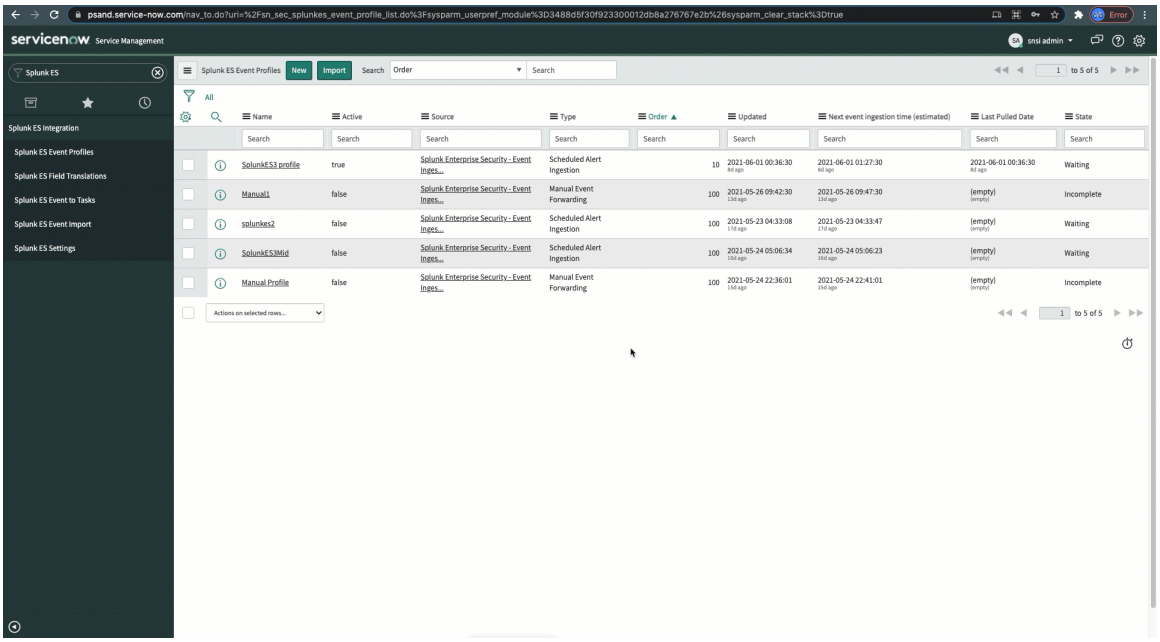
手順

1. 次のように移動する。 **All** (すべて) > **Splunk ES** 統合 > **Splunk ES** イベントプロファイル.
2. 別の Now Platform インスタンスにエクスポートするプロファイルを選択します。
   エクスポートするプロファイルは複数選択できます。
3. [アクション] メニューから、[エクスポート] をクリックします。
4. エクスポート完了メッセージが表示されたら、[ダウンロード] をクリックします。

   次の図は、Now Platform インスタンス (psand.service-now.com) からプロファイル (SplunkES3profile) をエクスポートする方法を示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



エクスポートされた payload.xml ファイルがコンピューターにダウンロードされます。ファイルには、プロファイル名、相関ルール、マッピング、フィルター、集計基準、フィールド変換、フェッチされたサンプルデータ、スケジュール、および構成タイルソース情報が含まれます。複数のプロファイルを選択してダウンロードすると、同じ payload.xml ファイルに表示されます。

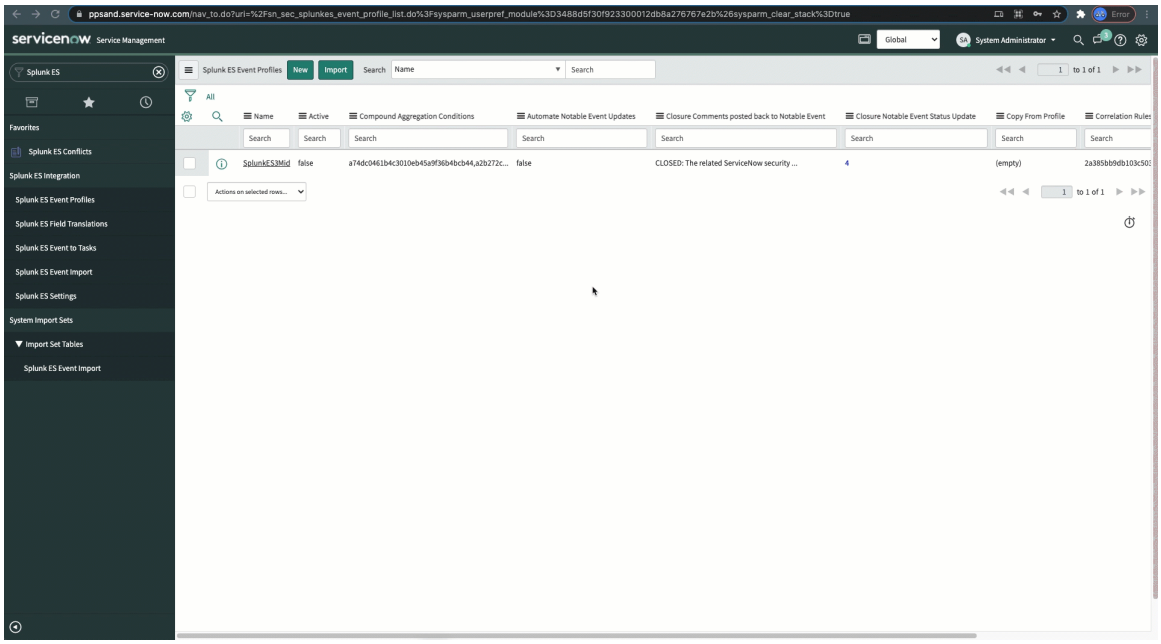
これで、別の Now Platform インスタンスでプロファイルをインポートできます。

5. 次のように移動する。 **Splunk ES** 統合 > **Splunk ES** イベントプロファイル.
6. [インポート] をクリックします。
7. [ファイルを選択] をクリックし、コンピューターで XML ファイルを選択します。
8. [アップロード] をクリックします。
9. [プロファイルを閉じてリロード] をクリックします。

次の図は、Now Platform インスタンス (psand.service-now.com) からプロファイル (SplunkES3profile) を Now Platform インスタンス (ppsand.service-now.com) にインポートする方法を示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



別の Now Platform インスタンスからプロファイルが正常にインポートされました。

エクスポートされたソース (Splunk API アカウントと Splunk サーバー URL) と MID サーバー構成設定が有効で、インポートされた Now Platform インスタンスで使用できることを確認します。必要に応じて Splunk Enterprise Security 構成を更新します。

10. オプション: プロファイルをインポートした後、MID サーバーの設定を確認します。
11. オプション: 次のように移動する。 セキュリティオペレーション > 統合設定.
12. オプション: Splunk Enterprise Security 構成タイルを選択し、[更新] をクリックします。
13. オプション: ソースおよび MID サーバーの詳細を確認し、必要に応じて更新します。

Splunk Enterprise Security 注目イベントの取り込み統合用チェックリスト

このチェックリストを使用して、統合のすべてのタスクをガイドします。次のチェックリストには、セットアップとインストールのタスク、および統合の予想される結果を含むユースケースの例が含まれています。

始める前に

必要なロール：admin、sn_si.admin、sn_si.analyst、Splunk Enterprise Security アドミン

このタスクについて

次のテーブルを使用して、統合のセットアップ、インストール、および構成の進捗状況を追跡します。次のステップに進む前に、ステップのすべてのタスクを完了してください。テーブルの各行にタスクがリストされており、タスクの実行に必要なロールが特定されています。インストールおよび構成ガイドの番号付けされたトピックも参照されます。

各タスクに必要なロールは次のテーブルでステップごとにリストされています。

手順

1. 統合のセットアップ、インストール、および構成の進捗状況を追跡します。
   次のステップに進む前に、ステップのすべてのタスクを完了してください。
2. テーブル内のステップを記載されている順に実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト

☐	Now Platform アドミンロールを持つユーザーとして、Now Platform インスタンスを設定します。 ○ 必要に応じて、sn_si.admin ロールと sn_si.analyst ロールをユーザーにアサインします。 ○ Splunk サーバーが企業ネットワーク内に展開されている場合は、MID サーバーをインストールして構成します。 ○ ServiceNow セキュリティインシデントレスポンス プラグインが Now Platform のリリースに対して有効になっていることを確認します。 ○ (オプション) Splunk Enterprise Security コンソールから Now Platform インスタンスに手動でイベントを転送する場合は、Splunk Enterprise Security アドミン権限を持つユーザーに (sn_sec_splunkes.api_account_access) ロールが割り当てられていることを確認します。 詳細については、「Splunk Enterprise Security 統合での Now Platform インスタンスの設定」を参照してください。
☐	Now Platform アドミンロールを持つユーザーとして、ServiceNow Store から Splunk Enterprise Security アプリケーションをインストールして設定します。 **a.** Now Platform インスタンスにアプリケーションがダウンロードされ、インストールされます。 **b.** アプリケーションを設定し、Splunk Enterprise Security コンソールに接続します。 詳細については、「Splunk Enterprise Security 注目イベントの取り込み統合用の ServiceNow アプリケーションのインストールと設定」を参照してください。
☐	(オプション) Splunk Enterprise Security コンソールから Now Platform インスタンスにイベントを手動でエクスポートする場合は、次のタスクを実行します。 ○ Splunk Enterprise Security アドミニストレーターは、Splunk Enterprise Security コンソールで splunkbase から ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security をインストールして設定し、有効にします。 ○ Splunk Enterprise Security アドミニストレーターとして、まだ設定されていない場合は、Splunk Enterprise Security コンソールに検索を注目イベントとして保存します。 詳細については、「Splunk Enterprise Security 注目イベントの取り込み統合での手動イベント取り込み用の Splunk 環境設定」を参照してください。
☐	Now Platform sn_si.admin ロールを持つユーザーとして、イベントプロファイルを作成して名前を付けます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

	選択リストからプロファイルタイプを選択します。オプションは、サンプルデータを取り込むために使用するスケジュール済みアラートプロファイル、または Splunk Enterprise Security コンソールから手動で添付ファイルデータをエクスポートするために使用するイベントプロファイルです。 ○ スケジュール済みアラートの場合は、利用可能なアラートを選択します。 ○ 手動でエクスポートされたデータのプロファイルの場合は、新しいマップを作成するか、既存のマップをコピーします。 詳細については、「Splunk Enterprise Security イベントの取り込み統合でのイベントプロファイルの作成と名前の設定」を参照してください。
☐	Now Platform sn_si.admin ロールを持つユーザーとして、取り込まれた値またはエクスポートされた添付ファイルデータを Splunk Enterprise Security から Now Platform セキュリティインシデントにマップします。 **a.** スケジュール済みアラートのサンプルデータをフェッチします。 **b.** (オプション) Splunk Enterprise Security から手動でイベントの 添付ファイルデータをエクスポートします。 **c.** デフォルトのマッピング構成を編集します。 **d.** 必要に応じて、フィルター条件を追加し、既存のセキュリティインシデントにアラートを追加し、スクリプトエディターを使用します。 詳細については、「Splunk Enterprise Security 統合での注目イベントフィールドのマッピング」と「Splunk ES 注目イベントのインシデントレビューと貢献イベントの詳細のマッピング作成 (スケジュール済みの取り込み)」を参照してください。
☐	○ Now Platform sn_si.admin ロールを持つユーザーとして、Now Platform セキュリティインシデントに表示される Splunk Enterprise のデータをプレビューします。 ○ エラーを修正するか、不足しているデータを追加して、エラーメッセージが表示されないようにします。 詳細については、「Splunk Enterprise Security イベントの取り込み統合のセキュリティインシデントをプレビューする」を参照してください。
☐	Now Platform sn_si.admin ロールを持つユーザーとして、スケジュール済みアラートを使用してプロファイルのアラート取得をスケジュールします。 詳細については、「Splunk Enterprise Security イベントの取り込み統合での新規および更新された注目イベントのスケジュール設定と取得」を参照してください。

これでセットアップ手順を完了し、統合に期待される結果を検証できました。

Splunk - インシデント拡張統合

Splunk - インシデント拡張統合はログを検索し、関連するサイティング情報をセキュリティインシデントに追加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

探索	セットアップ
セキュリティインシデントレスポンス統合	Splunk Search Integration for セキュリティオペレーション の開始

使用	開発
• サイティング検索の実行 • Security Operations Integration - サイティング検索フロー • Security Operations Integration - Splunk サイティング検索フロー • サイティング検索の詳細の表示 • サイティング検索結果の表示	• ServiceNow セキュリティオペレーション 統合開発のガイドライン • 統合を作成するためのヒント • 開発者トレーニング • 開発者ドキュメント • アプリケーションとともにインストールされているコンポーネントの検索

トラブルシューティングと追加情報

- 統合のトラブルシューティング
- Security Operations Community で質問や回答をする
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

自動翻訳

Splunk Search Integration for セキュリティオペレーション の開始

Splunk ソフトウェアは、マシンで生成されたビッグデータを検索、監視、および分析し、セキュリティオペレーション と簡単に統合できます。Splunk - インシデント拡張統合を使用する前に、ServiceNow Store から統合をダウンロードし、適切な API Base URL とログイン認証情報を追加する必要があります。

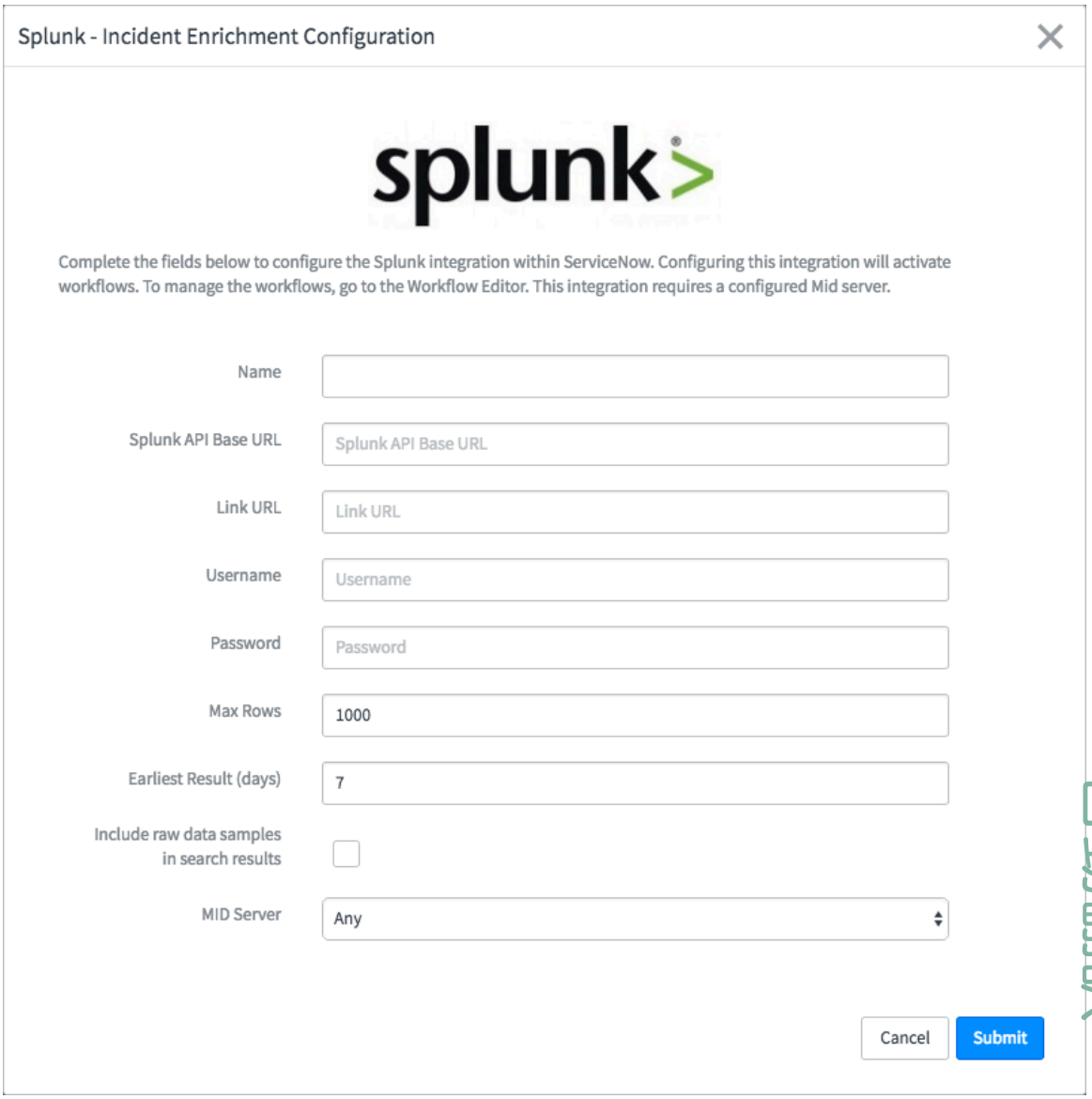
始める前に

必要なロール：sn_si_admin

手順

1. から統合をダウンロードします ServiceNow Store.
2. インストールが完了したら、Splunk にアクセスし、プロファイルの下の API キーと API ID を取得します。
3. インスタンスで、 セキュリティオペレーション > 統合設定.
   利用可能なセキュリティ統合が一連のカードとして表示されます。
4. Splunk - インシデント拡張カードで、[新規] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

5. 必要に応じて、フィールドに入力します。

フィールド	説明
名前	この構成の名前。
Splunk API のベース URL	Splunk サイトから取得したベース URL。
リンク URL	[オプション] Splunk Web インターフェイスにリンクするリンク URL (利用可能な場合)。
ユーザー名	Splunk ユーザー名。
パスワード	Splunk パスワード。
最大行数	検索する行の最大行数。
最も早い結果 (日数)	表示する最も早い結果 (日数単位)。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
検索結果に生データサンプルを含める	サイティング検索結果に生データのサンプルを含めるには、これを選択します。返されるデータの量は、[セキュリティインシデントレスポンス] プロパティの [生データの行数] プロパティの設定によって異なります。
MID サーバー	[任意] を選択して、 任意のアクティブな MID サーバーを使用するか、特定の MID サーバー名を選択します。

注:
この統合を設定すると、ワークフローが有効になります。ワークフローを管理するには、[ワークフローエディター] に移動します。

6. **[Submit]** をクリックします。
統合構成カードが表示されます。
7. 新しい構成カードを表示すると、[構成] または [削除] をクリックして、構成を変更または削除できます。
8. 統合構成カードの元のリストに戻るには、[構成を表示] ドロップダウンから [いいえ] を選択します。

セキュリティインシデントレスポンス のモバイルエクスペリエンス

Android または iOS モバイルデバイスを使用して、Security Operations Center (SOC) タスクを管理します。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

セキュリティインシデントレスポンス

Now Platform® インスタンスの セキュリティインシデントレスポンス (SIR) 製品の基本的な概念を理解していない場合は、「セキュリティインシデントレスポンス の概要」を参照して、脅威インテリジェンスの詳細と、この製品が組織に対するサイバー脅威の優先順位付けと解決にどのように役立つかを確認してください。

概要

Security Operations Center (SOC) マネージャーまたは Now Platform セキュリティアナリスト ロール (sn_si.analyst) を持つユーザーは、モバイルデバイスから Now Platform インスタンスに直接ログインできます。セキュリティインシデントレスポンスモバイルアプリ では、最新および重大な SIR セキュリティインシデントと応答タスクを表示、編集、およびアサインすることができます。Notifications で、自分に割り当てられた重大なセキュリティインシデントが到着したときに通知されます。

セキュリティインシデントレスポンスモバイルアプリ を使用すると、モバイルデバイスから次の SIR 関連のタスクを実行できます。

- 重大なセキュリティインシデントと応答タスクのリストを表示する。
- 事前定義された通知基準を満たすセキュリティインシデントとタスクの詳細な通知を受信する。
- 事前定義されたクエリまたはフィルターのセットに基づくセキュリティインシデントまたはタスクのグループを表示する。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- セキュリティインシデントの作業メモと関連リストを表示する。
- セキュリティインシデントを更新し、作業メモまたは添付ファイルを追加する。
- セキュリティインシデントのフィールドを編集する。
- 自分またはセキュリティチームの他のメンバーにセキュリティインシデントをアサインする。

設定されている場合、セキュリティインシデントレスポンスモバイルアプリ を使用して、SIR セキュリティインシデントの次の関連リストを表示できます。

- 構成アイテム
- 影響を受けるユーザー
- 影響を受けるサービス
- 子セキュリティインシデント
- 類似のセキュリティインシデント (Now Platform ではサポートされません)
- 観測事象
- 応答タスク
- タスク
- タスク SLA
- 添付ファイル (Now Platform ではサポートされません)

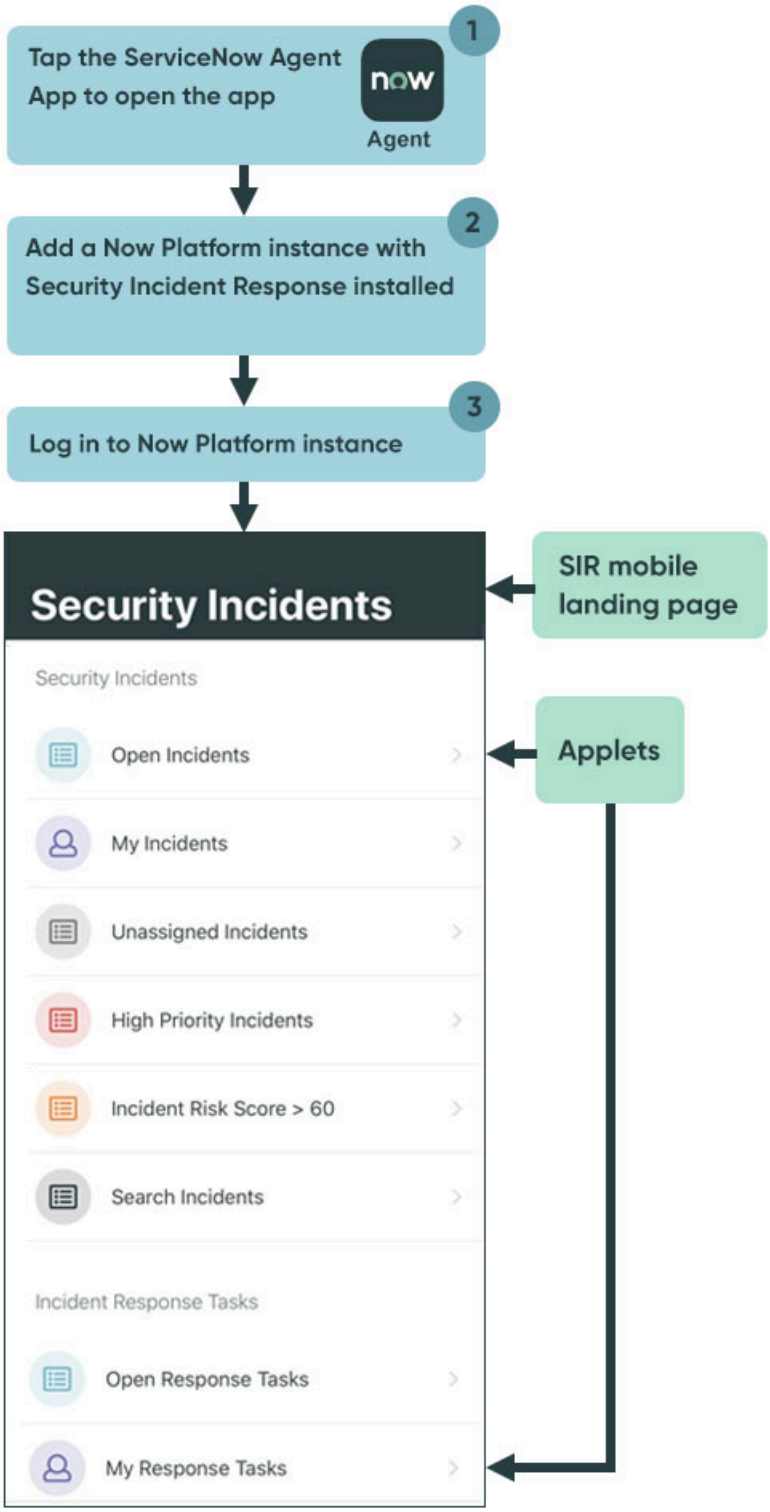
次の図は、モバイルデバイスから Now Platform インスタンスにログインする方法と、ログイン後に表示される セキュリティインシデントレスポンスモバイルアプリのランディング画面の構造を示しています。

Now Platform インスタンスを設定し、セキュリティインシデントレスポンスモバイルアプリ をインストールする方法の詳細な手順については、「セキュリティインシデントレスポンスモバイルアプリ のチェックリストをセットアップ」を参照してください。ログイン方法については、「セキュリティインシデントレスポンスモバイルアプリ へのログイン」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンスモバイルアプリ



アプリケーション

アプリケーションとは、Now Platform インスタンス内で特定の機能を提供する、セキュリティインシデントレスポンス (SIR)、脆弱性対応 (VR)、ガバナンス、リスク、コンプライアンス (GRC) などの ServiceNow　ソフトウェアコンポーネントです。セキュリティインシデントレスポンス コアアプリケーションと セキュリティインシデントレスポンスモバイルアプリ を Now Platform インスタンスにインストールした後、ログインすると、Android または iOS モバイルデバイスの下部にコアアプリケーションのアイコンが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンスモバイルアプリ (セキュリティインシデント) アイコン

フォルダー

各 ServiceNow® モバイル アプリケーションには、カテゴリ別にアプレットを分離するフォルダーが含まれています。前のランディングページの画像では、[セキュリティインシデント] と [インシデント応答タスク] がフォルダーです。

アプレット

アプレットは、アプリケーション内のさまざまなオプションです。[セキュリティインシデント] セクションと [インシデント応答タスク] セクションの下にあるアイコンは、セキュリティインシデントレスポンスモバイルアプリ で使用可能なアプレットです。

セキュリティインシデントレスポンスモバイルアプリ® のチェックリストをセットアップ

次のチェックリストには、Now Platform® インスタンスおよびモバイルデバイスで セキュリティインシデントレスポンスモバイルアプリを使用する前に完了する必要があるセットアップタスクが含まれています。

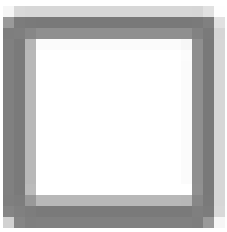
始める前に

オプションとして、このチェックリストを印刷し、セキュリティインシデントレスポンスモバイルアプリで必要な設定タスク全体のガイドとして使用します。モバイルデバイスで SIR セキュリティインシデントを表示および編集できるように、リストの各アイテムが完了していることを確認します。

チェックリストのアイテムは、ハイライト表示されたテキストで表示されます。右側の列の各アイテムの後に詳細情報が表示されます。このタスクの完了までの推定時間：15 ～ 20 分。

必要なロール：admin、sn_si.analyst

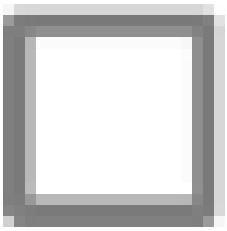
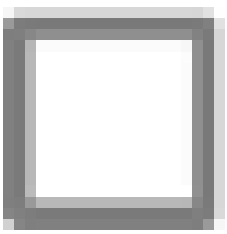
モバイルチェックリスト

アイテム	説明
	admin ロールを持つユーザーは、セキュリティインシデントレスポンス コアアプリケーションが Now Platform インスタンスにインストールされていることを確認します。これは、モバイルデバイスで表示する Now Platform インスタンスです。 **注:** セキュリティインシデントレスポンス コアアプリケーションと Now Platform インスタンスは、ファミリーリリースが同じである必要があります。 1. コアアプリケーションがインスタンスにインストールされていることを確認するには、[プラグイン] に移動して、セキュリティインシデントレスポンスを検索します。 2. セキュリティインシデントレスポンス コアアプリケーションがまだインストールされていない場合は、[インストール] をクリックして、インストールします。 セキュリティインシデントレスポンス コアアプリケーションのインストールの詳細については、「セキュリティインシデントレスポンス のインストールと構成」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モバイルチェックリスト (続く)

アイテム	説明
	セキュリティインシデントレスポンス コアアプリケーションがプラグインに表示されない場合、コアアプリケーションのインストールとアプリケーションに対するエンタイトルメントの詳細については、「セキュリティオペレーションおよび ServiceNow Store」を参照してください。
	admin ロールを持つユーザーは、モバイルデバイスで表示する Now Platform インスタンスに セキュリティインシデントレスポンスモバイルアプリ がインストールされていることを確認します。 **注:** セキュリティインシデントレスポンスモバイルアプリ と Now Platform インスタンスは、ファミリリリースが同じである必要があります。 ServiceNow Store から セキュリティインシデントレスポンスモバイルアプリ をダウンロードして、Now Platform インスタンスにインストールします。 セキュリティインシデントレスポンスモバイルアプリ をインストールすると、その依存関係である com.glide.sg および com.glide.sg.agent_native_client もインストールされます。 これらの依存関係がインストールされていることを確認するには： **1.** [プラグイン] に移動します。 **2.** プラグイン ID (com.glide.sg および com.glide.sg.agent_native_client) を検索します。 **3.** アクティブ化されていない場合は、これらのプラグインをアクティブ化します。これらのプラグインは セキュリティインシデントレスポンスモバイルアプリ に必要です。 アプリケーションのインストールとアプリケーションに対するエンタイトルメントの詳細については、「セキュリティオペレーション および ServiceNow Store」を参照してください。
	Now Platform admin ロールを持つユーザーは、Now Platform インスタンスで、モバイルユーザーに必要なロールをアサインしたことを確認します。 **1.** ユーザーにアサインされているロールを表示するには、次に移動します: ユーザーとグループ > ユーザー. **2.** ユーザー名、続いてロール関連リストを選択します。このユーザーにアサインされているすべてのロールが表示されます。 **3.** ユーザーがアサインされていることを確認するか、IT インフラストラクチャライブラリロール (itil) を持つユーザーをアサインします。itil ロールを持つユーザーは、セキュリティインシデントを作成、オープン、更新、およびクローズできます。itil ロールを持つユーザーのみにタスクをアサインすることができます。 **4.** ユーザーがアサインされていることを確認するか、セキュリティアナリストロール (sn_si.analyst) を持つユーザーをアサインします。sn_si.analyst ロールを持つユーザーは、セキュリティインシデントレコードの読み取りと編集ができます。このロールは、itil ロールをアサインすると自動的に追加されます。 **5.** 必要なアサイン先グループを作成し、こうしたグループにモバイルユーザーをアサインしたことを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モバイルチェックリスト (続く)

アイテム	説明
	注: モバイルアプリケーションに多数のユーザーがいる場合は、sn_si.analyst ロールをグループにアサインすることもできます。グループに追加する各ユーザーは、このロールを継承します。 セキュリティアナリストの詳細については、「セキュリティアナリストのアサイン」を参照してください。 ユーザーの詳細、およびユーザーとグループへのロールのアサインの詳細については、「ユーザー管理」を参照してください。
☐	sn_si.analyst ロールを持つユーザーは、モバイルデバイスで最新の ServiceNow Agent アプリをダウンロードしてインストールします。 最新バージョンの Agent アプリは、Apple iOS App Store と Google Play ストアで入手できます。
☐	sn_si.analyst ロールを持つユーザーは、モバイルデバイスと Now Platform インスタンスで通知が有効になっていることを確認します。 重要なセキュリティインシデントが自分または自分のアサイン先グループにアサインされると、通知によって知らされます。タイムリーな修復を支援するには、通知を有効にした後、セキュリティインシデントレスポンスモバイルアプリ 内の通知をクリックしてセキュリティインシデントに直接移動します。 Now Platform インスタンスで通知を有効にしてモバイルデバイスに表示されるようにするには、次の手順を実行します。 **1.** セキュリティインシデントレスポンスモバイルアプリ を Now Platform インスタンスにダウンロードしてインストールしたことを確認します。 **2.** Now Platform インスタンスの [システムの設定] の [通知] で、**ServiceNow Mobile** アプリケーションが有効になっていることを確認します。 通知の設定の詳細については、「Setting user notification preferences in Core UI (コア UI のユーザー通知設定の設定)」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モバイルチェックリスト (続く)

アイテム	説明
	Now Platform の通知は、モバイルデバイスのメッセージ画面にも表示されます。モバイルデバイスの設定でも通知が有効になっていることを確認します。

モバイルデバイスと、セキュリティインシデントレスポンスモバイルアプリ 用の Now Platform が正常に設定されました。次のステップでは、モバイルデバイスで Now Platform インスタンスにログインします。

セキュリティインシデントレスポンスモバイルアプリ へのログイン

セキュリティインシデントレスポンスモバイルアプリを開き、セキュリティインシデントレスポンスを含む Now Platform インスタンスをモバイルデバイスに追加します。

始める前に

必要なロール：sn_si.analyst

このタスクについて

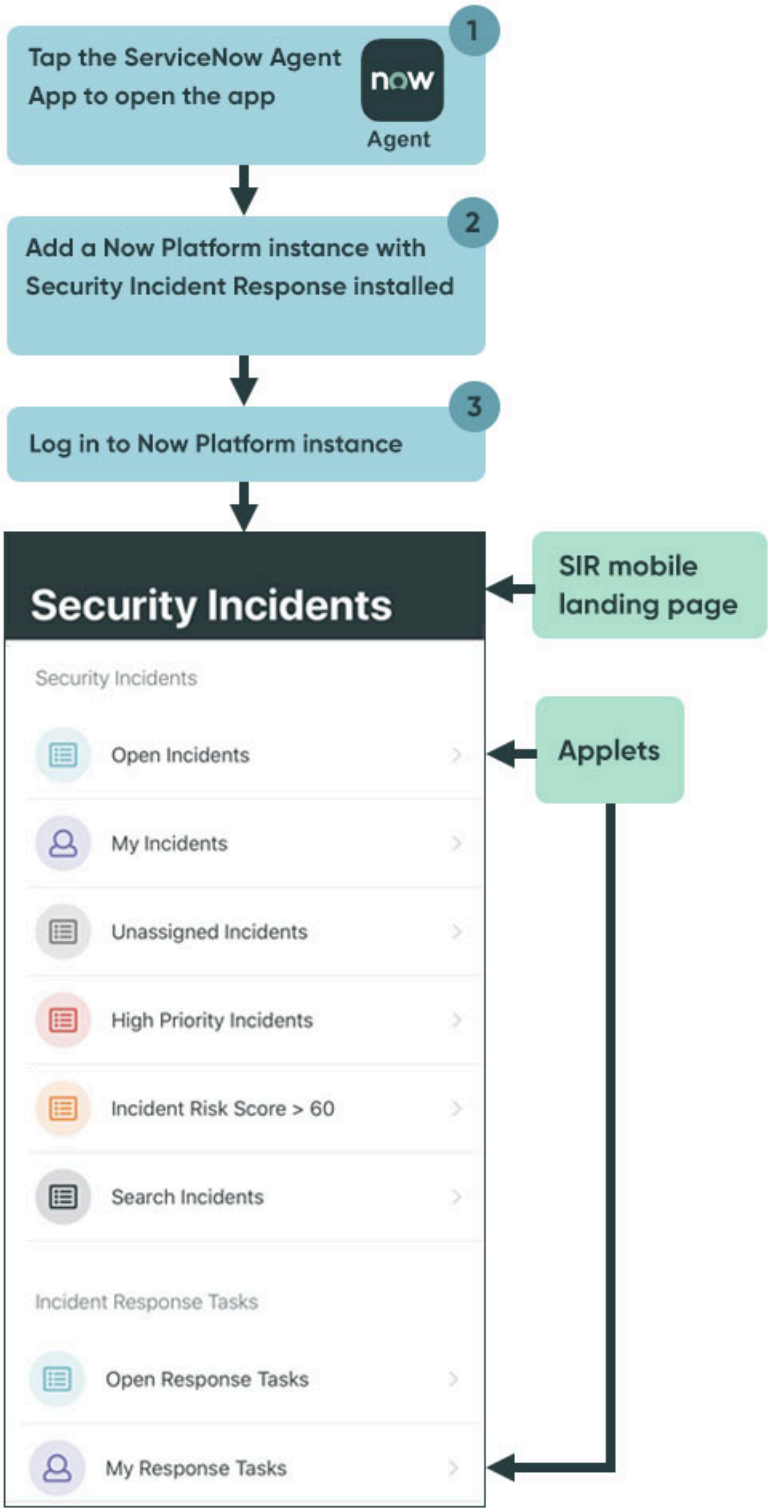
このタスクの完了にかかる時間：5 ～ 10 分。

「セキュリティインシデントレスポンスモバイルアプリ のチェックリストをセットアップ」で説明されているセットアップ手順を完了していることを確認します。

自動翻訳

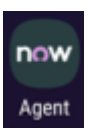
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントレスポンスモバイルアプリ



手順

1. モバイルデバイスで、**ServiceNow** エージェントアプリをタップして開きます。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Now Platform インスタンスにまだログインしていない場合は、 [インスタンス] 画面が表示されます。

2. セキュリティインシデントレスポンス コアアプリケーションを含む Now Platform インスタンスがまだモバイルデバイスに追加されていない場合は、次の手順に従って追加します。

   a. 表示される [インスタンス] 画面で、 をタップします。
   Now Platform インスタンスのアドレスを入力して保存するように求める画面が表示されます。

   b. フィールドに入力します。

フィールド	説明
インスタンスアドレスを入力するか、QR コードをスキャンしてください。	1 つ選択して続行します。 ▪ .service-now.com の前に、Now Platform インスタンスの名前 (例：sirmobileny) を入力します。 ▪ アドレスを入力します。これは、モバイルデバイスで表示する Now Platform インスタンスの URL のアドレスです (例：https://sirmobileny.service-now.com)。 ▪ QR コードをスキャンします。
(オプション) ニックネームを入力	このインスタンスのニックネームを入力します。デバイスに複数のインスタンスが存在する場合、ニックネームを使用することで、Now Platform のインスタンスをすばやく見つけることができます。

   c. [保存してログイン **(Save and Login)]** をタップします。

3. 表示される ServiceNow ログイン画面で、追加する Now Platform インスタンスの [ユーザー名] と [パスワード] を入力し、[ログイン] をタップします。
   セキュリティインシデントのランディング画面が表示されます。セキュリティインシデントレスポンスモバイルアプリ に正常にログインしました。
4. ログイン後、セキュリティインシデントレスポンスモバイルアプリ で通知が有効になっていることを確認します。

   a. 下部のランディング画面で、[通知] をタップします。

   b. [通知] 画面で、[通知を有効にします] をタップします。
   Now Platform からの通知は、セキュリティインシデントレスポンスモバイルアプリ の [通知] 画面に表示されます。

5. モバイルデバイスでインスタンスにログインすると、そのインスタンスがデバイスのデフォルトの Now Platform インスタンスになります。
   デバイス上の別の Now Platform を表示するには、デフォルトのインスタンスからログアウトする必要があります。ログアウトするには：

   a. [設定] アイコンをタップします。

   b. [ログアウト] をタップします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[インスタンス] 画面に、モバイルデバイスに追加した Now Platform インスタンスが表示されます。

c. オプション: 別のインスタンスをタップしてログインするか、前の手順に従って別のインスタンスを追加します。

デバイスで **[ServiceNow** エージェント] アプリをタップした後に セキュリティインシデントレスポンスモバイルアプリ のインスタンス画面が表示されない場合は、デバイスで **[ServiceNow** エージェント] が信頼できるアプリとして許可されていることを確認してください。信頼できるアプリとしてのアクセスを許可するには、デバイスの [設定] および [一般的なデバイス管理] に移動し、オプション ([アプリを信頼 (Trust app)] など) をタップしてアクセスを許可します。

ログイン画面に認証情報を入力した後にエラーメッセージが表示された場合は、Now Platform インスタンスのユーザー名とパスワードが正しいことを確認してください。

ランディング画面の表示に問題がある場合は、ネットワーク接続を確認してください。

ServiceNow エージェントアプリをタップしても [インスタンス] 画面を表示できない場合は、デバイスからアンインストールしてください。Apple iOS App Store または Google Play ストアから最新バージョンのアプリを入手して、再インストールしてみてください。

セキュリティインシデントレスポンスモバイルアプリ でのオープンセキュリティインシデントの表示、編集、およびアサイン

セキュリティインシデントアナリストは、オープン中の セキュリティインシデントレスポンス (SIR) セキュリティインシデントをモバイルデバイスから表示、編集、およびアサインできます。インシデントの詳細については、関連リストおよび作業メモの監査記録を参照してください。

始める前に

必要なロール：sn_si.analyst

このタスクについて

レコードのリストから、オープンセキュリティインシデントを自分にアサインするか、再アサインします。または、アサインの前にレコードの詳細と関連リストを表示するか、作業メモを追加します。このタスクの完了にかかる時間：5 ～ 10 分。

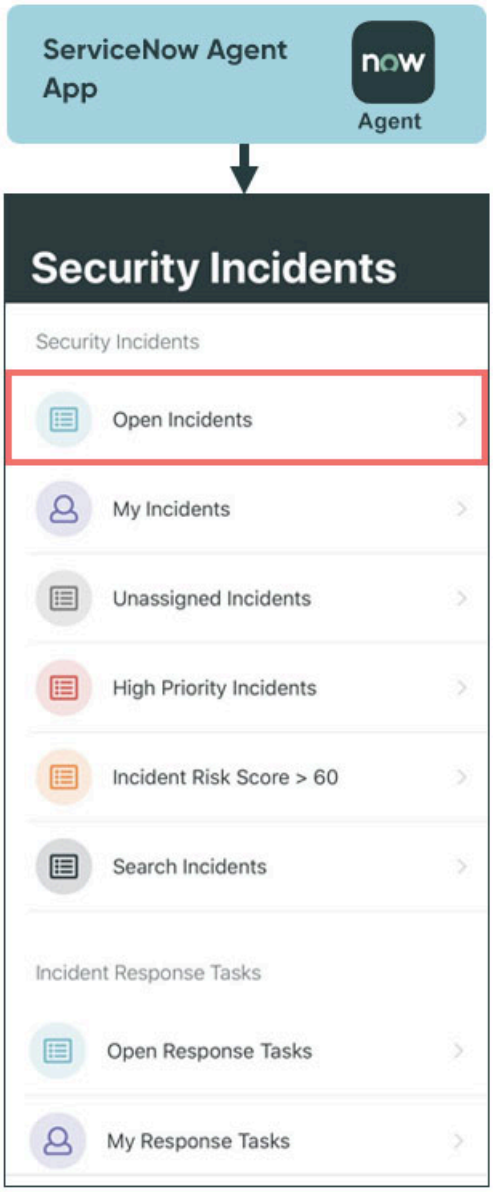
手順

1. モバイルデバイスで Now Platform インスタンスにログインしていない場合は、「セキュリティインシデントレスポンスモバイルアプリ へのログイン」を参照してください。
2. [セキュリティインシデント] ランディング画面を表示して、[オープン中のインシデント] をタップします。

   ログイン後に セキュリティインシデントレスポンスモバイルアプリ から移動した場合は、Now Agent アプリをタップすると、いつでも最後に表示していた画面に戻ります。

自動翻訳

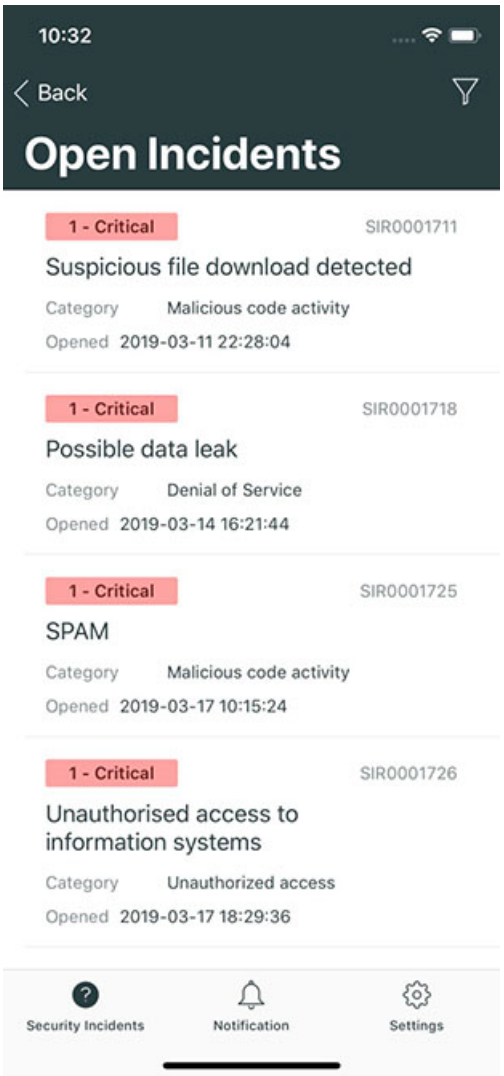
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[オープン中のインシデント] 画面に、オープンセキュリティインシデントレコードのリストが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

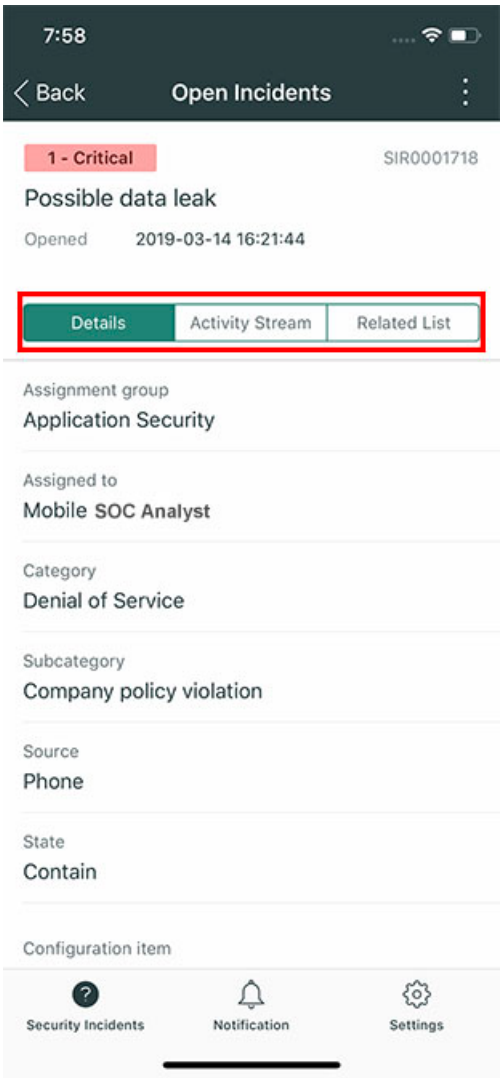


自動翻訳

3. オプション: 特定の基準に一致するセキュリティインシデントを検索するには、「セキュリティインシデントレスポンスモバイルアプリ でのセキュリティインシデントの検索」を参照してください。

   または、表示されているフィルターアイコン ( ) を使用して、リストのレコード数を制限するフィルターを設定します。モバイルアプリの画面でのレコードのフィルタリングは、Now Platform で条件ビルダーを使用したフィルタリングと同様に機能します。
4. オープンセキュリティインシデントのリストから直接インシデントを自分にアサインするか、再アサインするには、レコードを左にスワイプしてメニューを開きます。
5. 表示されるメニューでいずれかを選択して、続行します。
6. または、オープンセキュリティインシデントレコードの詳細を表示し、関連付けられたレコードと関連リストをさらに表示するには、[オープン中のインシデント] 画面を表示して、リスト上のレコードをタップします。
7. 表示されるオープンレコードで、次の表のいずれかのオプションを選択して続行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

セキュリティインシデントレスポンスモバイルアプリ で自分にアサインされたセキュリティインシデントの表示、編集、および再アサイン

セキュリティインシデントアナリストは、自分にアサインされた セキュリティインシデントレスポンス (SIR) インシデントを表示、編集、および再アサインします。インシデントの詳細については、関連リストおよび作業メモの監査記録を参照してください。

始める前に

必要なロール：sn_si.analyst

このタスクについて

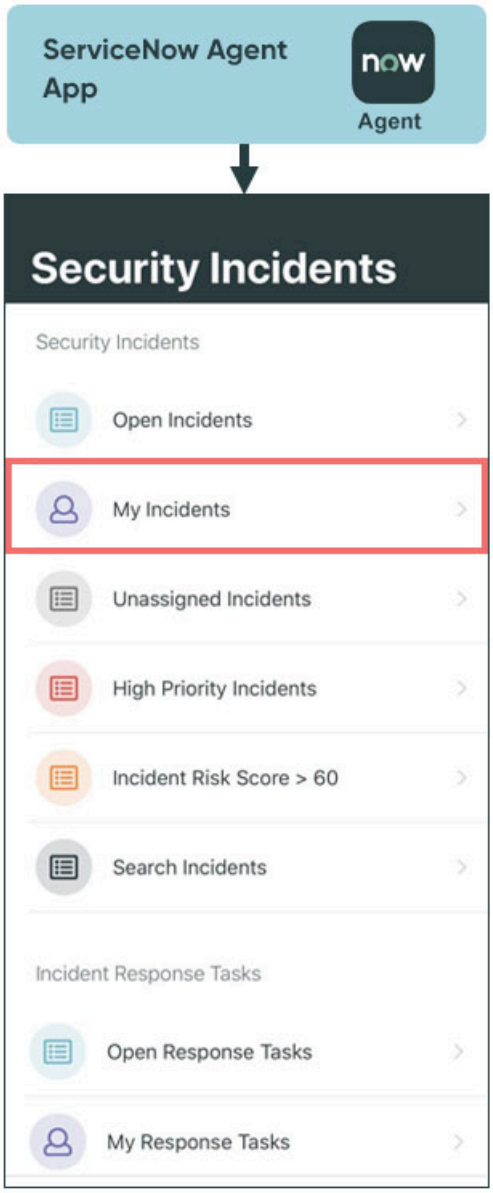
レコードのリストから、オープンセキュリティインシデントをグループ内の別のアナリストに再アサインします。または、アサインの前にレコードの詳細と関連リストを表示するか、作業メモを追加します。このタスクの完了にかかる時間：5 ～ 10 分。

手順

1. モバイルデバイスで Now Platform インスタンスにログインしていない場合は、「セキュリティインシデントレスポンスモバイルアプリ へのログイン」を参照してください。
2. [セキュリティインシデント] ランディング画面を表示して、[自分のインシデント] をタップします。

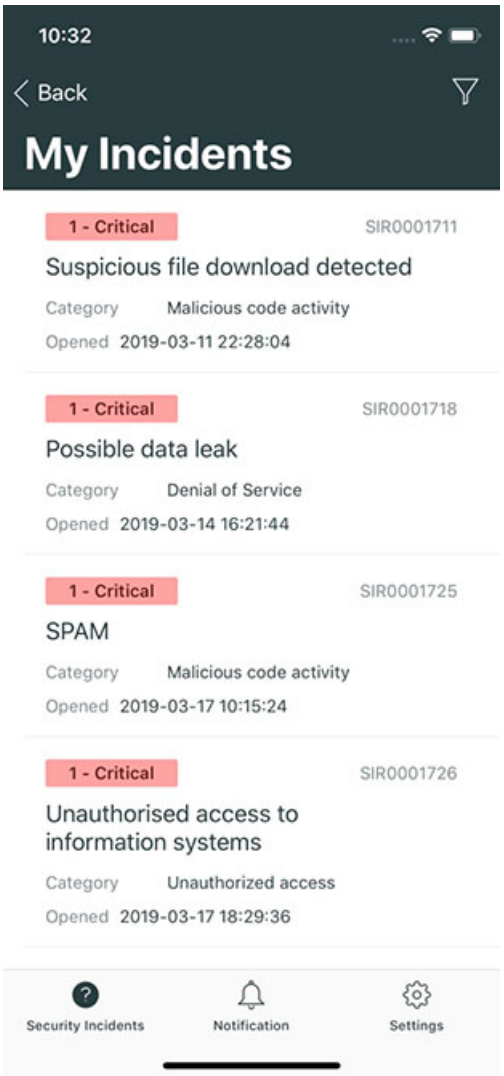
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログイン後に セキュリティインシデントレスポンスモバイルアプリ から移動した場合は、Now Agent アプリをタップすると、いつでも最後に表示していた画面に戻ります。



[自分のインシデント] 画面に、自分にアサインされているオープンセキュリティインシデントレコードのリストが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



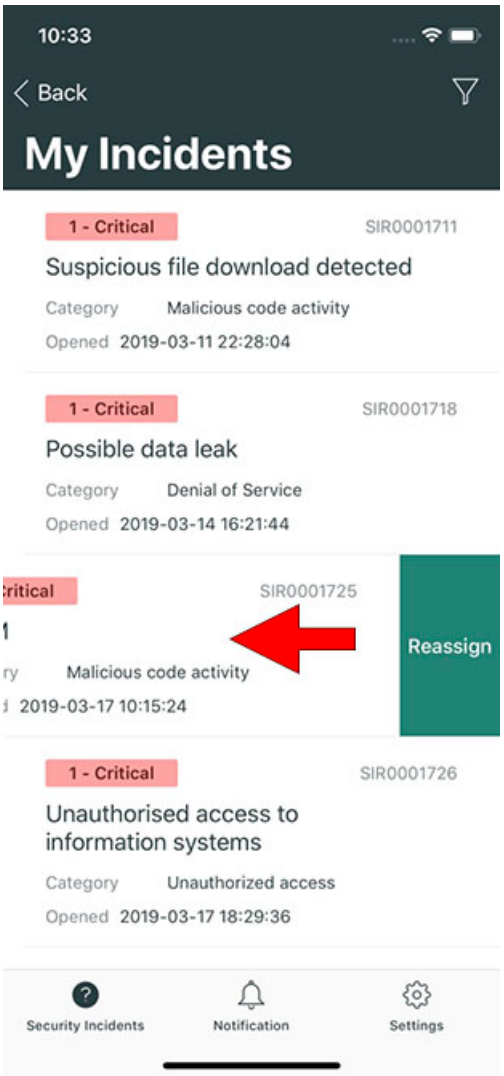
自動翻訳

3. オプション: 特定の基準に一致するセキュリティインシデントを検索するには、「セキュリティインシデントレスポンスモバイルアプリ でのセキュリティインシデントの検索」を参照してください。

   または、表示されているフィルターアイコン ( ) を使用して、リストのレコード数を制限するフィルターを設定します。モバイルアプリの画面でのレコードのフィルタリングは、Now Platform で条件ビルダーを使用したフィルタリングと同様に機能します。

4. リストからインシデントを直接再アサインするには、オープンセキュリティインシデントレコードのリストが表示された状態で、レコードを左にスワイプしてメニューを開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



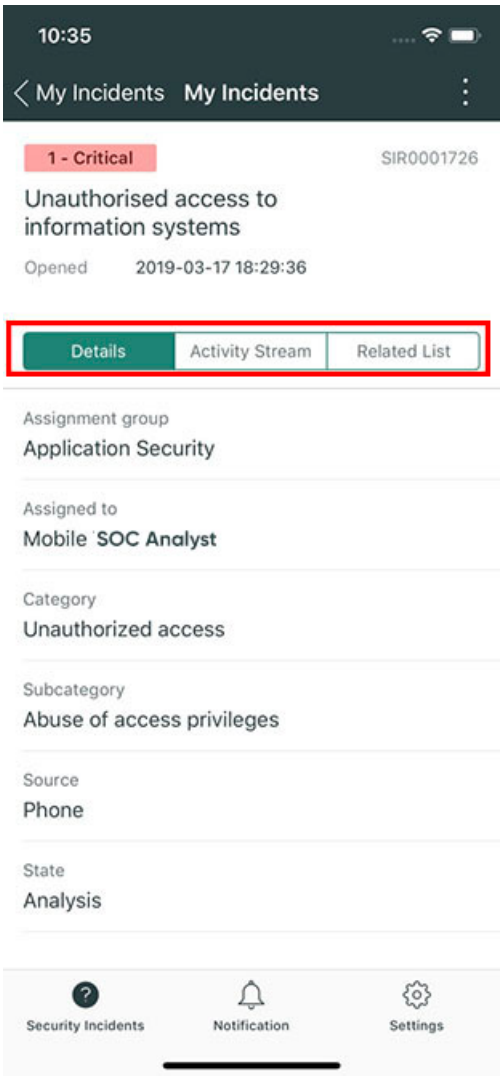
自動翻訳

5. 表示されるメニューから、[アサイン先グループ] または [アサイン先] フィールドを編集します。

6. または、オープンセキュリティインシデントレコードの詳細を表示するには、[自分のインシデント] 画面を表示して、リスト上のレコードをタップします。

7. 表示されるオープンレコードで、次の表のいずれかのオプションを選択して続行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

セキュリティインシデントレスポンスモバイルアプリ での未アサインのセキュリティインシデントの表示、編集、およびアサイン

モバイルデバイスから、未アサインの セキュリティインシデントレスポンス (SIR) インシデントを表示、編集、およびアサインします。インシデントの詳細については、関連リストおよび作業メモの監査記録を参照してください。

始める前に

必要なロール：sn_si.analyst

このタスクについて

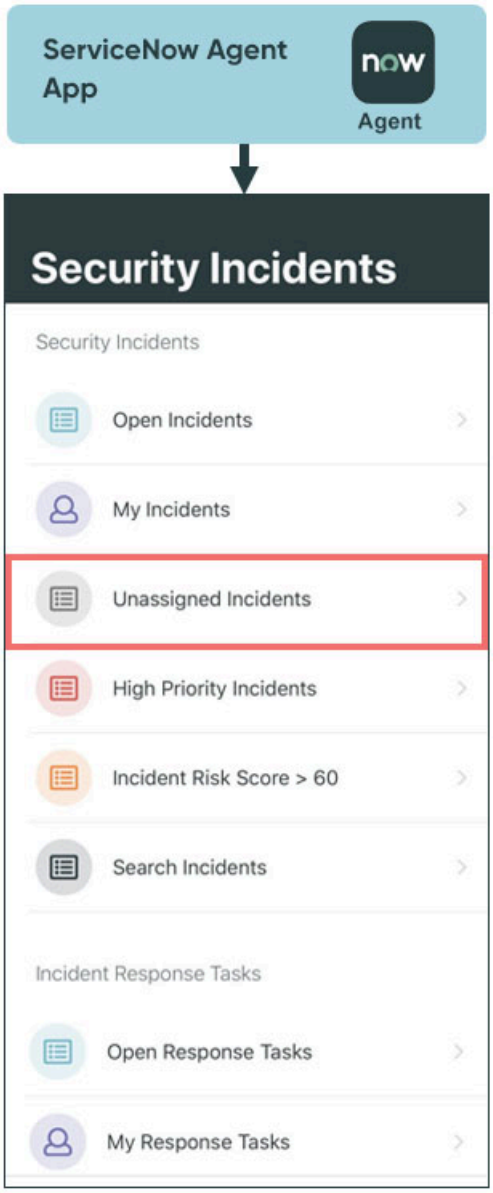
レコードのリストから、未アサインのオープンセキュリティインシデントを自分またはグループ内の別のアナリストにアサインします。または、アサインの前にレコードの詳細と関連リストを表示するか、作業メモを追加します。このタスクの完了にかかる時間：5 ～ 10 分。

手順

1. モバイルデバイスで Now Platform インスタンスにログインしていない場合、詳細については、「セキュリティインシデントレスポンスモバイルアプリ へのログイン」を参照してください。
2. [セキュリティインシデント] ランディング画面を表示して、[未アサインのインシデント] をタップします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

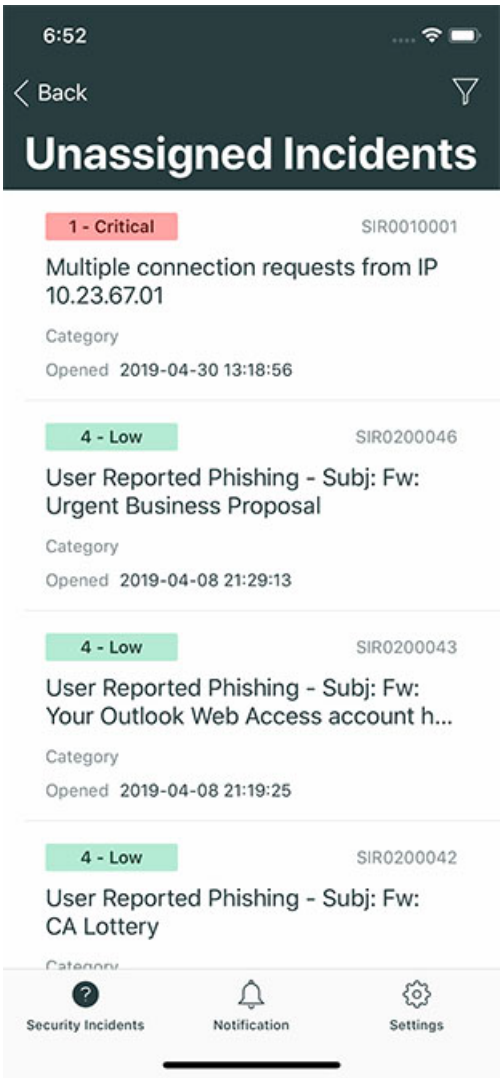
ログイン後に セキュリティインシデントレスポンスモバイルアプリ から移動した場合は、Now Agent アプリをタップすると、いつでも最後に表示していた画面に戻ります。



[未アサインのインシデント] 画面に、未アサインのセキュリティインシデントレコードのリストが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



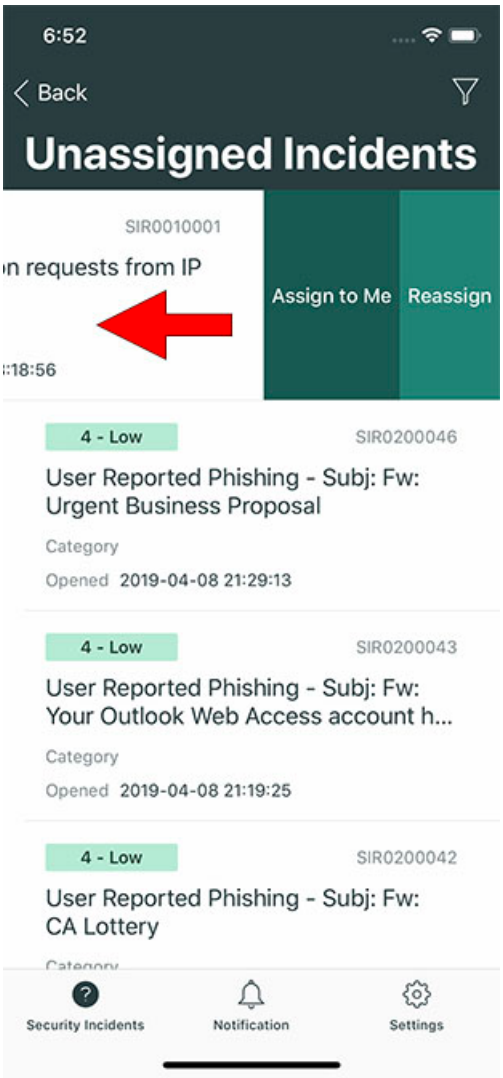
自動翻訳

3. オプション: 特定の基準に一致するセキュリティインシデントを検索するには、「セキュリティインシデントレスポンスモバイルアプリ でのセキュリティインシデントの検索」を参照してください。

   または、表示されているフィルターアイコン ( ) を使用して、リストのレコード数を制限するフィルターを設定します。モバイルアプリの画面でのレコードのフィルタリングは、Now Platform で条件ビルダーを使用したフィルタリングと同様に機能します。

4. リストからオープンセキュリティインシデントレコードを直接アサインまたは再アサインするには、未アサインのオープンセキュリティインシデントレコードのリストが表示された状態で、レコードを左にスワイプしてメニューを開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

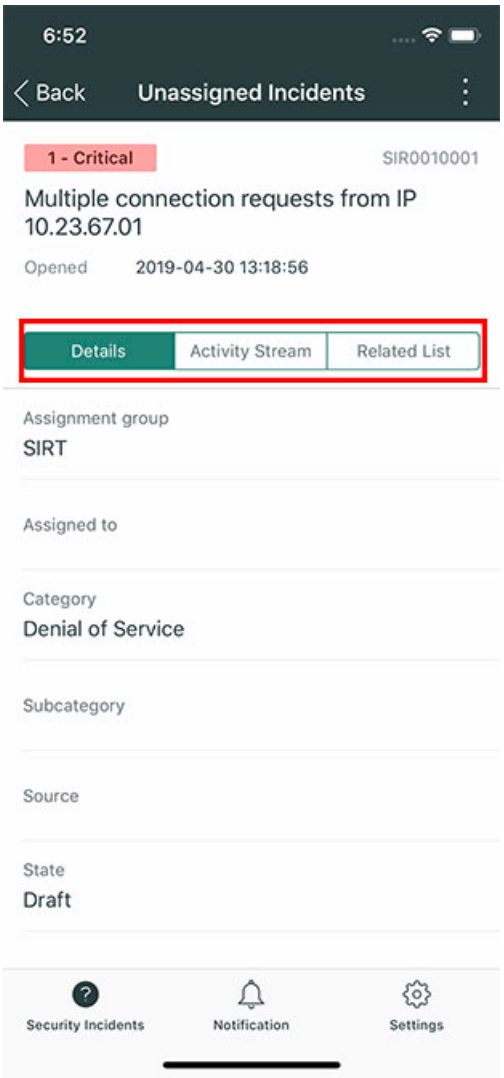


5. メニューでいずれかを選択して続行します。

6. または、表示された [未アサインのインシデント] 画面で、リスト上のレコードをタップします。

7. 表示されるオープンレコードで、次の表のいずれかのオプションを選択して続行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

セキュリティインシデントレスポンスモバイルアプリ での優先度の高いインシデントの表示、編集、およびアサイン

モバイルデバイスから、優先度の高い セキュリティインシデントレスポンス (SIR) インシデントを表示、編集、およびアサインします。インシデントの詳細については、関連リストおよび作業メモの監査記録を参照してください。

始める前に

必要なロール：sn_si.analyst

このタスクについて

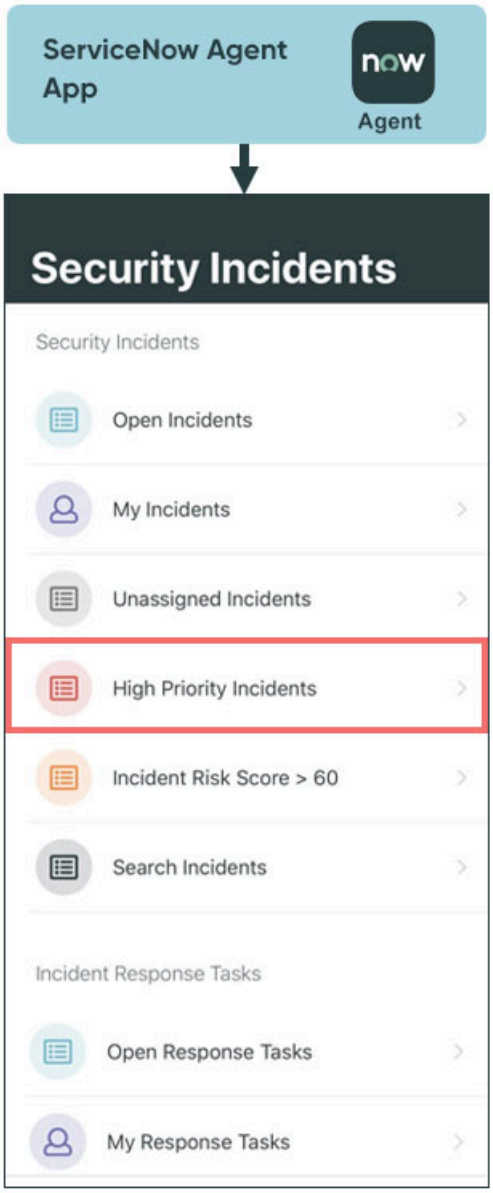
レコードのリストから、重大なオープンセキュリティインシデントを自分またはグループ内の別のアナリストにアサインします。または、アサインの前にレコードの詳細と関連リストを表示するか、作業メモを追加します。このタスクの完了にかかる時間：5 ～ 10 分。

手順

1. モバイルデバイスで Now Platform インスタンスにログインしていない場合、詳細については、「セキュリティインシデントレスポンスモバイルアプリ へのログイン」を参照してください。
2. [セキュリティインシデント] ランディング画面を表示して、[高優先度のインシデント] をタップします。

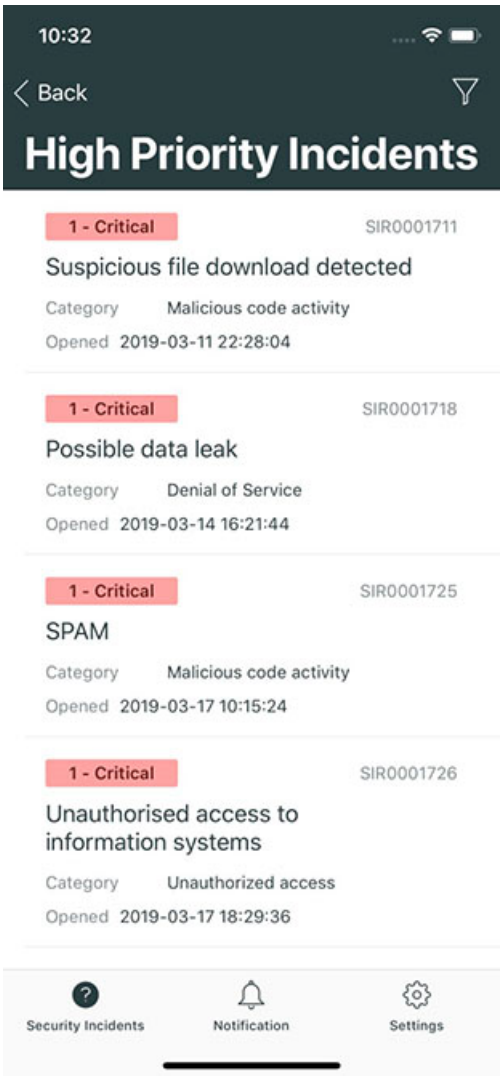
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログイン後に セキュリティインシデントレスポンスモバイルアプリ から移動した場合は、Now Agent アプリをタップすると、いつでも最後に表示していた画面に戻ります。



[高優先度のインシデント] 画面に、重要な (高優先度の) セキュリティインシデントのリストが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



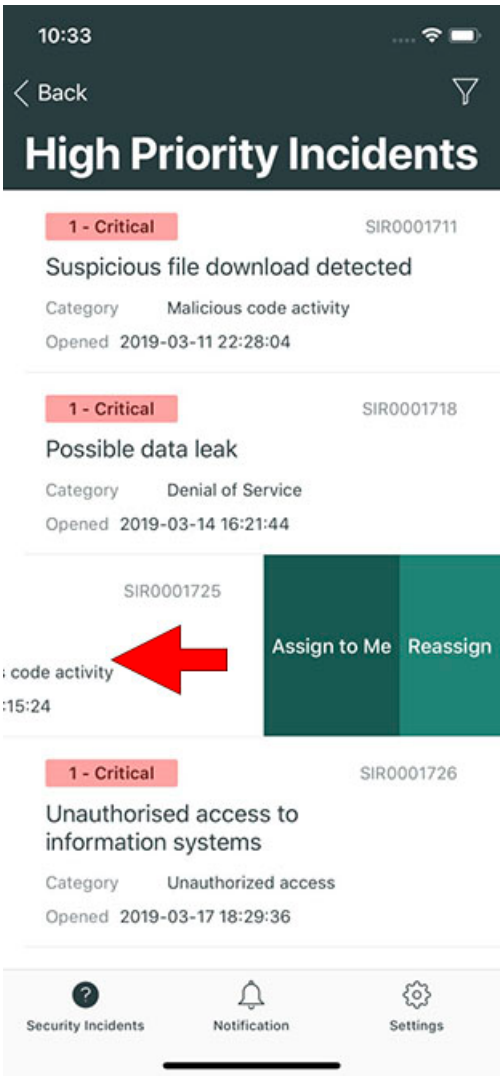
自動翻訳

3. オプション: 特定の基準に一致するセキュリティインシデントを検索するには、「セキュリティインシデントレスポンスモバイルアプリ でのセキュリティインシデントの検索」を参照してください。

   または、表示されているフィルターアイコン ( ) を使用して、リストのレコード数を制限するフィルターを設定します。モバイルアプリの画面でのレコードのフィルタリングは、Now Platform で条件ビルダーを使用したフィルタリングと同様に機能します。

4. 高優先度のオープンセキュリティインシデントレコードのリストが表示された状態で、レコードを左にスワイプしてメニューを開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

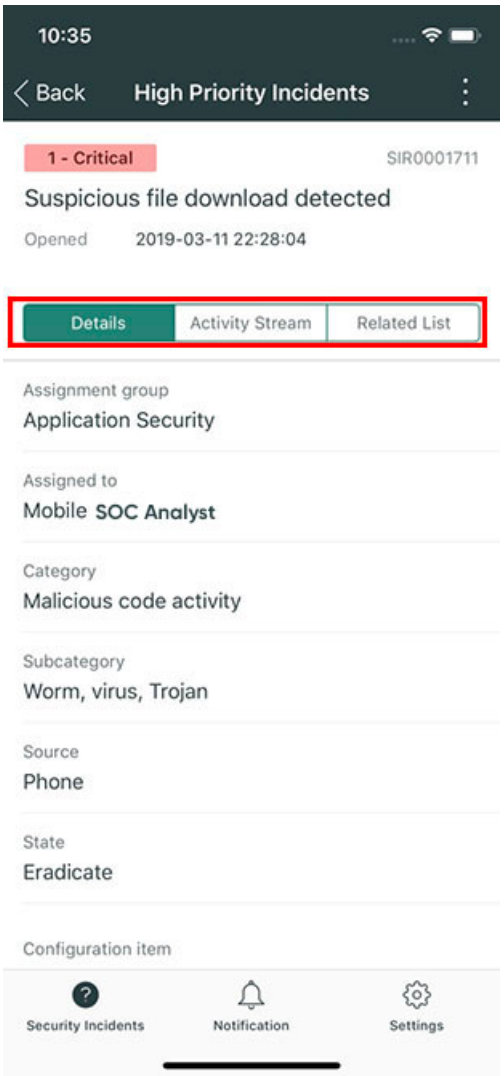


5. 1 つ選択して続行します。

6. オープンセキュリティインシデントレコードの詳細を表示し、関連付けられたレコードと関連リストをさらに表示するには、[高優先度のインシデント] 画面を表示して、リスト上のレコードをタップします。

7. 表示されるオープンレコードで、次の表のいずれかのオプションを選択して続行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

セキュリティインシデントレスポンスモバイルアプリ でのリスクスコアが **60** を超えるセキュリティインシデントの表示、編集、およびアサイン

モバイルデバイスから、リスクスコアフィールドの値が 60 より大きい セキュリティインシデントレスポンス (SIR) インシデントを表示および編集します。インシデントの詳細については、関連リストおよび作業メモの監査記録を参照してください。

始める前に

必要なロール：sn_si.analyst

このタスクについて

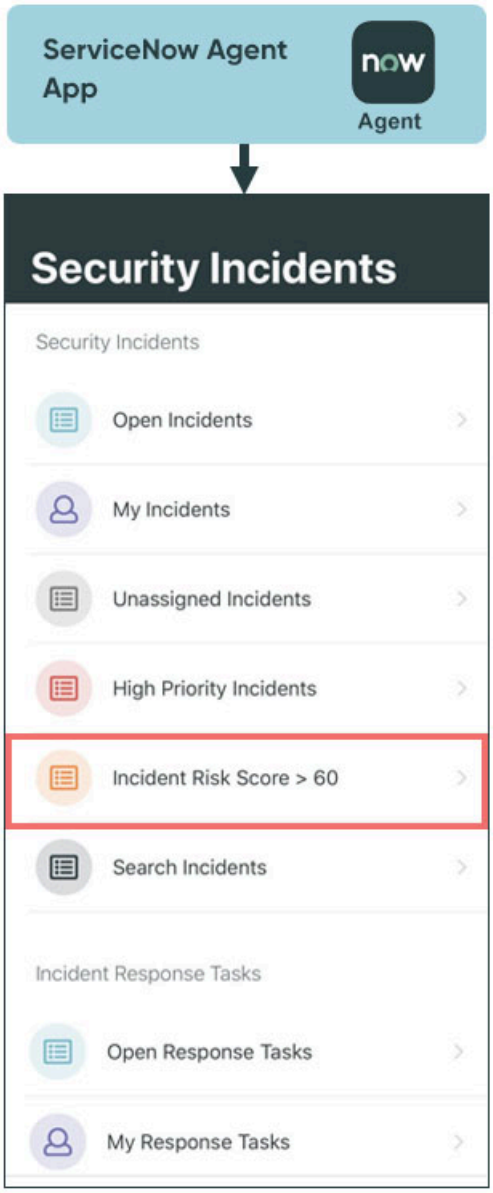
レコードのリストから、リスクスコアが 60 を超えるオープンセキュリティインシデントを自分またはグループ内の別のアナリストにアサインします。または、アサインの前にレコードの詳細と関連リストを表示するか、作業メモを追加します。このタスクの完了にかかる時間：5 ～ 10 分。

手順

1. モバイルデバイスで Now Platform インスタンスにログインしていない場合、詳細については、「セキュリティインシデントレスポンスモバイルアプリ へのログイン」を参照してください。
2. [セキュリティインシデント] ランディング画面を表示して、[リスクスコア **> 60]** をタップします。

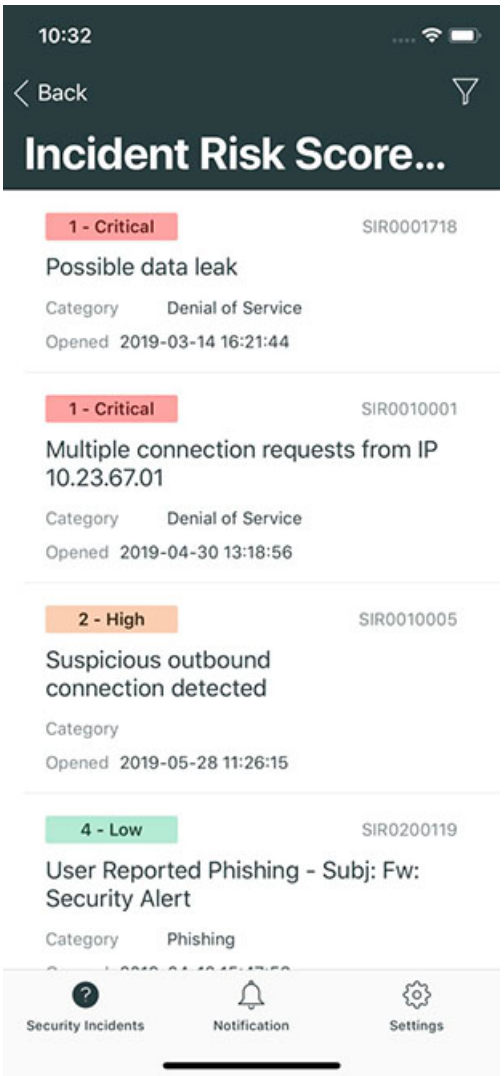
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログイン後に セキュリティインシデントレスポンスモバイルアプリ から移動した場合は、Now Agent アプリをタップすると、いつでも最後に表示していた画面に戻ります。



[インシデントリスクスコア] 画面に、セキュリティインシデントのリストが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



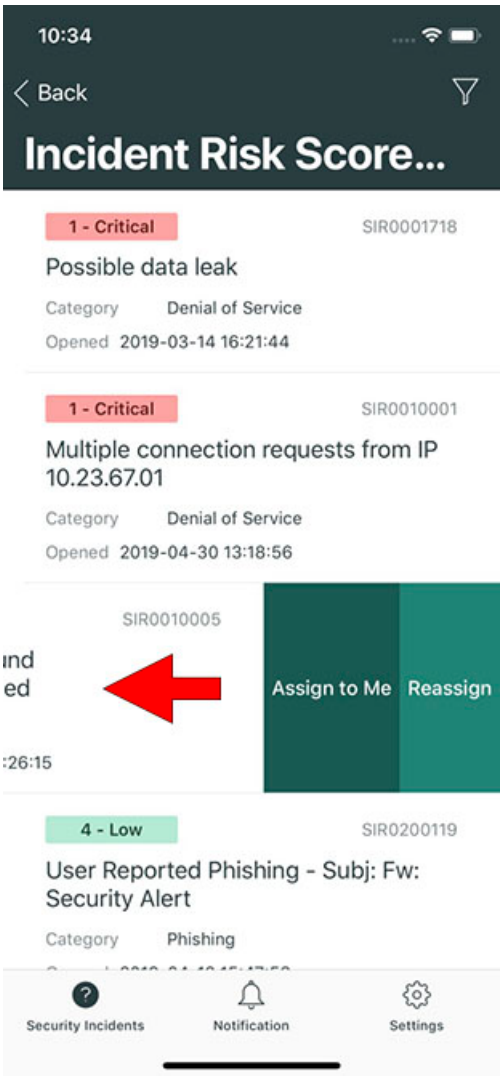
自動翻訳

3. オプション: 特定の基準に一致するセキュリティインシデントを検索するには、「セキュリティインシデントレスポンスモバイルアプリ でのセキュリティインシデントの検索」を参照してください。

   または、表示されているフィルターアイコン ( ) を使用して、リストのレコード数を制限するフィルターを設定します。モバイルアプリの画面でのレコードのフィルタリングは、Now Platform で条件ビルダーを使用したフィルタリングと同様に機能します。

4. 表示されたオープンセキュリティインシデントレコードのリストから直接セキュリティインシデントを自分にアサインするか、再アサインするには、レコードを左にスワイプしてメニューを開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

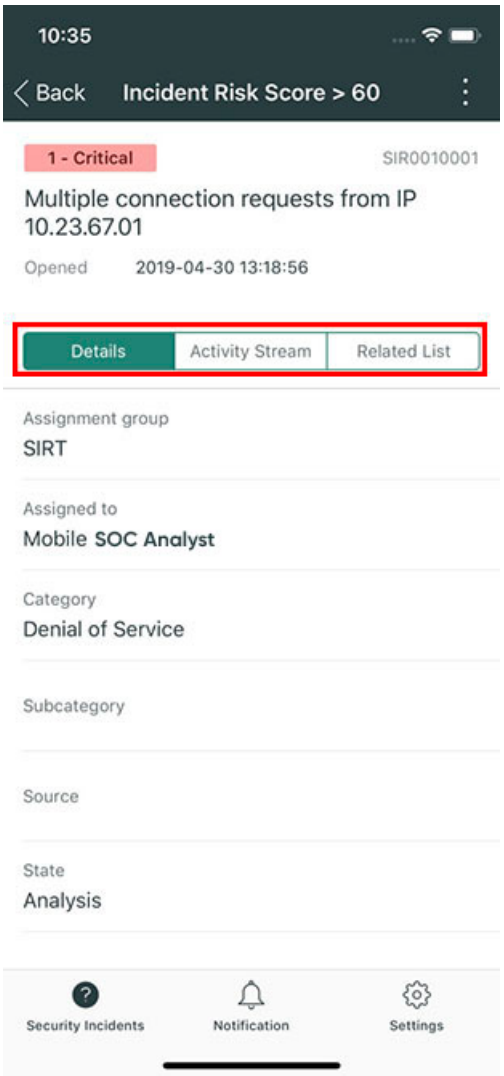


5. 1 つ選択して続行します。

6. または、オープンセキュリティインシデントレコードの詳細を表示し、関連付けられたレコードと関連リストをさらに表示するには、[インシデントリスクスコア] 画面を表示して、リスト上のレコードをタップします。
7. 表示されるオープンレコードで、次の表のいずれかのオプションを選択して続行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

セキュリティインシデントレスポンスモバイルアプリ でのセキュリティインシデントの検索

Now Platform® インスタンスで セキュリティインシデントレスポンス (SIR) セキュリティインシデントを検索します。入力した特定の検索条件に一致するインシデントのみが表示されます。

始める前に

必要なロール：sn_si.analyst

このタスクについて

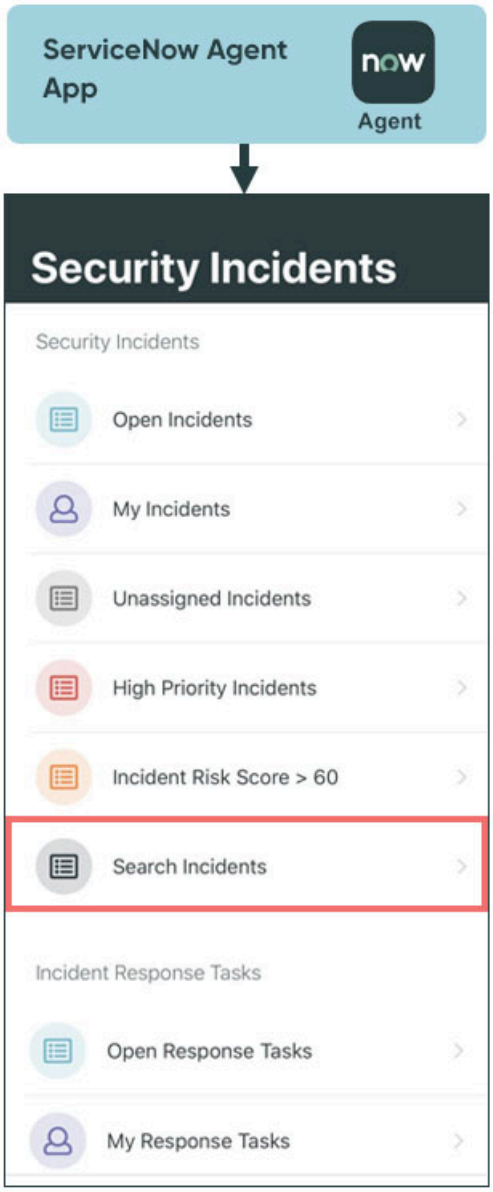
このタスクの完了にかかる時間：5 ～ 10 分。

手順

1. モバイルデバイスで Now Platform インスタンスにログインしていない場合、詳細については、「セキュリティインシデントレスポンスモバイルアプリ へのログイン」を参照してください。
2. [セキュリティインシデント] ランディング画面を表示して、[インシデントを検索] をタップします。

   ログイン後に セキュリティインシデントレスポンスモバイルアプリ から移動した場合は、Now Agent をタップすると、いつでも最後に表示していた画面に戻ります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. 返される検索結果の数を制限するために、フォームのできるだけ多くのフィールドに入力することをお勧めします。
検索条件を追加するには、次の表を参照してください。表の後にある説明に従って、既存の検索条件の編集、検索条件のクリア、または検索の送信を行います。

タップするフィールド	Android デバイスにエントリーを追加するには	iOS デバイスにエントリーを追加するには
数値	セキュリティインシデントの英数字の値を入力します (例：SIR0010004 など)。この番号は、セキュリティインシデントの右上に表示されます。 この機能では、数値文字列と部分的な数値文字列の検索を実行します。より絞り込んだ検索を行うには、入力する桁数	セキュリティインシデントの英数字の値を入力します (例：SIR0010004 など)。この番号は、セキュリティインシデントの右上に表示されます。 この機能では、数値文字列と部分的な数値文字列の検索を実行します。より絞り込んだ検索を行うには、入力する桁数

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タップするフィールド	Android デバイスにエントリーを追加するには	iOS デバイスにエントリーを追加するには
	を増やします。ワイルドカード (*) は使用できません。 新しいフィールドをタップしてさらに条件を入力するか、 をタップして検索を送信します。	を増やします。ワイルドカード (*) は使用できません。新しいフィールドをタップしてさらに条件を入力するか、[検索] をタップして検索を送信します。
簡単な説明	フィールドにテキストを入力します (例：malware など)。 この機能では、[簡単な説明] フィールドのテキスト文字列と部分的なテキスト文字列の検索を実行します。より絞り込んだ検索を行うには、入力するテキストを増やします。ワイルドカード (*) は使用できません。 新しいフィールドをタップしてさらに条件を入力するか、 をタップして検索を送信します。	フィールドにテキストを入力します (例：malware など)。 この機能では、[簡単な説明] フィールドのテキスト文字列と部分的なテキスト文字列の検索を実行します。より絞り込んだ検索を行うには、入力するテキストを増やします。ワイルドカード (*) は使用できません。新しいフィールドをタップしてさらに条件を入力するか、[検索] をタップして検索を送信します。
優先度	エントリーを追加するには、1 つ以上のアイテムをタップするか、検索アイコンをタップして検索フィールドにエントリーを入力します。チェックマークアイコンをタップすると、[インシデントを検索] 画面に戻ります。	エントリーを追加するには、1 つ以上のアイテムをタップするか、検索アイコンをタップして検索フィールドにエントリーを入力します。[完了] をタップすると、[インシデントを検索] 画面に戻ります。
カテゴリ	エントリーを追加するには、1 つ以上のアイテムをタップするか、検索アイコンをタップして検索フィールドにエントリーを入力します。チェックマークアイコンをタップすると、[インシデントを検索] 画面に戻ります。	エントリーを追加するには、1 つ以上のアイテムをタップするか、検索アイコンをタップして検索フィールドにエントリーを入力します。[完了] をタップすると、[インシデントを検索] 画面に戻ります。
ステータス	エントリーを追加するには、1 つ以上のアイテムをタップするか、検索アイコンをタップして検索フィールドにエントリーを入力します。チェックマークアイコンをタップすると、[インシデントを検索] 画面に戻ります。	エントリーを追加するには、1 つ以上のアイテムをタップするか、検索アイコンをタップして検索フィールドにエントリーを入力します。[完了] をタップすると、[インシデントを検索] 画面に戻ります。
アサイン先	リストから 1 つを選択するか、検索アイコンをタップし	リストから 1 つを選択するか、検索アイコンをタップし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タップするフィールド	Android デバイスにエントリーを追加するには	iOS デバイスにエントリーを追加するには
	て検索フィールドにエントリーを入力します。 エントリーなしの場合に、[アサイン先グループ] および [アサイン先] フィールドの値をクリアするには、[なし] を選択します。	て検索フィールドにエントリーを入力します。 エントリーなしの場合に、[アサイン先グループ] および [アサイン先] フィールドの値をクリアするには、[なし] を選択します。
アサイン先グループ	リストから 1 つを選択するか、検索アイコンをタップして検索フィールドにエントリーを入力します。 エントリーなしの場合に、[アサイン先グループ] および [アサイン先] フィールドの値をクリアするには、[なし] を選択します。	リストから 1 つを選択するか、検索アイコンをタップして検索フィールドにエントリーを入力します。 エントリーなしの場合に、[アサイン先グループ] および [アサイン先] フィールドの値をクリアするには、[なし] を選択します。

Android デバイスの場合、[インシデントを検索] 画面を表示され、すべての条件が入力された状態で、いずれかを選択して続行します。

4. iOS デバイスの場合、[インシデントを検索] 画面を表示して、いずれかを選択して続行します。

5. オプション: 検索で複数のレコードが返される場合は、「セキュリティインシデントレスポンスモバイルアプリ でのレコードのフィルタリング」により、検索結果を絞り込むことができます。

セキュリティインシデントレスポンスモバイルアプリ でのオープン応答タスクの表示、編集、および再アサイン

オープン応答タスクを表示、編集、および再アサインします。変更は、親セキュリティインシデントのセキュリティインシデントレスポンスタスクに保存されます。

始める前に

必要なロール：sn_si.analyst

このタスクについて

レコードのリストから、未アサインのオープン応答タスクを自分またはグループ内の別のアナリストにアサインします。または、アサインの前にレコードの詳細を表示するか、作業メモを追加します。このタスクの完了にかかる時間：5 ～ 10 分。

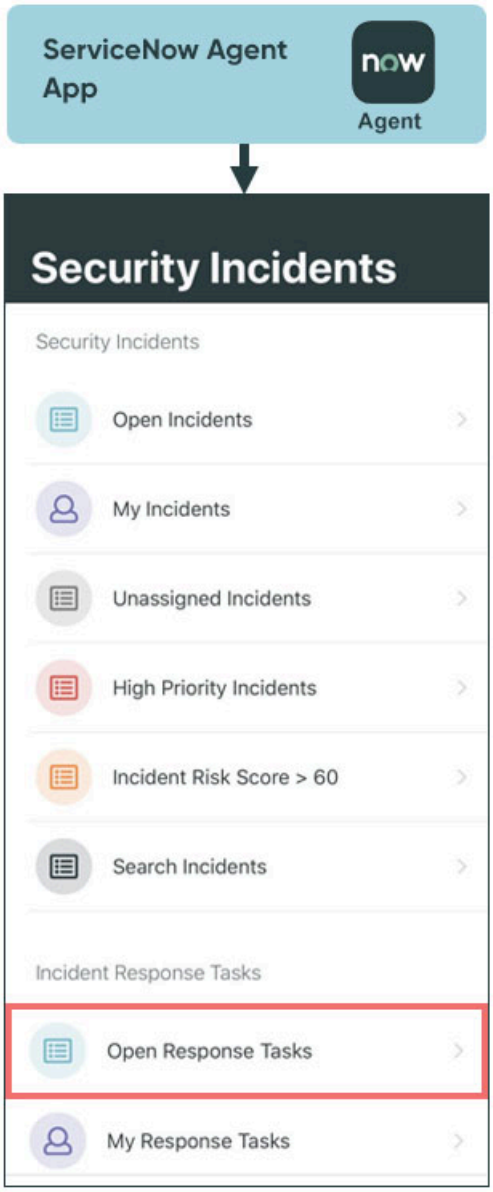
手順

1. モバイルデバイスで Now Platform インスタンスにログインしていない場合、詳細については、「セキュリティインシデントレスポンスモバイルアプリ へのログイン」を参照してください。
2. [セキュリティインシデント] ランディング画面を表示して、[オープンの対応タスク] をタップします。

   ログイン後に セキュリティインシデントレスポンスモバイルアプリ から移動した場合は、Now Agent アプリをタップすると、いつでも最後に表示していた画面に戻ります。

自動翻訳

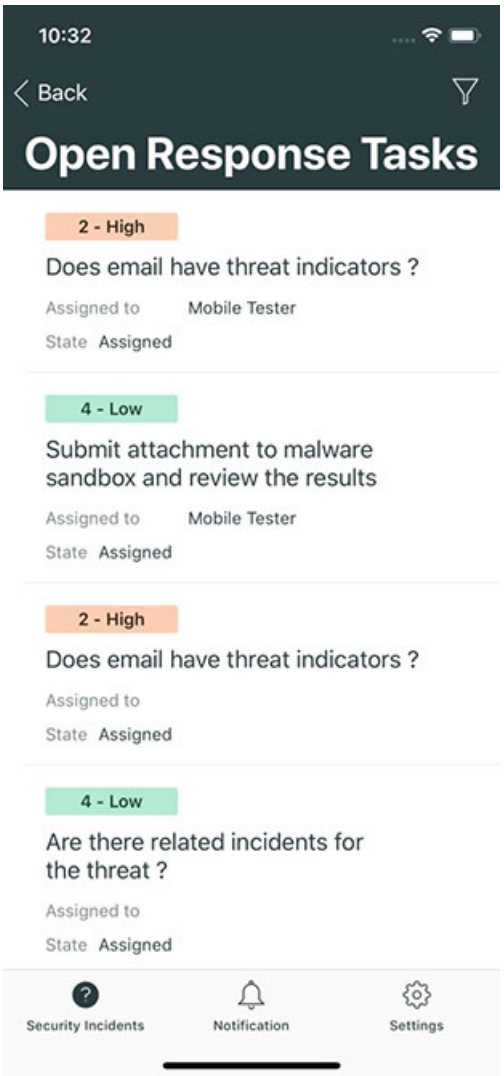
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[オープンの対応タスク] 画面に、オープンタスクのリストが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

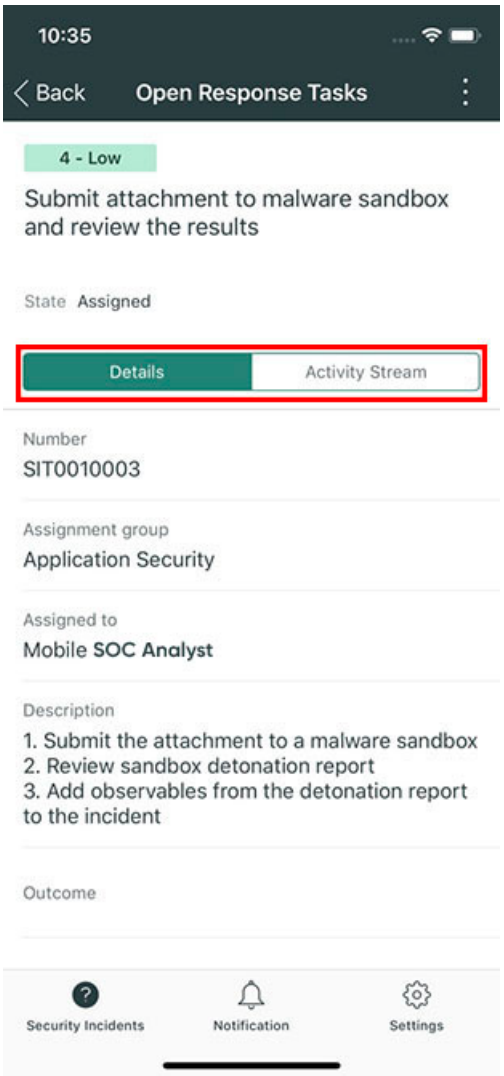


自動翻訳

3. オプション: 特定の基準に一致するタスクを検索するには、「セキュリティインシデントレスポンスモバイルアプリ でのセキュリティインシデントの検索」を参照してください。

   または、表示されているフィルターアイコン ( ) を使用して、リストのレコード数を制限するフィルターを設定します。モバイルアプリの画面でのレコードのフィルタリングは、Now Platform で条件ビルダーを使用したフィルタリングと同様に機能します。
4. オープンの対応タスクのリストが表示された状態で、リストから直接アサインまたは再アサインするには、レコードを左にスワイプしてメニューを開きます。
5. 1 つ選択して続行します。
6. または、オープンの対応タスクのレコードの詳細を表示するには、[オープンの対応タスク] 画面を表示して、リスト上のレコードをタップします。
7. 応答タスクレコードのタブが表示されたら、次の表のいずれかを選択して続行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

セキュリティインシデントレスポンスモバイルアプリ での応答タスクの表示、編集、および再アサイン

自分にアサインされた応答タスクを表示、編集、および再アサインします。変更は、親セキュリティインシデントのセキュリティインシデントレスポンスタスクに保存されます。

始める前に

必要なロール：sn_si.analyst

このタスクについて

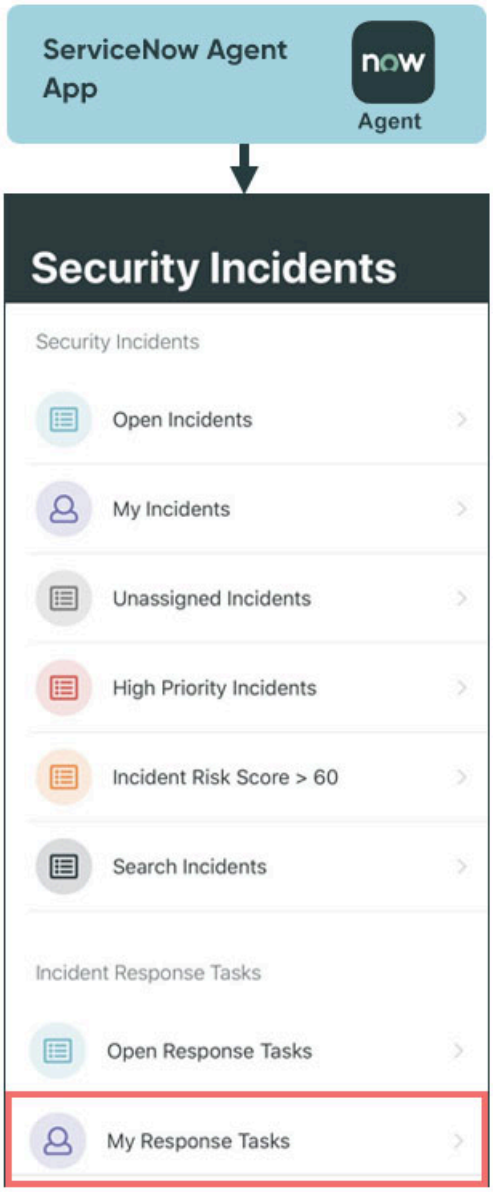
レコードのリストから、自分にアサインされているオープン応答タスクをグループ内の別のアナリストに再アサインします。または、再アサインの前にレコードの詳細を表示するか、作業メモを追加します。このタスクの完了にかかる時間：5 ～ 10 分。

手順

1. モバイルデバイスで Now Platform インスタンスにログインしていない場合、詳細については、「セキュリティインシデントレスポンスモバイルアプリ へのログイン」を参照してください。
2. [セキュリティインシデント] ランディング画面を表示して、[自分の対応タスク] をタップします。

   ログイン後に セキュリティインシデントレスポンスモバイルアプリ から移動した場合は、Now Agent (履行者) アプリをタップすると、いつでも最後に表示していた画面に戻ります。

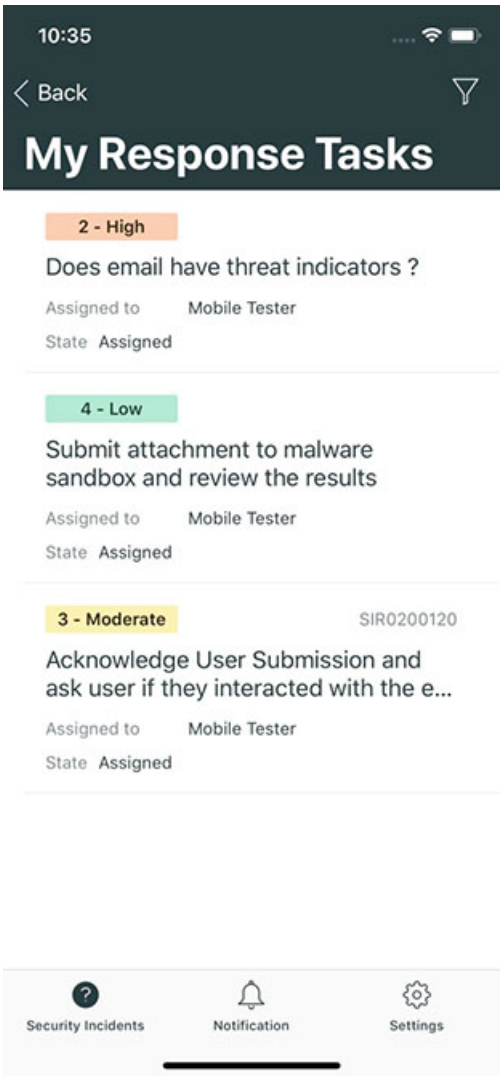
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[自分の対応タスク] 画面に、自分にアサインされている応答タスクのリストが表示されます。

自動翻訳

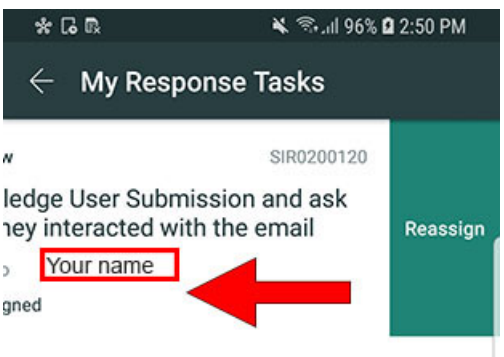
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

3. オプション: 特定の基準に一致するタスクを検索するには、「セキュリティインシデントレスポンスモバイルアプリ でのセキュリティインシデントの検索」を参照してください。

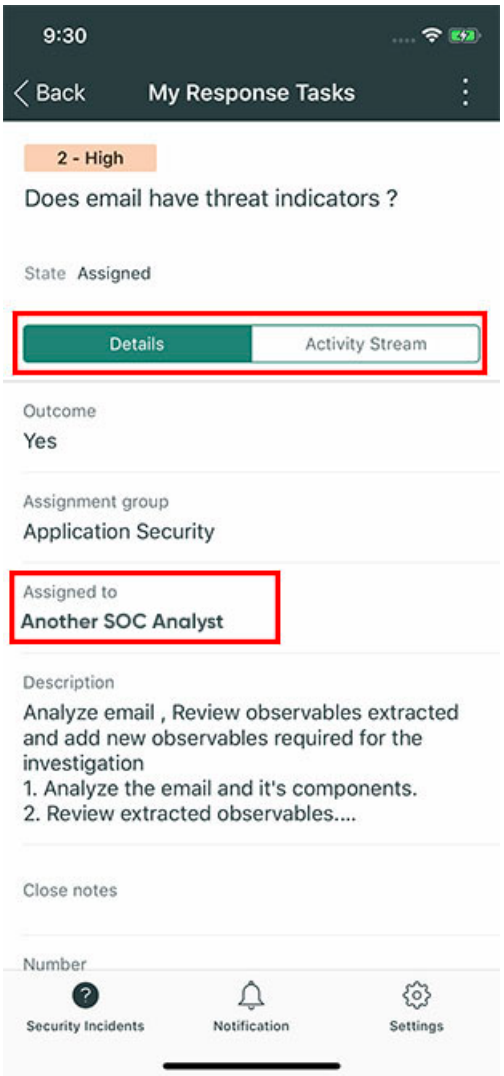
   または、表示されているフィルターアイコン ( ) を使用して、リストのレコード数を制限するフィルターを設定します。モバイルアプリの画面でのレコードのフィルタリングは、Now Platform で条件ビルダーを使用したフィルタリングと同様に機能します。
4. 自分にアサインされているタスクレコードのリストから直接タスクを再アサインするには、レコードを左にスワイプしてメニューを開きます。



5. [再アサイン] をタップします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. 表示される [対応タスクを別のユーザーにアサイン] 画面で、フィールドをタップして展開し、タスクの別のグループまたはユーザーを選択します。
7. 送信アイコン ( ) または [送信] をタップして変更を保存し、応答タスクを更新します。
   レコードが更新されたことを確認するメッセージが表示されます。タスクが親セキュリティインシデントの新しいユーザーにアサインされ、Now Platform インスタンスが更新されます。
8. オープン応答タスクの詳細を表示し、作業メモを表示するには、[自分の対応タスク] 画面を表示して、リスト上のレコードをタップします。
9. 応答タスクのフィールドが表示されたら、次の表のいずれかを選択して続行します。



セキュリティインシデントレスポンスモバイルアプリ でのレコードのフィルタリング

追加のフィルターを設定して、画面に表示されるレコードの数を制限します。モバイルアプリでのレコードのフィルタリングは、Now Platform で条件ビルダーを使用したフィルタリングと同様に機能します。

始める前に
必要なロール：sn_si.analyst

このタスクについて
このタスクの所要時間：5 分

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 検索結果をさらに絞り込む場合、または表示されるレコードリストに追加のフィルター基準を入力する場合は、フィルターアイコン ( ) をタップします。
2. [フィルター] 画面を表示した状態で、フィールドをタップして展開します。
3. 表示されるオプションから、チェックボックスをタップするか、フィルターのアイテムをタップします。
   フィルターの多くでは、複数のオプションを選択できます。
4. 戻る矢印 () をタップするか、[完了] をタップして、フィールドに加えた変更を保存します。
   選択した条件が [フィルター] 画面に表示されます。基準と一致するレコードの数も画面の上部に表示されます。[リセット] をタップして、すべてのフィルターを削除し、デフォルト設定に戻します。
5. オプション: フィルター条件の設定を続行するには、[フィルター] 画面で手順 1 ～ 4 を繰り返します。
6. 交差アイコン () をタップして、AND 条件を作成します。
   または、交差アイコン () をタップして、OR 条件を作成します。
7. 必要なすべての条件を追加したら、表示された [フィルター] 画面で [完了] をタップします。
   フィルター基準に一致するレコードのみが画面に表示されます。

セキュリティインシデントレスポンスオーケストレーション

セキュリティインシデントレスポンスオーケストレーション アクティビティを使用すると、ワークフローオーケストレーションを使用して、Windows または UNIX ベースのシステムおよび環境とやり取りし、データを取得できます。

セキュリティインシデントレスポンスオーケストレーションのセットアップ

セキュリティインシデントレスポンスオーケストレーション を使用する前に、CMDB の入力、MID サーバーの構成、認証情報の構成など、システム各部のセットアップ手順を実行します。

始める前に
必要なロール：admin
セキュリティインシデントレスポンス を使用するには、ドメイン名が完全に入力された CMDB が必要です。詳細については、次を参照してください： ディスカバリー。

このタスクについて

手順

1. セキュリティインシデントレスポンス プラグインをアクティブ化します。
2. MID サーバーの構成。
3. Windows MID サーバーサービスの認証情報の設定。

セキュリティインシデントレスポンスオーケストレーションのワークフローとワークフローテンプレートを理解する

セキュリティインシデントレスポンス ベースシステムには、セキュリティインシデントレコードと連携するように設計された一連のワークフローとワークフローテンプレートが含まれています。

始める前に
必要なロール：sn_si.basic

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタスクについて
適切なロール (sn_sec_cmn.admin) を持っている場合は、すべてのワークフローとワークフローテンプレートをニーズに合わせて調整できます。ワークフローは Security Operations システム全体で使用され、さまざまなタスクを実行できます。
ただし、ワークフローテンプレートは、セキュリティインシデントの [カテゴリ] フィールドの値を選択することでトリガーされます。トリガーされると、選択内容に関連付けられたワークフローテンプレートにより、特定のタイプの脅威に対処する方法をセキュリティアナリストに指示するワークフローテンプレートが起動します。

たとえば、セキュリティインシデントの [カテゴリ] フィールドから [サービス拒否] を選択すると、[セキュリティインシデント - サービス拒否 - テンプレート **(Security Incident - Denial of Service - Template)]** が実行され、アナリストは DOS のターゲットがビジネスクリティカルであるかどうかを判断するように指示されます。その場合、次のタスクによってセキュリティインシデントの優先度が **[1** - 重大] に設定され、次のタスクが実行されます。などができます

したがって、セキュリティインシデントレスポンス ワークフローとワークフローテンプレートは、テンプレートがセキュリティインシデント内の特定の機能セットに使用される点を除いて、基本的に同じです。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > ワークフロー > セキュリティワークフローを表示.
2. ベースシステムに含まれるワークフローとワークフローテンプレートのリストが表示されます。セキュリティオペレーション アプリケーションスイートで作成した新しいワークフローもリストに含まれます。
3. 表示するワークフローまたはワークフローテンプレートの名前をクリックします。

> **注:**
> ワークフローはいくつかの方法でトリガーできます。ワークフローをワークフロートリガーに関連付けても、必ずしもワークフローがアクティブになるとは限りません。

セキュリティインシデントレスポンスオーケストレーション のワークフローおよびアクティビティ

セキュリティインシデントレスポンスオーケストレーション には、いくつかのワークフローとアクティビティが含まれています。

sn_sec_cmn.admin ロールを持つユーザーのみが、 ワークフローエディター 。

IoC 変更のためのルックアップ要求の作成 **(Create Lookup Request for IoC Changes)** ワークフロー

[セキュリティインシデントレスポンス **- IoC** 変更のためのルックアップ要求の作成 **(Create Lookup Request for IoC Changes)]** フローは、ビジネスルールによってトリガーされ、IoC が追加または変更されたときに自動的に実行されます。マルウェアスキャンは、新規データが入力されたときとスキャンされたときにのみトリガーされます。

始める前に
必要なロール：sn_si.basic

このタスクについて
IoC が空の場合、ワークフローは実行されません。履歴スキャンは維持され、セキュリティインシデントの [セキュリティスキャン要求 **]** タブと作業メモで表示できます。既存のセキュリティインシデントは自動的に更新されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

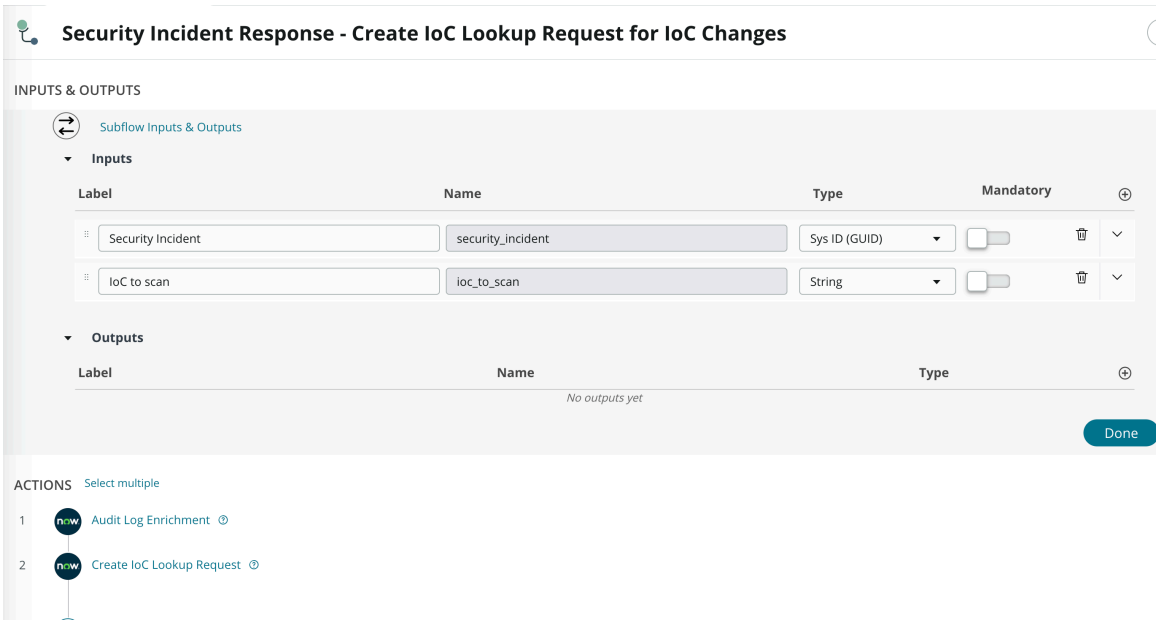
重要:

「セキュリティインシデントレスポンス - **IoC** 変更のためのルックアップ要求の作成」のワークフローはフローデザイナーに移行されます。フローは、「sn_ti_scanne」にレコードが 1 つ以上ある場合にのみトリガーされます。

フローデザイナーアクションは次のとおりです。

- 監査ログの拡張
- [IoC ルックアップ要求を作成] アクティビティ

IoC 変更ワークフロー



[**IoC** ルックアップ要求を作成] アクティビティ

[IoC ルックアップ要求を作成] アクティビティは、任意のワークフローで使用して、追加または変更された IoC フィールドのマルウェアルックアップ要求を作成できます。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	ルックアップ要求が作成されました。
失敗	ルックアップ要求が作成されませんでした。

入力変数

変数	説明
IoCtring	JSON 形式の IoC 情報。IP、ハッシュ、URL
sild	セキュリティインシデントシステム識別子

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
scnReqID	ルックアップ要求識別子

セキュリティインシデントレスポンス - ネットワーク統計情報を取得フロー

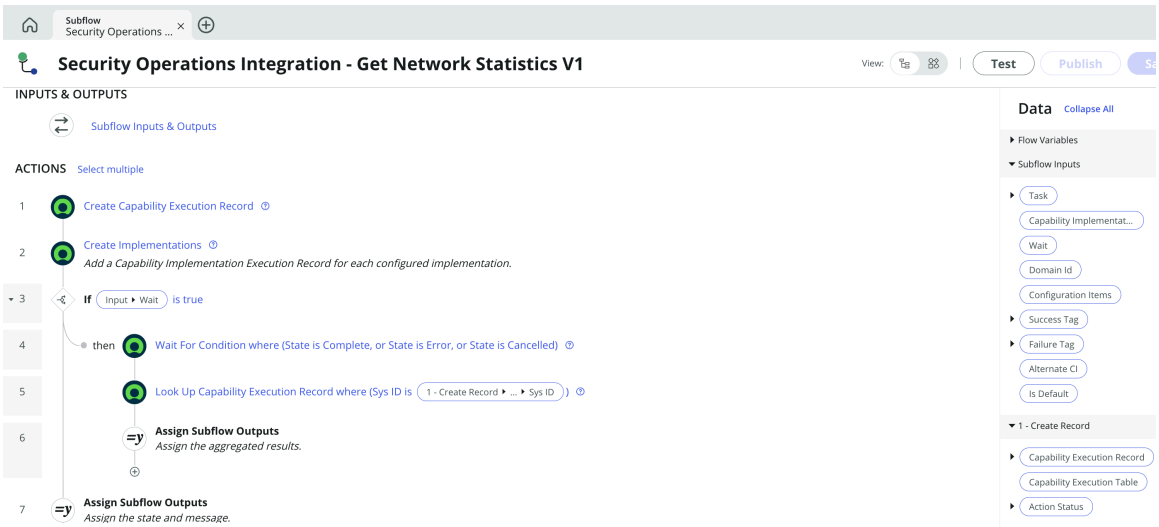
application **Security Incident Response** (セキュリティインシデントレスポンス) > ネットワーク統計情報を取得 フローは、[分析] ステータスのセキュリティインシデントに追加されたときに、影響を受ける Windows ベースのリソースのネットワーク統計情報を取得します。

始める前に
必要なロール：sn_si.analyst

このタスクについて
構成アイテムを含む新しいセキュリティインシデントの場合、ステータスが [分析] に変わるとフローが自動的に実行されます。

既存のセキュリティインシデントは、[分析] ステータスのときに新しい構成アイテムを追加すると自動的に更新されます。

ネットワーク統計情報を取得



フロープロセスアクションには次のものが含まれます。

[構成アイテム FQDN を取得] フローアクション

OS によるシェルスクリプトの決定

ステートメントが Powershell によって実行される場合

[実行トラッキング:フローを開始] アクション

netstat フローアクションを介してネットワーク統計情報を取得

機能トラッキング:失敗フローアクション

拡張データレコードフローアクションを作成

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

機能トラッキング:失敗フローアクション - 拡張 ID を返します。

機能トラッキング:フローアクションを完了

手順

1. 任意のセキュリティインシデントを開きます。
2. 必要に応じて [ステータス **(State)]** を [分析] に更新します。
3. 構成アイテム (コンピューター、サーバーなど) を追加します。
4. **[Update** (更新)] をクリックします。
   セキュリティインシデントレスポンスオーケストレーション でネットワーク統計情報を提供します。 関連リンク > セキュリティインシデントの拡張 学習します。詳細については、「セキュリティオペレーション 拡張データマッピング」を参照してください。

   ここでは、このフローに固有のアクションについて説明します。他のアクションの詳細については、「 一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

セキュリティインシデントレスポンス - 実行中のサービスを取得ワークフロー

[セキュリティインシデントレスポンス - 実行中のサービスを取得ワークフロー] は、Windows ベースの ServiceNow 構成アイテム (CI) から実行中のサービスのリストを取得します。このワークフローは、調査中にインシデントの拡張に使用されます。

始める前に
必要なロール：sn_si.analyst

このタスクについて
[セキュリティインシデントレスポンス - 実行中のサービスを取得ワークフロー] は、ステータスが [分析] に変わった後に、Windows セキュリティインシデントに新しい構成アイテムを追加すると、自動的に実行されます。このワークフローが取得する情報は、セキュリティインシデントの [拡張データを表示] タブに表示されます。

> **注:**
> セキュリティインシデントが [ドラフト] ステータスのままだと、[セキュリティインシデントレスポンス - 実行中のサービスを取得ワークフロー] は実行されません。

ワークフローアクティビティには次のものが含まれます。

[監査ログ拡張スクリプト (Audit Log Enrichment Script)] アクティビティ

[構成アイテム FQDN を取得] フローアクション

[OS によるシェルスクリプトの確認] アクティビティ

[PowerShell による実行？(Is Execution via PowerShell)] アクティビティ

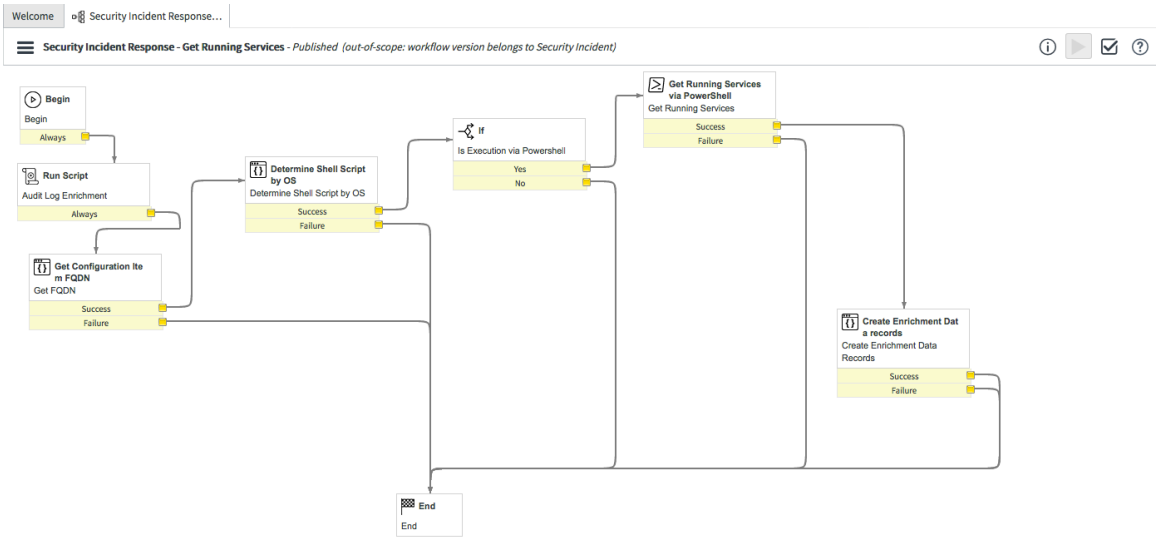
[実行中のサービスを取得 - WMI 拡張] アクティビティ

拡張データレコードフローアクションを作成

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

実行中のサービスを取得



手順

1. 任意のセキュリティインシデントを開きます。
2. 必要に応じて [ステータス **(State)**] を [分析] に更新します。
3. Windows ベースの構成アイテム (サーバー、ラップトップなど) を追加します。
4. **[Update** (更新)] をクリックします。
   セキュリティインシデントレスポンス で実行中のサービス情報を提供します 関連リンク > セキュリティインシデントの拡張学習します。詳細については、「セキュリティオペレーション 拡張データマッピング」を参照してください。

[OS によるシェルスクリプトの確認] アクティビティ

[OS によるシェルスクリプトの確認] ワークフローアクティビティは、ワークフローで使用するオペレーティングシステムを決定します。

[OS によるシェルスクリプトの確認] アクティビティを任意のワークフローで使用して、構成アイテムを含むシステムで実行されているオペレーティングシステムに基づいて実行するシェルスクリプトを決定できます。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	オペレーティングシステムが見つかりました。
失敗	オペレーティングシステムが見つかりませんでした。その他のエラー情報は、アクティビティ出力エラーで確認できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

変数	説明
ciSysId	構成アイテムのシステム識別子。
processType	テーブルからプルするスクリプトを定義する内部識別子。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
processScript	実行中のプロセスを収集する ECC エージェント。
executionTemplate	スクリプトをプローブ経由で実行するか、PowerShell を使用して実行するかを決定します。
enrichmentMappingId	応答データの変換に使用される拡張マッピングのシステム識別子。

実行中のサービスを取得 - WMI 拡張

[セキュリティインシデントレスポンス - 実行中のサービスを取得] ワークフローは、セキュリティインシデントに追加された構成アイテムで実行中のサービスを収集します。

[実行中のサービスを取得 - WMI 拡張] アクティビティが自動的に起動され、Windows ホストの実行中のサービス情報が取得されます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

入力変数

変数	説明
target [文字列]	ターゲットシステムの完全修飾ドメイン名 (FQDN)。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
response [文字列]	ターゲットシステムで現在実行中のサービスを表す JSON 文字列。 JSON データには次のものが含まれます。 name サービスの名前。 pid 実行中のサービスのプロセス識別子。 service_type

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数 (続く)

変数	説明
	(オプション) 実行中のサービスのタイプ。 start_name サービスのシステム名。 path 実行中のサービスの実行可能ファイルのパス。 start_mode 実行中のサービスの開始モード。 display_name ユーザーに表示される実行中のサービスの名前。

制限

MID サーバーは **PowerShell** をサポートしている必要があります。

SHA-256 ハッシュには PowerShell V4 が必要です。

procdump フローを実行

[procdump を実行] フローは、指定されたプロセスでプロセスダンプを実行し、セキュリティアナリストがターゲットにできるファイルに保存します。

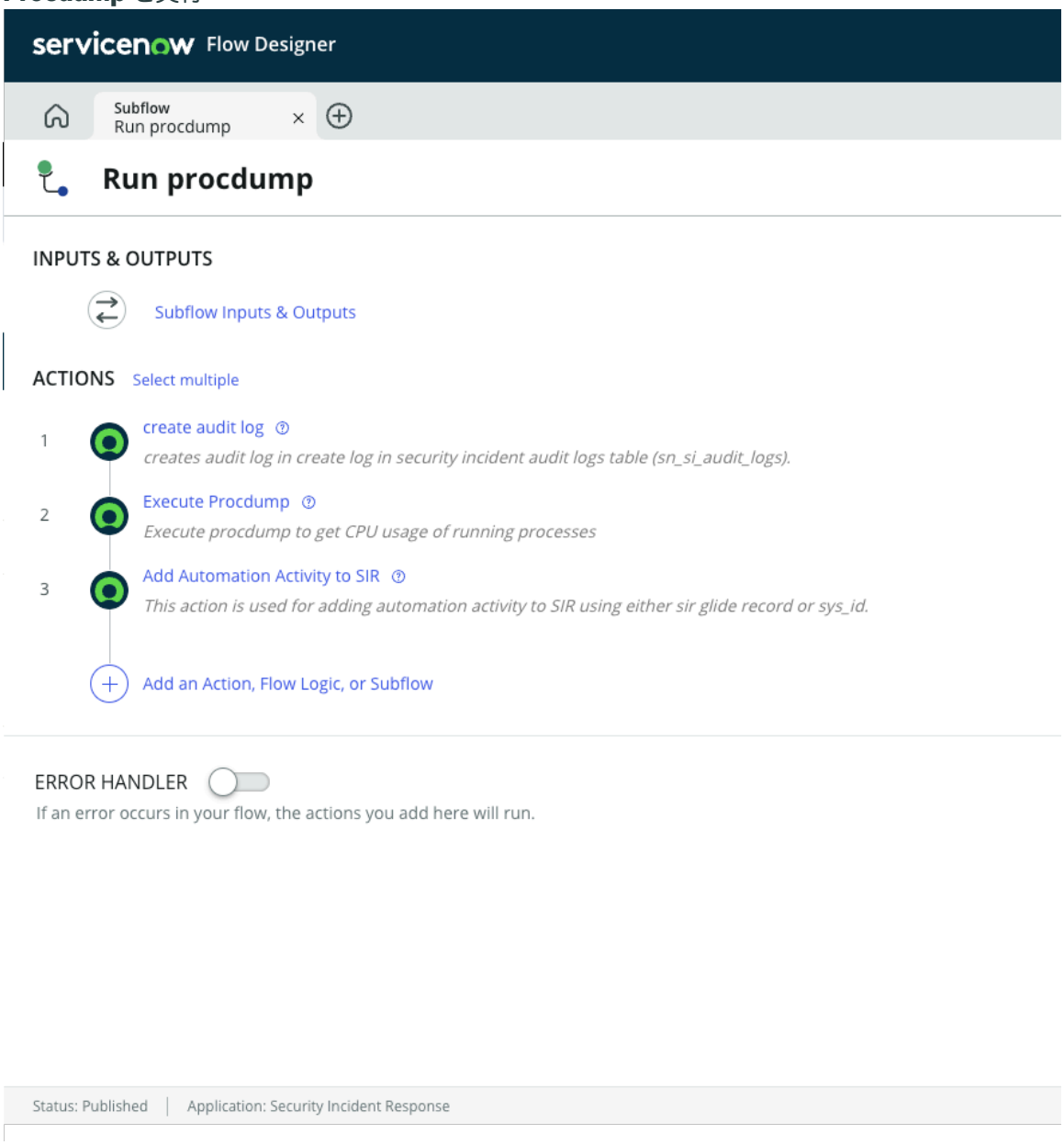
必要なロール：sn_si.analyst

このフローは、拡張プロセスが選択され、[**procdump** を実行] UI アクションが実行されるとトリガーされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Procdump を実行



自動翻訳

Procdump が失敗する理由には次のようなものがあります。

- ダンプパスが無効
- ファイル共有パスが無効
- Procdump が実行されている Windows マシンの完全修飾ドメイン名をフェッチできない
- プロセス名が指定されていない
- PROCDUMP 環境変数が見つからない
- ダンプファイルのコピーをダンプパスからファイル共有パスにコピーできない

procdump action を実行

[Procdump を実行] は、選択したプロセスで procdump を実行し、データをファイルにダンプして、内部ネットワーク上の共有サイトに投稿する PowerShell アクションです。アナリストは、セキュリティインシデントで赤くハイライト表示された、拒否リストに載っているプロセスを表示して、ファイルで追加の分析を実行できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

結果

このアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	procdump はprocess_nameで正常に実行されました。詳細は actionOutput.response で確認できます。
失敗	procdump はprocess_nameでの実行に失敗しました。詳細は actionOutput.response で確認できます。

入力変数

入力変数は、要求された出力を作成するために使用されます。

入力変数

変数	説明
targetId	[必須] procdump を実行するターゲット ID
process_name	[必須] procdump のプロセス名
dump_path	[必須] 生成されるダンプファイルの保存先のローカルファイルパス
dump_filename	[必須] procdump によって生成されるファイルのファイル名。ダンプファイル名に含まれるすべての特殊文字は、ファイルの生成時にハイフン (-) で置き換えられます。
file_share_path	[必須] ダンプファイルのコピー先のファイル共有パス

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。

出力変数

変数	説明
share_path	[必須] ダンプファイルのコピー先のファイル共有パス
response	procdump の結果の JSON 表現
result	procdump の結果

セキュリティインシデント - 応答タスクの結果の評価 **(Evaluate response task outcome)** ワークフロー

セキュリティインシデント - 応答タスクの結果の評価 (Evaluate response task outcome) ワークフローは、使用するタスクを決定し、選択したワークフローへの入力として指定された結果エバリュエーターレコードに基づいて、選択したワークフローと評価スクリプトを呼び出します。

始める前に

必要なロール：sn_si.write

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタスクについて
このワークフローは、評価されるタスクの作成アクティビティと同時に実行することが想定されています。評価スクリプトは、応答タスクのコンテキスト情報 (その親セキュリティインシデントなど) を使用して、構成された機能のアーティファクト (サイティング検索レコードや実行中のプロセスなど) を照会し、応答タスクの適切な結果を決定します。結果はワークフローアクティビティによって異なる可能性がありますが、一般に [はい] または [いいえ] です。結果エバリュエーターレコードを作成するときは、ワークフローが構成済みで、[タスクに基づく機能] ボックスがオンになっており、タスク入力変数が設定されている機能のみ選択できます。

ワークフロープロセスアクティビティには次のものが含まれます。

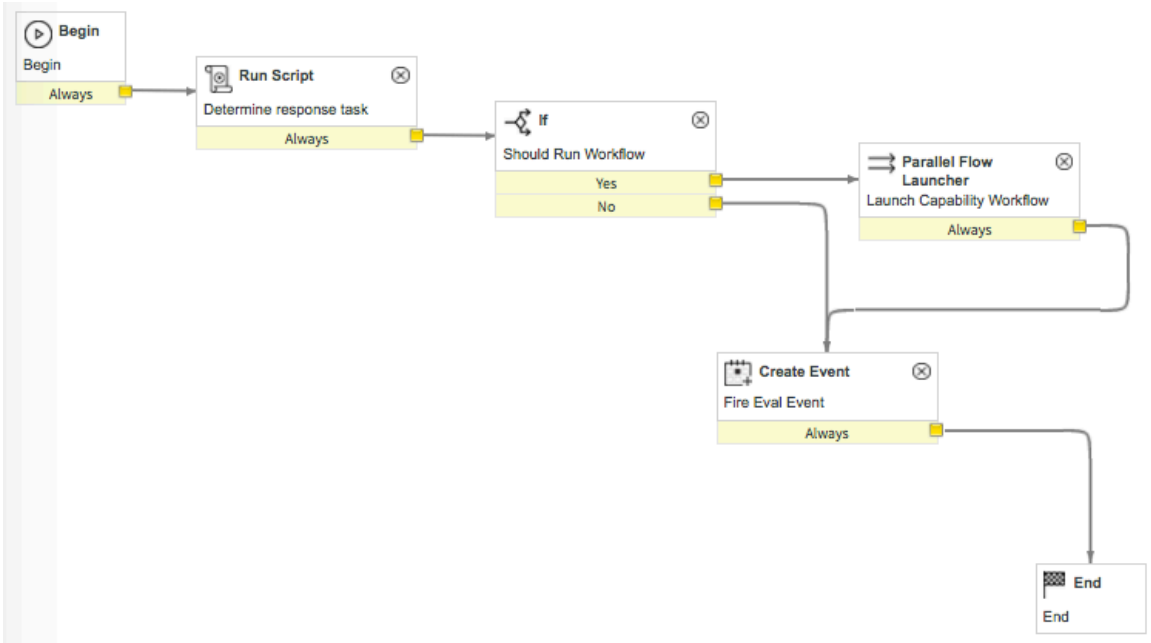
スクリプトを実行 - 応答タスクを決定 (Determine response task)

実行要不要 (Should Run) ワークフロー

パラレルフローランチャー - 機能の起動 (Launch Capability) ワークフロー

評価イベントを作成

応答タスクの結果の評価



セキュリティインシデントレスポンスのワークフローテンプレート

セキュリティインシデントレスポンスオーケストレーション に付属するワークフローテンプレートを使用すると、基本的なセキュリティ運用関連の分析手順を実行できます。テンプレートはそのまま使用することも、カスタマイズして特定のニーズに合わせたワークフローを作成することもできます。ワークフローテンプレートは、デフォルトでは非アクティブになっています。

sn_sec_cmn.admin ロールを持つユーザーのみが、ワークフローエディター を使用できます。

セキュリティインシデント機密データエクスポージャーワークフローテンプレート

セキュリティインシデント - 機密データエクスポージャー - テンプレートを使用すると、機密データエクスポージャーを処理するために設計された一連のタスクを実行できます。

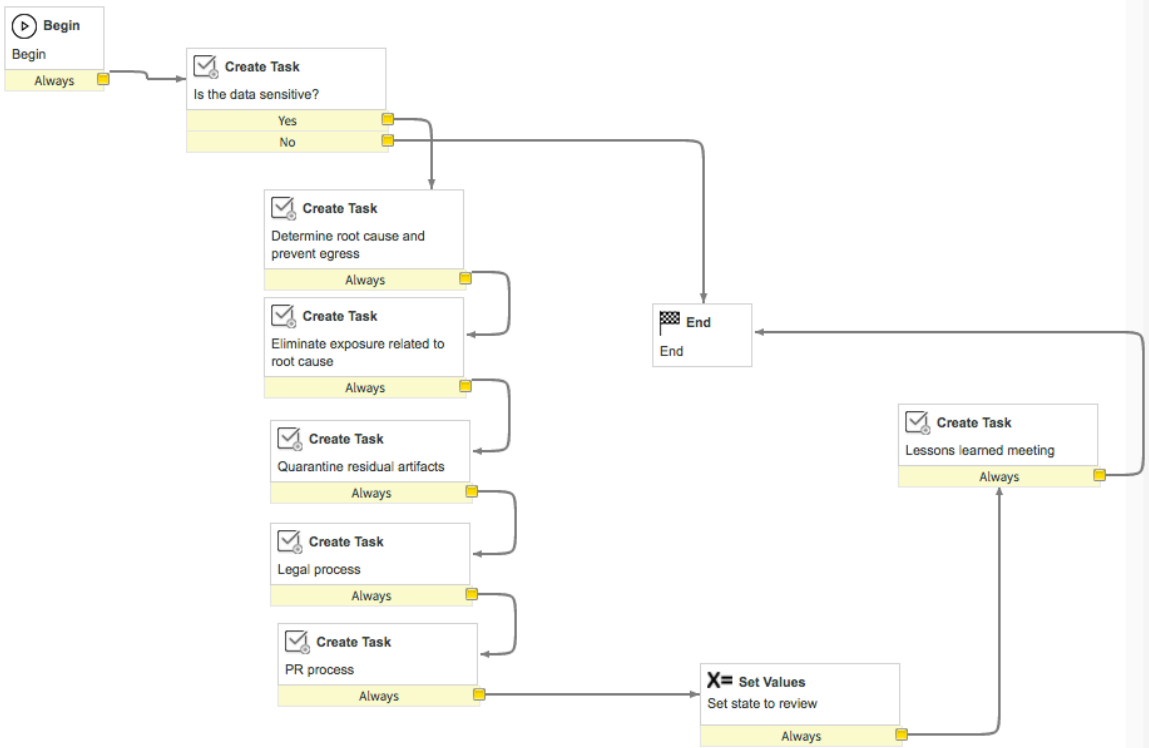
始める前に
必要なロール：sn_si.write

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
このワークフローは、セキュリティインシデントの [カテゴリ] が [機密性の高い個人 **ID** データの公開] に設定または変更されたときにトリガーされます。このアクションにより、ワークフローの最初のアクティビティとして応答タスクが作成されます。

機密性の高い個人 **ID** データの公開



手順

1. 機密データへのエクスポージャーを処理するセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[機密性の高い個人 **ID** データの公開] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかフローが終了します。

機密データエクスポージャーテンプレートの応答タスク

応答タスク	説明	結果
データは機密ですか？(Is the data sensitive?)	このセキュリティインシデントに関連するデータに機密性または秘密性があるかどうかを判断します。タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、次の応答タスクが実行されます。 [いいえ] を選択すると、フローは終了します。
根本原因の特定とエグレスの防止 (Determine root cause and prevent egress)	攻撃の根本原因を特定し、エグレスフィルタリングを追加してデータ漏えいを停止し、必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	説明	結果
根本原因に関連するエクスポージャーの除去 (Eliminate exposure related to root cause)	根本原因に基づいて、エクスポージャーを除去する手順を実行し、必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。
残存アーティファクトの隔離 (Quarantine residual artifacts)	残存アーティファクトを隔離する手順を実行し、必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。
法務プロセス (Legal process)	この分析の法的要件を満たすための手順を実行し、必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。
PR プロセス (PR process)	この分析の PR 要件を満たすための手順を実行し、必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。
ステータスをレビューに設定 (Set state to review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)]** が自動的に [レビュー] に変更されます。
学んだ教訓に関するミーティング	反省会を開催し、この機密データに対して実行された作業をトリアージします。必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、タスクをクローズするまで、セキュリティインシデントは [レビュー] ステータスのままになります。

自動翻訳

セキュリティインシデントサービス拒否ワークフローテンプレート

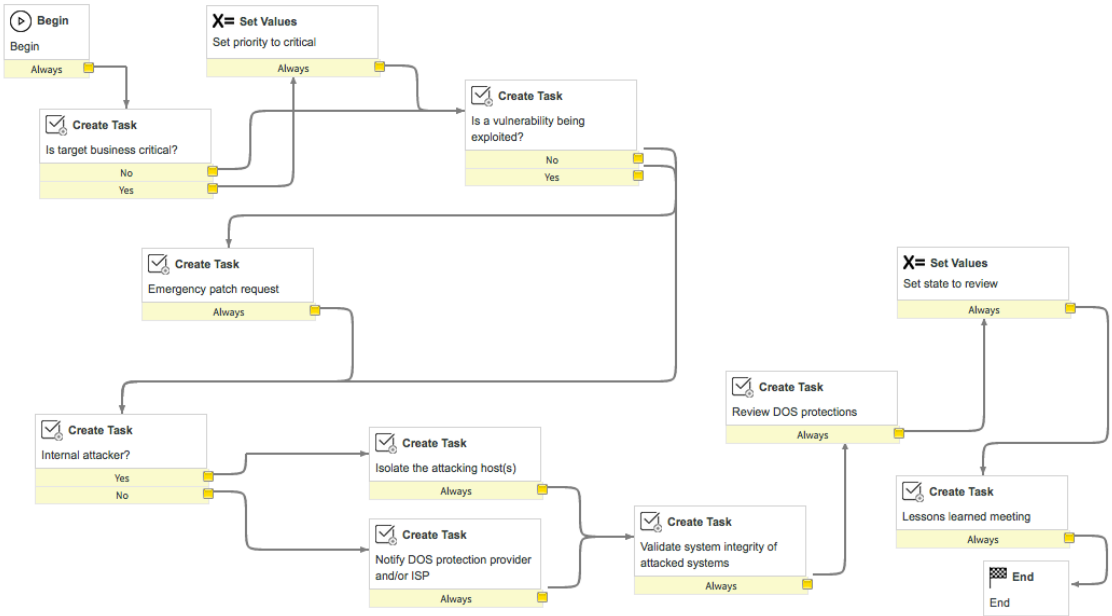
セキュリティインシデント - サービス拒否 - テンプレートを使用すると、サービス拒否 (DoS) 攻撃を処理するように設計された一連のタスクを実行できます。

始める前に
必要なロール：sn_si.write

このタスクについて
このワークフローは、セキュリティインシデントの [カテゴリ] が [サービス拒否] に設定された場合にトリガーされます。このアクションにより、ワークフローの最初のアクティビティとして応答タスクが作成されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サービス拒否 (DoS)



手順

1. このサービス拒否の事例のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[サービス拒否] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかフローが終了します。

サービス拒否テンプレートの応答タスク

応答タスク	アクション	結果
ターゲットはビジネスクリティカルですか？(Is target business critical?)	この DoS 攻撃のターゲットがビジネスクリティカルかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、[優先度を重要に設定 **(Set priority to critical)]** タスクが実行されます。 [いいえ] を選択した場合、[脆弱性は利用されていますか？**(Is a vulnerability being exploited?)]** タスクが実行されます。
優先度を重要に設定 (Set priority to critical)	アクションは要求されません。	セキュリティインシデントの [優先度] が自動的に [重要] に変更され、[脆弱性は利用されていますか？**(Is a vulnerability being exploited?)]** タスクが実行されます。
脆弱性は利用されていますか？(Is a vulnerability being exploited?)	この DoS 攻撃がソフトウェアの脆弱性を利用しているかどうかを判断します。	[はい] を選択すると、 [緊急パッチ要求 **(Emergency patch request)]** タスクが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
	タスク内の [結果] で [はい] または [いいえ] を選択します。	[いいえ] を選択すると、 [内部攻撃者？ **(Internal attacker?)]** タスクが実行されます。
緊急パッチ要求 (Emergency patch request)	攻撃されているシステムの緊急パッチ要求を発行します。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、次の応答タスクが実行されます。
内部攻撃者？ (Internal attacker?)	この DoS 攻撃の発信元が組織内であるかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、[攻撃ホストの隔離 **(Isolate attacking host(s))]** タスクが実行されます。 [いいえ] を選択すると、**[DoS** 保護プロバイダーや **ISP** に通知 **(Notify DOS protection provider and/or ISP)]** タスクが実行されます。
攻撃ホストを隔離 (Isolate the attacking host(s))	攻撃の原因となっている内部ホストを隔離するために必要な手順を実行します。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	この手順を完了すると、[攻撃されたシステムの整合性を検証 **(Validate system integrity of attacked systems)]** タスクが実行されます。
DoS 保護プロバイダーや ISP に通知 (Notify DOS protection provider and/or ISP)	サービス拒否保護プロバイダーまたはインターネットサービスプロバイダーに連絡して攻撃を通知するために必要な手順を実行します。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、次の応答タスクが実行されます。
攻撃されたシステムの整合性を検証 (Validate system integrity of attacked systems)	攻撃されたコンピューターの完全性を評価および検証するために必要な手順を実行します。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、次の応答タスクが実行されます。
DoS 保護のレビュー (Review DOS protections)	既存の DoS 保護および手順のレビューを実施します。必要な変更を行います。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、次の応答タスクが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
ステータスをレビューに設定 (Set state to review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)**] が、自動的に [レビュー] に変更されます。 [学んだ教訓に関するミーティング] タスクが実行されます。
学んだ教訓に関するミーティング	反省会を開催し、このサービス拒否インシデントに対して実行された作業をトリアージします。 必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、フローは終了します。

セキュリティインシデント - 失われた機器ワークフローテンプレート

セキュリティインシデント - 失われた機器 - テンプレートを使用すると、紛失した機器を処理するために設計された一連のタスクを実行できます。

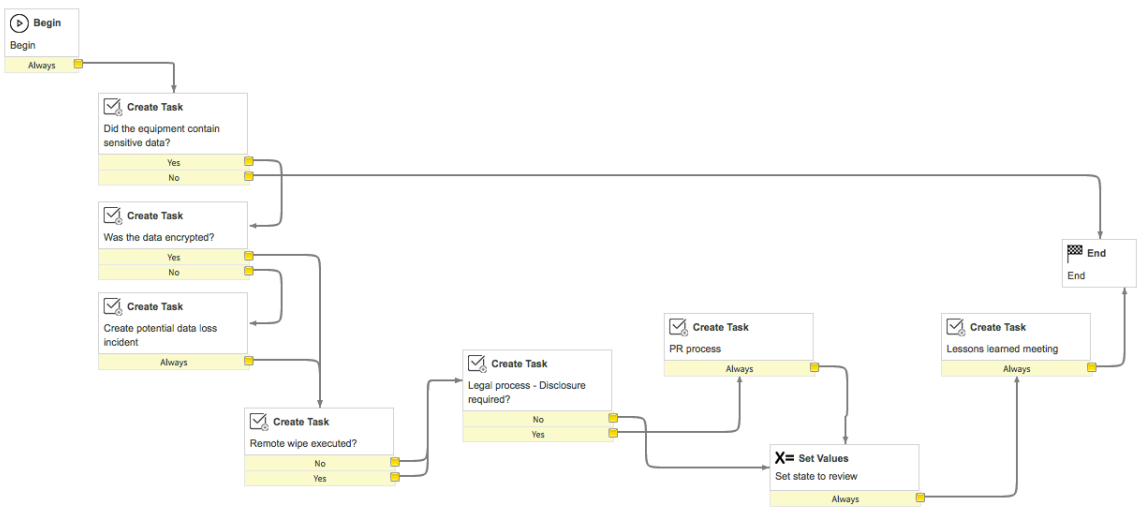
始める前に

必要なロール：sn_si.write

このタスクについて

このワークフローは、セキュリティインシデントの [カテゴリ] が [機器の損失] に設定された場合にトリガーされます。このアクションにより、ワークフローの最初のアクティビティとして応答タスクが作成されます。

機器の損失



手順

1. 機器の損失のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で [機器の損失] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかフローが終了します。

失われた機器テンプレートの応答タスク

応答タスク	アクション	結果
機器に機密データは含まれていましたか？(Did the equipment contain sensitive data?)	このセキュリティインシデントに関連する機器に何らかの機密/秘密情報が含まれていたかどうかを判断します。 必要に応じてタスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択した場合、[データは暗号化されていましたか？**(Was the data encrypted?)]** タスクが実行されます。 [いいえ] を選択すると、フローは終了します。
データは暗号化されていましたか？(Was the data encrypted?)	紛失したデバイスの機密データが暗号化されていたかどうかを判断します。 必要に応じてタスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、[リモートワイプを作成しましたか？**(Remote wipe created?)]** 応答タスクが実行されます。 [いいえ] を選択すると、[データ損失の可能性インシデントの作成 **(Create potential data loss incident)]** 応答タスクが実行されます。
データ損失の可能性インシデントの作成 (Create potential data loss incident)	データ損失の可能性インシデントを作成するために必要な手順を実行します。 完了したら、必要に応じてタスクのステータスを [完了] または [未完了] に設定します。	[リモートワイプを作成しましたか？**(Remote wipe created?)]** 応答タスクが実行されます。
リモートワイプを作成しましたか？(Remote wipe created?)	紛失した機器のリモートワイプを実行するために必要な手順を実行します。 必要に応じてタスク内の [結果] で [はい] または [いいえ] を選択します。	[法務プロセス - 開示が必要？**(Legal process - Disclosure required?)]** タスクが実行されます。
法務プロセス - 開示が必要？(Legal process - Disclosure required?)	この分析の法的要件を満たすための手順を実行します。 法的開示が必要な場合は [はい] を選択し、必要ない場合は [いいえ] を選択します。	[学んだ教訓に関するミーティング] タスクが実行されます。
PR プロセス (PR process)	この分析の PR 要件を満たすために必要な手順を実行します。 完了したら、必要に応じてタスクのステータスを [完了] または [未完了] に設定します。	[ステータスをレビューに設定 **(Set state to review)]** タスクが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
ステータスをレビューに設定 (Set state to review)	アクションは必要ありません。	セキュリティインシデントの [ステータス **(State)**] が、自動的に [レビュー] に変更されます。
学んだ教訓に関するミーティング	反省会を開催し、この失われた機器インシデントに対して実行された作業をトリアージします。 完了したら、必要に応じてタスクのステータスを [完了] または [未完了] に設定します。	フローが終了します。

セキュリティインシデント - 悪意のあるソフトウェアワークフローテンプレート

セキュリティインシデント - 悪意のあるソフトウェア - テンプレートを使用すると、ネットワーク上の悪意のあるソフトウェアを処理するように設計された一連のタスクを実行できます。

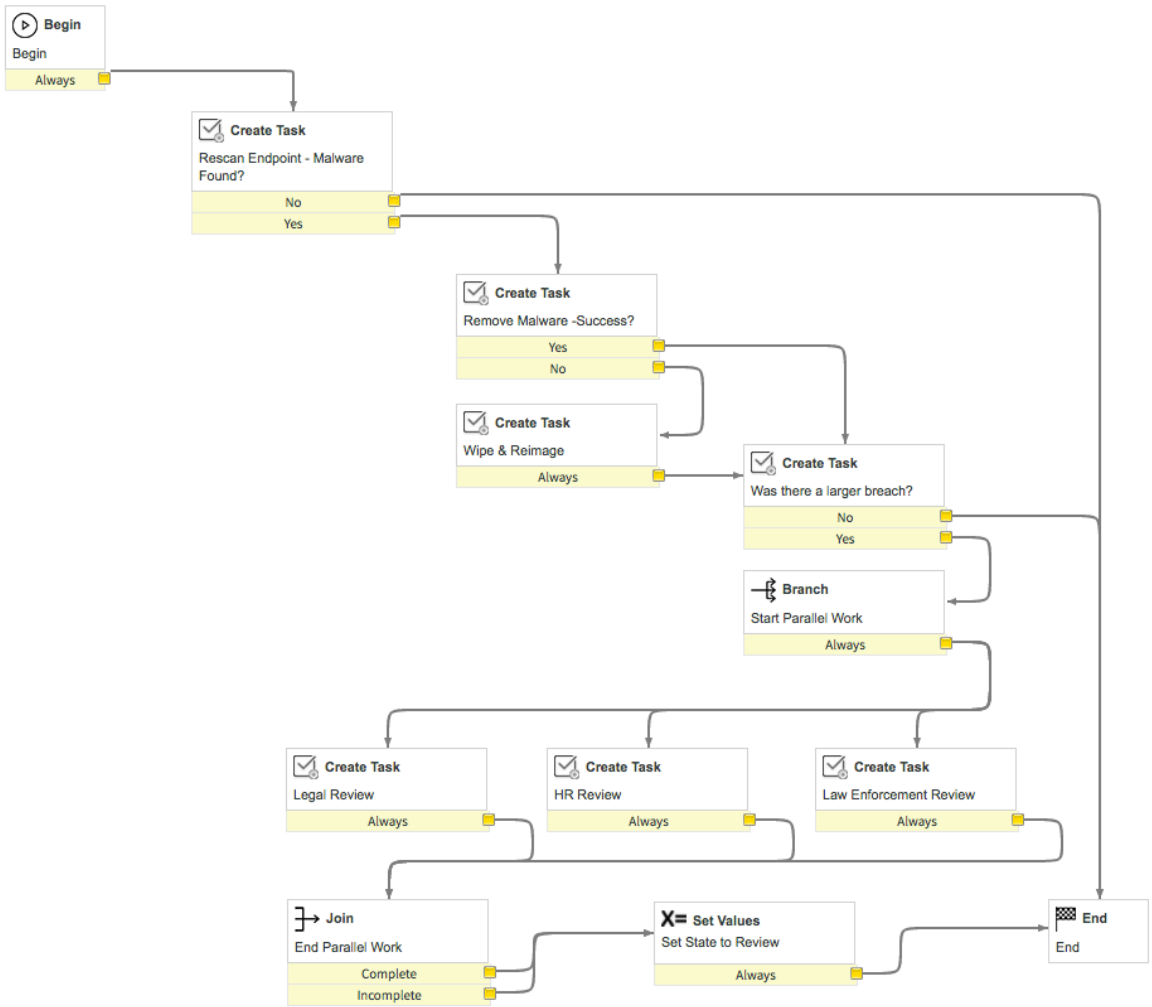
始める前に
必要なロール：sn_si.write

このタスクについて
このワークフローは、セキュリティインシデントの [カテゴリ] が [悪意のあるソフトウェア] に設定された場合にトリガーされます。このアクションにより、ワークフローの最初のアクティビティとして応答タスクが作成されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

悪意のあるソフトウェア



自動翻訳

手順

1. この潜在的な攻撃のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[悪意のあるコードアクティビティ] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかワークフローが終了します。

悪意のあるソフトウェアテンプレートの応答タスク

応答タスク	アクション	結果
スキャンエンドポイント - マルウェアは見つかりましたか？(Scan Endpoint - Malware Found?)	スキャンを実行した後、マルウェアが検出されたかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択した場合、[マルウェアの削除 - 成功？**(Remove Malware - Success?)**] タスクが実行されます。 [いいえ] を選択すると、フローは終了します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
マルウェアの削除 - 成功？(Remove Malware - Success?)	マルウェアが正常に削除されたかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、[大規模な侵害はありましたか？**(Was there a larger breach?)]** タスクが実行されます。 [いいえ] を選択すると、[ワイプと再イメージ化 **(Wipe & Reimage)]** タスクが実行されます。
ワイプと再イメージ化 (Wipe & Reimage)	検出されたマルウェアを正常に削除できなかった場合、このタスクは、マルウェアに感染したコンピューターのワイプと再イメージ化を実行するように指示します。	タスクが完了すると、[ステータスをレビューに設定 **(Set state to review)]** タスクが実行されます。
大規模な侵害がありましたか？(Was there a larger breach?)	悪意のあるソフトウェアによって発生した侵害が最初に考えられていたよりも大規模かどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、次のタスクが並行して実行されます。 ○ 法務レビュー ○ 人事レビュー (HR Review) ○ 法律の執行レビュー (Law Enforcement Review) [いいえ] を選択すると、フローは終了します。
法務レビュー 人事レビュー (HR Review) 法律の執行レビュー (Law Enforcement Review)	悪意のあるソフトウェアを除去するために実行したプロセスを、これらの各部門がレビューするために必要な手順を実行します。	タスクが完了すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
ステータスをレビューに設定 (Set State to Review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)]** が自動的に [レビュー] に変更され、フローが終了します。

セキュリティインシデント - フィッシングワークフローテンプレート

セキュリティインシデント - フィッシング - テンプレートを使用すると、ネットワーク上のスピアフィッシングメールを処理するように設計された一連のタスクを実行できます。

始める前に

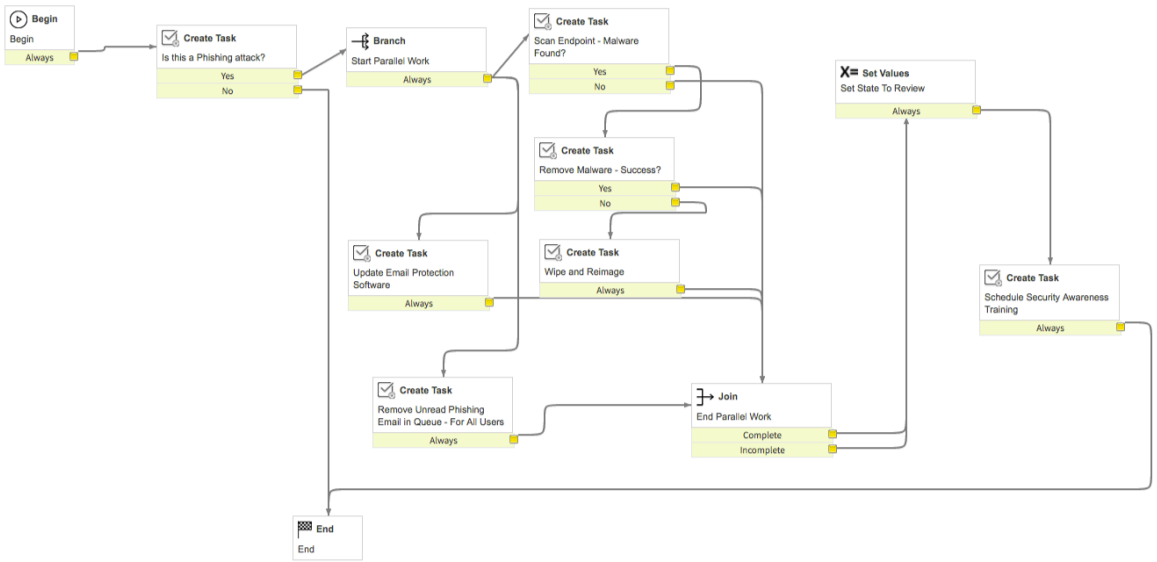
必要なロール：sn_si.write

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
このワークフローは、セキュリティインシデントの [カテゴリ] が [スピアフィッシング] に設定された場合にトリガーされます。このアクションにより、ワークフローの最初のアクティビティとして応答タスクが作成されます。

スピアフィッシング



手順

1. この潜在的なスピアフィッシング攻撃のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[スピアフィッシング] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかワークフローが終了します。

スピアフィッシングテンプレートの応答タスク

応答タスク	アクション	結果
これはフィッシング攻撃ですか？(Is this a Phishing attack?)	これがフィッシング攻撃かどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、次のタスクが並行して実行されます。 ○ スキャンエンドポイント - マルウェアは見つかりましたか？(Scan Endpoint - Malware Found?) ○ メール保護ソフトウェアの更新 (Update Email Protection Software) ○ キュー内の未読フィッシングメールの削除 - すべてのユーザー (Remove

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
		Unread Phishing Email in Queue - For All Users) [いいえ] を選択すると、フローは終了します。
スキャンエンドポイント - マルウェアは見つかりましたか？(Scan Endpoint - Malware Found?)	スキャンを実行した後、マルウェアが検出されたかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択した場合、[マルウェアの削除 - 成功？ **(Remove Malware - Success?)]** タスクが実行されます。 [いいえ] を選択すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
マルウェアの削除 - 成功？(Remove Malware - Success?)	マルウェアが正常に削除されたかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。 [いいえ] を選択すると、[ワイプと再イメージ化 **(Wipe and reimage)]** タスクが実行されます。
ワイプと再イメージ化 (Wipe and Reimage)	検出されたマルウェアを正常に削除できなかった場合、このタスクは、マルウェアに感染したコンピューターのワイプと再イメージ化を実行するように指示します。	タスクが完了すると、[ステータスをレビューに設定 **(Set state to review)]** タスクが実行されます。
メール保護ソフトウェアの更新 (Update Email Protection Software)	これがフィッシング攻撃であると判断された場合は、それに応じてメール保護ソフトウェアを更新するように求められます。	タスクが完了すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
キュー内の未読フィッシングメールの削除 - すべてのユーザー (Remove Unread Phishing Email in Queue - For All Users)	すべてのユーザーについて、まだキュー内にあるフィッシングメールを削除するために必要な手順を実行します。	タスクが完了すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
ステータスをレビューに設定 (Set State to Review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)]** が、自動的に [レビュー] に変更されます。 [セキュリティ認識向上トレーニングをスケジュール **(Schedule Security Awareness Training)]** タスクが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
セキュリティ認識向上トレーニングをスケジュール (Schedule Security Awareness Training)	従業員のセキュリティ認識を高めるためのトレーニングをスケジュールします。 必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクが完了すると、フローは終了します。

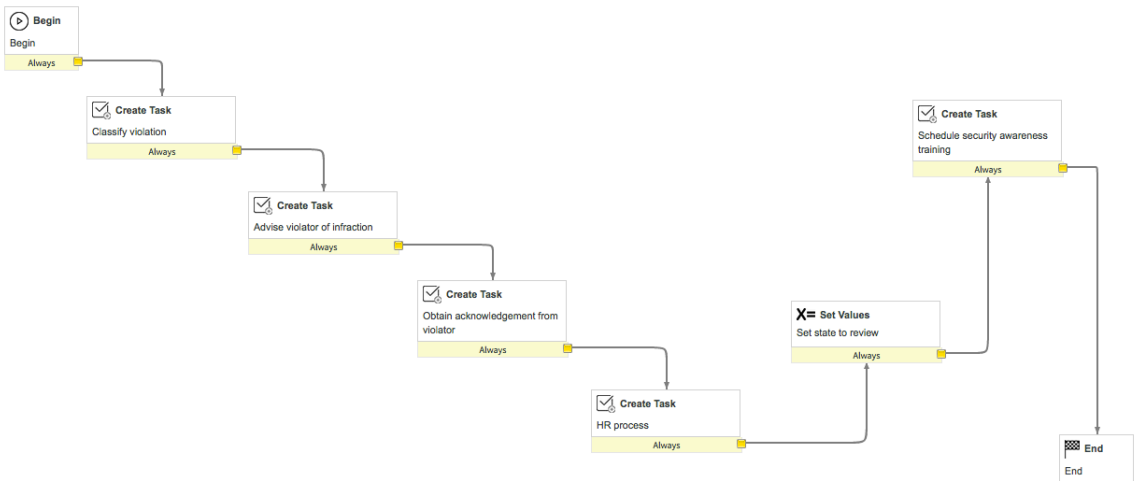
セキュリティインシデント - ポリシー違反ワークフローテンプレート

セキュリティインシデント - ポリシー違反 - テンプレートを使用すると、セキュリティポリシー違反を処理するために設計された一連のタスクを実行できます。

始める前に
必要なロール：sn_si.write

このタスクについて
このワークフローは、セキュリティインシデントの [カテゴリ] が [ポリシー違反] に設定された場合にトリガーされます。このアクションにより、ワークフローの最初のアクティビティとして応答タスクが作成されます。

ポリシー違反



手順

1. ポリシー違反のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で [ポリシー違反] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかワークフローが終了します。

ポリシー違反テンプレートの応答タスク

応答タスク	アクション	結果
違反の分類 (Classify violation)	この違反行為が組織のセキュリティポリシーにどのように違反しているかを分類します。	[違反者へのアドバイス **(Advise violator of**

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

応答タスク	アクション	結果
	完了したら、タスクの [ステータス **(State)]** フィールドを更新します。	**infraction)]** 応答タスクが実行されます。
違反者へのアドバイス (Advise violator of infraction)	違反行為の性質を違反者に伝えます。 伝達したら、タスクの [ステータス **(State)]** フィールドを更新します。	[違反者から確認を取る **(Obtain acknowledgement from violator)]** 応答タスクが実行されます。
違反者から確認を取る (Obtain acknowledgement from violator)	違反者から確認を取ります。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	**[HR** プロセス **(HR process)]** 応答タスクが実行されます。
HR プロセス (HR process)	この違反に関する必要なすべての情報を HR に伝えます。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	[ステータスをレビューに設定 **(Set state to review)]** 応答タスクが実行されます。
ステータスをレビューに設定 (Set state to review)	アクションは必要ありません。	セキュリティインシデントの [ステータス **(State)]** が、自動的に [レビュー] に変更されます。
セキュリティ認識向上トレーニングをスケジュール (Schedule security awareness training)	今後類似のセキュリティ違反を防ぐ方法について、スタッフを教育するセキュリティ認識向上トレーニングを実施します。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、フローは終了します。

自動翻訳

セキュリティインシデント - 偵察ワークフローテンプレート

偵察は通常、デバイスまたはシステムのエクスプロイトが目的の攻撃を進めるための準備段階です。セキュリティインシデント - 偵察 - テンプレートを使用すると、ネットワーク上の偵察を処理するように設計された一連のタスクを実行できます。

始める前に

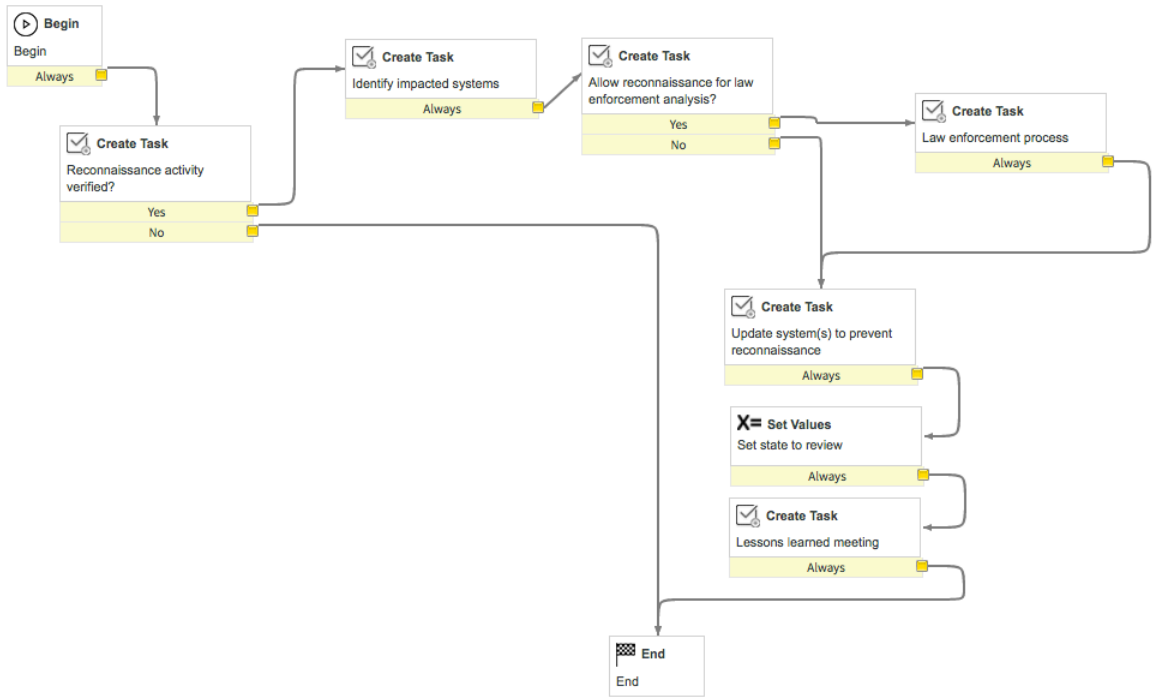
必要なロール：sn_si.write

このタスクについて

このワークフローは、セキュリティインシデントの [カテゴリ] が [偵察アクティビティ **(Reconnaissance activity)]** に設定された場合にトリガーされます。このアクションにより、ワークフローの最初のアクティビティとして応答タスクが作成されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

踏査アクティビティ



手順

1. この潜在的な攻撃のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[偵察アクティビティ **(Reconnaissance activity)]** を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかワークフローが終了します。

偵察テンプレートの応答タスク

応答タスク	アクション	結果
偵察アクティビティは検証されましたか？(Reconnaissance activity verified?)	観測された偵察が検証されているかどうかを確認します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、[影響を受けるシステムの特定 **(Identify impacted systems)]** タスクが実行されます。 [いいえ] を選択すると、フローは終了します。
影響を受けるシステムの特定 (Identify impacted systems)	偵察の影響を受けるシステムを特定します。	このタスクが完了すると、 [法執行機関による偵察の分析を許可しますか？**(Allow reconnaissance for law enforcement analysis?)]** タスクが実行されます。
法執行機関による偵察の分析を許可しますか？(Allow reconnaissance for law enforcement analysis?)	法執行機関に偵察の分析を依頼するかどうかを決定します。	[はい] を選択すると、[法律の執行プロセス **(Law enforcement process)]** タスクが実行されます。 [いいえ] を選択すると、[システムを更新して偵察を防止 **(Update system(s) to**

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
	タスク内の [結果] で [はい] または [いいえ] を選択します。	**prevent reconnaissance)]** タスクが実行されます。
法律の執行プロセス (Law enforcement process)	会社で定義されている法律の執行プロセスを実行します。	このタスクが完了すると、[システムを更新して偵察を防止 **(Update system(s) to prevent reconnaissance)]** タスクが実行されます。
システムを更新して偵察を防止 (Update system(s) to prevent reconnaissance)	偵察の影響を受けるシステムを更新するために必要な手順を実行します。	このタスクが完了すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
ステータスをレビューに設定 (Set state to review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)]** が自動的に [レビュー] に変更され、[学んだ教訓に関するミーティング] タスクが実行されます。
学んだ教訓に関するミーティング	反省会を開催し、この偵察インシデントに対して実行された作業をトリアージします。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	このタスクが完了すると、フローは終了します。

自動翻訳

セキュリティインシデント - 不正サーバーまたはサービスワークフローテンプレート

セキュリティインシデント - 不正サーバーまたはサービス - テンプレートを使用すると、ネットワークに影響を与える不正なサーバーやサービスからのアクティビティの処理用に設計された一連のタスクを実行できます。

始める前に

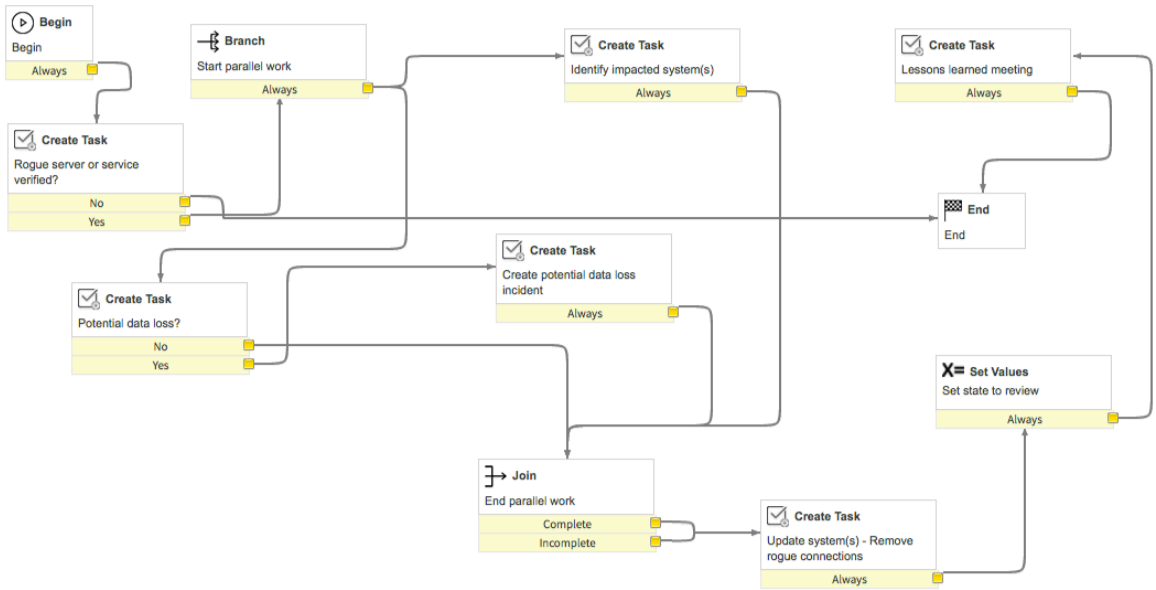
必要なロール：sn_si.write

このタスクについて

このワークフローは、セキュリティインシデントの [カテゴリ] が [不正サーバーまたはサービス] に設定された場合にトリガーされます。このアクションにより、ワークフローの最初のアクティビティとして応答タスクが作成されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

不正サーバーまたはサービス



手順

1. この潜在的な攻撃のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[不正サーバーまたはサービスアクティビティ **(Rogue server or service activity)**] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかワークフローが終了します。

不正サーバーまたはサービステンプレートの応答タスク

応答タスク	アクション	結果
不正サーバーまたはサービスは検証されましたか？(Rogue server or service verified?)	不正サーバーまたはサービスとの接続がネットワーク上で検証されているかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、次の 2 つのタスクが並行して実行されます。 ○ 影響を受けるシステムの特定 **(Identify impacted system(s))** ○ データ損失の可能性？**(Potential data loss?)** [いいえ] を選択すると、フローは終了します。
影響を受けるシステムの特定 (Identify impacted system(s))	不正サーバーまたはサービスとの接触によって影響を受けるシステムを特定します。	このタスクが完了すると、[システムの更新 - 不正接続の削除 **(Update system(s) - Remove rogue connections)**] タスクが実行されます。
データ損失の可能性？(Potential data loss?)	不正サーバーまたはサービスとの接続が原因でデータ損失が発生したかどうかを判断します。	[はい] を選択すると、[データ損失の可能性インシデントの作成 **(Create potential data loss incident)**] タスクが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
	タスク内の [結果] で [はい] または [いいえ] を選択します。	[いいえ] を選択すると、[システムの更新 - 不正接続の削除 **(Update system(s) - Remove rogue connections)]** タスクが実行されます。
データ損失の可能性インシデントの作成 (Create potential data loss incident)	データ損失の可能性のセキュリティインシデントを作成するために必要な手順を実行します。	このタスクが完了すると、[システムの更新 - 不正接続の削除 **(Update system(s) - Remove rogue connections)]** タスクが実行されます。
システムの更新 - 不正接続の削除 (Update system(s) - Remove rogue connections)	不正接続を削除するために必要な手順を実行します。	このタスクが完了すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
ステータスをレビューに設定 (Set state to review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)]** が自動的に [レビュー] に変更され、[学んだ教訓に関するミーティング] タスクが実行されます。
学んだ教訓に関するミーティング	反省会を開催し、この不正サーバーまたはサービスインシデントに対して実行された作業をトリアージします。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	このタスクが完了すると、フローは終了します。

セキュリティインシデント - スパムワークフローテンプレート

セキュリティインシデント - スパム - テンプレートを使用すると、ネットワーク上のメールスパムを処理するように設計された一連のタスクを実行できます。

始める前に

必要なロール：sn_si.write

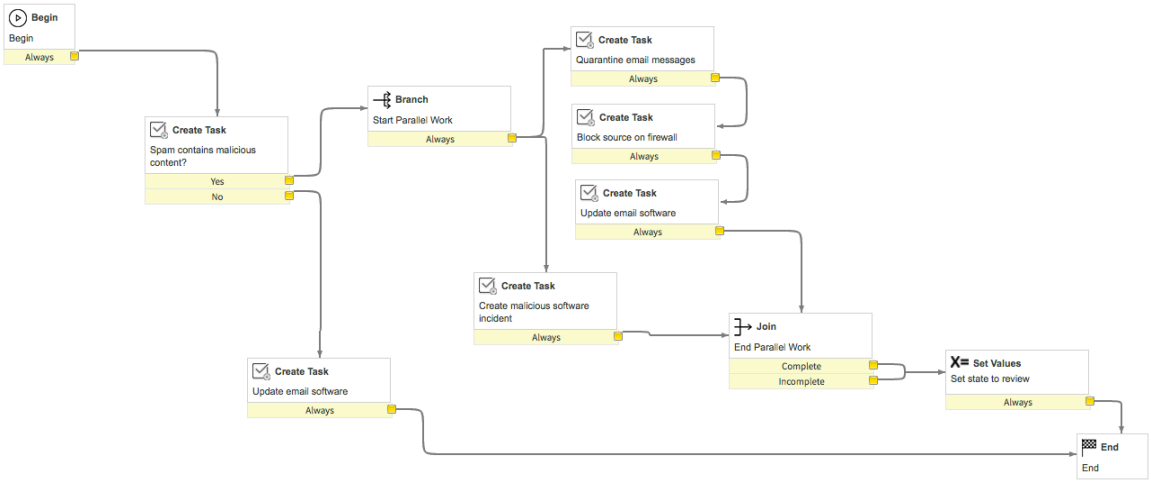
このタスクについて

このワークフローは、セキュリティインシデントの [カテゴリ] が [スパムソース] に設定または変更された場合にトリガーされます。このアクションにより、ワークフローの最初のアクティビティとして応答タスクが作成されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スパムソース



手順

1. スパムメールを処理するセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[スパムソース] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかワークフローが終了します。

スパムテンプレートの応答タスク

応答タスク	アクション	結果
スパムに悪意のあるコンテンツは含まれていますか？ (Spam contains malicious content?)	スパムに悪意のあるソフトウェアが含まれているかどうかを判断します。タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、次の応答タスクが実行されます。 ○ メールメッセージの隔離 **(Quarantine email message)** ○ 悪意のあるソフトウェアインシデントの作成 **(Create malicious software incident)** [いいえ] を選択すると、[メールソフトウェアの更新 **(Update email software)**] が実行されます。
悪意のあるソフトウェアインシデントの作成 (Create malicious software incident)	セキュリティインシデントを作成する手順を実行し、必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、この応答タスクは、次の 3 つの応答タスクが完了するまで待機します。その後、セキュリティインシデントのステータスは [レビュー] に移行します。
メールメッセージの隔離 (Quarantine email message)	スパムを隔離する手順を実行し、必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
ファイアウォールでソースをブロック (Block source on firewall)	ファイアウォールでメールアドレスをブロックする手順を実行し、必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。
メールソフトウェアの更新 (Update email software)	メールアドレスをブロックリストに追加し、必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。 **注:** この応答タスクは、[スパムに悪意のあるコンテンツは含まれていますか？**(Spam contains malicious content?)]** 応答タスクに [いいえ] と回答した場合も実行されます。
ステータスをレビューに設定 (Set state to review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)]** が自動的に [レビュー] に変更されます。

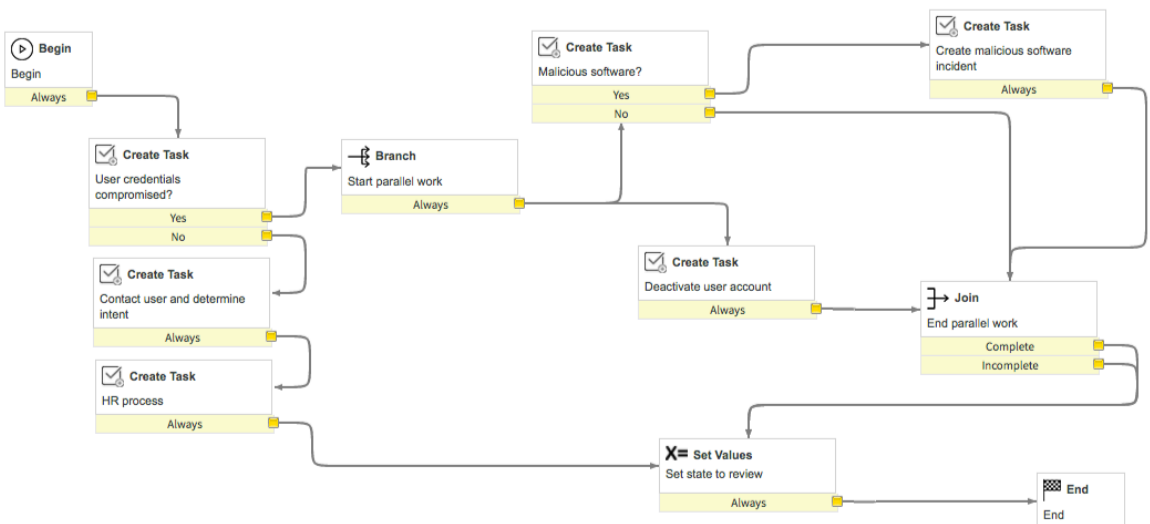
セキュリティインシデント - 無許可のアクセスワークフローテンプレート

セキュリティインシデント - 無許可のアクセス - テンプレートを使用すると、ネットワークに対する不正アクセスを処理するように設計された一連のタスクを実行できます。

始める前に
必要なロール：sn_si.write

このタスクについて
このワークフローは、セキュリティインシデントの [カテゴリ] が [無許可のアクセス] に設定された場合にトリガーされます。このアクションにより、ワークフローの最初のアクティビティとして応答タスクが作成されます。

無許可のアクセス



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. この潜在的な攻撃のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[無許可のアクセス] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかワークフローが終了します。

不正アクセステンプレートの応答タスク

応答タスク	アクション	結果
ユーザーの認証情報は侵害されましたか？ (User credentials compromised?)	ユーザーの認証情報が侵害されているかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、次の 2 つのタスクが並行して実行されます。 ○ 悪意のあるソフトウェア？ **(Malicious Software?)** ○ ユーザーアカウントの非アクティブ化 **(Deactivate user account)** [いいえ] を選択すると、[ユーザーに連絡して意図を確認 **(Contact user and determine intent)]** タスクが実行されます。
悪意のあるソフトウェア？(Malicious Software?)	不正アクセスによって悪意のあるソフトウェアが導入されたかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、[悪意のあるソフトウェアインシデントの作成 **(Create malicious software incident)]** タスクが実行されます。 [いいえ] を選択すると、[ステータスをレビューに設定 **(Set state to review)]** タスクが実行されます。
悪意のあるソフトウェアインシデントの作成 (Create malicious software incident)	不正アクセスのセキュリティインシデントを作成するために必要な手順を実行します。	このタスクが完了すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
ユーザーアカウントの非アクティブ化 (Deactivate user account)	侵害されたユーザーアカウントを非アクティブにするために必要な手順を実行します。	このタスクが完了すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
ユーザーに連絡して意図を確認 (Contact user and determine intent)	不正アクセスを行ったユーザーに連絡し、アクセスを試みた理由を確認するために必要な手順を実行します。	このタスクが完了すると、**[HR** プロセス **(HR process)]** タスクが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
HR プロセス (HR process)	人事に連絡して必要に応じて懲戒処分を実施するために必要な手順を実行します。	このタスクが完了すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
ステータスをレビューに設定 (Set state to review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)]** が自動的に [レビュー] に変更され、フローが終了します。

セキュリティインシデント - **Web/BBS** の改ざんワークフローテンプレート

セキュリティインシデント - Web/BBS の改ざん - テンプレートを使用すると、組織の BBS または Web サイトのいずれかに向けられた破壊行為を処理するように設計された一連のタスクを実行できます。

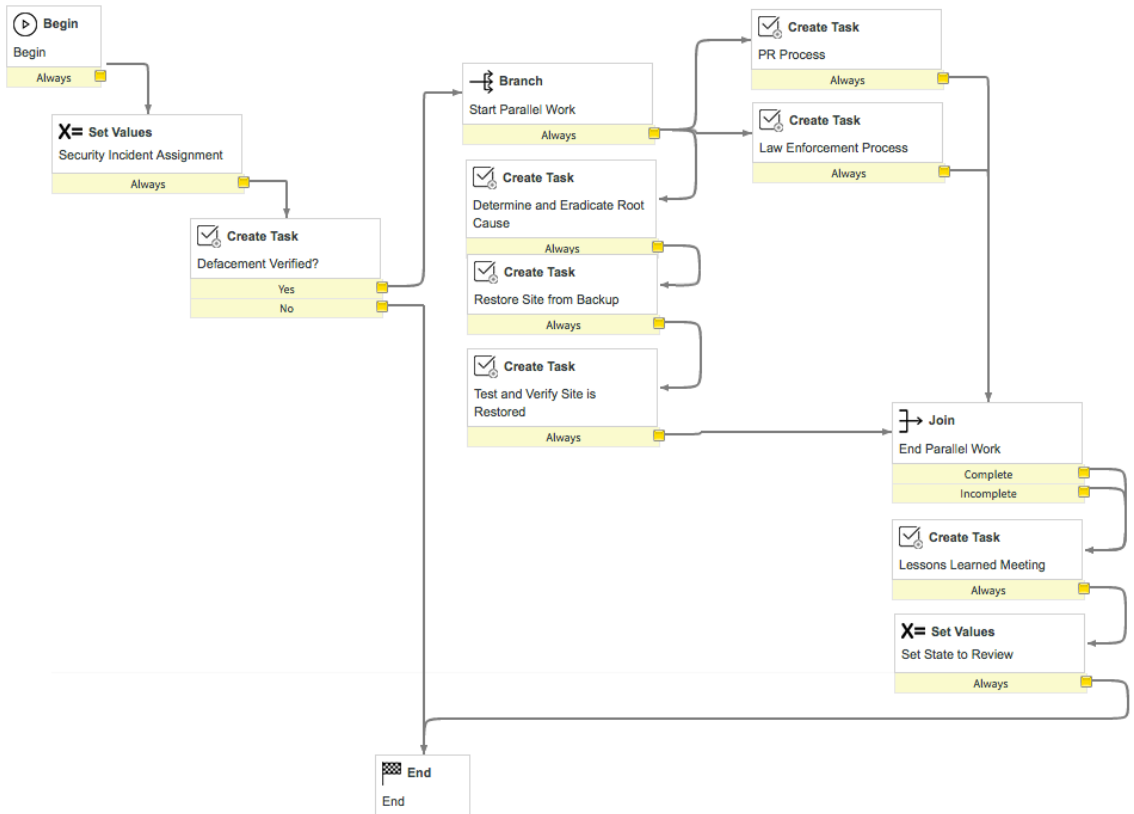
始める前に

必要なロール：sn_si.write

このタスクについて

このワークフローは、セキュリティインシデントの [カテゴリ] が **[Web/BBS** の改ざん] に設定された場合にトリガーされます。このアクションにより、ワークフローの最初のアクティビティとして応答タスクが作成されます。

Web/BBS の改ざん



手順

1. この Web または BBS の改ざんの事例のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、**[Web/BBS** の改ざん] を選択します。
3. レコードを保存します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

4. 下にスクロールして、[応答タスク] 関連リストを開きます。
一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかワークフローが終了します。

Web/BBS 改ざんテンプレートの応答タスク

応答タスク	アクション	結果
セキュリティインシデントアサイン	Web サイトまたは BBS の改ざんが報告された各インシデントのセキュリティインシデントを作成します。	次の応答タスクが実行されます。
改ざんは検証されていますか？ (Defacement verified?)	Web サイトまたは BBS が実際に改ざんされているかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、次の応答タスクが実行されます。 ○ **PR プロセス (PR process)** ○ 法律の執行プロセス **(Law enforcement process)** ○ 根本原因の特定と除去 **(Determine and eradicate root cause)** [いいえ] を選択すると、フローは終了します。
PR プロセス (PR process)	Web サイトまたは BBS が改ざんされたことを一般に通知するために必要な手順を実行します。 PR プロセスが完了したら、必要に応じてタスクのステータスを [完了] または [未完了] に設定します。	[学んだ教訓に関するミーティング] タスクが実行されます。
法律の執行プロセス (Law enforcement process)	攻撃に関して適切な法執行機関を関与させるために必要な手順を実行します。 完了したら、必要に応じてタスクのステータスを [完了] または [未完了] に設定します。	[学んだ教訓に関するミーティング] タスクが実行されます。
根本原因の特定と除去 (Determine and eradicate root cause)	改ざんの根本原因を発見して除去するために必要な手順を実行します。 必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、次の応答タスクが実行されます。
バックアップからサイトを復元 (Restore site from backup)	Web サイトまたは BBS のバックアップと復元に必要な手順を実行します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、次の応答タスクが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
	必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	
サイト復元のテストと検証 (Test and verify site is restored)	サイトが復元されたことを検証します。 完了したら、必要に応じてタスクのステータスを [完了] または [未完了] に設定します。	[学んだ教訓に関するミーティング] タスクが実行されます。
学んだ教訓に関するミーティング	反省会を開催し、この Web サイト/BBS 改ざんインシデントに対して実行された作業をトリアージします。 必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル]に変更すると、[ステータスをレビューに設定 **(Set state to review)**] タスクが実行されます。
ステータスをレビューに設定 (Set state to review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)**] が、自動的に [レビュー] に変更されます。 フローが終了します。

セキュリティインシデントレスポンスフローテンプレート

セキュリティインシデントレスポンス ベースシステムには、フローデザイナーを使用して作成され、セキュリティインシデントレコードと連携する一連のワークフローテンプレートが含まれています。

sn_sec_cmn.admin ロールを持つユーザーのみが Security Operations ワークフローテンプレートを追加または編集できます。また、フローテンプレートの更新には、sn_si_admin ロールを持つユーザーが必要です。

アクティブ化に関する重要な情報

ワークフローエディターで作成されたワークフローテンプレートとフローデザイナーで作成されたフローテンプレートは、デフォルトではどちらも非アクティブになっています。ワークフローテンプレートは、ワークフロートリガーを使用してアクティブ化できます。フローデザイナーテンプレートは、フローデザイナーを使用してアクティブ化できます。

注:
両方のタイプで同じテンプレートをアクティブ化しないように注意してください。たとえば、セキュリティインシデント機密データエクスポージャーワークフローテンプレートとセキュリティインシデント機密データエクスポージャーフローテンプレートを両方アクティブ化しないでください。これを行うと、ワークフローとフローの両方が実行され、重複する情報が作成されます。

セキュリティインシデント機密データエクスポージャーフローテンプレート

セキュリティインシデント - 機密データエクスポージャー - テンプレートを使用すると、機密データエクスポージャーを処理するために設計された一連のタスクを実行できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_si.write

このタスクについて
このフローは、セキュリティインシデントの [カテゴリ] が [機密性の高い個人 **ID** データの公開] に設定または変更されたときにトリガーされます。

手順

1. 機密データへのエクスポージャーを処理するセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[機密性の高い個人 **ID** データの公開] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが実行されるかフローが終了します。

機密データエクスポージャーテンプレートの応答タスク

応答タスク	説明	結果
データは機密ですか？(Is the data sensitive?)	このセキュリティインシデントに関連するデータに機密性または秘密性があるかどうかを判断します。タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、次の応答タスクが実行されます。 [いいえ] を選択すると、フローは終了します。
根本原因の特定とエグレスの防止 (Determine root cause and prevent egress)	攻撃の根本原因を特定し、エグレスフィルタリングを追加してデータ漏えいを停止し、必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。
根本原因に関連するエクスポージャーの除去 (Eliminate exposure related to root cause)	根本原因に基づいて、エクスポージャーを除去する手順を実行し、必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。
残存アーティファクトの隔離 (Quarantine residual artifacts)	残存アーティファクトを隔離する手順を実行し、必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。
法務プロセス (Legal process)	この分析の法的要件を満たすための手順を実行し、必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。
PR プロセス (PR process)	この分析の PR 要件を満たすための手順を実行し、必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	説明	結果
ステータスをレビューに設定 (Set state to review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)**] が自動的に [レビュー] に変更されます。
学んだ教訓に関するミーティング	反省会を開催し、この機密データに対して実行された作業をトリアージします。必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、タスクをクローズするまで、セキュリティインシデントは [レビュー] ステータスのままになります。

セキュリティインシデントサービス拒否フローテンプレート

セキュリティインシデント - サービス拒否 - テンプレートを使用すると、サービス拒否 (DoS) 攻撃を処理するように設計された一連のタスクを実行できます。

始める前に
必要なロール：sn_si.write

このタスクについて
このフローは、セキュリティインシデントの [カテゴリ] が [サービス拒否] に設定された場合にトリガーされます。

手順

1. このサービス拒否の事例のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[サービス拒否] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかワークフローが終了します。

サービス拒否テンプレートの応答タスク

応答タスク	アクション	結果
ターゲットはビジネスクリティカルですか？(Is target business critical?)	この DoS 攻撃のターゲットがビジネスクリティカルかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、[優先度を重要に設定 **(Set priority to critical)**] タスクが実行されます。 [いいえ] を選択した場合、[脆弱性は利用されていますか？**(Is a vulnerability being exploited?)**] タスクが実行されます。
優先度を重要に設定 (Set priority to critical)	アクションは要求されません。	セキュリティインシデントの [優先度] が自動的に [重要] に変更され、[脆弱性は利用されていますか？**(Is a vulnerability being exploited?)**] タスクが実行されます。
脆弱性は利用されていますか？(Is a	この DoS 攻撃がソフトウェアの脆弱性を利用しているかどうかを判断します。	[はい] を選択すると、 [緊急パッチ要求 **(Emergency patch request)**] タスクが実行されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

応答タスク	アクション	結果
vulnerability being exploited?)	タスク内の [結果] で [はい] または [いいえ] を選択します。	[いいえ] を選択すると、 [内部攻撃者？ **(Internal attacker?)]** タスクが実行されます。
緊急パッチ要求 (Emergency patch request)	攻撃されているシステムの緊急パッチ要求を発行します。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、次の応答タスクが実行されます。
内部攻撃者？ (Internal attacker?)	この DoS 攻撃の発信元が組織内であるかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、[攻撃ホストの隔離 **(Isolate attacking host(s))]** タスクが実行されます。 [いいえ] を選択すると、**[DoS** 保護プロバイダーや **ISP** に通知 **(Notify DOS protection provider and/or ISP)]** タスクが実行されます。
攻撃ホストを隔離 (Isolate the attacking host(s))	攻撃の原因となっている内部ホストを隔離するために必要な手順を実行します。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	この手順を完了すると、[攻撃されたシステムの整合性を検証 **(Validate system integrity of attacked systems)]** タスクが実行されます。
DoS 保護プロバイダーや ISP に通知 (Notify DOS protection provider and/or ISP)	サービス拒否保護プロバイダーまたはインターネットサービスプロバイダーに連絡して攻撃を通知するために必要な手順を実行します。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、次の応答タスクが実行されます。
攻撃されたシステムの整合性を検証 (Validate system integrity of attacked systems)	攻撃されたコンピューターの完全性を評価および検証するために必要な手順を実行します。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、次の応答タスクが実行されます。
DoS 保護のレビュー (Review DOS protections)	既存の DoS 保護および手順のレビューを実施します。必要な変更を行います。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、次の応答タスクが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
ステータスをレビューに設定 (Set state to review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)**] が、自動的に [レビュー] に変更されます。 [学んだ教訓に関するミーティング] タスクが実行されます。
学んだ教訓に関するミーティング	反省会を開催し、このサービス拒否インシデントに対して実行された作業をトリアージします。 必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、フローは終了します。

セキュリティインシデント - 失われた機器フローテンプレート

セキュリティインシデント - 失われた機器 - テンプレートを使用すると、紛失した機器を処理するために設計された一連のタスクを実行できます。

始める前に
必要なロール：sn_si.write

このタスクについて
このフローは、セキュリティインシデントの [カテゴリ] が [機器の損失] に設定された場合にトリガーされます。

手順

1. このサービス拒否の事例のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で [機器の損失] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかフローが終了します。

失われた機器テンプレートの応答タスク

応答タスク	アクション	結果
機器に機密データは含まれていましたか？(Did the equipment contain sensitive data?)	このセキュリティインシデントに関連する機器に何らかの機密/秘密情報が含まれていたかどうかを判断します。 必要に応じてタスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択した場合、[データは暗号化されていましたか？**(Was the data encrypted?)**] タスクが実行されます。 [いいえ] を選択すると、フローは終了します。
データは暗号化されていましたか？(Was the data encrypted?)	紛失したデバイスの機密データが暗号化されていたかどうかを判断します。	[はい] を選択すると、[リモートワイプを作成しましたか？**(Remote wipe**

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
	必要に応じてタスク内の [結果] で [はい] または [いいえ] を選択します。	**created?)]** 応答タスクが実行されます。 [いいえ] を選択すると、[データ損失の可能性インシデントの作成 **(Create potential data loss incident)]** 応答タスクが実行されます。
データ損失の可能性インシデントの作成 (Create potential data loss incident)	データ損失の可能性インシデントを作成するために必要な手順を実行します。 完了したら、必要に応じてタスクのステータスを [完了] または [未完了] に設定します。	[リモートワイプを作成しましたか？ **(Remote wipe created?)]** 応答タスクが実行されます。
リモートワイプを作成しましたか？(Remote wipe created?)	紛失した機器のリモートワイプを実行するために必要な手順を実行します。 必要に応じてタスク内の [結果] で [はい] または [いいえ] を選択します。	[法務プロセス - 開示が必要？ **(Legal process - Disclosure required?)]** タスクが実行されます。
法務プロセス - 開示が必要？(Legal process - Disclosure required?)	この分析の法的要件を満たすための手順を実行します。 法的開示が必要な場合は [はい] を選択し、必要ない場合は [いいえ] を選択します。	[学んだ教訓に関するミーティング] タスクが実行されます。
PR プロセス (PR process)	この分析の PR 要件を満たすために必要な手順を実行します。 完了したら、必要に応じてタスクのステータスを [完了] または [未完了] に設定します。	[ステータスをレビューに設定 **(Set state to review)]** タスクが実行されます。
ステータスをレビューに設定 (Set state to review)	アクションは必要ありません。	セキュリティインシデントの [ステータス **(State)]** が、自動的に [レビュー] に変更されます。
学んだ教訓に関するミーティング	反省会を開催し、この失われた機器インシデントに対して実行された作業をトリアージします。 完了したら、必要に応じてタスクのステータスを [完了] または [未完了] に設定します。	フローが終了します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデント - 悪意のあるソフトウェアフローテンプレート

セキュリティインシデント - 悪意のあるソフトウェア - テンプレートを使用すると、ネットワーク上の悪意のあるソフトウェアを処理するように設計された一連のタスクを実行できます。

始める前に

必要なロール：sn_si.write

このタスクについて

このフローは、セキュリティインシデントの [カテゴリ] が [悪意のあるコードアクティビティ] に設定された場合にトリガーされます。

手順

1. この潜在的な攻撃のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[悪意のあるコードアクティビティ] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかフローが終了します。

悪意のあるソフトウェアテンプレートの応答タスク

応答タスク	アクション	結果
スキャンエンドポイント - マルウェアは見つかりましたか？(Scan Endpoint - Malware Found?)	スキャンを実行した後、マルウェアが検出されたかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択した場合、[マルウェアの削除 - 成功？**(Remove Malware - Success?)**] タスクが実行されます。 [いいえ] を選択すると、フローは終了します。
マルウェアの削除 - 成功？(Remove Malware - Success?)	マルウェアが正常に削除されたかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、[大規模な侵害はありましたか？**(Was there a larger breach?)**] タスクが実行されます。 [いいえ] を選択すると、[ワイプと再イメージ化 **(Wipe & Reimage)**] タスクが実行されます。
ワイプと再イメージ化 (Wipe & Reimage)	検出されたマルウェアを正常に削除できなかった場合、このタスクは、マルウェアに感染したコンピューターのワイプと再イメージ化を実行するように指示します。	タスクが完了すると、[ステータスをレビューに設定 **(Set state to review)**] タスクが実行されます。
大規模な侵害がありましたか？(Was there a larger breach?)	悪意のあるソフトウェアによって発生した侵害が最初に考えられていたよりも大規模かどうかを判断します。	[はい] を選択すると、次のタスクが並行して実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
	タスク内の [結果] で [はい] または [いいえ] を選択します。	○ 法務レビュー ○ 人事レビュー (HR Review) ○ 法律の執行レビュー (Law Enforcement Review) [いいえ] を選択すると、フローは終了します。
法務レビュー 人事レビュー (HR Review) 法律の執行レビュー (Law Enforcement Review)	悪意のあるソフトウェアを除去するために実行したプロセスを、これらの各部門がレビューするために必要な手順を実行します。	タスクが完了すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
ステータスをレビューに設定 (Set State to Review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)]** が自動的に [レビュー] に変更され、フローが終了します。

セキュリティインシデント - フィッシングフローテンプレート

セキュリティインシデント - フィッシング - テンプレートを使用すると、ネットワーク上のスピアフィッシングメールを処理するように設計された一連のタスクを実行できます。

始める前に

必要なロール：sn_si.write

このタスクについて

このフローは、セキュリティインシデントの [カテゴリ] が [スピアフィッシング] に設定された場合にトリガーされます。

手順

1. この潜在的なスピアフィッシング攻撃のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[スピアフィッシング] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかフローが終了します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スピアフィッシングテンプレートの応答タスク

応答タスク	アクション	結果
これはフィッシング攻撃ですか？(Is this a Phishing attack?)	これがフィッシング攻撃かどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、次のタスクが並行して実行されます。 ○ スキャンエンドポイント - マルウェアは見つかりましたか？(Scan Endpoint - Malware Found?) ○ メール保護ソフトウェアの更新 (Update Email Protection Software) ○ キュー内の未読フィッシングメールの削除 - すべてのユーザー (Remove Unread Phishing Email in Queue - For All Users) [いいえ] を選択すると、フローは終了します。
スキャンエンドポイント - マルウェアは見つかりましたか？(Scan Endpoint - Malware Found?)	スキャンを実行した後、マルウェアが検出されたかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択した場合、[マルウェアの削除 - 成功？ **(Remove Malware - Success?)]** タスクが実行されます。 [いいえ] を選択すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
マルウェアの削除 - 成功？(Remove Malware - Success?)	マルウェアが正常に削除されたかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。 [いいえ] を選択すると、[ワイプと再イメージ化 **(Wipe and reimage)]** タスクが実行されます。
ワイプと再イメージ化 (Wipe and Reimage)	検出されたマルウェアを正常に削除できなかった場合、このタスクは、マルウェアに感染したコンピューターのワイプと再イメージ化を実行するように指示します。	タスクが完了すると、[ステータスをレビューに設定 **(Set state to review)]** タスクが実行されます。
メール保護ソフトウェアの更新 (Update Email Protection Software)	これがフィッシング攻撃であると判断された場合は、それに応じてメー	タスクが完了すると、[ステータスをレビューに設定

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
	ル保護ソフトウェアを更新するように求められます。	**(Set State to Review)]** タスクが実行されます。
キュー内の未読フィッシングメールの削除 - すべてのユーザー (Remove Unread Phishing Email in Queue - For All Users)	すべてのユーザーについて、まだキュー内にあるフィッシングメールを削除するために必要な手順を実行します。	タスクが完了すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
ステータスをレビューに設定 (Set State to Review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)]** が、自動的に [レビュー] に変更されます。 [セキュリティ認識向上トレーニングをスケジュール **(Schedule Security Awareness Training)]** タスクが実行されます。
セキュリティ認識向上トレーニングをスケジュール (Schedule Security Awareness Training)	従業員のセキュリティ認識を高めるためのトレーニングをスケジュールします。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクが完了すると、フローは終了します。

セキュリティインシデント - ポリシー違反フローテンプレート

セキュリティインシデント - ポリシー違反 - テンプレートを使用すると、セキュリティポリシー違反を処理するために設計された一連のタスクを実行できます。

始める前に
必要なロール：sn_si.write

このタスクについて
このフローは、セキュリティインシデントの [カテゴリ] が [ポリシー違反] に設定された場合にトリガーされます。

手順

1. ポリシー違反のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で [ポリシー違反] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかフローが終了します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ポリシー違反テンプレートの応答タスク

応答タスク	アクション	結果
違反の分類 (Classify violation)	この違反行為が組織のセキュリティポリシーにどのように違反しているかを分類します。 完了したら、タスクの [ステータス **(State)]** フィールドを更新します。	[違反者へのアドバイス **(Advise violator of infraction)]** 応答タスクが実行されます。
違反者へのアドバイス (Advise violator of infraction)	違反行為の性質を違反者に伝えます。 伝達したら、タスクの [ステータス **(State)]** フィールドを更新します。	[違反者から確認を取る **(Obtain acknowledgement from violator)]** 応答タスクが実行されます。
違反者から確認を取る (Obtain acknowledgement from violator)	違反者から確認を取ります。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	**[HR** プロセス **(HR process)]** 応答タスクが実行されます。
HR プロセス (HR process)	この違反に関する必要なすべての情報を HR に伝えます。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	[ステータスをレビューに設定 **(Set state to review)]** 応答タスクが実行されます。
ステータスをレビューに設定 (Set state to review)	アクションは必要ありません。	セキュリティインシデントの [ステータス **(State)]** が、自動的に [レビュー] に変更されます。
セキュリティ認識向上トレーニングをスケジュール (Schedule security awareness training)	今後類似のセキュリティ違反を防ぐ方法について、スタッフを教育するセキュリティ認識向上トレーニングを実施します。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、フローは終了します。

セキュリティインシデント - 偵察フローテンプレート

偵察は通常、デバイスまたはシステムのエクスプロイトが目的の攻撃を進めるための準備段階です。セキュリティインシデント - 偵察 - テンプレートを使用すると、ネットワーク上の偵察を処理するように設計された一連のタスクを実行できます。

始める前に

必要なロール：sn_si.write

このタスクについて

このフローは、セキュリティインシデントの [カテゴリ] が [偵察アクティビティ **(Reconnaissance activity)]** に設定された場合にトリガーされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. この潜在的な攻撃のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[偵察アクティビティ **(Reconnaissance activity)]** を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかフローが終了します。

偵察テンプレートの応答タスク

応答タスク	アクション	結果
偵察アクティビティは検証されましたか？(Reconnaissance activity verified?)	観測された偵察が検証されているかどうかを確認します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、[影響を受けるシステムの特定 **(Identify impacted systems)]** タスクが実行されます。 [いいえ] を選択すると、フローは終了します。
影響を受けるシステムの特定 (Identify impacted systems)	偵察の影響を受けるシステムを特定します。	このタスクが完了すると、 [法執行機関による偵察の分析を許可しますか？**(Allow reconnaissance for law enforcement analysis?)]** タスクが実行されます。
法執行機関による偵察の分析を許可しますか？(Allow reconnaissance for law enforcement analysis?)	法執行機関に偵察の分析を依頼するかどうかを決定します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、[法律の執行プロセス **(Law enforcement process)]** タスクが実行されます。 [いいえ] を選択すると、[システムを更新して偵察を防止 **(Update system(s) to prevent reconnaissance)]** タスクが実行されます。
法律の執行プロセス (Law enforcement process)	会社で定義されている法律の執行プロセスを実行します。	このタスクが完了すると、[システムを更新して偵察を防止 **(Update system(s) to prevent reconnaissance)]** タスクが実行されます。
システムを更新して偵察を防止 (Update system(s) to prevent reconnaissance)	偵察の影響を受けるシステムを更新するために必要な手順を実行します。	このタスクが完了すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
ステータスをレビューに設定 (Set state to review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)]** が自動的に [レビュー] に変更され、[学んだ教訓に関するミーティング] タスクが実行されます。
学んだ教訓に関するミーティング	反省会を開催し、この偵察インシデントに対して実行された作業をトリアージします。	このタスクが完了すると、フローは終了します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
	必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	

セキュリティインシデント - 不正サーバーまたはサービスフローテンプレート

セキュリティインシデント - 不正サーバーまたはサービス - テンプレートを使用すると、ネットワークに影響を与える不正なサーバーやサービスからのアクティビティの処理用に設計された一連のタスクを実行できます。

始める前に
必要なロール：sn_si.write

このタスクについて
このフローは、セキュリティインシデントの [カテゴリ] が [不正サーバーまたはサービス] に設定された場合にトリガーされます。

手順

1. この潜在的な攻撃のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[不正サーバーまたはサービスアクティビティ **(Rogue server or service activity)**] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかフローが終了します。

   #### 不正サーバーまたはサービステンプレートの応答タスク

応答タスク	アクション	結果
不正サーバーまたはサービスは検証されましたか？(Rogue server or service verified?)	不正サーバーまたはサービスとの接続がネットワーク上で検証されているかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、次の 2 つのタスクが並行して実行されます。 ○ 影響を受けるシステムの特定 **(Identify impacted system(s))** ○ データ損失の可能性？**(Potential data loss?)** [いいえ] を選択すると、フローは終了します。
影響を受けるシステムの特定 (Identify impacted system(s))	不正サーバーまたはサービスとの接触によって影響を受けるシステムを特定します。	このタスクが完了すると、[システムの更新 - 不正接続の削除 **(Update system(s) - Remove rogue connections)**] タスクが実行されます。
データ損失の可能性？(Potential data loss?)	不正サーバーまたはサービスとの接続が原因でデータ損失が発生したかどうかを判断します。	[はい] を選択すると、[データ損失の可能性インシデントの作成 **(Create potential data loss incident)**] タスクが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
	タスク内の [結果] で [はい] または [いいえ] を選択します。	[いいえ] を選択すると、[システムの更新 - 不正接続の削除 **(Update system(s) - Remove rogue connections)]** タスクが実行されます。
データ損失の可能性インシデントの作成 (Create potential data loss incident)	データ損失の可能性のセキュリティインシデントを作成するために必要な手順を実行します。	このタスクが完了すると、[システムの更新 - 不正接続の削除 **(Update system(s) - Remove rogue connections)]** タスクが実行されます。
システムの更新 - 不正接続の削除 (Update system(s) - Remove rogue connections)	不正接続を削除するために必要な手順を実行します。	このタスクが完了すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
ステータスをレビューに設定 (Set state to review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)]** が自動的に [レビュー] に変更され、[学んだ教訓に関するミーティング] タスクが実行されます。
学んだ教訓に関するミーティング	反省会を開催し、この不正サーバーまたはサービスインシデントに対して実行された作業をトリアージします。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	このタスクが完了すると、フローは終了します。

セキュリティインシデント - スパムフローテンプレート

セキュリティインシデント - スパム - テンプレートを使用すると、ネットワーク上のメールスパムを処理するように設計された一連のタスクを実行できます。

始める前に

必要なロール：sn_si.write

このタスクについて

このフローは、セキュリティインシデントの [カテゴリ] が [スパムソース] に設定または変更された場合にトリガーされます。

手順

1. スパムメールを処理するセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[スパムソース] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかフローが終了します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スパムテンプレートの応答タスク

応答タスク	アクション	結果
スパムに悪意のあるコンテンツは含まれていますか？ (Spam contains malicious content?)	スパムに悪意のあるソフトウェアが含まれているかどうかを判断します。タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、次の応答タスクが実行されます。 ○ メールメッセージの隔離 **(Quarantine email message)** ○ 悪意のあるソフトウェアインシデントの作成 **(Create malicious software incident)** [いいえ] を選択すると、[メールソフトウェアの更新 **(Update email software)**] が実行されます。
悪意のあるソフトウェアインシデントの作成 (Create malicious software incident)	セキュリティインシデントを作成する手順を実行し、必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、この応答タスクは、次の 3 つの応答タスクが完了するまで待機します。その後、セキュリティインシデントのステータスは [レビュー] に移行します。
メールメッセージの隔離 (Quarantine email message)	スパムを隔離する手順を実行し、必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。
ファイアウォールでソースをブロック (Block source on firewall)	ファイアウォールでメールアドレスをブロックする手順を実行し、必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。
メールソフトウェアの更新 (Update email software)	メールアドレスをブロックリストに追加し、必要に応じてタスクの [ステータス **(State)**] フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更すると、次の応答タスクが実行されます。 **注:** この応答タスクは、[スパムに悪意のあるコンテンツは含まれていますか？**(Spam contains malicious content?)**] 応答タスクに [いいえ] と回答した場合も実行されます。
ステータスをレビューに設定 (Set state to review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)**] が自動的に [レビュー] に変更されます。

セキュリティインシデント - 無許可のアクセスフローテンプレート

セキュリティインシデント - 無許可のアクセス - テンプレートを使用すると、ネットワークに対する不正アクセスを処理するように設計された一連のタスクを実行できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_si.write

このタスクについて
このフローは、セキュリティインシデントの [カテゴリ] が [無許可のアクセス] に設定された場合にトリガーされます。

手順

1. この潜在的な攻撃のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、[無許可のアクセス] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかフローが終了します。

不正アクセステンプレートの応答タスク

応答タスク	アクション	結果
ユーザーの認証情報は侵害されましたか？ (User credentials compromised?)	ユーザーの認証情報が侵害されているかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、次の 2 つのタスクが並行して実行されます。 ○ 悪意のあるソフトウェア？ **(Malicious Software?)** ○ ユーザーアカウントの非アクティブ化 **(Deactivate user account)** [いいえ] を選択すると、[ユーザーに連絡して意図を確認 **(Contact user and determine intent)]** タスクが実行されます。
悪意のあるソフトウェア？(Malicious Software?)	不正アクセスによって悪意のあるソフトウェアが導入されたかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、[悪意のあるソフトウェアインシデントの作成 **(Create malicious software incident)]** タスクが実行されます。 [いいえ] を選択すると、[ステータスをレビューに設定 **(Set state to review)]** タスクが実行されます。
悪意のあるソフトウェアインシデントの作成 (Create malicious software incident)	不正アクセスのセキュリティインシデントを作成するために必要な手順を実行します。	このタスクが完了すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
ユーザーアカウントの非アクティブ化 (Deactivate user account)	侵害されたユーザーアカウントを非アクティブにするために必要な手順を実行します。	このタスクが完了すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
ユーザーに連絡して意図を確認 (Contact	不正アクセスを行ったユーザーに連絡し、アクセスを試みた	このタスクが完了すると、**[HR** プロセス **(HR process)]** タスクが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
user and determine intent)	理由を確認するために必要な手順を実行します。	
HR プロセス (HR process)	人事に連絡して必要に応じて懲戒処分を実施するために必要な手順を実行します。	このタスクが完了すると、[ステータスをレビューに設定 **(Set State to Review)]** タスクが実行されます。
ステータスをレビューに設定 (Set state to review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)]** が自動的に [レビュー] に変更され、フローが終了します。

セキュリティインシデント - **Web/BBS** の改ざんフローテンプレート

セキュリティインシデント - Web/BBS の改ざん - テンプレートを使用すると、組織の BBS または Web サイトのいずれかに向けられた破壊行為を処理するように設計された一連のタスクを実行できます。

始める前に
必要なロール：sn_si.write

このタスクについて
このフローは、セキュリティインシデントの [カテゴリ] が **[Web/BBS** の改ざん] に設定された場合にトリガーされます。

手順

1. この Web または BBS の改ざんの事例のセキュリティインシデントを開くか、新しいセキュリティインシデントを作成します。
2. [カテゴリ] で、**[Web/BBS** の改ざん] を選択します。
3. レコードを保存します。
4. 下にスクロールして、[応答タスク] 関連リストを開きます。
   一連の応答タスクの最初のタスクが表示されます。レコードが保存されるたびに、前のタスクへの対応に応じて、次の応答タスクが作成されるかフローが終了します。

Web/BBS 改ざんテンプレートの応答タスク

応答タスク	アクション	結果
セキュリティインシデントアサイン	Web サイトまたは BBS の改ざんが報告された各インシデントのセキュリティインシデントを作成します。	次の応答タスクが実行されます。
改ざんは検証されていますか？ (Defacement verified?)	Web サイトまたは BBS が実際に改ざんされているかどうかを判断します。 タスク内の [結果] で [はい] または [いいえ] を選択します。	[はい] を選択すると、次の応答タスクが実行されます。 ○ **PR** プロセス **(PR process)** ○ 法律の執行プロセス **(Law enforcement process)** ○ 根本原因の特定と除去 **(Determine and eradicate root cause)** [いいえ] を選択すると、フローは終了します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

応答タスク	アクション	結果
PR プロセス (PR process)	Web サイトまたは BBS が改ざんされたことを一般に通知するために必要な手順を実行します。 PR プロセスが完了したら、必要に応じてタスクのステータスを [完了] または [未完了] に設定します。	[学んだ教訓に関するミーティング] タスクが実行されます。
法律の執行プロセス (Law enforcement process)	攻撃に関して適切な法執行機関を関与させるために必要な手順を実行します。 完了したら、必要に応じてタスクのステータスを [完了] または [未完了] に設定します。	[学んだ教訓に関するミーティング] タスクが実行されます。
根本原因の特定と除去 (Determine and eradicate root cause)	改ざんの根本原因を発見して除去するために必要な手順を実行します。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、次の応答タスクが実行されます。
バックアップからサイトを復元 (Restore site from backup)	Web サイトまたは BBS のバックアップと復元に必要な手順を実行します。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル] に変更した場合、次の応答タスクが実行されます。
サイト復元のテストと検証 (Test and verify site is restored)	サイトが復元されたことを検証します。 完了したら、必要に応じてタスクのステータスを [完了] または [未完了] に設定します。	[学んだ教訓に関するミーティング] タスクが実行されます。
学んだ教訓に関するミーティング	反省会を開催し、この Web サイト/BBS 改ざんインシデントに対して実行された作業をトリアージします。 必要に応じてタスクの [ステータス **(State)]** フィールドを更新します。	タスクのステータスを [完了してクローズ] または [キャンセル]に変更すると、[ステータスをレビューに設定 **(Set state to review)]** タスクが実行されます。
ステータスをレビューに設定 (Set state to review)	アクションは要求されません。	セキュリティインシデントの [ステータス **(State)]** が、自動的に [レビュー] に変更されます。 フローが終了します。

自動翻訳

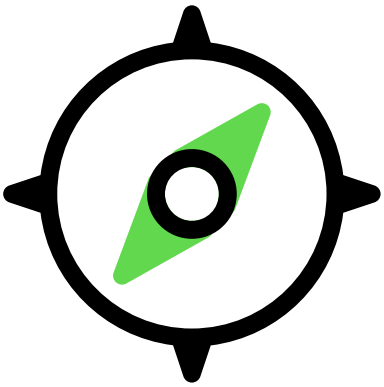
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威インテリジェンス

ServiceNow® 脅威インテリジェンス アプリケーションでは、セキュリティ侵害のインジケーター (IoC) を検出し、脅威インテリジェンスデータでセキュリティインシデントに対する強化できます。

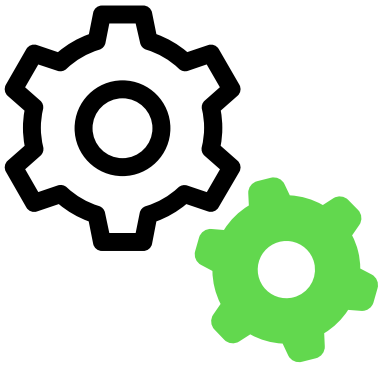
始めましょう

探索



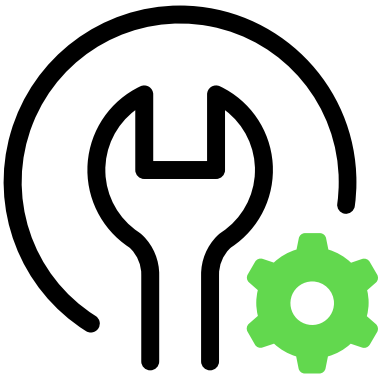
脅威インテリジェンスの概念とその主な機能について説明します。

構成



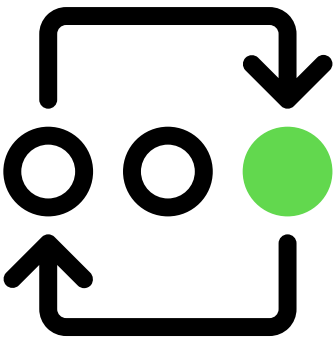
セットアップし、インストールされているコンポーネントと、ビジネスニーズを満たすために必要なユーザーロールについて学習します。

管理



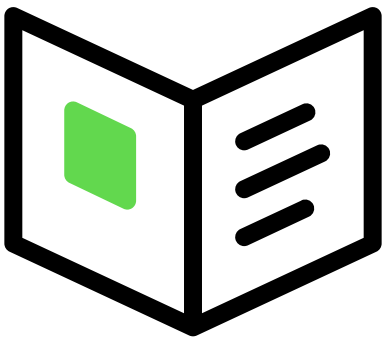
脅威インテリジェンスプロパティを設定します。

統合



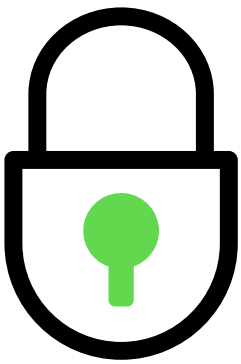
ServiceNow およびサードパーティアプリケーションと統合することで、脅威インテリジェンス機能を拡張します。

使用



セキュリティ侵害のインジケーター (IoC) とさまざまなアーティファクトを管理します。

MITRE ATT&CK フレームワーク



MITRE-ATT&CKフレームワークを管理し、脅威を迅速に特定し、サイバー攻撃への対応を調整します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

不審なアクティビティに関する情報を収集して、セキュリティケース管理を管理します。

学習リソース

- 開発者トレーニング
- 開発者ドキュメント
- アプリケーションとともにインストールされているコンポーネントの検索

トラブルシューティングとサポート

- について質問し、他のリソースを調べる 脅威インテリジェンス の ServiceNow コミュニティ
- 既知のエラーポータルで既知のエラー記事を検索する
- 連絡先 カスタマーサービス & サポート
- セキュリティオペレーションリソースライブラリ
- セキュリティオペレーションコミュニティ

脅威インテリジェンス の概要

脅威インテリジェンス アプリケーションは、会社の脅威情報構造化記述形式 (STIX™) データにアクセスして評価基準を提供できます。脅威インテリジェンス には セキュリティケース管理 アプリケーションが含まれています。これは、標的を定めたキャンペーンや国家レベルの攻撃者による組織を脅かす脅威を分析するための手段を提供します。

STIX は、標準化および構造化された方法でサイバー脅威情報を記述するための言語です。STIX データと検知指標情報自動交換手順 (TAXII™) プロファイルを使用すると、脅威専門チームは共有されたサイバー脅威情報を使用して、以前に会社や他のソースから特定された脅威を隔離できます。TAXII により、サイバー脅威情報の広範な自動交換が可能になります。

脅威インテリジェンス は STIX バージョン 1.1、2.0、および 2.1 をサポートしています。

STIX™ および TAXII™ は MITER Corporation の商標です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

ドメインセパレーションと 脅威インテリジェンス

ドメインセパレーションは、セキュリティインシデントレスポンスの一部として利用可能な 脅威インテリジェンス モジュールでサポートされています。 ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル：ベーシック

- ベーシックレベルサポートを含みます。
- ビジネスロジック：サービスプロバイダー (SP) によって顧客ごとにプロセスを作成または変更できます。ユースケースには、単一のインスタンスでの複数のサービスプロバイダー顧客によるアプリケーションの正しい使用が反映されています。
- インスタンスのオーナーは、特定のアプリケーションに期待される通りに、テナントごとに MVP ビジネスロジックとデータパラメーターを設定できる必要があります。

サンプルユースケース：アドミンは、レコードを他のテナントに対してはクローズしないが、1 つのテナントに対してクローズする場合、コメントを必須にすることができる必要があります。

サポートレベルの詳細については、「アプリケーションでのドメインセパレーションのサポート」を参照してください。

概要

(セキュリティインシデントレスポンスアプリケーションの一部である) 脅威インテリジェンスモジュールでは、ドメインセパレーションにより、サービスプロバイダー (SP) が次の方法で脅威情報リポジトリを作成および管理できます。

- 脅威のソースおよび検知指標情報自動交換手順 (TAXII) プロファイル
- 観測事象
- セキュリティ侵害のインジケーター
- 脅威の攻撃モード/方法、および顧客ベース全体でのケース管理による、運用コストの削減とサービス品質の向上

顧客データは、ワークフロー、ダッシュボード、レポートなどに別個の顧客ワークスペースを使用することで分離され、他のクライアントに公開されることはありません。

脅威インテリジェンス でのドメインセパレーションのサポート (バージョンリリース別)

脅威インテリジェンスモジュールのドメインセパレーション (セキュリティインシデントレスポンスアプリケーションの一部) は、次の製品機能をカバーしています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- セキュリティインシデント観測事象は、ID/認証情報/スコープでインシデントが生成されるユーザーの適切なドメインに送信されます。インシデントから抽出された観測事象は、セキュリティインシデントのドメインに格納されます。
- サイバー脅威情報フィードを提供する 1 つ以上の TAXII 収集をダウンロードするための TAXII サービスプロファイルの設定。構成は、プロファイルが設定されているドメインに保存されます。
- 構成が実行されているドメイン内の IOC リポジトリへの脅威フィードのダウンロードの設定。
- 情報を自動的に提供する脅威インテリジェンスソースのドメイン、またはユーザーが手動で新しい攻撃モード/方法を追加するドメインでの攻撃モード/方法の作成。
- ケースに関連するインシデント、観測事象、CI、ユーザー、および侵害のインジケーター (IOC) の長期調査のためのケースの作成。ケースは、ユーザーが作成したドメインに保存されます。

注:
上記のすべてのケースでは、NOW Platform における分離されたドメインでの可視化の包括的な原則が適用されます。通常どおり、親ドメインのインシデントは子ドメインのアーティファクトを参照できますが、その逆はできません。

脅威インテリジェンス (セキュリティインシデントレスポンス の一部) におけるドメインセパレーションの仕組み

脅威インテリジェンスは、セキュリティインシデントレスポンスの一部として Professional Tier および Enterprise Tier にありますが、Standard Tier には属していません。したがって、別のプラグインが必要です。脅威インテリジェンスモジュール (セキュリティインシデントレスポンス アプリケーションの一部) は、組織内のセキュリティインシデントに関連する脅威インテリジェンス情報を作成および管理します。次のユースケースはドメインセパレーションに対応しています。

- インシデント作成時のセキュリティインシデント観測事象の作成
  - メールパーサーから (プラットフォームベース、ユーザーから報告されたフィッシング、カスタム)
  - サードパーティのセキュリティ情報およびイベント管理 (SIEM) ストアのアプリケーションから
  - SOC アナリストが手動で入力
- 脅威フィードソースからの観測事象の収集 - TAXII 収集からの脅威インテリジェンスソース
- セキュリティインシデント観測事象の管理
  - 観測事象を関連インジケーターに関連付ける
  - 観測事象をセキュリティインシデントに関連付ける
  - 観測事象を子観測事象に関連付ける
  - 観測事象を脅威フィードソースに関連付ける
  - セキュリティ注釈を観測事象に追加する
- セキュリティ侵害のインジケーターの管理
  - 観測事象を関連インジケーターに関連付ける
  - インジケーターを攻撃モード/方法に関連付ける
  - インジケーターをインジケータータイプに関連付ける
  - インジケーターを脅威フィードソースに関連付ける
  - セキュリティ注釈をインジケーターに追加する
- ケースの管理

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ケースを作成する (手動またはインシデントから)
- 新規ケースを編集して詳細を追加する (ケースタイプと重大度を選択し、インシデント、観測事象、構成アイテム、ユーザー、インジケーターを追加)
- テストケースを削除する

ドメインセパレーションのセットアップ

脅威インテリジェンスのドメインセパレーションを設定するには、追加の手順は必要ありません。インスタンスがドメインセパレーションされると、すべての脅威インテリジェンステーブルで [ドメイン] 列が取得されます。

ドメインセパレーションデータ

データはドメインセパレーションできます。これは、次のことを意味します。

- ドメイン内のセキュリティインシデント観測事象を他のドメインのスコープから表示することはできません。
- ドメインの侵害のインジケーターを他のドメインのスコープから表示することはできません。
- ドメインに関連付けられた攻撃モード/方法を他のドメインのスコープから表示することはできません。
- ドメインに関連付けられた TAXII サービスプロファイルを他のドメインのスコープからは表示することはできません。
- ドメインに関連付けられた脅威インテリジェンスソースを他のドメインのスコープからは表示することはできません。
- ドメインに関連付けられたケースを他のドメインの他のドメインのスコープからは表示することはできません。

脅威インテリジェンスプロパティはグローバルレベルで設定されるため、ドメインセパレーションされません。次のような設定があります。

- IP アドレス/URL の追加情報を取得するためのドメイン名
- 取得に使用する API キー
- リモートのスキャナーに送信する前のローカル IoC テーブルのルックアップ
- ローカルの観測事象を考慮する日数
- 脅威情報ソースから受信していない場合、攻撃モード/方法を非アクティブとしてマークする
- 指定された日数の間どのソースからも受信していない場合、インジケーターを非アクティブとしてマークする

構成

脅威インテリジェンス機能構成のすべての側面は、ドメインセパレーション環境では自己完結型です。

次のタスクをドメインごとに構成する必要があります。

1. TAXII サービスプロファイルの作成
   - ディスカバリーサービス構成を選択する
   - コレクションサービス構成を選択する：ユーザーおよびユーザーグループにロールをアサインします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. 脅威インテリジェンスソースの作成
   - 脅威インテリジェンス情報を提供する REST サービスを構成する
   - 脅威インテリジェンス情報のダウンロードをスケジュールする
   - ソースに割り当てる脅威の詳細情報を選択する
3. 攻撃モード/方法の作成 (手動)
   - ソース、マルウェアタイプ、攻撃メカニズム、攻撃者タイプ、説明、処理、意図した効果、最初の確認、最終確認
   - 関連インジケーター、子攻撃モード/方法、関連するセキュリティインシデント

   注:
   攻撃モード/方法も脅威フィードのソースから自動的に作成されます。

4. 次の脅威情報カテゴリのデフォルトリストの設定：
   - 攻撃メカニズム
   - ディスカバリー方法
   - フィード
   - インジケータータイプ
   - 意図した効果
   - 通知
   - 観測事象タイプ
   - レート制限定義
   - 攻撃者タイプ
   - 攻撃の動機
   - インフラストラクチャタイプ
   - マルウェア機能
   - マルウェアタイプ
   - レポートタイプ
   - 攻撃者ロール
   - ツールタイプ

テナントドメインが独自のアプリケーションデータを管理する方法

- テナントドメインオーナーは、独自の TAXII サービスプロファイルを作成できます。
- テナントドメインオーナーは、独自の脅威インテリジェンスソースを作成できます。
- テナントドメインオーナーは、独自の攻撃モード/方法を作成できます。
- テナントドメインオーナーは、脅威情報カテゴリの独自のデフォルトリストを作成できます。

注:
ビジネスロジックとプロセスにより、脅威インテリジェンスソースのダウンロードスケジュールをインスタンスオーナーがドメインセパレーションできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連情報

サービスプロバイダーのドメインセパレーション

脅威インテリジェンスのセットアップ

インスタンスで 脅威インテリジェンス を実行する前に、ServiceNow Store からダウンロードする必要があります。プロパティを設定し、脅威のソースを定義することもできます。

脅威インテリジェンス のインストール

インスタンスで 脅威インテリジェンス を実行する前に、ServiceNow Store からダウンロードする必要があります。

始める前に

インストールの前に、次のセットアップチェックリストを完了します。これらのセットアップタスクは、インストールと構成をスムーズに行うために必要です。

セットアップタスク	説明
インスタンスに必要な ServiceNow ロールがあることを確認します。	インストール、構成、および予想される結果の検証には、次のロールが必要です。 • まだアサインされていない場合、システムアドミニストレーター [admin] は、アプリケーションをインストールし、脅威アドミン [sn_ti.admin] ロールをアサインします。 • 脅威アドミン [sn_ti.admin] は構成を監視し、期待される結果を検証します。

必要なロール：admin

手順

の指示に従ってください からのアプリケーションのダウンロード ServiceNow Store.

次のタスク

脅威インテリジェンス プロパティの設定。

脅威インテリジェンスと一緒にインストールされるコンポーネント

いくつかのタイプのコンポーネント (テーブル、ユーザーロールなど) が、脅威インテリジェンスプラグインのアクティブ化とともにインストールされます。

注:
アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「アプリケーションとともにインストールされているコンポーネントの検索」を参照してください。

この機能ではデモデータを利用できます。

インストールされるロール

ロール タイトル [名前]	説明	含んでいるロール
脅威アドミン	すべての脅威プロパティ、SLA、および通知を完全に制御できます。	sn_ti.write

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロール タイトル [名前]	説明	含んでいるロール
[sn_ti.admin]		
脅威リーダー [sn_ti.read]	脅威情報への読み取りアクセス権があります。	sn.sec_cmn.int_read
脅威ライター [sn_ti.write]	脅威情報への書き込みアクセス権があります。 攻撃モード、インジケーター、または観測事象は削除できません。脅威アドミンのみが削除できます。	• sn_sec_cmn.int_write • sn_ti.read
MITRE アナリスト [sn_ti.mitre_analyst]	このロールは、脅威インテリジェンス の MITRE-ATT&CK モジュールおよび SIR モジュールへの読み取りアクセスを有効にします。	• sn_ti.read • sn_si.read

インストールされるテーブル

テーブル	説明
攻撃メカニズム [sn_ti_attack_mechanism]	脆弱性を悪用するときに頻繁に使用されるメカニズムに基づいて、攻撃パターンを階層的に整理します。このビューのメンバーであるカテゴリは、システムを攻撃するために使用されるさまざまなテクニックを表します。
攻撃モード/方法 [sn_ti_attack_mode]	攻撃モードと方法は、サイバー攻撃者の行動を表します。これらは、攻撃者の行動とその方法を詳細なレベルで特徴付けます。
ディスカバリー方法 [sn_ti_discovery_method]	インシデントがどのように検出されたかを表す式
フィード [sn_ti_feed]	脅威の概要で脅威フィード (RSS) を構成するために使用されます。
インジケーター攻撃モード/方法 [sn_ti_m2m_indicator_attack_mode]	攻撃モード/方法をインジケーターにマッピングするために使用されます。
セキュリティ侵害のインジケーター [sn_ti_indicator]	サイバーセキュリティコンテキスト内で対象となるアーティファクトや動作を表すことを目的とした、特定の観測事象のパターンを伝えるために使用されます。
セキュリティ侵害のインジケーターのメタデータ [sn_ti_indicator_metadata]	TAXII レコードを入力するために使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
インジケーターソース [sn_ti_m2m_indicator_source]	特定のインジケーターをレポートするすべてのソースを収集するために使用されます。
インジケータータイプ [sn_ti_indicator_type]	特定の観測可能な条件を識別するパターンと、そのパターンの意味、いつどのように影響するかなどのコンテキスト情報で構成されるサイバー脅威インジケーターを特徴付けます。
関連するインジケータータイプ [sn_ti_m2m_indicator_indicator_type]	インジケーターを該当するタイプにリンクします。
インシデント数 [sn_ti_observable]	観測事象に関連付けられたセキュリティインシデントの数。
意図した効果 [sn_ti_intended_effect]	攻撃者の意図した効果を表すために使用されます。
IP スキャン結果 [sn_ti_ip_result]	IP ルックアップの結果を表示するために使用されます。
マルウェアレート制限 [sn_ti_rate_limit]	ルックアップソースで使用するレート制限を定義します。
マルウェアスキャン [sn_ti_scan]	ルックアップ。ルックアップ対象、ルックアップ対象のソース、およびルックアップ結果の概要が含まれています。
マルウェアスキャンキューエントリー [sn_ti_scan_q_entry]	ルックアップまたは処理のためにキューに格納されるルックアップレコード。指定されたレート制限内で要求を容易にします。
マルウェアスキャン結果 [sn_ti_scan_result]	ルックアップの結果を表示します。
マルウェアスキャナー [sn_ti_scanner]	ルックアップの実行に使用するサードパーティのルックアップソースを定義します。
マルウェアスキャナーレート制限 [sn_ti_scanner_rate_limit]	ルックアップソースをレート制限に関連付けます。
マルウェアタイプ [sn_ti_malware_type]	マルウェアインスタンスのタイプを表すために使用されます。
観測事象 [sn_ti_observable]	STIX の観測事象は、コンピューターとネットワークの運用に関連するステートフルなプロパティまたは測定可能なイベントを表します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
観測事象コンテキストタイプ [sn_ti_observable_context_type]	観測事象のコンテキスト (ソース、IP アドレスなど) を格納します。
観測事象インジケーター [sn_ti_m2m_observable_indicator]	観測事象をインジケーターに関連付けるために使用されます。
観測事象ソース [sn_ti_observable_source]	観測事象を脅威ソースに関連付けるために使用されます。
観測事象タイプ [sn_ti_observable_type]	IP アドレスなどのさまざまなタイプの観測事象を一覧表示します。
観測事象タイプカテゴリ [sn_ti_observable_type_category]	観測事象の最初の分類 (IP アドレスや URL など) を格納します。これは、観測事象のタイプをより正確に決定するために使用されます。
関連する攻撃モード/方法 [sn_ti_m2m_attack_mode_attack_mode]	攻撃モードを相互に関連付けるために使用されます。
関連する観測事象 [sn_ti_m2m_observables]	観測事象を相互に関連付けるために使用されます。
スキャンタイプ [sn_ti_scan_type]	ファイル、URL、および IP の初期レコードを含むルックアップタイプの定義。
セキュリティケース [sn_ti_case]	ケース管理を使用して作成されたセキュリティケースレコードを保存します。
セキュリティケース IoC [sn_ti_case_ioc]	観測事象とケースの関係を管理するために使用されます。
セキュリティケース関連タスク [sn_ti_m2m_case_task]	タスク (セキュリティインシデント、変更要求など) とセキュリティケースの関係を管理するために使用されます。
セキュリティケースの関係性の除外 [sn_ti_case_relationship_exclusion]	セキュリティケースへの関連レコードの包含と除外の定義を提供します。
サイティング [sn_ti_sighting]	サイティング検索要求の実行で使用される、観測事象とサイティング検索の詳細結果の間の m2m リンク。
サイティング構成アイテム [sn_ti_m2m_sighting_ci]	構成アイテムをサイティング検索にマッピングします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
サイティング検索の詳細 [sn_ti_sighting_search_detail]	見つかった内部/外部アイテムの数など、サイティング検索の詳細。
サイティング検索結果 [sn_ti_sighting_search]	サイティング検索実行のヘッダー。
サポートされる観測事象タイプ [sn_ti_m2m_ind_type_obs_type]	インジケータータイプを有効な観測事象タイプに関連付けます。
サポートされるスキャンタイプ [sn_ti_supported_scan_type]	ルックアップタイプをルックアップソース/ベンダー固有の実装にマッピングします。特定のルックアップソースがタイプをサポートしていることを示します。
タスク攻撃モード/方法 [sn_ti_m2m_task_attack_mode]	攻撃モードをタスクに関連付けます。
タスクインジケーター [sn_ti_m2m_task_indicator]	インジケーターをタスクに関連付けます。
タスク観測事象 [sn_ti_m2m_task_observable]	観測事象をタスクに関連付けます。
タスクのサイティング [sn_ti_m2m_task_sighting]	サイティングレコードに関連するタスクレコード (セキュリティインシデントおよびケース) を保存します。
TAXII 収集 [sn_ti_taxii_collection]	TAXII サーバーによってインポートできるサイバーリスクインテリジェンスフィードを定義します。
TAXII プロファイル [sn_ti_taxii_profile]	サイバーリスクインテリジェンスを共有するためのリポジトリを定義します。TAXII 収集を含みます。
攻撃者タイプ [sn_ti_threat_actor_type]	推定される意図や過去に観察された動作など、サイバー攻撃の脅威を表す悪意のあるアクター (攻撃者) の特性を提供します。
脅威インテリジェンスソース [sn_ti_source]	脅威データをインポートするソースを定義します。
関連する攻撃の動機 [sn_ti_stix2_m2m_object_attack_motivation]	STIX オブジェクトに関連付けられたすべての攻撃の動機を収集します。
関連インフラストラクチャタイプ [sn_ti_stix2_m2m_infra_type]	インフラストラクチャをそのタイプとリンクします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
関連キルチェーンフェーズ [sn_ti_stix2_m2m_indicator_kill_chain_phase]	キルチェーンフェーズをインジケーターにリンクします。
関連キルチェーンフェーズ [sn_ti_stix2_m2m_object_kill_chain_phase]	キルチェーンフェーズを STIX オブジェクトにリンクします。
関連するマルウェア機能 [sn_ti_stix2_m2m_malware_capability]	マルウェアとその機能をリンクします。
関連するマルウェアタイプ [sn_ti_stix2_m2m_malware_malware_type]	マルウェアとそのタイプをリンクします。
関連する観測事象 [sn_ti_stix2_m2m_malware_observable]	マルウェアに関連付けられたすべての観測事象を収集します。
関連する観測事象 [sn_ti_stix2_m2m_observed_data_observable]	観測されたデータに関連付けられたすべての観測事象を収集します。
関連レポートタイプ [sn_ti_stix2_m2m_report_report_type]	脅威レポートをそのタイプとリンクします。
関連する攻撃者ロール [sn_ti_stix2_m2m_threat_actor_threat_actor_role]	攻撃者をそのロールにリンクします。
関連する攻撃者タイプ [sn_ti_stix2_m2m_threat_actor_threat_actor_type]	攻撃者をそのタイプにリンクします。
関連するツールタイプ [sn_ti_stix2_m2m_tool_tool_type]	ツールをそのタイプにリンクします。
攻撃の動機 [sn_ti_stix2_attack_motivation]	攻撃の動機は、攻撃の強度と永続性を形成します。攻撃者と侵入セットは通常、根底にある感情や状況を反映して行動するため、防御者は攻撃の方法を知ることができます。
攻撃パターン [sn_ti_stix2_attack_pattern]	攻撃者が標的の侵害を試みるのに使用する方法を記述する TTP タイプ。
キャンペーン [sn_ti_stix2_campaign]	攻撃者の行動をグループ化したもの。一連の特定の標的に対して、時間の経過とともに発生する一連の悪意のあるアクティビティまたは攻撃 (波と呼ばれる場合もある) を表します。
対処措置	インテリジェンスに対して実行する可能性があるアクションに関する、インテリジェ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
[sn_ti_stix2_course_of_action]	ンスのプロデューサーからコンシューマーへの推奨事項。
外部参照 [sn_ti_stix2_external_reference]	STIX の外部で示される情報へのポインター。
ID サイティング [sn_ti_stix2_m2m_sighting_identity]	サイティングに関連付けられたすべての ID を収集します。
ID [sn_ti_stix2_identity]	実際の個人、組織、またはグループ (例：ACME, Inc.)、および個人、組織、システム、またはグループのクラス (例：ファイナンスセクター)。
インジケーターの外部参照 [sn_ti_stix2_indicator_external_reference]	インジケーターに関連付けられた外部参照を表します。
インジケーターのサイティング [sn_ti_stix2_indicator_sighting]	インジケーターのサイティングを表します。
インフラストラクチャタイプ [sn_ti_stix2_infrastructure_type]	さまざまなインフラストラクチャタイプを表します。
インフラストラクチャ [sn_ti_stix2_infrastructure]	何らかの目的をサポートすることを意図した、すべてのシステム、ソフトウェアサービス、および関連する物理または仮想リソースを記述する TTP タイプ (攻撃の一部として使用される C2 サーバー、防御の一部であるサーバー、またはデバイス、攻撃の標的となるデータベースサーバーなど)。
インストール済みソフトウェア [sn_ti_stix2_m2m_malware_analysis_sw]	マルウェア分析に関連するすべてのソフトウェア (SCO ソフトウェアタイプ) を収集します。
侵入セット [sn_ti_stix2_intrusion_set]	単一の組織によってオーケストレーションされていると考えられている、共通のプロパティを持つ攻撃者の一連の行動およびリソースをグループ化したもの。
キルチェーンフェーズ [sn_ti_stix2_kill_chain_phase]	キルチェーンに関連付けられたキルチェーンフェーズを表します。
キルチェーン [sn_ti_stix2_kill_chain]	さまざまなキルチェーンを表します。
ロケーション [sn_ti_stix2_location]	STIX を介して提供される地理的な場所を表します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
マルウェア分析 [sn_ti_stix2_malware_analysis]	マルウェアのインスタンスまたはファミリで実行された特定の静的または動的分析のメタデータと結果。
マルウェア機能 [sn_ti_stix2_malware_capability]	マルウェアファミリまたはインスタンスが示す一般的な機能を表します。
マルウェアオペレーティングシステム [sn_ti_stix2_m2m_malware_operating_system]	マルウェアに関連するすべてのオペレーティングシステム (SCO ソフトウェアタイプ) を収集します。
マルウェア [sn_ti_stix2_malware]	悪意のあるコードを表す TTP のタイプ。
マーキング定義 [sn_ti_stix2_marking_definition]	STIX オブジェクトの処理または共有の要件を表します。
オブジェクトのサイティング [sn_ti_stix2_object_sighting]	STIX オブジェクトのサイティングを表します。
オブジェクトとインジケーターの関係 [sn_ti_stix2_m2m_object_indicator]	STIX オブジェクトと STIX インジケーター間のすべての関係を収集します。
オブジェクトとオブジェクトの関係 [sn_ti_stix2_m2m_object]	STIX オブジェクトと他の STIX オブジェクト (インジケーターを除く) 間のすべての関係を収集します。
オブジェクトと観測事象の関係 [sn_ti_stix2_m2m_object_observable]	STIX 観測事象と STIX オブジェクト間のすべての関係を収集します。
観測されたデータのサイティング [sn_ti_stix2_m2m_sighting_observed_data]	サイティングに関連付けられたすべての観測データオブジェクトを収集します。
観測データ [sn_ti_stix2_observed_data]	STIX サイバー観測可能オブジェクト (SCO) を使用して、ファイル、システム、ネットワークなどのサイバーセキュリティ関連エンティティに関する情報を提供します。
レポートタイプ [sn_ti_stix2_report_type]	脅威レポートの主な目的または対象を表します。
報告された観測事象 [sn_ti_stix2_m2m_malware_analysis_observable]	マルウェア分析に関連付けられたすべての観測事象を収集します。
STIX V2 オブジェクト [sn_ti_stix2_object]	STIX オブジェクトの共通の親テーブル。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
STIX V2 サイティング [sn_ti_stix2_sighting]	STIX サイティングテーブルの共通の親テーブル。
攻撃者ロール [sn_ti_stix2_threat_actor_role]	攻撃者が実行できるロールを表します。
攻撃者 [sn_ti_stix2_threat_actor]	攻撃者は、悪意を持って行動すると考えられている個人、グループ、または組織です。
脅威グループ化 [sn_ti_stix2_threat_grouping]	共通のコンテキストを共有するすべての STIX オブジェクトをグループ化します。
脅威メモ [sn_ti_stix2_threat_note]	対応する STIX オブジェクトに含まれていないコンテキストと追加の分析を提供します。
脅威に関する意見 [sn_ti_stix2_threat_opinion]	別のエンティティによって生成された STIX オブジェクト内の情報の正確性を評価します。
脅威レポート [sn_ti_stix2_threat_report]	レポートは、攻撃者、マルウェア、または攻撃テクニックの説明 (コンテキストおよび関連する詳細を含む) など、1 つ以上のトピックに焦点を当てた脅威インテリジェンスのコレクションです。これらは、包括的なサイバー脅威ストーリーとして公開できるように、関連する脅威インテリジェンスをグループ化するために使用されます。
ツールタイプ [sn_ti_stix2_tool_type]	攻撃を実行するために使用できるツールのカテゴリ。
ツール [sn_ti_stix2_tool]	ツールは、攻撃者が攻撃を実行するために使用する正当なソフトウェアです。
脆弱性 [sn_ti_stix2_vulnerability]	ソフトウェアおよび一部のハードウェアコンポーネント (例：ファームウェア) に含まれる計算ロジック (例：コード) の要件、設計、または実装の脆弱性または欠陥を表します。これらは、そのシステムの機密性、完全性、または可用性に悪影響を及ぼすために直接悪用されます。

脅威インテリジェンス プロパティの設定

脅威インテリジェンス プロパティを使用すると、API キーの設定など、システム機能のさまざまな側面を制御できます。

始める前に
必要なロール：sn_ti.admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > アドミニストレーション > プロパティ.
2. 必要に応じて、次のプロパティを設定します。

脅威インテリジェンスのプロパティ

プロパティ	説明
IP アドレス/URL の追加情報を取得するためのドメイン名 sn_ti.ip_lookup.web_site	IoC データベースに追加情報を取得するために使用するドメイン名。このプロパティは、[観測事象] フォームに追加情報を入力するために ThreatAdditionalInfo スクリプトインクルードによって使用されます。 デフォルト値：http://api.ipinfodb.com/v3/ip-country/ **注:** サードパーティ API の pinfodb.com は追加料金なしで利用できるため、多くの商用ソフトウェアプログラムで使用されています。別のドメイン名に置き換える場合は、次のフィールドにも API キーを入力する必要があります。
ドメインに使用される API キー (存在する場合) sn_ti.ip_lookup.api_key	追加情報を IoC データベースに取得するために使用する API キー。このプロパティは、[観測事象] フォームに追加情報を入力するために ThreatAdditionalInfo スクリプトインクルードによって (sn_ti.ip_lookup.web_site プロパティとともに) 使用されます。
観測事象が IoC に関連付けられている場合、または悪意があると判断された場合は、その観測事象で自動脅威ルックアップを実行しない。 sn_ti.scan_ioc_before_sending **注:** 次のプロパティ (sn_ti.scan_ioc_num_days) で期間を定義する必要があります。	構成された期間 (日数) 中に観測事象が IoC に関連付けられている場合、または悪意があると判断された場合は、その観測事象で自動脅威ルックアップを実行しないオプション。観測事象に対して脅威ルックアップの検索を実行する必要がある場合は、手動で実行できます。 デフォルト値：はい
期間 (日数) sn_ti.scan_ioc_num_days	観測事象の自動脅威ルックアップをスキップする期間を定義するオプション。 デフォルト値 (日数)：30

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明
既に実行されている観測事象では、自動脅威ルックアップを実行しない。 sn_ti.enable_threat_lookup_bypass 注: 次のプロパティ (sn_ti.threat_lookup_bypass_times) で期間を定義する必要があります。	観測事象の脅威のルックアップ結果が既に存在する場合は、構成した時間が経過するまで、同じ観測事象の自動脅威ルックアップの再実行をスキップするオプションがあります。 デフォルト値：いいえ 注: このプロパティを有効にする場合は、適切な値を追加していることを確認してください。
期間 (分) sn_ti.threat_lookup_bypass_time	観測事象の自動脅威ルックアップを再実行できる期間を定義するオプション。 デフォルト値 (分)：0
観測事象結果に対するユーザーの上書きの有効期間を設定します。 sn_ti.enable_observable_finding_system_override 注: 次のプロパティ (sn_ti.observable_finding_override_expiry) で有効性を定義する必要があります。	観測事象結果に対するユーザーの上書きの有効期間を設定するオプション。観測事象の脅威ルックアップの結果は、この有効期間中はベースシステムによって変更されません。 デフォルト値：いいえ 注: このプロパティを有効にする場合は、適切な値を追加していることを確認してください。
有効性 (分) sn_ti.observable_finding_override_expiry	観測事象結果の有効期間を定義するオプション。 デフォルト値 (分)：なし
指定された日数の間、どのソースからも受けていない攻撃モード/方法は非アクティブとしてマークします sn_ti.attack_mode_inactivate_days	攻撃モード/方法を最後に受信してから、レコードが非アクティブとマークされるまでの日数。 デフォルト値：360 注: [アクティブ] チェックボックスは、デフォルトでは [攻撃モード/方法] フォームに表示されません。ただし、追加することはできます。攻撃モード/方法が非アクティブの場合、他のフォームでは選択できません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明
指定された日数の間どのソースからも受け取っていないインジケーターを非アクティブとしてマークします sn_ti.indicator_inactivate_days	インジケーターを最後に受信してから、レコードが非アクティブとマークされるまでの日数。 デフォルト値：180 注: [アクティブ] チェックボックスは、デフォルトでは [インジケーター] フォームに表示されません。ただし、追加することはできます。インジケーターが非アクティブの場合、他のフォームでは選択できません。
解析可能な STIX 添付ファイルの最大ペイロードサイズ (MB) sn_ti.stix.max_payload_size	解析できる STIX 添付ファイルの最大ペイロード サイズを指定します。 デフォルト値：なし 最大許容値：制限なし
送信 HTTP 接続で TAXII 収集データをフェッチするまでの最大待機時間 (秒) sn_ti.taxii.http.max_timeout	TAXII 収集データの次のパケットをフェッチするまでに送信 HTTP 接続が待機する最大時間を指定します。 デフォルト値：300
TAXII サーバーから 1 回の REST コールで取得されるオブジェクトの最大数 (TAXII バージョン 2.0 および 2.1 にのみ適用) sn_ti.taxii.max_page_size	1 ページで TAXII サーバーから 1 回の REST 呼び出しで取得されるオブジェクトの最大数を指定します。 デフォルト値：5000 最大許容値：50000
TAXII2. X REST 呼び出しの試行失敗の最大回数 sn_ti.taxii2.retry_count	TAXII REST 呼び出しの試行失敗の最大回数を指定します。 デフォルト値：3

3. [保存] をクリックします。

脅威のソースを定義する

脅威インテリジェンス の脅威ソースのリストを管理できます。各ソースには、ソースをクエリする頻度を定義する機能があります。また、脅威ソースをオンデマンドで実行して、必要な脅威情報構造化記述形式 (Structured Threat Information eXpression) (STIX) データをインポートすることもできます。

始める前に
必要なロール：sn_ti.admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
脅威インテリジェンス は、脅威関連情報をインポートするために、STIX と検知指標情報自動交換手順 (Trusted Automated Exchange of Indicator InformationTrusted) (TAXII) の 2 つのテクノロジーを採用しています。

STIX は、セキュリティ侵害のインジケーター (IoC) アクティビティ (IP アドレスやファイルハッシュなど) を含む広範囲のサイバー脅威情報や、攻撃モード/方法などの脅威に関するコンテキスト情報を表すための標準化された構造化言語を提供し、これらの情報はサイバー攻撃者の動機、能力、およびアクティビティをより完全に特徴付けることができます。このように、STIX データは、サイバー脅威から組織を守るための最善の方法に関する貴重な情報を提供するものです。

検知指標情報自動交換手順 (Trusted Automated Exchange of Indicator InformationTrusted) (TAXII) は、サイバー脅威情報の自動交換を促進するために使用されます。TAXII は、サイバー脅威の検出、予防、緩和のために、組織や製品/サービスの境界を超えて実用的なサイバー脅威情報を共有できるようにする一連のサービスとメッセージ交換を定義しています。TAXII プロファイルは、STIX 形式の情報を共有するためのリポジトリとして設定できます。各プロファイルには、1 つ以上の TAXII 収集またはフィードが含まれています。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > ソース > 脅威のソース.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
名前	脅威ソースの名前。
アプリケーション	このレコードを含んでいるアプリケーション。
有効	脅威ソースをアクティブ化するには、チェックボックスをオンにします。
詳細	[統合ファクトリスクリプト] および [プロセッサをレポート] フィールドにスクリプトを表示するには、このチェックボックスをオンにします。
説明	脅威ソースの説明

4. 必要に応じて、[スケジュール] セクションのフィールドに入力します。

フィールド	説明
実行	統合を実行する頻度、[日次 (Daily)]、[週次 (Weekly)]、[定期的 (Periodically)] など。前述のとおり、このフィールドの設定に基づいて後続のフィールドが表示されます。
曜日	統合を実行する日。 ○ [実行] フィールドで [週次 **(Weekly)]** を選択した場合、このフィールドには曜日が表示されます。 ○ [実行] フィールドで [月次 **(Monthly)]** を選択した場合、このフィールドには月日が表示されます。
時刻	統合を開始する時刻。
繰り返し間隔	[実行] フィールドで [定期的 **(Periodically)]** を選択した場合、このフィールドには統合が再度実行されるまでの日数と時間が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
開始中	[実行] フィールドで [定期的 **(Periodically)]** を選択した場合、このフィールドには定期的な更新の起点として使用される日付と時刻が表示されます。
条件付き	条件付きパラメーターを追加する場合は、このフィールドを選択します。
条件	[条件付き **(Conditional)]** チェックボックスをオンにした場合は、ここに条件を入力します。

5. 必要に応じて、[脅威の詳細] セクションのフィールドに入力します。

フィールド	説明
インジケーター	データに明示的にインジケーターが指定されていない場合に使用するインジケーター。ブロックリストが空の場合、観測事象ごとに新しいインジケーターが作成されます。
インジケータータイプ	作成されたが、データに明示的にインジケータータイプが指定されていないインジケーターに使用するインジケータータイプ。
攻撃モード/方法	データに明示的に攻撃モード/方法が指定されていない場合に使用する攻撃モード/方法。
観測事象タイプ	作成されたが、データに明示的に観測事象タイプが指定されていない観測事象に使用する観測事象タイプ。[SI1]
重み付け	信頼性の計算で使用するこのソースの重み付け値を入力します。

注:
[インジケーター]、[インジケータータイプ]、[攻撃モード/方法]、および [観測可能タイプ] の各フィールドの使用方法は実装に固有のものです。デフォルトのプロセッサ SimpleBlocklistProcessor は、ツールヒントに記載されているとおりに動作します。ただし、TAXII の脅威ソースは完全にデータ駆動型です。カスタムの脅威ソースプロセッサであれば、独自の戦略を使用できます。これらのフィールドは基本的に統合/プロセッサに公開するアイテムであり、実装によってその使用方法が決まります。

6. 必要に応じて、[ソースの詳細] セクションのフィールドに入力します。

フィールド	説明
エンドポイント	脅威インテリジェンス が脅威ソースにアクセスする Web サービスのエンドポイント URL を入力します。ロックアイコンをクリックして URL をロックします。
REST メッセージを使用	脅威ソースにアクセスするために REST メッセージが必要な場合は、このチェックボックスをオンにします。**[REST** メッセージ **]** フィールドと **[REST** メソッド] フィールドが必須になります。
REST メッセージ	ルックアップアイコンをクリックし、リストから REST メッセージを選択するか、[新規] をクリックして新しい REST メッセージを定義します。
REST メソッド	ルックアップアイコンをクリックし、リストから REST メッセージを選択するか、[新規] をクリックして新しい REST メソッドを定義します。
統合スクリプト	デフォルトの統合スクリプトは、**[SimpleRESTSecurityDataIntegration]** です。簡単な REST コールを実行し、応答を添付ファイルとして保存して

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	から、添付ファイルをプロセッサに返します。このスクリプトは、ほとんどの組織のニーズに対応しています。必要に応じて、ルックアップアイコンをクリックして、別の統合スクリプトを選択するか、新しい統合スクリプトを定義できます。
統合ファクトリスクリプト	[詳細 **(Advanced)]** チェックボックスをオンにすると、このフィールドには統合スクリプトをビルドするための実際のスクリプトが表示されます。必要に応じてスクリプトを編集できます。この機能はカスタム実装の場合に便利です。通常、ベースシステムの統合では、カスタムコンストラクタロジックは必要ありません。
プロセッサをレポート	デフォルトの統合スクリプトは、**[SimpleBlocklistProcessor]** です。このスクリプトは、シンプルなブロックリスト (URL や IP アドレスなどの観測事象を含む 1 列のドキュメント) を受け取り、観測事象を作成するシンプルなプロセッサです。さまざまな [脅威の詳細] フィールドを使用して、観測事象の作成時に設定するフィールドを決定します。
プロセッサ生成スクリプト	[詳細 **(Advanced)]** チェックボックスをオンにすると、このフィールドにはプロセッサをビルドするための実際のスクリプトが表示されます。必要に応じてスクリプトを編集できます。一般的に、このスクリプトはカスタム実装の場合に便利です。通常、ベースシステムの統合では、カスタムコンストラクタロジックは必要ありません。

7. [Submit] をクリックします。

> **注:**
> 脅威ソースのページネーションを設定する方法の詳細については、『KB1213825』の記事を参照してください。

TAXII プロファイルを作成する

STIX 形式の情報を共有するために、TAXII プロファイルを管理できます。各プロファイルには、1 つ以上の TAXII 収集またはフィードが含まれています。

始める前に
必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > ソース > **TAXII** プロファイル.

2. [**New**] をクリックします。

3. 必要に応じて次のフィールドに入力します。

4. 必要に応じて、[ディスカバリーサービス構成] セクションのフィールドに入力します。

5. 必要に応じて、[コレクションサービス構成] セクションのフィールドに入力します。

6. [Submit] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

IoC リポジトリ

IoC リポジトリには STIX オブジェクトが含まれており、これらの各オブジェクトには特定の情報が含まれています。

関係を介して STIX オブジェクトを結合すると、Cyber 脅威インテリジェンス (CTI) を簡単に表現したり、複雑に表現したりできます。

脅威インテリジェンス は STIX バージョン 1.1、2.0、および 2.1 をサポートしています。

攻撃のモードと方法

攻撃モードと方法は、戦術、テクニック、手順 (TTP) とも呼ばれ、サイバー攻撃者の行動を表します。これらは、これらの攻撃者の行動とその方法を詳細なレベルで特徴付けます。攻撃のモードと方法は STIX 1.1 に適用されます。

たとえば、攻撃モード/方法には、マルウェアを使用してクレジットカードの認証情報を盗む攻撃があります。また、関連する戦術 (下位レベルの詳細) では、悪意のあるコードを含むファイルが添付された標的型メールを送信する攻撃もあります。これらの攻撃では、添付ファイルを開くとコードが実行され、キーボード操作からクレジットカード情報をキャプチャしたり、HTTP を使用してコマンドとコントロールサーバーと通信して情報を転送したりします。

攻撃のモードと方法は STIX 1.1 に適用されます。

攻撃モード/方法を定義する

攻撃モードと方法は STIX データとともにインポートされますが、必要に応じて新しいモード/方法を追加できます。

始める前に
必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 攻撃モード/方法.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
分類タグを選択	レコードにメタデータを追加するために分類タグを設定しアクティブ化した場合、1 つ以上のタグを選択して、攻撃モード/方法の感度を指定できます。 分類タグを設定またはアクティブ化していない場合、このドロップダウンリストは表示されません。
タイトル	この攻撃モード/方法の記述名を入力します。
マルウェアタイプ	この攻撃モード/方法のマルウェアタイプを選択します。利用可能なマルウェアタイプは、STIX データとしてベンダーサーバーから取得されます。
ソース	この攻撃モード/方法の脅威のデータソースを選択します。一部のデータソースはベースシステムに含まれています。必要に応じて、新しいデータソースを作成できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
攻撃メカニズム	この攻撃モード/方法の攻撃メカニズムを選択します。攻撃メカニズムは、システムを攻撃するために使用されるさまざまなテクニックを表します。利用可能な攻撃メカニズムは、STIX データとしてベンダーサーバーから取得されます。
初回確認日	この日付は、STIX データとしてベンダーサーバーから取得されます。
最終確認日	この日付は、STIX データとしてベンダーサーバーから取得されます。
攻撃者タイプ	この攻撃モード/方法の攻撃者タイプを選択します。攻撃者タイプは、サイバー攻撃の脅威をもたらす攻撃者を特徴付けるもので、推定される意図や歴史的に観察された行動などが含まれます。利用可能な攻撃者タイプは、STIX データとしてベンダーサーバーから取得されます。
説明	この攻撃モード/方法の説明を入力します。
処理	この攻撃モード/方法の処理方法の指示を入力します。
意図した効果	この攻撃タイプの意図した効果を入力します。

4. フォームヘッダーを右クリックし、[保存] をクリックします。
次の関連リストのいずれかを表示して、追加情報を表示できます。

関連リスト	説明
関連するインジケーター	脅威のソースによって識別された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
子攻撃モード/方法	親攻撃モード/方法の子である攻撃モード/方法を一覧表示します。
関連タスク	親攻撃モード/方法に関連する変更を一覧表示します。

IoC を攻撃モード/方法に追加する

インジケーターを STIX データとしてインポートするだけでなく、IoC を攻撃モード/方法に手動で追加できます。

始める前に
必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 攻撃モード/方法.
2. IoC を追加する攻撃モードをクリックします。
3. [関連インジケーター **(Related Indicators)]** の関連リストをクリックします。
4. [編集] をクリックします。
5. 必要に応じて、フィルターを使用して追加する IoC を特定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

6. スラッシュバケットを使用して、[関連インジケーター **(Related Indicators)**] リストに IoC を追加します。
7. [保存] をクリックします。

関連する攻撃モード/方法を追加する

攻撃モード/方法を STIX データとしてインポートするだけでなく、関連する攻撃モード/方法を手動で追加できます。

始める前に
必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 攻撃モード/方法.
2. 関連する攻撃モード/方法を追加する攻撃モードをクリックします。
3. [子攻撃モード/方法 **(Child Attack mode/method)**] の関連リストをクリックします。
4. [編集] をクリックします。
5. 必要に応じて、フィルターを使用して現在の攻撃モード/方法に関連付ける攻撃モード/方法を特定します。
6. スラッシュバケットを使用して、[子攻撃モード/方法 **(Child Attack mode/method)**] リストに攻撃モード/方法を追加します。
7. [保存] をクリックします。

関連タスクを攻撃モード/方法に追加する

関連タスク (変更やインシデントなど) を STIX データとしてインポートするだけでなく、それらを攻撃モード/方法に手動で追加できます。

始める前に
必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 攻撃モード/方法.
2. 関連タスクを追加する攻撃モードをクリックします。
3. [関連タスク] の関連リストをクリックします。
4. [編集] をクリックします。
5. 必要に応じて、フィルターを使用して攻撃モード/方法に関連付けるタスクを特定します。
6. スラッシュバケットを使用して、タスクを [関連タスク] リストに追加します。
7. [保存] をクリックします。

セキュリティ侵害のインジケーター

セキュリティ侵害のインジケーター (IoC) は、ネットワークまたはオペレーティングシステムで検出された、侵入を示す可能性のあるアーティファクトです。一般的な IoC は、ウイルス署名と IP アドレス、マルウェアファイルまたは URL の MD5 ハッシュ、またはドメイン名です。IoC は STIX 1.1 および 2.x に適用されます。

IoC には、単一の観測事象または観測事象のコレクション (例：単一の既知の不正な URL、または特定のファイルといくつかの特定のレジストリキー値の存在) があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インシデント応答とコンピューターフォレンジックのプロセスで特定された IoC は、侵入検知システムとウイルス対策ソフトウェアを使用して、今後の攻撃の試みを早期に検出するために使用できます。

IoC は STIX 1.1 および 2.x に適用されます。

IoC を表示する

IoC はインジケーターとも呼ばれ、通常は脅威のデータソースから STIX データとして取得されます。必要に応じて、IoC を作成することもできます。

始める前に
必要なロール：sn_ti.write

手順

1. スケジュール済みジョブが 定義されたデータソースから IoC データを取得したら、次に移動します: 脅威インテリジェンス > **IoC** リポジトリ > インジケーター.
   取得された IoC が一覧表示されます。
2. 表示する IoC をクリックします。
3. 次の情報が表示されます。

フィールド	説明
分類タグを選択	レコードにメタデータを追加するためにセキュリティタグを設定しアクティブ化した場合、1 つ以上のタグを選択して、IoC の感度を指定できます。 セキュリティタグを設定またはアクティブ化していない場合、このドロップダウンリストは表示されません。
タイトル	このインジケーターの記述名。
初回確認日	システム内でこのインジケーターが最初に観測された日付。
最終確認日	システム内でこのインジケーターが観測された直近の日付。
発生回数	インジケーターが発生した回数。
供給回数	定義された脅威のソースからインジケーターがインポートされた回数。
メモ	インジケーターに関する追加のメモ。このフィールドには、JSON キー/値ペアを含めることもできます。

4. 次の関連リストのいずれかをクリックして、追加情報を確認できます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連リンクと関連リスト	説明
	[関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
関連する観測事象	現在のインジケーターにリンクされている観測事象を一覧表示します。
関連する攻撃モード/方法	このインジケーターに関連するものとして識別された関連する攻撃モード/方法を一覧表示します。
関連するタイプ	この IoC に関連する他のインジケータータイプを一覧表示します。
インジケーターソース	このインジケーターのタイプを、ソースの信頼性レベルと共に一覧表示します。
関連タスク	IoC に関連するすべてのタスク、変更、およびインシデントを一覧表示します。
インジケーターメタデータ	[メモ] フィールドに有効な JSON キー/値ペアが含まれている場合、それらは解析され、表示されます。JSON キー/値ペアがない場合、または JSON が無効である場合、この関連リストは表示されません。
セキュリティ注釈	
インジケーターの外部参照	
関連キルチェーンフェーズ	このオブジェクトに関連付けられたキルチェーンフェーズを一覧表示します。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。

関連する観測事象を **IoC** に追加する

観測事象を STIX データとしてインポートするだけでなく、関連する観測事象を IoC に手動で追加できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_ti.write

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > インジケーター.
2. 関連する観測事象を追加するインジケーターをクリックします。
3. [関連する観測事象] の関連リストをクリックします。
4. [編集] をクリックします。
5. 必要に応じて、フィルターを使用して IoC に関連付ける観測事象を特定します。
6. スラッシュバケットを使用して、[関連する観測事象] リストに観測事象を追加します。
7. [保存] をクリックします。

関連する攻撃モード/方法を **IoC** に追加する

関連する攻撃モード/方法を STIX データとしてインポートするだけでなく、関連する攻撃モード/方法を手動で IoC に追加できます。

始める前に
必要なロール：sn_ti.write

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > インジケーター.
2. 関連する攻撃モード/方法を追加するインジケーターをクリックします。
3. [関連する攻撃モード/方法] の関連リストをクリックします。
4. [編集] をクリックします。
5. 必要に応じて、フィルターを使用して IoC に関連付ける攻撃モード/方法を特定します。
6. スラッシュバケットを使用して、[関連する攻撃モード/方法] リストに攻撃モード/方法を追加します。
7. [保存] をクリックします。

関連するインジケータータイプを識別する

IoC に関連付けられたインジケータータイプが定義されていない場合は、すべてのタイプの観測事象が追跡されます。ただし、1 つ以上のインジケータータイプを IoC に関連付けると、その IoC に関連付けることができる観測事象のタイプが制限されます。

始める前に
必要なロール：sn_ti.write

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > インジケーター.
2. インジケータータイプを関連付けるインジケーターをクリックします。
3. [関連タイプ **(Associated Type)**] の関連リストをクリックします。
4. [編集] をクリックします。
5. 必要に応じて、フィルターを使用して IoC に関連付けるインジケーターを特定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. スラッシュバケットを使用して、インジケータータイプを [関連タイプ **(Associated Type)**] のリストに追加します。
7. [保存] をクリックします。

インジケーターソースを識別する

通常、インジケーターソースは脅威のインポートプロセスの一部として自動的に追跡されますが、さらに多くのソースを手動で追加できます。

始める前に
必要なロール：sn_ti.write

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > インジケーター.
2. インジケーターソースを追加するインジケーターをクリックします。
3. [インジケーターソース] の関連リストをクリックします。
4. [編集] をクリックします。
5. 必要に応じて、フィルターを使用して IoC に関連付けるインジケーターソースを特定します。
6. スラッシュバケットを使用して、[インジケーターソース] リストにインジケーターソースを追加します。
7. [保存] をクリックします。

関連タスクを **IoC** に追加する

関連タスク (変更やインシデントなど) を STIX データとしてインポートするだけでなく、それらを IoC に手動で追加できます。

始める前に
必要なロール：sn_ti.write

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > インジケーター.
2. 関連タスクを追加する IoC をクリックします。
3. [関連タスク] の関連リストをクリックします。
4. [編集] をクリックします。
5. 必要に応じて、フィルターを使用して IoC に関連付けるタスクを特定します。
6. スラッシュバケットを使用して、タスクを [関連タスク] リストに追加します。
7. [保存] をクリックします。

観測事象

観測事象は、コンピューターやネットワークの操作に関連するステートフルなプロパティ (ファイルの MD5 ハッシュやレジストリキーの値など) または測定可能なイベント (レジストリキーの作成やファイルの削除など) を表します。観測事象は STIX 1.1 および 2.x に適用されます。

サイバー観測事象のセットは、サイバー脅威の動作を表すコンテキスト情報と組み合わせると、セキュリティ侵害のインジケーターを特定するのに役立ちます。

観測事象は STIX 1.1 および 2.x に適用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

観測事象を定義する

観測事象は、STIX データとしてベンダーサーバーから取得されます。ただし、必要に応じて観測事象を作成できます。

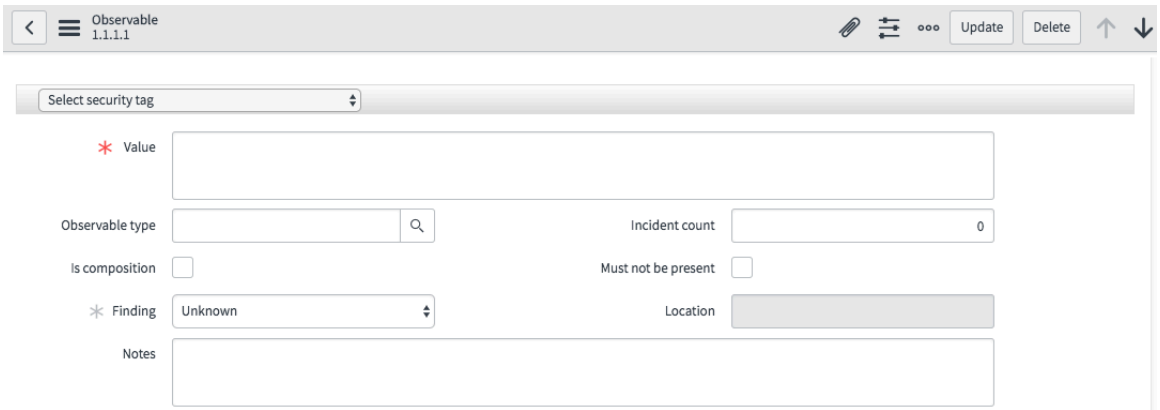
始める前に

必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 観察事項.

2. [**New**] をクリックします。



3. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
分類タグを選択	レコードにメタデータを追加するためにセキュリティタグを設定しアクティブ化した場合、1 つ以上のタグを選択して、観測事象の感度を指定できます。 セキュリティタグを設定またはアクティブ化していない場合、このドロップダウンリストは表示されません。
値	観測事象に関連付けられている値 (IP アドレスやハッシュなど)。 **注:** IP アドレスまたはハッシュに対する脅威スキャン がマルウェアまたはその他のエラーを返した場合、IP アドレスまたはハッシュの値が観測事象 [sn_ti_observable] テーブルに自動的に追加されます。そのため、[観測事象] フォームから検索できます。
観測可能タイプ	IP アドレスやファイルハッシュなどの観測事象の分類を選択します。これらの観測事象タイプは、[観測事象タイプ] モジュールで定義されます。
インシデント数	観測事象値が検出された回数。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
構成である	このフィールドは、観測事象レコードが保存された後にのみ表示されます。 [観測事象タイプ] が [観測事象構成] 以外に設定されていて、この新しい観測事象が構成である場合は、このチェックボックスをオンにします。 [観測事象タイプ] が既に [観測事象構成] に設定されている場合、このチェックボックスはオンになっていて、読み取り専用になります。 観測事象構成は、子観測事象を含む観測事象です。
結果	次のいずれかを選択します。 ○ [悪意がある]：観測事象が組織に有害であることを示します。 ○ [不審]：観測事象が組織に有害であるおそれがあることを示します。 ○ [クリーン]：観測事象が組織に有害でないことを示します。 ○ [不明]：観測事象の結果がまだ確定していないことを示します。 ○ デフォルト値：[不明]。詳細については、「脅威のルックアップ検索計算ツール」を参照してください。 **注:** アップグレード後、既存の観測事象は [悪意がある] としてマークされます。
演算子	このフィールドは、[構成である] チェックボックスがオンの場合にのみ表示されます。このフィールドの設定に応じて、関連するインジケーターが存在するかどうかを決定するときに観測事象とその子が考慮されます。 関連するインジケーターが存在すると判断されるためにすべての子観測事象が存在する必要がある場合は、このフィールドを **[AND]** に設定します。 関連するインジケーターが存在すると判断されるためにいずれかの子観測事象が存在する必要がある場合は、このフィールドを **[OR]** に設定します。
存在できない	このフィールドは、観測事象レコードが保存された後にのみ表示されます。 このフィールドを選択した場合、観測事象が存在しないことが潜在的な問題 (レジストリーキーの欠落など) であることを示します。
ロケーション	2 つのプロパティの設定と 1 つのスクリプトインクルード定義を使用して、このフィールドに IoC データをさらにロードする をロードできます。
メモ	観測事象に関する追加のメモを入力します。

4. フォームヘッダーを右クリックし、[保存] をクリックします。
次の関連リストのいずれかをクリックして、追加情報を表示できるようになりました。

関連リスト	説明
関連するインジケーター	脅威のソースによって識別された、インジケーターを一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連リスト	説明
関連タスク	観測事象に関連する変更を一覧表示します。
子観測事象	脅威のソースによって識別された、関連する観測事象を一覧表示します。
IP の一致リソース	観測事象が IP アドレスの場合、このリストには、一致する IP アドレスを持つすべてのリソース (構成アイテム) が表示されます。
観測事象ソース	この観測事象のタイプを、ソースの信頼性レベルと共に一覧表示します。
セキュリティ注釈	この観測事象に追加されたセキュリティ注釈を一覧表示します。

関連する **IoC** を観測事象に追加する

観測事象を STIX データとしてインポートするだけでなく、関連する観測事象を IoC に手動で追加できます。

始める前に
必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 観察事項.
2. 関連する IoC を追加する観測事象をクリックします。
3. [関連インジケーター **(Related Indicators)**] の関連リストをクリックします。
4. [編集] をクリックします。
5. 必要に応じて、フィルターを使用して観測事象に関連付けるインジケーターを特定します。
6. スラッシュバケットを使用して、[関連インジケーター **(Related Indicators)**] リストにインジケーターを追加します。
7. [保存] をクリックします。

関連タスクを観測事象に追加する

関連タスク (変更やインシデントなど) を STIX データとしてインポートするだけでなく、それらを観測事象に手動で追加できます。

始める前に
必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 観察事項.
2. 関連タスクを追加する観測事象をクリックします。
3. [関連タスク] の関連リストをクリックします。
4. [編集] をクリックします。
5. 必要に応じて、フィルターを使用して観測事象に関連付けるタスクを特定します。
6. スラッシュバケットを使用して、タスクを [関連タスク] リストに追加します。
7. [保存] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連する観測事象を追加する

観測事象を STIX データとしてインポートするだけでなく、関連する観測事象を手動で追加できます。

始める前に
必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 観察事項.
2. 関連する観測事象を追加する観測事象をクリックします。
3. [子観測事象 **(Child Observables)]** の関連リストをクリックします。
4. [編集] をクリックします。
5. 必要に応じて、フィルターを使用して現在の観測事象に関連付ける観測事象を特定します。
6. スラッシュバケットを使用して、[子観測事象 **(Child Observables)]** リストに観測事象を追加します。
7. [保存] をクリックします。

IoC データをさらにロードする

2 つのプロパティの設定とスクリプトインクルードの定義に応じて、観測事象フォームに IP アドレスと Web サイトの位置情報をロードできます。さらにカスタマイズして、国コード、都市名などの他の情報を追加することもできます。

始める前に
次の 2 つのプロパティを設定する必要があります。

- **[IP** アドレス/URL の追加情報を取得するためのドメイン名] [sn_ti.ip_lookup.web_site]
- [上記のドメインに使用される **API** キー (存在する場合)] [sn_ti.ip_lookup.api_key]

必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 観察事項.
2. IoC データをさらに表示する観測事象の IP アドレスまたは URL をクリックします。
   [場所] フィールドには、IoC の位置情報が表示されます。
3. [データを追加] ボタンをクリックして、追加の IoC データをロードします。
4. 観測事象フォームを設定して、国コードや都市コードなど、場所に関連した他のフィールドを追加することもできます。

> **注:**
> 場所に関連した情報をさらにロードするには、**[ThreatAdditionalInfo]** スクリプトインクルードを編集し、追加情報を提供する Web サイトからの適切な API キーを指定します。

観測事象ソースを識別する

観測事象のソースが定義されていない場合は、すべてのソースタイプが使用されます。ただし、1 つ以上の脅威ソースを観測事象に追加すると、使用されるソースが制限されます。

始める前に
必要なロール：sn_ti.admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 観察事項.
2. 観測事象ソースを追加する観測事象をクリックします。
3. [観測事象ソース **(Observable Sources)**] の関連リストをクリックします。
4. [編集] をクリックします。
5. 必要に応じて、フィルターを使用して観測事象に関連付けるソースを特定します。
6. スラッシュバケットを使用して、[観測事象ソース **(Observable Sources)**] リストに観測事象ソースを追加します。
7. [保存] をクリックします。

観測事象のルックアップを実行する

脅威インテリジェンスのルックアップを 1 つ以上の観測事象で実行し、既知のセキュリティ上の脅威に関連するかどうかを判断します。実行されるスキャンの実装は、アクティブ化した実装によって異なります。

始める前に
ルックアップを実行する前に、脅威インテリジェンスプラグインをアクティブ化する必要があります。1 つ以上のスキャン実装用のプラグインもインストールする必要があります。

- Crowdstrike Falcon Intelligence 統合
- OPSWAT Metadefender
- Security Operations Have I been pwned?
- VirusTotal

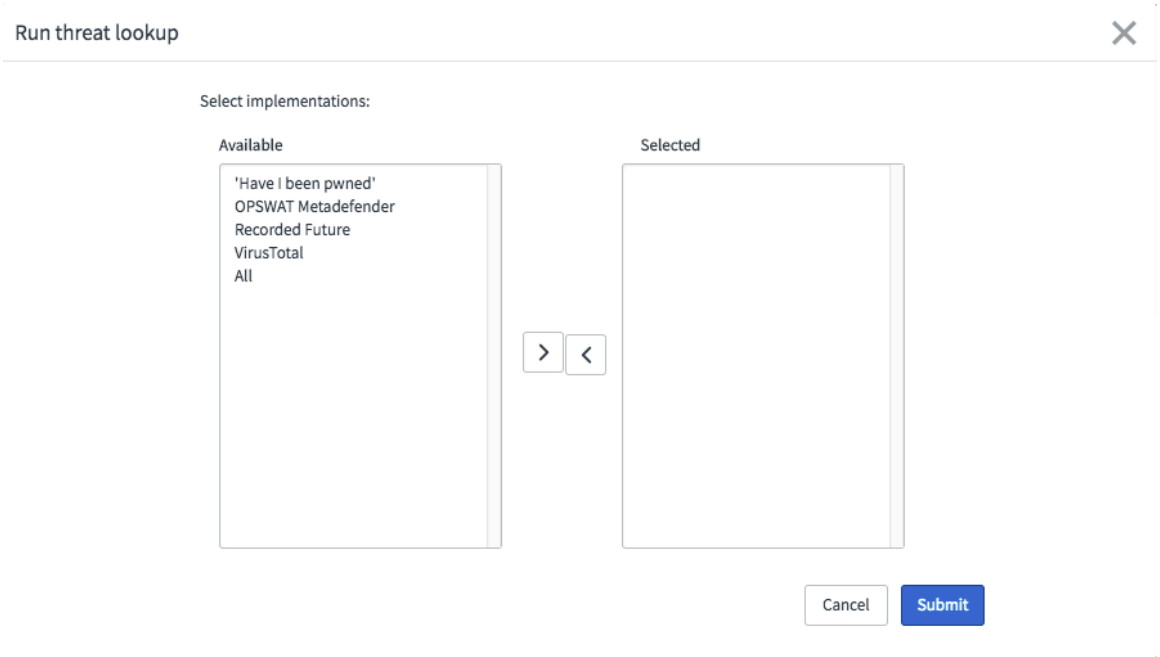
必要なロール：sn_ti.write

手順

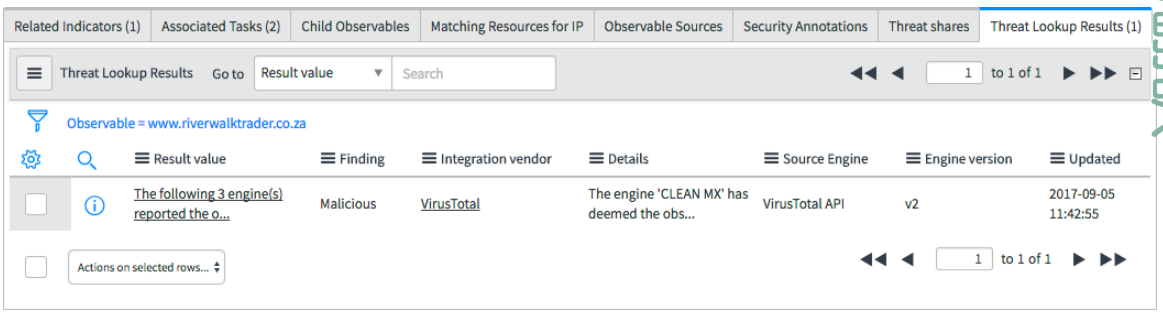
1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 観察事項.
2. 次のいずれかの手順を実行します。
   - 複数の観測事象に対してルックアップを実行するには、観測事象を選択し、[選択した行のアクション] をクリックして、[脅威のルックアップを実行] を選択します。
   - 単一の観測事象でルックアップを実行するには、観測事象レコードを開き、[脅威のルックアップを実行] 関連リンクをクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. 使用する脅威のルックアップの実装を選択するか、[すべて] を選択してアクティブなすべての実装を使用してルックアップを実行し、[送信] をクリックします。
   脅威のルックアップが開始されたことを示すメッセージが表示されます。Security Operations Integration - 脅威のルックアップフロー が実行され、選択した脅威のルックアップ実装の実装ワークフローも実行されます。ルックアップが実行され、結果が生成されます。
4. ルックアップが完了したら、[脅威のルックアップの結果] タブをクリックして結果を表示します。



[最近の脅威のルックアップ結果 **(Recent Threat Lookup Result)**]：[最近の脅威のルックアップ結果 **(Recent Threat Lookup Result)**] タブをクリックすると、各統合ベンダーからの最新または最近の脅威のルックアップ結果を表示することもできます。

> **注:**
> [最近の脅威のルックアップ結果 **(Recent Threat Lookup Result)**] タブはベースシステムには含まれていません。

このタブを有効にするには、次の手順を実行します。

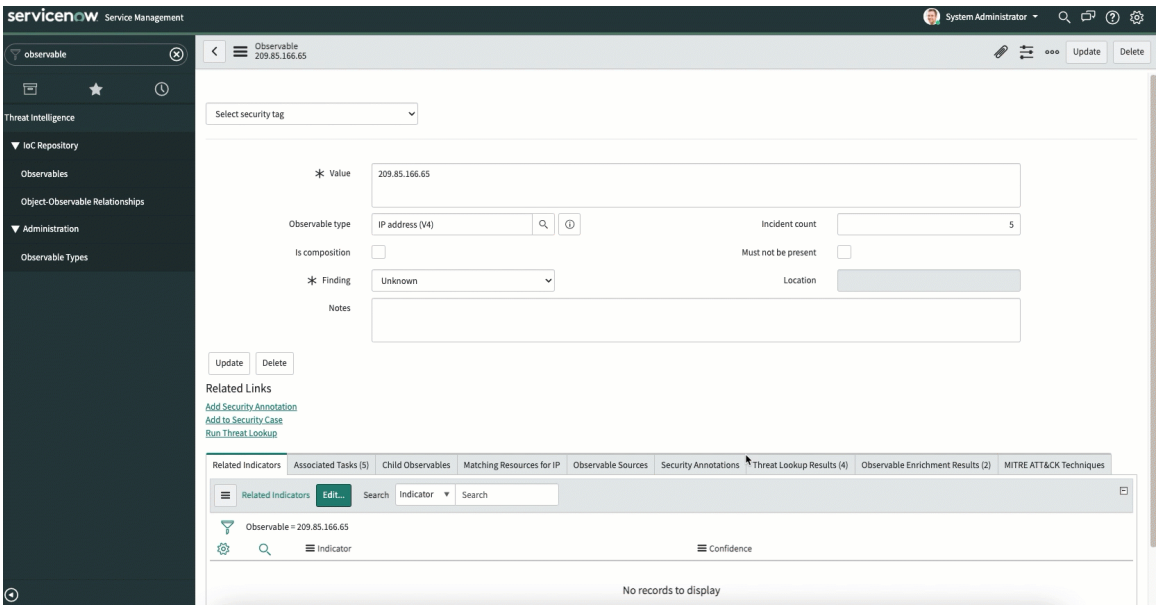
a. フォームヘッダーを右クリックします。

b. 次のように移動する。 構成 > 関連リスト.

c. [利用可能] リストで [最近の脅威のルックアップ結果 **(Recent Threat Lookup Results)**] を見つけて、[選択済み] リストに移動します。

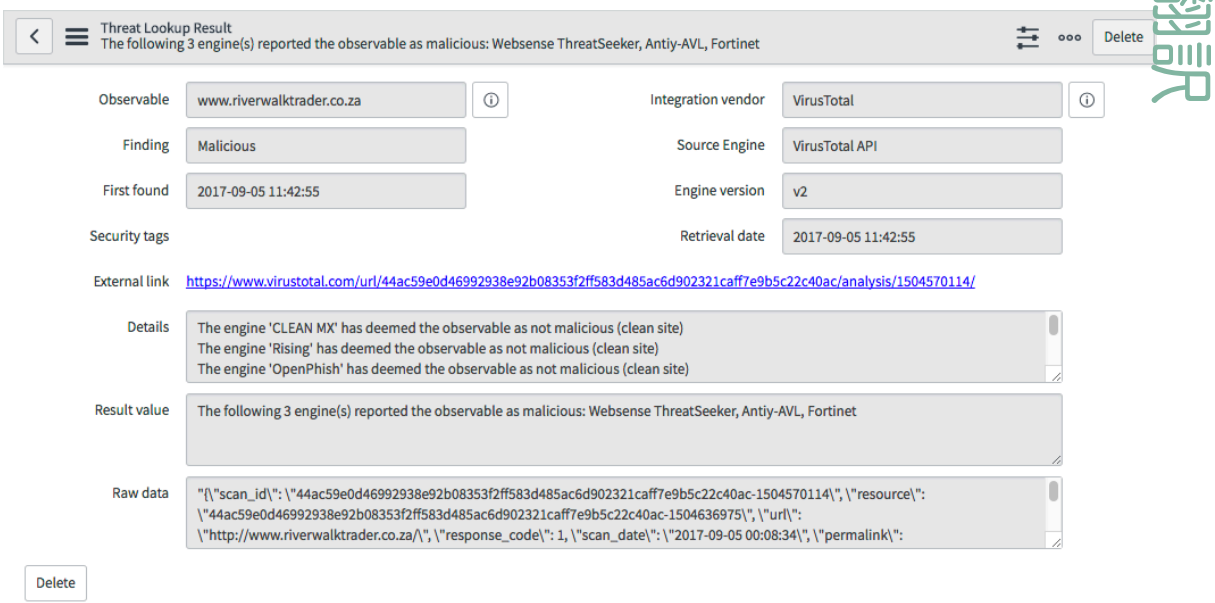
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

d. [保存] をクリックします。
[最近の脅威のルックアップ結果 **(Recent Threat Lookup Result)]** タブで、各統合ベンダーからの最近の脅威のルックアップ結果を表示できるようになりました。



5. 特定のルックアップの生の結果など、詳細を表示するには、[結果の値] をクリックします。

注:
VirusTotal または OPSWAT Metadefender 実装が使用されると、以下に示すように詳細が統合されます。



観測事象に対して脅威の拡張を実行する

脅威インテリジェンスの拡張を 1 つ以上の観測事象で実行し、既知のセキュリティ上の脅威に関連するかどうかを判断します。実行される実装は、アクティブ化した実装によって異なります。

始める前に

拡張を実行する前に、脅威インテリジェンスプラグインをアクティブ化する必要があります。1 つ以上の拡張実装用のプラグインもインストールする必要があります。

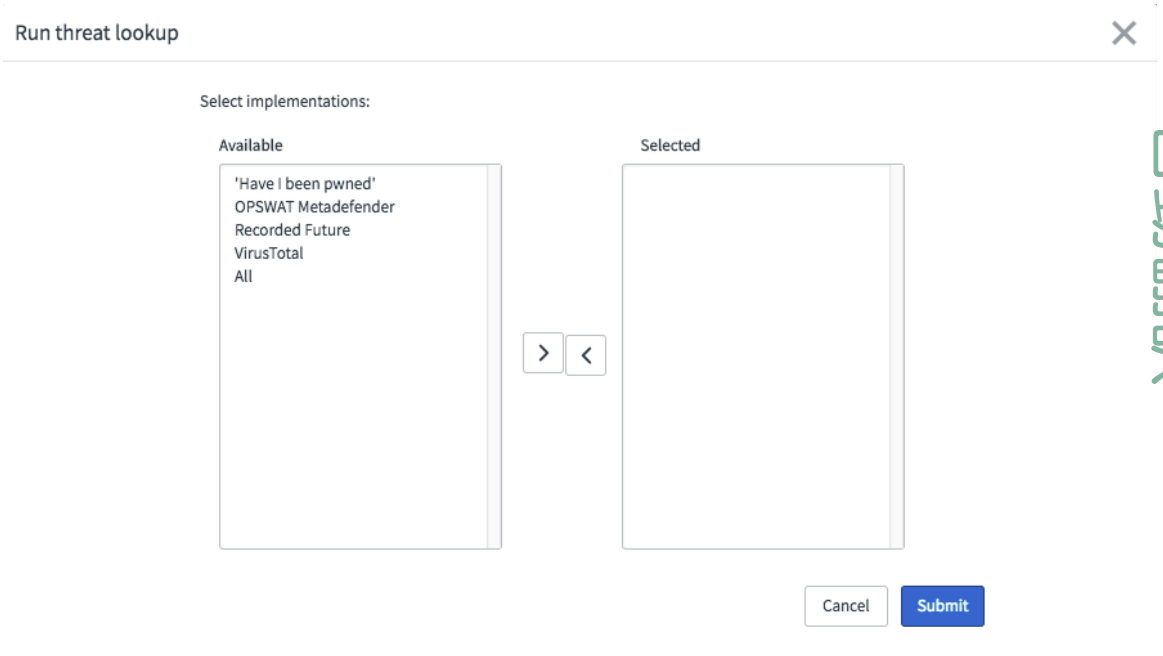
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- Crowdstrike Falcon Intelligence 統合
- OPSWAT Metadefender
- Security Operations Have I been pwned?
- VirusTotal
- WhoIs?

必要なロール：sn_ti.admin

手順

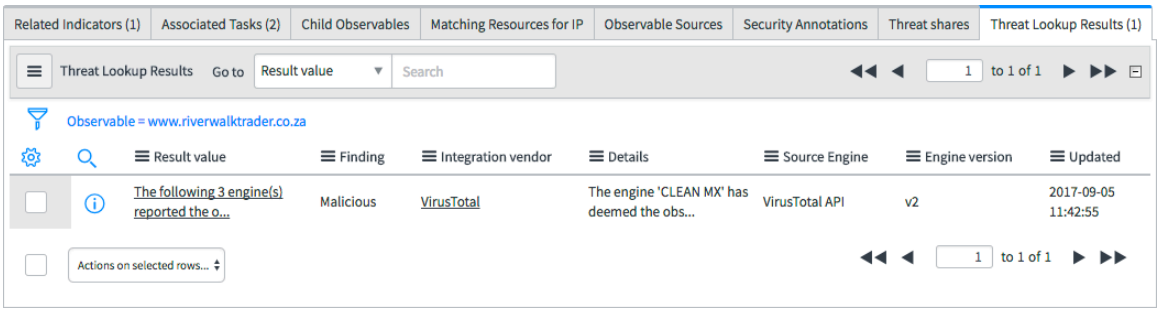
1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 観察事項.
2. 次のいずれかの手順を実行します。
   - 複数の観測事象に対してルックアップを実行するには、観測事象を選択し、[選択した行のアクション] をクリックして、[脅威のルックアップを実行] を選択します。
   - 単一の観測事象でルックアップを実行するには、観測事象レコードを開き、[脅威のルックアップを実行] 関連リンクをクリックします。



3. 使用する脅威のルックアップの実装を選択するか、[すべて] を選択してアクティブなすべての実装を使用してルックアップを実行し、[送信] をクリックします。
   脅威のルックアップが開始されたことを示すメッセージが表示されます。Security Operations Integration - 脅威のルックアップフロー が実行され、選択した脅威のルックアップ実装の実装ワークフローも実行されます。ルックアップが実行され、結果が生成されます。
4. ルックアップが完了したら、[脅威のルックアップの結果] タブをクリックして結果を表示します。

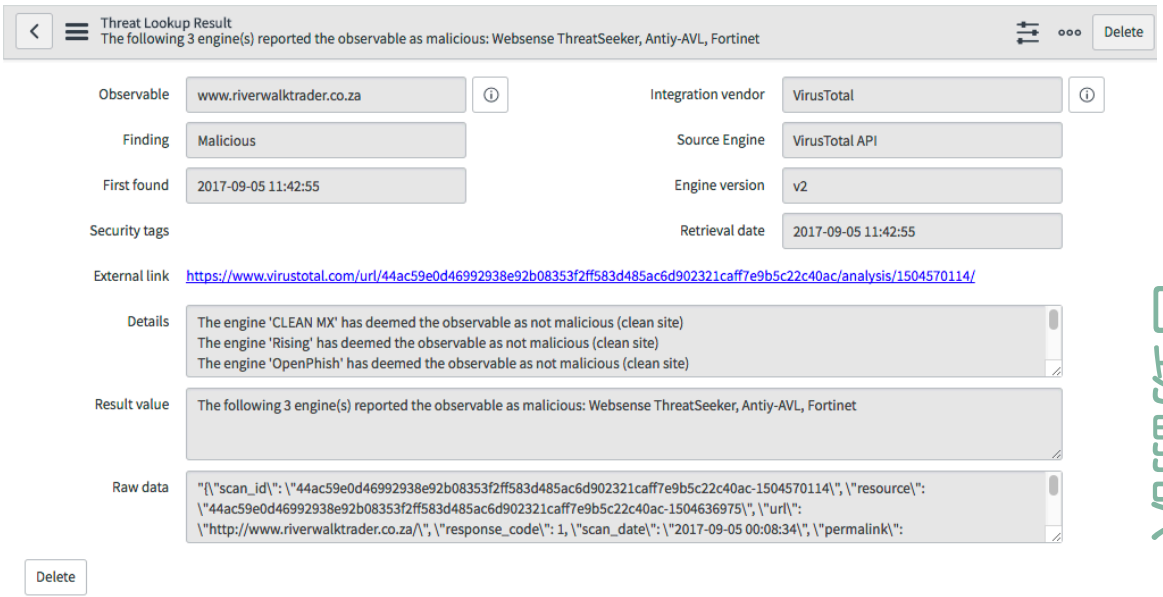
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. 特定のルックアップの生の結果など、詳細を表示するには、[結果の値] をクリックします。

注:
VirusTotal または OPSWAT Metadefender 実装が使用されると、以下に示すように詳細が統合されます。



自動翻訳

攻撃パターン

攻撃パターンは、攻撃者がターゲットを侵害しようとする方法を記述する戦術、テクニック、手順 (TTP) の一種です。攻撃パターンは STIX 2.x に適用されます。

攻撃パターンは、攻撃を分類するために使用されます。これらは、特定の攻撃をパターンに一般化し、攻撃がどのように実行されるかについての詳細な情報を提供します。

たとえば、スピアフィッシングは、リンクをクリックしたり、添付ファイルを開いてマルウェアに感染させることを目的に、入念に細工したメールメッセージを攻撃者が送信する一般的な攻撃です。攻撃パターンは具体的であり、特定の攻撃者によるスピアフィッシング (例：標的がコンテストに勝った) なども攻撃パターンになります。

攻撃パターンの定義

攻撃を分類できるように攻撃パターンを定義します。

始める前に

必要なロール：sn_ti.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 攻撃パターン.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

次のタスク

次の関連リストのいずれかをクリックすると、攻撃パターンに関連するオブジェクトの追加情報が表示できます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
関連キルチェーンフェーズ	このオブジェクトに関連付けられたキルチェーンフェーズを一覧表示します。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
対処措置	このオブジェクト (攻撃を阻止するための技術的または自動応答 (パッチの適用、ファイアウォールの再構成)) に関連付けられた対処措置を一覧表示します。
ID	このオブジェクトに関連付けられた ID のリスト。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連リンクと関連リスト	説明
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

キャンペーン

キャンペーンは、攻撃者の行動をグループ化したものです。これらの動作は、一連の特定の標的に対して時間の経過とともに発生する一連の悪意のあるアクティビティまたは攻撃を表します。キャンペーンは STIX 2.x に適用されます。

通常、キャンペーンには明確に定義された目標があり、侵入セットの一部である場合があります。

キャンペーンは、多くの場合、侵入セットと攻撃者に起因します。攻撃者は、侵入セットの既知のインフラストラクチャを再利用するか、そのキャンペーンを実行するための新しいインフラストラクチャをセットアップする可能性があります。

キャンペーンでは、ユーザーまたは標的とするリソースに対して発生するインシデントと、使用するリソースに共通の目標があります。

たとえば、犯罪組織が ACME 銀行の役員を攻撃したとします。彼らは、特定のマルウェアの亜種と新しいサーバーを使用して攻撃し、別の銀行との今後の合併に関する機密情報を取得します。

キャンペーンの定義

キャンペーンを定義して攻撃者の行動をグループ化します。

始める前に

必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > キャンペーン.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

次のタスク

次の関連リストのいずれかをクリックすると、キャンペーンに関連するオブジェクトの追加情報が表示できます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連リンクと関連リスト	説明
	ブジェクト識別子を指定するために使用されます。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
ID	このオブジェクトに関連付けられた ID のリスト。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

自動翻訳

対処措置

対処措置は、攻撃を阻止するため、または進行中の攻撃に対処するために実行されるアクションです。対処措置は STIX 2.x に適用されます。

対処措置は、技術的または自動化された対応 (パッチの適用、ファイアウォールの再構成) を示しています。また、従業員のトレーニングやポリシーの変更など、高レベルのアクションを記述することもできます。

たとえば、脆弱性を緩和する対処措置には、それを修正するパッチの適用が含まれます。

対処措置の定義

攻撃を阻止したり、進行中の攻撃に対処するための対処措置を定義します。

始める前に

必要なロール：sn_ti.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 対処措置.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

次のタスク
次の関連リストのいずれかをクリックすると、対処措置に関連するオブジェクトの追加情報が表示されます。

関連リンク	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

ID

ID は、実際の個人、組織、またはグループ (ACME, Inc.)、および個人、システム、またはグループのクラス (ファイナンスセクター) を表します。ID は STIX 2.x に適用されます。

ID SDO は、基本的な識別情報、連絡先情報、および ID が属するセクターをキャプチャできます。ID は、攻撃の標的、情報ソース、オブジェクト作成者、および攻撃者の ID を表します。

ID の定義

実際の個人、組織、またはグループを表す ID を定義します。

始める前に
必要なロール：sn_ti.admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > **ID**.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

次のタスク
次の関連リストのいずれかをクリックすると、ID に関連するオブジェクトの追加情報が表示されます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。

インフラストラクチャ

インフラストラクチャ SDO は、戦術、テクニック、手順 (TTP) の一種です。これらは、攻撃の何らかの目的をサポートするためのシステム、ソフトウェアサービス、および関連する物理または仮想リソースを表します。インフラストラクチャは STIX 2.x に適用されます。

攻撃の要素は、他の SDO または SCO によって表されます。これに対し、インフラストラクチャ SDO は、インフラストラクチャを構成するデータの名前付きグループを表します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インフラストラクチャの例には、攻撃で使用される C2 サーバー、防御の一部であるデバイス (サーバー)、または攻撃の標的となるデータベースサーバーが含まれます。

インフラストラクチャの定義

攻撃の何らかの目的をサポートするためのシステム、ソフトウェアサービス、および関連する物理または仮想リソースであるインフラストラクチャを定義します。

始める前に

必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > インフラストラクチャ.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

次のタスク

次の関連リストのいずれかをクリックして、追加情報を表示できるようになりました。他のオブジェクトをインフラストラクチャに関連付けることもできます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
関連タイプ	このオブジェクトに関連付けられたインジケータータイプを一覧表示します。
関連キルチェーンフェーズ	このオブジェクトに関連付けられたキルチェーンフェーズを一覧表示します。
関連する観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
関連インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連リンクと関連リスト	説明
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
観測データ	このオブジェクトに関連付けられた観測データを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

侵入セット

侵入セットは、共通のプロパティを持つ攻撃者の行動とリソースのグループ化されたセットです。通常、侵入セットには単一の組織が含まれます。侵入セットは STIX 2.x に適用されます。

侵入セットは、複数のキャンペーンまたはその他のアクティビティをキャプチャできます。これらのアクティビティは、既知または不明な攻撃者を示す属性を共有しています。

攻撃の背後にいる攻撃者が不明な場合でも、新しいアクティビティを侵入セットに関連付けることができます。攻撃者は、ある侵入セットから別の侵入セットのサポートに移行することも、複数の侵入セットをサポートすることもできます。

侵入セットは攻撃パッケージ全体であり、潜在的に複数の目的を達成するために複数のキャンペーンで長期間使用される可能性があります。

侵入セットの定義

共通のプロパティを持つ攻撃者の行動とリソースのグループ化されたセットである侵入セットを定義します。

始める前に

必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 委託セット.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のタスク
次の関連リストのいずれかをクリックすると、侵入セットに関連するオブジェクトの追加情報が表示されます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
関連する攻撃の動機	この侵入セットで達成しようとする理由の第 2 の動機を一覧表示します。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
ID	このオブジェクトに関連付けられた ID のリスト。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

場所

場所は地理的な場所を表します。場所は、主に他の SDO にコンテキストを提供するために使用されます。場所は STIX 2.x に適用されます。

場所には、地域 (北米)、住所 (米国、ニューヨーク)、緯度、経度の一部またはすべてを含めることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

場所 SDO は、ID または侵入セットに関連付けて、ID または侵入セットがその場所にあることを示すことができます。また、マルウェアまたは攻撃パターンに関連付けて、標的の被害者が特定の場所にいることを示すこともできます。

たとえば、関係で場所を使用して、Bourgeois Swallow 侵入セットが東ヨーロッパから発信されていることを説明できます。

次のプロパティまたはプロパティのセットのうち、少なくとも 1 つを指定する必要があります。

- region
- country
- latitude または longitude

場所の定義

地理的な場所を定義して、他の SDO に多くのコンテキストを提供します。

始める前に

必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 所在地.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

次のタスク

次の関連リストのいずれかをクリックすると、場所に関連するオブジェクトの追加情報が表示されます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
ID	このオブジェクトに関連付けられた ID のリスト。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連リンクと関連リスト	説明
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。

マルウェア

マルウェアは、悪意のあるコードを表す TTP の一種です。これは、システムに密かに挿入されるプログラムを指します。マルウェアは STIX 2.x に適用されます。

マルウェアの目的は、被害者のデータ、アプリケーション、またはオペレーティングシステム (OS) の機密性、完全性、または可用性を侵害することです。

マルウェア SDO は、分析から導出されたデータからマルウェアインスタンスとファミリを特徴付け、識別、分類します。この SDO は、マルウェアの仕組みと動作に関する詳細情報をキャプチャします。

マルウェアの定義

悪意のあるコードを表すマルウェアを定義します。

始める前に

必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > マルウェア.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

次のタスク

次の関連リストのいずれかをクリックすると、マルウェアに関連するオブジェクトの追加情報が表示されます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

関連リンクと関連リスト	説明
	[関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
関連タイプ	このオブジェクトに関連付けられたインジケータータイプを一覧表示します。
関連機能	このオブジェクトで識別され、関連付けられた機能を一覧表示します。
関連キルチェーンフェーズ	このオブジェクトに関連付けられたキルチェーンフェーズを一覧表示します。
関連する観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
関連付けられたマルウェア	このオブジェクトで識別された関連マルウェアを一覧表示します。
関連オペレーティングシステム	オブジェクトが実行可能なオペレーティングシステム。これは、仮想化されたオペレーティングシステムとベアメタルで実行されているオペレーティングシステムに適用されます。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
対処措置	このオブジェクト (攻撃を阻止するための技術的または自動応答 (パッチの適用、ファイアウォールの再構成)) に関連付けられた対処措置を一覧表示します。
ID	このオブジェクトに関連付けられた ID のリスト。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア分析	このオブジェクトに関連付けられたマルウェア分析レポートを一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連リンクと関連リスト	説明
報告された観測事象	このオブジェクトの一部として報告された観測事象を一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

マルウェア分析

マルウェア分析は、マルウェアのメタデータと結果をキャプチャします。マルウェア分析は STIX 2.x に適用されます。

マルウェア分析には、マルウェアのインスタンスまたはファミリに対して実行される静的分析または動的分析が含まれます。

マルウェア分析の定義

マルウェアのインスタンスまたはファミリで実行された特定の静的または動的分析のメタデータと結果をキャプチャするマルウェア分析を定義します。

始める前に

必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > マルウェア分析.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

次のタスク

次の関連リストのいずれかをクリックすると、マルウェア分析に関連するオブジェクトの追加情報が表示されます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連リンクと関連リスト	説明
関連付けられたマルウェア	このオブジェクトで識別された関連マルウェアを一覧表示します。
報告された観測事象	このオブジェクトの一部として報告された観測事象を一覧表示します。
インストール済みソフトウェア	マルウェアのインスタンスまたはファミリの動的分析に使用される、オペレーティングシステムにインストールされているすべての非標準ソフトウェアを一覧表示します。

観測データ

観測データは、STIX サイバー観測可能オブジェクト (SCO) を使用して、ファイル、システム、ネットワークなどのサイバーセキュリティ関連エンティティに関する情報を伝えます。観測データは STIX 2.x に適用されます。

観測データは、単一のエンティティ (ファイル、ネットワーク接続) の単一の観測事象と、エンティティの複数の観測事象の集計の両方をキャプチャします。

観測データを単独で (関係なしで) 使用して、任意のソースから収集された生データを提供することができます。ソースには、アナリストレポート、サンドボックス、ネットワークおよびホストベースのディスカバリーツールが含まれます。

たとえば、観測データは、IP アドレス、ネットワーク接続、ファイル、またはレジストリキーに関する情報をキャプチャできます。観測データはインテリジェンスのアサーションではなく、意味を示すコンテキストがない生の情報です。

観測データの定義

STIX サイバー観測可能オブジェクト (SCO) を用いて、ファイル、システム、ネットワークなどのサイバーセキュリティ関連エンティティに関する情報を伝える観測データを定義します。

始める前に

必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 観測データ.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

次のタスク

次の関連リストのいずれかをクリックすると、観測データに関連するオブジェクトの追加情報が表示されます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連リンクと関連リスト	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
関連する観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。

攻撃者

攻撃者は、悪意を持って行動する個人、グループ、または組織です。攻撃者は STIX 2.x に適用されます。

攻撃者は侵入セットではありませんが、時間の経過とともにさまざまな侵入セット、グループ、または組織をサポートするか、それらと関係する可能性があります。

攻撃者は、自身のリソースと侵入セットのリソースを使用して攻撃し、標的に対してキャンペーンを実行します。

攻撃者は、その動機、能力、目標、高度なレベル、過去のアクティビティ、アクセス可能なリソース、および組織内での役割によって特定できます。

攻撃者の定義

攻撃者 (悪意を持って行動する個人、グループ、または組織) を定義します。

始める前に

必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 攻撃者.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

次のタスク

次の関連リストのいずれかをクリックすると、攻撃者に関連するオブジェクトの追加情報が表示されます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連リンクと関連リスト	説明
	[関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
関連タイプ	このオブジェクトに関連付けられたインジケータータイプを一覧表示します。
関連付けられているロール	攻撃者に関連するロールを一覧表示します。
関連する攻撃の動機	攻撃者に関連する攻撃の動機を一覧表示します。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
ID	このオブジェクトに関連付けられた ID のリスト。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

脅威グループ化

脅威グループ化オブジェクトは、参照される STIX オブジェクトに共有コンテキストがあることを明示的に示します。脅威グループ化は STIX 2.x に適用されます。

脅威グループ化オブジェクトは一連のデータを表しますが、十分に分析することで、データが成熟し、インシデントまたは脅威レポートを STIX レポートオブジェクトとして提供できます。たとえ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ば、グループ化を使用して、進行中の調査の特徴を明らかにし、セキュリティイベントまたはインシデントにすることができます。

脅威グループ化オブジェクトを使用して、参照されている STIX オブジェクトが進行中の分析プロセスに関連していると判断することもできます。たとえば、脅威アナリストは、脅威コミュニティの他のユーザーと協力して一連のキャンペーンとインジケーターを調べることができます。

脅威グループ化 SDO には、SDO、SCO、および SRO への参照のリスト、コンテンツで共有されるコンテキストの明示、テキストによる説明、およびグループ化の名前が含まれています。

脅威グループ化の定義

脅威グループ化を、共有コンテキストを持つオブジェクトとして定義します。

始める前に
必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 脅威グループ化.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

次のタスク
次の関連リストのいずれかをクリックすると、脅威グループ化に関連するオブジェクトの追加情報が表示されます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
グループ化されたオブジェクト	脅威グループ化の一部としてグループ化されたオブジェクトを一覧表示します。
グループ化されたインジケーター	脅威グループ化の一部としてグループ化されたインジケーターを一覧表示します。
グループ化された観測事象	脅威グループ化の一部としてグループ化された観測事象を一覧表示します。

マーキング定義

マーキング定義オブジェクトは、特定のマーキングを示します。

データのマーキングは、データを使用および共有する方法に関する制限、権限、およびその他のガイダンスを示します。

たとえば、データを再共有してはならない、または保存中のデータを暗号化する必要があるという制限付きでデータを共有できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

STIX では、データマーキングはマーキング定義オブジェクトを使用して指定されます。これらの定義は、オブジェクトマーキングを使用して STIX オブジェクトに適用され、詳細なマーキングを介して STIX オブジェクトの個々のプロパティに適用されます。

マーキング定義の定義

特定のマーキングを表すマーキング定義を定義します。

始める前に
必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > マーキング定義.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

次のタスク
次の関連リストのいずれかをクリックすると、マーキング定義に関連するオブジェクトの追加情報が表示されます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
マークされたオブジェクト	マーキング定義でマークされたオブジェクトのリスト。
マークされたインジケーター	マーキング定義でマークされたインジケーターのリスト。

自動翻訳

脅威メモ

脅威メモは、そのメモが関連する STIX オブジェクト、マーク定義オブジェクト、または言語コンテンツオブジェクトに含まれていない追加の分析を提供するための情報テキストを提供します。脅威メモは STIX 2.x に適用されます。

たとえば、アナリストが別の組織によって作成されたキャンペーンオブジェクトにメモを追加する場合があります。そのメモには、ハッカーフォーラムでそのキャンペーンに関連する投稿を見たことを示すことができます。

メモは通常、人間のアナリストによって作成され、人間向けのテキストで構成されます。メモには、メモを作成した作成者をキャプチャするための追加のプロパティが含まれています。

脅威メモの定義

既存のオブジェクトでは利用できない詳細なコンテキストまたは分析を提供する脅威メモを定義します。

始める前に
必要なロール：sn_ti.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 脅威メモ.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

次のタスク
次の関連リストのいずれかをクリックすると、脅威メモに関連するオブジェクトの追加情報が表示されます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
関連オブジェクト	脅威メモが適用されるオブジェクトのリスト。
関連するインジケーター	脅威メモが適用されるインジケーターのリスト。
関連する観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。

脅威に関する意見

意見は、別のエンティティによって生成された STIX オブジェクト内の情報の正確性を評価するものです。脅威に関する意見は STIX 2.x に適用されます。

意見プロパティは、固定スケールを使用して賛成または反対のレベルをキャプチャします。固定スケールは、複数の意見にまたがる一貫した統計操作を可能にする数値マッピングもサポートしています。

たとえば、消費組織のアナリストがキャンペーンオブジェクトに「強く反対」し、その理由を説明するとします。

意見は主観的なものであり、仕様にはそれらを解釈する最善の方法は記載されていません。

意見は人間のアナリストによって作成され、人間向けのテキストで構成されます。意見には、意見を作成した作成者をキャプチャするための追加のプロパティが含まれています。

脅威に関する意見の定義

STIX オブジェクト内の情報の正確性の評価として脅威に関する意見を定義します。

始める前に
必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 脅威に関する意見.
2. [**New**] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 必要に応じて、フォームのフィールドに入力します。

4. **[Submit]** をクリックします。

次のタスク

次の関連リストのいずれかをクリックすると、脅威に関する意見に関連するオブジェクトの追加情報が表示されます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
関連オブジェクト	脅威に関する意見が適用されるオブジェクトのリスト。
関連するインジケーター	脅威に関する意見が適用されるインジケーターのリスト。
関連する観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。

脅威レポート

脅威レポートは、1 つ以上のトピックに焦点を当てた脅威インテリジェンスのコレクションです。脅威レポートは STIX 2.x に適用されます。

脅威レポートには、コンテキストや関連する詳細を含む、攻撃者、マルウェア、攻撃手法の説明が含まれます。これらは、包括的なサイバー脅威ストーリーとして公開できるように、関連する脅威インテリジェンスをグループ化するために使用されます。

脅威レポート SDO には、レポートの説明と名前とともに STIX オブジェクトへの参照のリストが含まれています。

脅威レポートの定義

コンテキストや関連する詳細を含む、攻撃者、マルウェア、攻撃テクニックについて説明した脅威レポートを定義します。

始める前に

必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 脅威レポート.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

4. **[Submit]** をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のタスク

次の関連リストのいずれかをクリックすると、脅威レポートに関連するオブジェクトの追加情報が表示されます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
関連タイプ	このオブジェクトに関連付けられたインジケータータイプを一覧表示します。
報告されたオブジェクト	脅威レポートで報告されたオブジェクトのリスト。
報告されたインジケーター	脅威レポートで報告されたインジケーターのリスト。
報告された観測事象	脅威レポートで報告された観測事象のリスト。

サイティング

サイティングは、インジケーターまたはオブジェクトが確認されたことを示します。オブジェクトには、マルウェア、ツール、攻撃者などがあります。

サイティングは、標的が誰であるか、どのように攻撃が実行されたかを追跡し、攻撃動作の傾向を追跡します。

サイティング関係オブジェクトには、汎用関係オブジェクトに存在しない追加のプロパティが含まれています。これらの追加プロパティは、サイティング関係に固有のデータを示します。

たとえば、カウント (発生した回数) を示します。

観測されたものがない場合はサイティングがないため、サイティングは関係としてキャプチャされます。

- 観測されたもの (マルウェア、キャンペーン、その他の SDO など)
- 誰がそれを観測したか、どこで観測されたか (ID として表示)
- システムおよびネットワークでの確認内容 (観測データとして表示)

インジケーターのサイティングの定義

インジケーターが確認されたことを示すサイティングを定義します。

始める前に

必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > インジケーターのサイティング.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. **[Submit]** をクリックします。

次のタスク
次の関連リストのいずれかをクリックすると、インジケーターのサイティングに関連するオブジェクトの追加情報が表示されます。

関連リスト	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
ID	このオブジェクトに関連付けられた ID のリスト。
観測データ	このオブジェクトに関連付けられた観測データを一覧表示します。

オブジェクトのサイティングの定義

オブジェクト (マルウェア、ツール、攻撃者など) が確認されたことを示すオブジェクトのサイティングを定義します。

始める前に
必要なロール：sn_ti.admin

手順
1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > オブジェクトのサイティング.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

4. **[Submit]** をクリックします。

次のタスク
次の関連リストのいずれかをクリックすると、オブジェクトのサイティングに関連するオブジェクトの追加情報が表示されます。

関連リスト	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
ID	このオブジェクトに関連付けられた ID のリスト。
観測データ	このオブジェクトに関連付けられた観測データを一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ツール

ツールは、攻撃者が攻撃を行うために使用する正当なソフトウェアのことです。ツールは STIX 2.x に適用されます。

ツールを使用すると、攻撃者がツールをいつどのように使用してキャンペーンを実行するかを知ることができます。マルウェアとは異なり、これらのツールまたはソフトウェアパッケージはシステム上で見つかることが多く、パワーユーザー、アドミン、ネットワークアドミニストレーター、または通常のユーザーにとっても正当な目的を持っています。

たとえば、リモートアクセスツール (RDP) やネットワークスキャンツール (Nmap) は、攻撃者が攻撃中に使用するツールです。

ツールの定義

攻撃者が攻撃を実行するために使用する正当なソフトウェアとしてツールを定義します。

始める前に

必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > ツール.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

次のタスク

次の関連リストのいずれかをクリックすると、ツールオブジェクトに関連するオブジェクトの追加情報が表示されます。

関連リンクと関連リスト	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
関連キルチェーンフェーズ	このオブジェクトに関連付けられたキルチェーンフェーズを一覧表示します。
関連タイプ	このオブジェクトに関連付けられたインジケータータイプを一覧表示します。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
対処措置	このオブジェクト (攻撃を阻止するための技術的または自動応答 (パッチの適用、ファイアウォールの再構成)) に関連付けられた対処措置を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連リンクと関連リスト	説明
ID	このオブジェクトに関連付けられた ID のリスト。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。

自動翻訳

脆弱性

脆弱性とは、攻撃者が悪用するソフトウェアまたはハードウェアコンポーネントの弱点または欠陥のことです。脆弱性は STIX 2.x に適用されます。

脆弱性または欠陥は、ソフトウェアまたはハードウェアコンポーネントに含まれるコードの要件、設計、または実装にあります。この脆弱性は、そのシステムの機密性、完全性、または可用性に悪影響を及ぼすために直接悪用されます。

CVE は、公開されている既知の問題 [CVE] の共通名を提供する情報セキュリティの脆弱性とエクスポージャーのリストです。

たとえば、マルウェアが CVE-2015-12345 を悪用する場合、マルウェアオブジェクトは CVE-2015-12345 を参照する脆弱性オブジェクトにリンクされます。

脆弱性の定義

攻撃者が悪用するソフトウェアまたはハードウェアコンポーネントの弱点または欠陥として脆弱性を定義します。

始める前に

必要なロール：sn_ti.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > 脆弱性.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

次のタスク

次の関連リストのいずれかをクリックすると、脆弱性オブジェクトに関連するオブジェクトの追加情報が表示されます。

関連リンクと関連リスト	説明
関係を表示	STIX オブジェクトの関係を表示できる STIX Visualizer を開きます。 [関係を表示] は、関連するオブジェクトがオブジェクトにある場合にのみ表示されます。
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
対処措置	このオブジェクト (攻撃を阻止するための技術的または自動応答 (パッチの適用、ファイアウォールの再構成)) に関連付けられた対処措置を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関係

関係オブジェクトを使用して、2 つの SDO または STIX サイバー観測可能オブジェクト (SCO) をリンクし、それらが互いにどのように関連しているかを記述します。

STIX 関係オブジェクト (SRO) は、さまざまな STIX オブジェクト間の関係のタイプを表します。次の関係オブジェクトを使用できます。

- オブジェクトとオブジェクトの関係：このオブジェクトは、インジケーターオブジェクトを除く SDO 間の関係を定義します。オブジェクトとオブジェクトで定義された関係の例は、攻撃パターンがマルウェアを配信する関係です。
- オブジェクトとインジケーターの関係：このオブジェクトは、インジケーターオブジェクトと SDO の間の関係を定義します。オブジェクトとインジケーターで定義された関係の例は、インジケーターがキャンペーンの証拠を検出する関係です。
- オブジェクトと観測事象の関係：このオブジェクトは、SDO と観測事象オブジェクトの間の関係を定義します。オブジェクトと観測事象で定義された関係の例は、潜在的な攻撃の情報を提供するサイバー観測事象オブジェクトでインフラストラクチャが構成されている関係です。

STIX オブジェクト関係

関係オブジェクト	ソースの例	ターゲットの例	説明の例
オブジェクトとオブジェクトの関係	攻撃パターン	マルウェア	この関係は、このマルウェアインスタンス (またはファミリ) を配信するためにこの攻撃パターンが使用されることを示しています。
オブジェクトとインジケーターの関係	インジケーター	攻撃パターン、キャンペーン、インフラストラクチャ、侵入セット、マルウェア、攻撃者、ツール	この関係は、関連する攻撃パターン、キャンペーン、インフラストラクチャ、侵入セット、マルウェア、攻撃者、またはツールの証拠をインジケーターが検出できることを示しています。 証拠が直接的でない場合があります。たとえば、特定のキャンペーンでよく使用されるマルウェアなど、キャンペーンの二次的証拠をインジケーターで検出することもできます。
オブジェクトと観測事象の関係	インフラストラクチャ	観測データ	この関係は、観測されたデータオブジェクトからの情報に基づいてインジケーターが作成されていることを示しています。 オブジェクトと観測事象で定義された関係の

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

STIX オブジェクト関係 (続く)

関係オブジェクト	ソースの例	ターゲットの例	説明の例
			例は、潜在的な攻撃の情報を提供するサイバー観測事象オブジェクトでインフラストラクチャが構成されている関係です。

オブジェクトとオブジェクトの関係の定義

SDO 間の関係を定義します (インジケーターオブジェクトを除く)。

始める前に
必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > オブジェクト **-** オブジェクト **-** リレーションシップ.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

オブジェクトとインジケーターの関係の定義

インジケーターオブジェクトと他の SDO 間の関係を定義します。

始める前に
必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > オブジェクト **-** インジケーター **-** リレーションシップ.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

オブジェクトと観測事象の関係の定義

SDO と観測事象オブジェクト (SCO) 間の関係を定義します。

始める前に
必要なロール：sn_ti.admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **IoC** リポジトリ > オブジェクト **-** 観察事項 **-** リレーションシップ.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。
4. **[Submit]** をクリックします。

STIX Visualizer

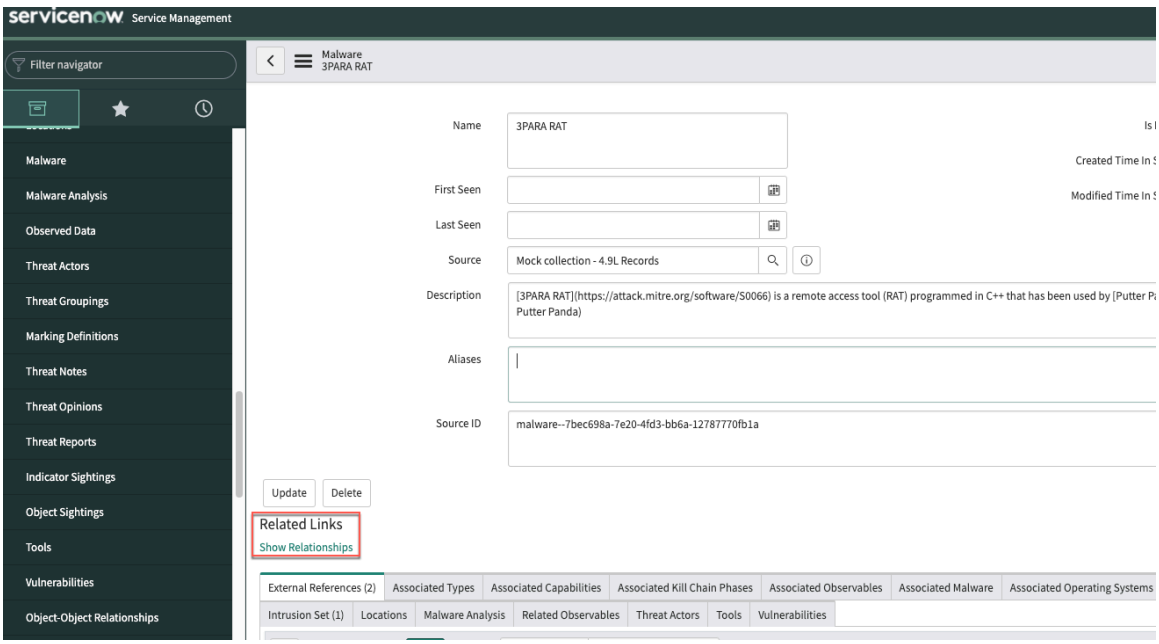
STIX Visualizer は、STIX オブジェクトの構造とその関係を視覚的に表します。

詳細ペインで、選択したオブジェクトまたは関係に関する詳細情報を確認できます。

関係グラフは、オブジェクトの関係を示し、調査するためのコンテキストを提供します。グラフ内の任意のノードをクリックすると、詳細が表示されます。

> **注:**
> STIX Visualizer は、レポートおよび観測データオブジェクトを除くすべての SDO で使用できます。

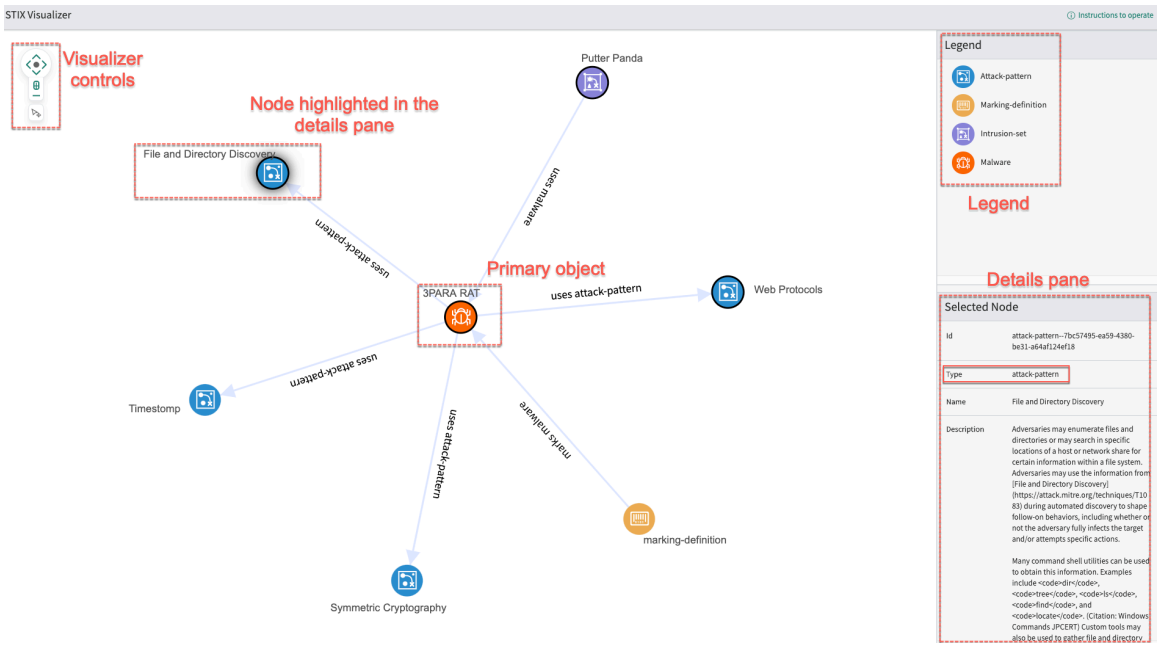
STIX Visualizer へのアクセス



いずれかの SDO の [関連リンク] セクションで [関係を表示] をクリックして、STIX Visualizer を表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

STIX Visualizer での詳細の表示



Visualizer では、さらに調査するためのコンテキストを提供するオブジェクトとその関係を表示できます。Visualizer は、色とアイコンを使用してオブジェクトに関するさまざまな情報を示します。

オブジェクトをズームインしたり、ノードをドラッグしたり、特定の関係に焦点を当てたりすることができます。

任意のオブジェクトをクリックして詳細ペインを開きます。詳細ペインでは、オブジェクトに関連付けられている詳細情報を確認できます。

MITRE-ATT&CK™ フレームワークの概要

MITRE-ATT&CK フレームワークは、サイバー攻撃に対抗する特定の脅威モデルと方法論を開発するために組織が利用できる一般的な戦術、テクニック、手順 (TTP) のナレッジベースです。

概要

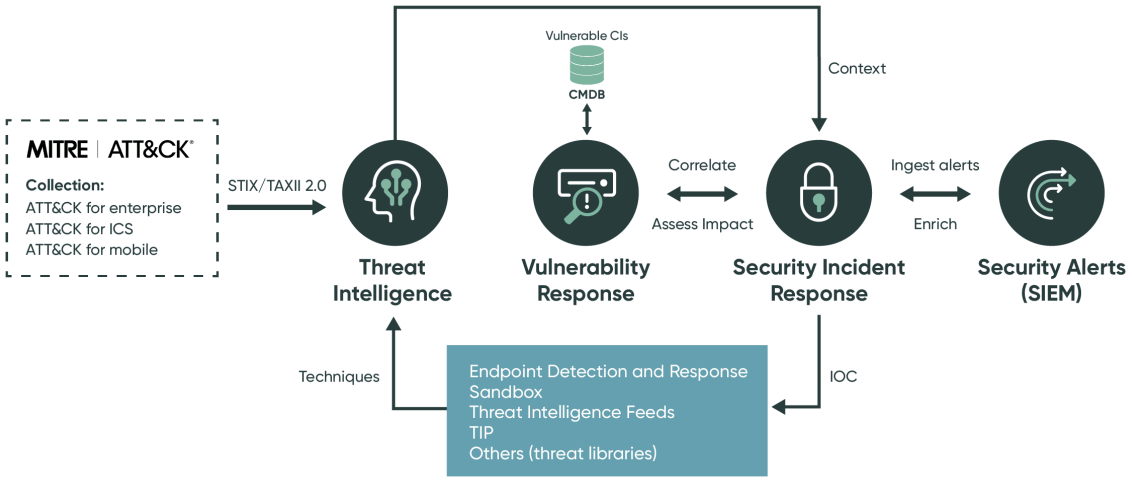
MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) フレームワークでは、サイバー攻撃の各ステージで使用されるさまざまな攻撃テクニックを文書化して追跡します。

サイバー脅威インテリジェンスコミュニティでは、MITRE-ATT&CK フレームワークのナレッジベースを使用することで、脅威を迅速に特定し、サイバー攻撃への対応を調整できます。

MITRE-ATT&CK および Security Operations

MITRE-ATT&CK 情報が セキュリティオペレーション アプリケーションにどう流れていくかは、次の図を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



- application プリロード済み TAXII クライアント は TAXII サーバーに接続して、 データコレクション を 脅威インテリジェンスに取り込みます。
- 既存の Security Information and Event Manager (SIEM) 統合が脅威データ (アラートとイベント) を関連する TTP とともに取り込み、これらがセキュリティインシデントに関連付けられます。
- IoC がセキュリティインシデントに関連付けられている場合は、脅威インテリジェンス が脅威フィードを自動的に検索して関連する情報を確認し、IoC をサードパーティのソース (EDR、サンドボックス、TIP など) に送信してさらに分析します。
- サードパーティのソースに MITRE-ATT&CK 情報が含まれている場合は、 脅威インテリジェンス テクニック情報を抽出 また、相関と分析のために 脅威インテリジェンス リポジトリのデータを拡張します。
- MITRE-ATT&CK では、各テクニックの CVE コンテキスト情報 も共有されます。セキュリティチームは、脆弱性対応 で悪用されたテクニックを確認して、ビジネスクリティカルな資産が脅威にさらされているかどうかを判断できます。

MITRE-ATT&CK のマトリクス、戦術、テクニック

MITRE-ATT&CK フレームワークのコアは、攻撃者の戦術とテクニックのマトリクスです。一連の戦術は、インシデントのステージで攻撃者が達成しようとしていることを表しています。セキュリティチームがこのシーケンスを理解できれば、攻撃者の次の動きを予測してキルチェーンを断ち切ることができます。ATT&CK は次のマトリクスで構成されています。

- Enterprise ATT&CK：攻撃者が企業ネットワークやクラウドを侵害し操作するために取る行動や行為を説明します。

  注:
  Pre ATT&CK マトリクスは MITRE によって廃止され、Enterprise マトリクスに統合されました。

- ICS ATT&CK：産業用コントールシステム (ICS) のネットワーク内で攻撃者が行うアクションを説明します。
- Mobile ATT&CK：モバイルデバイスに焦点を当てた攻撃者の行動や行為を説明します。

戦術は、ATT&CK テクニックの理由を表します。これは、アクションを実行するための攻撃者の戦術的目標です。

テクニックは、攻撃者がアクションを実行して戦術的目標を達成する方法を表します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テクニックは複数の戦術に関連付けられている場合があります。たとえば、アクセストークン操作は、特権エスカレーションまたは防御回避のいずれかの戦術を達成するために攻撃者によって使用されます。

インシデント応答にインテントベースのアプローチを使用する

インテントベースの応答では、組織がセキュリティインシデントを関連付けて広範囲の攻撃を特定するのに役立つ、動的なコンテキストに応じたキルチェーンフレームワークを使用します。セキュリティチームは、インテントベースの応答を使用して、組織がどのように攻撃され、攻撃者が次に何をする可能性があるかを理解できます。このタイプの応答により、攻撃者の行動を予測できるため、リソースを効果的に集中できます。

セキュリティチームは、セキュリティインシデントレスポンス を使用して、IP アドレス、ファイルハッシュ、ドメインなどのセキュリティ侵害のインジケーター (IOC) に焦点を当てることで、各セキュリティインシデントのライフサイクルを管理できます。

セキュリティインシデントレスポンス と MITRE-ATT&CK フレームワークを統合することで、セキュリティインシデントは企業規模の大規模な攻撃のリンクとして処理されます。

Security Operations で **MITRE-ATT&CK** を活用した場合の組織へのメリット

MITRE-ATT&CK フレームワークを使用すると、組織は次のことができます。

- セキュリティインシデントを適切に分析して対応するための MITRE-ATT&CK 戦術、テクニック、および手順 (TTP) をセキュリティアナリストに提供します。
- MITRE-ATT&CK フレームワークのコンテキストで脅威を検出して封じ込めるためのプレイブックを使用して、インシデントワークフローを自動化します。
- MITRE-ATT&CK の情報を使用してセキュリティ侵害のインジケーターと脅威ハンティングを優先順位付けします。
- MITRE-ATT&CK フレームワークのコンテキストで組織の高レベルのセキュリティ体制を把握します。

MITRE-ATT&CK 管理

Now Platform の MITRE-ATT&CK リポジトリで データソースを設定しマッピングし、全体的なテクニックディスカバリー範囲をマッピングして保持できます。

MITRE-ATT&CK フレームワークの開始

MITRE-ATT&CK のセットアップを開始する前に、次の情報を確認します。

チェックリスト

セットアップタスク	説明
必要な Now Platform、脅威インテリジェンス、および セキュリティインシデントレスポンス のロールがアサインされていることを確認します。	MITRE-ATT&CK の機能全体で次のロールが使用されます。 • システムアドミニストレーター (admin) は、ServiceNow Store からアプリケーションをインストールし、セキュリティインシデントアドミン (sn_si.admin) と脅威インテリ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト (続く)

セットアップタスク	説明
	ジェンスアドミン (sn_ti.admin) にロールをアサインします。 • sn_ti.admin • sn_si.admin • sn_si.analyst • sn_ti.read • sn_ti.write • sn_ti.mitre_analyst：セキュリティインシデントレスポンス と 脅威インテリジェンス Support Common の間で MITRE 機能を相互操作できるように、MITRE アナリストロールが導入されました。このロールでは、脅威インテリジェンス MITRE モジュールと セキュリティインシデントレスポンス モジュールの両方を読み取り専用モードで表示できます。 • sn_si.read 詳細については、「脅威インテリジェンスのセットアップ」を参照してください。
MITRE-ATT&CK モジュールをサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。 • 脅威インテリジェンス Support Common UI コンポーネント (sn_ti_seismic)：バージョン 1.0 以降 • 脅威インテリジェンス Support Common：バージョン 12.0 以降 • 脅威インテリジェンス ：バージョン 12.0 以降 • セキュリティインシデントレスポンス ：バージョン 12.0 以降 統合のための Now Platform インスタンスの設定の詳細については、「Security Operations 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト (続く)

セットアップタスク	説明
ドメインセパレーション	データ、プロセス、および管理タスクを分離する場合は、「ドメインセパレーション」を確認してください。

MITRE - STIX データモデルの概要 ™

Now Platform の MITRE-ATT&CK フレームワークを効率的に使用して理解するには、MITRE および STIX で使用されている用語を確認してください。

MITRE オブジェクトから STIX へのマッピング

STIX は、標準化および構造化された方法でサイバー脅威情報を記述するための言語です。脅威インテリジェンス モジュールの親データモデルは STIX オブジェクトです。MITRE オブジェクトは親 STIX データモデルのサブセットです。MITRE-ATT&CK フレームワークでは、MITRE は特定のラベルとオブジェクトを持つ同様の STIX 情報を提供します。

MITRE から STIX オブジェクトへのマッピング

MITRE の用語	STIX の用語
テクニック	攻撃パターン
緩和	対処措置
グループ	侵入セット
マルウェア	マルウェア
ツール	ツール

脅威インテリジェンス モジュールのデータ拡張

脅威インテリジェンス 脅威ソースのリストを維持し、広範なサイバー脅威情報が含まれる必要な STIX データをインポートできます。TAXII プロファイルを使用して、サイバー脅威情報を自動交換することもできます。

注:
詳細については、「脅威のソースの定義」と「TAXII プロファイルの作成」を参照してください。

MITRE-ATT&CK モジュールのデータ拡張

マルウェア、グループ、緩和、およびツールのオブジェクトを MITRE-ATT&CK リポジトリのテクニックに拡張できます。

[MITRE ATT&CK リポジトリ] モジュールでは、新しいオブジェクトを作成し、テクニックと新しいオブジェクト間の関係を確立できますが、このモジュールでは関係タイプは定義できません。関係タイプを定義するには、 脅威インテリジェンス > **IoC** リポジトリ > オブジェクトとオブジェクトのリレーションシップ 移動します

既存のテクニックと既存のオブジェクトの間で関係タイプをマッピングする場合は、テクニックをターゲットオブジェクトとして、オブジェクトをソースオブジェクトとして定義する必要があります。これを行うには、 **IoC** リポジトリ > オブジェクトとオブジェクトのリレーションシップ 移動します

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

グループを作成して攻撃パターンに関連付けることはできますが、MITRE ATT&CK リポジトリで確立できるのはグループと攻撃パターンの関係のみです。オブジェクト間の関係タイプを定義するには、IoC リポジトリで行う必要があります。

> **注:**
> 詳細については、次を参照してください。 延ばす MITRE-ATT&CK データ および IoC リポジトリ。

ドメインセパレーションと MITRE-ATT&CK

これは、MITRE-ATT&CK に関するドメインセパレーションの概要です。ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。その後、どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル

サポート：ベーシック。

MITRE-ATT&CK のドメインセパレーションの仕組み

ドメインセパレーションを実現するには、次の手順に従います。

- それぞれのドメインで、必要な sn_ti.admin ロールを持つユーザーを作成します。
- すべてのドメインについて次を複製します。
  - TAXII コレクション

    > **注:**
    > - グローバルドメインでコレクションをアクティブ化しないでください。ドメインで複製されて利用可能なコレクションのみをアクティブ化します。
    > - コレクションの [実行方法] フィールドを、それぞれのドメインの sn_ti.admin ロールを持つユーザーに変更します。

  - テクニックディスカバリー範囲の定義
  - テクニック抽出ルール
  - 検出ルール - MITRE ATT&CK マッピング
  - 緩和対象範囲
    - すべての緩和対象範囲定義レコードをコピーします。
    - 緩和対象範囲計算ツールをコピーするか、それぞれのドメインに新しい計算ツールを作成します。
  - 脅威グループ - テクニックヒートマップ定義

TAXII 収集の複製

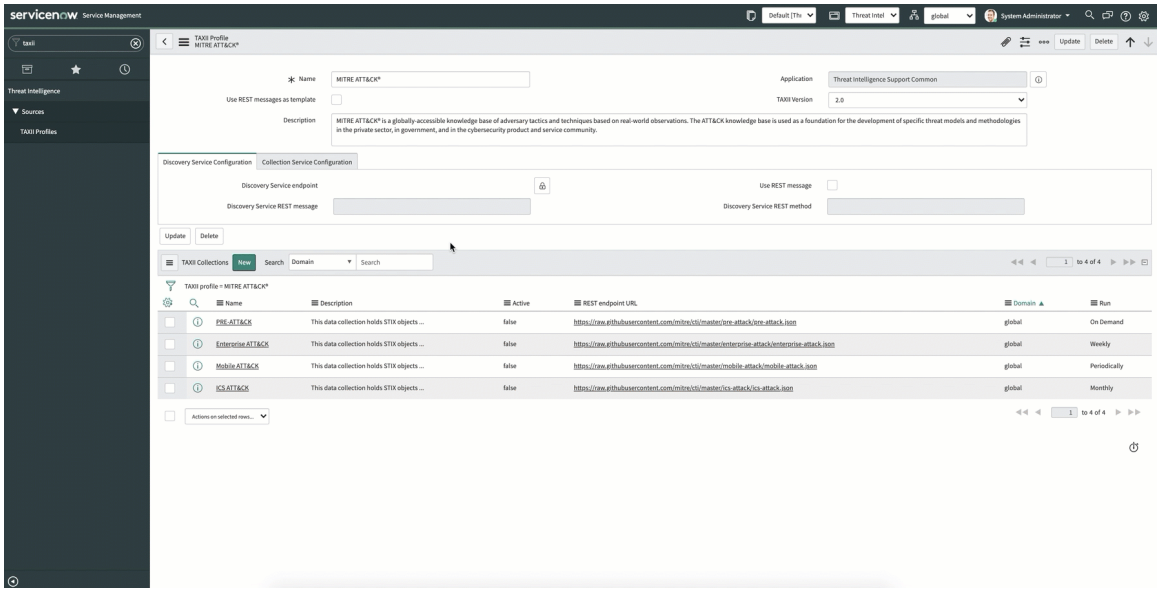
1. 次のように移動する。 脅威インテリジェンス > ソース > **TAXII** プロファイル.
2. ヘッダーバーで、ドメインピッカーを使用してドメインを選択します。
3. 組織に関連する TAXII 収集 (エンタープライズ ATT&CK、モバイル ATT&CK、または ICS ATT&CK) を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. ヘッダーバーを右クリックして、[挿入と維持] を選択します。重複した TAXII 収集が選択したドメインに作成されます
5. MITRE ATT&CK TAXII プロファイルに戻り、重複する TAXII 収集を表示します。

次の図は、ドメインの TOP/Initech を選択して、ドメイン内の TAXII 収集を複製し、複製された TAXII 収集を確認する方法を示しています。



MITRE-ATT&CK™ フレームワークを設定する

MITRE-ATT&CK プロファイルをアクティブ化し、組織内で脅威検出の MITRE-ATT&CK コレクションを設定できるように、スケジュール済みジョブを設定します。

始める前に

必要なロール：sn_ti.admin

このタスクについて

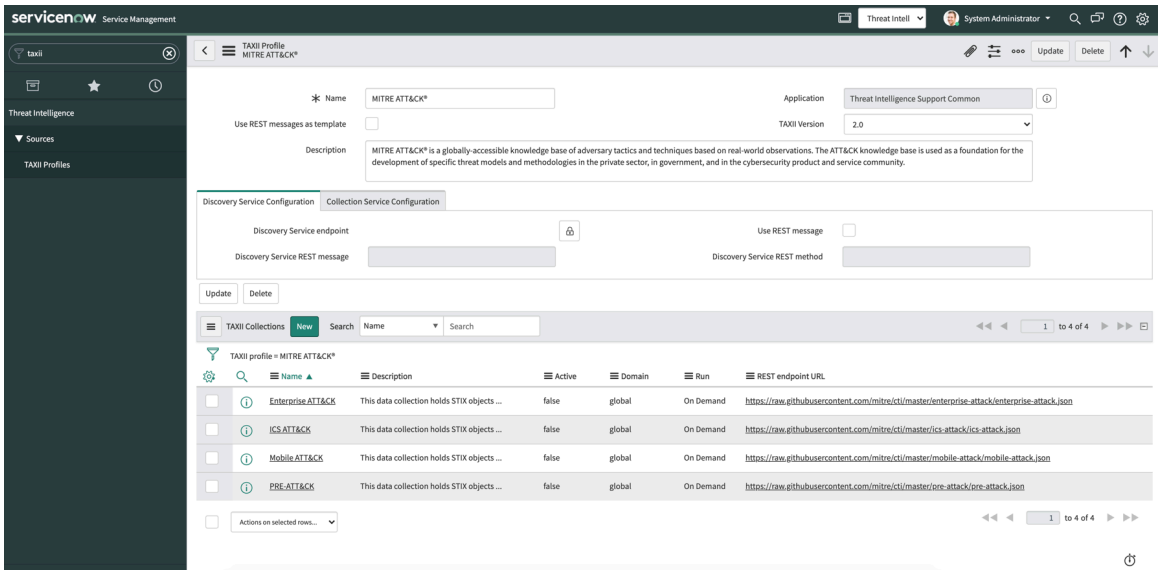
脅威情報構造化記述形式 (Structured Threat Information eXpression) (STIX™) とは、サイバー脅威情報を標準化および構造化された方法で記述するための言語です。STIX データと検知指標情報自動交換手順 (Trusted Automated Exchange of Indicator InformationTrusted) (TAXII™) のプロファイルを使用することで、セキュリティチームは共有されたサイバー脅威情報を使用して、自社や他のソースから前に確認された脅威を分離することができます。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > ソース > **TAXII** プロファイル.
   利用可能な TAXII プロファイルが表示されます。
2. ベースシステムに提供されている **[MITRE ATT&CK]** プロファイルをクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. TAXII コレクションをアクティブ化するには、組織に関連する TAXII コレクション (エンタープライズ ATT&CK、モバイル ATT&CK、または ICS ATT&CK) の [アクティブ] オプションを true に設定します。

TAXII 収集	説明
エンタープライズ ATT&CK	攻撃者が企業ネットワークやクラウドを侵害し操作するために取る行動や行為を説明します。 **注:** Pre ATT&CK マトリクスは MITRE によって廃止され、Enterprise マトリクスに統合されました。
モバイル ATT&CK	モバイルデバイスに焦点を当てた攻撃者の行動や行為を説明します。
ICS ATT&CK	産業用コントールシステム (ICS) のネットワーク内で攻撃者が行うアクションを説明します。

4. このコレクションを定期的に更新するには、組織に応じて適切な [実行] オプションを設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

デフォルトでは、このオプションは [オンデマンド] に設定されています。

注:

a. コレクションは 脅威インテリジェンス Core プラグインの一部としてパッケージ化されています。脅威インテリジェンス Support Common - バージョン 12.0 以降、および 脅威インテリジェンス - バージョン 12.0 以降をインストールまたは更新すると、コレクションデータが自動入力されます。

b. TAXII コレクションは、組織で使用する予定のコレクションのみをアクティブ化し、他のコレクションは無効にします。たとえば、エンタープライズ ATT&CK マトリクスを使用する予定であれば、TAXII コレクションレベルおよびマトリクスレベルでエンタープライズ ATT&CK をアクティブ化します。TAXII コレクションおよびマトリクスレベルで、他のモバイル ATT&CK マトリクスと ICS ATT&CK マトリクスを無効にします。

c. TAXII コレクションの関連リストでは、[実行] オプションで [毎日 (Daily)] を選択すると、エラーが発生し、オプションはデフォルトで [オンデマンド] になります。このエラーは、MITRE サーバーの負荷を最適化するために、MITRE-ATT&CK データの更新を毎日行うことが制限されているために発生します。また、MITRE は ATT&CK のデータを年に 2 回のみ更新します。

d. TAXII コレクションは、TAXII コレクションをアクティブ化しない限り更新されません。

e. 既存のコレクションの更新は、各コレクションの「実行」頻度をスケジュール設定することで、MITRE サーバーから取得できます。

f. MITRE-ATT&CK リポジトリのデータ (テクニックに対するマルウェア、グループ、緩和、およびツールオブジェクト) に対して行ったカスタマイズは、スケジュール設定済みの更新時に保存されます。

g. MITRE は MITRE-ATT&CK ナレッジベースを更新し、一部のオブジェクトが取り消しまたは使用廃止とされ、新しいオブジェクトが追加され、既存のオブジェクトが変更されます。MITRE が戦術やテクニックを取り消す場合、これらのオブジェクトは Now Platform で取り消し済みとしてマークされます。取り消されたオブジェクトはリポジトリに保持されますが、Now Platform では使用できません。

次のタスク

TAXII プロファイルのセットアップが完了すると、MITRE-ATT&CK リポジトリのデータが定期的に Now Platform にインポートされます。このデータを表示するには、次に移動します: **MITRE ATT&CK** リポジトリ > マトリクス AND **MITRE ATT&CK** リポジトリ > テクニック.

マトリクスを管理する

MITRE TAXII コレクションからインポートされたマトリクスを管理します。マトリクスとは、戦術やテクニックのコレクションです。マトリクスを表示して、自分のコレクションが MITRE-ATT&CK リポジトリで使用可能かどうかを確認できます。

始める前に

注:
組織で使用する予定のマトリクスのみがアクティブ化され、他のマトリクスが無効になっていることを確認および検証してください。たとえば、エンタープライズ ATT&CK マトリクスを使用する予定であれば、TAXII 収集レベルおよびマトリクスレベルでエンタープライズ ATT&CK マトリクスがアクティブ化されています。TAXII コレクションおよびマトリクスレベルで、他のモバイル ATT&CK マトリクスと ICS ATT&CK マトリクスを無効にします。

必要なロール：

- sn_ti.admin：削除アクセス
- sn_ti.read：読み取りアクセス
- sn_ti.write：作成、書き込みアクセス

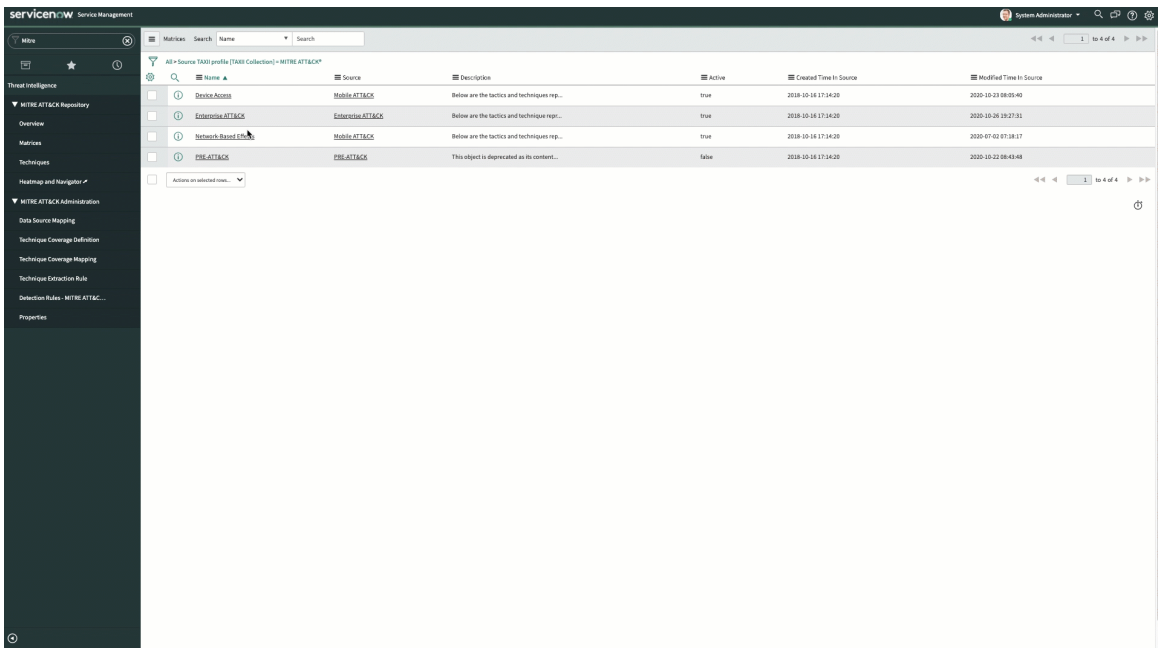
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** リポジトリ > マトリクス.
   デフォルトでは、すべてのマトリクスが無効になっています。
2. マトリクスをアクティブ化するには、[アクティブ] を指定してダブルクリックし、**[true]** を選択します。
3. すべての関連情報を表示するには、マトリクスをクリックします。
4. このコレクションに関連付けられているすべての戦術を表示するには、**[MITRE** 戦術] タブをクリックします。
5. 選択した戦術に関連するその他の詳細とテクニックを表示するには、戦術をクリックします。
6. **[MITRE ATT&CK** テクニック] タブでテクニックを選択します。
7. 関連リストに、選択したテクニックで利用可能な関連性を表示します。

   次の図では、エンタープライズ ATT&CK マトリクスから初期アクセス (TA0001) 戦術、さらにはフィッシング (T1566) テクニックへのナビゲーションパスを示しています。攻撃パターン - フィッシングテクニックのページでは、関連リスト (戦術、サブテクニック、グループ、緩和、外部参照、マルウェア、およびツール) を表示できます。



次のタスク
選択したテクニックに基づいて、これらの関連リストオブジェクトの一部の情報を拡張できます。たとえば、グループ、緩和、外部参照、マルウェア、ツールなどの新しい情報を追加できます。

テクニックの管理

MITRE TAXII コレクションからインポートされたテクニックを管理します。テクニックには、攻撃者が特定の戦術を使用するために開発したさまざまな方法が含まれています。組織に関係のないテクニックは、確認して非アクティブ化できます。STIX では、テクニックは攻撃パターンと呼びます。

始める前に
必要なロール：

- sn_ti.admin：削除アクセス
- sn_si.admin：作成、書き込み、削除アクセス

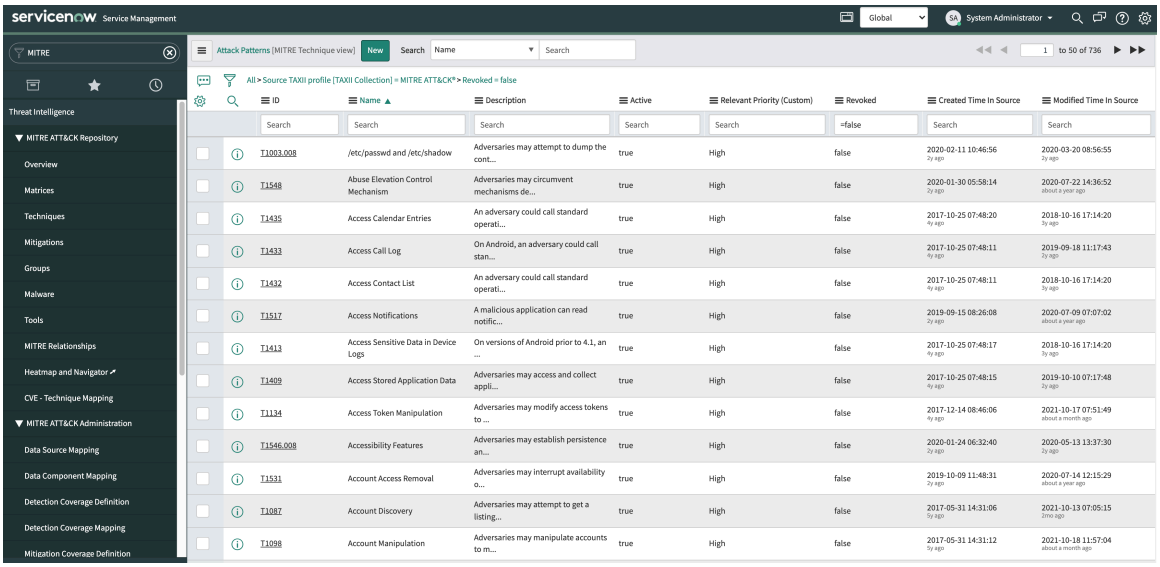
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- sn_ti.read：読み取りアクセス
- sn_ti.write：作成、書き込みアクセス

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** リポジトリ > テクニック.



これで、テクニックとサブテクニックのリストが表示されます。

2. 組織に関連しないテクニックを確認して非アクティブ化するには、選択したテクニックのリストビューに移動し、[アクティブ] 列で設定を **[false]** に更新します。
MITRE-ATT&CK リポジトリ内の他のオブジェクトで使用されていないテクニックを非アクティブ化します。

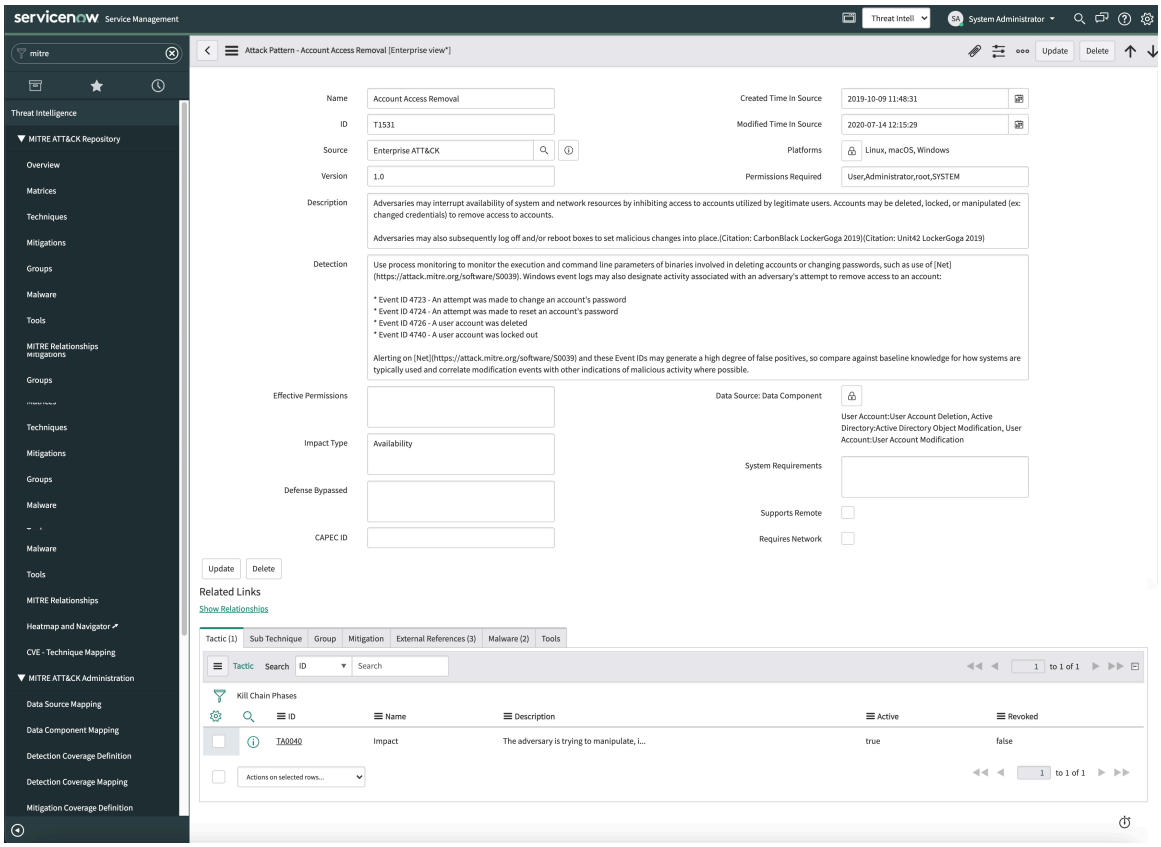
3. テクニックに優先度を付けるには、[関連する優先度 (カスタム)] フィールドで優先度をアサインします。
ベースシステム関連の優先度は、[なし] に設定されています。[関連する優先度 (カスタム)] フィールドは、MITRE-ATT&CK TAXII コレクションからインポートされたものではなく、Now Platform に導入されたカスタムフィールドです。関連する優先度情報を使用して、データソースのマッピング時、またはヒートマップの分析時に、ダッシュボードでテクニックをフィルタリングして優先度を付けることができます。

4. テクニックをクリックして、このテクニックに関連するすべての情報を表示します。

次の図では、アカウントアクセス削除テクニック、その ID、ソース、および他の関連情報を表示できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
MITRE によって導入されたデータソース：データコンポーネント要素は、前の [データソース] フィールドを置き換えるものです。データコンポーネントは、データソースにコンテキストの追加サブレイヤーを提供します。MITRE-ATT&CK リポジトリに古い TAXII コレクションが含まれている場合は、[データソース] フィールドを表示できます。それ以外の場合は、[データソース：データコンポーネント] フィールドのデータコンポーネントの追加コンテキストでデータソースを表示できます。ソースがエンタープライズ ATT&CK の場合にのみ、新しいデータコンポーネントフィールドを表示できます。詳細については、「data component mapping (データコンポーネントのマッピング)」を参照してください。

5. これらのオブジェクトがどのように関連しているかを表示するには、[関係を表示] をクリックします。

次のタスク

これらの関連リストオブジェクトの一部では、情報を拡張できます。たとえば、グループ、緩和、外部参照の情報を新たに追加できます。

緩和の管理

MITRE TAXII コレクションからインポートされた緩和を管理します。緩和により、攻撃者が組織に対してテクニックまたはサブテクニックを実行することを防ぐことができます。STIX では、緩和は対処措置として知られています。

始める前に

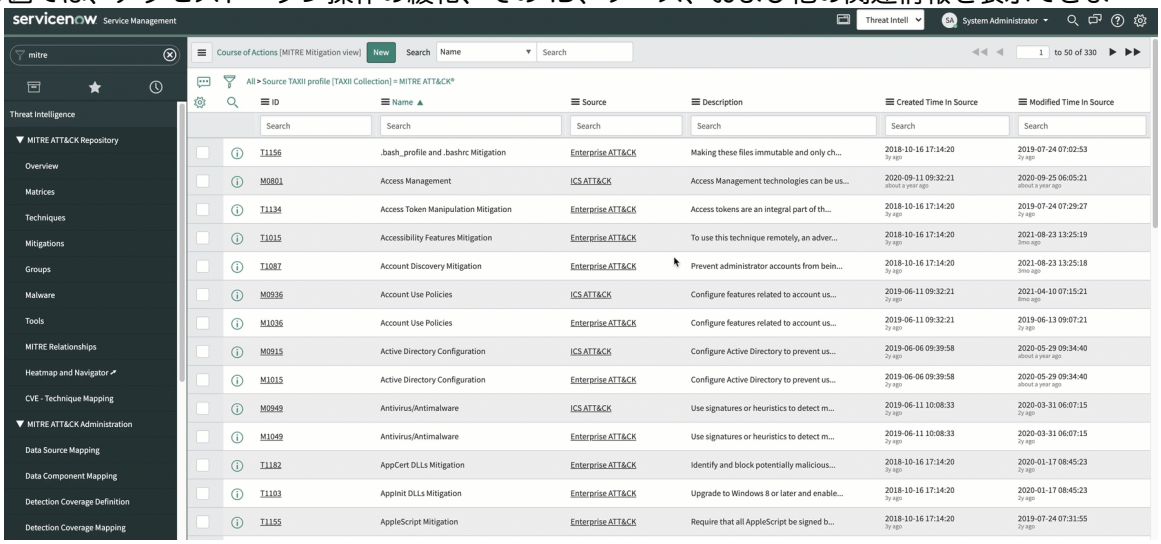
必要なロール：

- sn_ti.admin：削除アクセス
- sn_ti.read：読み取りアクセス
- sn_ti.write：作成、書き込みアクセス

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** リポジトリ > 緩和.
   緩和が一覧表示されます。
2. 緩和をクリックして、すべての関連情報を表示します。
   次の図では、アクセストークン操作の緩和、その ID、ソース、および他の関連情報を表示できます。



   す。
3. これらのオブジェクトがどのように関連しているかを表示するには、[関係を表示] をクリックします。

次のタスク
テクニックモジュールを使用して、緩和データを追加または変更します。

グループの管理

MITRE TAXII コレクションからインポートされたグループを管理します。グループは、セキュリティコミュニティで共通の名前で追跡される、関連する侵入アクティビティのセットです。アナリストは、脅威グループ、アクティビティグループ、攻撃者、侵入セット、キャンペーンなどのさまざまな用語を使用して、アクティビティのクラスターを追跡します。STIX では、グループは侵入セットと呼ばれます。

始める前に
必要なロール：

- sn_ti.admin：削除アクセス
- sn_ti.read：読み取りアクセス
- sn_ti.write：作成、書き込みアクセス

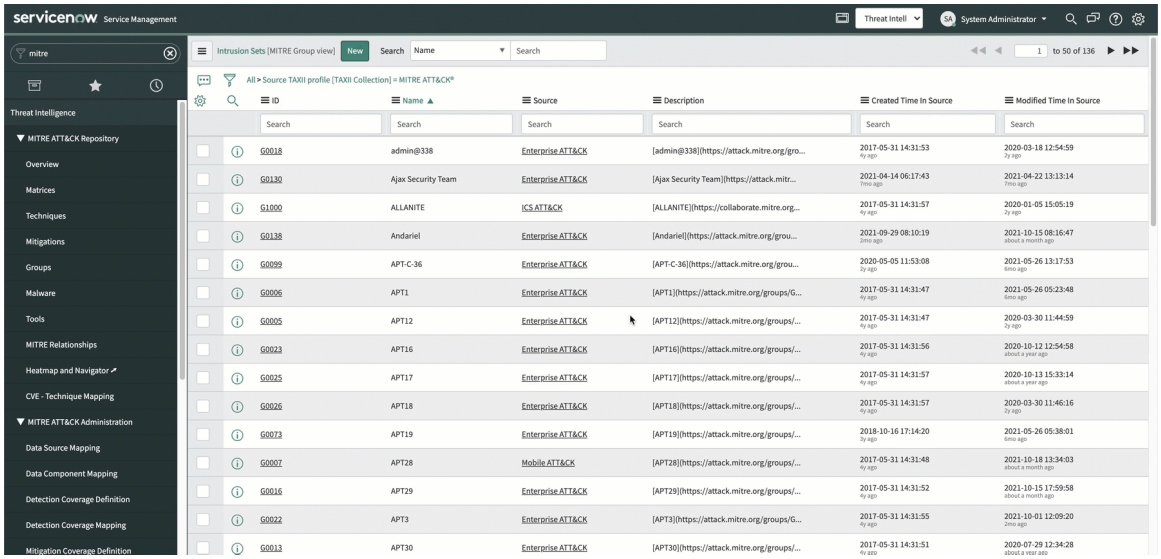
手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** リポジトリ > グループ.
   リストされたグループを表示できます。
2. グループをクリックして、関連するすべての情報を表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図では、Ajax セキュリティチームグループ、その ID、ソース、および他の関連情報の詳細を表示できま



す。

3. これらのオブジェクトがどのように関連しているかを表示するには、[関係を表示] をクリックします。

> **注:**
> 詳細に調査できるように脅威グループをセキュリティケースに関連付けるには、[セキュリティケースに追加] をクリックします。

次のタスク
テクニックモジュールを使用して、グループデータを追加または変更します。

マルウェアの管理

MITRE TAXII コレクションからインポートしたマルウェア情報を管理します。マルウェアは、悪意のあるコードを表す TTP の一種です。これは、システムに密かに挿入されるプログラムを指します。マルウェアの目的は、被害者のデータ、アプリケーション、またはオペレーティングシステム (OS) の機密性、完全性、または可用性を侵害することです。

始める前に

必要なロール：

- sn_ti.admin：削除アクセス
- sn_ti.read：読み取りアクセス
- sn_ti.write：作成、書き込みアクセス

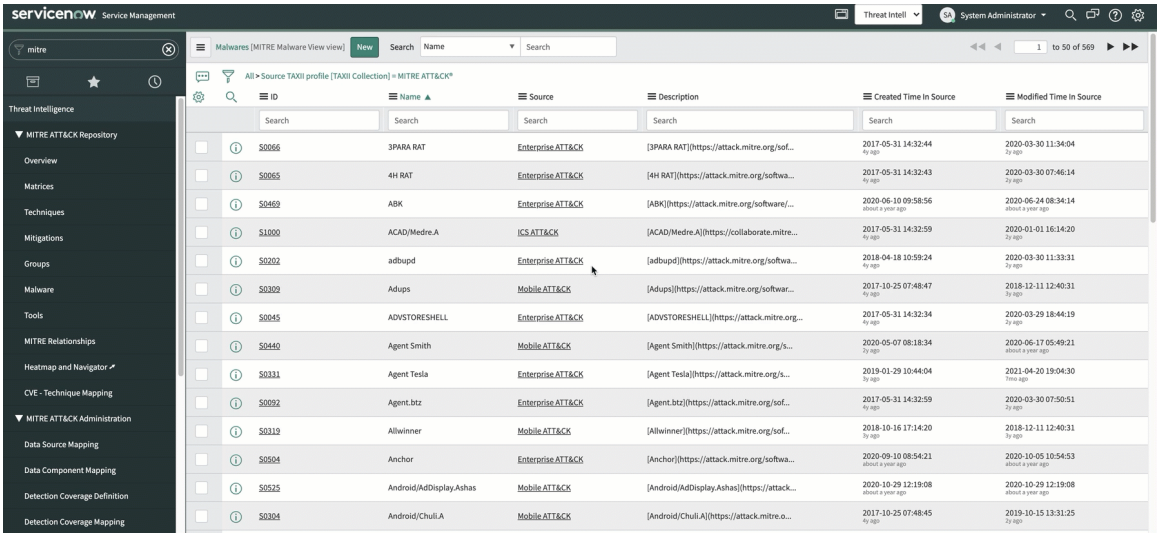
手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** リポジトリ > マルウェア.
   リストされたマルウェアを表示できます。
2. マルウェアをクリックして、すべての関連情報を表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図では、3PARA RAT マルウェア、その ID、ソース、および他の関連情報の詳細を表示できま



す。

3. これらのオブジェクトがどのように関連しているかを表示するには、[関係を表示] をクリックします。

次のタスク

テクニックモジュールを使用して、マルウェアデータを追加または変更します。

管理ツール

MITRE TAXII コレクションからインポートしたツール情報を管理します。ツールは、攻撃者が攻撃を行うために使用する正当なソフトウェアのことです。

始める前に

必要なロール：

- sn_ti.admin：削除アクセス
- sn_ti.read：読み取りアクセス
- sn_ti.write：作成、書き込みアクセス

このタスクについて

ツールを使用すると、攻撃者がツールをいつどのように使用してキャンペーンを実行するかを知ることができます。マルウェアとは異なり、これらのツールまたはソフトウェアパッケージはシステム上で見つかることが多く、パワーユーザー、アドミン、ネットワークアドミニストレーター、または通常のユーザーにとっても正当な目的を持っています。

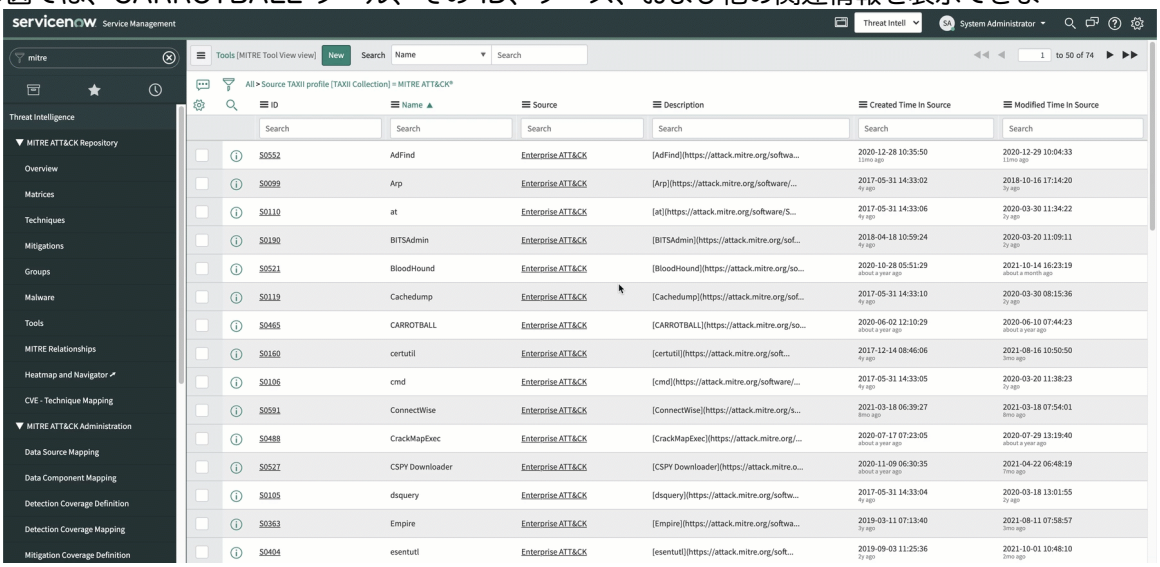
手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** リポジトリ > ツール.
   ツールリストを表示できます。
2. ツールを選択して、すべての関連情報を表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図では、CARROTBALL ツール、その ID、ソース、および他の関連情報を表示できます。



3. これらのオブジェクトがどのように関連しているかを表示するには、[関係を表示] をクリックします。

次のタスク
テクニックモジュールを使用して、ツールデータを表示または変更します。

MITRE との関係の管理

MITRE TAXII コレクションからインポートした MITRE との関係情報を管理します。

始める前に
必要なロール：

- sn_ti.admin：削除アクセス
- sn_ti.read：読み取りアクセス
- sn_ti.write：作成、書き込みアクセス

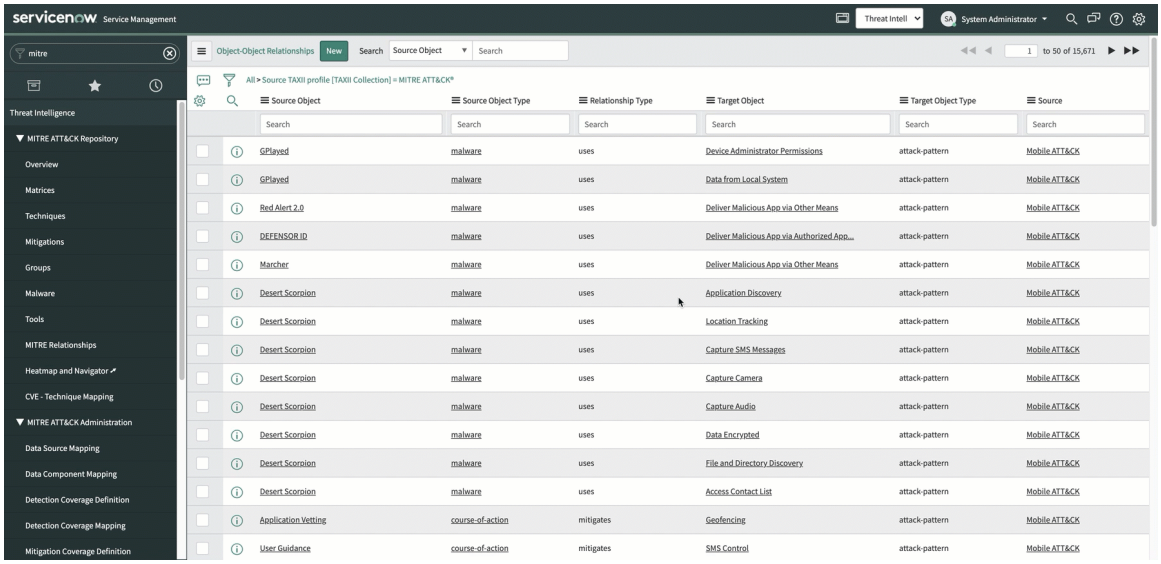
手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** リポジトリ > **MITRE** 関係.
   ツールリストを表示できます。
2. ソースオブジェクトをクリックして、すべての関連情報を表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図では、赤色のアラート 2.0 オブジェクト、その ID、ソース、および他の関連情報を表示できま



す。

3. これらのオブジェクトがどのように関連しているかを表示するには、[関係を表示] をクリックします。

次のタスク
テクニックモジュールを使用して、MITRE の関係データを追加または変更します。

CVE とテクニックマッピングの管理

MITRE TAXII コレクションをインポートした後にマッピングされる CVE とテクニック情報を管理します。

始める前に
必要なロール：

- sn_ti.admin：削除アクセス
- sn_si.admin：作成、書き込み、削除アクセス
- sn_ti.read：読み取りアクセス
- sn_ti.write：作成、書き込みアクセス

> **注:**
> **[CVE -** テクニックマッピング **]** モジュールは、脆弱性対応製品が環境にインストールされている場合にのみ使用できます。

このタスクについて
MITRE TAXII コレクションをインポートすると、環境内の CVE および関連する MITRE-ATT&CK テクニックとの関係を表示できます。CVE と攻撃パターンの関連付けを作成することもできます。

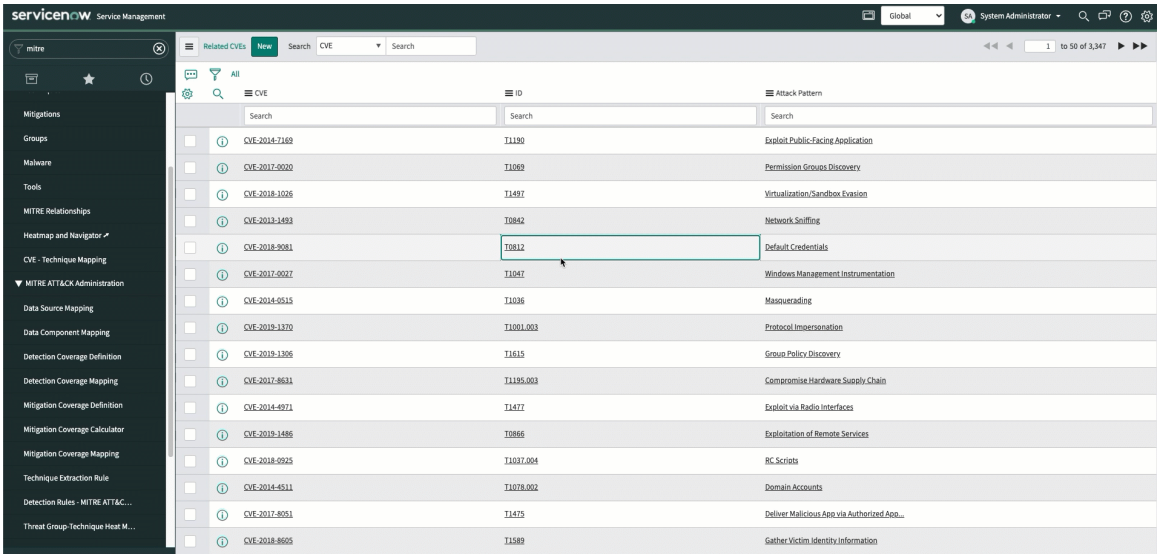
手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** リポジトリ > **CVE -** テクニックマッピング.
   リストされた CVE とテクニックを表示できます。
2. CVE をクリックして、脆弱性データベースエントリーを表示します。

自動翻訳

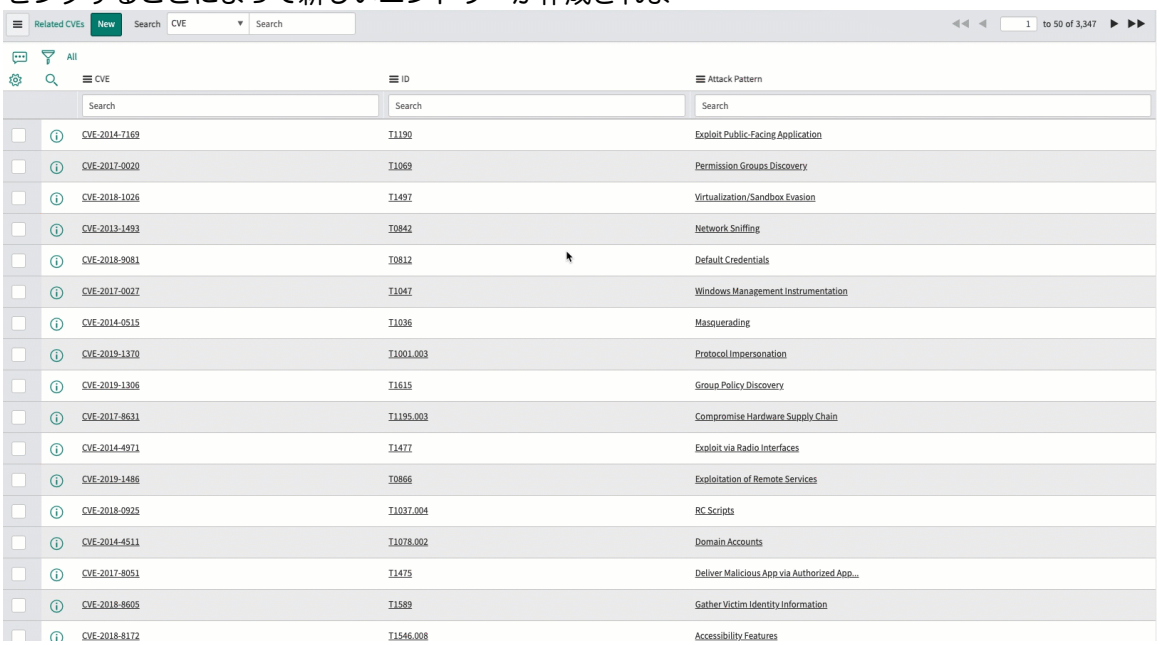
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図では、CVE-2014-7169 の CVE リストと脆弱性データベースエントリーの詳細を表示できま



す。

3. エントリーを追加するには、[新規] をクリックし、CVE を攻撃パターンにマッピングして、[送信] をクリックします。
次の図では、CVE-2014-0515 を成り済まし攻撃パターンとマッピングすることによって新しいエントリーが作成されま



す。

MITRE-ATT&CK データを拡張する

Now Platform の MITRE-ATT&CK リポジトリデータを増やすことで、拡張します。

始める前に

必要なロール：

- sn_ti.admin：削除アクセス
- sn_ti.read：読み取りアクセス
- sn_ti.write：作成、書き込みアクセス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
マルウェア、グループ、緩和、およびツールのオブジェクトを MITRE-ATT&CK リポジトリのテクニックに拡張できます。

[MITRE ATT&CK リポジトリ] モジュールでは、新しいオブジェクトを作成し、テクニックと新しいオブジェクトの間の関係を確立できますが、このモジュールでは関係タイプは定義できません。関係タイプの定義の詳細については、「object to object relationships (オブジェクト間の関係)」を参照してください。関係タイプを定義するには、 脅威インテリジェンス > **IoC** リポジトリ > オブジェクトとオブジェクトのリレーションシップ 移動します

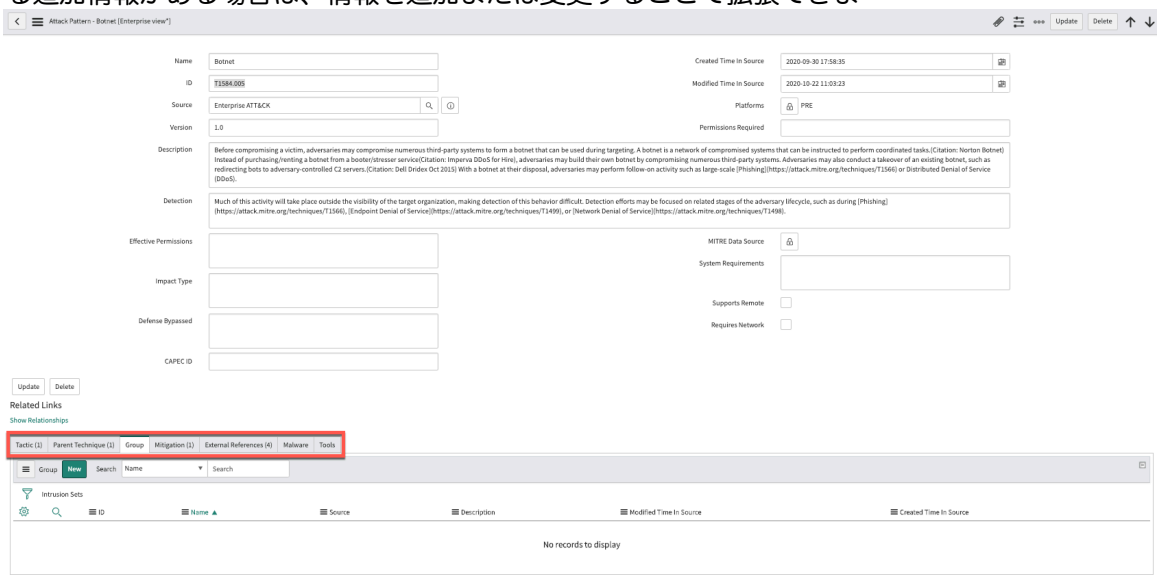
既存のテクニックと既存のオブジェクトの間で関係タイプをマッピングする場合は、テクニックをターゲットオブジェクトとして、オブジェクトをソースオブジェクトとして定義する必要があります。これを行うには、 **IoC** リポジトリ > オブジェクトとオブジェクトのリレーションシップ 移動します

グループを作成して攻撃パターンに関連付けることはできますが、MITRE ATT&CK リポジトリで確立できるのはグループと攻撃パターンの関係のみです。オブジェクト間の関係タイプを定義するには、IoC リポジトリで行う必要があります。

注:
オブジェクトに対して行ったカスタマイズは、スケジュール設定済みの更新時に保存されます。

手順

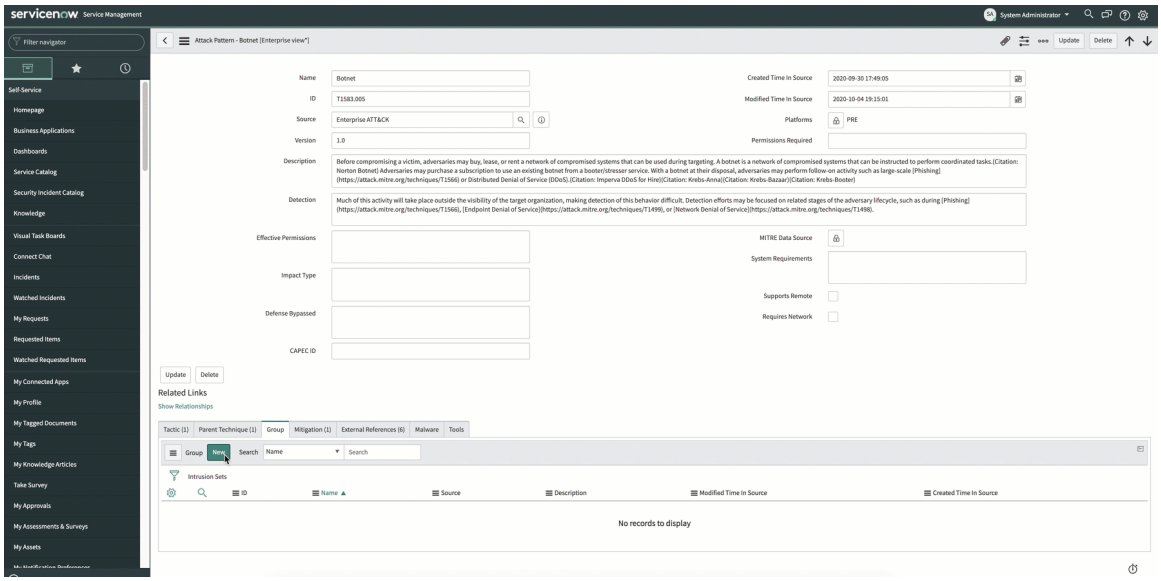
1. 次のように移動する。 脅威インテリジェンス > **MITRE ATT&CK** リポジトリ > テクニック.
2. テクニックまたはサブテクニックをクリックして、このテクニックに関連するすべての情報を表示します。
   次の図では、ボットネット (T1584.005) テクニックがどのグループにも関連付けられていないことがわかります。テクニックまたはサブテクニックに関する追加情報がある場合は、情報を追加または変更することで拡張できます。



3. 関連リストをクリックしてデータを拡張し、新しいグループに関連付けます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図では、グループ [Custom1] がボットネットのサブテクニックに関連付けられています。



データソースと検出ツールのマッピングの定義

MITRE-ATT&CK 戦術およびテクニックのデータソースと検出ツールのマッピングを定義します。データソースマッピングは、データソースの関連性と可用性、および環境内のデータソースを監視するための検出ツールを提供します。

始める前に

必要なロール：

- sn_ti.admin、sn_si.admin：書き込み、削除アクセス
- sn_ti.read：読み取りアクセス

このタスクについて

組織がテクニックを効果的に検出するために必要なデータソースと検出ツールを特定できます。

たとえば、組織が 5 つのテクニックに重点を置いている場合、それらのソースを監視するために 10 個のデータソースと 10 個の検出ツールが必要です。組織に 2 つのデータソースと 5 つの検出ツールがないことが判明したとします。この演習では、データソースを可視化し、組織との関連性を把握して、対象範囲内のギャップを特定できます。適切なデータソースと検出ツールを使用して、環境の拡張に集中することもできます。

すべてのアクティブな戦術、テクニック、ID、およびデータソースは、以下に基づいて自動的に入力されます TAXII プロファイル

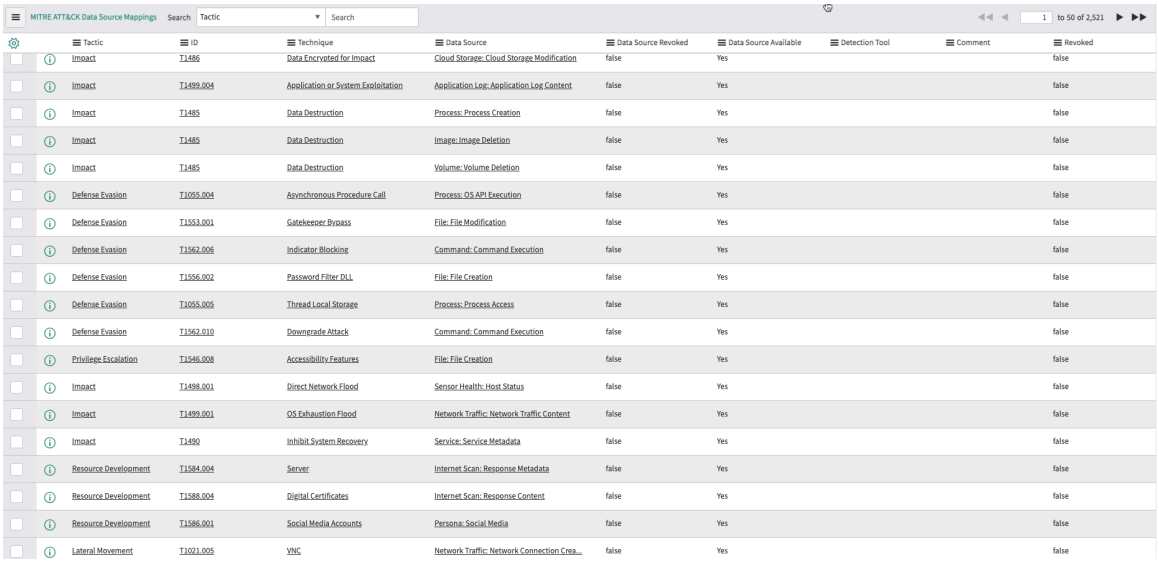
手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** 管理 > データソースマッピング.

   次の図は、コレクションの更新に基づいて入力された戦術、テクニック、およびそれらの ID のリストを示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



Tactic	ID	Technique	Data Source	Data Source Revoked	Data Source Available	Detection Tool	Comment	Revoked
Impact	T1486	Data Encrypted for Impact	Cloud Storage: Cloud Storage Modification	false	Yes			false
Impact	T1499.004	Application or System Exploitation	Application Log: Application Log Content	false	Yes			false
Impact	T1485	Data Destruction	Process: Process Creation	false	Yes			false
Impact	T1485	Data Destruction	Image: Image Deletion	false	Yes			false
Impact	T1485	Data Destruction	Volume: Volume Deletion	false	Yes			false
Defense Evasion	T1055.004	Asynchronous Procedure Call	Process: OS API Execution	false	Yes			false
Defense Evasion	T1553.001	Gatekeeper Bypass	File: File Modification	false	Yes			false
Defense Evasion	T1562.006	Indicator Blocking	Command: Command Execution	false	Yes			false
Defense Evasion	T1556.002	Password Filter DLL	File: File Creation	false	Yes			false
Defense Evasion	T1055.005	Thread Local Storage	Process: Process Access	false	Yes			false
Defense Evasion	T1562.010	Downgrade Attack	Command: Command Execution	false	Yes			false
Privilege Escalation	T1546.008	Accessibility Features	File: File Creation	false	Yes			false
Impact	T1498.001	Direct Network Flood	Sensor Health: Host Status	false	Yes			false
Impact	T1499.001	OS Exhaustion Flood	Network Traffic: Network Traffic Content	false	Yes			false
Impact	T1490	Inhibit System Recovery	Service: Service Metadata	false	Yes			false
Resource Development	T1584.004	Server	Internet Scan: Response Metadata	false	Yes			false
Resource Development	T1588.004	Digital Certificates	Internet Scan: Response Content	false	Yes			false
Resource Development	T1586.001	Social Media Accounts	Persona: Social Media	false	Yes			false
Lateral Movement	T1021.005	VNC	Network Traffic: Network Connection Crea...	false	Yes			false

フィールド	説明
戦術	アクションを実行するための攻撃者の目標または理由
ID	テクニックの一意の ID。
テクニック	テクニックは、攻撃者がアクションを実行して戦術的目標を達成する方法を表します。
データソース	テクニックに関連付けられているデータソース。
データソースが取り消されました	true に設定すると、データソースは取り消されますが、データソースマッピングは保持されます。 データソース値が MITREで見つからない場合、[データソースが取り消されました] の値は自動的に true とマークされます。更新された MITRE データにテクニックとデータソースの関係がない場合、レコードのデータソースマッピングは取り消されます。 デフォルト値：false
利用可能なデータソース	データソースの可用性。
検出ツール	使用されているテクニックを検出することによってデータソースを補足するツール。検出ツールは、SIR のアラートセンサーとマッピングされます。
取り消し済み	更新された MITRE データにテクニックとデータソースの関係がない場合、レコードのデータソースマッピングは取り消されます。 デフォルト値：false

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. 一覧表示されたデータソースを確認し、自分の環境に基づいて [利用可能なデータソース] フィールドの値を変更します。

3. 注:
リストビューからこのエントリーを編集することはできません。

[検出ツール] フィールドで、次の手順を実行します。

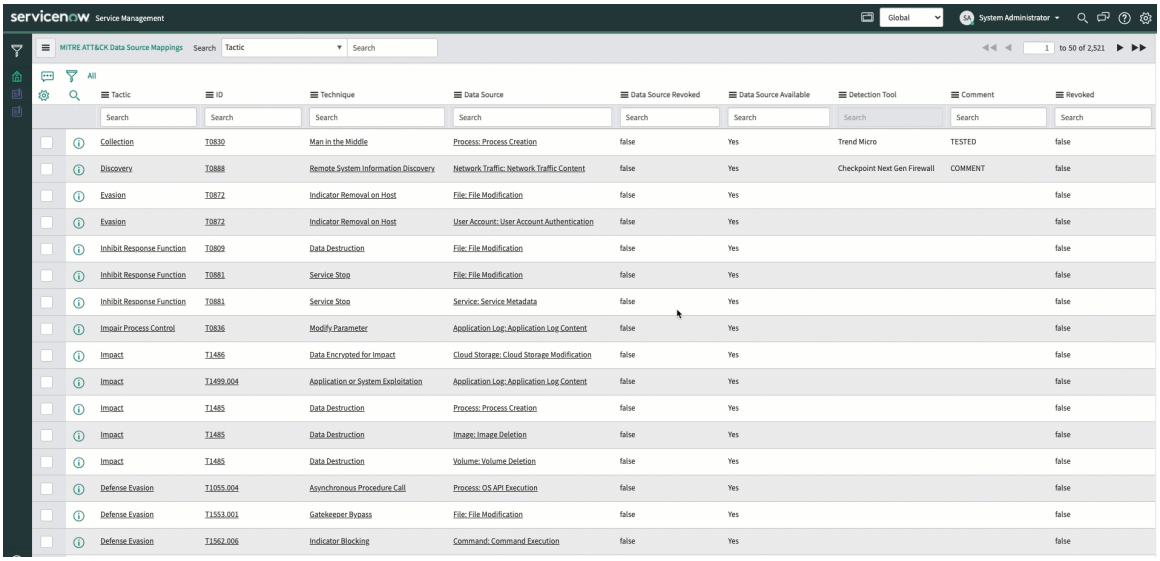
a. 情報アイコンをクリックして、[レコードを開く] をクリックします。

b. [検出ツール] エントリーのロックを解除します。

c. ルックアップリストを使用して検出ツールを選択します。検出ツールは複数選択できます。

d. [更新] をクリックします。

次の図では、データソースを監視するために複数の検出ツールが追加されています。



データソースとデータコンポーネントのマッピングの定義

最新の TAXII コレクションを使用していて、データソース、データコンポーネント、およびさまざまなテクニック間の関係を維持する場合は、データコンポーネントマッピングを使用します。データソースに追加のサブレイヤーコンテキストを提供するデータコンポーネントの追加コンテキストでデータソースをマッピングすることで、MITRE-ATT&CK 内の攻撃者の行動をより理解することができます。

始める前に

必要なロール：

- sn_ti.admin、sn_si.admin：書き込み、削除アクセス
- sn_ti.read：読み取りアクセス

このタスクについて

データソースとデータコンポーネントをマッピングすることで、データソースやコンポーネント、および組織に関連するテクニックを可視化できます。

たとえば、組織が 7 つのテクニックに焦点を当てている場合、5 つのデータソースと、これらのソースを監視するための 10 のデータコンポーネント必要であると考えられます。内部ツールの評価により、組織には 2 つのデータソースと 4 つのデータコンポーネントがないことが判明しました。このマッピング演習によって、データソース、コンポーネントとテクニック、組織との関連性が可視

自動翻訳

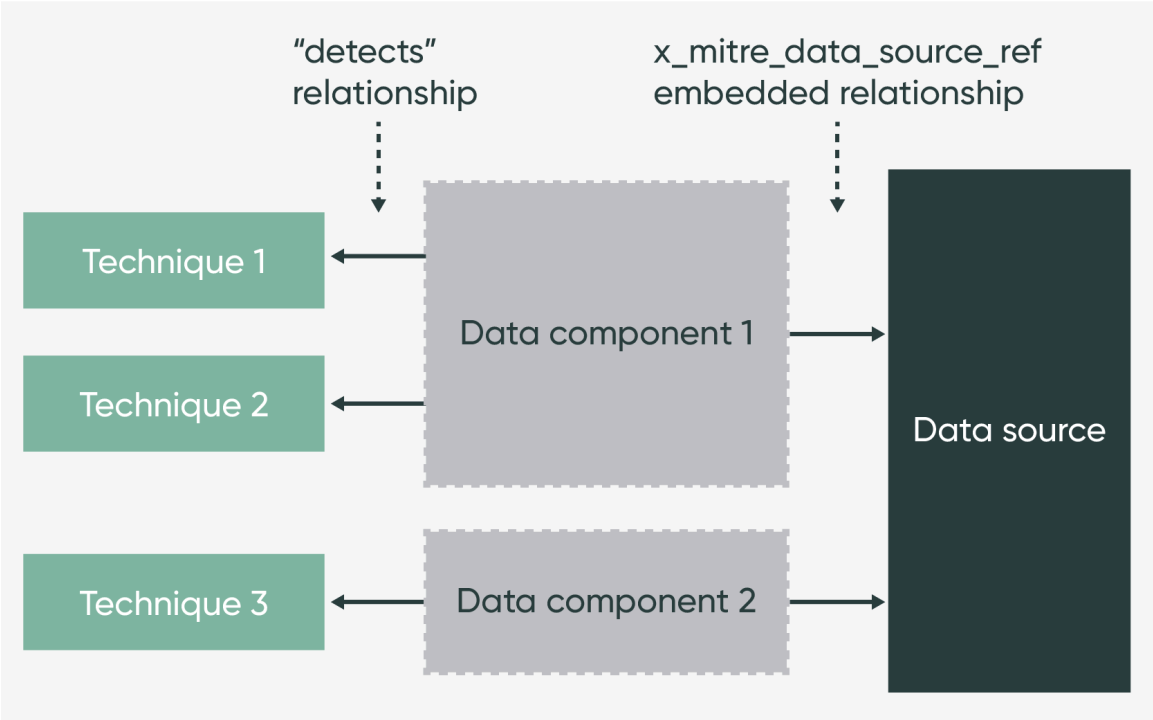
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

化され、範囲におけるギャップを確認することができます。これにより、適切なデータソースとアラートセンサーに投資を集中させて、攻撃者の脅威を検出して緩和できます。

MITRE-ATT&CK フレームワークでは、データソースの構造が更新されています (データソース：データコンポーネント)。このデータソースの新しい形式は、データソースに追加のコンテキストを提供します。データソースオブジェクトは、データソースの名前、コレクションされたデータに関する主な詳細 (ファイル、プロセス、ネットワークトラフィックなど)、および攻撃者の動作を検出するために必要な特定の値やプロパティを備えています。

次の図は、データソースとデータコンポーネントに対する MITRE-ATT&CK STIX™ の構造表示を示しています。データソースとデータコンポーネントの両方がカスタム STIX オブジェクトとしてキャプチャされているのがわかります。この図は、各データソースに 1 つ以上のデータコンポーネントが含まれており、各データコンポーネントが 1 つ以上のテクニックを検出することを示しています。

データソースとデータコンポーネントの一般的な構造



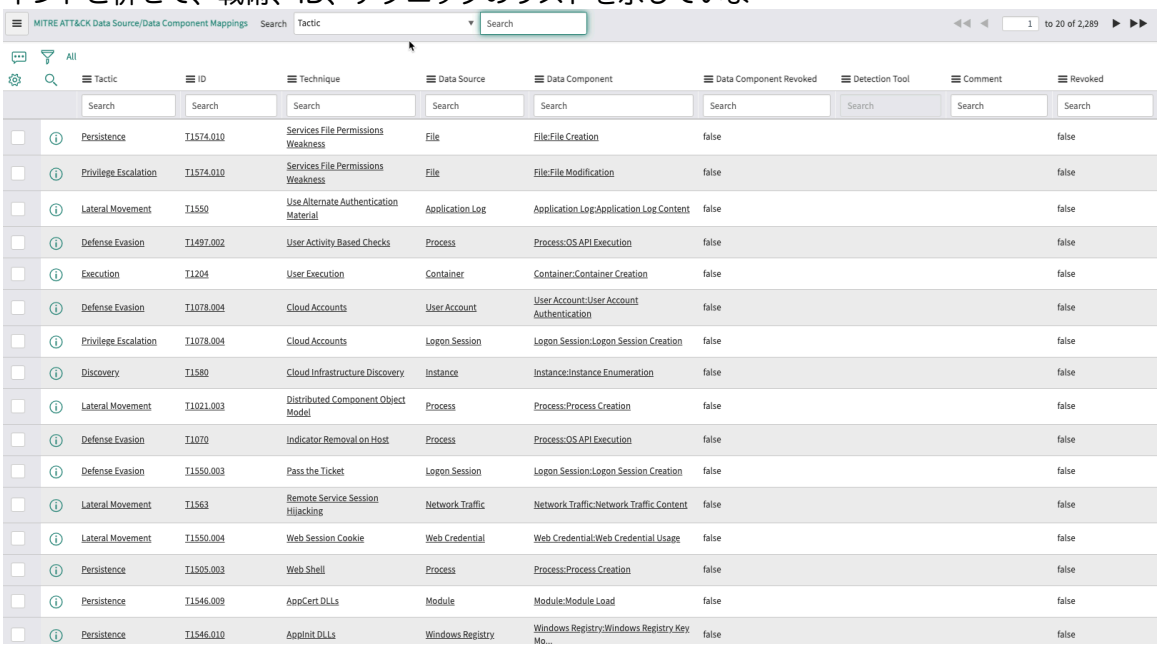
MITRE-ATT&CK リポジトリに古い TAXII コレクションが含まれていて、データソースをさまざまなテクニックにマッピングしている場合は、引き続きデータソースマッピング を使用できます。ただし、最新の TAXII コレクションを使用していて、データソース、データコンポーネント、およびさまざまなテクニック間の関係を維持する場合は、データコンポーネントマッピングを使用してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** 管理 > データコンポーネントマッピング.
   次の図は、コレクションの更新に基づくデータソースとデータコンポーネントと併せて、戦術、ID、テクニックのリストを示していま



す。

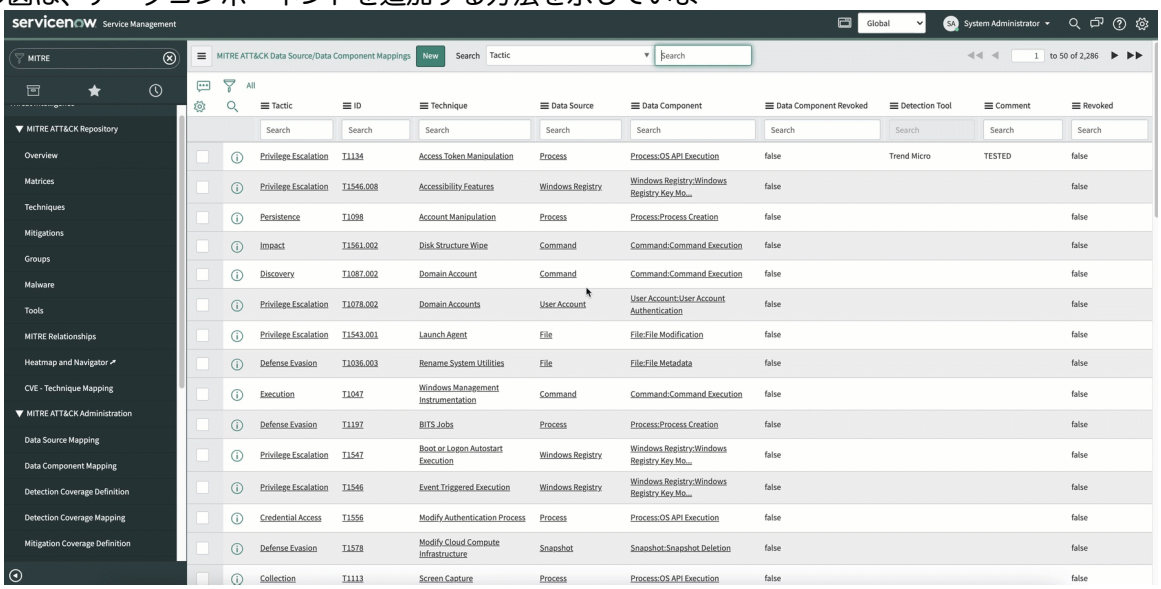
フィールド	説明
戦術	アクションを実行するための攻撃者の目標または理由
ID	テクニックの一意の ID。
テクニック	テクニックは、攻撃者がアクションを実行して戦術的目標を達成する方法を表します。
データソース	テクニックに関連付けられているデータソース。
データコンポーネント	データソースに関連付けられているデータコンポーネント。データコンポーネントは、親データソースを 1 つだけ持つことができます。
取り消されたデータコンポーネント	MITRE-ATT&CK ナレッジベースでデータコンポーネントが取り消されたかどうかを示します。
検出ツール	使用されているテクニックを検出することによってデータソースを補足するツール。検出ツールは、SIR のアラートセンサーとマッピングされます。
コメント	データソースとデータコンポーネントのマッピングの説明。
取り消し済み	データコンポーネントのテクニックへのマッピングが MITRE-ATT&CK によって取り消されたかどうかを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. 一覧表示されたデータソースとデータコンポーネントを確認し、自分の環境に基づいて値を変更します。
3. 次の手順を実行して、データコンポーネントを追加します。
   a. 次のように移動する。 脅威インテリジェンス > **MITRE ATT&CK** 管理 > テクニック.
   b. データソース：データコンポーネントの情報を変更するテクニックをクリックします。
   c. データソース：データコンポーネントのロックを解除します。
   d. ルックアップリストを使用して、MITRE-ATT&CK データコンポーネントを選択します。
   e. データソース：データコンポーネントをロックします。
   f. [更新] をクリックします。

次の図は、データコンポーネントを追加する方法を示していま



す。

テクニックディスカバリー範囲の定義

組織が特定の攻撃者のテクニックを測定して検出する必要があるテクニックディスカバリー範囲を定義します。

始める前に

- 必要なロール：sn_ti.admin、sn_si.admin：書き込みアクセス
- 必要なロール：sn_ti.read：読み取りアクセス

このタスクについて

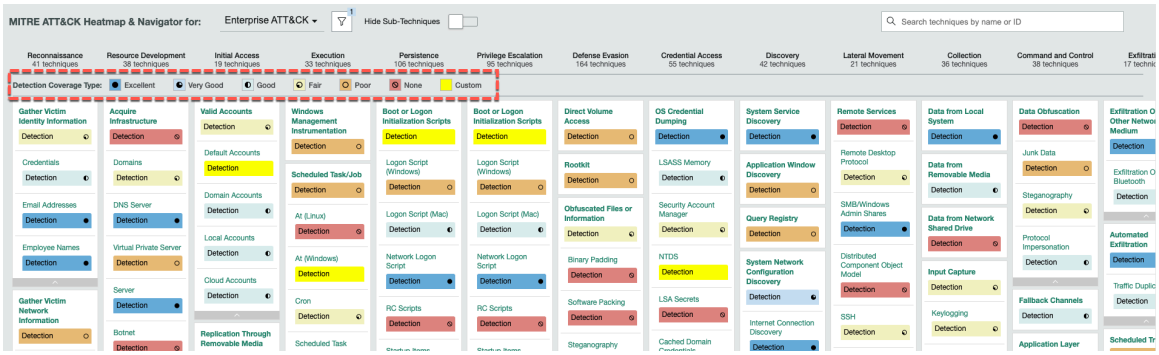
テクニック対象範囲の定義は、テクニック検出マッピング全体で使用されます。ベースシステムのテクニック対象範囲を使用できます。ベースシステムのテクニック対象範囲 は、範囲タイプ [なし]、[不満]、[普通]、[良好]、[とても良好]、および [優秀] で構成されます。ベースシステムのテクニック対象範囲も、事前定義された色に関連付けられています。対象範囲タイプのエントリーと色をカスタマイズしたり、独自のエントリーを作成したりできます。たとえば、ベースシステムの対象範囲タイプを [適用外]、[一部範囲 (Partial Coverage)]、および [完全範囲 (Complete Coverage)] に変更できます。または、0 ～ 25%、25 ～ 50%、50 ～ 100% などの対象範囲タイプの数値測定を作成することもできます。ベースシステム対象範囲の変更のタイプは、共有されている例に限定されません。

対象範囲のタイプと色のカスタマイズは、全体的なテクニック検出マッピングで使用され、ヒートマップでも使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
ベースシステムの対象範囲の定義を変更すると、テクニックとともに対象範囲タイプのアイコンがヒートマップに表示されなくなります。ベースシステムの定義されたテクニックディスカバリー範囲および対象範囲の色と同じフィールドを変更すると、ヒートマップは正常に機能します。ただし、全体的なテクニックディスカバリー範囲から既存のフィールドを削除すると、ヒートマップには対象範囲タイプのアイコンが表示されません。



手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** 管理 > 検出範囲の定義.
2. 全体的なテクニック検出エントリーを確認し、環境に合わせてエントリーをカスタマイズします。

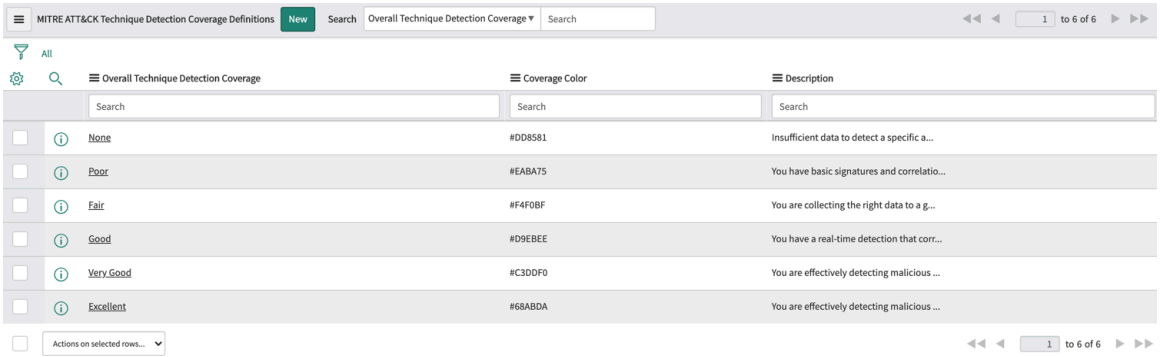
ディスカバリー範囲の定義

フィールド	説明
全体的なテクニックディスカバリー範囲	全体的なテクニックディスカバリー範囲の名前。ベースシステムのテクニック対象範囲は、[なし]、[不満]、[普通]、[良好]、[とても良好]、および [優秀] で構成されます。
対象範囲の色	ディスカバリー範囲スコアに割り当てられた色。定義した色は、ヒートマップのテクニックディスカバリー範囲に使用されます。 HEX コードと RGB(A) 値を使用して色をカスタマイズできます。
説明	全体的なテクニックディスカバリー範囲。「スコアリング定義」のベースシステム定義を参照してください。

次の図は、[ディスカバリー範囲の定義] リストを示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. エントリーを追加するには、[新規] をクリックし、エントリーを入力して、[送信] をクリックします。

MITRE-ATT&CK 採点の定義

組織が特定の攻撃者のテクニックをどれだけ効果的に検出できるかを測定できるように、組織の MITRE-ATT&CK 採点システムを定義します。

採点の定義

スコア	スコアマッピング	説明
なし	0	特定の攻撃者のテクニックを検出するのに十分なデータがありません。
不満	1	特定の攻撃者のテクニックを検出するために、基本的な署名と相関ルールが用意されています。脅威検出はリアルタイムではなく、テクニックの最小限の側面のみに対応しています。たとえば、ハンティングは一度に 1 つのエンドポイントでのみ実行されます。組織には、数千または数百のイベントがまだある可能性があるため、これらのイベントをハンティング担当者が確認し、他のイベントと関連付けて外れ値を見つける必要があります。誤検出の数が多くなっています。
普通	2	適切なデータを大量に収集し、データ品質は普通です。たとえば、組織が Sysmon ログ、ETW、PowerShell ログなどの追加を開始するとします。ただし、脅威の検出はまだリアルタイムではありません。組織には、データを効果的に集計および分析するための適切なツールがない場合があります。データを正確に分析するには、手動でクエリを実行して関連付ける必要があります。誤検出の数が多くなっています。
良好	3	エンドポイント全体で複数のデータを関連付けて統合するリアルタイム検出。脅威検出は、テクニックの手順の多くの側面に対応しています。攻撃者は、回避と難読化によって検出をバイパスする可能性があります。組織は誤検出を簡単に識別して除外できます。組織は、基本的なデータ科学技術を使用して中央リポジトリのデータを分析します。
とても良好	4	悪意のあるテクニックをリアルタイムで効果的に検出し、テクニックの手順のほとんどの側面に対応します。攻撃者が回避や難読化の方法で検出をバイパスする可能性は、[良好] レベルよりも困難です。組織は誤

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

採点の定義 (続く)

スコア	スコアマッピング	説明
		検出を簡単に識別して除外できます。組織は、高度なデータ科学技術を使用して攻撃者のテクニックを検出します。
優秀	5	悪意のあるテクニックをリアルタイムで効果的に検出し、テクニックの手順のすべての側面に対応します。組織は、適切な自動化とデータ品質を使用して、環境を十分に把握しています。攻撃者が回避や難読化の方法で検出をパイパスする可能性は、[良好] レベルよりも困難です。誤検出の数が少なくなっています。

テクニックディスカバリー範囲をテクニックにマッピングする

組織が特定の攻撃者のテクニックを検出できるようにするテクニックを使用して、全体的なテクニックディスカバリー範囲をマッピングします。

始める前に

- 必要なロール：sn_ti.admin、sn_si.admin：書き込みアクセス
- 必要なロール：sn_ti.read：読み取りアクセス

このタスクについて

テクニックディスカバリー範囲を使用すると、組織の全体的なテクニックディスカバリー範囲の概要を把握できます。たとえば、攻撃者が組織を攻撃している場合、攻撃者のテクニックを検出するために必要な範囲が表示されます。

テクニックと ID は、アクティブ化したすべてのコレクションとテクニックに対して自動入力されます。定義した範囲タイプとスコアリング定義は、全体的なテクニックディスカバリー範囲で選択できるオプションとして使用できます。

全体的なテクニックディスカバリー範囲をテクニックを使用してマッピングし、マッピングを完了することができます。1 つのテクニックは、1 つの全体的なテクニックディスカバリー範囲にのみ関連付けることができます。

定義したテクニックディスカバリー範囲のマッピングは、ヒートマップにおける範囲の可視化で使用されます。

注:
組織固有の算出方法を使用して、全体的なテクニックディスカバリー範囲を算出できます。スコアリング定義には、Breach & Attack Simulation (BAS) 製品、Cyber Analytics Repository (CAR)、または必要に応じてその他の方法を使用し、この手順で全体的なテクニックディスカバリー範囲のマッピングに使用することができます。

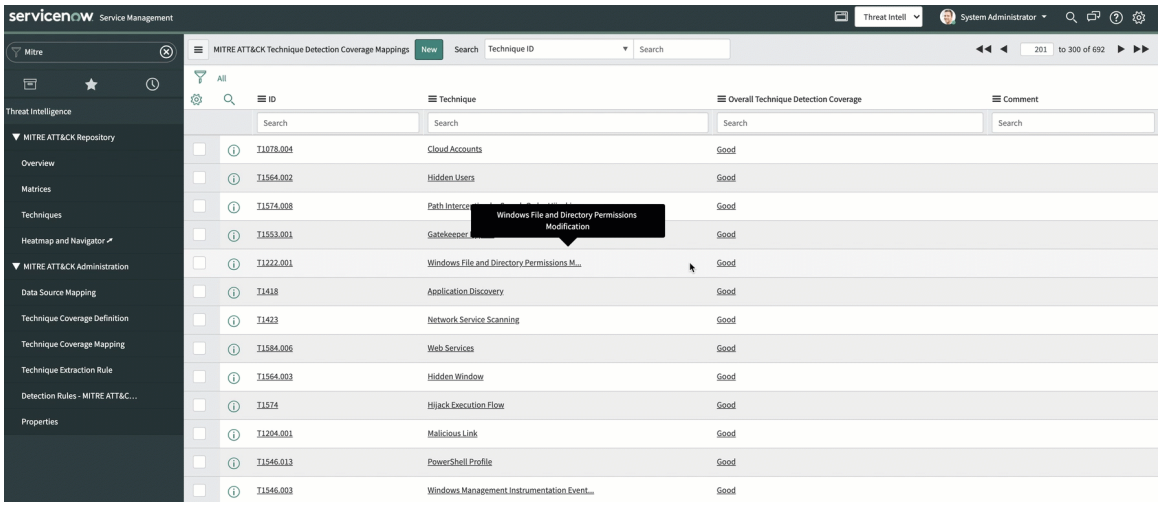
手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** 管理 > 検出範囲のマッピング.

   この図では、クラウドアカウント (T1078.004) サブテクニックが組織内で優れた範囲を持ち、全体的なテクニックディスカバリー範囲が [優秀 **(Excellent)**] にマッピングされていることがわかります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



2. 各テクニックを確認して、ディスカバリー範囲の定義と組織における範囲の可用性に基づいて、全体的なテクニックディスカバリー範囲をマッピングします。

緩和対象範囲の定義

特定のテクニックによって発生する攻撃を組織がどの程度阻止できるかを可視化できるように、テクニックに関連する各緩和策の緩和対象範囲を定義します。

始める前に

- 必要なロール：sn_ti.admin、sn_si.admin：作成、書き込み、削除アクセス
- 必要なロール：sn_ti.read：読み取りアクセス

このタスクについて

緩和対象範囲の定義は、緩和対象範囲およびテクニック対象範囲のマッピング全体で使用されます。ベースシステムの緩和対象範囲を使用できます。ベースシステムの緩和対象範囲 は、範囲タイプ [なし]、[不満]、[普通]、[良好]、[とても良好]、および [優秀] で構成されます。ベースシステムの緩和対象範囲も、事前定義された色 (対象範囲パーセンテージ) に関連付けられています。対象範囲タイプ (対象範囲タイプの追加または削除)、対象範囲パーセンテージの下限と上限、および色をカスタマイズしたり、カスタムの緩和対象範囲を作成したりできます。

対象範囲タイプと色またはパーセンテージのカスタマイズは、緩和対象範囲マッピングで使用され、ヒートマップでも使用されます。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** 管理 > 緩和対象範囲の定義.
2. 緩和検出エントリーを確認し、環境に合わせてエントリーをカスタマイズします。

テクニック緩和対象範囲の定義

フィールド	説明
全体的なテクニック緩和対象範囲	テクニック緩和対象範囲の名前。ベースシステムの緩和対象範囲は、[なし]、[不満]、[普通]、[良好]、[とても良好]、および [優秀] で構成されます。
対象範囲パーセンテージの下限	緩和対象範囲のパーセンテージ下限。0 ～ 100 の数値を定義します。

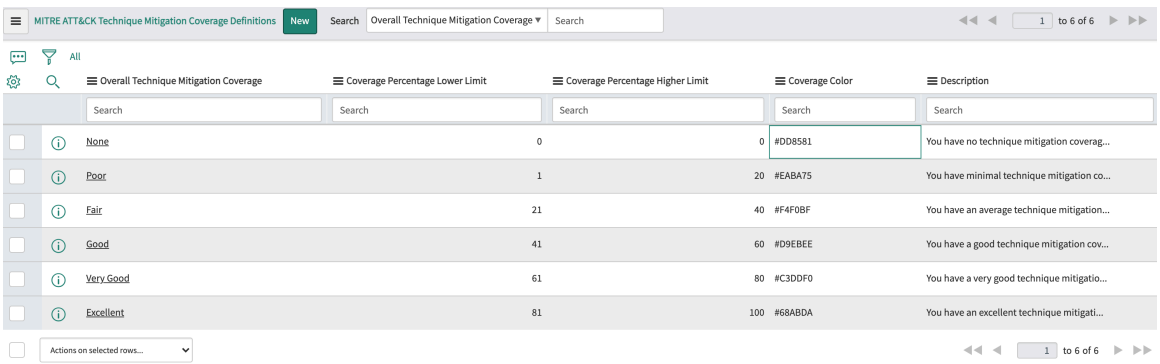
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
対象範囲パーセンテージの上限	緩和対象範囲のパーセンテージ上限。0 ～ 100 の数値を定義します。
対象範囲の色	ディスカバリー範囲スコアに割り当てられた色。定義した色は、ヒートマップのテクニック緩和対象範囲に使用されます。 HEX コードと RGB(A) 値を使用して色をカスタマイズできます。
説明	全体的な緩和ディスカバリー範囲。「テクニック緩和対象範囲の定義」のベースシステム定義を参照してください。

注:
パーセンテージ制限 (下限または上限) をカスタマイズする場合は、対象範囲パーセンテージが重複していないことを確認してください。たとえば、対象範囲レコードの範囲が 0 ～ 20 の場合、対象範囲のパーセンテージ範囲が重複しないように、次の連続するレコードの下限範囲を 21 以上にする必要があります。

次の図は、[緩和対象範囲の定義] リストを示しています。



3. エントリーを追加するには、[新規] をクリックし、エントリーを入力して、[送信] をクリックします。

テクニック緩和対象範囲の定義

組織が特定の攻撃者のテクニックを効果的に検出できるように、組織の緩和対象範囲を定義します。

MITRE ATT&CK テクニック緩和対象範囲の定義

全体的なテクニック緩和対象範囲	対象範囲パーセンテージの下限	対象範囲パーセンテージの上限	対象範囲の色	説明
なし	0	0	#DD8581	テクニック緩和対象範囲がなく、どのシナリオでも防御コントロールで攻撃を阻止できません。
不満	1	20	#EABA75	最小限のテクニック緩和対象範囲しかありません。攻撃の可能性は非常に高く、防御コン

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

MITRE ATT&CK テクニック緩和対象範囲の定義 (続く)

全体的なテクニック緩和対象範囲	対象範囲パーセンテージの下限	対象範囲パーセンテージの上限	対象範囲の色	説明
				トロールで攻撃を阻止できるのはシナリオの 0 ～ 20% です。
普通	21	40	#F4F0BF	平均的なテクニック緩和対象範囲があります。攻撃の可能性は高く、防御コントロールで攻撃を阻止できるのはシナリオの 21 ～ 40% です。
良好	41	60	#D9EBEE	広いテクニック緩和対象範囲があります。攻撃の可能性は比較的高く、防御コントロールで攻撃を阻止できるのはシナリオの 41 ～ 60% です。
とても良好	61	80	#C3DDF0	非常に広いテクニック緩和対象範囲があります。攻撃の可能性は低く、防御コントロールで攻撃を阻止できるのはシナリオの 61 ～ 80% です。
優秀	81	100	#68ABDA	優秀なテクニック緩和範囲があり、このテクニックを使用する攻撃の可能性は非常に低く、防御コントロールで攻撃を 81 ～ 100% 阻止できます。

自動翻訳

緩和対象範囲をテクニックにマッピングする

組織の全体的な緩和戦略が検出できるようにするテクニックを使用して、緩和対象範囲をマッピングします。

始める前に

- 必要なロール：sn_ti.admin、sn_si.admin：書き込み、削除アクセス
- 必要なロール：sn_ti.read：読み取りアクセス

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
緩和により、攻撃者が組織に対してテクニックまたはサブテクニックを実行することを防ぐことができます。各 MITRE-ATT&CK テクニックには、攻撃される可能性を抑えるために組織で展開できる緩和策が含まれています。緩和対象範囲を使用して、組織の全体的な緩和戦略の概要を把握できます。たとえば、攻撃者が組織を攻撃している場合、攻撃者のテクニックを緩和するためにどのような対象範囲があるのかが分かります。

テクニックと緩和に関する情報は、アクティブ化したすべてのコレクションとテクニックに対して自動入力されます。定義した緩和対象範囲の定義は、テクニック緩和対象範囲で選択できます。

組織に関連する緩和を特定できます。緩和が関連する場合、緩和戦略が展開されているかどうかを定義できます。組織の SOC ポリシーの一部として戦略を適用するかどうかを指定できます。また、攻撃者のテクニックを緩和するための予防ツールが組織にあるかどうかを確認し、セキュリティリスクを最小限に抑えるために組織が展開しているセキュリティコントロールをマッピングすることもできます。各レコードの緩和対象範囲 (パーセンテージ) を入力してください。

各テクニックの情報をマッピングすると、緩和対象範囲計算ツールによって、計算されたテクニック緩和対象範囲が自動入力されます。テクニックの全体的な緩和対象範囲を計算するには、テクニック緩和マッピングレコードがアクティブであり、組織に関連している必要があります。非アクティブで関連性のないレコードは、全体的なテクニック緩和対象範囲の計算では考慮されません。計算されたテクニック緩和対象範囲の値と緩和対象範囲の定義に基づいて、全体的なテクニック緩和対象範囲 (計算済み) が入力されます。

対象範囲タイプと色またはパーセンテージのカスタマイズは、緩和対象範囲マッピングで使用され、ヒートマップでも使用されます。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** 管理 > 緩和対象範囲のマッピング.
2. 緩和マッピングに対する各テクニックを確認し、[緩和対象範囲 (パーセンテージ)]を更新して、組織における対象範囲の可用性を計算します。

テクニック緩和対象範囲のマッピング

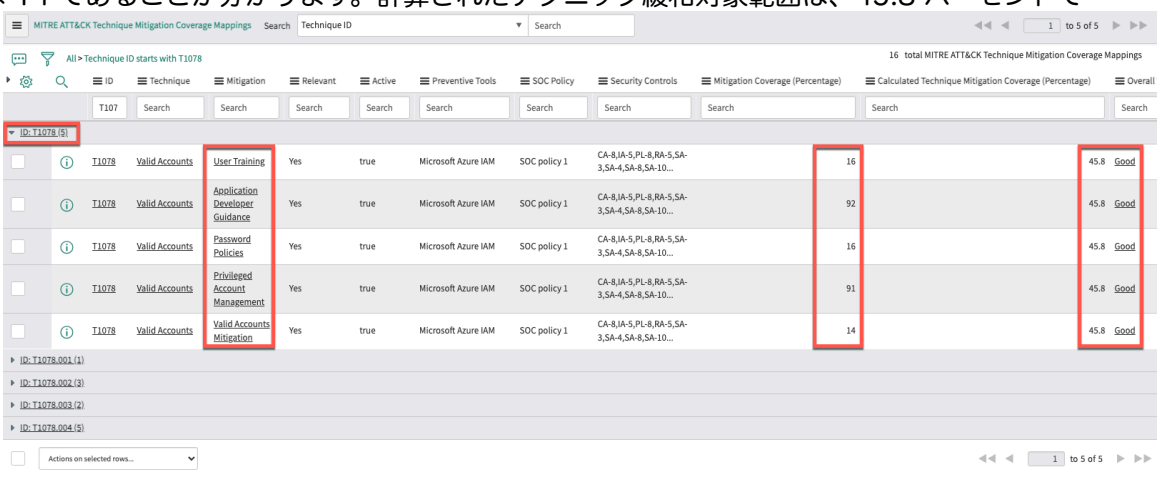
フィールド	説明
ID	テクニックの一意の ID。ID は、アクティブ化したすべてのコレクションとテクニックに対して自動入力されます。
テクニック	テクニックは、攻撃者がアクションを実行して戦術的目標を達成する方法を表します。テクニックに関する情報は、アクティブ化したすべてのコレクションとテクニックに対して自動入力されます。
緩和	攻撃者が組織に対してテクニックやサブテクニックを実行することを防ぐことができる緩和策。緩和に関する情報は、アクティブ化したすべてのコレクションとテクニックに対して自動入力されます。
関連	緩和が組織に関連しているかどうかを指定するオプション。
有効	緩和戦略が組織に展開されているかどうかを指定するオプション。これは、テクニック緩和対

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	象範囲を計算するために必要なオプションです。
予防ツール	攻撃者のテクニックを緩和するための予防ツールが組織にあるかどうかを指定するオプション。
SOC ポリシー	組織内の緩和戦略を定義する SOC ポリシー。
セキュリティコントロール	組織のセキュリティコントロールには、セキュリティリスクを最小限に抑えるための緩和戦略が含まれています。
緩和対象範囲 (パーセンテージ)	テクニック緩和対象範囲を計算するための採点システム。0 ～ 100 の数値を定義します。これは、テクニック緩和対象範囲を計算するために必要なオプションです。
計算されたテクニック緩和対象範囲 (パーセンテージ)	計算されたテクニック緩和対象範囲 (パーセンテージ)。この値は、緩和対象範囲計算ツールで定義された式に基づいて決定されます。
全体的なテクニック緩和対象範囲 (計算済み)	全体的なテクニック緩和対象範囲。この値は、組織のために定義された緩和対象範囲に基づいて決定されます。
コメント	テクニックと緩和対象範囲のマッピングに関する説明。
取り消し済み	緩和対象範囲のマッピングに対するテクニックが取り消されています。

この図では、「有効なアカウント」テクニックに 5 つの緩和策が関連付けられており、それぞれの緩和対象範囲 (パーセンテージ) がユーザートレーニングは 16、アプリケーション開発者ガイダンスは 92、パスワードポリシーは 16、特権アカウント管理は 91、有効なアカウント緩和策は 14 であることが分かります。計算されたテクニック緩和対象範囲は、45.8 パーセントで



す。

全体的なテクニック緩和対象範囲計算ツール

全体的なテクニック緩和対象範囲は、緩和対象範囲計算ツールに定義された式に基づいて決定されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に

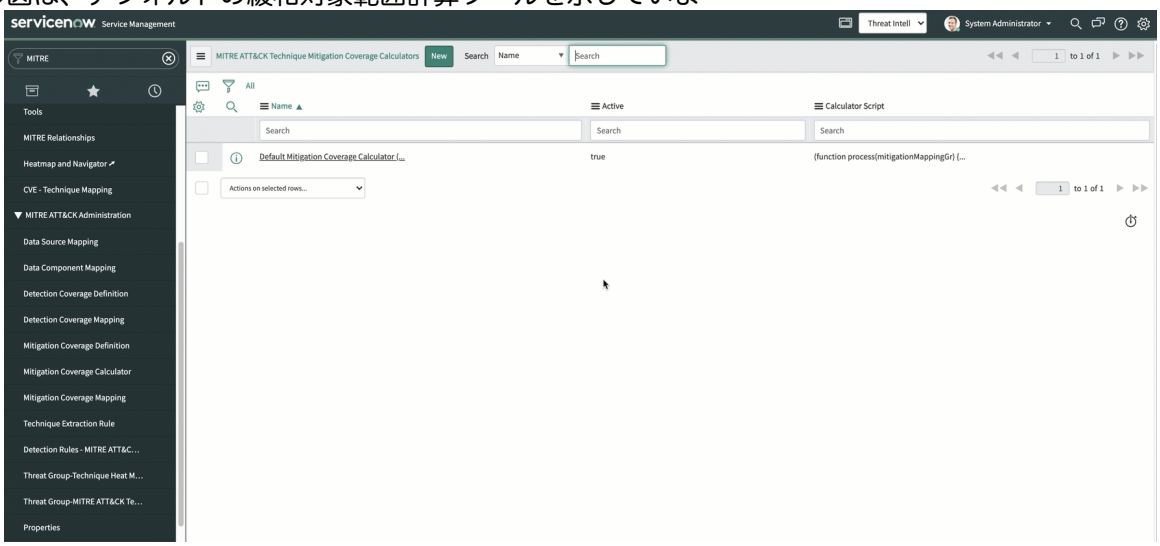
- 必要なロール：sn_ti.admin、sn_si.admin：作成、書き込み、削除アクセス
- 必要なロール：sn_ti.read：読み取りアクセス

このタスクについて

- ドメインごとに 1 つの緩和対象範囲計算ツールのみをアクティブに設定できます。
- ベースシステムの緩和対象範囲計算ツールは平均的な計算ツールです。
- 計算ツールのスクリプトをカスタマイズする場合は、最終出力が 0 ～ 100 の数値になるようにする必要があります。
- 緩和対象範囲の定義は、最終出力の範囲に基づいて適用されます。

手順

次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** 管理 > 緩和対象範囲計算ツール.
次の図は、デフォルトの緩和対象範囲計算ツールを示していま



す。

検出ルールの作成とマッピング

検出ルールを作成し、戦術とテクニックに対してマッピングします。このマッピングを使用すると、組織内の検出ルールの対象範囲を確認できます。

始める前に
必要なロール：

- sn_ti.admin、sn_si.admin：作成、書き込み、削除アクセス
- sn_ti.read：読み取りアクセス

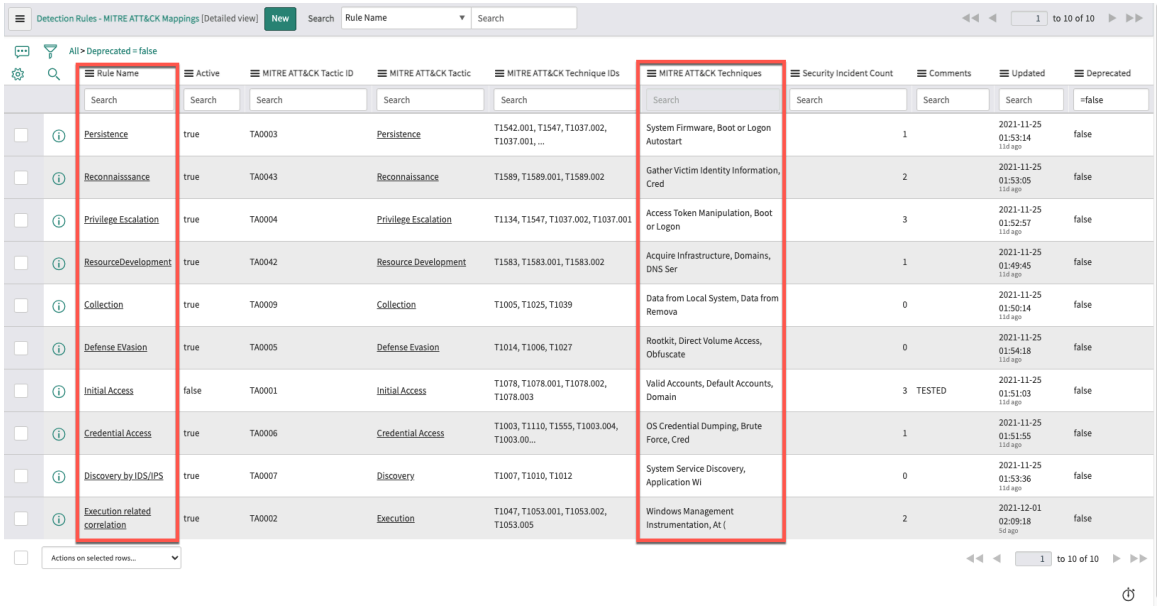
このタスクについて
検出ルールのマッピングにより、組織は特定のテクニックを識別できる検出ルールを確認できます。

マッピングの主な目的は、特定のテクニックを使用して攻撃者から攻撃を受けたときにアラートまたはイベントをトリガーするタイミングを判断するのに必要な検出ルールが組織にある場合に、可視化することです。

たとえば、さまざまなテクニックにマッピングされた検出ルールのリストを示す次の図を表示します。この情報は、 the MITRE-ATT&CK ナビゲーター.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



ベースシステムの SIEM 自動抽出ルールを使用しない場合は、検出ルールマッピングに基づいて MITRE-ATT&CK TTP の自動ロールアップを有効にします。セキュリティインシデントをトリガーするアラートまたはイベントルールを [アラートルール] の名前フィールドに入力できます。SIEM 統合、メール解析、手動作成などを使用して、[アラートルール名] フィールドに入力することもできます。詳細については、「検出ルールからの MITRE-ATT&CK 情報をロールアップする」を参照してください。

自動翻訳

注:

検出ルール機能が更新され、1 つの戦術を複数のテクニックにマッピングできるようになりました。以前は、1 つの戦術を 1 つのテクニックにしかマッピングできませんでした。脅威インテリジェンス プラグインをバージョン 12.0.4 から上位のバージョンにアップグレードする場合は、MITRE-ATT&CK モジュールの検出ルールを使用する前に次の点を確認してください。

- ルール名、アラートセンサー、ソース、カテゴリ、サブカテゴリ、および MITRE-ATT&CK 戦術のフィールドが共通の場合、複数のレコードが単一のレコードに結合されます。
- 古いレコードは、[廃止] 列で [true]、[アクティブ] 列で [false] とマークされます。
- 新しく結合されたレコードは、[廃止] 列で [false]、[アクティブ] 列で [true] とマークされます。
- アップグレードを確認し、すべての検出ルールが正常に移行されたことを確認したら、[廃止] 列で [true] とマークされた古いレコードを削除できます。

手順

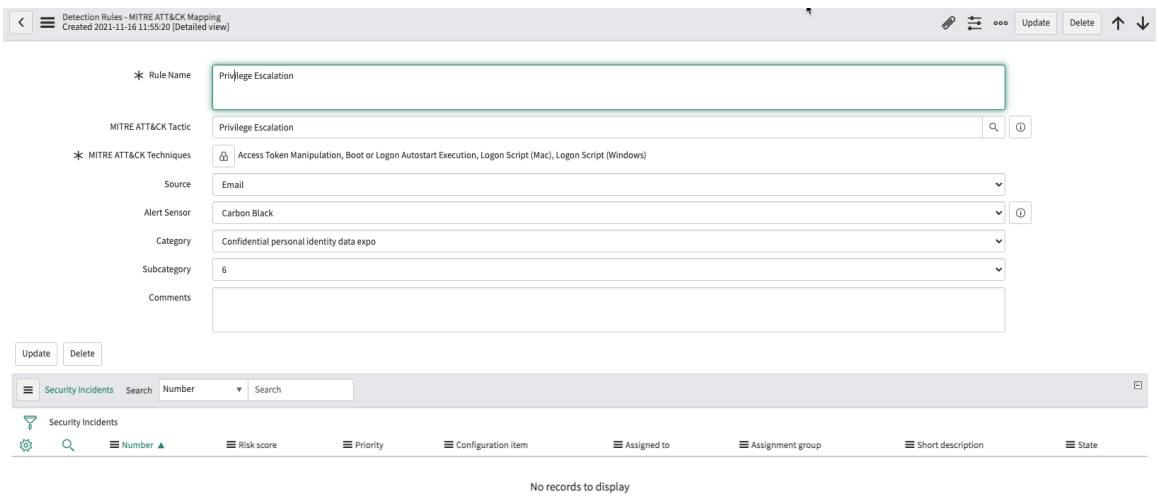
1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** 管理 > 検出ルール **- MITRE ATT&CK** マッピング.
2. 検出ルールを作成するには、次のいずれかの方法を使用します。
   方法 1：検出ルールを手動で作成します。
   a. [新規] をクリックし、フォームのフィールドに入力します。

検出ルール **- MITRE-ATT&CK** マッピング

フィールド	説明
ルール名	検出ルールの名前。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
MITRE-ATT&CK 戦術	関連する MITRE-ATT&CK 戦術。
MITRE-ATT&CK テクニック	関連する MITRE-ATT&CK テクニック。1 つの戦術で複数のテクニックを選択できます。
ソース	メール、ファイアウォール、ネットワーク監視などのセキュリティインシデントのソース。
アラートセンサー	CarbonBlack、CrowdStrike、McAfee などのアラートまたはイベントデータを取り込むためのセキュリティ統合
サブカテゴリ	問題をさらに細かく定義するサブカテゴリ。
カテゴリ	セキュリティ問題のタイプを識別するカテゴリ。
MITRE-ATT&CK テクニック	関連する MITRE-ATT&CK テクニック。1 つの戦術で複数のテクニックを選択できます。
セキュリティインシデント数	テクニックが追加されるセキュリティインシデントの数。この数は、アラートルールからセキュリティインシデントへの MITRE-ATT&CK 情報の自動ロールアップを有効にした場合に表示されます。
不使用	検出ルールのマッピングは廃止されました。
有効	検出ルールがアクティブで環境に展開されているかどうかを指定するオプション。



b. [Submit] をクリックします。

方法 2：検出ルールをインポートして作成します。

a. [ルール名] 列ヘッダーを右クリックします。

b. リストから、[インポート] をクリックします。

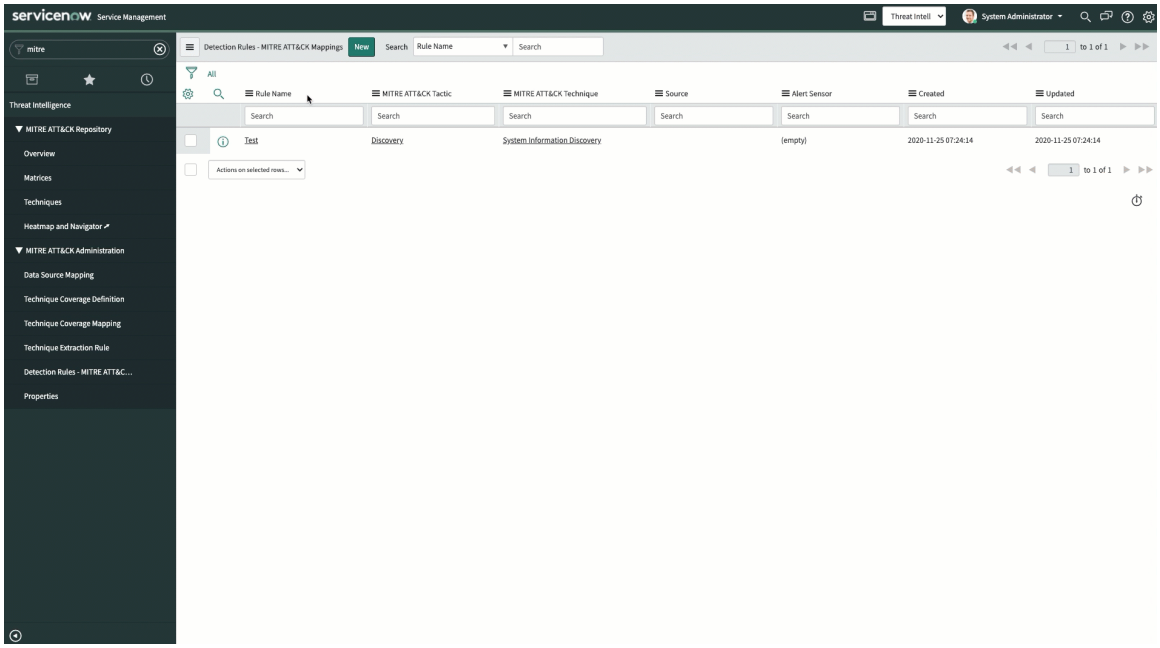
c. [Excel テンプレートを作成] をクリックします。

d. エクスポートが完了したら、[ダウンロード] をクリックします。sn_ti_alert_rules_mitre_attack_technique_mapping というファイル名の Excel テンプレートがコンピューターにダウンロードされます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

次の図では、Excel テンプレートをエクスポートして、スプレッドシートに詳細を入力し、ファイルをアップロードして、フィールドをプレビューしてから、Now Platform にインポートする方法を示しています。



e. スプレッドシートを開き、2 番目のシートタブを選択して、入力内容を確認します。フォームでフィールドに入力し、ファイルを保存します。

テンプレートのインポート

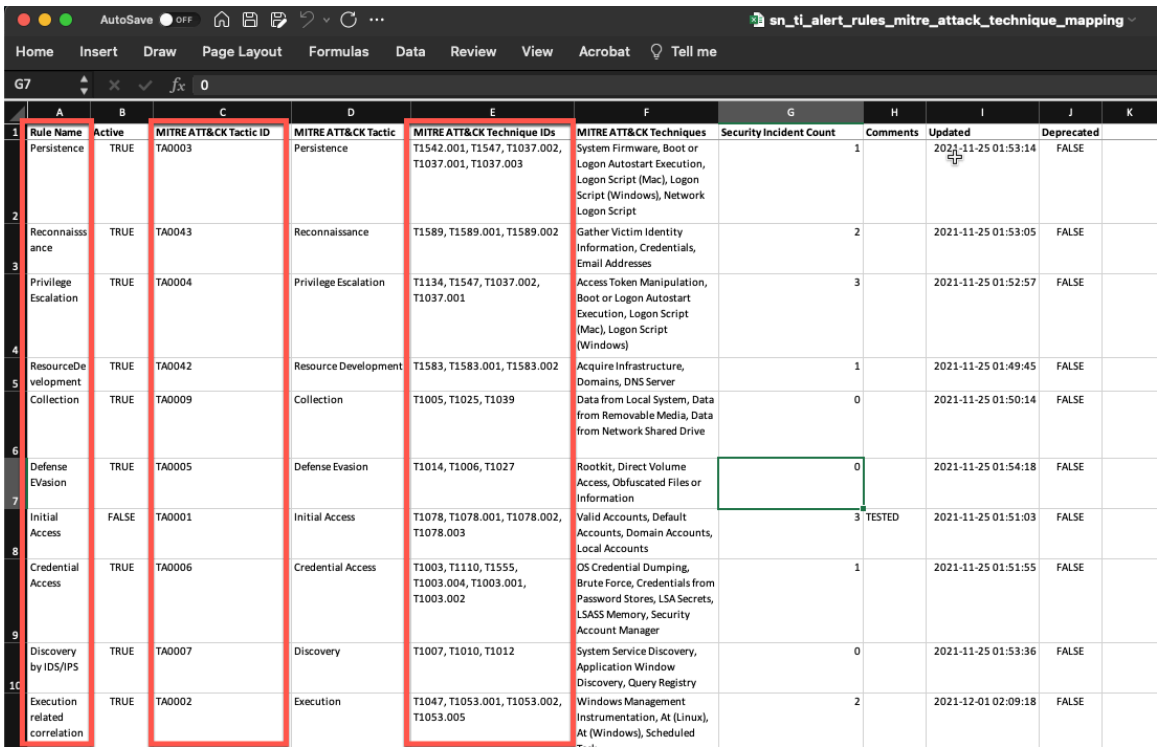
フィールド	説明
ルール名	検出ルールの名前。
有効	検出ルールがアクティブで環境に展開されているかどうかを指定するオプション。
アラートセンサー	CarbonBlack、CrowdStrike、McAfee などのアラートまたはイベントデータを取り込むためのセキュリティ統合
カテゴリ	セキュリティ問題のタイプを識別するカテゴリ。
コメント	検出ルールに関する説明。
不使用	検出ルールのマッピングは廃止されました。
MITRE-ATT&CK テクニック ID	アクセシビリティ機能の MITRE-ATT&CK テクニック ID (T1546.008 など)。
MITRE-ATT&CK 戦術 ID	永続性の MITRE-ATT&CK 戦術 ID (TA0003 など)。
セキュリティインシデント数	テクニックが追加されるセキュリティインシデントの数。この数は、アラートルールからセキュリティインシデントへの MITRE-ATT&CK 情報の自動ロールアップを有効にし、検出ルールがアクティブの場合に表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ソース	メール、ファイアウォール、ネットワーク監視などのセキュリティインシデントのソース。
サブカテゴリ	問題をさらに細かく定義するサブカテゴリ。
MITRE-ATT&CK 戦術	関連する MITRE-ATT&CK 戦術。
MITRE-ATT&CK テクニック	関連する MITRE-ATT&CK テクニック。

次の図は、スプレッドシートテンプレートを示しています。必須フィールド ([ルール名]、[MITRE-ATT&CK 戦術 ID]、および [MITRE-ATT&CK テクニック ID]) は赤でハイライト表示されています。



	A	B	C	D	E	F	G	H	I	J	K
1	Rule Name	Active	MITRE ATT&CK Tactic ID	MITRE ATT&CK Tactic	MITRE ATT&CK Technique IDs	MITRE ATT&CK Techniques	Security Incident Count	Comments	Updated	Deprecated	
2	Persistence	TRUE	TA0003	Persistence	T1542.001, T1547, T1037.002, T1037.001, T1037.003	System Firmware, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows), Network Logon Script	1		2021-11-25 01:53:14	FALSE	
3	Reconnaissance	TRUE	TA0043	Reconnaissance	T1589, T1589.001, T1589.002	Gather Victim Identity Information, Credentials, Email Addresses	2		2021-11-25 01:53:05	FALSE	
4	Privilege Escalation	TRUE	TA0004	Privilege Escalation	T1134, T1547, T1037.002, T1037.001	Access Token Manipulation, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows)	3		2021-11-25 01:52:57	FALSE	
5	ResourceDevelopment	TRUE	TA0042	Resource Development	T1583, T1583.001, T1583.002	Acquire Infrastructure, Domains, DNS Server	1		2021-11-25 01:49:45	FALSE	
6	Collection	TRUE	TA0009	Collection	T1005, T1025, T1039	Data from Local System, Data from Removable Media, Data from Network Shared Drive	0		2021-11-25 01:50:14	FALSE	
7	Defense EVasion	TRUE	TA0005	Defense Evasion	T1014, T1006, T1027	Rootkit, Direct Volume Access, Obfuscated Files or Information	0		2021-11-25 01:54:18	FALSE	
8	Initial Access	FALSE	TA0001	Initial Access	T1078, T1078.001, T1078.002, T1078.003	Valid Accounts, Default Accounts, Domain Accounts, Local Accounts	3	TESTED	2021-11-25 01:51:03	FALSE	
9	Credential Access	TRUE	TA0006	Credential Access	T1003, T1110, T1555, T1003.004, T1003.001, T1003.002	OS Credential Dumping, Brute Force, Credentials from Password Stores, LSA Secrets, LSASS Memory, Security Account Manager	1		2021-11-25 01:51:55	FALSE	
10	Discovery by IDS/IPS	TRUE	TA0007	Discovery	T1007, T1010, T1012	System Service Discovery, Application Window Discovery, Query Registry	0		2021-11-25 01:53:36	FALSE	
	Execution related correlation	TRUE	TA0002	Execution	T1047, T1053.001, T1053.002, T1053.005	Windows Management Instrumentation, At (Linux), At (Windows), Scheduled	2		2021-12-01 02:09:18	FALSE	

f. [ファイルを選択] をクリックし、コンピューターでスプレッドシートを選択します。

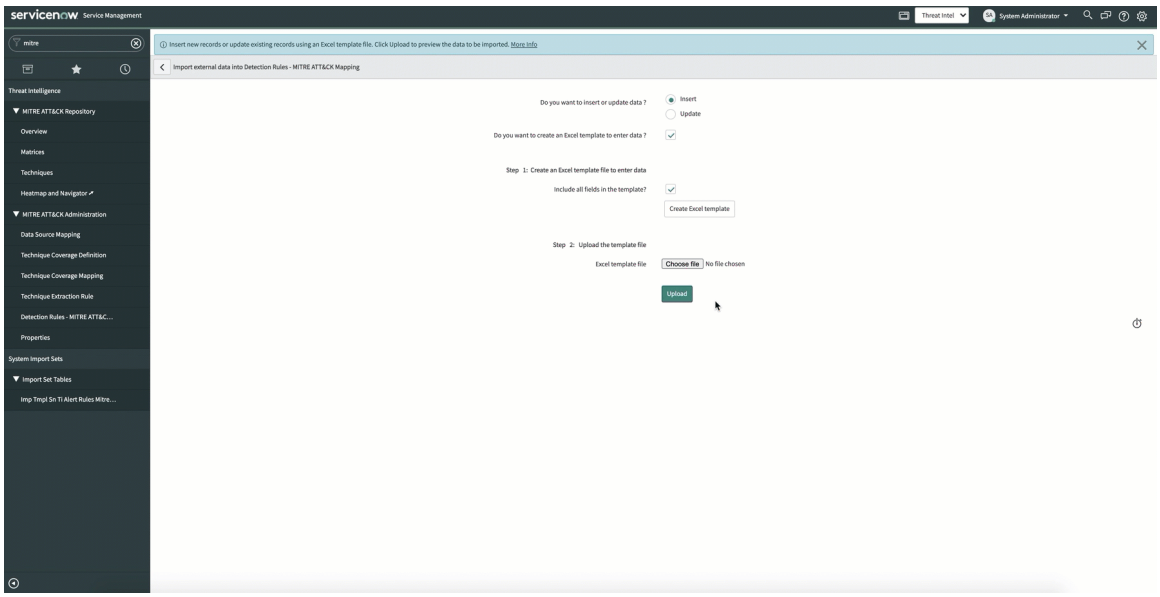
g. [アップロード] をクリックします。

h. [インポートされたデータをプレビュー] をクリックします。

i. マッピングをプレビューし、[インポート完了] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図は、スプレッドシートをアップロードして、データをプレビューし、エラーがないか確認してから、検出ルールマッピングのインポートプロセスを完了する方法を示しています。



MITRE-ATT&CK 情報をインポートするための自動抽出テクニックルール

ベースシステムの自動抽出ルールを使用して、既存のサードパーティ統合から MITRE-ATT&CK 情報をインポートします。

脅威のルックアップ自動抽出ルールの使用

脅威のルックアップ自動抽出ルールを使用して、既存の 脅威インテリジェンス サードパーティ統合から MITRE-ATT&CK 情報をインポートします。

始める前に

必要なロール：

- sn_ti.admin、sn_si.admin：作成、書き込み、削除アクセス
- sn_ti.read：読み取りアクセス

このタスクについて

サンドボックスや TIP などの 脅威インテリジェンス 統合が MITRE-ATT&CK フレームワークをサポートし、各統合レベルで MITRE-ATT&CK 情報が解析されると、その情報が各脅威のルックアップの結果レコードに表示されます。ただし、すべての 脅威インテリジェンス 統合が MITRE-ATT&CK 情報を解析するわけではありません。脅威のルックアップのグローバル自動抽出ルールは、すべての 脅威インテリジェンス 統合から MITRE-ATT&CK 情報を抽出できます。

脅威のルックアップの結果からセキュリティインシデントに MITRE-ATT&CK 情報を自動的にロールアップするように選択できます。脅威のルックアップ結果をセキュリティインシデントに自動的にロールアップするには、システムのプロパティを有効にします。また、個々の脅威のルックアップに、情報を手動でロールアップすることもできます。

脅威インテリジェンス 統合によってテクニックや戦術などの MITRE-ATT&CK 情報が提供される場合、ベースシステムの 脅威インテリジェンス は、サードパーティ統合の生のペイロードから脅威のルックアップの結果レコードに自動的に MITRE-ATT&CK 情報を抽出します。

脅威のルックアップレコードの生のペイロードフィールドで MITRE-ATT&CK 情報が利用できない場合は、サードパーティ統合からの自動抽出に独自のルールを定義する必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** 管理 > テクニック抽出ルール.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

[テクニック抽出ルール] フォーム

フィールド	説明
名前	自動抽出ルールの名前。
ルールタイプ	自動抽出ルールのタイプ。[脅威のルックアップ] を選択します。
自動抽出を無視	デフォルトでクリアされている設定。この設定により、MITRE-ATT&CK テクニックの自動抽出が有効になります。
ソースエンジン	ソースエンジン。
グローバル	ソースエンジンの設定。ソースエンジンを [グローバル] に設定すると、すべての脅威のルックアップの統合結果で抽出が実行されます。
説明	自動抽出ルールの説明。
プロセスメソッド	正規表現、または生のペイロードからテクニック情報をリンクするために指定するスクリプトメソッド。
正規表現抽出	正規表現抽出メソッドを使用するときに、[ターゲットフィールド] に指定するオプション。正規表現がデフォルトです。
スクリプト抽出	スクリプトの実行時に選択するプロセス。このスクリプトは以下を確認します。 ○ ThreatLookupResultSysId：脅威のルックアップ結果レコードの sys_id ○ sourceName：脅威のルックアップソースの名前。
戦術の抽出	生のペイロードから戦術関連情報を抽出するために指定するオプション。ペイロードに特定の戦術とテクニックに関連する情報が含まれている場合は、その情報を抽出してセキュリティインシデントに追加できます。

4. **[Submit]** をクリックします。

SIEM 自動抽出ルールの使用

SIEM 自動抽出ルールを使用して、既存の セキュリティオペレーション SIEM サードパーティ統合から MITRE-ATT&CK 情報をインポートします。

始める前に
必要なロール：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- sn_ti.admin、sn_si.admin：作成、書き込み、削除アクセス
- sn_ti.read：読み取りアクセス

このタスクについて
テクニック抽出ルールは、Splunk、IBM QRadar、ArcSight 統合などのすべてのベースシステム セキュリティオペレーション SIEM 統合で使用できます。Now Platform がこれらの SIEM 統合からアラートやイベントデータを取り込み、それらに MITRE-ATT&CK 情報が含まれている場合、Now Platform は生のペイロードを処理し、MITRE-ATT&CK 情報を自動抽出します。

Now Platform にベースシステム SIEM 統合が含まれている場合は、テクニック抽出ルールは MITRE-ATT&CK モジュールに既に作成されていることを意味します。必要に応じてルールを確認し、変更する必要があります。

SIEM 自動抽出ルールまたはアラートルールのいずれかを一度に有効にします。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** 管理 > テクニック抽出ルール.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

[テクニック抽出ルール] フォーム

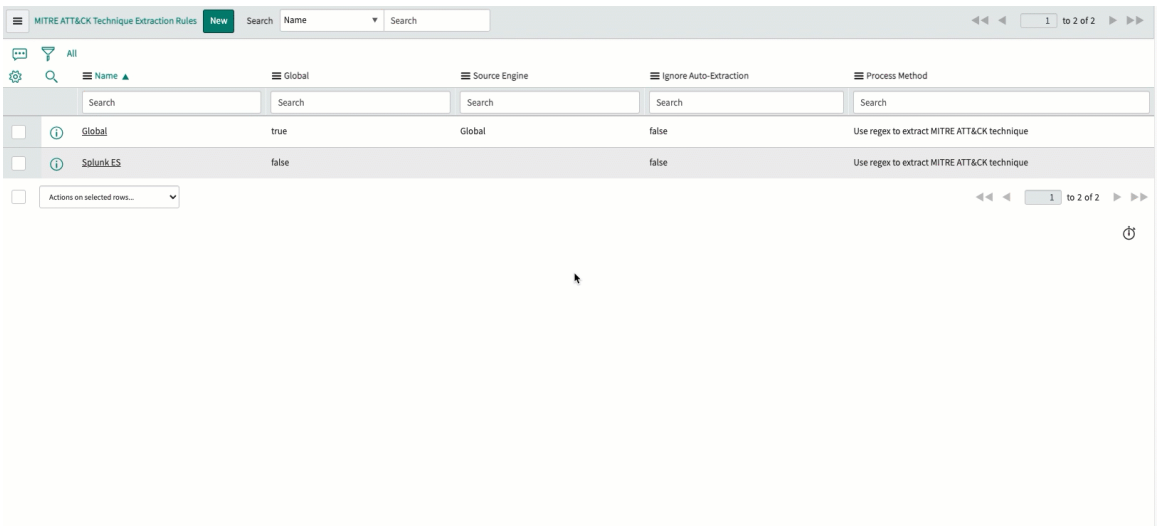
フィールド	説明
名前	自動抽出ルールの名前。
ルールタイプ	自動抽出ルールのタイプ。**[SIEM]** を選択します。
自動抽出を無視	デフォルトでクリアされている設定。この設定により、MITRE-ATT&CK テクニックの自動抽出が有効になります。
テーブルのインポート	ベースシステムの SIEM 統合用に自動的にマッピングされるインポートテーブル。他の SIEM 統合について MITRE-ATT&CK の情報がないかこのフィールドを確認し、それに従ってマッピングします。
インポートフィールド	ベースシステムの SIEM 統合用に自動的にマッピングされるインポートフィールド。他の SIEM 統合について MITRE-ATT&CK の情報がないかこのフィールドを確認し、それに従ってマッピングします。
説明	自動抽出ルール。
プロセスメソッド	正規表現、または生のペイロードからテクニック情報をリンクするために指定するスクリプトメソッド。
正規表現抽出	正規表現メソッドを使用するときに、[ターゲットフィールド] に指定するオプション。正規表現抽出はデフォルトのプロセスメソッドです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
スクリプト抽出	MITRE-ATT&CK 情報の抽出方法をカスタマイズする場合に使用するスクリプトプロセスメソッド。
戦術の抽出	生のペイロードから戦術関連情報を抽出するために指定するオプション。ペイロードに特定の戦術とテクニックに関連する情報が含まれている場合は、その情報を抽出してセキュリティインシデントに追加できます。

次の図では、フォームビューに Splunk Enterprise SIEM テクニック抽出ルールの例が示されています。このルールは、他のすべての SIEM テクニック抽出ルールに似ています。



4. **[Submit]** をクリックします。

脅威グループと **MITRE-ATT&CK** テクニックのマッピングを確認する

MITRE TAXII コレクションからインポートされる、脅威グループとテクニックのオブジェクト間の関係マッピング情報を確認します。このマッピングにより、テクニックグループと対応するテクニックマッピングを表示できます。

始める前に

必要なロール：

- sn_ti.admin、sn_si.admin：作成、書き込み、削除アクセス
- sn_ti.read：読み取りアクセス

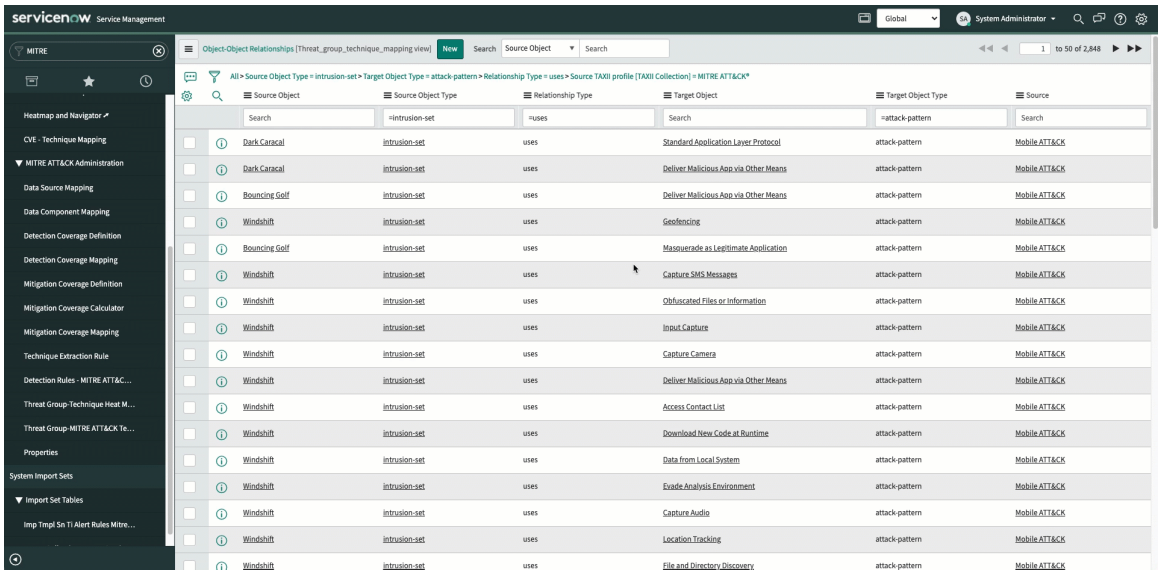
手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** 管理 > 脅威グループ-**MITRE ATT&CK** テクニック.
2. [ソースオブジェクト] を右クリックし、[ソースオブジェクトによるグループ化 **(Group By Source Object)]** を選択して、脅威グループに関連付けられたすべての攻撃パターンを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図は、脅威グループ admin@338 と、この脅威グループが採用するさまざまな攻撃パターンで、エンタープライズ攻撃ソースの一部を示しています。



脅威グループ - テクニックヒートマップ定義

ヒートマップ上で脅威グループが組織への攻撃に使用している攻撃パターンを測定、検出できるように、脅威グループ - テクニックヒートマップ定義を行います。多数の攻撃者がいる場合、特定のテクニックを使用する攻撃の可能性が高くなります。

始める前に
必要なロール：

- sn_ti.admin、sn_si.admin：書き込みアクセス
- sn_ti.read：読み取りアクセス

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** 管理 > 脅威グループ-テクニックヒートマップ定義.
2. 脅威グループ - テクニックヒートマップ定義を確認し、環境に応じてエントリーをカスタマイズします。

脅威グループ - テクニックヒートマップ定義

フィールド	説明
脅威グループの数 (最小範囲)	特定のテクニックを使用する脅威グループの最小数。
脅威グループの数 (最大範囲)	特定のテクニックを使用する脅威グループの最大数。多数の攻撃者がいる場合、特定のテクニックを使用する攻撃の可能性が高くなります。
ヒートマップの色	脅威グループカテゴリにアサインされた色。定義した色は、ヒートマップ内で脅威グループカテゴリを強調表示するために使用されます。

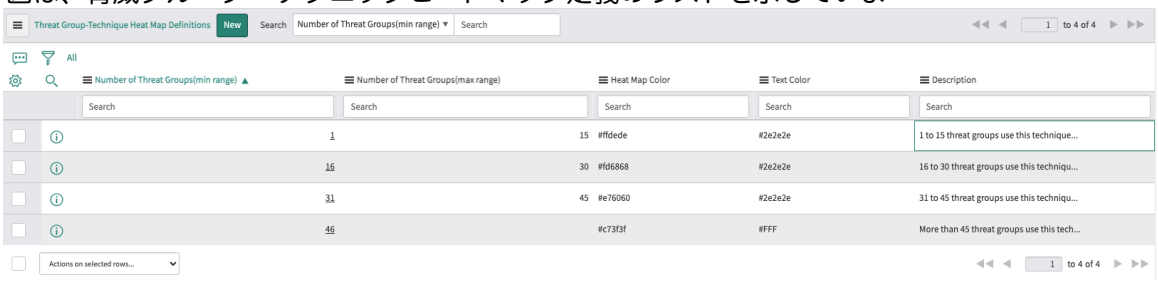
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	HEX コードと RGB(A) 値を使用して色をカスタマイズできます。
テキストの色	脅威グループテキストにアサインされた色。定義した色は、ヒートマップ内で脅威グループを強調表示するために使用されます。 HEX コードと RGB(A) 値を使用して色をカスタマイズできます。
説明	脅威グループの範囲と定義に関する説明。

注:
脅威グループの範囲 (最小または最大) をカスタマイズする場合は、脅威グループ数の範囲が重複していないことを確認してください。

次の図は、脅威グループ - テクニックヒートマップ定義のリストを示していま



す。

3. エントリーを追加するには、[新規] をクリックし、エントリーを入力して、[送信] をクリックします。

MITRE-ATT&CK のシステムプロパティの確認

MITRE-ATT&CK のシステムプロパティ値を確認します。

始める前に
必要なロール：sn_ti.admin、sn_si.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** 管理 > プロパティ.
2. フォームのフィールドに入力します。

[MITRE-ATT&CK プロパティ] フォーム

フィールド	説明
観測事象からセキュリティインシデントに MITER ATT&CK 情報を自動的にロールアップ [sn_ti.rollup_mitre_att&ck_technique_observable_to_si]	観測事象からセキュリティインシデントへの MITRE-ATT&CK 情報のロールアップ。詳細については、「MITRE ATT&CK 情報の観測事象への関連付け」を参照してください。 デフォルト値：はい

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
脅威ルックアップ結果からセキュリティインシデントに MITER ATT&CK 情報を自動的にロールアップ [sn_ti.rollup_mitre_att&ck_technique_threat_lookup_si]	脅威ルックアップ結果からセキュリティインシデントへの MITRE-ATT&CK 情報のロールアップ。詳細については、「脅威ルックアップの自動抽出」を参照してください。 デフォルト値：はい
アラートルールからセキュリティインシデントに MITER ATT&CK 情報を自動的にロールアップ [sn_ti.rollup_mitre_att&ck_technique_alert_rule_si]	アラートルールからセキュリティインシデントへの MITRE-ATT&CK TTP 情報の自動ロールアップ。詳細については、「マップ検出ルール」を参照してください。 デフォルト値：いいえ
子セキュリティインシデントから親セキュリティインシデントに MITER ATT&CK 情報を自動的にロールアップ [sn_ti.rollup_mitre_att&ck_technique_child_si_si]	子セキュリティインシデントから親セキュリティインシデントに MITRE-ATT&CK 情報を自動的にロールアップします。 デフォルト値：はい
このプロパティを有効にすると、[検出ルール - MITER ATT&CK マッピング] テーブルの検出ルールを使用して、カテゴリやサブカテゴリなどの [セキュリティインシデント] フィールドをマッピングできます [sn_ti.enable_category_mapping_with_alert_rule]	[検出ルール - MITRE ATT&CK マッピング] ページのカテゴリとサブカテゴリ。 デフォルト値：いいえ
「CVE - VUL カウント」を計算するための時間 (単位：時間) [sn_ti.time_to_calculate_cve_vits_count]	CVE および VUL 情報を計算する予約時間 (単位：時間)。 デフォルト値：24

3. [保存] をクリックします。

MITRE-ATT&CK を使用した脅威の検出と分析

脅威インテリジェンス および SIR モジュール全体で MITRE-ATT&CK フレームワークを使用して、組織に対する脅威を検出および分析します。

MITRE-ATT&CK™ 情報のセキュリティインシデントへの関連付け

セキュリティインシデントと脅威を適切に分析できるように、MITRE-ATT&CK の戦術とテクニックをセキュリティインシデントに関連付けます。

始める前に

必要なロール：sn_si.analyst

このタスクについて

セキュリティインシデントと脅威を相関付けて適切に分析できるように、MITRE-ATT&CK の戦術とテクニックの情報をセキュリティインシデントに関連付けます。たとえば、組織が 脅威インテリジェンス レポートや セキュリティインシデントレスポンス の外部の他のソースなどのサードパーティソースから、戦術、テクニック、手順 (TTP) 関連の情報を受け取っている場合があります。その後、適切に相関付けて脅威分析できるように、この情報を SIR に追加します。

脅威のルックアップの自動抽出結果から、観測事象から、または子セキュリティインシデントからセキュリティインシデントに MITRE-ATT&CK 情報を自動的にロールアップすることもできます。セ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

キュリティインシデントに自動的にロールアップするには、システムプロパティを有効にします。また、脅威のルックアップまたは観測事象ごとに、情報を手動でロールアップすることもできます。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. MITRE-ATT&CK 情報で拡張するセキュリティインシデントを選択します。
3. **[MITRE ATT&CK** テクニックの関連付け **(Associate MITRE ATT&CK Technique)]** 関連リンクをクリックします。
   [MITRE ATT&CK テクニックの関連付け (Associate MITRE ATT&CK Technique)] ペインが表示されます。

   この図は、関連リストに移動して [MITRE-ATT&CK テクニックの関連付け] を探し、ソースの Enterprise ATT&CK を確認して、戦術の影響を追加し、テクニックのシステムシャットダウン/再起動を追加する方法を示しています。

   MITRE 情報をセキュリティインシデントに関連付けます　。
4. [ソース] を選択します。

   > **注:**
   > アクティブ化されたコレクションとマトリクスのみがソースリストに表示されます。

   ソースに関連付けられている戦術とテクニックを選択できます。複数のリソースを関連付けることもできます。
5. [戦術] と [テクニック] を選択します。
6. オプション: セキュリティインシデントとの関連性に基づいて情報を確認し、次の操作を実行します。
   - 関連付けを完全に削除するには、ゴミ箱アイコンをクリックします。このアイコンをクリックすると、ソースとそれに関連付けられている戦術とテクニックが削除されます。
   - 戦術を削除するには、戦術の横にある [-] アイコンをクリックします。
   - テクニックを削除するには、テクニックの横にある [x] アイコンをクリックします。
7. [保存] をクリックします。

タスクの結果

MITRE-ATT&CK 情報がセキュリティインシデントに関連付けられます。これで、関連情報を **MITRE ATT&CK** カードに表示できます。

MITRE-ATT&CK 情報をクローズ済みセキュリティインシデントに関連付ける

MITRE-ATT&CK の戦術とテクニックをクローズ済みセキュリティインシデントに関連付けて、セキュリティインシデントと脅威を適切に分析できるようになりました。

MITRE 情報をセキュリティインシデントに関連付けます

MITRE-ATT&CK カードを使用してセキュリティインシデントの関連情報を表示する

MITRE-ATT&CK カードを使用して、セキュリティインシデントの MITRE-ATT&CK 関連情報を表示できます。

脅威のルックアップ、観測事象、または SIEM 統合から情報がロールアップされた後、セキュリティインシデントに追加されます。次に、集計された情報が MITRE-ATT&CK カードに表示されます。**[MITRE ATT&CK** カード] には、次の 2 つのビューがあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ナビゲータービュー：このビューは、MITRE-ATT&CK ナビゲーターに似ており、観測事象や脅威のルックアップのテーブルから手動で追加されたりロールアップされたすべてのテクニックを表示します。[テクニックの由来を表示 **(Show origin of techniques)]** では、テクニックが手動でロールアップされているまたはソースを通している場合に、テクニックの由来を表示します。**[ID** を表示 **(Show ID)]** はテクニック ID を表示します。

  次の図は、**[MITRE ATT&CK** カード] ナビゲータービューに移動する方法を示しています。利用可能なリンクのいずれかをクリックすると、脅威インテリジェンス モジュールで情報が表示されます。

  MITRE ATT&CK カード：ナビゲータービューとリストビュー

- リストビュー：このビューは、リスト形式またはテーブル形式でデータを表示します。このビューでは、さまざまなテーブルとグループに及んでいるすべてのデータを表示できます。

  次の図は、MITRE ATT&CK カードのリストビューに移動する方法を示しています。利用可能なリンクのいずれかをクリックすると、脅威インテリジェンス モジュールで情報が表示されます。

MITRE-ATT&CK 情報の観測事象への関連付け

セキュリティインシデントと脅威を詳細なレベルで分析できるように、MITRE-ATT&CK の戦術とテクニックを観測事象に関連付けます。

始める前に

必要なロール：sn_si.analyst

このタスクについて

一部の SIEM は、イベント、アラート、または観測事象とともに MITRE-ATT&CK 情報を提供します。MITRE-ATT&CK 情報を詳細なレベルで関連付けるには、情報を観測事象に追加します。

観測事象からセキュリティインシデントに MITRE-ATT&CK 情報を自動的にロールアップするように選択できます。観測事象をセキュリティインシデントに自動的にロールアップするには、システムプロパティを有効にします。または、観測事象ごとに情報を手動でロールアップすることもできます。

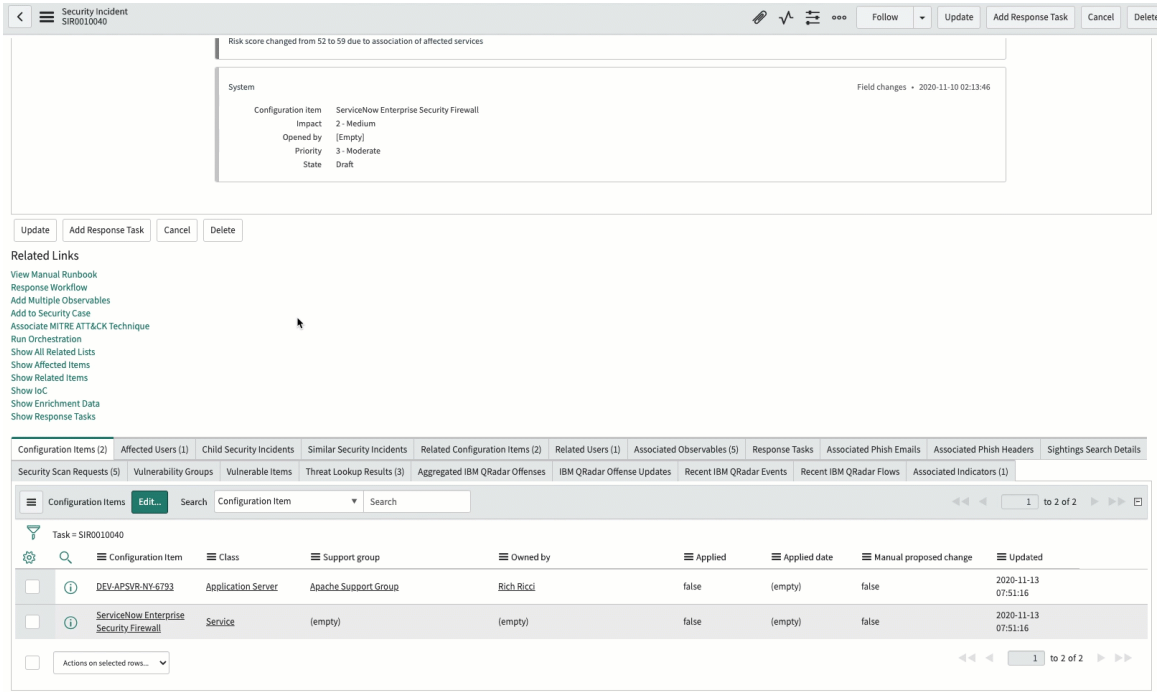
手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. MITRE-ATT&CK 情報で拡張するセキュリティインシデントを選択します。
3. [すべての関連リストを表示] と [関連する観測事象 **(Associated Observables)]** タブをクリックします。
4. 関連付ける観測事象をポイントし、右クリックして、**[MITRE ATT&CK** テクニックの関連付け **(Associate MITRE ATT&CK Technique)]** を選択します。

   次の図では、関連リストから **[MITRE ATT&CK** テクニックの関連付け **(Associate MITRE ATT&CK Technique)]** に移動して、ソースを確認し、戦術とテクニックを追加する方法を示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. ソースリストで、[ソース] を確認します。

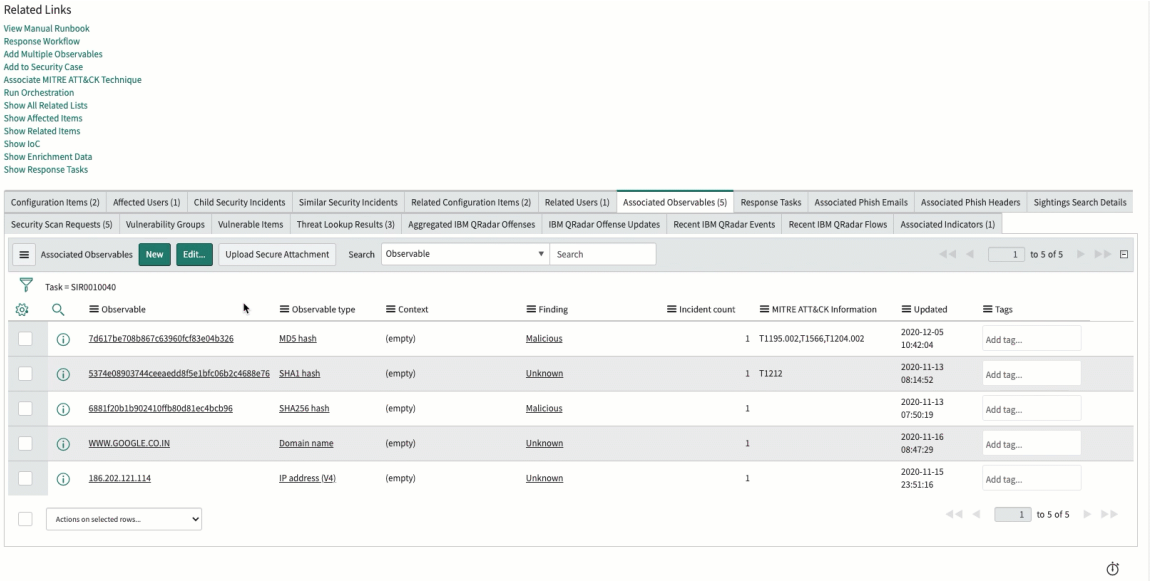
   注:
   アクティブ化されたコレクションとマトリクスのみがソースリストに表示されます。

6. [戦術] と [テクニック] を確認し、観測事象との関連性に基づいて追加または削除します。
7. [保存] をクリックします。
   追加した戦術とテクニックは、[観測事象] 関連リストの MITRE-ATT&CK 情報列に表示されます。
8. 観測事象を選択し、[アクション] メニューから **[MITRE ATT&CK** 情報を **SI** にロールアップ] をクリックします。
   有効にしている場合 の自動ロールアップ MITRE-ATT&CK 観測事象からセキュリティインシデントへの情報の場合、情報は自動的にロールアップされます。自動ロールアップを有効にしていない場合は、手動で行う必要があります。

   次の図は、観測事象を選択して MITRE-ATT&CK 情報をセキュリティインシデントにロールアップする方法を示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



9. 観測事象に関連付けられているテクニックの集計ビューを表示するには、リストから 2 つ以上の観測事象を選択し、選択した行リストの [アクション] メニューから **[MITRE ATT&CK** 情報] をクリックします。

タスクの結果
選択した観測事象の MITRE ATT&CK 情報の集計ビューが表示されます。

MITRE-ATT&CK 情報をセキュリティケースに関連付ける

MITRE-ATT&CK の戦術とテクニックをセキュリティケースに関連付け、セキュリティケース管理と脅威分析をより細いレベルで行うことができます。

始める前に
必要なロール：sn_si.analyst

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > ケースの管理 > すべてのケース.
2. MITRE-ATT&CK 情報で拡張するセキュリティケースを選択します。
3. 関連リストから、**[MITRE ATT&CK** テクニックの関連付け **(Associate MITRE ATT&CK Technique)]** をクリックします。

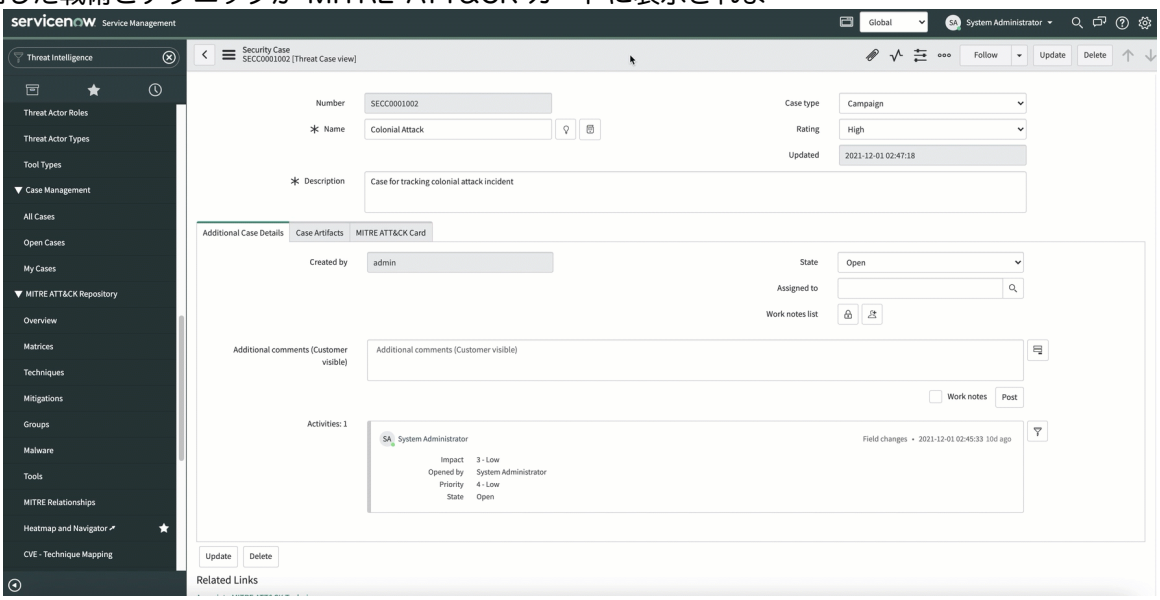
   次の図では、関連リストから **[MITRE ATT&CK** テクニックの関連付け **(Associate MITRE ATT&CK Technique)]** に移動し、ソースを確認して、戦術とテクニックを追加する方法を示しています。

4. ソースリストで、[ソース] を確認します。
5. [戦術] および [テクニック] を確認して、ケースとの関連性を基に追加や削除を行います。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [保存] をクリックします。
   追加した戦術とテクニックが MITRE-ATT&CK カードに表示されま



す。

脅威のルックアップの結果を使用して **MITRE-ATT&CK** 情報をロールアップする

MITRE-ATT&CK 情報の自動ロールアップを有効にしていない場合、手動で行うことができます。

始める前に

必要なロール：sn_si.analyst

このタスクについて

有効にしている場合 の自動ロールアップ MITRE-ATT&CK 脅威のルックアップの結果からの情報 セキュリティインシデントに移動すると、情報が自動的にロールアップされます。自動ロールアップを有効にしていない場合、手動で行うことができます。

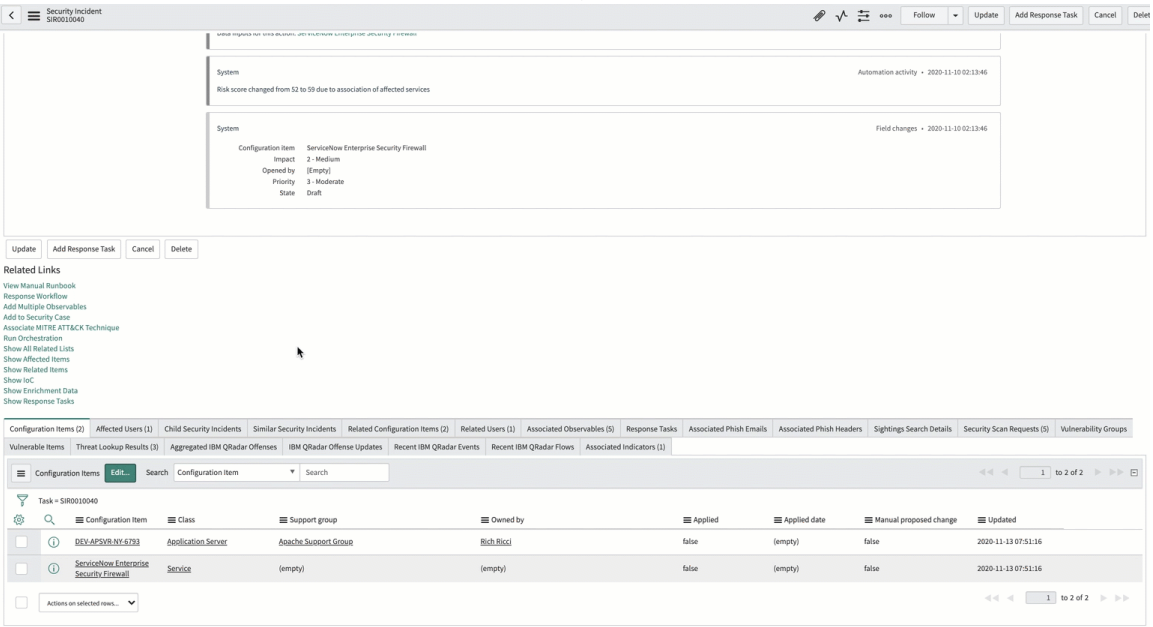
手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. MITRE-ATT&CK 情報で拡張するセキュリティインシデントを選択します。
3. [すべての関連リストを表示] および [脅威のルックアップ結果] タブをクリックします。
4. 観測事象を選択し、[アクション] メニューから **[MITRE ATT&CK** 情報を **SI** にロールアップ] をクリックします。
   複数の観測事象を選択して、情報をロールアップできます。
5. [リロード] をクリックして変更を確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の例では、観測事象の選択方法、および驚異のルックアップ結果のセキュリティインシデントへのロールアップ方法を示しています。



す。
MITRE-ATT&CK カードを表示して、脅威のルックアップ結果がセキュリティインシデントにロールアップされていることを確認できます。

検出ルールからの **MITRE-ATT&CK** 情報をロールアップする

検出ルールからセキュリティインシデントへの MITRE-ATT&CK 情報のロールアップを可能にして、セキュリティインシデントと脅威の分析を強化します。

始める前に
必要なロール：なし。

次を実行していることを確認してください。

- [プロパティ] モジュールの [アラートルールからセキュリティインシデントに MITER ATT&CK 情報を自動的にロールアップ] プロパティを有効にします。デフォルトでは、このオプションは無効になっています。詳細については、「Review the MITRE-ATT&CK system properties (MITRE-ATT&CK システムのプロパティを確認する)」を参照してください。
- [検出ルール - MITRE ATT&CK TTP マッピング] モジュールで、検出ルールの MITRE-ATT&CK TTP へのマッピングを実行します。検出ルール名は、セキュリティインシデントをトリガーするアラートルール名と一致する必要があります。詳細については、「検出ルールの作成とマッピング」を参照してください。

このタスクについて
ベースシステムの SIEM 自動抽出ルールを使用しない場合は、検出ルールマッピングに基づいて MITRE-ATT&CK TTP の自動ロールアップを有効にします。セキュリティインシデントをトリガーするアラートまたはイベントルールを [アラートルール] の名前フィールドに入力できます。また、SIEM 統合、メールの解析、手動での作成などを利用して、[アラートルール] の名前フィールドに入力することができます。

手順

1. 次のように移動する。 **MITRE ATT&CK** 管理 > プロパティ.
2. [アラートルールからセキュリティインシデントに MITER ATT&CK 情報を自動的にロールアップ (Rollup MITRE ATT&ACK information automatically from alert rules to security incidents)] プロパティを有効にし、[保存] をクリックします。

自動翻訳

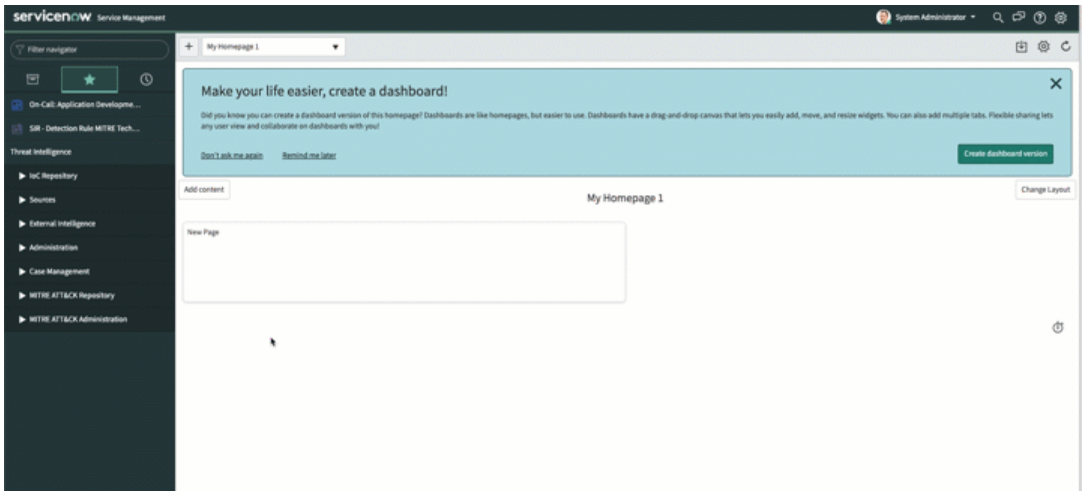
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

デフォルトでは、このオプションは無効になっています。

3. セキュリティインシデントの [アラートルール] の名前フィールドに、必要なアラートルールを入力する必要があります。

   注:
   正確な [アラートルール] の名前を追加していることを確認してください。複数のルールを追加するには、カンマ区切り文字を使用してルールを追加する必要があります。

4. フォームを右クリックし、[保存] をクリックします。
   セキュリティインシデントのアラートルール名の値が [検出ルール - MITRE ATT&CK TTP マッピング] モジュールのレコードと一致する場合、アラートルールに関連付けられた対応するテクニックと戦術が自動的にセキュリティインシデントにリンクされます。



5. セキュリティインシデントを開き、**[MITRE ATT&CK** カード] を選択して、テクニックがロールアップされているかどうかを検証します。
6. [テクニックの由来を表示 **(Show origin of techniques)]** オプションを有効にして、テクニックの由来を表示します。
   テクニックの由来は、検出ルールである必要があります。

子セキュリティインシデントから **MITRE-ATT&CK** 情報をロールアップする

MITRE-ATT&CK 情報の自動ロールアップを有効にしていない場合、手動で行うことができます。

始める前に

必要なロール：sn_si.analyst

このタスクについて

有効にしている場合 の自動ロールアップ MITRE-ATT&CK 子セキュリティインシデントからの情報の場合、情報は自動的にロールアップされます。自動ロールアップを有効にしていない場合、手動で行うことができます。

手順

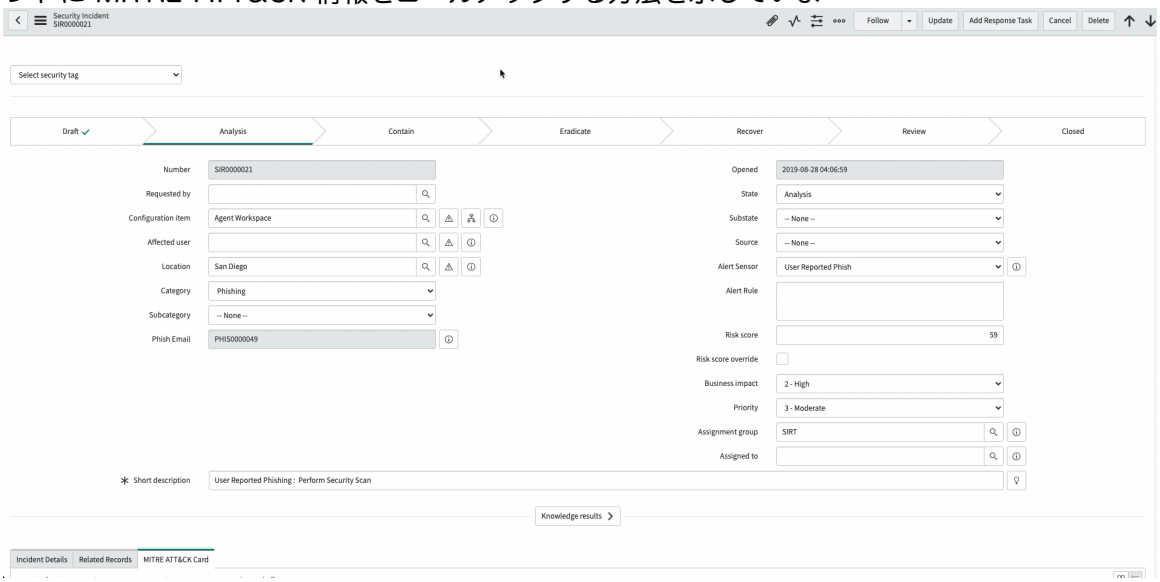
1. 次のように移動する。 **All** (すべて) > インシデント > すべてのインシデントを表示.
2. 子 MITRE-ATT&CK 情報を拡張する増やす親セキュリティインシデントを選択します。
3. [すべての関連リストを表示] および [子セキュリティインシデント] タブをクリックします。
4. 子セキュリティインシデントを選択し、[アクション] メニューから **[MITRE ATT&CK** 情報を **SI** にロールアップ] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[MITRE ATT&CK 情報] をクリックすると、MITRE ATT&CK 情報をロールアップする前に、子セキュリティインシデントの MITRE 情報を表示できます。

5. [リロード] をクリックして変更を確認します。
6. **[MITRE ATT&CK カード]** をクリックして、テクニックの由来を表示します。
   次の図は、子セキュリティインシデントを選択して、親セキュリティインシデントに MITRE-ATT&CK 情報をロールアップする方法を示しています。



MITRE-ATT&CK カードを表示して、子セキュリティインシデントの MITRE-ATT&CK 情報が親セキュリティインシデントにロールアップされていることを確認できます。

MITRE-ATT&CK 固有のフィルターを使用したリンク分析と脅威ハンティング

組織が脅威ハンティングを開始できるように、観測事象、セキュリティインシデント、および MITRE-ATT&CK 関連情報を関連付けてリンク分析を実行します。

始める前に

必要なロール：sn_ti.mitre_analyst、sn_si.read

このタスクについて

セキュリティインシデントを MITRE-ATT&CK 情報に関連付けると、MITRE-ATT&CK 固有のフィルターを脅威ハンティングに使用できます。MITRE-ATT&CK フィルターを既存の セキュリティインシデントレスポンス フィルターとともに使用して、リンク分析を関連付けます。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. [カスタマイズリストの更新] をクリックして、MITRE 列を追加します。
3. MITRE 関連情報とセキュリティインシデントまたは観測事象との関連付けを表示できるように、フィルター条件を選択します。
   - MITRE-ATT&CK 攻撃者グループ
   - MITRE-ATT&CK データソース
   - MITRE-ATT&CK 手順 (マルウェア)
   - MITRE-ATT&CK 手順 (ツール)
   - MITRE-ATT&CK 戦術
   - MITRE-ATT&CK テクニック

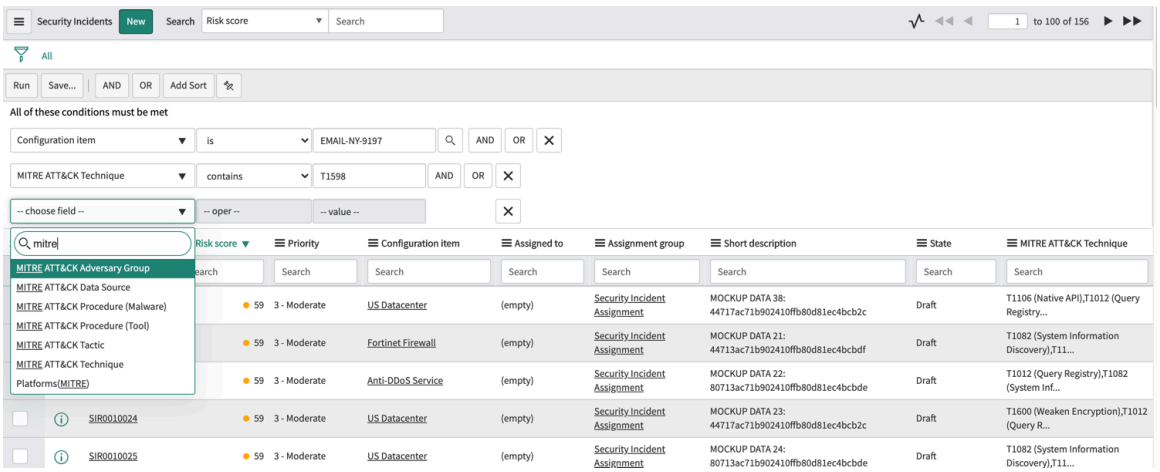
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. 上記の基準に基づいてフィルター条件を作成し、[実行] をクリックして、セキュリティインシデント、観測事象、および MITRE-ATT&CK 関連情報間のリンク分析または相関を実行します。

   注:
   MITRE-ATT&CK データは文字列として格納され、フィルター条件の演算子としては [含む] のみを使用できます。

   たとえば、構成アイテム (CI) が侵害されていることを確認する場合は、CI を選択します。次に、MITRE-ATT&CK テクニック ID を追加して、CI を存在するテクニックと関連付けます。その後、フィルター基準のビルドを続行して、情報を関連付け、脅威ハンティングを行うことができます。



MITRE-ATT&CK のヒートマップとナビゲーター

MITRE-ATT&CK のヒートマップとナビゲーターを使用して、基本的なナビゲーションを行い、全体的なテクニックディスカバリー範囲をビジュアル化できます。

MITRE-ATT&CK のヒートマップとナビゲーターの概要

ナビゲーターとプライマリフィルターを使用して、ATT&CK マトリクスの基本的なナビゲーションと観測を行うことができます。ヒートマップは、組織の対象範囲の死角を含むディスカバリー範囲のスペクトラムをハイライト表示します。これは、テクニックディスカバリー範囲をマッピングした後に使用できます。

ヒートマップとナビゲーターでは、次のことができます。

- 組織の検出機能を迅速かつ効率的に特定し、テクニックディスカバリー範囲のギャップをハイライト表示します。
- 関連機能を使用して脅威をハンティングし、脅威の相関付けを実行します。

MITRE-ATT&CK のヒートマップとナビゲーターにアクセスする

MITRE-ATT&CK のヒートマップとナビゲーターにアクセスして、ATT&CK を利用できるマトリクスをビジュアル化できます。

始める前に
必要なロール：sn_ti.read、sn_ti.mitre_analyst

このタスクについて
ヒートマップを確認し、フィルターを使用して相関をとり、MITRE-ATT&CK 情報、観測事象、および組織内のセキュリティインシデントのリンク分析を実行できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** リポジトリ > ヒートマップとナビゲーター.
   ヒートマップとナビゲーターが新しいタブで開きます。
2. ヒートマップに入力するソースを選択します。

   注:
   アクティブ化されたコレクションとマトリクスのみがソースリストに表示されます。

   次の図は、ヒートマップとナビゲーターに移動する方法、およびソース (この例ではエンタープライズ ATT&CK) を選択する方法を示しています。

   ヒートマップに入力するソースに移動して選択する
3. 検索ボックスを使用すると、名前または ID を使用することで、特定の戦術やテクニックをすばやく見つけることができます。

   次の図は、戦術、テクニック、またはそれらに含まれている情報を検索する方法を示しています。検索を使用して、特定の戦術またはテクニックにすばやくドリルダウンします。
4. [フィルター] をクリックし、[プライマリ] または [詳細 (Advanced)] フィルターからフィルターを選択します。
5. [適用] をクリックし、次のようにフィルターをコントロールします。
   - フィルターを保存するには、カスタムビューを作成します。3 つのカスタムビューを作成して保存できます。
   - 選択したフィルターを削除するには、[デフォルトフィルターを復元] をクリックしてデフォルトの保存されたビューをロードします。
   - すべてのフィルターと既存のビューをクリアするには、[すべてのフィルターをクリア] をクリックします。

   注:
   保存するビューはユーザーに固有のものです。
6. [サブテクニックを非表示 **(Hide Sub-Techniques)**] をクリックして、ヒートマップビューからすべてのサブテクニックを削除します。
   テクニックにサブテクニックがある場合は、展開アイコンをクリックしてサブテクニックを表示できます。

カスタムビューの使用

MITRE-ATT&CK のヒートマップとナビゲーターのカスタムビューを使用すると、お気に入りのフィルターを保存して、次回ヒートマップにアクセスしたときに表示できます。

注:
各ユーザーの MITRE-ATT&CK コレクションごとに 3 つのカスタムビューを作成して保存できます。

ビューの作成

[プライマリ] フィルターまたは [詳細] フィルターから必要なフィルターを選択したら、[フィルター] ヘッダーの省略記号 (...) ボタンをクリックし、[新規ビューを作成] を選択します。カスタムビュー名を入力し、[ビューを保存] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

デフォルトビュー

[デフォルトビューとして保存] をクリックすると、次にヒートマップにアクセスしたときにビューが直接ロードされます。各コレクションのデフォルトビューを設定できます。

> **注:**
> 脅威インテリジェンス プラグインを古いバージョンからアップグレードすると、古いバージョンの既存のデフォルトビューがカスタムビューとして表示されます。

ヒートマップにカスタムビューを作成する方法を示す図

ビューの更新

必要な [プライマリ] フィルターまたは [詳細] フィルターを変更することで、既存のカスタムビューを更新できます。カスタムビューを選択し、必要に応じてフィルターを更新して、[フィルター] ヘッダーの省略記号 (...) ボタンをクリックし、[ビューの更新] を選択してフィルターを保存します。

カスタムビューを更新する方法を示す図。

カスタムビューの管理

各カスタムビューの横にあるチェックボックスを使用して、選択したカスタムビューフィルターを適用します。

各カスタムビュー名の横にある省略記号 (...) ボタンをクリックして、カスタムビューを次のように制御します。

- デフォルトビューを設定します。
- デフォルトビューとしてのカスタムビューを削除します。カスタムビューは削除されません。
- カスタムビューの名前を変更します。
- カスタムビューを削除します。

カスタムビューを管理する方法を示す図。

保存されたビューのエクスポート

保存されたカスタムビューを JSON ファイルにエクスポートするには、[フィルター] ヘッダーの省略記号 (…) をクリックし、[保存されたビューのエクスポート **(Export saved views)]** を選択します。ローカルコンピューターにダウンロードするカスタムビューのダウンロードアイコンをクリックします。

カスタムビューをエクスポートする方法を示す図。

ビューのインポート

JSON ファイルのみをインポートできます。カスタムビューをインポートするには、[フィルター] ヘッダーの省略記号 (…) ボタンをクリックし、[ビューのインポート **(json)]** を選択します。

ビューをインポートする場合は、次の条件を確認してください。

- インポートできるのは JSON ファイル形式のみです。
- 一度にインポートできるビューまたはファイルは 1 つのみです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- フィルターに既に 3 つのカスタムビューがある場合は、インポートできません。カスタムビューを削除し、ビューをインポートします。
- 既存のカスタムビュー名のビューをインポートすることはできません。インポートする前にビューの名前を変更します。

ビューをエクスポートする方法を示す図。

プライマリフィルターを使用したナビゲーター

プライマリフィルターを使用して、MITRE-ATT&CK ナビゲーターでテクニックをフィルタリングします。MITRE-ATT&CK リポジトリ内の情報を選択できます。

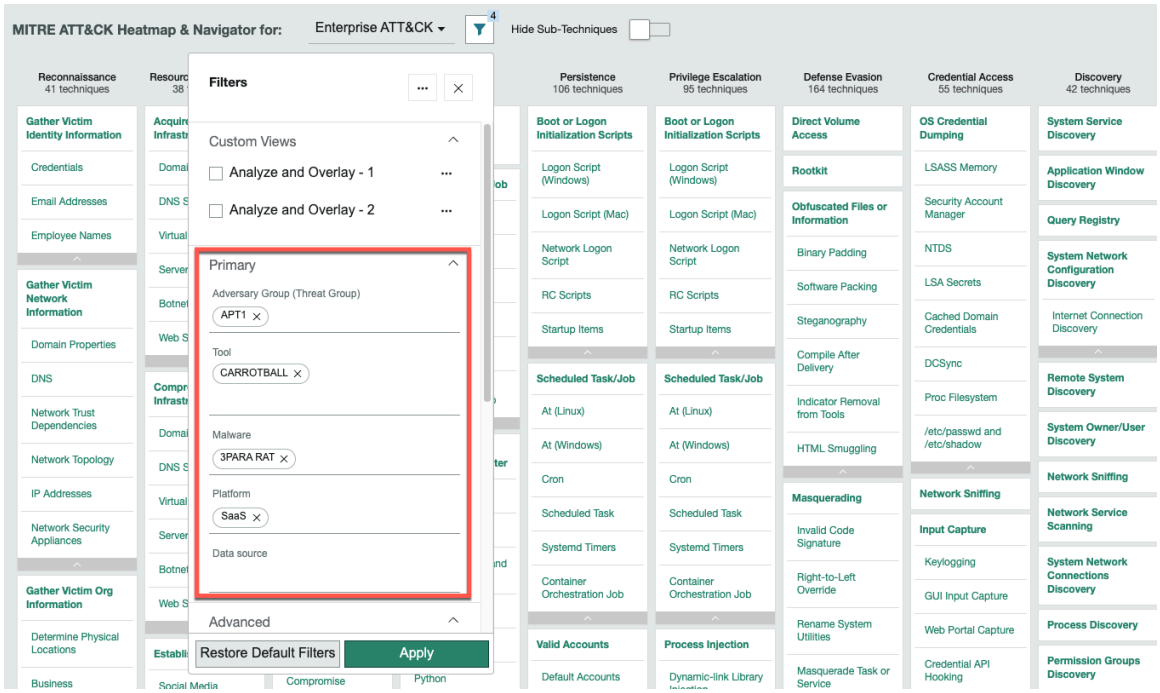
フィルター	説明
攻撃者グループ (脅威グループ)	セキュリティコミュニティで共通の名前で追跡される、関連する侵入アクティビティのセット。グループは、さまざまな脅威グループ、アクティビティグループ、攻撃者、侵入セット、およびキャンペーンを意味します。[攻撃者グループ (脅威グループ)] フィルターに複数のグループを追加できます。 たとえば、APT1 と AT12 はどちらも中国に起因する脅威グループであるため追加するとします。両方のグループが異なるソースを標的にする可能性がありますが、同様のテクニックを使用できます。
ツール	攻撃者が攻撃を実行するために使用する正当なソフトウェア。攻撃者がどのようにどのツールを使用しているかを把握できれば、攻撃者がどのようにキャンペーンを実行するかを理解できます。ツールには、エンタープライズシステムに存在しないソフトウェアと、Microsoft Windows ユーティリティなど、環境に既に存在するオペレーティングシステムの一部として利用可能なソフトウェアの両方が含まれています。 たとえば、gsecdump は、APTI1 攻撃者グループが Microsoft Windows オペレーティングシステムからパスワードハッシュと LSA シークレット (ローカルセキュリティ機関) を取得するために使用する、公開されている認証情報ダンパーです。
マルウェア	攻撃者が悪意のある目的で使用することを意図した、商用、カスタムのクローズソース、またはオープンソースのソフトウェア。 例としては、PlugX、CHOPStick などがあります。
プラットフォーム	特定のプラットフォームで MITRE-ATT&CK を表す戦術とテクニック。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィルター	説明
	たとえば、MITRE-ATT&CK は Enterprise ATT&CK マトリクスのプラットフォーム (Microsoft Windows、macOS、Linux、PRE、AWS、GCP、Azure、Azur AD、Office 365、SaaS、Network) をサポートしています。
データソース	環境内で収集し、MITRE-ATT&CK テクニックを検出するために使用するデータソース。 例として、DLL モニタリング、ブラウザー拡張があります。

次の図は、MITRE-ATT&CK ナビゲーターで利用可能なすべてのプライマリフィルターを示しています。



プライマリ機能と高度な機能を備えたヒートマップの使用

詳細フィルターを備えたヒートマップを使用して、セキュリティインシデントを MITRE-ATT&CK 情報と関連付けることができます。

テクニック **ID** の表示

[テクニック **ID** を表示] フィルターを選択すると、テクニック名と MITRE-ATT&CK テクニック ID を表示できます。

ヒートマップでテクニック ID を表示

関連するテクニックを優先度別に表示

関連する優先度に基づいて、ナビゲーターでテクニックをフィルタリングするには、[テクニックの関連性の優先度でフィルター] を選択し、メニューから[関連する優先度] を選択します。フィルタリングに複数の優先度を割り当てることができます。ヒートマップのテクニックをポイントして、テクニックの優先度を確認することもできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連する優先度情報は、[テクニック] の [関連する優先度] フィールドで設定した優先度に基づいています。

この図は、関連する優先度によるフィルタリングを示しています。

テクニックディスカバリー範囲の表示

ヒートマップで全体的なテクニックディスカバリー範囲を表示するには、[テクニックディスカバリー範囲を表示] フィルターを選択します。ヒートマップは、対象範囲の死角を含むディスカバリー範囲の視覚的スペクトラムをハイライト表示します。ベースシステムのスコアリング定義と色は、[テクニックディスカバリー範囲]で定義されています。情報は、全体的なテクニックディスカバリー範囲から自動抽出されます。

たとえば、赤でマークされたヒートマップの領域は、検出がないことを示します。青色でマークされた領域は、完全な検出機能が存在することを示します。オレンジ、黄色、およびライトブルーでマークされた領域は、部分的な検出機能を反映しています。

- 色の可視化は、定義したテクニック定義と色分けに基づいています。
- 対象範囲の可視化は、定義したテクニックディスカバリー範囲のマッピングに基づいています。
- ベースシステムの対象範囲の定義を変更すると、テクニックとともに対象範囲タイプのアイコンがヒートマップに表示されなくなります。

> **注:**
> ベースシステムの定義されたテクニックディスカバリー範囲および対象範囲の色と同じフィールドを変更すると、ヒートマップは正常に機能します。

この図では、すべてのテクニックとサブテクニックのテクニックディスカバリー範囲とその対象範囲タイプが色とアイコンで示されています。

ヒートマップのテクニックディスカバリー範囲

テクニック緩和対象範囲の表示

ヒートマップで全体的なテクニック緩和対象範囲を表示するには、[テクニック緩和対象範囲を表示 (Display technique mitigation coverage)] フィルターを選択します。ヒートマップは、対象範囲のない領域を含む、緩和対象範囲の視覚的スペクトラムをハイライト表示します。緩和対象範囲、色、およびパーセンテージ範囲は、[緩和対象範囲の定義] で定義されています。情報は、[全体的なテクニック緩和対象範囲] から抽出されます。

たとえば、赤でハイライト表示されたテクニックは緩和対象範囲がないことを示し、オレンジ色は緩和対象範囲が狭いことを示し、青は緩和対象範囲が広いことを示します。

- 色の可視化は、定義したテクニック緩和定義と色分けに基づいています。
- 対象範囲の可視化は、定義したテクニック緩和対象範囲のマッピングに基づいています。
- ベースシステムの緩和対象範囲の定義を変更すると、テクニックとともに緩和対象範囲タイプのアイコンがヒートマップに表示されなくなります。

> **注:**
> ベースシステムの定義されたテクニック緩和対象範囲および対象範囲の色と同じフィールドを変更すると、ヒートマップは正常に機能します。

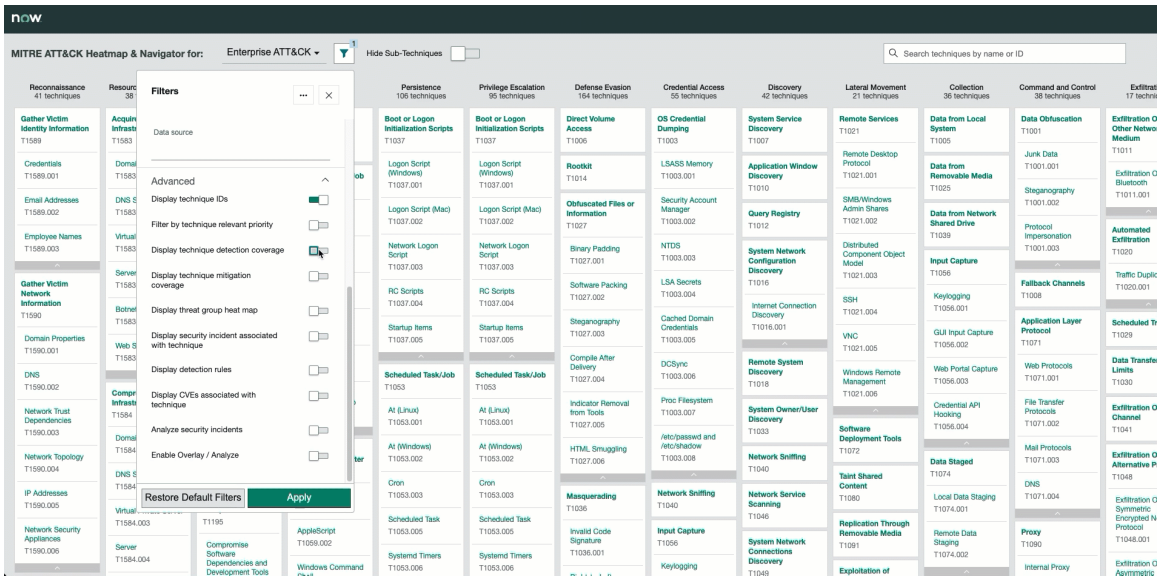
テクニック緩和対象範囲のヒートマップを示す図

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

検出と緩和対象範囲の表示

テクニック検出とテクニック緩和対象範囲フィルターを一緒に使用して、組織のテクニック検出と緩和対象範囲を把握できます。



この図は、検出と緩和フィルターを一緒に使用する方法を示しています。

脅威グループの表示

ヒートマップのテクニック情報に脅威グループを表示するには、[脅威グループヒートマップを表示 **(Display threat group heat map)]** を選択します。特定のテクニックを使用している脅威グループの数を測定できます。多数の攻撃者がいる場合、特定のテクニックを使用する攻撃の可能性が高くなります。脅威グループ範囲とヒートマップの色は、[脅威グループテクニックヒートマップ定義] で定義されています。

- ヒートマップとテキストの色の可視化は、[脅威グループ - テクニックヒートマップ定義] に基づいています。
- 脅威グループの範囲の可視化は、脅威グループからテクニックへのマッピングに基づいています。
- テクニックディスカバリー範囲またはテクニック緩和対象範囲が有効になっている場合は、[脅威グループヒートマップを表示 **(Display threat group heat map)]** フィルターを使用できません。ヒートマップ上の脅威グループ情報を示す図

テクニックに関連するセキュリティインシデントの表示

組織で頻繁に悪用され、セキュリティインシデントを引き起こしたテクニックを表示するには、[テクニックに関連するセキュリティインシデントを表示] をクリックします。リンクをクリックすると、分析のために新しいウィンドウで開き、関連する各セキュリティインシデントに関する詳細情報を表示できます。 テクニックに関連するセキュリティインシデント

- 優先度：[セキュリティインシデント優先度] を選択して、セキュリティインシデントの優先度でフィルタリングします。
- 日付範囲：[セキュリティインシデントの日付範囲] を選択して、日付範囲でセキュリティ問題をフィルタリングします。
- 誤検出：[誤検出セキュリティインシデントをフィルター] を選択して、誤検出の問題を削除します。このフィルターを選択すると、ヒートマップに表示されるセキュリティインシデントの数が減少します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このフィルターと [テクニックディスカバリー範囲を表示] フィルターを使用すると、選択した日付までの組織のテクニックディスカバリー範囲の関連性を把握できます。

たとえば、両方のフィルターをオンにすると、防御回避戦術では成り済ましテクニックが範囲の対象外になることがわかります。さらに詳しく調べると、成り済ましテクニックは成り済ましタスクまたはサービスに関連しており、それに関連付けられているセキュリティインシデントもあります。これは、成り済ましテクニックではテクニックディスカバリー範囲にギャップがあり、全体的なテクニックディスカバリー範囲を変更する必要があることを示しています。

検出ルールの表示

特定のテクニックに検出ルールが定義されているかどうかを表示するには、[検出ルールを表示] をクリックします。関連する各検出ルールとその定義を表示することもできます。

この情報は、定義した検出ルールのマッピングに基づいています。 関連する検出ルールの表示

テクニックに関連する **CVE** の表示

各テクニックに関連付けられている共通脆弱性識別子 (CVE) 情報を表示するには、[テクニックに関連する **CVE** を表示] をクリックします。CVE とテクニックの情報は、CVE - テクニックマッピングモジュールで提供される情報に基づいています。これにより、既知の脆弱性を把握できるようになり、攻撃者が組織の脆弱性を悪用できるかどうかの可能性を確認できます。

重要:
ヒートマップが拡張され、VIT に関連付けられている関連 CVE のみが表示されます。

CVE とテクニックに関連付けられた VIT を表示するには、**[CVE** とテクニックに関連付けられた **VIT** を表示 **(Display VITs associated with CVE and techniques)]** を選択します。さらに、VIT なしでテクニックをさらにフィルタリングするには、**[VIT** なしで テクニックを非表示 **(Hide techniques without VITs)]** を選択します。表示する CVE および VIT 情報は、お使いの環境の 脆弱性対応 製品から取得されます。ヒートマップに CVE および VIT のフィルター済みリストを表示し、ヒートマップからすべてのテクニックの各 CVE または VIT に移動できます。

注:

- [テクニックに関連する **CVE** を表示] は、脆弱性対応 製品が環境にインストールされている場合にのみ使用できます。
- VIT および CVE 情報は、 MITRE-ATT&CK プロパティ. ベースシステムのスケジュール済みジョブは 24 時間に設定されています。

このフィルターと [テクニックに関連するセキュリティインシデントを表示] フィルターを使用すると、既知の脆弱性が組織内でセキュリティインシデントを引き起こしたかどうかを確認できます。

各 CVE に関する詳細情報を表示して、CVE が組織に関連するかどうかを分析できます。これを行うには、脆弱性一致アイテムを表示します。脆弱性一致アイテムが作成されると、脆弱性対応 モジュール内の関連する CI 情報に関する詳細情報を表示できます。重大度と優先度を確認して、情報に基づいた意思決定を行うこともできます。 CVE を確認して情報に基づいた意思決定を行う

セキュリティインシデントの分析

セキュリティインシデントを分析し、攻撃者が使用したテクニックを確認するには、[セキュリティインシデントを分析] をクリックします。カンマ区切りの文字列を使用して、複数のセキュリティインシデントを追加して分析できます。

このフィルターは、セキュリティインシデントの分析に役立ちます。インシデントが発生した理由、悪用されたテクニック、既知の攻撃者が関与していたかどうか、攻撃者が特定のシーケンスを攻撃に使用したかどうかなどを確認できます。複数のセキュリティインシデントを同時に分析できるため、

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

情報を関連付けて、それらが関連するかどうか、または独立したインシデントであるかどうかを確認できます。セキュリティインシデントが関連しており、パターンが観察された場合、キルチェーンの進捗状況を確認して、攻撃を阻止したり、組織の防御戦略を策定したりすることができます。

[セキュリティインシデントを分析] フィルターとプライマリフィルター (攻撃者グループなど) を使用すると、既知の攻撃者が関与しているかどうかを関連付けることができます。たとえば、複数のセキュリティインシデントが分析されている場合、セキュリティインシデントに関連するテクニックはキルチェーンの形で存在します。攻撃者と情報を重ね合わせると、セキュリティインシデントに関連するテクニックと攻撃者に関連するテクニックが重複していることがわかります。両方のフィルターが有効になっている場合は、重複するテクニック情報のみが表示されます。

セキュリティインシデントの分析

オーバーレイを使用したセキュリティインシデントと攻撃者グループの分析

[オーバーレイ/分析を有効にする **(Enable Overlay/Analyze)]** フィルターを使用すると、攻撃者の動作を表示して、1 つ以上のセキュリティインシデントを分析して情報を関連付け、攻撃が独立したインシデントなのか、既知の攻撃者による連携した攻撃なのかを確認できます。

たとえば、セキュリティインシデントと攻撃者のキルチェーンの動作を同じビューで表示できます。このビューは、攻撃と既知の攻撃者の動作を知らせる重複情報を提供します。これにより、既知の攻撃者による独立した攻撃なのか、それとも連携した攻撃なのかを分析できます。

オーバーレイ分析フィルターを有効にすると、[攻撃者グループ] フィルターを除くすべてのプライマリフィルターが無視され、ビューの生成中に高度なフィルター [テクニックの関連性の優先度でフィルター] が無視されます。

オーバーレイ分析フィルターを有効にしたら、カラーパレットを使用して次の色を割り当てます。

- セキュリティインシデントの分析
- 攻撃者グループ
- オーバーレイ

次の図は、攻撃者グループ APT18 がキルチェーンの複数のテクニックと戦術にわたることを示しています。この分析では、追跡している攻撃者グループとセキュリティインシデントにオーバーレイする 3 つのテクニックがあることも分かります。 この図は、攻撃者とセキュリティインシデントのオーバーレイ情報を示しています。

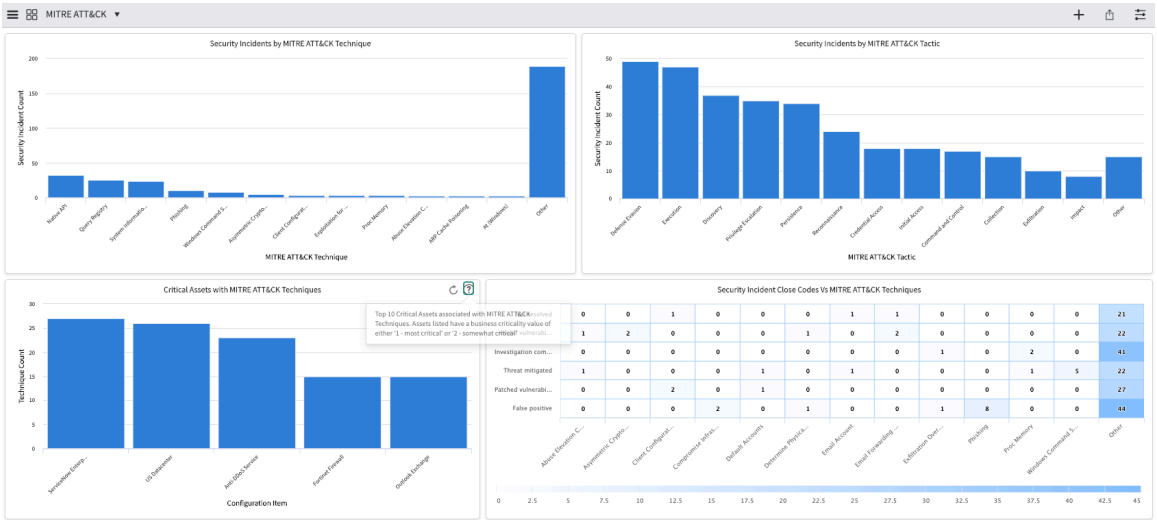
MITRE-ATT&CK ダッシュボードの使用

MITRE-ATT&CK ダッシュボードは、組織で使用されているデータソースの対象範囲、戦術、およびテクニックの概要を提供します。

MITRE-ATT&CK 概要モジュールには、傾向やレポートを含むセキュリティインシデントに関する MITRE-ATT&CK 情報が表示されます。ウィジェットの任意の部分 (棒、データポイント、テーブルなど) をポイントして、その部分に固有の一般的なデータを表示できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



MITRE-ATT&CK ダッシュボードを使用してセキュリティ関連データを確認する

MITRE-ATT&CK ダッシュボードを使用して、組織で使用されているデータソース範囲、戦術、およびテクニックの概要を把握できます。

始める前に

必要なロール：sn_si.ciso、sn_si.analyst、sn_si.manager、sn_ti.read

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > **MITRE ATT&CK** リポジトリ > 概要.
2. 次のウィジェットをクリックして、その他の詳細を表示します。
   - MITRE-ATT&CK テクニックによるセキュリティインシデント
   - MITRE-ATT&CK 戦術によるセキュリティインシデント
   - MITRE-ATT&CK テクニックを用いた重要な資産
   - セキュリティインシデントクローズコードと MITRE-ATT&CK テクニックの比較
   - ディスカバリー範囲別の MITRE ATT&CK テクニック
   - 緩和対象範囲別の MITRE ATT&CK テクニック
   - MITRE ATT&CK テクニックによる脅威グループ
   - MITRE ATT&CK テクニックによる CVE

MITRE-ATT&CK ウィジェット

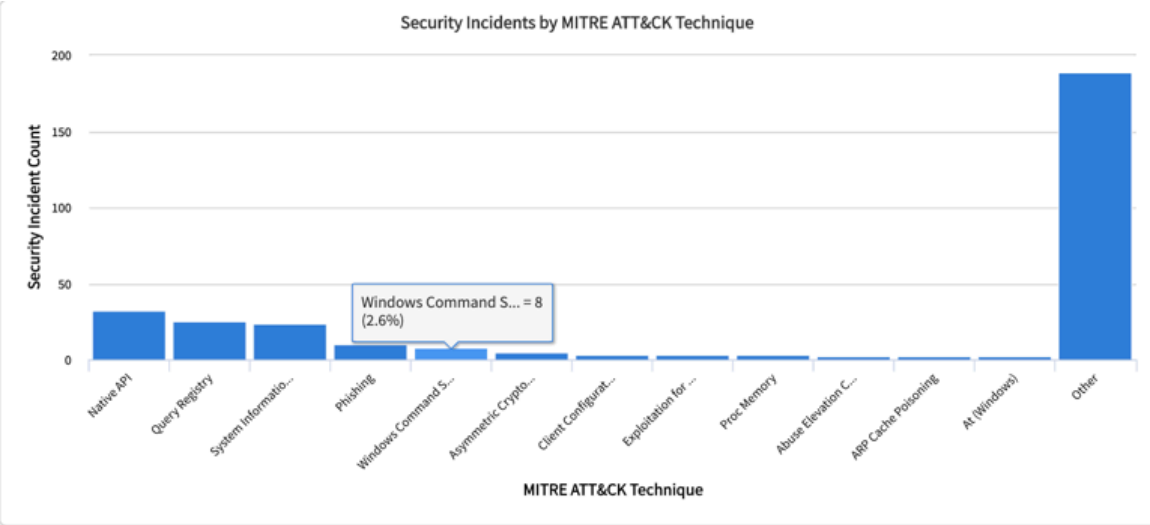
MITRE-ATT&CK 概要モジュールは、MITRE-ATT&CK 情報を環境内のセキュリティインシデント情報と関連付けることができるウィジェットで構成されています。

MITRE-ATT&CK テクニック別のセキュリティインシデントの例

この例では、**[MITRE ATT&CK** テクニック別セキュリティインシデント **(Security Incidents by MITRE ATT&CK Technique)]** ウィジェットに、過去 90 日間の組織環境内のセキュリティインシデント別のテクニックが表示されます。

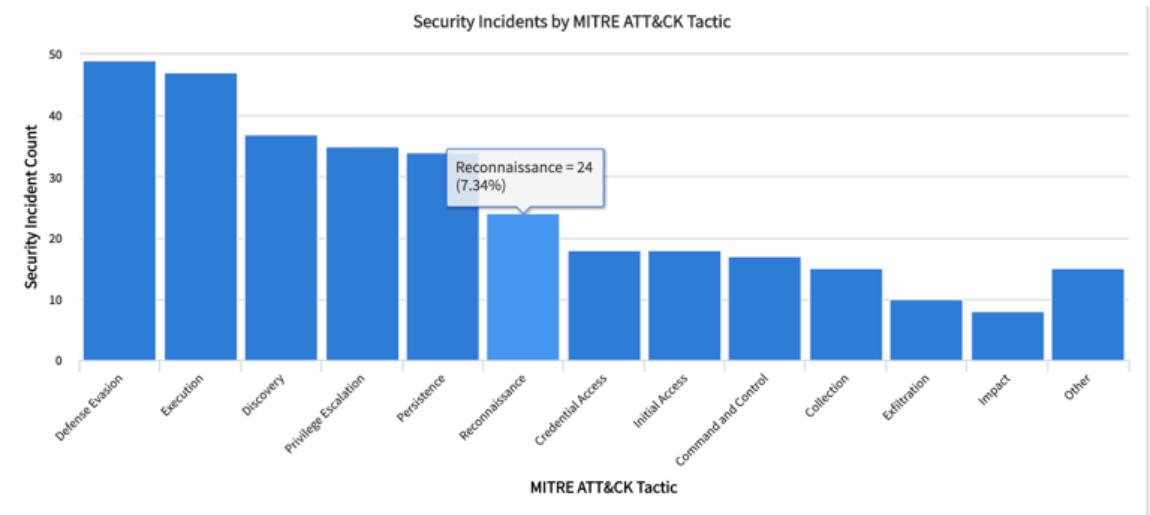
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



MITRE-ATT&CK 戦術別のセキュリティインシデントの例

この例では、**[MITRE ATT&CK 戦術別セキュリティインシデント (Security Incidents by MITRE ATT&CK Tactic)]** ウィジェットに、過去 90 日間の組織環境内のセキュリティインシデント別の上位戦術が表示されます。



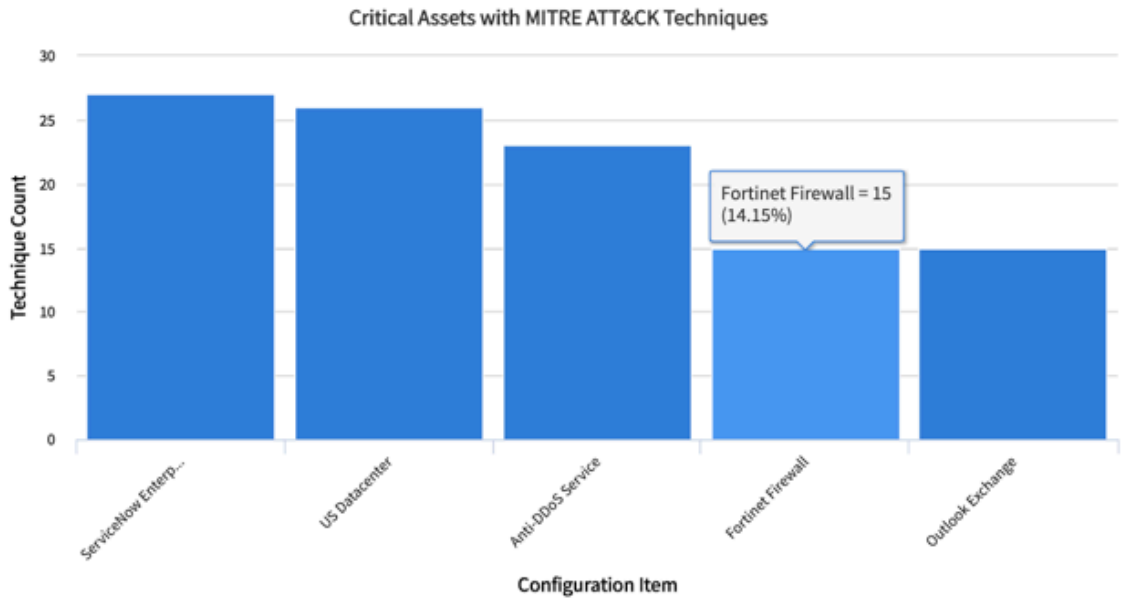
MITRE-ATT&CK テクニックを使用した重要資産の例

この例では、**[MITRE ATT&CK テクニックを使用した重要資産 (Critical Assets with MITRE ATT&CK Techniques)]** ウィジェットに、MITRE-ATT&CK テクニックに関連付けられている上位 10 件の重要な資産が表示されます。資産のビジネス上の重要度は 1 (最重要) または 2 (やや重要) です。

このレポートにより、組織は重要資産に対する攻撃に使用されるテクニックのタイプと数を確認できます。

自動翻訳

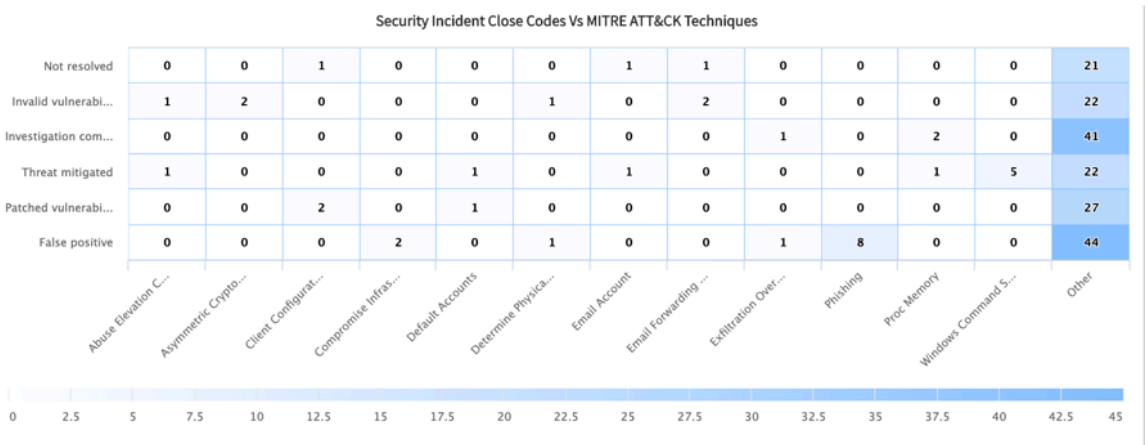
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



セキュリティインシデントクローズコードと **MITRE-ATT&CK** テクニックの例

この例では、[セキュリティインシデントクローズコードと *MITRE-ATT&CK* テクニック **(Security Incident Close Codes Vs Techniques)]** ウィジェットに、組織環境内で特定された上位のテクニックに対してマッピングされたセキュリティインシデントクローズコードが表示されます。

X 軸は、企業に対する攻撃に使用された上位のテクニックを表し、Y 軸はクローズ済みコードを表します。



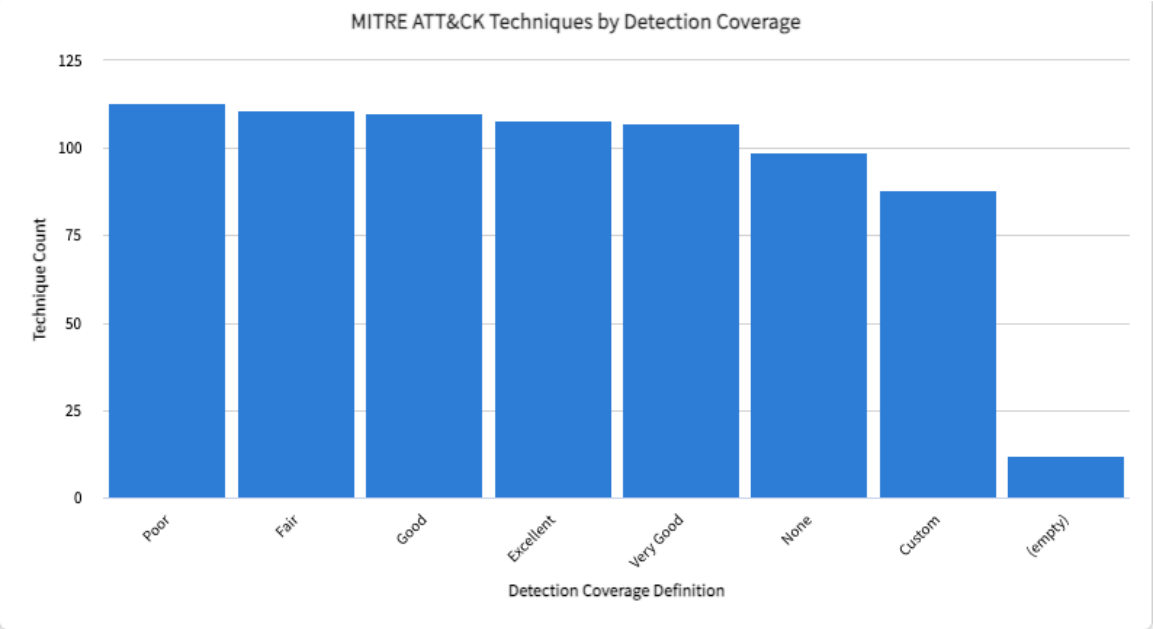
MITRE-ATT&CK テクニック別のディスカバリー範囲の例

この例では、[ディスカバリー範囲別 **MITRE-ATT&CK** テクニック **(MITRE-ATT&CK Techniques by Detection Coverage)]** ウィジェットに、環境内のテクニック数がディスカバリー範囲別に表示されます。

X 軸はテクニック数を表し、Y 軸はディスカバリー範囲タイプを表します。

自動翻訳

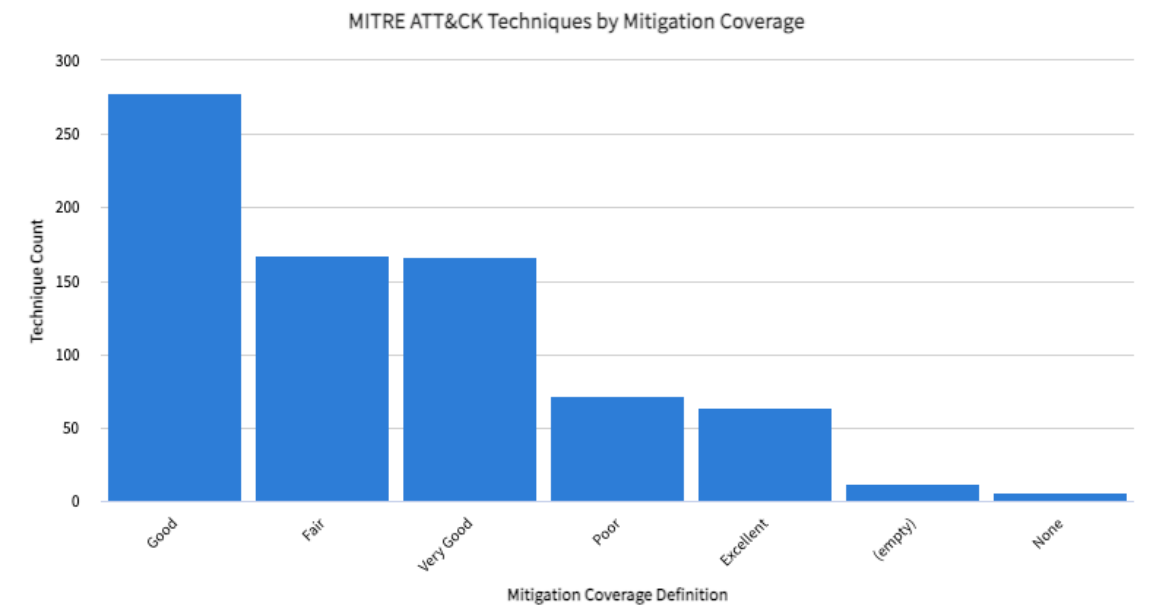
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



MITRE-ATT&CK テクニック別の緩和対象範囲の例

この例では、[緩和対象範囲別 **MITRE-ATT&CK** テクニック **(MITRE-ATT&CK Techniques by Mitigation Coverage)]** ウィジェットに、環境内のテクニック数が緩和対象範囲別に表示されます。

X 軸はテクニック数を表し、Y 軸は緩和対象範囲タイプを表します。



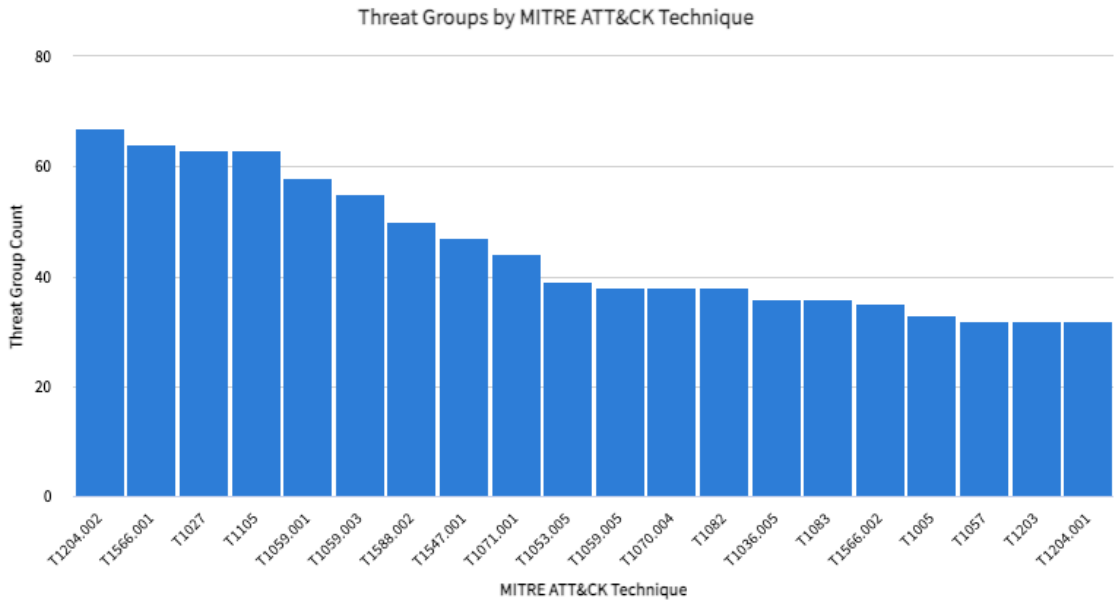
MITRE-ATT&CK テクニック別の脅威グループの例

この例では、**[MITRE-ATT&CK** テクニック別の脅威グループ **(Threat Groups by MITRE-ATT&CK Technique)]** ウィジェットに、テクニックが脅威グループ数別に表示されます。このウィジェットには、脅威グループ数が最も多い 20 のテクニックが表示されます。

X 軸は脅威グループ数を表し、Y 軸は MITRE-ATT&CK テクニックを表します。

自動翻訳

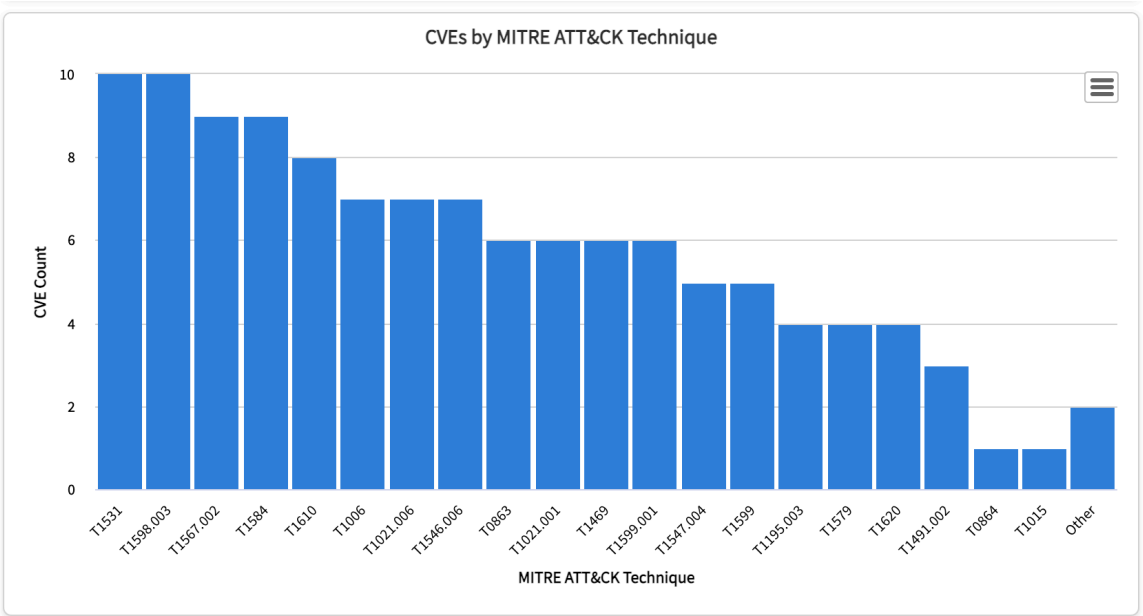
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



MITRE-ATT&CK テクニック別の CVE の例

この例では、**[MITRE-ATT&CK テクニック別 CVE (CVEs by MITRE-ATT&CK Technique)]** ウィジェットに、環境内のテクニックと関連 CVE の数が表示されます。

X 軸は関連の CVE 数を表し、Y 軸は MITRE-ATT&CK テクニックを表します。



脅威インテリジェンス の管理

脅威インテリジェンス ベースシステムは、アクティブ化するとすぐに使用できます。[管理] アプリケーションメニューで特定のモジュールにレコードを追加できますが、ほとんどのモジュールには既に業界標準の情報が入力されています。

脅威インテリジェンス のナビゲーションバーの [管理] モジュールでは、次のアプリケーションを使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威インテリジェンスの管理アプリケーション

アプリケーション	説明
プロパティ	脅威インテリジェンス プロパティを使用すると、API キーの設定など、システム機能のさまざまな側面を制御できます。
攻撃メカニズム	このモジュールでは、脆弱性を悪用するときに頻繁に使用されるメカニズムに基づいて、攻撃パターンを階層的に整理します。
攻撃の動機	このモジュールでは、考えられる攻撃の動機を示します。これらは攻撃者または侵入セットによる攻撃の強度を形成します。
ディスカバリー方法	このモジュールでは、セキュリティインシデントがどのように検出されるかについて説明します。
フィード	この機能は廃止されました。
インジケータータイプ	このモジュールは、特定の観測可能な条件を識別するパターンと、そのパターンの意味、いつどのように影響するかなどのコンテキスト情報で構成されるサイバー脅威インジケーターを特徴付けるのに使用されます。
インフラストラクチャタイプ	このモジュールでは、考えられるインフラストラクチャの分類を一覧表示します。
意図した効果	このアプリケーションは、攻撃者の意図した効果を表すために使用されます。
マルウェア機能	このモジュールでは、マルウェアの考えられる機能を一覧表示します。
マルウェアタイプ	このモジュールでは、考えられるマルウェアの分類を一覧表示します。
通知	このモジュールは メール通知。これには、送信時期、受信者、および内容の指定が必要です。
観測事象タイプ	このモジュールでは、IP アドレスやファイルハッシュなど、考えられる観測事象の分類を一覧表示します。
レポートタイプ	このモジュールでは、考えられる脅威レポートの分類を一覧表示します。
攻撃者ロール	このモジュールでは、攻撃者が果たす役割を一覧表示します。
攻撃者タイプ	このモジュールは、推定される意図や過去に観察された動作など、サイバー攻撃の脅威をもたらす攻撃者を特徴付けます。
脅威のルックアップ検索計算ツール	このモジュールは、受信した応答に基づいて結果を計算します。脅威のルックアップ検索計算ツールでは、計算された結果を提供するサードパーティ統合の場合、システム内のサポートされている検出結果に結果をマッピングします。詳細については、「脅威のルックアップ検索計算ツール」を参照してください。
ツールタイプ	このモジュールでは、考えられるツールの分類を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威のルックアップ検索計算ツール

脅威のルックアップ検索計算ツールを使用すると、受信した応答に基づいて観測事象の検出結果を計算できます。

統合用に脅威のルックアップ検索計算ツールを作成し、スクリプトを使用してさまざまな観測事象の検出結果をどのよう識別するかを決定できます。脅威のルックアップ検索計算ツールには、ベースシステムに付属するサンプルスクリプトが含まれています。これを使用して観測事象の結果を特定したり、要件に従ってこのスクリプトを変更したりできます。

脅威のルックアップ検索計算ツールでは、計算された結果を提供するサードパーティ統合の場合、ベースシステム内のサポートされている検出結果に結果をマッピングします。

脅威のルックアップ結果のロールアップ

さまざまな統合ベンダーから観測事象に対して複数の脅威のルックアップ結果がある場合は、すべてのベンダーからの最新の脅威のルックアップ結果が考慮され、全体的な観測事象結果が次のようにマークされます。

脅威のルックアップ検索結果のロールアップ

最新の観測事象結果	全体的な観測事象結果
悪意がある	統合ベンダーの 1 つが観測事象を「悪意がある」と報告した場合、全体的な観測事象結果は [悪意がある] とマークされます。
不審	観測事象を「悪意がある」と報告した統合ベンダーはいないが、統合ベンダーの 1 つが「不審」と報告した場合、全体的な観測事象結果は [不審] とマークされます。
クリーン	すべての統合ベンダーが観測事象を「クリーン」と報告した場合、全体的な観測事象結果は [クリーン] とマークされます。
不明	観測事象を「悪意がある」と報告した統合ベンダーはいないが、統合ベンダーの 1 つが「不明」と報告した場合、全体的な観測事象結果は [不明] とマークされます。

脅威のルックアップ検索計算ツールの使用

脅威のルックアップ検索計算ツールを使用して、統合の観測事象結果を計算します。

始める前に

必要なロール：sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > アドミニストレーション > 脅威情報ルックアップ検索計算ツール.
2. [**New**] をクリックします。
3. フォームの各フィールドに入力します。
4. [更新] をクリックします。

自動翻訳

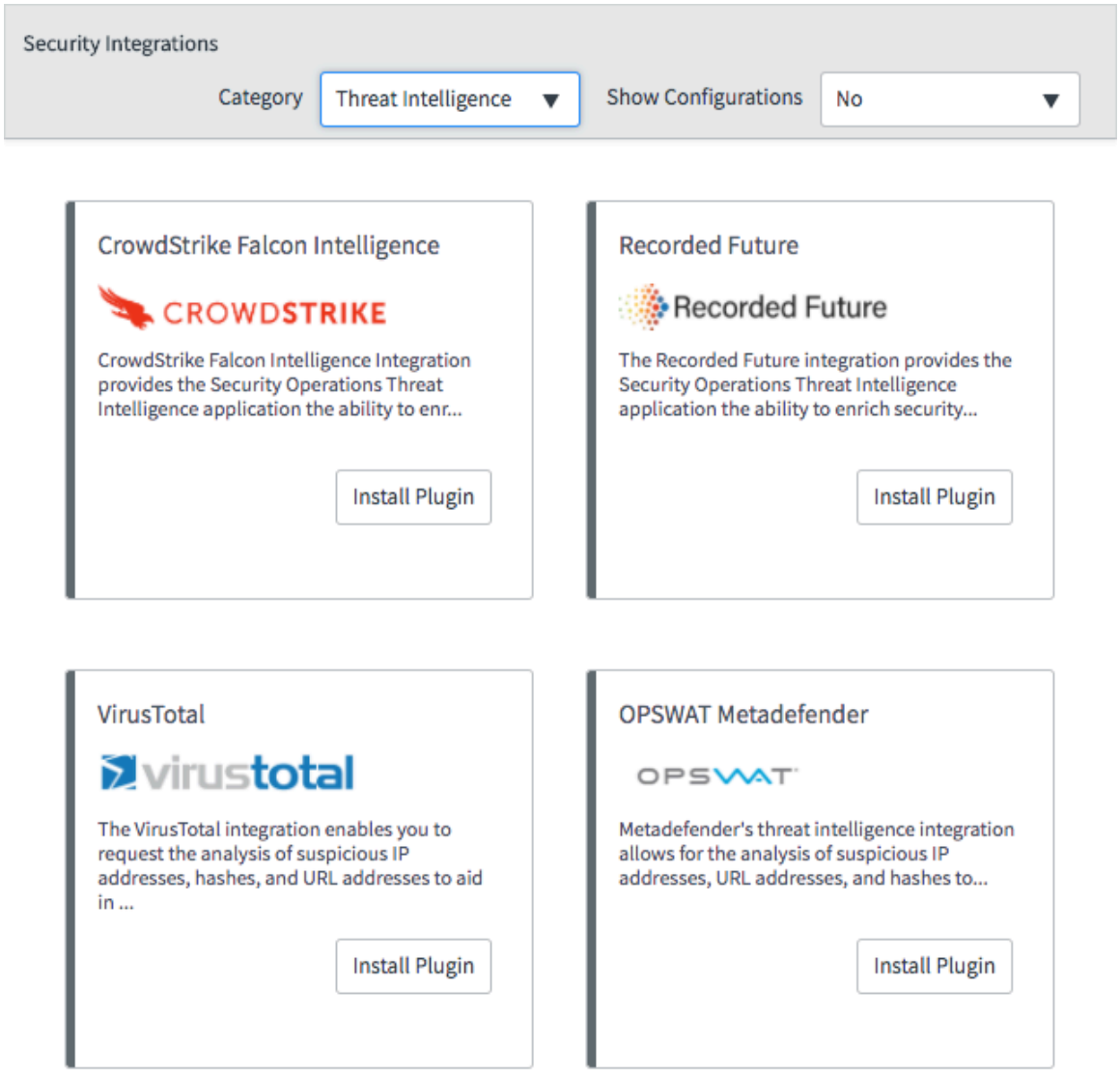
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威インテリジェンス の統合

脅威インテリジェンス ベースシステムには、サードパーティのマルウェア検出ソフトウェアパッケージへの統合が含まれています。このセクションでは、プラグインをアクティブ化し、ServiceNow とサードパーティの両方の統合機能を設定する手順について説明します。また、独自の統合を開発するための基本的なガイドラインと、ベースシステムに含まれる特定の統合の詳細も含まれています。

統合構成

ベースシステムには、アクティブ化して使用できる各統合実装の一連の「カード」が含まれています。また、セキュリティオペレーション プラグインに依存する ServiceNow Store に投稿された統合についてもカードが表示されます。統合カードを表示するには、次を選択します。 セキュリティオペレーション > 統合設定.



[カテゴリ] ドロップダウンメニューを使用すると、表示される統合をフィルタリングできます。[設定の表示] ドロップダウンメニューを使用すると、作成できる実装の複数のインスタンスを表示できます。

統合カードのボタン

統合カードには、統合の現在のステータスとカードのソースに応じて異なるボタンが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ボタン	説明
プラグインをインストール	このボタンをクリックして該当するプラグインをインストールし、統合をアクティブ化します。プラグインがインストールされると、ボタンが [構成] に変わります。
構成	統合を構成するための情報を入力するには、このボタンをクリックします。一部の統合では、サードパーティ統合の Web サイトから取得した API キーまたは URL を入力する必要があります。
新規	Carbon Black や IBM QRadar などの特定の統合では、同じ統合の複数の実装を定義できます。これらの統合では、プラグインをアクティブ化した後に [新規] をクリックします。カードを使用すると、プラグインをインストールし (該当する場合)、使用する実装を構成できます。
ページを開く	ベースシステムでは、インスタンスは、ServiceNow Store に対し、セキュリティオペレーション プラグインに依存するアプリケーションについてのクエリを実行します。これらのアプリケーションが見つかり、関連するアプリケーションプラグインが有効になると、それらの統合カードが他のセキュリティ統合カードとともに表示されます。[ページを開く] をクリックしてサードパーティアプリケーションの Web サイトにアクセスし、統合を構成します。構成が完了すると、[ページを開く] ボタンは [構成] に変わります。

Crowdstrike Falcon Intelligence 統合

CrowdStrike Falcon Intelligence は、セキュリティインシデントと関連する観測事象のデータで 脅威インテリジェンス を拡張します。

探索

- CrowdStrike Falcon Intelligence 統合の概要
- セキュリティインシデントレスポンス の統合

セットアップ

CrowdStrike Falcon Intelligence 統合のアクティブ化と構成

使用

- 観測事象のルックアップを実行する
- 脅威のルックアップ - CrowdStrike Falcon Intelligence フロー

開発

- ServiceNow セキュリティオペレーション 統合開発のガイドライン
- 統合を作成するためのヒント
- 開発者トレーニング
- 開発者ドキュメント
- アプリケーションとともにインストールされているコンポーネントの検索

トラブルシューティングとヘルプ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

- 統合のトラブルシューティング
- Security Operations Community で質問や回答をする
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

CrowdStrike Falcon Intelligence 統合の概要

CrowdStrike Falcon Intelligence は、 セキュリティオペレーションと簡単に統合できるサイバーセキュリティインテリジェンスを提供します。

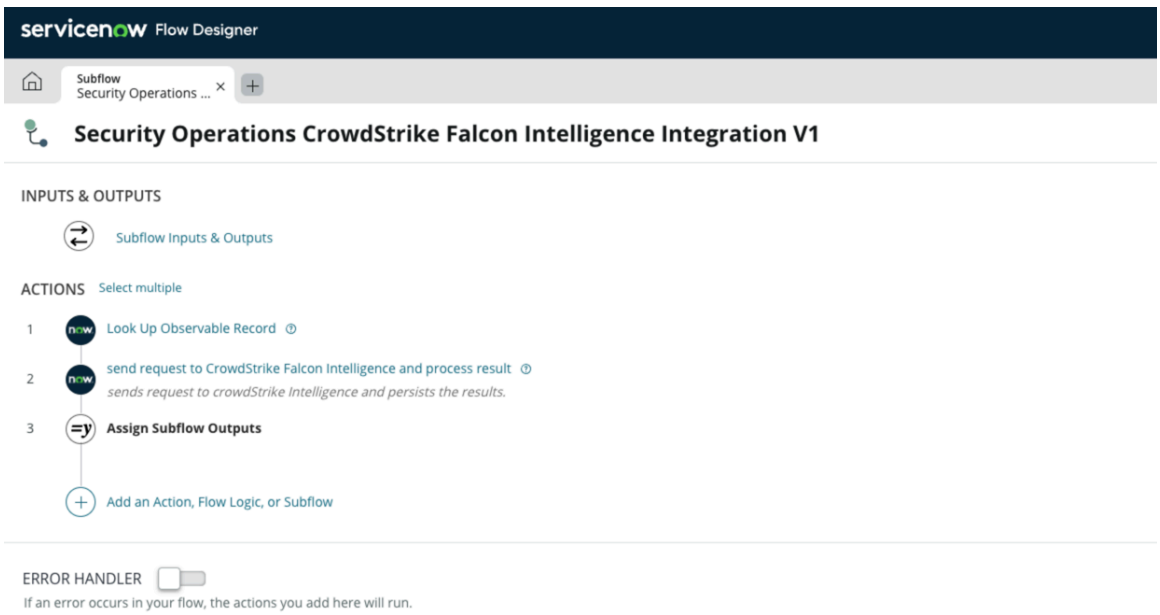
> **注:**
> CrowdStrike Falcon Intelligence 統合を実装するには 脅威インテリジェンス プラグインが必要です。

脅威のルックアップ - CrowdStrike Falcon Intelligence フロー

脅威のルックアップ - CrowdStrike Falcon Intelligence フローデザイナーは、選択された観測事象に対してルックアップを実行します。観測事象が CrowdStrike Falcon Intelligence によって認識されるタイプである場合、観測事象でマルウェアがスキャンされ、結果が返されます。

このフローは、1 つ以上の観測事象をウォッチリストに公開して、CrowdStrike Falcon Intelligence の実装が選択されている場合に、[Security Operations Integration - 脅威のルックアップ] 機能 によりトリガーされます。公開後、ウォッチリストは CrowdStrike Falcon Host ソフトウェアで表示できます。

必要なロール：admin



このフローデザイナーで使用されるアクティビティの詳細については、「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CrowdStrike Falcon Intelligence 統合のアクティブ化と構成

統合構成機能を使用すると、CrowdStrike Falcon Intelligence 統合を含むサードパーティのセキュリティ統合をすばやくアクティブ化して設定できます。CrowdStrike Falcon Intelligence を使用するには、ServiceNow Store からダウンロードして、適切な API キーと ID を追加する必要があります。

始める前に

必要なロール：admin

- CrowdStrike Falcon Intelligence 統合を使用する前に、脅威インテリジェンス プラグインをインストールしてアクティブ化する必要があります。
- CrowdStrike Falcon Intelligence プロファイルで API クライアント ID と API クライアントシークレットを取得します。
- CrowdStrike Falcon Intelligence 統合を以前のバージョンからアップグレードする場合は、既存の構成を削除して新しい構成を設定する必要があります。統合は OAUTH2 認証をサポートしています。この更新では、**[API** クライアント **ID]** と **[API** クライアントシークレット] を入力して認証し、構成を完了する必要があります。
- CrowdStrike Falcon Intelligence ポータルの **[API** スコープ] で、[インジケーター **(Falcon X)]** または **[IOC** (セキュリティ侵害のインジケーター)] の [読み取り] 設定を有効にします。

手順

1. から統合をダウンロードします ServiceNow Store.
2. インスタンスで、 セキュリティオペレーション > 統合 > 統合設定.
   利用可能なセキュリティ統合が一連のカードとして表示されます。
3. CrowdStrike Falcon Intelligence カードで、[構成] をクリックします。
4. フォームのフィールドに入力して構成を完了します。

CrowdStrike Falcon Intelligence 構成

フィールド	説明
名前	統合の名前 (例：demo-1)。
API クライアント **ID**	CrowdStrike Falcon Intelligence ポータルのアカウントプロファイルの設定セクションから取得するクライアント ID。
API クライアントシークレット	CrowdStrike Falcon Intelligence ポータルのアカウントプロファイルの設定セクションから取得するクライアント秘密キー。

5. **[Submit]** をクリックします。

タスクの結果

設定後、脅威インテリジェンス の観測事象およびセキュリティインシデントの観測事象のルックアップを実行するために CrowdStrike Falcon Intelligence を選択できます。

関連情報

観測事象のルックアップを実行する

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Have I been pwned? の統合

セキュリティオペレーション Have I been pwned? 統合を使用すると、ドメイン名とメールアドレスのルックアップを送信して、データ漏洩によってユーザーの個人データが侵害されているかどうかを判断できます。

探索	セットアップ
セキュリティインシデントレスポンス の統合	• Security Operations Have I been pwned? 統合セットアップ • Security Operations Have I been pwned? 統合のアクティブ化
使用	**開発**
観測事象のルックアップを実行する 脅威のルックアップ - Have I been pwned? フロー	• ServiceNow セキュリティオペレーション 統合開発のガイドライン • 統合を作成するためのヒント • 開発者トレーニング • 開発者ドキュメント • アプリケーションとともにインストールされているコンポーネントの検索
トラブルシューティングとヘルプ	
• 統合のトラブルシューティング • Security Operations Community で質問や回答をする • Known Error Portal で既知のエラー記事を検索 • 連絡先 カスタマーサービス & サポート	

Security Operations Have I been pwned? 統合セットアップ

Have I been pwned? は、データ漏洩によるオンラインアカウントの侵害または「pwned」(打ち負かされた) が原因でリスクにさらされている人がいるかどうかを評価するために使用される無料のリソースです。セキュリティオペレーション と簡単に統合できます。

Have I been pwned? 統合を使用する前に、プラグインをアクティブ化する必要があります。必要に応じて、X509 SSL 証明書を更新することもできます。

セキュリティオペレーション Have I been pwned? 統合を実装するには セキュリティインシデントレスポンス、脅威インテリジェンス、および セキュリティオペレーション Have I been pwned? プラグインが必要です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威のルックアップ - **Have I been pwned?** フロー

脅威のルックアップ - Have I been pwned? フローでは、選択された観測事象に対してルックアップが実行されます。観測事象が Have I been pwned? によって認識されるタイプである場合、観測事象でマルウェアがスキャンされ、結果が返されます。

必要なロール：sn_si_admin

このフローは、1 つ以上の観測事象で脅威のルックアップを実行し、Have I been pwned? の実装が選択されている場合に [Security Operations Integration - 脅威のルックアップ] 機能 でトリガーされます。詳細については、「観測事象のルックアップを実行する」を参照してください。

「Have **I been** pwned」フロー

このフローで実行されるアクティビティについて、詳細は「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

Security Operations Have I been pwned? 統合のアクティブ化

統合構成機能を使用すると、セキュリティオペレーション Have I been pwned? 統合を含むサードパーティのセキュリティ統合をすばやくアクティブ化して設定できます。Have I been pwned? 統合を使用する前に、ServiceNow Store からダウンロードする必要があります。

始める前に

- セキュリティオペレーション Have I been pwned? 統合を使用する前に、脅威インテリジェンスプラグインをインストールしてアクティブ化する必要があります。

必要なロール：sn_si_admin

手順

から統合をダウンロードします ServiceNow Store.
この統合はオープン API をサポートしており、追加の構成は必要ありません。脅威インテリジェンス の観測事象およびセキュリティインシデントの観測事象でルックアップを実行するために、Have I been pwned? を選択できるようになりました。

関連情報

観測事象のルックアップを実行する

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

X.509 証明書の更新

統合に SSL 接続が必要な場合は、サードパーティベンダーによって提供された証明書が ServiceNow でまだ信頼されていないか、有効期限が切れていることがあります。このタスクはオプションです。

始める前に
必要なロール：admin

手順

1. サードパーティベンダーから SSL 証明書を取得します。
   たとえば、次のように、Firefox ブラウザーの SSL エンドポイントから X.509 証明書 (PEM) をインポートできます。

   a. ブラウザーのアドレスバーにエンドポイント URL を入力します。
      例： `https://<3rdparty>/`。

   b. 住所のロックアイコンをクリックします。

   c. [詳細情報] をクリックし、[セキュリティ] タブをクリックします。

   d. [証明書を表示 **(View Certificate)]** をクリックし、[詳細] タブをクリックします。

   e. [エクスポート] をクリックして、PEM をローカルファイルシステムに保存します。

   f. 保存したファイルをテキストエディターで開き、内容をクリップボードにコピーします。
      `-----BEGIN CERTIFICATE-----` で始まり、`-----END CERTIFICATE-----` で終わる必要があります。

2. 次のように移動する。 システム定義 > 証明書.
3. [新規] をクリックし、統合の新規レコードを作成 します。
4. ダウンロードしてクリップボードにコピーした証明書を **[PEM** 証明書] に貼り付けます。
5. 証明書を ID プロバイダーレコードに追加します。
   a. 次のように移動する。 マルチプロバイダー **SSO** > **ID** プロバイダー.
   b. 新しい証明書を作成したアクティブなデフォルトの ID プロバイダーを選択します。
   c. **[X.509** 証明書] 関連リストまで下にスクロールし、[編集] をクリックします。
   d. 新しく作成した証明書を [選択済み] 列に移動します。
6. [保存] をクリックします。
   レコード内の他のフィールドは自動的に生成されます。

   > **注:**
   > 有効期限が切れた証明書がある場合は、それを削除する必要があります。期限切れの証明書を削除する方法については、「KB0691439 Replacing an expiring SAML certificate (期限切れ間近の SAML 証明書の置き換え)」を参照してください。

MISP integration for Security Operations

MISP integration for Security Operations を使用すると、サイティング検索、観測事象の拡張、および MISP でのイベントの作成または更新によって、セキュリティインシデントを調査できますMISP を使用することで、標的型攻撃をより迅速に調査し、検出率を向上させ、自分の環境での誤検出数を減らすことができます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

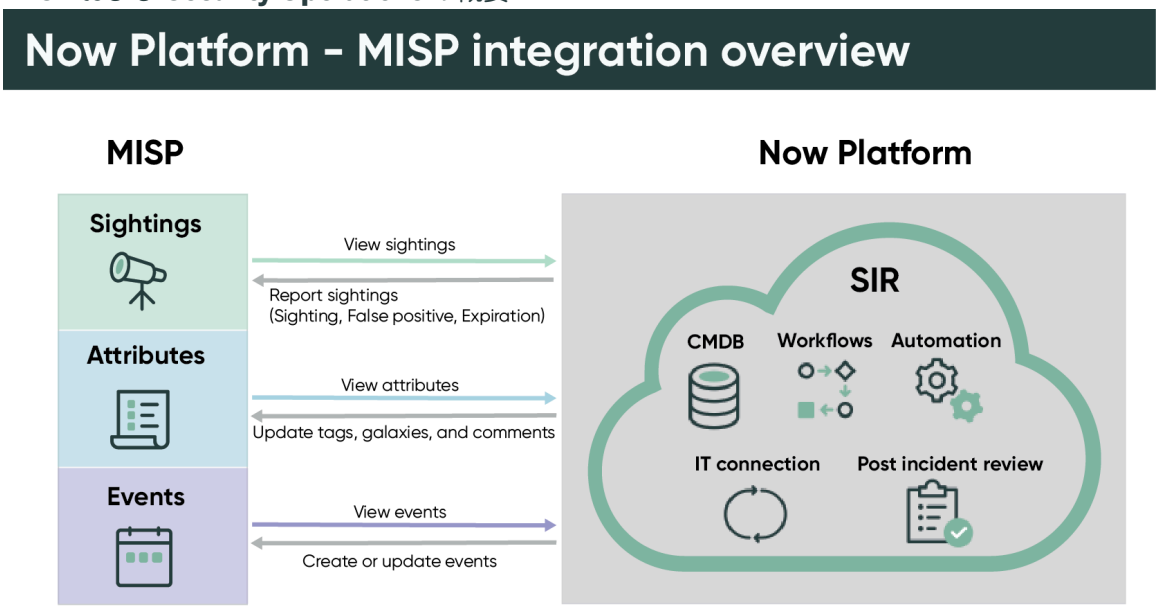
MISP の概要

MISP は Malware Information Sharing Platform の略で、信頼できるメンバーのコミュニティ内で、標的型マルウェアや攻撃に関する脅威インテリジェンスやセキュリティ侵害のインジケーター (IoC) を交換および共有できます。プライベートなコミュニティやオープンなコミュニティと MISP 情報を共有することもできます。MISP 情報を交換することで、標的型攻撃をより迅速に調査し、検出率を向上させ、自分の環境における誤検出数を減らすことができます。

MISP および Security Operations

MISP 情報が SecOps アプリケーションにどう流れていくかは、以下の例を参照してください。

MISP および Security Operations の概要



主な機能

この統合には、MISP の主な機能で実行できることも含まれています。

- プライベートおよびパブリックに接続 MISP インスタンス.
- 観測事象の手動および自動のサイティング検索をサポートする。
- ケース管理からサイティング検索を実行する。
- 属性に対するサイティングを報告または更新する。
  - 観測事象をサイティングとして報告する (グローバル)
  - 観測事象を誤検出として報告する (グローバル)
  - 観測事象を期限切れとして報告する
- 手動および自動の観測事象の拡張をサポートする。結果には、観測事象に関連付けられた MISP 属性およびイベント情報が含まれる。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- タグ、ギャラクシー、またはコメントの追加または更新を含む MISP の属性の拡張。
- でのイベント作成 MISP 差出人 SIR:SIRからのイベントの手動および自動作成MISPをサポートします。
- タグ、ギャラクシー、または属性の追加または更新を含む SIR からの MISPイベントを更新する。
- セキュリティインシデントに関連する観測事象を属性として MISP イベント.
- 自動抽出 MITRE-ATT&CK™ からの情報 MISP attributes をクリックし、その情報を SIR セキュリティインシデントに関連付けます。
- 自動追加 SIR MITRE-ATT&CK™ 情報をギャラクシーとして MISP イベント.

主要な概念

この統合には、知っておく必要がある次の主要な概念が含まれています。

- MISP は、脅威インテリジェンスプラットフォーム (TIP) です。TIP を使用して、セキュリティの脅威データをリアルタイムでコレクション、関連付け、共有、および統合して、アクションの優先順位付けをサポートし、攻撃の防止、検出、および応答を支援します。
- MISP は、脅威インテリジェンス管理 (TIM) です。TIM を使用して、コンテキストを通じて脅威データを脅威インテリジェンスに変換し、ユーザー定義のスコアリングと関連性に基づいて脅威に自動的に優先順位を付けることができます。
- MISP データレイヤー
  - イベントは、コンテキストにリンクされた情報をカプセル化したものです。
  - 属性は個々のデータポイントであり、インジケーターまたはサポートデータになります。
  - オブジェクトは、カスタムテンプレートの属性構成です。
  - オブジェクト参照は、他の構成要素の間の関係です。
  - サイティングは、検出されたデータポイントに時間指定で発生するものです。
- MISP コンテキストレイヤー
  - タグは、イベントまたは属性に付けられるラベルであり、分類に由来する場合もあります。
  - ギャラクシークラスターは、ギャラクシーに由来するイベントや属性にラベルを付けるために使用できるナレッジベースアイテムです。
  - クラスター関係とは、クラスター間の事前定義された関係を示します。
- インジケーターには、疑わしい、または悪意のあるサイバーアクティビティの検出に使用できるパターンが含まれています。
- MISP の属性は、ネットワークインジケーター (IP アドレス)、システムインジケーター (メモリ内の文字列)、または銀行口座の詳細などです。MISP の属性は、他の SIEM や STIX などの形式では観測事象と呼ばれています。
  - タイプは属性を説明するものです。たとえば、MD5 や URL などです。
  - 属性カテゴリは属性を説明するものです。たとえば、ペイロード配信などです。
  - IDS タグは、属性が自動的に検出に使用できるかどうかを決定します。

注:
MISP の概念の詳細については、「MISP Documentation website (MISP ドキュメント Web サイト)」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MISP integration for Security Operations を利用する組織のメリット

セキュリティアナリストは、脅威の状況認識を深め、維持する必要があります。つまり、膨大な量の脅威データを手作業で集約、統合しなければなりません。このようなデータのコレクション、集約、統合には貴重な時間を要するため、脅威の検出や分析が遅れることになります。MISP integration for Security Operations を使用すると、アナリストは MISP セキュリティインテリジェンスを既存の Now Platform インスタンスに統合することで、より多くの脅威を検出し、より迅速に対応できます。

MISP integration for Security Operations を使用すると、組織は次のアクションを実行できます。

- セキュリティアナリストが適切なコンテキストを用いて迅速に対応できるようにします。
- 脅威を検出して封じ込めるためのインシデントフローを自動化することで、セキュリティチームの効率を向上させます。
- 手作業による調査時間を短縮し、セキュリティアナリストが Now Platform 内からインジケーターの運用とキュレーションを行えるようにします。

この統合の詳細

ドキュメント識別子	ドキュメントタイトル
MISP ドキュメント Web サイト	MISP ドキュメント Web サイト
ServiceNow 製品ドキュメント Web サイト	ServiceNow 製品ドキュメント Web サイト

MISP 管理

Now Platform で MISP 統合を設定して、サイティング検索、観測事象の拡張を実行し、MISP のイベントを作成および更新できます。

MISP integration for Security Operations の開始

MISP integration for Security Operations を設定する前に、次の情報を確認します。

チェックリスト

セットアップタスク	説明
必要な Now Platform、脅威インテリジェンス、および セキュリティインシデントレスポンス のロールがアサインされていることを確認します。	Now Platform の MISP 機能全体で次のロールが使用されます。 • システムアドミニストレーター (admin) は、ServiceNow Store からアプリケーションをインストールし、セキュリティインシデントアドミン (sn_si.admin) と脅威インテリジェンスアドミン (sn_ti.admin) にロールをアサインします。 • sn_si.admin および sn_ti.admin は統合を構成し、MISP イベントの自動作成プロファイルを設定できます。 • sn_sec_misp.write - MISP アナリストロールには、イベントと属性データを含む MISP データに対する読み取りおよび書き込み権限があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト (続く)

セットアップタスク	説明
	詳細については、「脅威インテリジェンスのセットアップ」を参照してください。
必要な MISP ユーザーロールをアサインします。	次のものをレビュー MISP を使用するために必要なユーザーロールと権限 MISP integration for Security Operations. 注: MISP のユーザーロールの詳細については、「MISP documentation website (MISP ドキュメント Web サイト)」を参照してください。
MISP バージョン 2.4.137 以降を使用していることを確認します。	MISP integration for Security Operationsは最小限でテストされます MISP バージョン 2.4.137.
MISP モジュールをサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールしてアクティブ化します。 • セキュリティインシデントレスポンス • ServiceNow 統合ハブランタイム (com.glide.hub.integration.runtime) • ServiceNow 統合ハブアクションステップ - REST (com.glide.hub.action_step.rest) 統合のための Now Platform インスタンスの設定の詳細については、「Security Operations 製品またはアプリケーションのエンタイトルメントの取得」および「ServiceNow Store アプリケーションのアクティブ化」を参照してください。
ドメインセパレーション	データ、プロセス、および管理タスクを分離する場合は、「ドメインセパレーション」を確認してください。

MISP のユーザーロールおよび権限

MISP integration for Security Operations 統合で必要なユーザーロールを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

観測事象の拡張およびサイティング検索の権限

注:

- すべての **ServiceNow** *MISP* 統合機能には、**[Manage Organization Events** (組織のイベントの管理)] および **[Auth key access** (認証キーアクセス)] に対する基本的な権限が必要です。続行する前に、これらの基本的な権限を持っていることを確認してください。
- ローカルギャラクシーを追加するには、統合を設定するユーザーが、対応する *MISP* サーバーのホスト組織に属している必要があります。

MISP 機能	タガー	タグエディター
観測事象の拡張 (読み取り専用)	✓	✓
サイティング検索 (読み取り専用)	✓	✓

サイティングを報告する権限

MISP 機能	サイティングクリエーター
サイティングを報告	✓

属性とイベントの権限

MISP 機能	タガー	タグエディター
イベント/属性タグを編集	✓	✓
イベント/属性ギャラクシーを編集	✓	✓
属性コメントを編集	✓	✓
イベントに新しい属性を追加	✓	✓
MISP でイベントを作成	✓	✓

MISP integration for Security Operations をインストールして設定する

MISP データを使用してセキュリティインシデントの調査を開始できるように、Now Platform インスタンスの ServiceNow Store から MISP integration for Security Operations をインストールして設定します。

始める前に
MISP サーバーに有効な SSL 証明書がインストールされていることを確認します。

必要なロール：sn_si.admin

手順

1. ServiceNow Store から MISP integration for Security Operations をダウンロードして、インストールします。
2. 次のように移動する。 セキュリティオペレーション > 統合 > 統合設定.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. MISP-SIR/TI 統合タイルを検索し、[構成] をクリックします。
4. フォームのフィールドに入力します。

MISP - SIR/TI 統合構成フォーム

フィールド	説明
名前	MISP インスタンス構成の名前。
MISP サーバー URL	MISP サーバーの REST エンドポイントとして機能する MISP サーバーの URL。
API キー	MISP サーバーのユーザーアカウントに設定されている API キー。API キーは、MISP サーバーの **[Authkey]** に対応しています。
オンプレミス展開	MISP サーバーがオンプレミスのインスタンスに展開されている場合に選択できるオプション。[オンプレミス展開] オプションを選択した場合は、MID サーバー を使用して MISP サーバーに接続する必要があります。
MID アプリケーション	MISP との通信に使用される MID アプリケーション名を識別する文字列フィールド。 [オンプレミス展開] オプションを選択する場合は、このフィールドは必須です。アプリケーションの MID サーバーの設定方法については、「Configure a MID Server for each application (各アプリケーションの MID サーバーの設定)」を参照してください。

5. **[Submit]** をクリックします。

タスクの結果
構成の検証と送信が正常に完了すると、MISP - SIR/TI 統合が [セキュリティ統合] ページにタイルとして保存されます。

MISP 統合設定を確認する

MISP integration for Security Operations 設定を確認し、デフォルトのシステムプロパティを変更して環境に合わせます。

始める前に
必要なロール：sn_si.admin、sn_ti.admin

手順
1. 次のように移動する。 **All** (すべて) > **MISP** 統合 > 統合の設定.
2. 必要に応じて次の設定を変更します。

MISP 統合の設定

プロパティ名		説明
観測事象の拡張	新しいデータをフェッチするまでの時間 (時間)	新しいデータをフェッチできるまでの時間 (時間)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ名		説明
		タイプ：整数 デフォルト値：24
サイティング検索	新しい観測事象がセキュリティインシデントに関連付けられたときに、サイティング検索を自動的に実行します	新しい観測事象がセキュリティインシデントに関連付けられるたびに実行されるサイティング検索。 デフォルト値：はい
	MISP でのサイティング検索の検索間隔 (日数)	サイティング検索データが MISP で検索される日数。このオプションは、自動サイティング検索機能にのみ使用してください。 デフォルト値：90
データ同期	タグがフェッチされ、MISP と同期される間隔 (分単位)	統合構成時にフェッチされる MISP タグ。データが Now Platform に格納された後、このプロパティは MISP サーバーとのデータが同期される頻度を定義します。値は分単位で定義されます。 デフォルト値：1440 (分または 24 時間)
	構成されたソースから MISP Galaxies を更新する間隔期間 (分)	統合構成時にフェッチされる MISP ギャラクシー。データが Now Platform に格納された後、このプロパティは MISP サーバーとのデータが同期される頻度を定義します。値は分単位で定義されます。 デフォルト値：1440 (分または 24 時間)
	組織がフェッチされ、MISP と同期される間隔 (分単位)	統合構成時にフェッチされる MISP 組織。データが Now Platform に格納された後、このプロパティは MISP サーバーとのデータが同期される頻度を定義します。値は分単位で定義されます。 デフォルト値：1440 (分または 24 時間)
MITRE™ テクニック抽出	MISP 観測可能拡張結果 (タグ) からセキュリティインシデントに MITRE-ATT&CK テク	MISP 観測可能拡張結果 (タグ) からセキュリティインシデントに MITRE-ATT&CK 情報をロールアップします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ名		説明
	ニックを自動的にロールアップする	デフォルト値：はい
	MISP 観測可能拡張結果 (ギャラクシー) からセキュリティインシデントに MITRE-ATT&CK テクニックを自動的にロールアップする	MISP 観測可能エンリッチメント結果 (ギャラクシー) からセキュリティインシデントに MITRE-ATT&CK 情報をロールアップします。 デフォルト値：はい

注:

- MISP でMITRE™ テクニック抽出機能を使用するには、次のことを行う必要があります。の有効化 MITRE-ATT&CK の機能 脅威インテリジェンス module.
- MISP integration for Security Operations は、 MISP - MISP ギャラクシーと MISP タグについて 2 つのベースシステム MITRE-ATT&CK テクニック抽出ルールを導入しています。MITRE-ATT&CK の自動抽出ルールの詳細については、「MITRE-ATT&CK 情報をインポートするための自動抽出テクニックルール」を参照してください。

3. [保存] をクリックします。

タスクの結果
変更した統合の設定が保存され、適用されます。

MISP サイティング検索を設定する

MISP インスタンスで観測事象のサイティング検索を行うように、Now Platform を設定します。この情報をもとに、脅威の発生頻度を判断できます。

始める前に

- 次のものをレビュー MISP ユーザーロールと権限 MISP双方向機能を使用するために必要なもの。
- 必要なロール：sn_si.admin、sn_ti.admin

このタスクについて
[Security Operations Integration - サイティング検索] ワークフローでは、サイティング検索を実行します。このワークフローは、観測事象のリストを受け入れ、実装機能を検索し、サイティング検索設定に基づいてクエリを作成し、設定されたワークフローに基づいて検索を実行します。

MISP integration for Security Operations は、自動サイティング検索を設定できるベースシステムのサイティング検索プロファイルを提供しています。このプロファイルを使用すると、組織の関連する観測事象サイティング情報にアクセスしたり、他の組織からの外部発生回数を確認したりすることもできます。

手順

1. 次のように移動する。 **All** (すべて) > **MISP** 統合 > サイティング検索構成.

2. [**New**] をクリックします。

3. フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[サイティング検索構成] フォーム

フィールド	説明
名前	機能プロファイルの名前。
保存された検索	このオプションを選択したときに保存された検索構成。保存された検索構成クエリはサンプルクエリです。必要に応じて、自分の環境のパラメーターに置き換えて、保存された検索構成を追加で作成できます。
サイティング検索ソース	サイティング検索のソース。ソースとして MISP ログストアを選択します。
有効	保存された検索構成を有効にするオプション。アクティブな検索構成のみがサイティング検索を実行できます。
観測可能タイプ	IP アドレス、ハッシュ値、URL、ドメイン名などの観測事象タイプ。
検索あたりの最大観測事象の数	検索クエリから表示できる観測事象の最大数。
検索	デフォルトの検索文字列は、$(observable) です。ただし、MISP ログストアでサポートされているパラメーターを指定して、独自の検索クエリを定義できます。

4. **[Submit]** をクリックします。

タスクの結果
MISP サイティング検索構成プロファイルが作成されました。

自動イベントの作成方法を設定する

MISP でイベントを自動作成するように、Now Platform を設定します。

始める前に

- 次のものをレビュー MISP ユーザーロールと権限 MISP双方向機能を使用するために必要なもの。
- 必要なロール：sn_si.admin、sn_ti.admin

手順

1. 次のように移動する。 **All** (すべて) > **MISP** 統合 > イベントの自動作成プロファイル.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

名前フォーム

フィールド	説明
名前	イベントの自動作成プロファイルの名前。
説明	プロファイルの簡単な説明。より詳細な説明は、イベント作成の次のステージで属性によって共有されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
順序	トリガー条件が満たされたときのプロファイルの順序。デフォルトは 100 です。この設定はデフォルトのままにします。 複数のプロファイルを作成した場合、この値は、2 つ以上のプロファイルがトリガー条件を共有する場合の実行時の優先度を示します。番号が最も小さいプロファイルの優先度が最も高くなります。
ソース	イベント作成の MISP ソース。
有効	プロファイルがアクティブか非アクティブかを示すオプション。デフォルトでは、プロファイルがオフになっていることを示すために、このオプションはクリアされています。 このプロファイルは、プロファイルの設定手順をすべて完了し、[終了] をクリックするまでアクティブではありません。

4. [続行] をクリックします。

イベントのトリガー条件を設定する

Now Platform でイベントのトリガー条件を設定して、条件が満たされたときに MISP のイベントを自動的にトリガーできるようにします。

始める前に
必要なロール：sn_sec_misp.write

手順

1. [トリガー条件] フォームで、イベントをトリガーする詳細を入力します。
セキュリティインシデントフィールドまたは観測事象フィールドに基づくトリガー条件を指定することで、複合ロジックをビルドできます。観測事象には MISPに対応するイベントがない場合は、MISP にイベントを作成することもできます。観測事象には MISP に対応するイベントがない場合は、[セキュリティインシデントフィールドに基づいてトリガー]、[観測可能フィールドに基づいてトリガー]、および [MISP イベントを作成] の 3 つのトリガー条件の組み合わせを使用して複合ロジックをビルドすることができます。複数のトリガーを選択した場合は、AND 条件を使用して結合できます。OR 条件を使用する必要がある場合は、新しい条件でプロファイルを作成することを検討してください。

イベントのトリガー条件フォーム

フィールド	説明
セキュリティインシデントフィールドに基づいてトリガー	すべてのセキュリティインシデントのトリガー条件が満たされた場合に作成できる MISP イベント。
セキュリティインシデントのトリガー条件	条件ビルダーのリストやフィールドを使って設定できる、1 行目のフィルター。条件を追加するには、[AND] または [OR] をクリックします。[AND] を選択した場合は、すべての条件

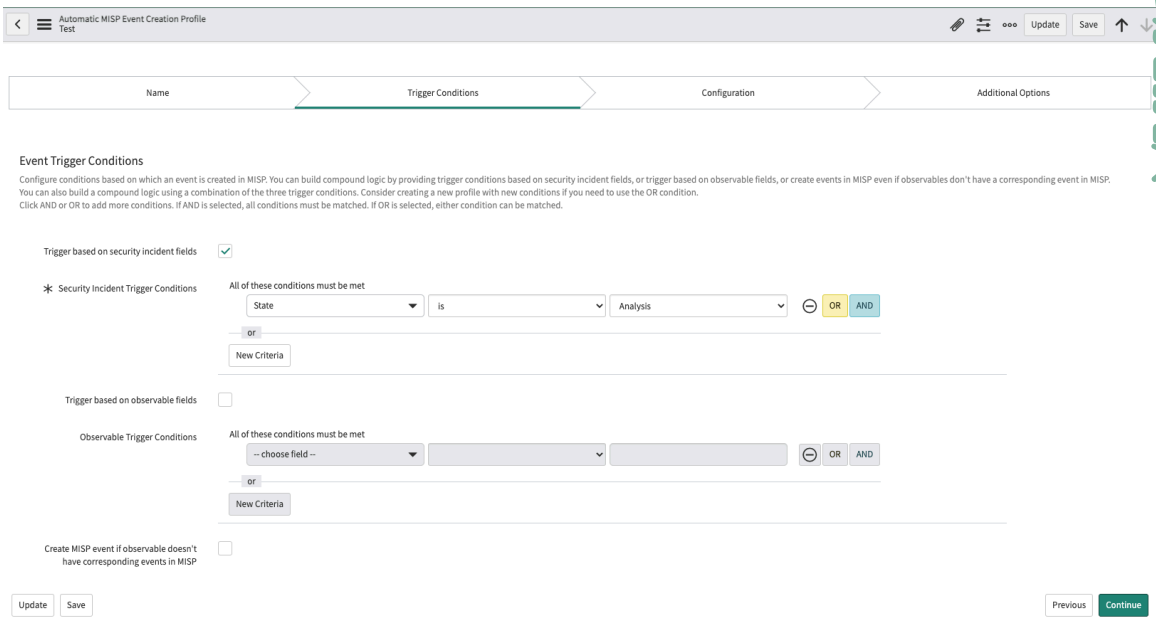
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	に一致する必要があります。[OR] を選択した場合は、いずれかの条件に一致します。 2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。
観測可能フィールドに基づいてトリガー	すべての観測事象のトリガー条件が満たされた場合に作成できる MISP イベント。
観測事象トリガー条件	条件ビルダーのリストやフィールドを使って設定できる、1 行目のフィルター。条件を追加するには、[AND] または [OR] をクリックします。[AND] を選択した場合は、すべての条件に一致する必要があります。[OR] を選択した場合は、いずれかの条件に一致します。 2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。
観測事象に対応するイベントが MISP にない場合は、MISP イベントを作成します	観測事象には MISP に対応するイベントがない場合に作成できる MISP イベント。

イベントのトリガー条件

次の例は、MISP イベント作成プロファイルを設定する際のイベントトリガー条件を示しています。



2. [続行] をクリックします。

MISP イベントフィールドをマッピングする

Now Platform の MISP イベントフィールドをマッピングして、MISP イベントが作成されたときにセキュリティインシデント情報を利用できるようにします。

始める前に

必要なロール：sn_sec_misp.write

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. フォームのフィールドに入力します。

デフォルトの **MISP** イベントフィールドマッピングフォーム

フィールド	説明
イベント情報	Now Platform セキュリティインシデントレスポンス から自動的に作成されるイベント情報。 [イベント情報] フィールドは、${SIR FIELD LABEL}$ を使用することで代替変数に対応しています。イベントの作成時に、これらの変数は実際のセキュリティインシデントフィールド値に置き換えられます。${URL}$ 代替変数は、セキュリティインシデントの URL に置き換えられます。
配布	イベントが公開された後、このイベントを表示できるユーザーを制御するオプション。このオプションは、イベントを他のサーバーに同期するかどうかも制御します。属性によって配布が受け継がれ、最も制限の多い設定が優先されます。配布オプションは次のとおりです。 ○ [自分の組織のみ (Your organization only)]：組織のメンバーのみがこのイベントを表示できるようにします。イベントは、組織のメンバーの 1 人が別のインスタンスにプルして、組織だけが閲覧できるようにすることができます。この設定のイベントは同期されません。 ○ [このコミュニティのみ (This community only)]：自分の組織、この MISP サーバー上の組織、およびこのサーバーと同期する MISP サーバーを実行している組織を含む、MISP コミュニティの一員であるユーザーがイベントを表示できるようにします。リンクサーバーに接続されている他の組織は、イベントの表示が制限されます。 ○ [接続されたコミュニティ]：この MISP サーバー上のすべての組織、このサーバーと同期する MISP サーバー上のすべての組織、および 2 ホップ離れたサーバーに接続するサーバーのホスト組織など、MISP コミュニティの一員であるユーザーがイベントを表示できるようにします。2 ホップ離れた、リンクサーバーに接続されている他の組織は、イベントの表示が制限されます。 ○ [すべてのコミュニティ]：すべての MISP コミュニティとイベントを共有します。
脅威レベル	イベントのリスクレベルを示すフィールド。インシデントは、3 つの異なる脅威のカテゴリ (低、中、高) に分類できます。このフィールド

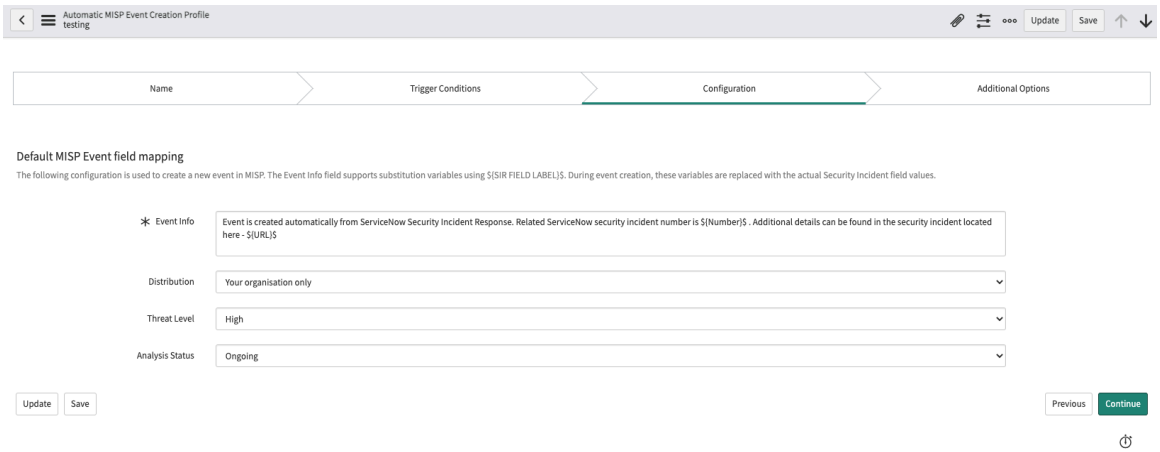
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	は未定義のままでも構いません。オプションは次のとおりです。 ○ 低：一般的な大量マルウェア ○ 中：高度で継続的な脅威 (APT) ○ 高：高度な APT およびゼロデイ攻撃
分析ステータス	次の使用可能なオプションがある、イベント分析の現在のステージ。 ○ 初期：分析を開始したばかりです ○ 進行中：分析中です ○ 完了：分析が完了しました

次の例は、MISP でのイベント作成に使用できるフォームを示しています。

デフォルトの **MISP** イベントフィールドマッピング



2. [続行] をクリックします。

SIR 観測事象の **MISP** イベントへの属性としてのマッピングまたは関連付け

MISP 属性タイプと SIR 観測事象は異なる場合があるため、セキュリティインシデントレスポンス観測事象タイプを MISP 属性タイプにマッピングします。

始める前に

必要なロール：sn_sec_misp.write

このタスクについて

MISP integration for Security Operations は、SIR 観測事象を属性として MISP イベントに追加するときに使用するベースシステムマッピングを提供します。

ベースシステムマッピングを選択し、環境に合わせて変更できます。たとえば、複数の SIR 観測事象を 1 つの MISP 属性タイプにのみマッピングすることができます。観測事象タイプがマッピングされていない場合は、デフォルトで [その他 **(other)**] MISP の属性タイプが選択されます。

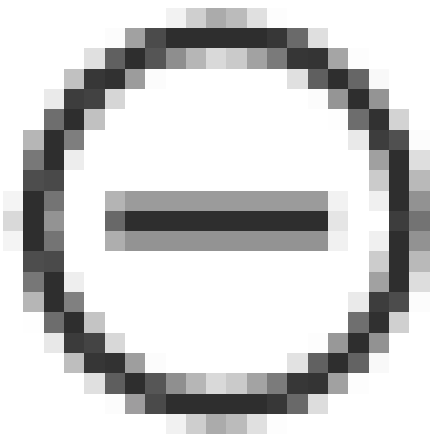
手順

1. [その他のオプション] フォームで、SIR 観測事象と MISP 属性タイプをマッピングします。
2. 次の表に示すように、セキュリティインシデントレスポンス 観測事象タイプを MISP 属性タイプにマッピングします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

SIR 観測事象と **MISP** 属性タイプのマッピング

フィールド	説明
関連するすべての観測事象を属性として追加	セキュリティインシデントで利用可能な観測事象を、属性として MISP イベントに追加するオプション。 このオプションは、[観測事象タイプから属性タイプへのマッピング (Observable Type to Attribute Type Mapping)] セクションのマッピングを有効にします。
観測事象タイプから属性タイプへのマッピング	SIR 観測事象タイプを MISP 属性タイプにマッピングするオプション。たとえば、SIR の CVE 番号を MISP の脆弱性属性にマッピングできます。 SIR 観測事象タイプは、1 つの MISP 属性タイプにのみ追加できます。 ベースシステムでは、SIR 観測事象タイプから MISP 属性タイプへのマッピングが提供されます。 SIR 観測事象タイプが MISP 属性タイプにマッピングされない場合、その観測事象は MISP の [その他 **(other)]** の属性タイプにマッピングされます。 新しいマッピングを追加するには、[観測事象タイプを追加 **(Add Observable Type)]** をクリックし、SIR 観測事象タイプを検索して、対応する MISP 属性タイプにマッピングします。 [マッピングを削除] アイコン  をクリックし、SIR および MISP 属性マッピングの関連付けを削除します。

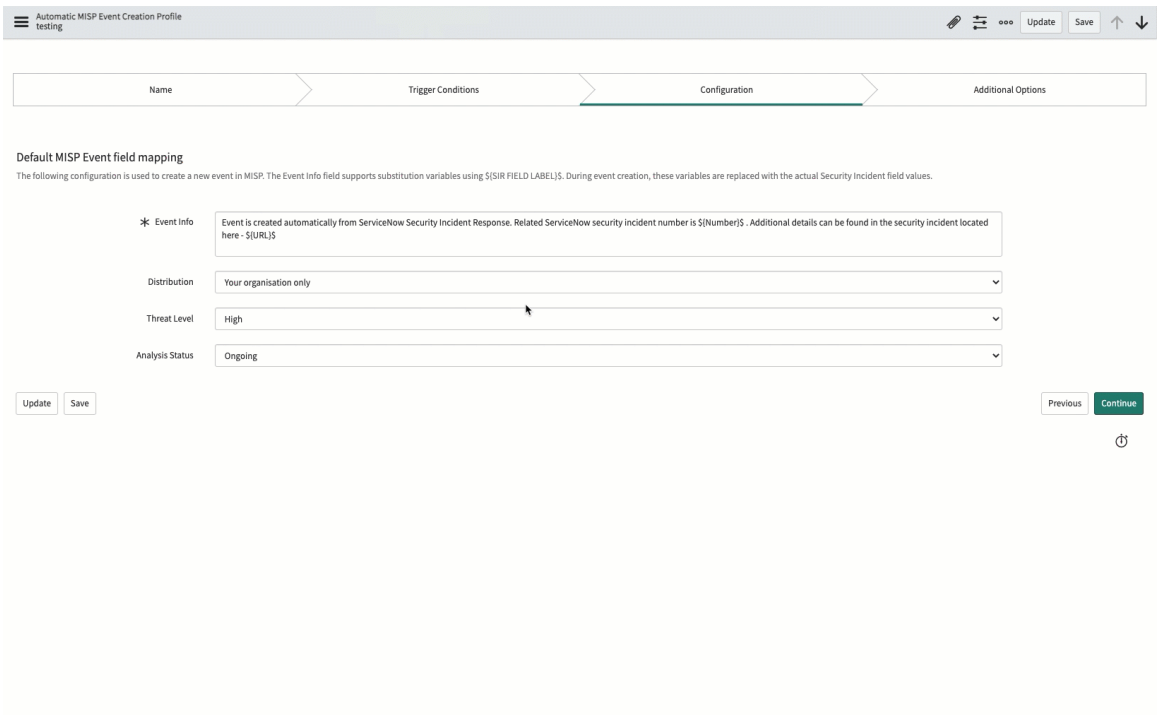
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: MISP 属性タイプの詳細については、「MISP documentation (MISP ドキュメント)」を参照してください。
セキュリティタグに基づいて観測事象をフィルタリングする	選択したセキュリティタグに基づいて観測事象をフィルタリングするオプション。 セキュリティタグ：観測事象をフィルタリングするタグを追加します。たとえば、「共有をブロック」または「TLP：白」というタグを追加する場合、いずれかの観測事象にこれらのタグのいずれかが関連付けられていると、MISP イベントの作成時にこれらの観測事象は MISP イベントに属性として追加されません。
観測事象の検出結果が悪意のある場合、属性 IDS フラグを設定	SIR で観測事象が悪意があるとしてマークされている場合に、MISP の対応する属性が IDS フラグを有効にしていることを示すオプション。IDS フラグが設定されていない場合、属性はコンテキスト情報と見なされ、自動侵入検出には使用されません。

次の例は、その他のオプションページに移動する方法を示しています。このページでは、SIR 観測事象と MISP 属性タイプのマッピングを有効にし、IPV6 ネットワークや IPV4 ネットワークなどの新しい SIR 観測可能タイプを追加して、MISP 属性タイプドメインの IP アドレスにマッピングできます。

SIR 観測事象と **MISP** 属性タイプのマッピング



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MITRE-ATT&CK 情報を MISP イベントに同期する

MITRE-ATT&CK 情報を MISP 属性と同期させて、セキュリティインシデントと脅威をより適切に分析します。

始める前に
必要なロール：sn_sec_misp.write

手順

[その他のオプション] フォームで、MITRE-ATT&CK 情報を MISP 属性と同期させるオプションを確認します。

[詳細オプション] フォーム

フィールド	説明
セキュリティインシデントの MITRE-ATT&CK テクニックをローカルギャラクシーとして MISP イベントに同期	Now Platform の セキュリティインシデント MITRE-ATT&CK テクニックを、MISP イベントのローカルギャラクシーとして同期するオプション。 **注:** ローカルギャラクシーを追加するには、統合を設定したユーザーが、対応する MISP サーバーのホスト組織に属している必要があります。
セキュリティインシデントの MITRE-ATT&CK テクニックをグローバルギャラクシーとして MISP イベントに同期	Now Platform の セキュリティインシデント MITRE-ATT&CK テクニックを、MISP イベントのグローバルギャラクシーとして同期するオプション。

タスクの結果
MISP から Now Platform に、イベントを自動で作成できるようにするプロファイルを作成しました。これで、[関連付けられた MISP イベント] 関連リストにイベントを表示できるようになりました。

イベントに MISP タグを追加する

作成された MISP イベントに MISP タグを追加します。

始める前に
必要なロール：sn_sec_misp.write

手順

1. [他のオプション] フォームで、フォームビューの [イベントに追加する **MISP** タグを選択 **(Select MISP tags to add to the event)]** セクションに移動します。
2. 作成したイベントにタグを追加するオプションを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[詳細オプション] フォーム

フィールド	説明
作成した MISP イベントにタグを追加する	ServiceNow から作成されたイベントに MISP タグを自動的に追加できるようにするオプション。
タグ (ローカル)	選択したタグがローカルタグとして MISP イベントに追加されます。
タグ (グローバル)	選択したタグがグローバルタグとして MISP イベントに追加されます。

3. [保存] をクリックします。

タスクの結果

MISP タグを追加すると、イベントの分類に役立ちます。

MISP イベントデータ

MISP イベントデータのレビューを行って、MISP のイベントに関する詳細情報を確認できます。

リストビューの **MISP** イベントデータ

からリストビューにアクセスする **MISP** > **MISP** イベントデータ.

MISP イベントデータの簡単な概要を取得するには、リストビューを使用します。

MISP イベントのリストビュー

フィールド	説明
イベント ID	イベントが最初に作成されたとき、または MISP サーバーにインポートされたときに、MISP によってアサインされたイベント ID。
Info	イベントの簡単な説明。
分析	以下の使用可能なオプションがある、イベント分析の現在のステージ。 • 初期：分析を開始したばかりです • 進行中：分析中です • 完了：分析が完了しました
脅威レベル	イベントのリスクレベル。インシデントは、3 つの異なる脅威のカテゴリ (低、中、高) に分類できます。このフィールドは未定義のままで構いません。オプションは次のとおりです。 • 低：一般的な大量マルウェア • 中：高度で継続的な脅威 (APT) • 高：高度な APT およびゼロデイ攻撃

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MISP イベントのリストビュー (続く)

フィールド	説明
MISP タグ	MISP イベントに関連付けられているタグ。
MISP Galaxies	MISP イベントに関連付けられているギャラクシー。
オーナー組織	MISP インスタンスのイベントを所有する組織。このフィールドはアドミンのみが見ることができます。
作成者組織	MISP インスタンスのイベントを作成した組織。
配布	個別属性の配布。属性には、イベントとは異なる配布レベルを設定できます。
MISP イベントハイパーリンク	MISP サーバーに保存されている MISP イベントへのリンク。
MISP ソース	イベントが作成された MISP ソース。

フォームビューの **MISP** イベントデータ

MISP イベントに関する詳細情報を取得するには、フォームビューを使用します。

MISP イベントのフォームビュー

フィールド	説明
イベント ID	イベントが最初に作成されたとき、または MISP サーバーにインポートされたときに、MISP によってアサインされたイベント ID。
UUID	イベントと属性を一意に識別する ID。
作成者組織	MISP インスタンスのイベントを作成した組織。
オーナー組織	MISP インスタンスのイベントを所有する組織。このフィールドはアドミンのみが見ることができます。
作成者ユーザー	MISP でイベントを作成したユーザー
前回の変更	イベントが最後に変更された日付
MISP ソース	イベントが作成された MISP ソース。
作成日 (MISP)	MISP サーバーでイベントが作成された、または最初にインポートされた日付。
脅威レベル	イベントのリスクレベル。インシデントは、3 つの異なる脅威のカテゴリ (低、中、高) に分類できます。このフィールドは未定義のままで構いません。オプションは次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MISP イベントのフォームビュー (続く)

フィールド	説明
	• 低：一般的な大量マルウェア • 中：高度で継続的な脅威 (APT) • 高：高度な APT およびゼロデイ攻撃
分析	以下の使用可能なオプションがある、イベント分析の現在のステージ。 • 初期：分析を開始したばかりです • 進行中：分析中です • 完了：分析が完了しました
配布	個別属性の配布。属性には、イベントとは異なる配布レベルを設定できます。
公開	イベントが公開されているかどうかのステータス。公開すると、対象となるすべてのエクスポートにイベントの属性が使用され、イベントアラートに登録されているユーザーに通知されます。
MISP イベントハイパーリンク	MISP サーバーに保存されている MISP イベントへのリンク。
Info	イベントの簡単な説明。
タグ (ローカル)	ホスト組織の MISP インスタンスで利用可能なタグで、同期とエクスポートのフィルタリングのためのタグ付けを可能にします。ローカルタグを使用しても、MISP イベントは変更されません。ローカルタグは、他の MISP インスタンスや共有コミュニティと同期される前に、常に削除されます。
タグ (グローバル)	グローバルで利用可能なタグで、他の MISP インスタンスや共有コミュニティと共有および同期されます。MISP インスタンスにグローバルタグを追加すると、イベントを変更できます。
ギャラクシー (ローカル)	同期とエクスポートのフィルタリングのために、ホスト組織の MISP インスタンスで利用可能なギャラクシーです。ローカルギャラクシーを使用しても、MISP イベントは変更されません。ローカルギャラクシーは、他の MISP インスタンスや共有コミュニティと同期される前に、常に削除されます。
ギャラクシー (グローバル)	グローバルで利用可能なギャラクシーで、他の MISP インスタンスや共有コミュニティと共有および同期されます。MISP インスタンスにグローバルギャラクシーを追加すると、イベントを変更できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連する **MISP** イベント

関連する MISP イベントのリストビューを使用して、セキュリティインシデントのコンテキストで手動または自動で作成されたイベントを表示できます。

関連付けられた **MISP** イベント

フィールド	説明
セキュリティインシデント	SIR のセキュリティインシデント。 セキュリティインシデントをクリックして、セキュリティインシデントを表示します。
MISP イベント	MISP イベント ID。 MISP イベントをクリックして、Now Platform で MISP イベントを表示します。
MISP ソース	イベントが作成された MISP ソース。 MISP ソースをクリックして、ソースを表示します。
イベント作成モード	イベントが手動で作成されたか、イベント作成プロファイルを使用して自動的に作成されたかを示すステータス。 MISP イベントをクリックして、関連する MISP イベントを表示します。
イベントの自動作成プロファイル	自動イベントの作成に使用されるイベント作成プロファイル。 プロファイルをクリックして、MISP イベントの自動作成プロファイルを表示します。

MISP ユーザー情報

MISP ユーザー情報ページを使用して、Now Platform MISP integration for Security Operations のすべての関連ユーザーを表示できます。

MISP ユーザー情報

フィールド	説明
ソース	ユーザーアカウントの MISP ソース。
ユーザー ID	ユーザーアカウントの作成時に MISP サーバーによってアサインされるユーザー ID。
ユーザーメール	ユーザーのメールアドレス。組織アドミンのみが、自分の組織のユーザーのメールアドレスを見ることができます。
組織	ユーザーが属する組織。
ロール名	ユーザーに付与されるユーザー権限を定義するロール名。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MISP ユーザー情報 (続く)

フィールド	説明
	MISP のロールの詳細については、「MISP documentation (MISP ドキュメント)」を参照してください。
ロール ID	MISP のユーザーロール ID。たとえば、Perm Admin、Perm Audit、Perm Taggger などです。
権限	ユーザーが持っている権限。MISP で使用できる権限は次のとおりです。 • 読み込み専用 • 自身のイベントの管理 • 組織のイベントの管理 • 組織のイベントの管理と公開
サイティング許可	ユーザーがサイティング検索を実行できるようにする権限。
タガー権限	ユーザーがタグ付けできるようにする権限。

ドメインセパレーションと **MISP**

ドメインセパレーションは MISP でサポートされています。ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。その後、どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル

サポート：ベーシック。

MISP のドメインセパレーションの仕組み

ドメインセパレーションを実現するには、次の手順に従います。

- ドメインに必要なロールを持つユーザーを作成します。
- ドメインで MISP integration for Security Operations 手順を実行します。

MISP 統合のトラブルシューティング

このセクションでは、MISP 統合を設定または実行する際に遭遇することがある一般的な問題を解決するのに役立つ、重要なトラブルシューティングのヒントについて説明します。

SSL の問題

MISP 統合を通して接続する場合は、MISP サーバーに有効な CA 証明書がインストールされており、有効期限が切れていないことを確認してください。RSA または独自の証明書をプラットフォームにインポートし、証明書の共通名がホスト名と一致することを確認できます。詳細については、「MISP integration for Security Operations をインストールして設定する」と「MISP のユーザーロールおよび権限」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

MISP を使用した脅威の調査と分析

Now Platform 脅威インテリジェンス モジュールと Now Platform SIR モジュールを通して MISP データを使用し、組織に対する脅威の調査と分析を行うことができます。

MISP のサイティング検索

MISP インスタンスの観測事象に対してサイティング検索を行い、フィッシング攻撃や悪意のある IP や URL による通信など、特定のタイプの攻撃がネットワーク上でどの程度の頻度で発生しているのかを把握することができます。各発生は 1 回のサイティングと見なされます。

MISP でのサイティング

サイティングとは、インジケーター、オブジェクト、または属性が観測され、その有効性が確認されたことを示します。MISP でのサイティングは、イベントの属性に応答できるようにするシステムです。ユーザーがある属性を観測したことが容易に確認できるように設計されているため、より高い信頼性を得ることができます。一つの属性は複数回サイティングできます。

注:
観測事象は、MISP では属性と呼びます。

一部の属性は、有効なサイティングではないことを意味する誤検出と見なされます。また、1 週間だけ実行されるフィッシングキャンペーンのように、特定の期間だけ有効な属性もあります。ある期間有効な属性に有効期限をアサインすることはできますが、各組織が属性にアサインできる有効期限は 1 つだけです。

対応する MISP サーバーでローカルとしてマークされた組織のユーザーによって MISP で作成されたサイティングは、内部サイティングと呼びます。対応する MISP サーバーでリモートとしてマークされた組織のユーザーによって MISP で作成されたサイティングは、外部サイティングと呼びます。

SIR のサイティング検索

[Security Operations Integration - サイティング検索] ワークフローでは、サイティング検索を実行します。この フローは、観測事象のリストを受け入れ、実装機能を検索し、サイティング検索構成に基づいてクエリを作成し、構成された フローに基づいて検索を実行します。

サイティング検索は、アナリストが脅威のまん延を時系列で見極めるのに役立ちます。セキュリティインシデントから、個別または複数の観測事象と検索対象の日付範囲を選択できます。結果は、セキュリティインシデントのサイティング、サイティング検索結果、およびサイティング検索の詳細の各関連リストに含まれます。

インシデントの分析を始める際、Now Platform を設定して、自動的にサイティング検索を実行したり、手動で観測事象のサイティング検索を実行したりして、同じフィッシング攻撃の影響を受けている組織内の他のユーザーを特定することができます。

MISP で自動サイティング検索を有効にする

MISP でサイティング検索が自動的に実行されるようにし、新しい観測事象がセキュリティインシデントに関連付けられるたびに [Security Operations Integration - サイティング検索] ワークフローがトリガーされるようにします。

始める前に
次のことを確認します。 のサイティング検索構成プロファイル MISP がアクティブです。

必要なロール：sn_si.analyst

このタスクについて
有効にすると で自動的に実行されるサイティング検索機能 MISP 統合構成の場合、新しい観測事象がセキュリティインシデントに関連付けられたときに、 MISP のサイティング検索がトリガーされます。デフォルトでは、[新しい観測事象がセキュリティインシデントに関連付けられたとき

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

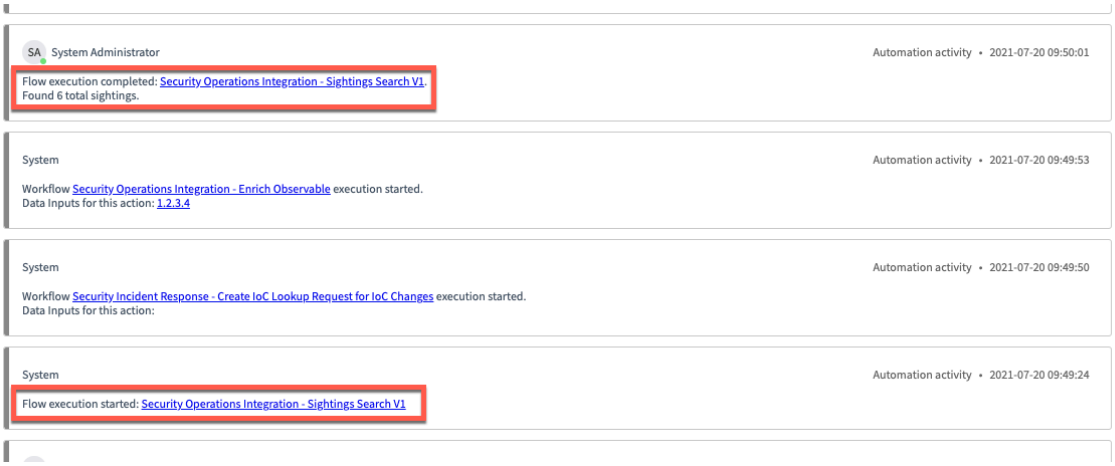
自動翻訳

に、サイティング検索を自動的に実行します **(Run Sighting Search automatically when new observables are associated with the security incident)]** オプションが有効になっています。

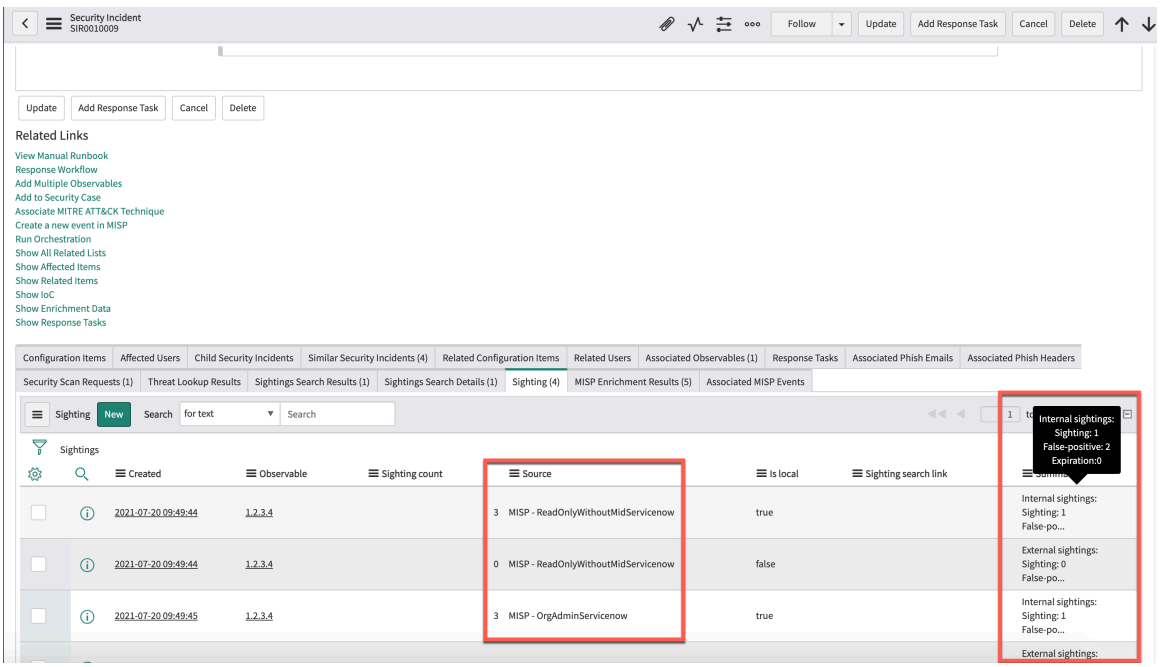
手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. MISP サイティング検索データに表示する観測事象を含んでいるセキュリティインシデントを選択します。
3. 新しい観測事象がセキュリティインシデントに関連付けられた後、作業メモを確認します。[Security Operations Integrations - サイティング検索] ワークフローがトリガーされると、作業メモが投稿されます。

   以下の例は、作業メモセクションを示しています。



4. ワークフロー実行後、すべてのイベント (グローバル) で観測され、内部発生回数および外部発生回数ごとに分類された観測事象の集計情報を表示します。サイティング、サイティング検索結果、およびサイティング検索の詳細の関連リストに情報を表示します。以下の例では、サイティング関連リストに作成されたサイティング検索レコードを示しています。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サイティング検索レコード

フィールド	説明
作成済み	サイティング検索レコードが作成された日時。
観測事象	クエリによって検索された観測事象。
サイティング回数	内部発生回数および外部発生回数。
ソース	観測事象のソース。観測事象が MISP 組織からのものである場合、レコードの前に MISP の文字が入ります。
ローカルか	サイティングが内部ユーザーによって報告されたかどうかのステータス。
サイティング検索リンク	MISP インスタンス内のサイティング検索リンク。
まとめ	レコードに関連付けられているサイティングのタイプ。サイティングには、サイティング、誤検出、および有効期限の 3 つのタイプがあります。 [サマリー] 列は、MISP integration for Security Operations がインストールされている場合にのみ表示されます。MISP 以外のソースが表示されている場合、そのレコードの [サマリー] 列にはエントリーがありません。

自動翻訳

MISP で手動サイティング検索を実行する

個々のまたは複数の観測事象を選択し、Now Platform MISP integration for Security Operationsアプリケーションで手動サイティング検索を行うことで、脅威のまん延を時系列で見極めることができます。

始める前に

- 次のものをレビュー MISP ユーザーロールと権限 MISP双方向機能を使用する場合。
- 必要なロール：sn_si.analyst

手順

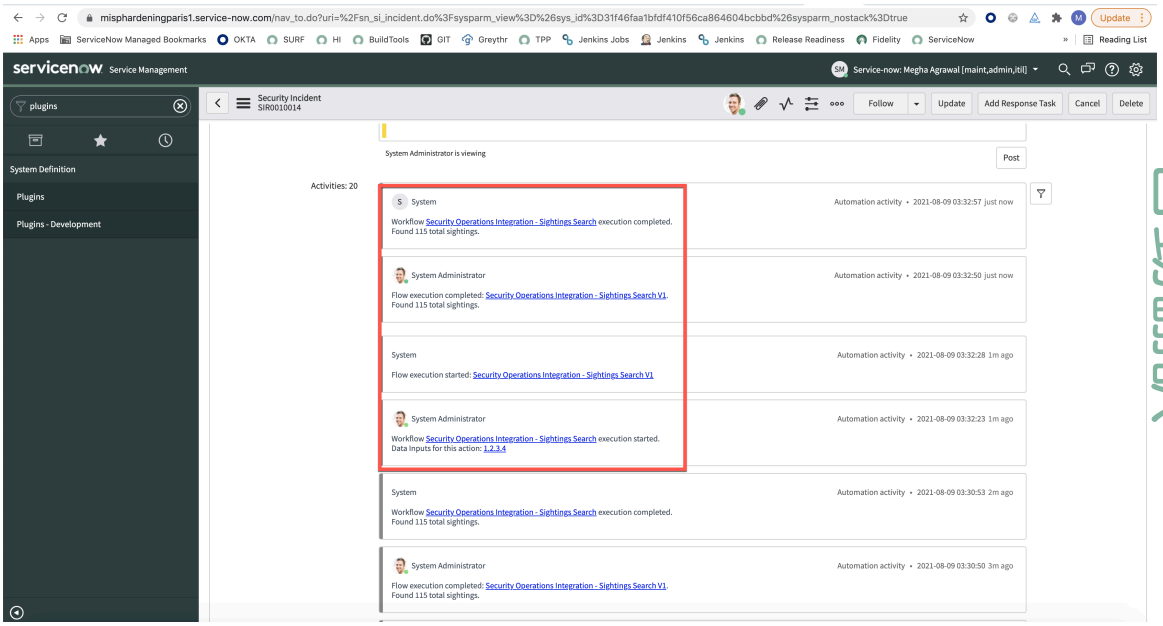
1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. MISP サイティング検索を実行する観測事象を含んでいるセキュリティインシデントを選択します。
3. [すべての関連リストを表示] と [関連する観測事象 **(Associated Observables)]** タブをクリックします。
4. 観測事象を選択した後、[アクション] メニューから、[サイティング検索を実行] をクリックします。
   サイティング検索では複数の観測事象を選択できます。
   [サイティング検索を実行] ダイアログボックスが開きます。
5. サイティング検索データを検索する日付範囲を指定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[サイティング検索を実行] ダイアログボックス

フィールド	説明
前の	検索するインシデントを作成するまでの時間数または日数。 デフォルトは 7 日です。制限は 99 時間または日です。
次の間	検索する日付の範囲。デフォルトの日付は次のとおりです。 ○ インシデントが作成された日時。 ○ インシデントのオープンの 7 日前となる日時。

6. [検索] をクリックします。
次の例は、作業メモの手動サイティング検索結果を示しています。



タスクの結果

サイティング検索レコードが作成されます。ワークフローの実行が完了すると、すべてのイベント (グローバル) で観測され、内部発生回数および外部発生回数ごとに分類された観測事象の集計情報を表示できます。集計された関連するサイティングデータは、セキュリティインシデントのサイティング、サイティング検索結果、およびサイティング検索の詳細の各関連リストで表示されます。

MISP にサイティングを報告する

脅威データのサイティングを報告することで、データの誤検出に対応し、真陽性の脅威が発生した際の注意を喚起できます。特定の観測事象または属性について、有効期限を追加することもできます。

始める前に

- 次のものをレビュー MISP ユーザーロールと権限 MISP双方向機能を使用する場合。
- 必要なロール：sn_si.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

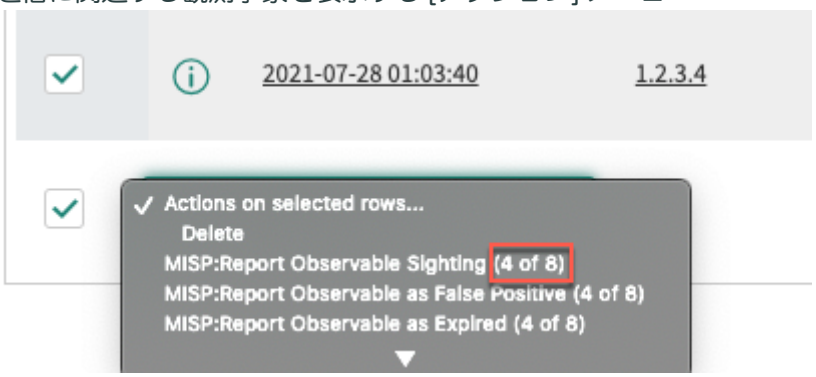
このタスクについて
MISP integration for Security Operations を使用すると、すべてのイベントについてグローバルに MISP にサイティングを報告できます。特定のイベントにサイティングを報告するには、MISP インスタンスを使用してローカルでサイティングを報告する必要があります。

MISP にサイティングを報告するには、MISP インスタンスで観測事象または属性が利用可能である必要があります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. MISP にサイティングを報告する観測事象を含んでいるセキュリティインシデントを選択します。
3. [すべての関連リストを表示] および [サイティング] 関連リストをクリックします。
4. 観測事象を選択し、[アクション] メニューから次のオプションのいずれかを選択します。
   MISP ソースに固有でない観測事象を選択すると、 [アクション] メニューには関連する MISP ソースの数が表示されます。次の例は、MISP に関連する 8 つの観測事象のうち 4 つを示しています。また、[アクション] メニューと送信に関連する観測事象を示しています。

送信に関連する観測事象を表示する [アクション] メニュー



5. オプション: [MISP：観測事象のサイティングの報告] オプションを選択した場合は、[観測事象のサイティングを MISP に報告] ダイアログボックスに入力する必要があります。

[観測事象のサイティングを **MISP** に報告] ダイアログボックス

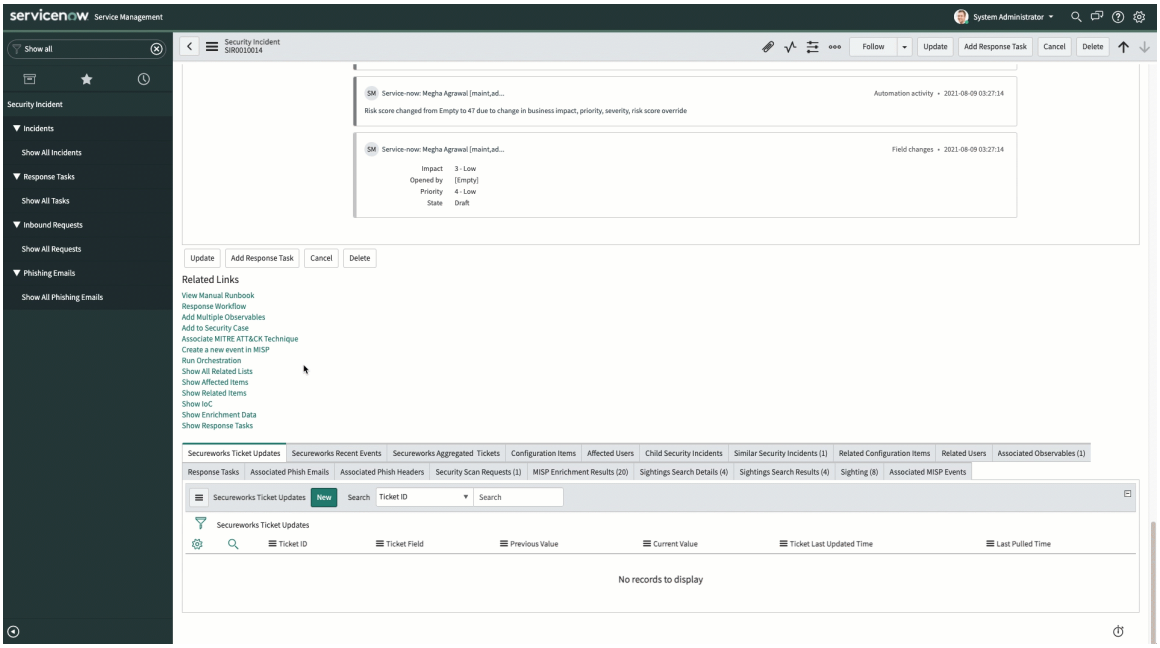
フィールド	説明
ソース	サイティングの MISP ソースに対応しているソースフィールド。
日付	観測事象がサイティングされた日付に対応している日付フィールド。日付が空の場合、MISP には現在の日時が入力されます。

次の例は、セキュリティインシデントの [サイティング] 関連リストに移動する方法を示しています。このリストから、観測事象を選択し、MISP に観測事象のサイティングを報告できます。成功メッセージは、MISP にサイティングが正常に送信されたことを示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

観測事象のサイティングを **MISP** に報告



a. [サイティングを報告] をクリックします。

6. オプション: [MISP：観測事象を誤検出として報告] オプションを選択した場合は、[観測事象を誤検出として MISP に報告] ダイアログボックスのフィールドに入力する必要があります。

観測事象を誤検出として **MISP** に報告

フィールド	説明
ソース (オプション)	MISP ソースに対応しているソースフィールド。このフィールドを使用して、観測事象を誤検出として宣言します。
日付	観測事象が誤検出であることが判明した日付に対応している日付フィールド。日付が空の場合、MISP には現在の日時が入力されます。

a. [誤検出を報告] をクリックします。

7. オプション: [MISP：観測事象を期限切れとしてレポート] オプションを選択した場合は、[観測事象の有効期限を MISP に報告] ダイアログボックスのフィールドに入力する必要があります。

[観測事象の有効期限を **MISP** に報告] ダイアログボックス

フィールド	説明
ソース	MISP ソースに対応しているソースフィールド。このフィールドを使用して、観測事象を期限切れとして設定します。
日付	観測事象が期限切れになった日付に対応している日付フィールド。日付が空の場合、MISP には現在の日時が入力されます。

a. [有効期限を報告 **(Report Expiry)]** をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスクの結果
サイティングは、MISP サーバーに正常に更新されました。

MISP での観測事象の拡張

インシデント応答の調査中にさまざまな MISP ソースからの追加情報で観測事象を拡張することによって、識別された脅威を封じ込めることができます。

MISP で観測事象の自動拡張を有効にする

新しい観測事象がセキュリティインシデントに関連付けられた場合、Now Platform MISP で観測事象の自動拡張を有効にします。

始める前に

- [スケジュール済みジョブを有効または無効にし、セキュリティインシデントの観測事象をルックアップします]オプションの セキュリティインシデントレスポンス システムプロパティを有効にして、SIR の観測事象の拡張機能をトリガーします。
- 必要なロール：sn_si.analyst

手順

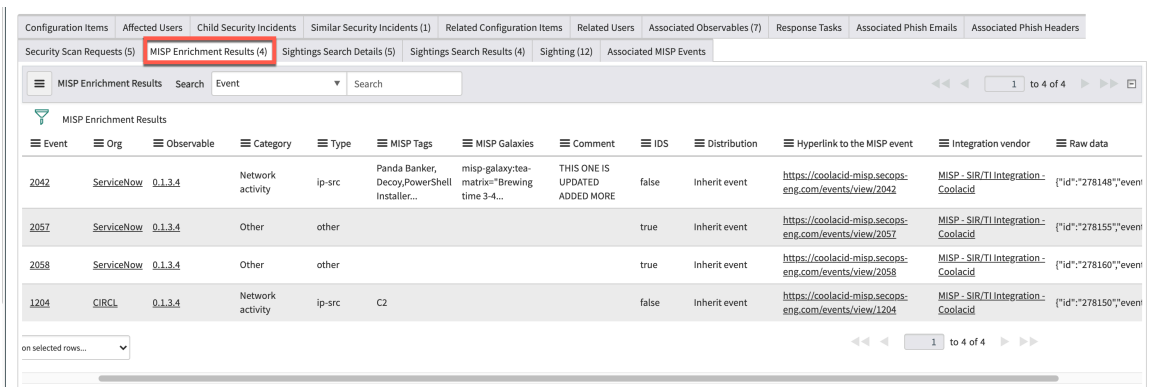
1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. MISP で観測事象データを拡張する観測事象を含んでいるセキュリティインシデントを選択します。
3. 新しい観測事象がセキュリティインシデントに関連付けられた後、作業メモを確認します。

   次の例は、[Security Operations Integration - 観測事象を拡張] フローがトリガーされたときに、作業メモが投稿されることを示しています。

4. セキュリティインシデントの MISP エンリッチメント結果関連リストに、フローの実行が完了した後にエンリッチメント結果を表示します。

   注:
   MISP エンリッチメント結果関連リストがセキュリティインシデント関連リストに表示されるように設定する必要があります。詳細については、「related list configuration (関連リストの設定)」を参照してください。

   次の例は、MISP のエンリッチメント結果を示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の表は、MISP のエンリッチメント結果を示しています。

MISP エンリッチメント結果

フィールド	説明
イベント	イベントの ID。[開く] をクリックして、Now Platform インスタンスでレコードを表示します。
Org	最初にイベントを作成した組織。
観測事象	イベントに関連付けられている観測事象。
カテゴリ	属性のカテゴリ。 MISP ドキュメント のカテゴリリストを表示します。
タイプ	属性のタイプ。 MISP ドキュメント のタイプリストを表示します。
MISP タグ	MISP 属性に関連付けられているタグのリスト。
MISP Galaxies	MISP 属性に関連付けられているギャラクシーのリスト。
コメント	属性を詳しく説明するコンテキストコメント。これらのコメントは相関には使用されず、単なる情報提供のためのものです。
IDS	すべての対象エクスポートに含めることができる、セキュリティ侵害のインジケーター。
配布	公開後の属性の配布。属性には、イベントとは異なる配布レベルを設定できます。いずれの場合も、最も低い配布レベルが使用されます。
MISP イベントへのハイパーリンク	MISP サーバーに保存されている MISP イベントへのリンク。
統合ベンダー	拡張用のデータを提供する統合ベンダー。
生データ	MISP 属性に関連付けられている生データ。

自動翻訳

MISP における観測事象の手動拡張の実行

個々のまたは複数の観測事象を選択し、手動で観測事象の拡張を行うことで、様々な MISP ソースからの追加情報で観測事象を拡張できます。

始める前に

- 次のものをレビュー MISP ユーザーロールと権限 MISP双方向機能を使用する場合。
- 必要なロール：sn_si.analyst

手順

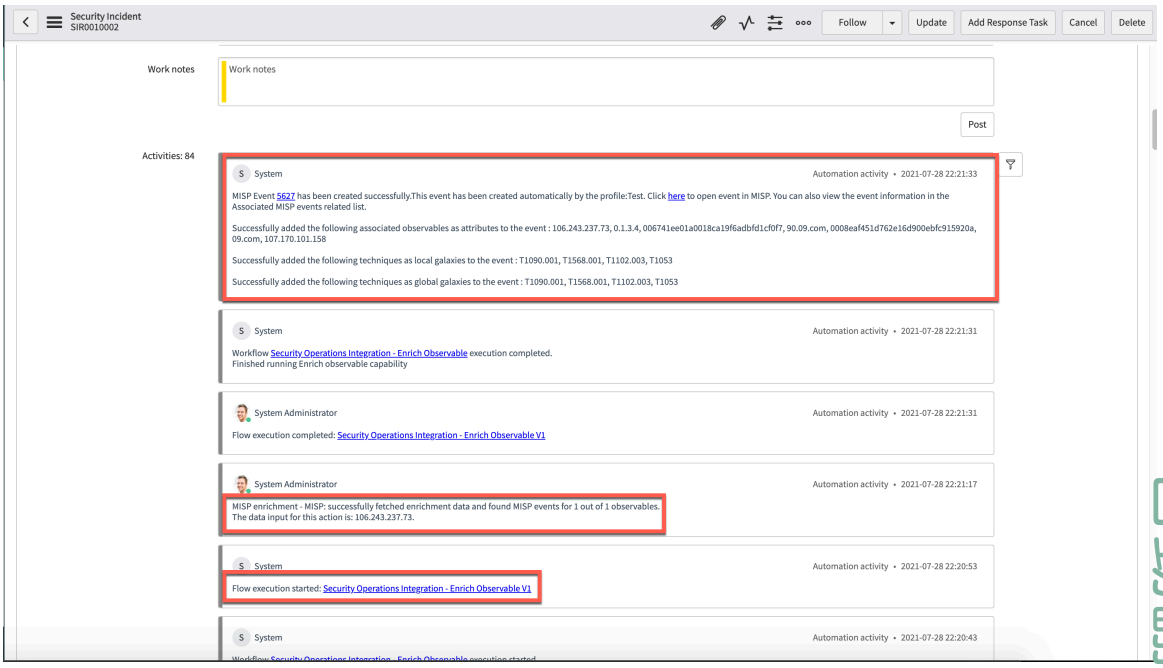
1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. 拡張を実行する観測事象を含んでいるセキュリティインシデントを選択します。
3. [すべての関連リストを表示] と [関連する観測事象 **(Associated Observables)]** タブをクリックします。
4. [アクション] メニューから観測事象を選択し、[観測事象の拡張を実行] をクリックします。
   サイティング検索では複数の観測事象を選択できます。
   [観測事象の拡張を実行] ダイアログボックスが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. MISP ソースを選択し、[選択済み (Selected)] 列で、選択した観測事象を拡張する実装を選択します。
6. **[Submit]** をクリックします。
   作業メモは、[Security Operations Integration - 観測事象を拡張] ワークフローがトリガーされたことを示しています。関連する実装ワークフローによって、拡張が実行されます。セキュリティインシデントの作業メモを表示して、ステータスを確認できます。

   次の例は、手動での観測事象拡張の作業メモを表示する方法を示しています。

   手動での観測事象拡張に関する作業メモ



   拡張メッセージには、作成されたイベントが一覧表示されます。Now Platform または MISP インスタンスでイベントを表示し、[MISP 拡張結果] タブでレコードの詳細を表示できます。

MISP 属性に対するタグの追加または削除

MISP のタグを追加または削除して、イベントや属性を分類します。タグ付けをグローバルに使用して分類を有効にするか、分類中に MISP イベントを変更しない場合はローカルにタグを使用することができます。

始める前に

- 次のものをレビュー MISP ユーザーロールと権限 MISP双方向機能を使用する場合。
- 編集する属性が、MISP ユーザーと同じ組織に属していることを確認します。
- 利用可能なタグとギャラクシーは、MISP ソースとその配布権限に基づくものです。
- 必要なロール：sn_sec_misp.write

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. タグを追加する観測事象、属性、またはイベントを含んでいるセキュリティインシデントを選択します。
3. [すべての関連リストを表示] および [MISP 拡張結果] 関連リストをクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

4. レコードの横にある [プレビュー] アイコン ⓘ をクリックし、[レコードを開く] をクリックします。
   次の例は、**[MISP** 拡張結果] を確認する方法、および MISP 拡張レコードを開く方法を示しています。

   MISP 拡張結果レコード
   MISP 拡張結果レコードを開く

5. MISP 拡張結果レコードを確認します。

MISP 拡張結果

フィールド	説明
観測事象	
イベント	イベントが最初に作成されたとき、または MISP にインポートされたときに、MISP サーバーによってアサインされたイベント ID。 イベントを確認するか、レコードをクリックして、MISP イベントデータページでイベントデータを表示します。
Org	MISP 属性を作成した組織。
カテゴリ	MISP で特定のイベントに追加する属性のカテゴリ。内部参照、ネットワークアクティビティ、金融詐欺などのオプションを選択できます。
タイプ	MISP 属性のタイプ。
統合ベンダー	観測事象拡張用のデータを提供する統合ベンダー。
作成日 (MISP)	イベントが最初に作成された、または MISP にインポートされた日付。
IDS	SIR で観測事象が悪意があるとしてマークされているかどうかのステータス。MISP の対応する属性も true としてマークされます。
配布	公開後にこのイベントを表示できるユーザーなど、配布オプションを制御できます。このオプションは、イベントを他のサーバーに同期するかどうかも制御します。属性によって配布が受け継がれ、最も制限の多い設定が優先されます。配布オプションは次のとおりです。 ○ [自分の組織のみ (Your organization only)]：組織のメンバーのみがこのイベントを表示できるようにします。イベントは、組織のメンバーの 1 人が別のインスタンスにプルして、組織だけが閲覧できるようにすることができます。この設定のイベントは同期されません。 ○ [このコミュニティのみ (This community only)]：自分の組織、この MISP サーバー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	上の組織、およびこのサーバーと同期する MISP サーバーを実行している組織を含む、MISP コミュニティの一員であるユーザーがイベントを表示できるようにします。これらのリンクサーバーに接続されている他の組織は、イベントの表示が制限されます。 ○ [接続されたコミュニティ]：この MISP サーバー上のすべての組織、このサーバーと同期する MISP サーバー上のすべての組織、および 2 ホップ離れたサーバーに接続するサーバーのホスト組織など、MISP コミュニティの一員であるユーザーがイベントを表示できるようにします。2 ホップ離れた、リンクサーバーに接続されている他の組織は、イベントの表示が制限されます。 ○ [すべてのコミュニティ]：すべての MISP コミュニティとイベントを共有し、イベントを自由に利用できるようにします。
MISP イベントへのハイパーリンク	MISP サーバーに保存されている MISP イベントへのリンク。
生データ	観測事象の拡張データレコードの生の詳細。
コメント	属性に追加するコメント。これらのコメントは情報提供のみを目的としており、相関には使用されません。
タグ (ローカル)	ホスト組織の MISP インスタンスで利用可能なタグで、同期とエクスポートのフィルタリングのためのタグ付けを可能にします。ローカルタグを使用しても、MISP イベントは変更されません。これらのタグは、他の MISP インスタンスや共有コミュニティと同期される前に、常に削除されます。
タグ (グローバル)	グローバルで利用可能なタグで、他の MISP インスタンスや共有コミュニティと共有および同期されます。MISP インスタンスにグローバルタグを追加すると、イベントが変更されます。
ギャラクシー (ローカル)	同期とエクスポートのフィルタリングのために、ホスト組織の MISP インスタンスで利用可能なギャラクシーです。ローカルギャラクシーを使用しても、MISP イベントは変更されません。これらのギャラクシーは、他の MISP インスタンスや共有コミュニティと同期される前に、常に削除されます。
ギャラクシー (グローバル)	グローバルで利用可能なギャラクシーで、他の MISP インスタンスや共有コミュニティと共有および同期されます。グローバルギャラクシー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	を追加すると、MISP イベントが変更されます。

6. ローカルタグまたはグローバルタグのいずれかを編集するには、次のオプションのいずれかで、[編集] アイコン をクリックします。

- タグ (ローカル)
- タグ (グローバル)

7. [MISP 属性タグ (MISP Attribute Tags)] ダイアログボックスで、検索して追加するタグの名前を入力します。
8. [タグを **MISP** 属性に更新] をクリックします。

   次の例は、ローカルタグの [編集] アイコンをクリックすることで、C3、アドウェア、C2、およびボットネット 3101 のタグを検索して追加し、MISP サーバーのタグを更新できることを示しています。確認メッセージは、MISP のすべてのタグが更新されたことを示しています。

   MISP 属性のローカルタグを追加する
   MISP サーバーでタグが正常に更新されました。
9. レコードの変更を表示するには、成功メッセージで [フォームのリロード] をクリックします。

MISP イベントまたは属性に対するギャラクシーの追加または削除

MISP のギャラクシーを追加または削除して、これらのオブジェクトを MISP のクラスターとして分類し、MISP イベントまたは属性に添付できるようにします。

始める前に

- 次のものをレビュー MISP ユーザーロールと権限 MISP双方向機能を使用する場合。
- ローカルギャラクシーを追加するには、統合を設定したユーザーが、対応する MISP サーバーのホスト組織に属している必要があります。
- 利用可能なタグとギャラクシーは、MISP ソースとその配布権限に基づくものです。
- 必要なロール：sn_sec_misp.write

手順

1. 次のいずれかのオプションで、[編集] アイコン をクリックします。

- ギャラクシー (ローカル)
- ギャラクシー (グローバル)

2. [MISP イベントギャラクシー (MISP Event Galaxies)] ダイアログボックスで詳細を入力します。

[MISP イベントギャラクシー **(MISP Event Galaxies)]** ダイアログボックス

フィールド	説明
イベント ID	イベントが最初に作成されたとき、または MISP にインポートされたときに、MISP サーバーによってアサインされたイベント ID。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
名前空間	ギャラクシーが保存されている名前空間。名前空間を使用して、類似のギャラクシーをグループ化できます。
ギャラクシー	クラスター情報を保存するギャラクシー。
クラスター	ギャラクシー内のクラスターに関する情報。

3. [ギャラクシーを **MISP** 属性に更新 **(Update Galaxies to MISP Attribute)**] をクリックします。
   次の例は、ローカルのギャラクシーの [編集] アイコンをクリックすることで、廃止された名前空間を選択し、[エンタープライズ攻撃 - 攻撃パターン] ギャラクシーを選択して、クラスター情報を追加できることを示しています。ギャラクシー情報が更新されると、成功メッセージが確認できます。

   Now Platform を使用して MISP にギャラクシー情報を追加する

4. レコードの変更を表示するには、成功メッセージで [フォームのリロード] をクリックします。

タスクの結果
MISP サーバーでギャラクシー情報が正常に更新されました。

MISP 属性にコメントを追加する

MISP 属性にコメントを追加します。追加するコメントは情報提供のみを目的としており、MISP データの相関には使用されません。

始める前に

- 次のものをレビュー MISP ユーザーロールと権限 MISP双方向機能を使用する場合。
- 編集する属性が、MISP ユーザーと同じ組織に属していることを確認します。
- 必要なロール：sn_sec_misp.write

手順

1. [コメント] フィールドの [編集] アイコン をクリックします。
2. [属性コメント] フィールドにコメントを入力します。
3. [コメントを **MISP** 属性に更新] をクリックします。
   次の例は、[コメント] フィールドの隣にある [編集] アイコンをクリックすることで、コメントを追加し、MISP 属性を更新できることを示しています。コメントが更新されると、成功メッセージが確認できます。

   Now Platform を使用して MISP にギャラクシー情報を追加する

4. レコードの変更を表示するには、成功メッセージで [フォームのリロード] をクリックします。

タスクの結果
MISP サーバーでコメントが正常に更新されました。

MISP でイベントを管理する

MISP のイベントは、Now Platform から自動または手動で作成できます。Now Platform から MISP のイベントデータを編集することもできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

MISP で自動作成されたイベントを検証する

Now Platform インスタンスでイベント作成プロファイルを設定した後、自動作成されたイベントを検証できます。

イベントの自動作成プロファイル

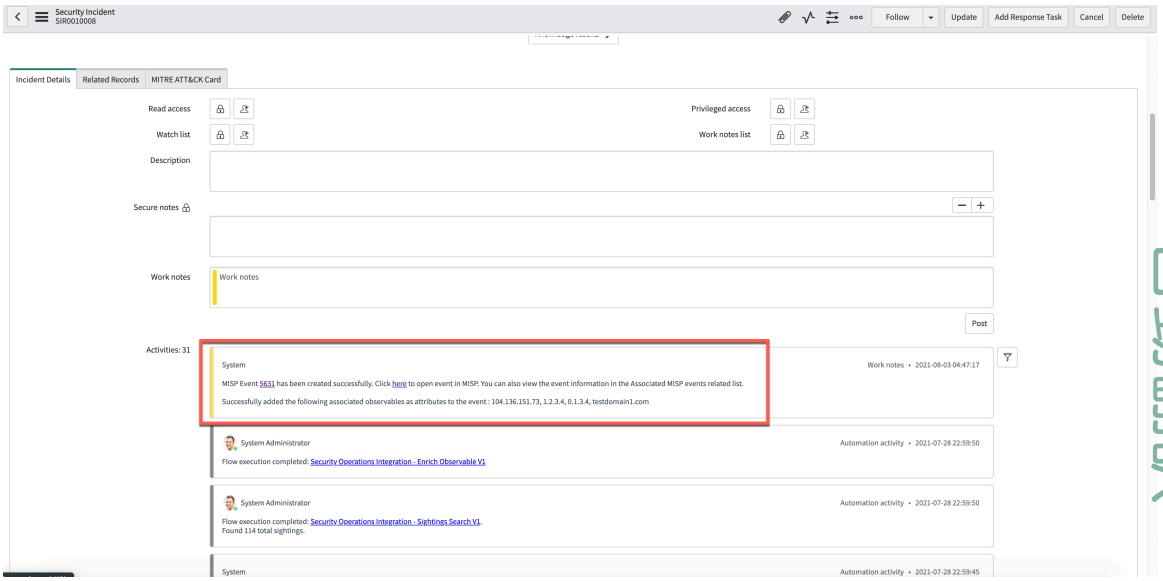
イベントの自動作成プロファイルの構成 は、sn_si.admin または sn_ti.admin ユーザーロールによって行われます。 **MISP** 統合 > イベントの自動作成プロファイル 移動します

MISP イベントデータを表示する

作成されたイベントは、次の方法で表示できます。

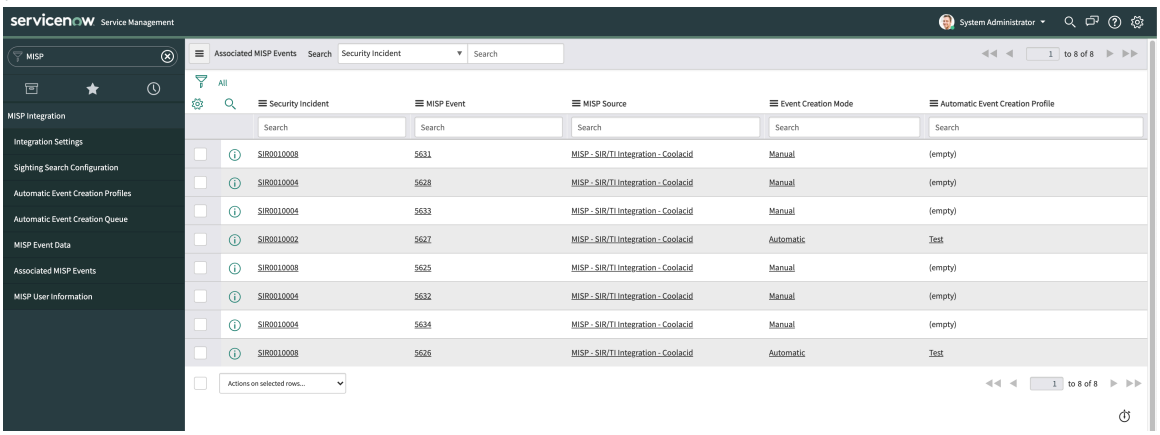
- 作成されたイベントの作業メモを表示します。イベントの詳細は、Now Platform インスタンスの他、次の例に示すように MISP サーバーに表示されたものを見ることもできます。

作成されたイベントの作業メモ



- 関連付けられた MISP イベントの関連リストをクリックします。ここでは、次の例に示すように、セキュリティインシデントと MISP リソースに関連するイベントを表示できます。

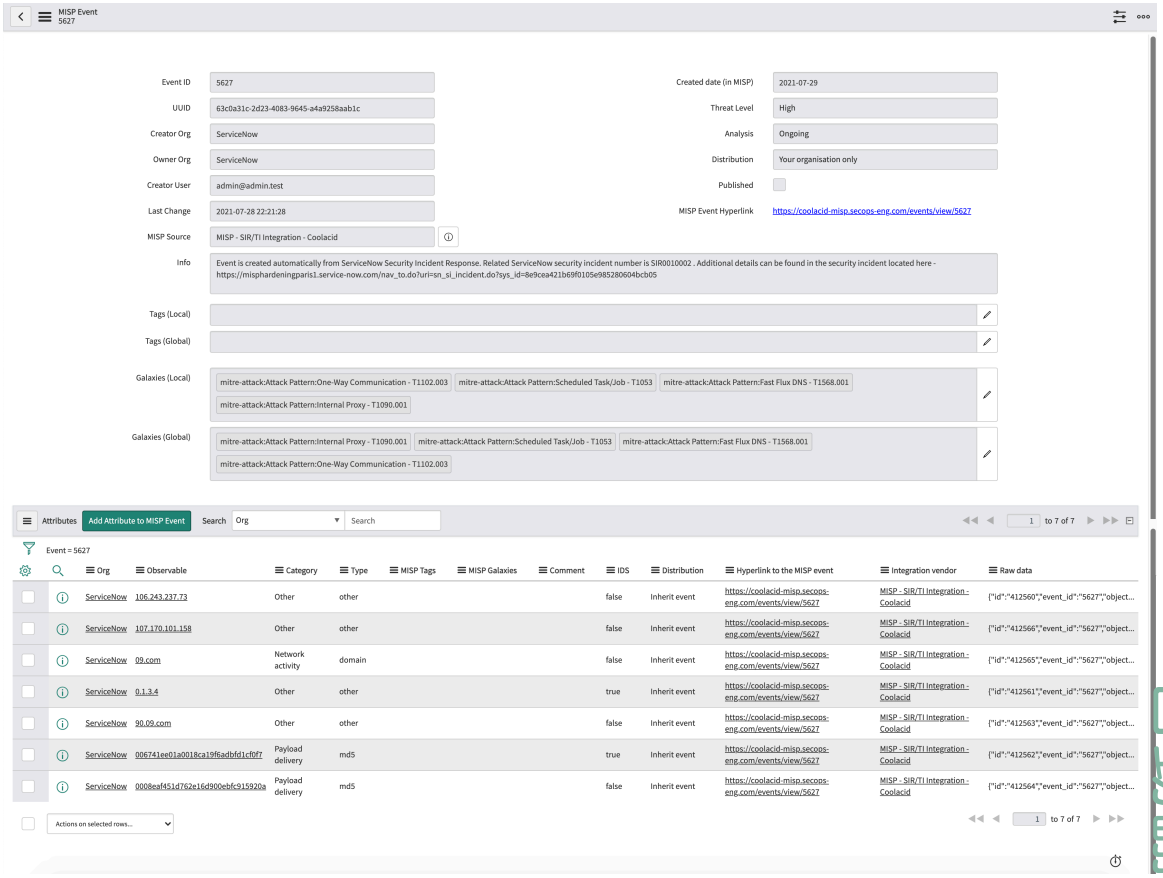
関連イベントのリスト



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 次の例に示すように、フォームビューで MISP イベントデータを表示して、MISP イベントに関する詳細情報を確認します。

フォームビューのイベントデータ



MISP に手動でイベントを作成する

Now Platform から MISP に手動でイベントを作成し、属性やオブジェクトとして表されるコンテキスト関連情報をキャプチャします。

始める前に

- 次のものをレビュー MISP ユーザーロールと権限 MISP双方向機能を使用する場合。
- 必要なロール：sn_sec_misp.write

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. イベントを作成する観測事象を含んでいるセキュリティインシデントを選択します。
3. **[MISP** で新しいイベントを作成] をクリックします。
4. [MISP で新しいイベントを作成] ダイアログボックスで、詳細を入力します。

MISP ダイアログボックスでイベントを作成する

フィールド	説明
日付	MISP でのイベントの作成日。
イベント情報	Now Platform セキュリティインシデントレスポンス から

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	自動的に作成されるイベント情報。
脅威レベル	イベントのリスクレベル。インシデントは、3 つの異なる脅威のカテゴリ (低、中、高) に分類できます。このフィールドは未定義のままでも構いません。オプションは次のとおりです。 ○ 低：一般的な大量マルウェア ○ 中：高度で継続的な脅威 (APT) ○ 高：高度な APT およびゼロデイ攻撃
ソース	イベント作成の MISP ソース。
配布	イベントが公開された後、このイベントを表示できるユーザーを制御するオプション。このオプションは、イベントを他のサーバーに同期するかどうかも制御します。属性によって配布が受け継がれます。最も制限の多い設定が優先されます。配布オプションは次のとおりです。 ○ [自分の組織のみ (Your organization only)]：自分の組織のメンバーのみがこのイベントを表示できるようにします。イベントは、組織のメンバーの 1 人が別のインスタンスにプルして、組織だけが閲覧できるようにすることができます。この設定のイベントは同期されません。 ○ [このコミュニティのみ (This community only)]：自分の組織、この MISP サーバー上の組織、およびこのサーバーと同期する MISP サーバーを実行している組織を含む、MISP コミュニティの一員であるユーザーがイベントを表示できるようにします。リンクサーバーに接続されている他の組織は、イベントの表示が制限されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド		説明
		○ [接続されたコミュニティ]：この MISP サーバー上のすべての組織、このサーバーと同期する MISP サーバー上のすべての組織、および 2 ホップ離れたサーバーに接続するサーバーのホスト組織など、MISP コミュニティの一員であるユーザーがイベントを表示できるようにします。このサーバーから 2 ホップ離れた、リンクサーバーに接続されている他の組織は、イベントの表示が制限されます。 ○ [すべてのコミュニティ]：すべての MISP コミュニティとイベントを共有します。
分析		以下の使用可能なオプションがある、イベント分析の現在のステージ。 ○ 初期：分析を開始したばかりです ○ 進行中：分析中です ○ 完了：分析が完了しました
詳細オプション	MISP イベントに属性として、SIR に関連する観測事象を追加します。	セキュリティインシデントで利用可能な観測事象を、属性として MISP イベントに追加するオプション。 このオプションは、[観測事象の検出結果が悪意のある場合、属性 **IDS** フラグを設定] オプションを有効にします。
	観測事象の検出結果が悪意のある場合、属性 IDS フラグを設定	SIR で悪意があるとしてマークされた観測事象。MISP の対応する属性も True としてマークされます。
	セキュリティタグに基づいて観測事象をフィルタリングする	選択したセキュリティタグに基づいて観測事象をフィルタリングするオプション。このオプションは、脅威インテリジェンスで MISP イベントを区別して管理する機能を提供します。 セキュリティタグ：観測事象をフィルタリングするタグを追加します。たとえば、「共有をブロック」または「TLP：白」というタグを追加する場合、

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド		説明
		いずれかの観測事象にこれらのタグのいずれかが関連付けられていると、MISP イベントの作成時にこれらの観測事象は MISP イベントに属性として追加されません。
	セキュリティインシデントの MITRE ATT&CK 手法をローカルギャラクシーとして MISP イベントに同期	Now Platform SIR セキュリティインシデント MITRE-ATT&CK　テクニックを、MISP イベントのローカルギャラクシーとして同期するオプション。
	セキュリティインシデントの MITER ATT&CK 手法をグローバル Galaxies として MISP イベントに同期	Now Platform SIR セキュリティインシデント MITRE-ATT&CK　テクニックを、MISP イベントのグローバルギャラクシーとして同期するオプション。
	MISP イベントにタグを追加する	ServiceNow から作成されたイベントに MISP タグを追加できるオプション。このオプションでは、次のオプションが表示されます。 ○ ローカル (タグ)：選択したタグは、ローカルタグとして MISP イベントに追加されます。 ○ グローバル (タグ)：選択したタグは、グローバルタグとして MISP イベントに追加されます。

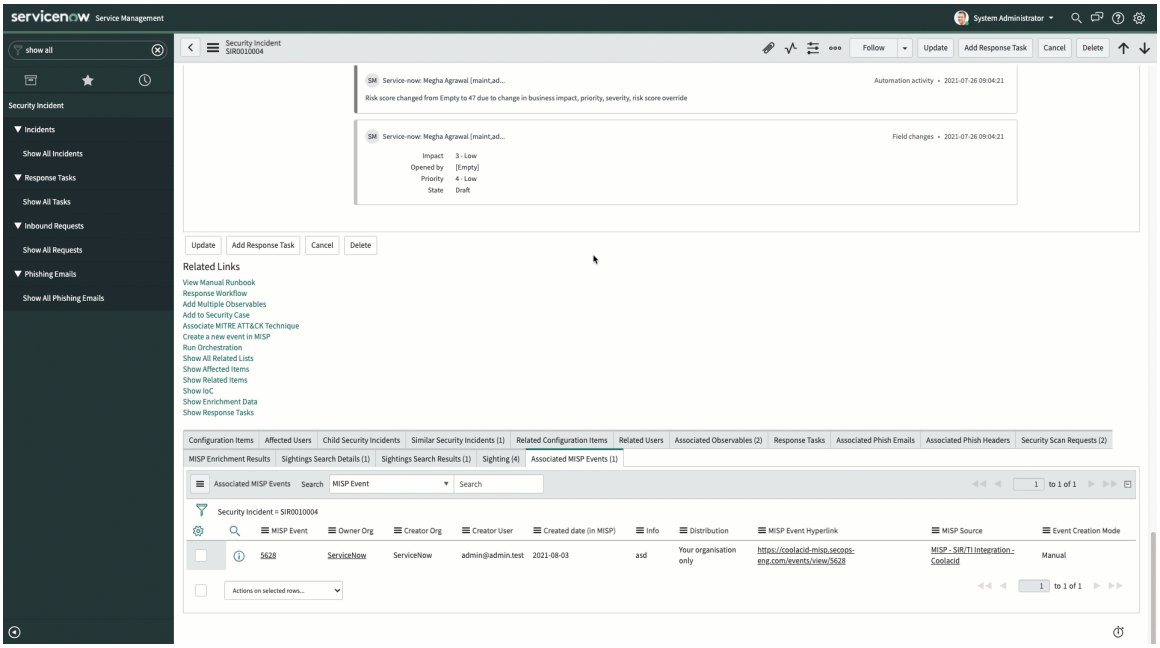
5. [新規 **MISP** イベントを作成] をクリックします。

次の例は、MISP でイベントを作成することで、セキュリティインシデントの結果を表示できることを示しています。次の例に示すように、作業メモ、Now Platform インスタンスのイベント、MISP サーバーのイベントを表示することもできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Now Platform から MISP でイベントを手動で作成する



結果は、次の方法で表示できます。

- セキュリティインシデントページの上部に成功メッセージが表示されます。イベントの詳細は、Now Platform インスタンスの他、MISP サーバーに表示されたものを見ることもできます。
- 作業メモには、詳細を含む成功メッセージを表示できます。イベントの詳細は、Now Platform インスタンスの他、MISP サーバーに表示されたものを見ることもできます。
- [関連付けられた MISP イベント] の関連リストでは、セキュリティインシデントや MISP リソースに関連するイベントを表示できます。

MISP イベントに属性を追加する

タイプ、カテゴリ、イベントに関するその他のコンテキスト情報など、イベントに属性を追加します。

始める前に

- 次のものをレビュー MISP ユーザーロールと権限 MISP双方向機能を使用する場合。
- 属性を追加または更新するイベントが、MISP ユーザーと同じ組織に属していることを確認します。
- 必要なロール：sn_sec_misp.write

手順

1. 次のように移動する。 **All** (すべて) > **MISP** > 関連付けられた **MISP** イベント.
   セキュリティインシデントの [関連付けられた MISP イベント] の関連リストに移動することもできます。
2. 属性を追加する MISP イベントをクリックします。
3. **[MISP** イベントに属性を追加] をクリックします。
4. [イベントに属性を追加] ダイアログボックスで、詳細を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[イベントに属性を追加] ダイアログボックス

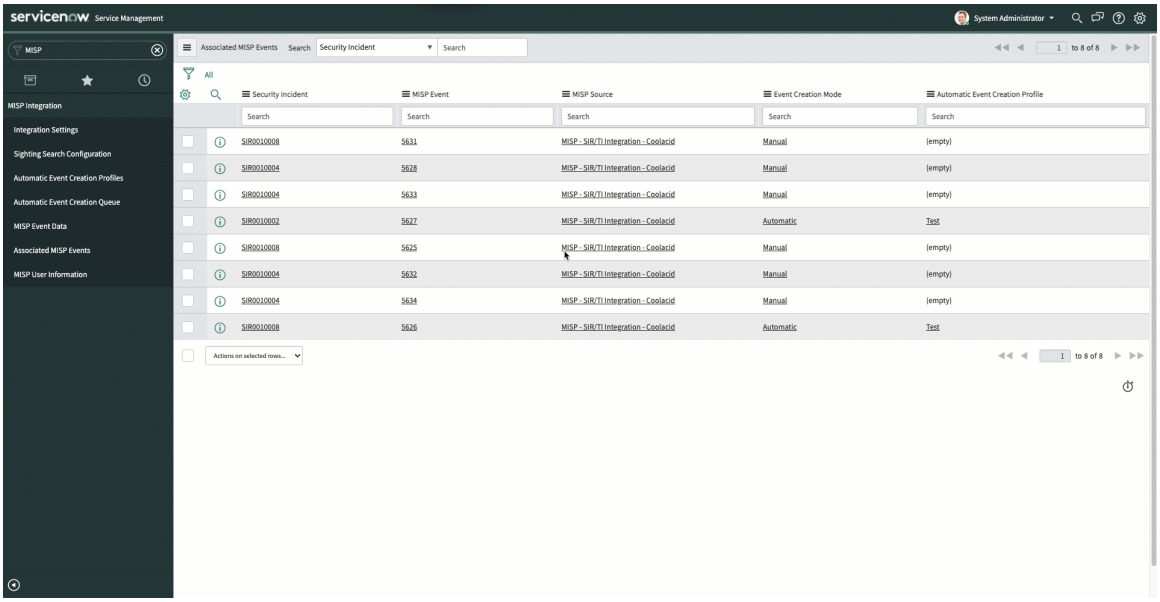
フィールド	説明
値	属性の実際の値。選択した属性タイプに有効とされるものに基づいて、値に関するデータを入力します。たとえば、ip-src (ソース IP アドレス) のタイプの属性の場合、11.11.11.11 が有効な値です。 **注:** イベントとコンテキストを共有する属性または観測事象のみを選択できます。観測事象が既に MISP の属性を持っていることはできません。
カテゴリ	属性のカテゴリ。カテゴリは、この属性に対するマルウェアの様相を示します。たとえば、マルウェアやネットワークアクティビティの永続化メカニズムが挙げられます。
タイプ	カテゴリを説明するタイプ。たとえば、攻撃者が IP アドレスを使用して攻撃する場合、送信元メールアドレスや添付ファイルで送信されたファイルは、すべてマルウェアのペイロード配信を表すことができます。これらのタイプの属性には、ペイロード配信というカテゴリがあります。
配布	この属性を表示できるユーザー。属性によって配布が受け継がれます。最も制限の多い設定が優先されます。
属性を IDS 署名として使用	SIR で悪意があるとしてマークされた観測事象。MISP の対応する属性も true としてマークされます。
コメント	属性に追加するコメント。

次の例は、[関連付けられた MISP イベント] の関連リストから移動することによって、イベントレコード 5627 を表示し、イベントに属性を追加できることを示しています。属性には、値 (testdomain.com)、外部分析としてのカテゴリ、ドメインタイプが含まれます。IDS を有効にすることもできます。イベントレコードの成功メッセージは、次の例に示すように、 属性がイベントに追加されたことを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MISP イベントに属性を追加する



5. **[MISP** イベントに属性を追加] をクリックします。

タスクの結果
追加された属性は [属性] セクションで表示できます。

MISP イベントにタグを追加する

Now Platform MISP にタグを追加して、イベントや属性を分類します。タグ付けをグローバルに使用して分類を有効にするか、分類中に MISP イベントを変更しない場合はローカルにタグを使用することができます。

始める前に

- 次のものをレビュー MISP ユーザーロールと権限 MISP双方向機能を使用する場合。
- 編集するイベントが、MISP ユーザーと同じ組織に属していることを確認します。
- 利用可能なタグとギャラクシーは、MISP ソースとその配布権限に基づくものです。
- 必要なロール：sn_sec_misp.write

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. タグを追加するイベントを含んでいるセキュリティインシデントを選択します。
3. [すべての関連リストを表示] および [MISP 拡張結果] 関連リストをクリックします。
4. エンリッチメント結果のリストからイベント ID をクリックします。
   から移動することもできます **MISP** > 関連付けられた **MISP** イベント 移動します
5. MISP イベントレコードを確認します。

MISP イベントのフォームビュー

フィールド	説明
イベント ID	イベントが最初に作成されたとき、または MISP サーバーにインポートされたとき

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	に、MISP によってアサインされたイベント ID。
UUID	イベントと属性を一意に識別する ID。
作成者組織	MISP インスタンスのイベントを作成した組織。
オーナー組織	MISP インスタンスのイベントを所有する組織。このフィールドはアドミンのみが見ることができます。
作成者ユーザー	MISP でイベントを作成したユーザー
前回の変更	イベントが最後に変更された日付
MISP ソース	イベントが作成された MISP ソース。
作成日 (MISP)	MISP サーバーでイベントが作成された、または最初にインポートされた日付。
脅威レベル	イベントのリスクレベル。インシデントは、3 つの異なる脅威のカテゴリ (低、中、高) に分類できます。このフィールドは未定義のままで構いません。オプションは次のとおりです。 ○ 低：一般的な大量マルウェア ○ 中：高度で継続的な脅威 (APT) ○ 高：高度な APT およびゼロデイ攻撃
分析	以下の使用可能なオプションがある、イベント分析の現在のステージ。 ○ 初期：分析を開始したばかりです ○ 進行中：分析中です ○ 完了：分析が完了しました
配布	個別属性の配布。属性には、イベントとは異なる配布レベルを設定できます。
公開	イベントが公開されているかどうかのステータス。公開すると、対象となるすべてのエクスポートにイベントの属性が使用され、イベントアラートに登録されているユーザーに通知されます。
MISP イベントハイパーリンク	MISP サーバーに保存されている MISP イベントへのリンク。
Info	イベントの簡単な説明。
タグ (ローカル)	ホスト組織の MISP インスタンスで利用可能なタグで、同期とエクスポートのフィルタリングのためのタグ付けを可能にします。ローカルタグを使用しても、MISP イベントは変更されません。ローカルタグは、他の MISP インスタンスや共有コミュニティと同期される前に、常に削除されます。
タグ (グローバル)	グローバルで利用可能なタグで、他の MISP インスタンスや共有コミュニティと共有および同

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	期されます。MISP インスタンスにグローバルタグを追加すると、イベントを変更できます。
ギャラクシー (ローカル)	同期とエクスポートのフィルタリングのために、ホスト組織の MISP インスタンスで利用可能なギャラクシーです。ローカルギャラクシーを使用しても、MISP イベントは変更されません。ローカルギャラクシーは、他の MISP インスタンスや共有コミュニティと同期される前に、常に削除されます。
ギャラクシー (グローバル)	グローバルで利用可能なギャラクシーで、他の MISP インスタンスや共有コミュニティと共有および同期されます。MISP インスタンスにグローバルギャラクシーを追加すると、イベントを変更できます。

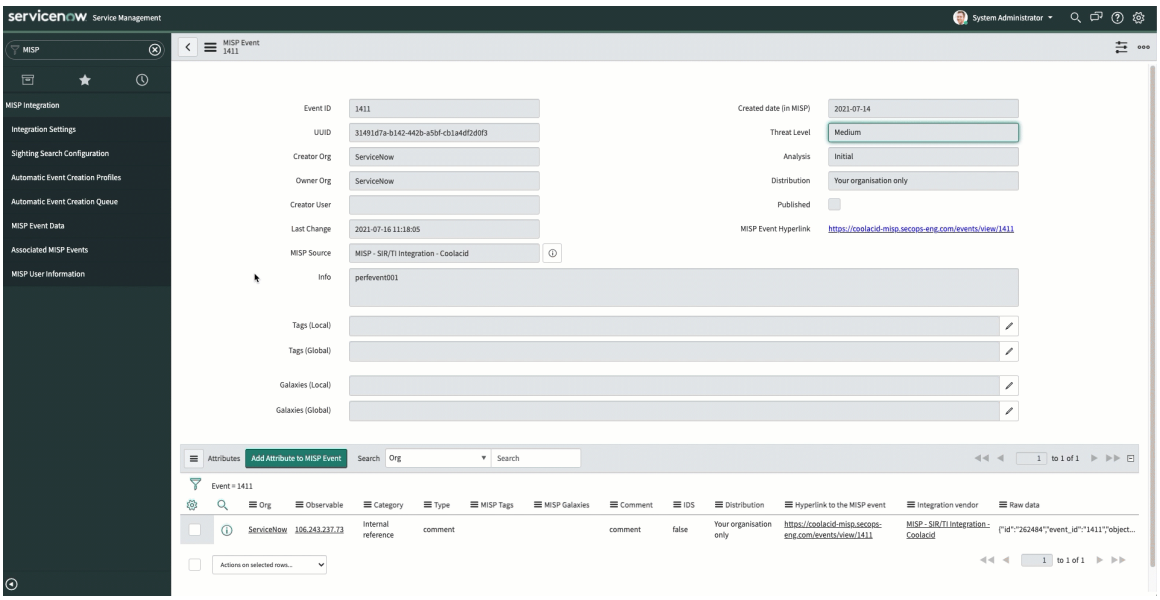
6. ローカルタグまたはグローバルタグのいずれかを編集するには、次のオプションのいずれかで、[編集] アイコン をクリックします。

   - タグ (ローカル)
   - タグ (グローバル)

7. [MISP イベントタグ (MISP Event Tags)] ダイアログボックスで、検索して追加するタグの名前を入力します。
8. [タグを **MISP** イベントに更新 **(Update Tags to MISP Event)**] をクリックします。

   次の例は、ローカルタグの [編集] アイコンをクリックすることで、C3、アドウェア、C2、およびボットネット 3101 のタグを検索して追加し、MISP サーバーのタグを更新できることを示しています。確認メッセージは、MISP のすべてのタグが更新されたことを示しています。

MISP イベントに対するタグの更新



9. 成功メッセージで [フォームのリロード] をクリックして、レコードの変更を表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

タスクの結果
MISP サーバーでタグが正常に更新されました。

MISP イベントまたは属性に対するギャラクシーの更新

Now Platform MISP のギャラクシーを追加または削除して、これらのオブジェクトを MISP インスタンスのクラスターとして分類し、MISP イベントまたは属性に添付できるようにします。

始める前に

- 次のものをレビュー MISP ユーザーロールと権限 MISP双方向機能を使用するために必要です。
- ローカルギャラクシーを追加するには、統合を設定したユーザーが、対応する MISP サーバーのホスト組織に属している必要があります。
- 利用可能なタグとギャラクシーは、MISP ソースとその配布権限に基づくものです。
- 必要なロール：sn_sec_misp.write

手順

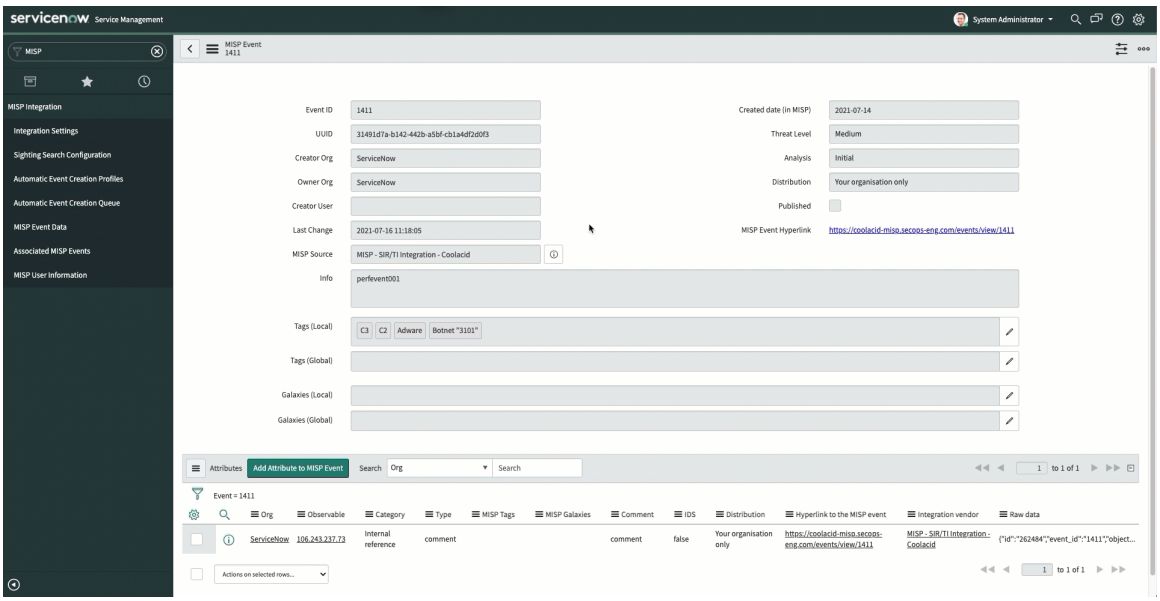
1. 次のいずれかのオプションで、[編集] アイコン をクリックします。

   - ギャラクシー (ローカル)
   - ギャラクシー (グローバル)

2. [MISP イベントギャラクシー (MISP Event Galaxies)] ダイアログで、タグを入力、検索して追加します。
3. [ギャラクシーを **MISP** イベントに更新 **(Update Galaxies to MISP Event)]** をクリックします。

   次の例は、ローカルギャラクシーの [編集] アイコンをクリックし、廃止された名前空間を選択し、[エンタープライズ攻撃 - 攻撃パターン] ギャラクシーを選択して、クラスター情報を追加する方法を示しています。ギャラクシー情報が更新されると、成功メッセージが確認できます。

MISP イベントに対するギャラクシー情報の更新



   MISP サーバーでギャラクシーが正常に更新されました。
4. 成功メッセージで [フォームのリロード] をクリックして、レコードの変更を表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MISP エンリッチメント結果を使用して MITRE-ATT&CK 情報をロールアップする

MISP 情報の自動ロールアップを有効にしていない場合は、MISP 拡張結果を手動でロールアップします。

始める前に
必要なロール：sn_si.analyst

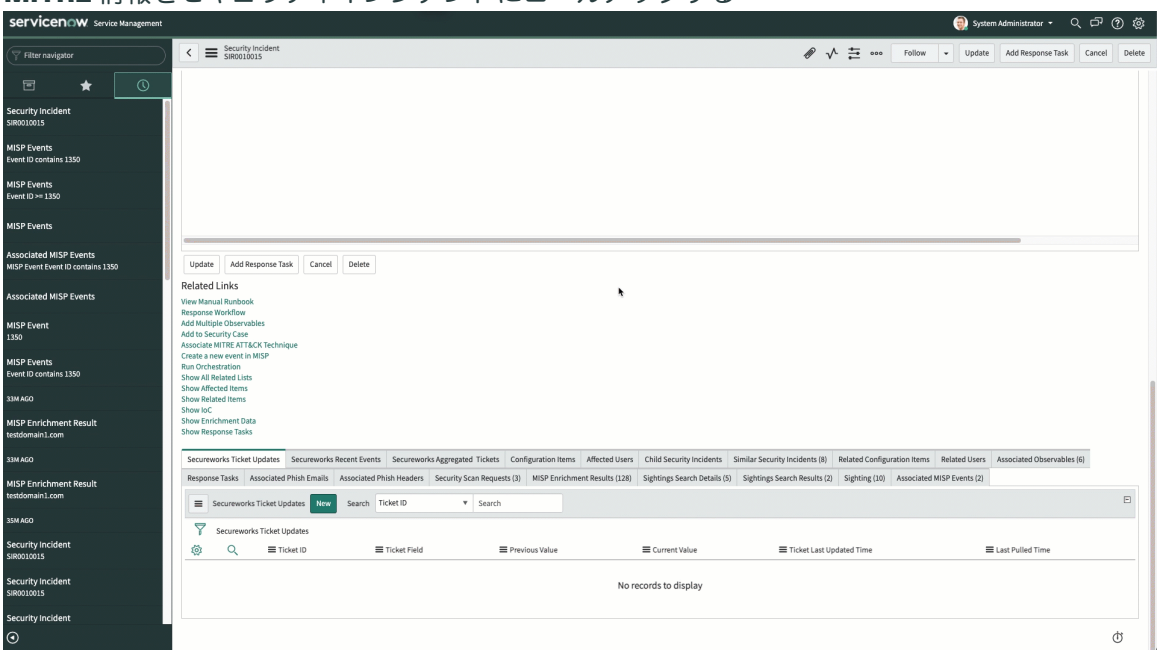
このタスクについて
ベースシステムの自動抽出ルールを使用して、MISP 統合から MITRE-ATT&CK 情報をインポートします。MISP integration for Security Operations は、 MISP - MISP ギャラクシーと MISP タグについて 2 つのベースシステム MITRE-ATT&CK テクニック抽出ルールを導入しています。MITRE-ATT&CK の自動抽出ルールの詳細については、「MITRE-ATT&CK 情報をインポートするための自動抽出テクニックルール」を参照してください。

有効にしている場合 の自動ロールアップ MITRE-ATT&CK を使用した情報 MISP エンリッチメント結果 セキュリティインシデントの場合、情報は自動的にロールアップされます。自動ロールアップを有効にしていない場合、このタスクは手動で行うことができます。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > すべてのインシデントを表示.
2. MITRE-ATT&CK 情報で拡張するセキュリティインシデントを選択します。
3. [すべての関連リストを表示] および **[MISP** 拡張結果] タブをクリックします。
4. 観測事象を選択し、 [アクション] メニューから **[MITRE ATT&CK** 情報を **SI** にロールアップ] をクリックします。
   複数の観測事象を選択して、情報をロールアップできます。
5. 変更を確認するには、[リロード] をクリックします。
   以下の例では、観測事象の選択方法、および MISP エンリッチメント結果のセキュリティインシデントへのロールアップ方法を示しています。

MITRE 情報をセキュリティインシデントにロールアップする



タスクの結果
MITRE-ATT&CK カードを表示して、MISP 拡張結果がセキュリティインシデントにロールアップされていることを確認できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

OPSWAT Metadefender 統合

OPSWAT Metadefender により、サードパーティの Metadefender スキャナーによって検出された脅威データを 脅威インテリジェンス アプリケーションへダウンロードし、追跡、優先順位付け、および解決できます。

探索	セットアップ
• OPSWAT Metadefender 統合の概要 • 脅威インテリジェンス の統合	OPSWAT Metadefender 統合のアクティブ化と構成
使用	**開発**
観測事象のルックアップを実行する	• ServiceNow セキュリティオペレーション 統合開発のガイドライン • 統合を作成するためのヒント • 開発者トレーニング • 開発者ドキュメント • アプリケーションとともにインストールされているコンポーネントの検索
トラブルシューティングとヘルプ	
• 統合のトラブルシューティング • Security Operations Community で質問や回答をする • Known Error Portal で既知のエラー記事を検索 • 連絡先 カスタマーサービス & サポート	

OPSWAT Metadefender 統合の概要

OPSWAT Metadefender は、複数のマルウェア対策マシンへのアクセスを提供し、セキュリティオペレーション と簡単に統合できるセキュリティソリューションです。

OPSWAT Metadefender 統合を使用する前に、プラグインをアクティブ化して統合を構成する必要があります。必要に応じて、X509 SSL 証明書を更新することもできます。

脅威のルックアップ - OPSWAT Metadefender フロー

脅威のルックアップ - OPSWAT Metadefender フローでは、選択された観測事象に対してルックアップが実行されます。観測事象が OPSWAT Metadefender によって認識されるタイプである場合、観測事象でマルウェアがスキャンされ、結果が返されます。

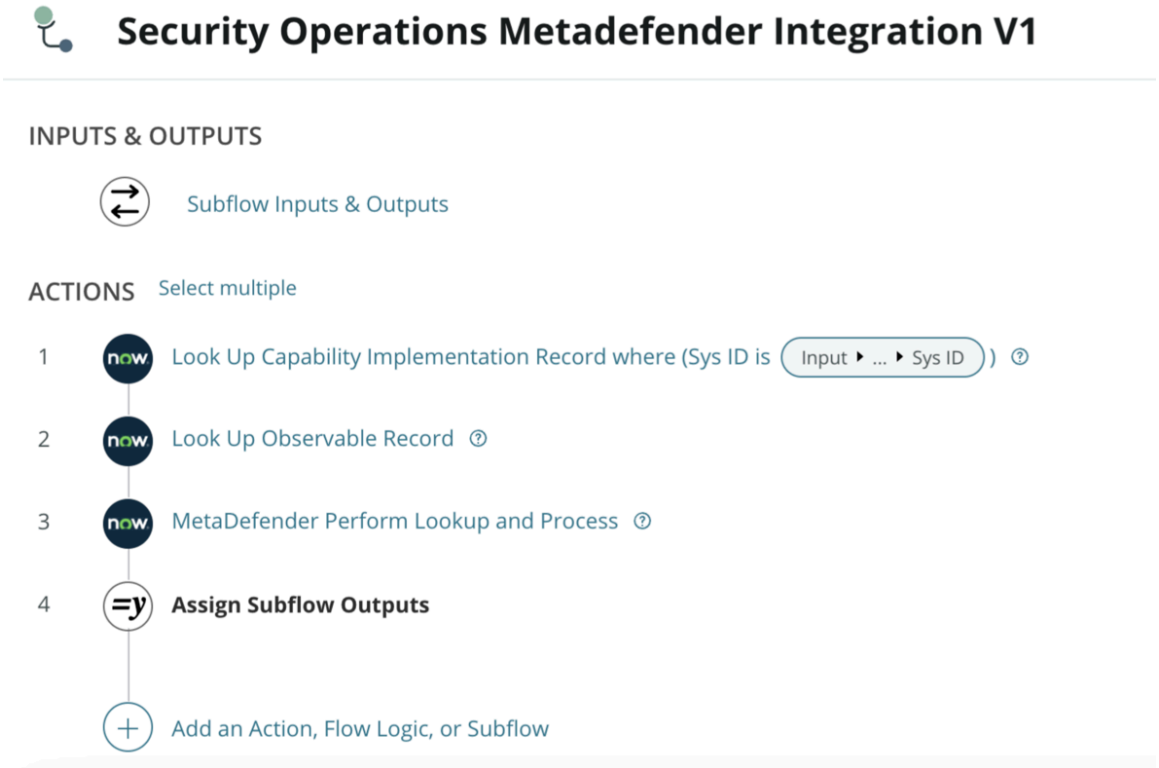
このフローは、1 つ以上の観測事象で脅威のルックアップを実行し、OPSWAT Metadefender の実装が選択されている場合に、[Security Operations Integration - 脅威のルックアップ] 機能 によりトリガーされます。詳細については、「観測事象のルックアップを実行する」を参照してください。

必要なロール：sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

脅威のルックアップ - **OPSWAT Metadefender** フロー



このフローで実行されるアクティビティについて、詳細は「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

OPSWAT Metadefender 統合のアクティブ化と構成

OPSWAT Metadefender 統合を使用する前に、ServiceNow Store からダウンロードする必要があります。

始める前に
必要なロール：admin

手順

1. から統合をダウンロードします ServiceNow Store.
2. 統合が完了したら、OPSWAT ポータルにアクセスし、Metadefender クラウド API キーを取得します。
3. インスタンスで、 セキュリティオペレーション > 統合 > 統合設定.
   利用可能なセキュリティ統合が一連のカードとして表示されます。
4. OPSWAT Metadefender カードで、[構成] をクリックします。
5. OPSWAT ポータルから取得した **API** キーを入力します (または貼り付けます)。
6. **[Submit]** をクリックします。

タスクの結果
設定後、脅威インテリジェンス の観測事象およびセキュリティインシデントの観測事象のルックアップを実行するために OPSWAT Metadefender を選択できます。

関連情報

観測事象のルックアップを実行する

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

X.509 証明書の更新

統合に SSL 接続が必要な場合は、サードパーティベンダーによって提供された証明書が ServiceNow でまだ信頼されていないか、有効期限が切れていることがあります。このタスクはオプションです。

始める前に
必要なロール：admin

手順

1. サードパーティベンダーから SSL 証明書を取得します。
   たとえば、次のように、Firefox ブラウザーの SSL エンドポイントから X.509 証明書 (PEM) をインポートできます。

   a. ブラウザーのアドレスバーにエンドポイント URL を入力します。
      例： `https://<3rdparty>/`。

   b. 住所のロックアイコンをクリックします。

   c. [詳細情報] をクリックし、[セキュリティ] タブをクリックします。

   d. [証明書を表示 **(View Certificate)]** をクリックし、[詳細] タブをクリックします。

   e. [エクスポート] をクリックして、PEM をローカルファイルシステムに保存します。

   f. 保存したファイルをテキストエディターで開き、内容をクリップボードにコピーします。
      `-----BEGIN CERTIFICATE-----` で始まり、`-----END CERTIFICATE-----` で終わる必要があります。

2. 次のように移動する。 システム定義 > 証明書.
3. [新規] をクリックし、統合の新規レコードを作成 します。
4. ダウンロードしてクリップボードにコピーした証明書を **[PEM** 証明書] に貼り付けます。
5. 証明書を ID プロバイダーレコードに追加します。
   a. 次のように移動する。 マルチプロバイダー **SSO** > **ID** プロバイダー.
   b. 新しい証明書を作成したアクティブなデフォルトの ID プロバイダーを選択します。
   c. **[X.509** 証明書] 関連リストまで下にスクロールし、[編集] をクリックします。
   d. 新しく作成した証明書を [選択済み] 列に移動します。
6. [保存] をクリックします。
   レコード内の他のフィールドは自動的に生成されます。

   > **注:**
   > 有効期限が切れた証明書がある場合は、それを削除する必要があります。期限切れの証明書を削除する方法については、「KB0691439 Replacing an expiring SAML certificate (期限切れ間近の SAML 証明書の置き換え)」を参照してください。

VirusTotal 統合

VirusTotal 統合を使用すると、不審な IP アドレス、ファイル、ファイルハッシュ、URL アドレスが悪意のあるものであるかどうかを判断できるように、それらの分析を依頼できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

探索	セットアップ
脅威インテリジェンス の統合	• VirusTotal 統合セットアップ • VirusTotal 統合のアクティブ化と構成
使用	**開発**
• 観測事象のルックアップを実行する • 脅威のルックアップ - VirusTotal ワークフロー	• ServiceNow セキュリティオペレーション 統合開発のガイドライン • 統合を作成するためのヒント • 開発者トレーニング • 開発者ドキュメント • アプリケーションとともにインストールされているコンポーネントの検索

トラブルシューティングとヘルプ

- 統合のトラブルシューティング
- Security Operations Community で質問や回答をする
- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

自動翻訳

VirusTotal 統合セットアップ

VirusTotal は、不審なファイルと URL を分析し、ウイルス、ワーム、トロイの木馬、およびあらゆる種類のマルウェアを迅速に検出する無料のサービスです。セキュリティオペレーション と簡単に統合できます。

VirusTotal 統合を使用する前に、プラグインをアクティブ化して、適切な API キーを追加する必要があります。必要に応じて、X509 SSL 証明書を更新することもできます。

VirusTotal ルックアップソースが使用されているときに、マルウェアが検出されると、観測事象が作成されます。IP ルックアップの場合、IP アドレスを共有する URL の追加リストが作成され、各 URL に対して観測事象が作成されます。

注:

- VirusTotal 統合を実装するには 脅威インテリジェンスプラグインが必要です。
- VirusTotal 統合がバージョン 3 API にアップグレードされました。

VirusTotal 統合のアクティブ化と構成

VirusTotal 統合を使用する前に、ServiceNow Store からダウンロードする必要があります。

始める前に
必要なロール：admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

VirusTotal を使用する前に、脅威インテリジェンス をインストールしてアクティブにする必要があります。VirusTotal 統合がバージョン 3 API にアップグレードされました。

手順

1. から統合をダウンロードします ServiceNow Store.
2. インストールが完了したら、VirusTotal にアクセスし、VirusTotal プロファイルから API キーを取得します。
3. インスタンスで、 セキュリティオペレーション > 統合設定.
   利用可能なセキュリティ統合が一連のカードとして表示されます。
4. VirusTotal カードで、[構成] をクリックします。

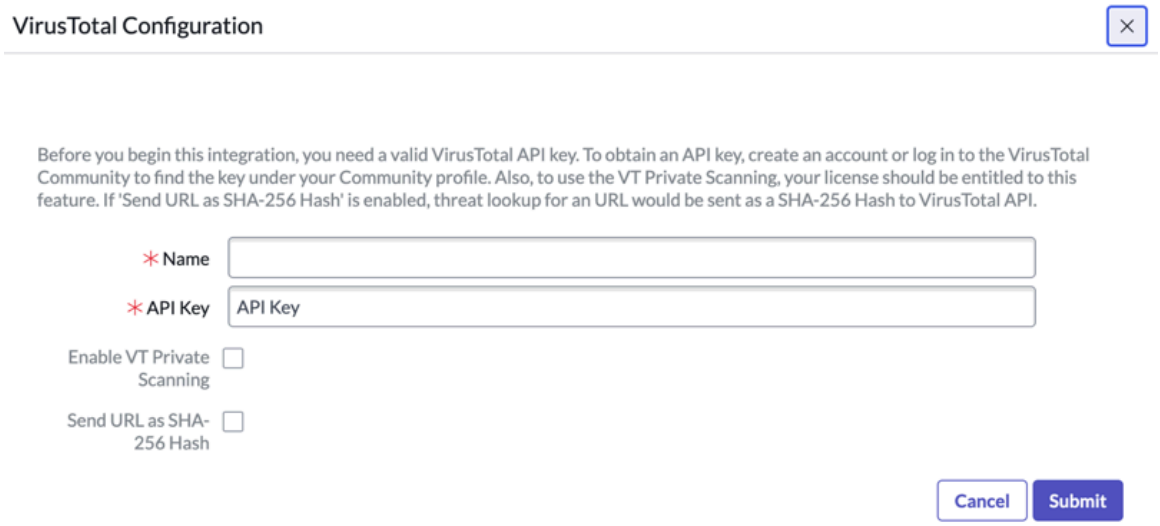
VirusTotal 構成

フィールド	説明
名前	統合の名前。例：VirusTotal。
API キー	VirusTotal サイトから取得した **API** キーを入力します (または貼り付けます)。
VT プライベートスキャンを有効にする	プライバシーを保護する方法で VirusTotal を使用してファイルを分析するには、このチェックボックスをオンにします。このオファリングを介してアップロードされたファイルは、組織外の誰とも共有されず、VirusTotal に短時間だけ残ります。 結果の分析も短期的なものであり、VirusTotal グループにのみ表示されます。 **重要:** VT プライベートスキャンを使用するには、VirusTotal ライセンスにこの機能を付与する必要があります。
URL を SHA-256 ハッシュとして送信	脅威をルックアップするためのハッシュとして URL を送信し、統合時にユーザーのプライバシーを保護するには、このチェックボックスをオンにします。 **注:** 無効にすると、URL は Base64 エンコードとして VirusTotal API に送信されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. [送信] をクリックします。



タスクの結果

設定後、脅威インテリジェンス の観測事象およびセキュリティインシデントの観測事象のルックアップを実行するために VirusTotal を選択できます。

関連情報

観測事象のルックアップを実行する

脅威のルックアップ - **VirusTotal** ワークフロー

脅威のルックアップ - VirusTotal ワークフローは、選択された観測事象に対してルックアップを実行します。観測事象が VirusTotal によって認識されるタイプである場合、観測事象でマルウェアがスキャンされ、結果が返されます。

始める前に

必要なロール：admin

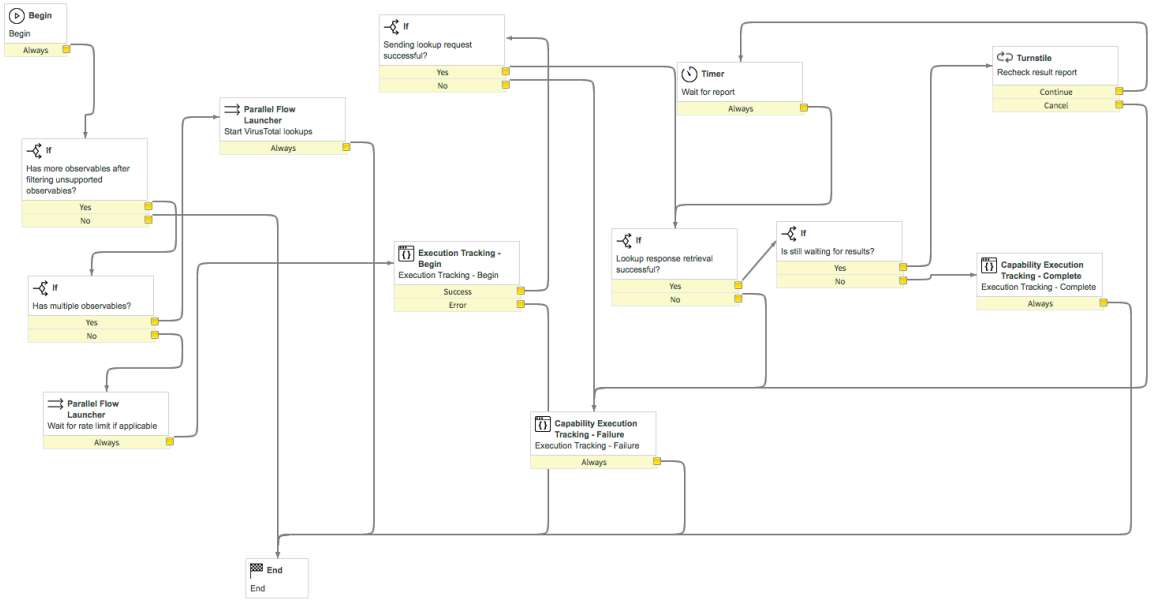
このタスクについて

このワークフローは、1 つ以上の観測事象で脅威のルックアップを実行し、VirusTotal 実装が選択されている場合に [Security Operations Integration - 脅威のルックアップ] 機能 でトリガーされます。詳細については、「観測事象のルックアップを実行する」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威のルックアップ - **VirusTotal** ワークフロー



このワークフローで使用されるアクティビティの詳細については、「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

WhoisXML API 統合

WhoisXML API 統合を使用すると、ドメイン名と URL の Whois ルックアップを送信して、URL 観測事象のコンテキストを取得し、脅威をより適切に判断することができます。

自動翻訳

探索

脅威インテリジェンス の統合

セットアップ

- WhoisXML API 統合セットアップ
- Security Operations Whois 統合のアクティブ化と構成

使用

[脅威インテリジェンス - IoC ルックアップを実行 (Run IoC Lookup)] ワークフロー

開発

- ServiceNow セキュリティオペレーション 統合開発のガイドライン
- 統合を作成するためのヒント
- 開発者トレーニング
- 開発者ドキュメント
- アプリケーションとともにインストールされているコンポーネントの検索

トラブルシューティングとヘルプ

- 統合のトラブルシューティング
- Security Operations Community で質問や回答をする

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(続く)

- Known Error Portal で既知のエラー記事を検索
- 連絡先 カスタマーサービス & サポート

WhoisXML API 統合セットアップ

Whois 統合を使用する前に、プラグインをアクティブ化して、認証情報を追加する必要があります。必要に応じて、X509 SSL 証明書を更新することもできます。

WhoisXML API 統合を実装するには、脅威インテリジェンス と WhoisXML API Integration プラグインが必要です。

Security Operations Whois 統合のアクティブ化と構成

統合構成機能を使用すると、Security Operations Whois 統合を含むサードパーティのセキュリティ統合をすばやくアクティブ化して設定できます。Security Operations Whois 統合を使用する前に、その統合を ServiceNow Store からダウンロードする必要があります。また、WhoisXML API からの有効なアカウントが必要です。

始める前に
Security Operations Whois 統合を使用する前に、脅威インテリジェンス をインストールしてアクティブ化する必要があります。

必要なロール：admin

手順

1. から統合をダウンロードします ServiceNow Store.
2. インストールが完了したら、次に移動します: セキュリティオペレーション > 統合設定.
   利用可能なセキュリティ統合が一連のカードとして表示されます。
3. Whols API カードで、[構成] をクリックします。
4. WhoisXML API アカウントのユーザー名とパスワードを入力します。
5. **[Submit]** をクリックします。

X.509 証明書の更新

統合に SSL 接続が必要な場合は、サードパーティベンダーによって提供された証明書が ServiceNow でまだ信頼されていないか、有効期限が切れていることがあります。このタスクはオプションです。

始める前に
必要なロール：admin

手順

1. サードパーティベンダーから SSL 証明書を取得します。
   たとえば、次のように、Firefox ブラウザーの SSL エンドポイントから X.509 証明書 (PEM) をインポートできます。

   a. ブラウザーのアドレスバーにエンドポイント URL を入力します。
      例： https://<3rdparty>/。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

b. 住所のロックアイコンをクリックします。

c. [詳細情報] をクリックし、[セキュリティ] タブをクリックします。

d. [証明書を表示 **(View Certificate)]** をクリックし、[詳細] タブをクリックします。

e. [エクスポート] をクリックして、PEM をローカルファイルシステムに保存します。

f. 保存したファイルをテキストエディターで開き、内容をクリップボードにコピーします。
`-----BEGIN CERTIFICATE-----` で始まり、`-----END CERTIFICATE-----` で終わる必要があります。

2. 次のように移動する。 システム定義 > 証明書.
3. [新規] をクリックし、統合の新規レコードを作成 します。
4. ダウンロードしてクリップボードにコピーした証明書を **[PEM** 証明書] に貼り付けます。
5. 証明書を ID プロバイダーレコードに追加します。
   a. 次のように移動する。 マルチプロバイダー **SSO** > **ID** プロバイダー.
   b. 新しい証明書を作成したアクティブなデフォルトの ID プロバイダーを選択します。
   c. [X.509 証明書] 関連リストまで下にスクロールし、[編集] をクリックします。
   d. 新しく作成した証明書を [選択済み] 列に移動します。
6. [保存] をクリックします。
   レコード内の他のフィールドは自動的に生成されます。

> **注:**
> 有効期限が切れた証明書がある場合は、それを削除する必要があります。期限切れの証明書を削除する方法については、「KB0691439 Replacing an expiring SAML certificate (期限切れ間近の SAML 証明書の置き換え)」を参照してください。

観測事象を拡張 **WhoIs** ワークフロー

観測事象を拡張 **WhoIs** ワークフローは、選択された観測事象に対して拡張を実行します。観測事象が WhoisXML API Integration で認識されるタイプであれば、拡張できます。

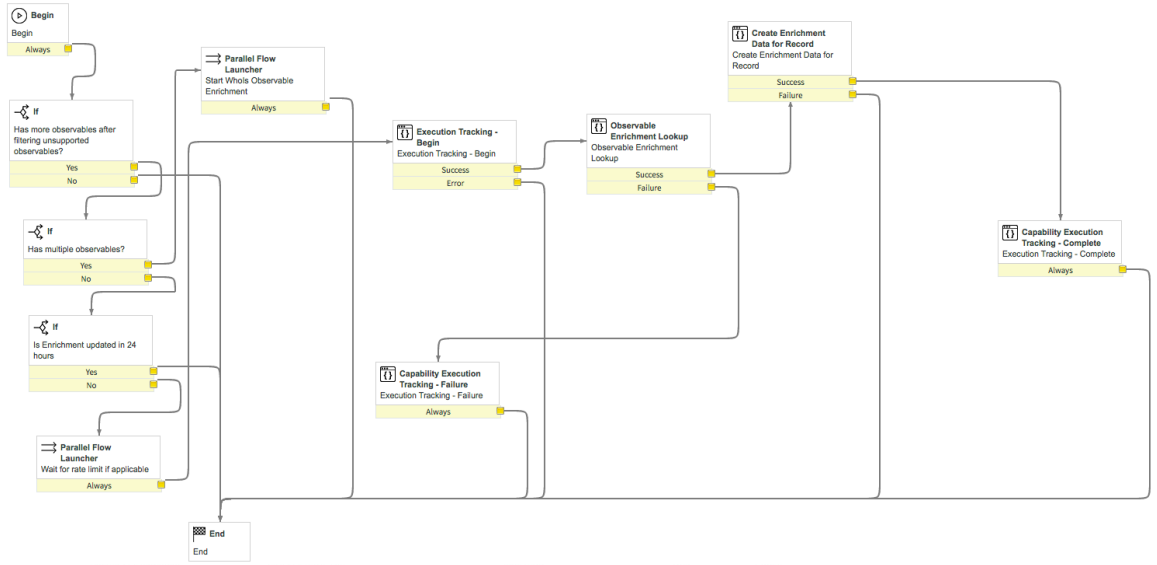
始める前に
必要なロール：admin

このタスクについて
このワークフローは、1 つ以上の観測事象で拡張を実行し、WhoIs 実装が選択されている場合に、Security Operations Integration - [観測事象を拡張] 機能 によりトリガーされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

観測事象を拡張 **WhoIs** ワークフロー



この統合に固有のアクティビティについては、ここで説明します。他のアクティビティの詳細については、「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

[観測事象の拡張ルックアップ] アクティビティ

[観測事象の拡張ルックアップ] ワークフローアクティビティは、観測事象の拡張プロセスを開始します。

[観測事象の拡張ルックアップ] アクティビティを任意の観測事象ワークフローで使用して、拡張を開始できます。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	ルックアップに成功しました。
失敗	ルックアップの実行中にエラーが発生しました。その他のエラー情報は、アクティビティ出力エラーで確認できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

変数	説明
Implementation_id	ルックアップの実行に使用される実装のシステム識別子。
domain_id	ルックアップが実行されているドメインのドメイン識別子。
observable_ids	目的のアクションを実行する 1 つ以上の観測事象。ID はワークフロー入力として使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

変数	説明
capabilityExcutionId	実装ワークフローを開始した機能のシステム識別子。Splunk や Elasticsearch などの統合機能実装ワークフローのみに必要です。
task_sys_id	ワークフローに関連付けられたタスクのシステム識別子。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
response_data	指定されたドメインの実装の API エンドポイントによって返される生データ。
mapping_id	拡張マッピングの識別子。たとえば、WhoIs 統合は、IP と URL の 2 つの異なる形式で、それぞれのマッピング ID を返します。

脅威インテリジェンスオーケストレーション

脅威インテリジェンスオーケストレーション アクティビティによって、ユーザーは、ワークフローオーケストレーションを使用して、他のセキュリティインシデントまたは他のシステムで過去に脅威が確認されたかどうかを判断できます。

セキュリティインシデントレスポンスオーケストレーション ワークフローの編集またはカスタムワークフローの作成の詳細については、「ワークフローの概要」および「ワークフローエディター ワークフローエディター」を参照してください。

脅威インテリジェンスオーケストレーションを設定する

脅威インテリジェンスオーケストレーション を使用する前に、CMDB の入力、MID サーバーの構成、認証情報の構成など、システムのさまざまな部分を設定する手順を実行します。

始める前に

必要なロール：admin
脅威インテリジェンスオーケストレーション を使用するには、ドメイン名が完全に入力された CMDB が必要です。詳細については、次を参照してください： 検出 。

このタスクについて

手順

1. 脅威インテリジェンス プラグインをアクティブ化します。
2. MID サーバーの構成
3. MID サーバーサービスの認証情報の設定
   これで、ワークフロー内で 脅威インテリジェンスオーケストレーション アクティビティを使用する準備ができました。

脅威インテリジェンスオーケストレーションのワークフローとアクティビティ

ベースシステムには、インスタンスでのアクションの自動化に使用できるワークフローとワークフローアクティビティが含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[脅威インテリジェンス - IoC ルックアップを実行 (Run IoC Lookup)] ワークフロー

[脅威インテリジェンス - **IoC** ルックアップを実行 **(Run IoC Lookup)]** ワークフローは、期限切れになっていない観測事象があるかどうかをチェックします。ある場合、ルックアップは [完了 **(Complete)]** に設定され、観測事象のデータで更新されます。

始める前に

必要なロール：sn_si.basic

> **注:**
> このワークフローは、脅威インテリジェンスオーケストレーション ビジネスルール ([既存の **IoC** テーブルを入力する **(Populate with existing IoC tables)] [** ルックアップをキューに入れる **(Queue the lookup)]**、および [観測事象を更新 **(Update observable)]**) をアクティビティに置き換えます。

ルックアップが挿入または更新され、条件を満たすと、ルックアップビジネスルールによってこのワークフローがトリガーされます。

このタスクについて

[脅威インテリジェンス - **IoC** ルックアップを実行 **(Run IoC Lookup)]** ワークフローは、期限切れになっていない観測事象があるかどうかをチェックします。ある場合、ルックアップは [完了 **(Complete)]** に設定され、観測事象のデータで更新されます。観測事象に関連付けられているインジケーターが再アクティブ化されます。

観測事象が期限切れの場合、ワークフローはルックアップを実行し、既存の期限切れの観測事象の [サイティング回数 **(Sighting count)]** を増やします。

相関する観測事象が存在しない場合、インジケーターがある新しい観測事象が作成されます。

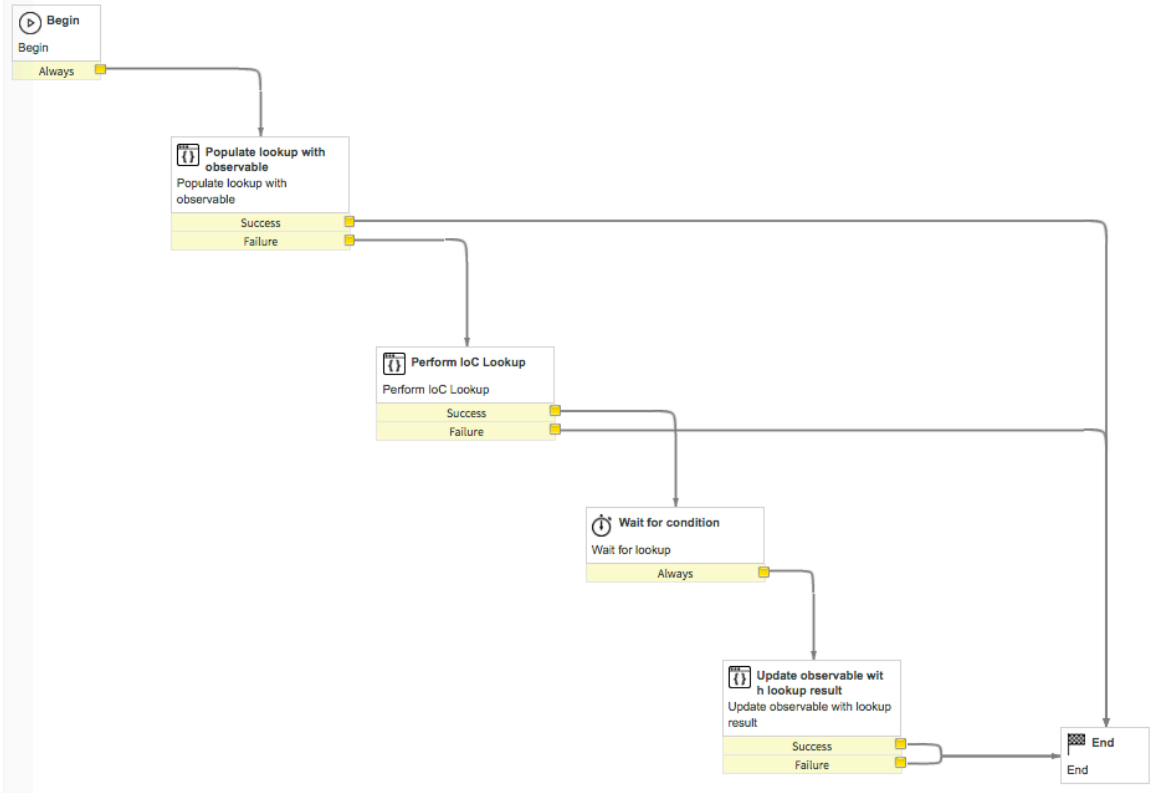
ワークフロープロセスアクティビティには次のものが含まれます。

- 観測事象アクティビティをルックアップに入力する
- IoC ルックアップアクティビティを実行する
- ルックアップ待ち (主要なアクティビティ)
- [ルックアップ結果によって観測事象を更新] アクティビティ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[脅威インテリジェンス - **IoC** ルックアップを実行 **(Run IoC Lookup)]** ワークフロー



観測事象アクティビティをルックアップに入力する

期限切れになっていない観測事象が見つかった場合、 [脅威インテリジェンスオーケストレーション - 観測事象をルックアップに入力] ワークフローアクティビティが既存の観測事象からのデータをルックアップに入力します。このアクティビティにより、調査と修復のプロセスを迅速化できます。

ワークフローによってトリガーされると、[観測事象をルックアップに入力] は、入力としてアクティビティに提供されたルックアップの [値] と [タイプ] に一致するルックアップに対して、既存の観測事象の検索を試行します。

観測事象が存在し、期限切れになっていない場合、このアクティビティは次を実行します。

- 観測事象で見つかった情報でルックアップを更新します。
- インジケーターが非アクティブの場合は再アクティブ化し、[発生回数]を増加させ、[最終確認日] の日付を更新します。
- [ステータス] を [完了 (Complete)] に設定します。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

入力変数	説明
scanID[文字列]	ルックアップ識別子

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数	説明
true	有効な観測事象と更新されたルックアップが見つかりました。
False	有効な観測事象が見つかりませんでした。観測事象がないか、期限切れです。

IoC ルックアップアクティビティを実行する

[脅威インテリジェンスオーケストレーション - **IoC** ルックアップを実行] ワークフローアクティビティは、指定されたルックアップを実行します。このアクティビティにより、調査と修復のプロセスを迅速化できます。

ワークフローによってトリガーされると、**[IoC** ルックアップを実行] は scanID を取得してルックアップレコードを検索し、ルックアップキューエントリーを作成してキューにルックアップ追加します。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

入力変数

変数	説明
scanID[文字列]	ルックアップ識別子

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
true	ルックアップをトリガーしました。
False	ルックアップをトリガーしませんでした。

[ルックアップ結果によって観測事象を更新] アクティビティ

[脅威インテリジェンスオーケストレーション - ルックアップ結果によって観測事象を更新] ワークフローアクティビティが観測事象レコードを更新します。存在しない場合は、新しい観測事象が作成されます。このアクティビティは、情報の記録に有効です。

ワークフローによってトリガーされると、[ルックアップ結果によって観測事象を更新] は、新しい [サイティング回数 **(Sighting count)]** を含めるように既存の観測事象を更新し、メモを追加し、非アクティブな場合はインジケーターを再アクティブ化します。インジケーターの [発生回数] および [最終確認日] の日付も更新されます。

相関する観測事象が存在しない場合、ワークフローは次のようにインジケーターを使用して新しい観測事象を作成します。

- IoC ルックアップを実行します
- 新しい観測事象を作成します
- 観測事象のインジケーターを作成します
- 観測事象に [サイティング回数 **(Sighting count)]** を追加します

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- インジケーターに [発生回数] および [最終確認日] の日付を追加します
- ルックアップの作成元を示すメッセージを追加します

。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

入力変数

変数	説明
scanID[文字列]	ルックアップ識別子

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
true	観測事象の更新または作成に成功しました。
False	観測事象の更新または作成に失敗しました。

[デフォルトの **IoC** ルックアップソースを実行] アクティビティ

脅威インテリジェンス - [デフォルトの **IoC** ルックアップソースを実行] は、ワークフローによってトリガーされると、ルックアップ要求 ID を取り込み、入力されたデータ値に応じて複数のルックアップを作成します。

データタイプごとに、各ルックアップソースのサポートされているルックアップタイプテーブルの **[include_in_bulk scan]** 列が評価されます。true の場合、ルックアップがルックアップ要求に追加されます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

入力変数

変数	説明
scan_request_id	ルックアップ要求システムの識別子

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
スキャン作成数	整数

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Security Case Management

セキュリティケース管理 は、脅威ハンティングに取り組んでいるセキュリティアナリストが、環境における不審なアクティビティに関する情報をコレクションする手段を提供します。セキュリティインシデント、観測事象、CI、影響を受けるユーザーなどのケースに関連したレコードをケースに追加して、広範かつ具体的な分析に対応できます。

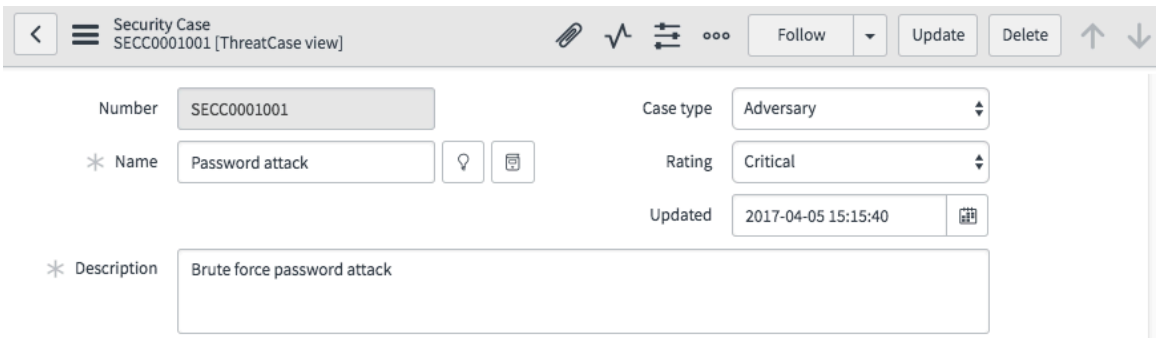
レコードや関連情報を簡単にピボットできるため、アナリストはターゲットキャンペーンや高度で継続的な脅威などに直面しているかどうかを評価できます。

セキュリティケースは、セキュリティケース管理、セキュリティインシデントレスポンス、脅威インテリジェンス など、インスタンスのさまざまなソースから作成できます。また、構成アイテム [cmdb.ci] テーブルおよびユーザー [sys.user] テーブルにある構成アイテムおよび影響を受けるユーザーから、それぞれケースを作成することもできます。ケースを作成した後、これらの各ソースを使用して、既存のケースに貴重な分析リソースを追加することもできます。

各セキュリティケースは、ヘッダーセクション、その他のケース詳細を含むセクション、および特定の脅威を識別して対処するための論拠をビルドするのに役立つレコードコレクションを含むケースアーティファクトセクションの 3 つの主要セクションで構成されています。

ケースヘッダー

ケースヘッダーセクション



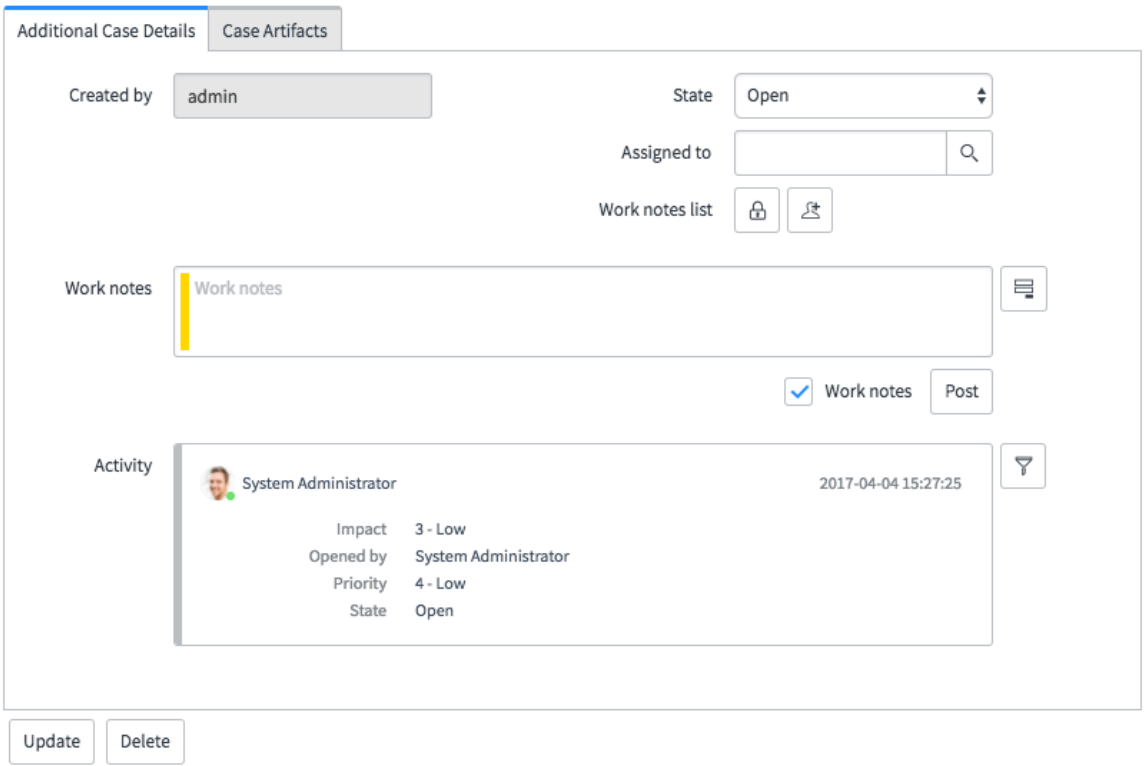
ケースヘッダーは、セキュリティケースの識別と分類に使用される基本情報を提供します。ケース番号には、SECC プリフィックスが使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

その他のケース詳細

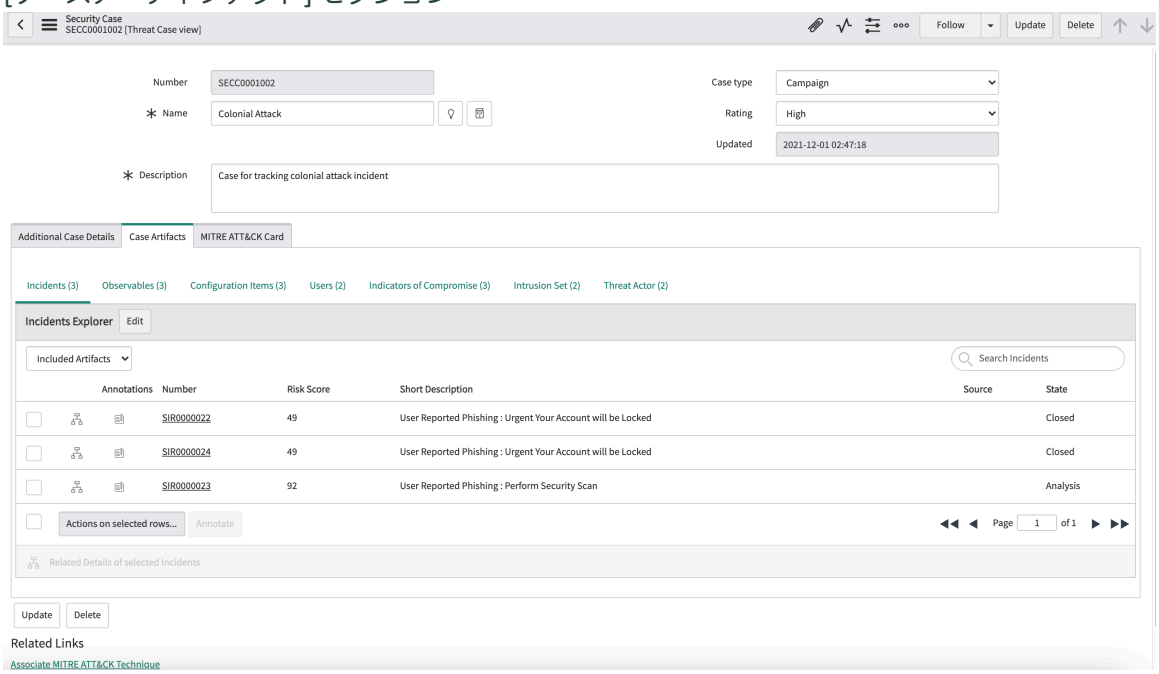
[その他のケース詳細] セクション



[その他のケース詳細] セクションには、現在のステータス、ケースについて記録された作業メモやアクティビティなどを含む、ケースに対して既に実行済みの分析に固有の情報が表示されます。

ケースアーティファクト

[ケースアーティファクト] セクション



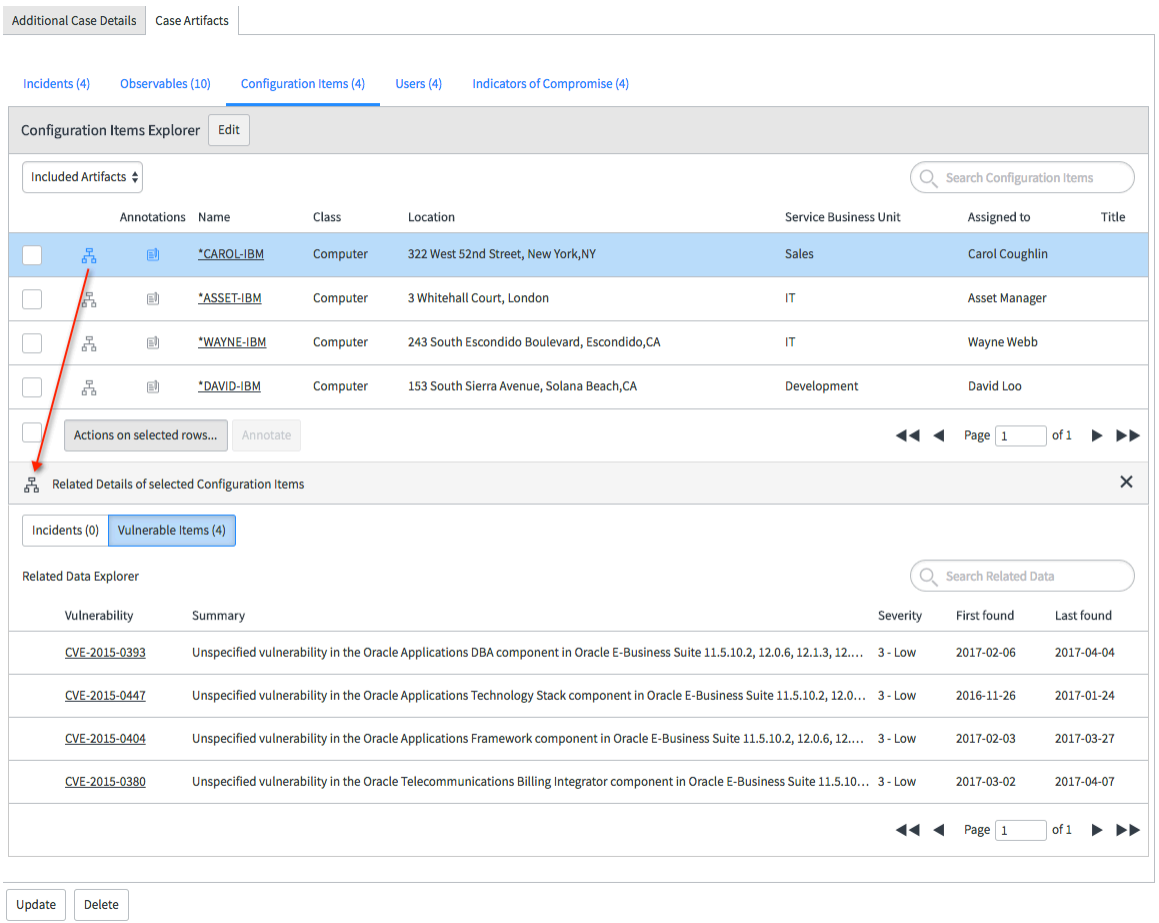
[ケースアーティファクト] セクションには、セキュリティケースに含まれる情報の一連のタブがあります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

各タブのコンテンツ内で検索を実行できます。既に安全であると評価したレコードや、調査において重要ではないと判断したレコードを除外することもできます。除外されたレコードは削除されず、非表示になります。必要に応じて、除外されたレコードを表示して再び追加することができます。

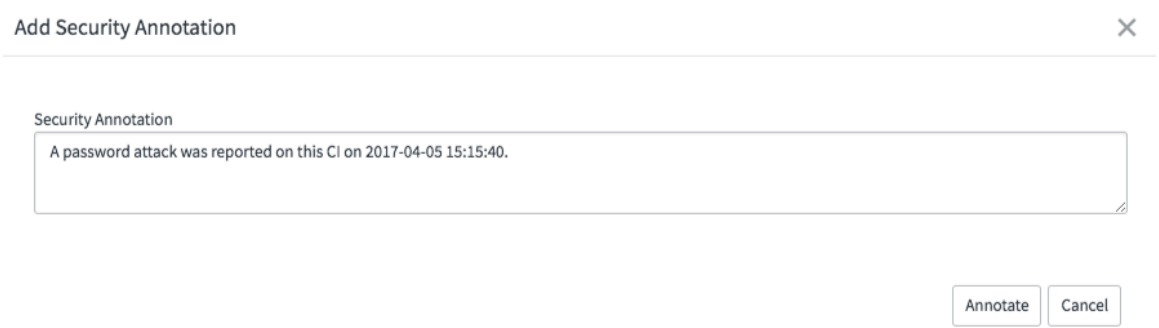
各タブ内で、[その他の詳細] アイコンをクリックすると、選択したレコードの関連情報を表示できます。たとえば、[構成アイテム] タブをクリックして構成アイテムエクスプローラーを表示し、特定の CI の [その他の詳細] をクリックすると、その CI に関連付けられたインシデント、脆弱性一致アイテム、および注釈を表示できます。

ケースアーティファクト - 関連する詳細



レコードを選択し、ケースに関連するアーティファクトの [注釈] ボタンをクリックして、レコードに注釈を追加することもできます。注釈とは、各アナリストが特定のアーティファクトに付けることができるメモのことです。

セキュリティ注釈



その他、アナリストが各ケースを調査する際に使用できるツールには、次のようなものがあります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ケースで観測事象のサイティング検索を実行する
- セキュリティアーティファクトの検索

Security Case Management でケースを作成する

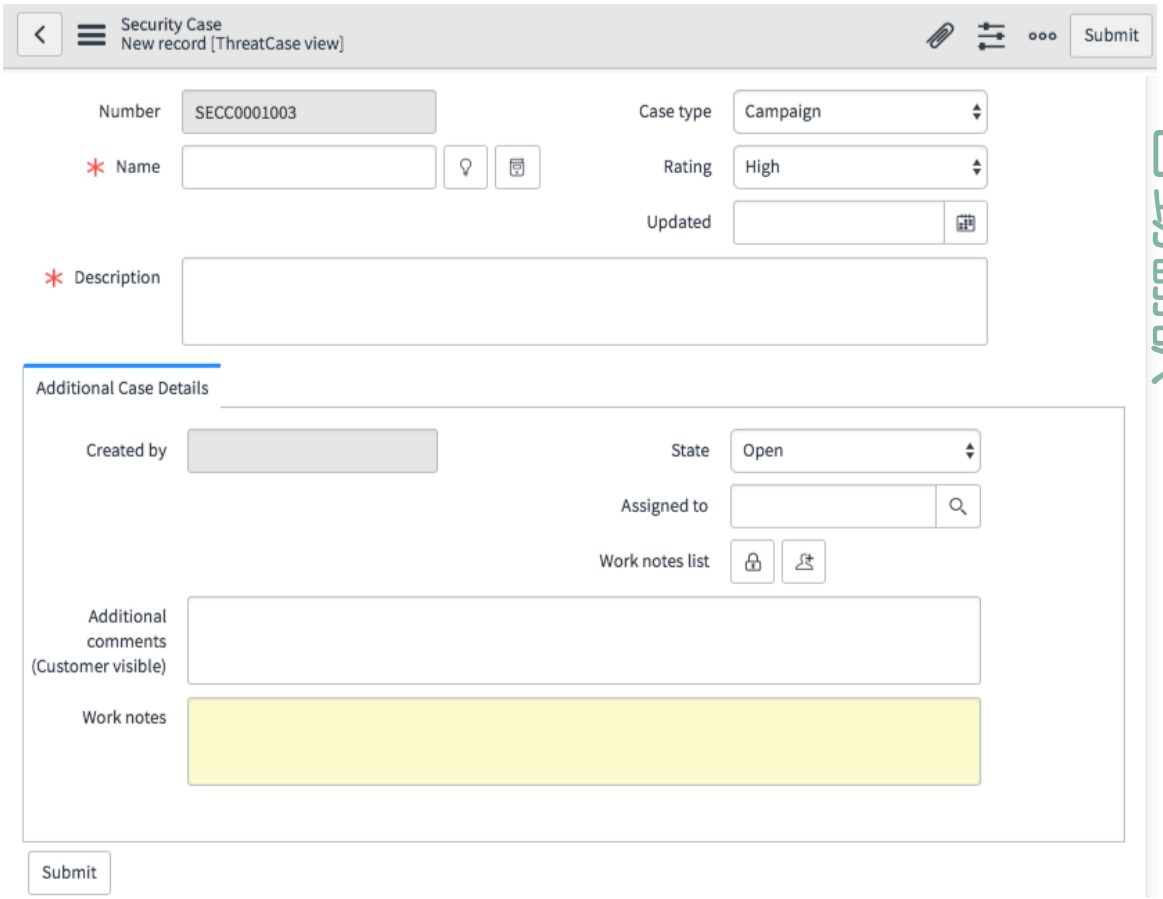
ケースは、組織を脅かすキャンペーンまたは国家に関する情報を追跡するために使用されます。ケースを作成した後、アーティファクトを追加することで、1 つのケースレコード内ですべての関連情報を確認および分析することができます。

始める前に
必要なロール：sn_ti.case_use

r

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > ケースの管理 > すべてのケース.
   [セキュリティケース] リストが開きます。
2. [新規] をクリックします。
   [セキュリティケース] 画面が開きます。



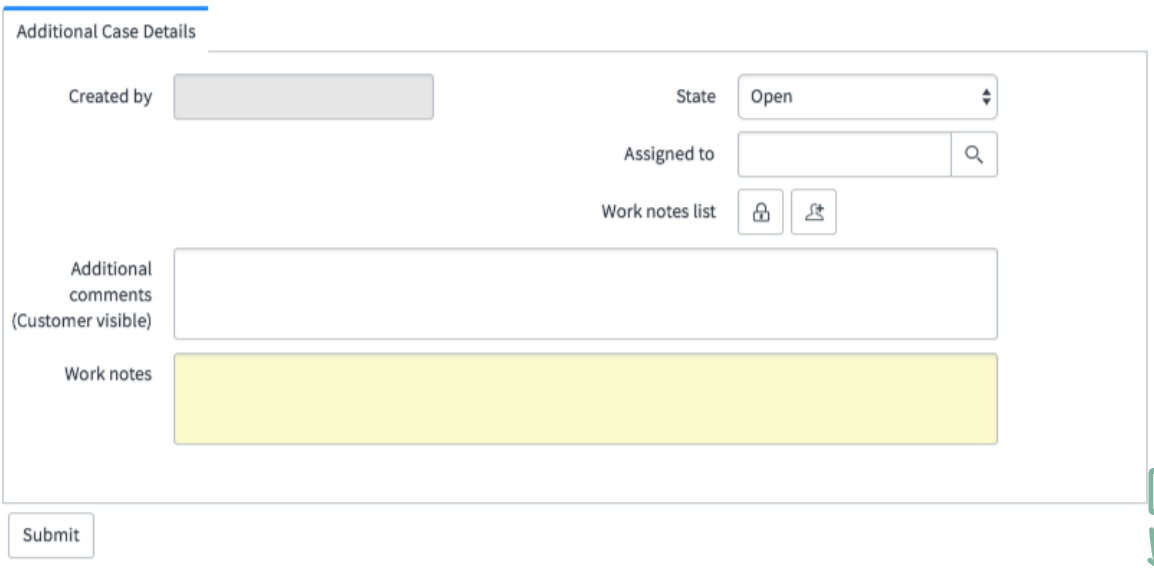
3. 必要に応じてフィールドを入力します。

フィールド	説明
ケース番号	[読み取り専用] ケース番号。
ケース名	ケースの記述名を入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ケースのタイプ	調査対象のケースタイプを選択します。
評価	このケースの重要性を選択します (重大から低)。
最終更新日	[読み取り専用] ケースが更新された最後の日時。
簡単な説明	ケースの簡単な説明です。

4. [その他のケース詳細] タブをクリックします。



5. 必要に応じてフィールドを入力します。

フィールド	説明
作成者	[読み取り専用] このケースを作成したユーザーの名前。
状況	ケースの現在のステータス。ケースの作成時、ステータスはデフォルトで [ドラフト] になっています。
アサイン先	ルックアップアイコンをクリックし、ケースをアナリストにアサインします。
作業メモリスト	ロックアイコンをクリックし、作業メモを表示できる内部ユーザーを追加します。
追加コメント	必要に応じて、顧客に表示されるケースのメモを入力します。
作業メモ	必要に応じて、ケースの作業メモを入力します。

6. **[Submit]** をクリックします。
   レコードが保存された後、[ケースアーティファクト] タブをクリックして、ケースにアーティファクトを追加できます。

ケースにアーティファクトを追加する

ケースを作成したら、セキュリティインシデント、CI、セキュリティ侵害のインジケーターなどのアーティファクトをケースに追加できます。これらのアーティファクトは、ケースを解決する手掛かりとなるものです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

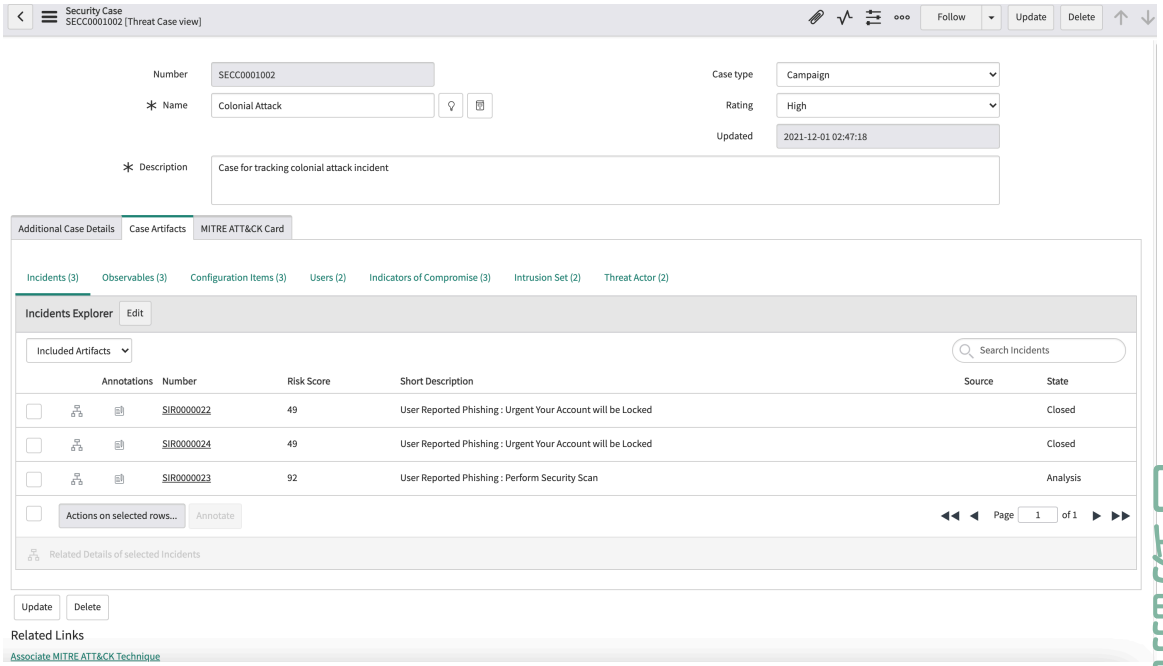
始める前に
セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

必要なロール：sn_ti.case_user_write

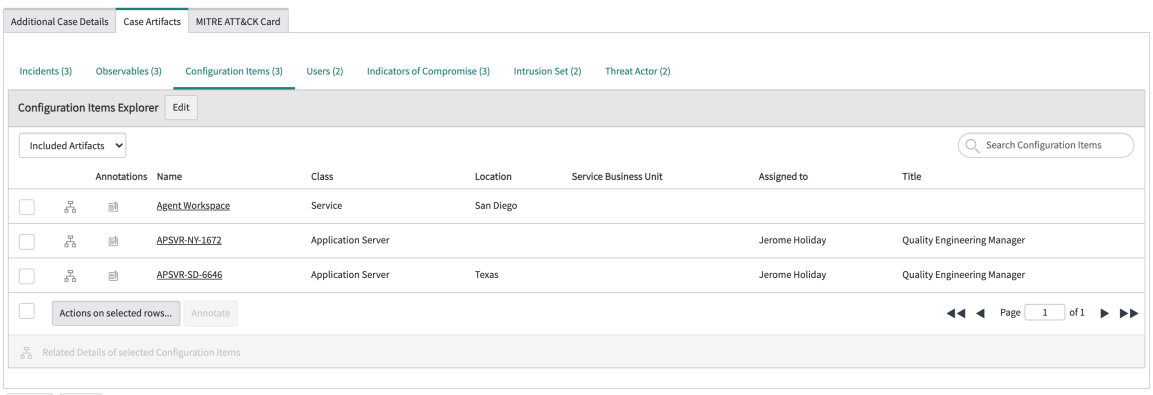
手順

1. アーティファクトを追加するテストケースを開きます。

2. [ケースアーティファクト] の関連リストをクリックします。

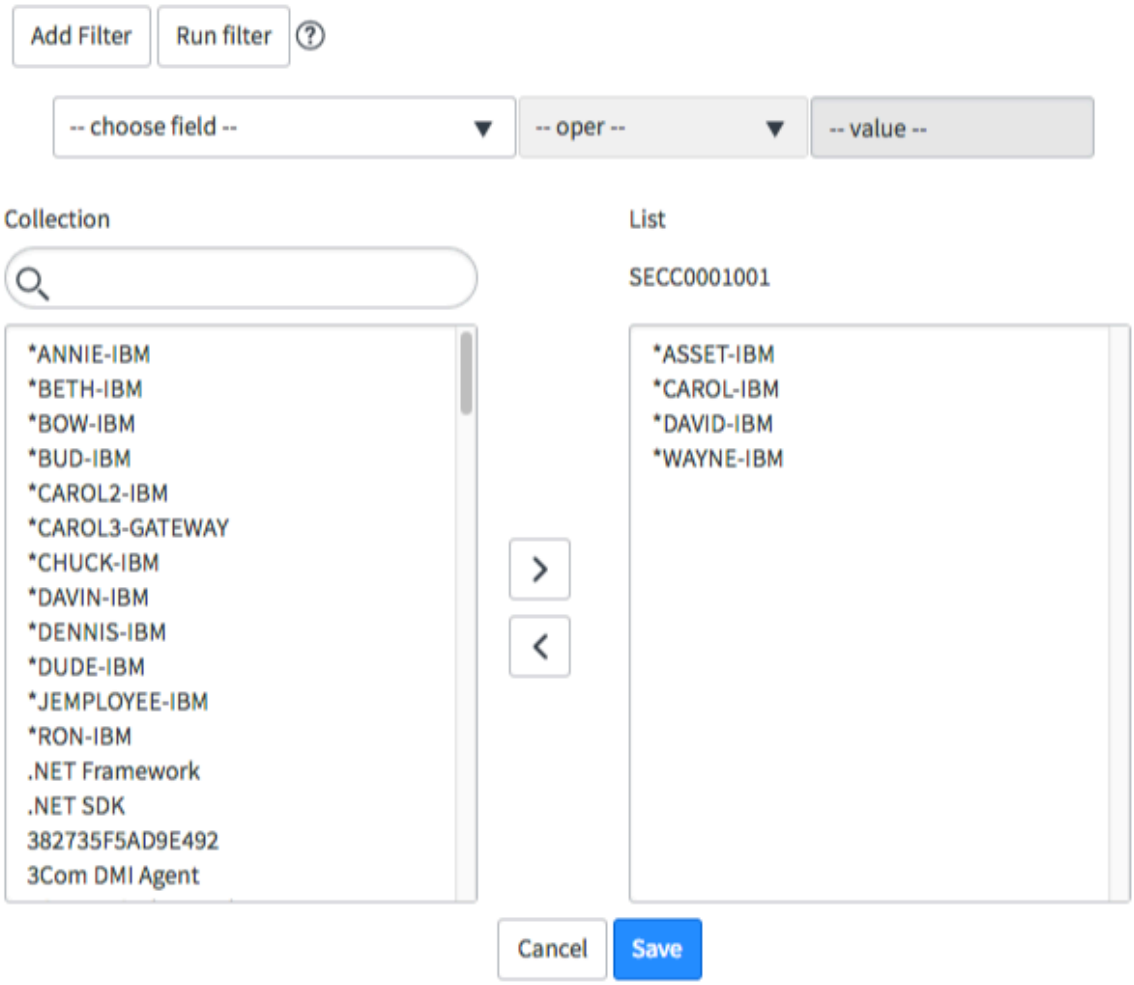


3. ケースに追加するアーティファクトタイプに関連するタブをクリックします。
たとえば、[構成アイテム] をクリックして、1 つ以上の CI をケースに追加します。



4. [編集] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

5. スラッシュバケットとフィルターを使用して、ケースに追加するアーティファクトレコードを見つけて、[コレクション] バケットから [リスト] バケットに移動し、[保存] をクリックします。
選択したタブにリストが表示され、選択したアーティファクトがリストに追加されます。

関連情報

- 既存のケースに IoC と観測事象を追加する
- 既存のケースにセキュリティインシデントを追加する
- 既存のケースに CI を追加する
- 既存のケースに影響を受けるユーザーを追加する

MITRE-ATT&CK 情報をセキュリティケースに関連付ける

MITRE-ATT&CK の戦術とテクニックをセキュリティケースに関連付け、セキュリティケース管理と脅威分析をより細いレベルで行うことができます。

始める前に
必要なロール：sn_si.analyst

手順

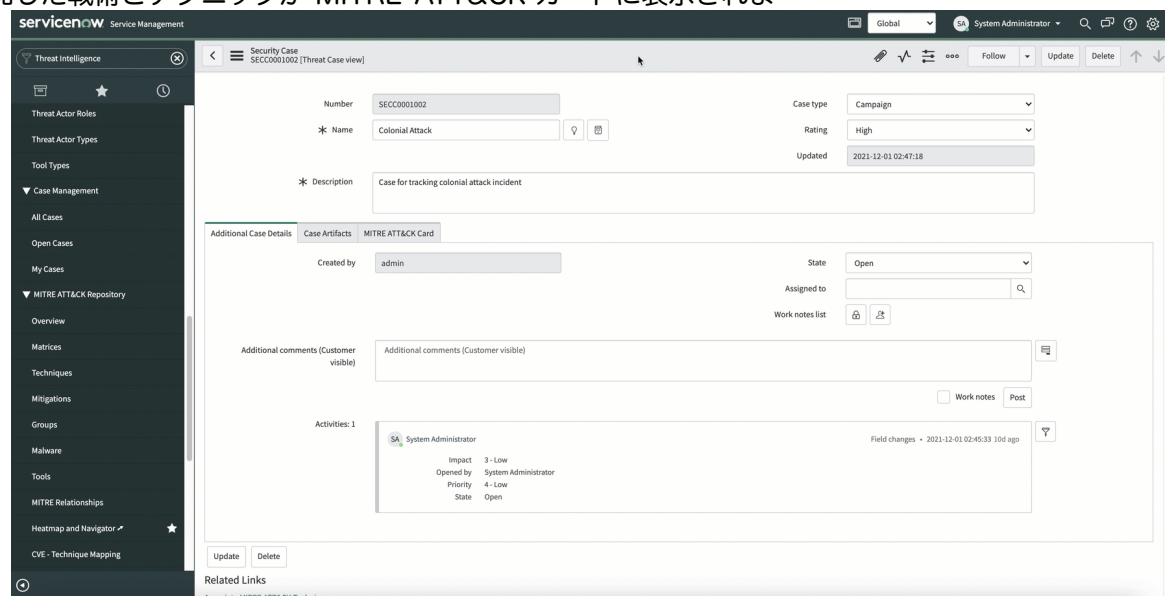
1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > ケースの管理 > すべてのケース.
2. MITRE-ATT&CK 情報で拡張するセキュリティケースを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 関連リストから、**[MITRE ATT&CK** テクニックの関連付け **(Associate MITRE ATT&CK Technique)]** をクリックします。

   次の図では、関連リストから **[MITRE ATT&CK** テクニックの関連付け **(Associate MITRE ATT&CK Technique)]** に移動し、ソースを確認して、戦術とテクニックを追加する方法を示しています。

4. ソースリストで、[ソース] を確認します。
5. [戦術] および [テクニック] を確認して、ケースとの関連性を基に追加や削除を行います。
6. [保存] をクリックします。
   追加した戦術とテクニックが MITRE-ATT&CK カードに表示されます。



セキュリティアーティファクトからのケース作成

セキュリティケース管理 から手動でケースを作成するだけでなく、セキュリティインシデント、セキュリティ侵害のインジケーター、影響を受けるユーザー、構成アイテムなどのセキュリティアーティファクトからケースを作成することができます。

ケースの **IoC** と観測事象

脅威インテリジェンス では、IoC と観測事象からケースを作成したり、既存のケースに IoC と観測事象を追加したりすることができます。ケースから直接観測事象を作成することもできます。

IoC または観測事象からケースを作成する

脅威インテリジェンス では、アーティファクト (IoC または観測事象) からケースを作成できます。IoC または観測事象を使用してケースを作成した後、セキュリティケース管理 を使用してデータを分析できます。

始める前に

セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

必要なロール：sn_ti.case_user_write

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

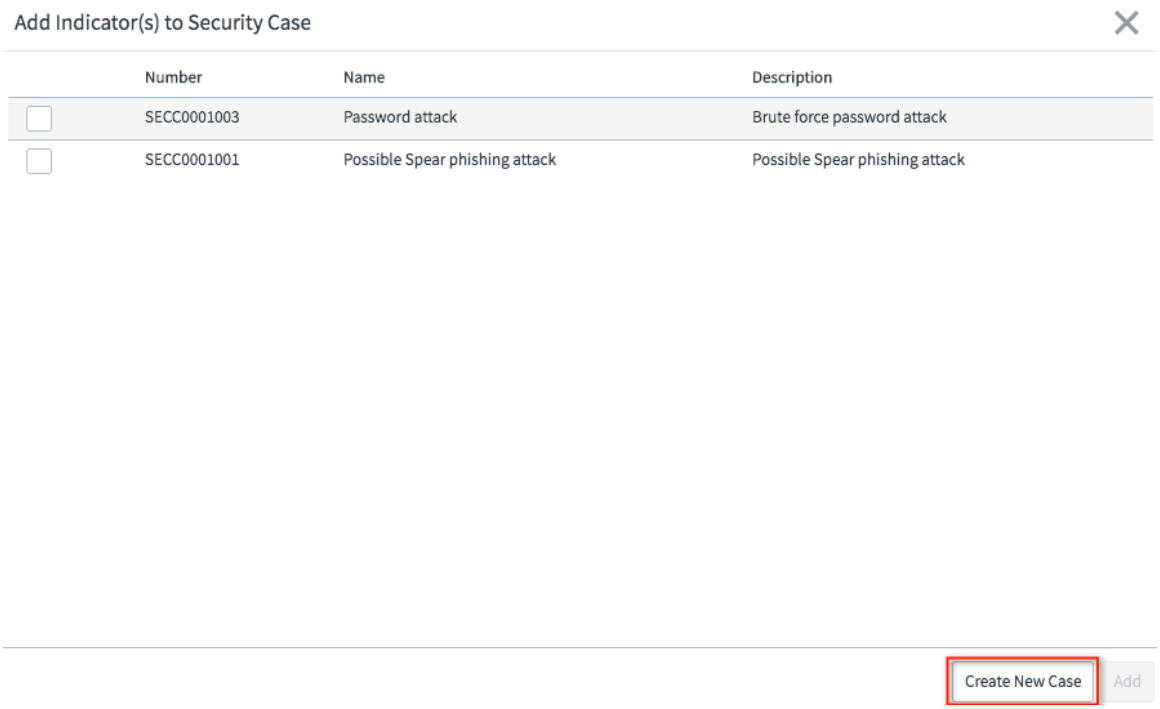
手順

1. ケースの追加に使用するアーティファクト (IoC または観測事象) に移動します。
   - IoC からケースを作成するには、次に移動します: 脅威インテリジェンス > **IoC** リポジトリ > インジケーター.
   - 観測事象からケースを作成するには、次に移動します: 脅威インテリジェンス > **IoC** リポジトリ > 観察事項.
2. リストで、新しいケースに追加するアーティファクトを選択します。

   注:
   複数の IoC または観測事象を選択すると、それらはすべてケースに追加されます。

3. [選択したアイテムのアクション **(Actions on selected items)**] ドロップダウンリストから、[セキュリティケースに追加 **(Add to Security Case)**] を選択します。

[セキュリティケースに追加 **(Add to Security Case)**] ダイアログボックスが開きます。既にケースがアサインされている場合は、リストに表示されます。



4. [新規ケースの作成] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. フィールドに入力します。

フィールド	説明
ケース名	このケースの名前を入力します。
説明	ケースアナリストに重要な説明を入力します。

6. **[Submit]** をクリックします。
   リスト上部に、新しいケースが作成されたことを示すメッセージと、セキュリティケース管理 のケースへのリンクが表示されます。
7. リンクをクリックして新しいケースを表示します。

既存のケースに **IoC** と観測事象を追加する

既存のケースに IoC と観測事象を追加できます。ケースにセキュリティインシデントを追加した後、セキュリティケース管理 を使用してデータを分析できます。

始める前に

セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

必要なロール：sn_ti.case_user_write

手順

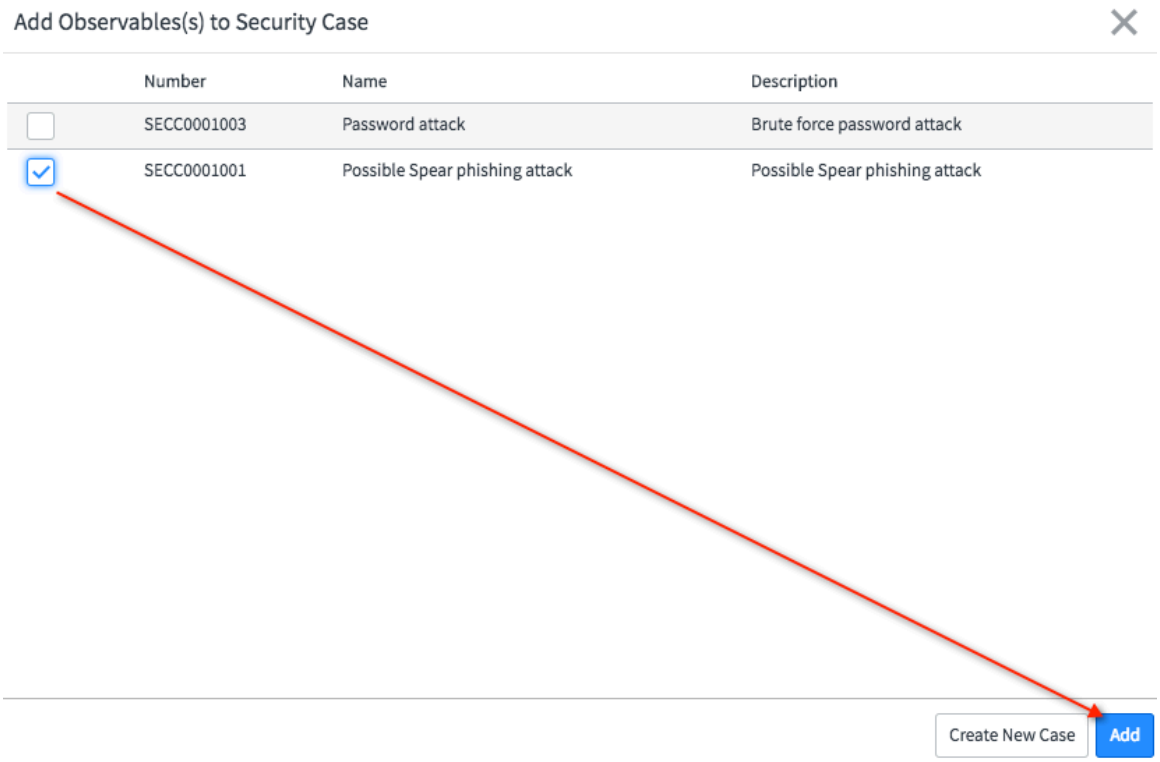
1. 既存のケースに追加するアーティファクト (IoC または観測事象) に移動します。
   - 1 つ以上のケースに IoC を追加するには、次に移動します: 脅威インテリジェンス > **IoC** リポジトリ > インジケーター.
   - 観測事象を 1 つ以上のケースに追加するには、次に移動します: 脅威インテリジェンス > **IoC** リポジトリ > 観察事項.
2. リストで、既存のケースに追加するアーティファクトレコードを選択します。

   注:
   複数のケースを選択すると、選択した IoC または観測事象は選択した各ケースに追加されます。

3. [選択したアイテムのアクション **(Actions on selected items)]** ドロップダウンリストから、[セキュリティケースに追加 **(Add to Security Case)]** を選択します。
   [セキュリティケースに追加 **(Add to Security Case)]** ダイアログボックスが開きます。既にケースがアサインされている場合は、リストに表示されます。
4. 選択した IoC または観測事象を追加するケースを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. [追加] をクリックします。
   選択したレコードがケースに追加されたことを示すメッセージと、セキュリティケース管理 のケースへのリンクが表示されます。

自動翻訳

ケースから観測事象を作成する

セキュリティケース管理 のケースから新しい観測事象を作成できます。

始める前に
必要なロール：sn_ti.case_user

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > ケースの管理 > すべてのケース.
   [セキュリティケース] リストが開きます。
2. 既存のケースを開くか、[新規 **(New)]** をクリック して新しいケースを作成します。
3. [ケースアーティファクト] の関連リンクをクリックし、[観測事象] タブをクリックします。
4. [新規 **(New)]**をクリックし、必要な情報を入力します。

フィールド	説明
値	[読み取り専用] ケース番号。
観測可能タイプ	ケースの記述名を入力します。
観測事象タイプカテゴリ	調査対象のケースタイプを選択します。
インシデント数	このケースの重要性を選択します (重大から低)。
結果	[読み取り専用] ケースが更新された最後の日時。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
メモ	ケースの簡単な説明です。

5. [その他のケース詳細] タブをクリックします。
6. 必要に応じてフィールドを入力します。

フィールド	説明
作成者	[読み取り専用] このケースを作成したユーザーの名前。
状況	ケースの現在のステータス。ケースの作成時、ステータスはデフォルトで [ドラフト] になっています。
作業メモリスト	チェックボックスをクリックすると、ケースレコードの [その他のケース詳細] セクションに作業メモが表示されます。
作業メモ	必要に応じて、ケースの作業メモを入力します。[作業メモリスト] が選択されている場合、作業メモはケースレコードの [その他のケース詳細] セクションに表示されます。

7. **[Submit]** をクリックします。
   必要に応じて、[ケースアーティファクト] タブをクリックして、ケースにアーティファクトを追加できます。

自動翻訳

ケースで観測事象のサイティング検索を実行する

サイティング検索機能で観測事象を検索し、発生頻度を判断できます。各発生は 1 回のサイティングと見なされます。選択した日数または日付範囲内でのサイティング回数に限定して、検索できます。

始める前に

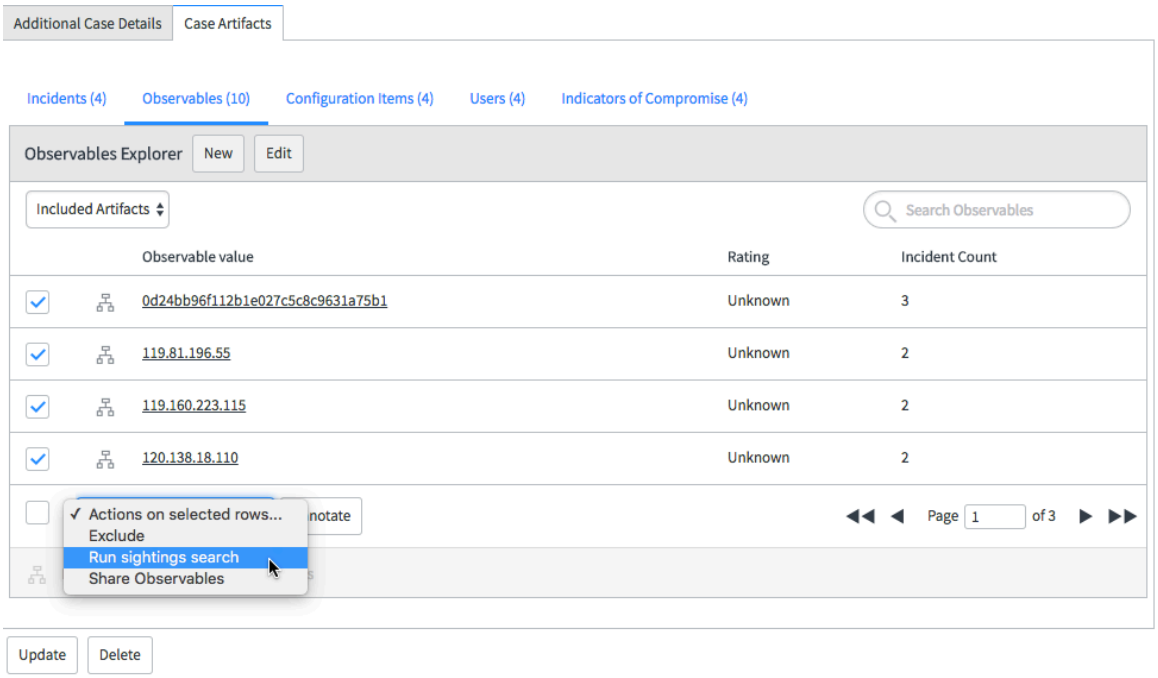
セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

必要なロール：sn_ti.case_user_write

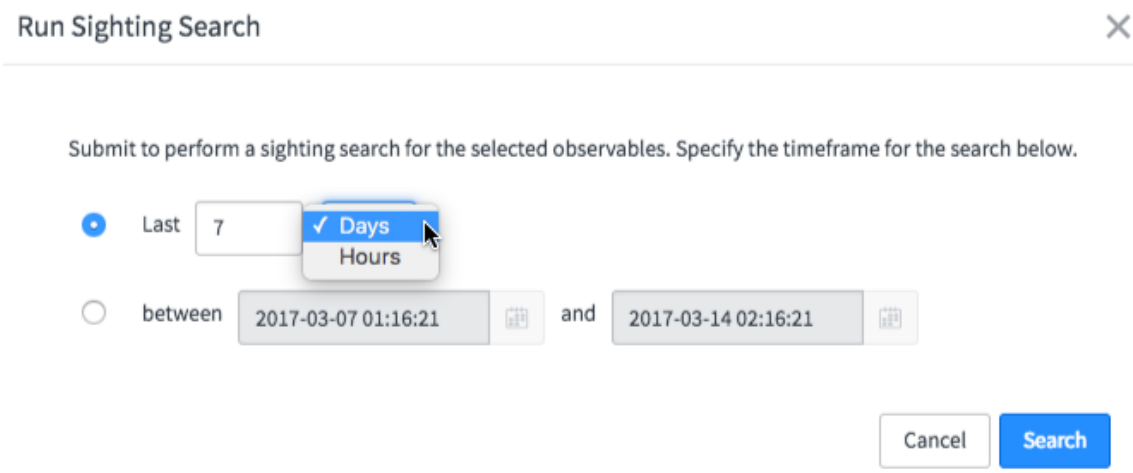
手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > ケースの管理 > すべてのケース.
2. サイティング検索を実行する観測事象を含んでいるケースを開きます。
3. [ケースアーティファクト] の関連リンクをクリックします。
4. [観測事象] タブをクリックします。
5. サイティング検索を実行する 1 つ以上の観測事象を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



6. [選択したアイテムのアクション **(Actions on selected items)]** ドロップダウンリストから、[サイティング検索を実行] を選択します。
   [サイティング検索を実行] ダイアログボックスが表示されます。



7. 選択した観測事象のサイティング検索を実行する日数または時間を入力するか、日付範囲を選択します。
8. [検索] をクリックします。

ケースにおけるセキュリティインシデント

セキュリティインシデントレスポンス では、セキュリティインシデント、CI、および影響を受けるユーザーからケースを作成したり、それらのアーティファクトを既存のケースに追加したりできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティインシデントからケースを作成する

セキュリティインシデントレスポンス で、セキュリティインシデントからケースを作成できます。セキュリティインシデントを使用して新しいケースを作成した後、セキュリティケース管理 を使用してデータを分析できます。

始める前に

セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

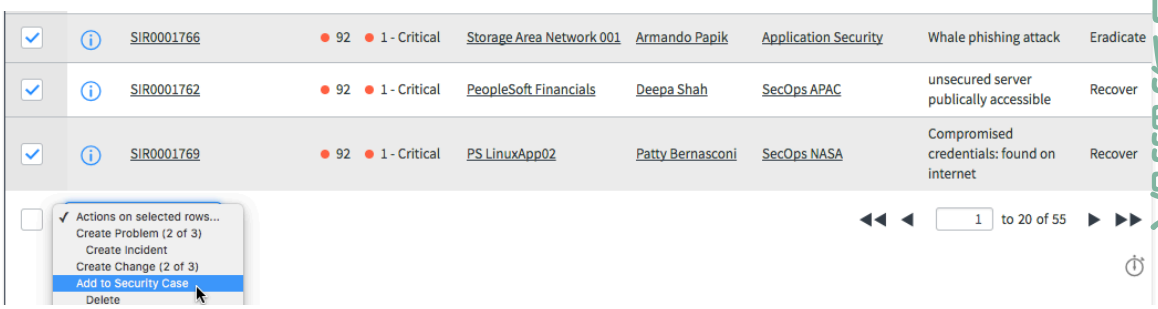
必要なロール：sn_ti.case_user_write

このタスクについて

ケースの作成に使用するセキュリティインシデントに移動する必要があります。

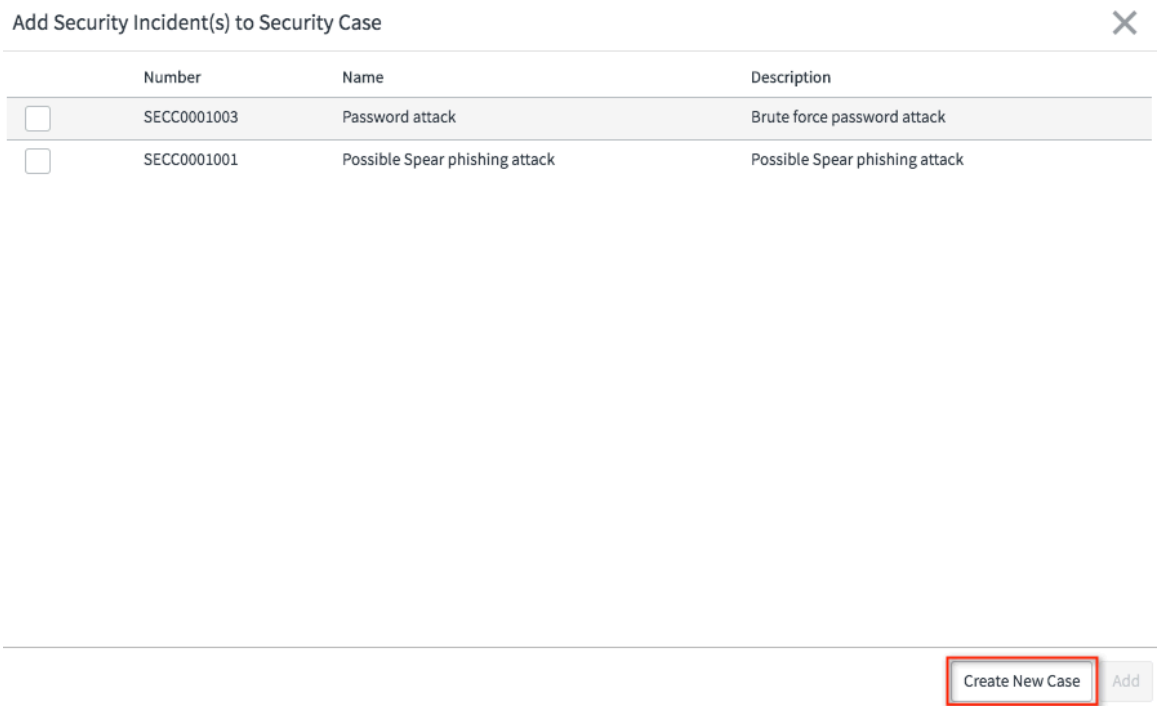
手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデント > オープンインシデントを表示.
   [セキュリティインシデント] リストが開きます。リストから、1 つ以上のセキュリティインシデントから新しいケースを作成するか、特定のセキュリティインシデントを選択してフォームから新しいケースを作成することができます。
2. リストからケースを作成するには、新しいケースに追加するアーティファクトを選択します。
3. [選択したアイテムのアクション **(Actions on selected items)]** ドロップダウンリストから、[セキュリティケースに追加 **(Add to Security Case)]** を選択します。



[セキュリティケースに追加 **(Add to Security Case)]** ダイアログボックスが開きます。既にケースがアサインされている場合は、リストに表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [新規ケースの作成] をクリックします。
5. フィールドに入力します。

フィールド	説明
ケース名	このケースの名前を入力します。
説明	ケースアナリストに重要な説明を入力します。

6. **[Submit]** をクリックします。
   リスト上部に、新しいケースが作成されたことを示すメッセージと、セキュリティケース管理 のケースへのリンクが表示されます。
7. リンクをクリックして新しいケースを表示します。

既存のケースにセキュリティインシデントを追加する

1 つ以上の既存のケースにセキュリティインシデントを追加できます。ケースにセキュリティインシデントを追加した後、セキュリティケース管理 を使用してデータを分析できます。

始める前に
セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

必要なロール：sn_ti.case_user_write

このタスクについて
既存のケースに追加するセキュリティインシデントに移動する必要があります。

自動翻訳

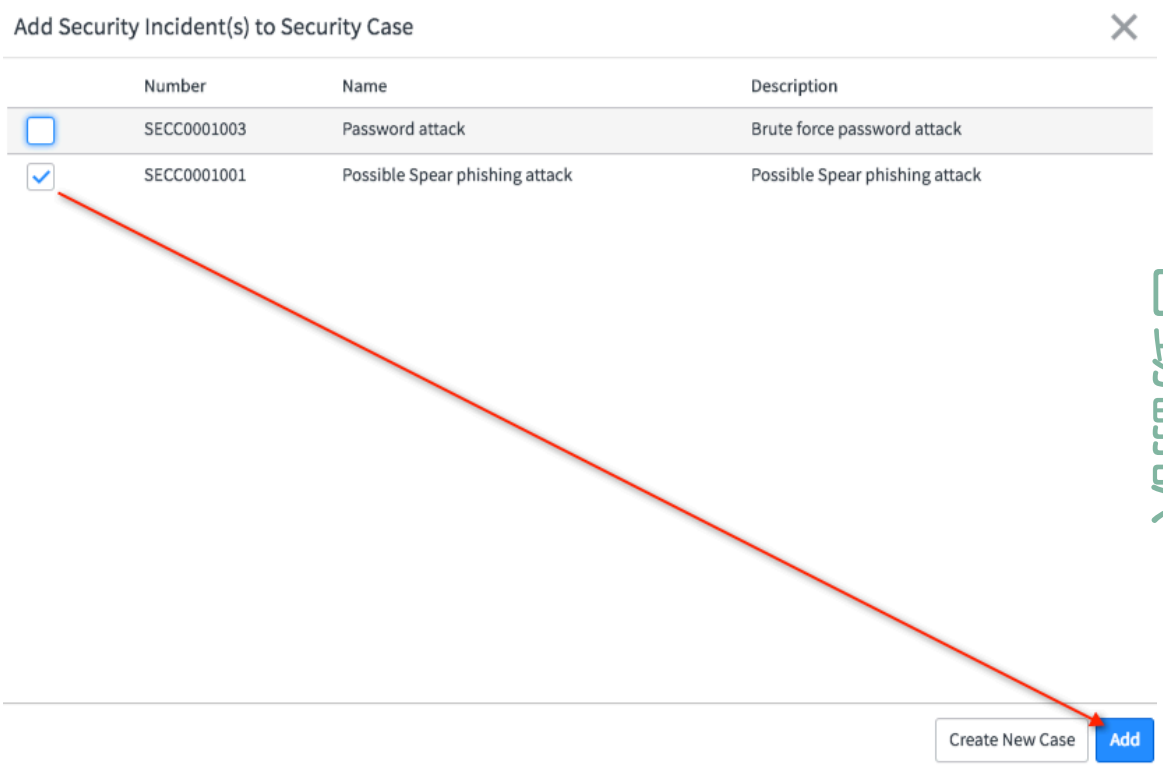
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティインシデント > インシデント > オープンインシデントを表示.
   [セキュリティインシデント] リストが開きます。
2. リストで、既存のケースに追加する 1 つ以上のセキュリティインシデントを選択します。

   注:
   複数のセキュリティインシデントを選択すると、選択したセキュリティインシデントが選択した各ケースに追加されます。

3. [選択したアイテムのアクション **(Actions on selected items)**] ドロップダウンリストから、[セキュリティケースに追加 **(Add to Security Case)**] を選択します。
   [セキュリティケースに追加 **(Add to Security Case)**] ダイアログボックスが開き、自分にアサインされたケースが表示されます。



4. 選択したセキュリティインシデントを追加するケースを選択します。
5. [追加] をクリックします。
   選択したレコードがケースに追加されたことを示すメッセージと、セキュリティケース管理 のケースへのリンクが表示されます。

ケースの構成アイテム

構成アイテム [cmdb_ci] テーブルの 1 つ以上の構成アイテム (CI) から、新しいケースを作成できます。既存のケースに CI を追加することもできます。

CI からケースを作成する

構成アイテム [cmdb_ci] テーブル内の構成アイテムから、セキュリティケースを作成できます。CI を使用して新しいケースを作成した後、セキュリティケース管理 を使用してデータを分析できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

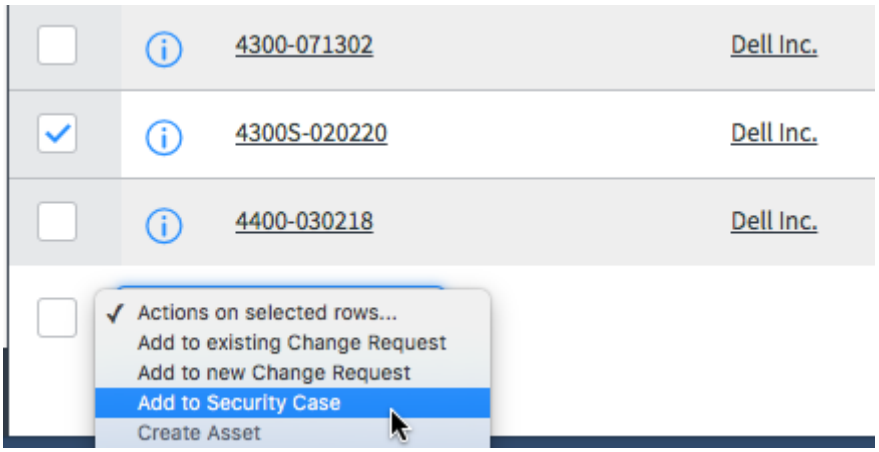
始める前に
セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

必要なロール：sn_ti.case_user_write

このタスクについて
ケースの作成に使用する構成アイテムに移動する必要があります。

手順

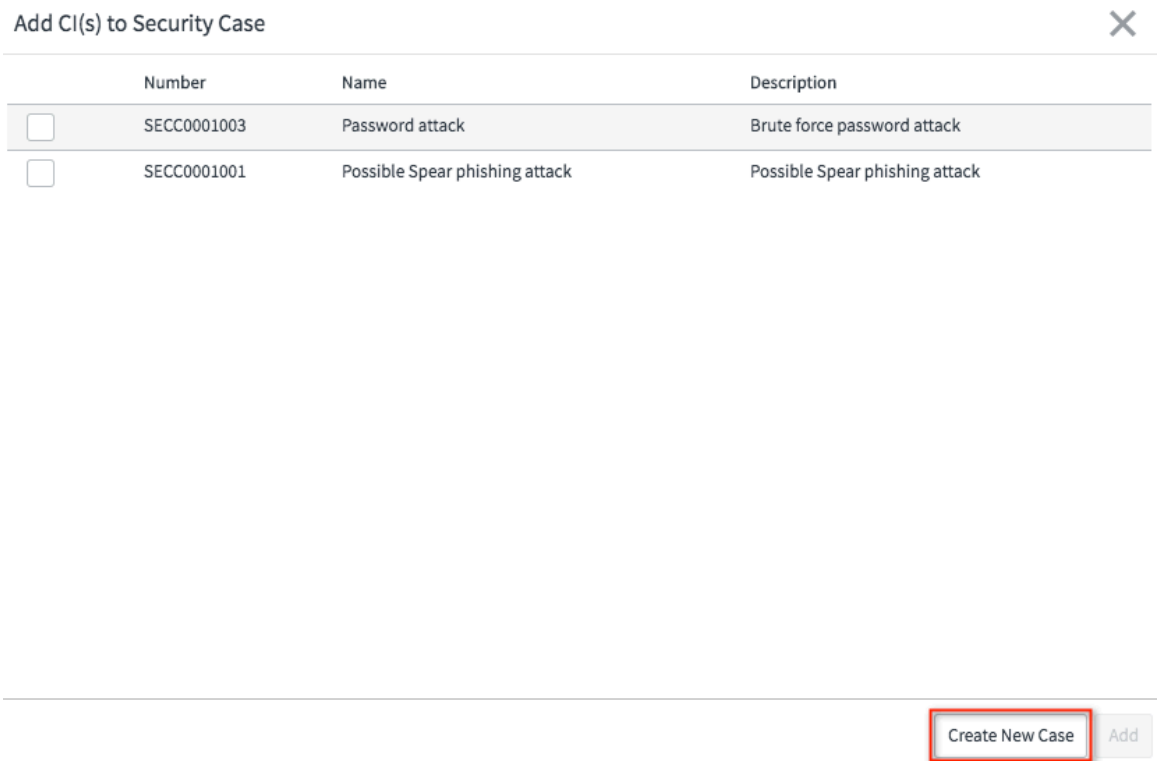
1. 次のように移動する。 **All** (すべて) > 構成 > ベースアイテム > コンピュータ をクリックしてコンピューターの CI を表示します。
   選択した CI タイプのリストが開きます。リストから、1 つ以上の CI から新しいケースを作成するか、特定の CI を選択してフォームから新しいケースを作成することができます。
2. リストから、新しいケースに追加する CI を選択します。
3. [選択したアイテムのアクション **(Actions on selected items)**] ドロップダウンリストから、[セキュリティケースに追加 **(Add to Security Case)**] を選択します。



[セキュリティケースに追加 **(Add to Security Case)**] ダイアログボックスが開きます。既にケースがアサインされている場合は、リストに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [新規ケースの作成] をクリックします。
5. フィールドに入力します。

フィールド	説明
ケース名	このケースの名前を入力します。
説明	ケースアナリストに重要な説明を入力します。

6. **[Submit]** をクリックします。
   リスト上部に、新しいケースが作成されたことを示すメッセージと、セキュリティケース管理 のケースへのリンクが表示されます。
7. リンクをクリックして新しいケースを表示します。

既存のケースに CI を追加する

1 つ以上の既存のケースに構成アイテムを追加できます。ケースに CI を追加した後、セキュリティケース管理 を使用してデータを分析できます。

始める前に
セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

必要なロール：sn_ti.case_user_write

このタスクについて
既存のケースに追加する CI に移動する必要があります。

自動翻訳

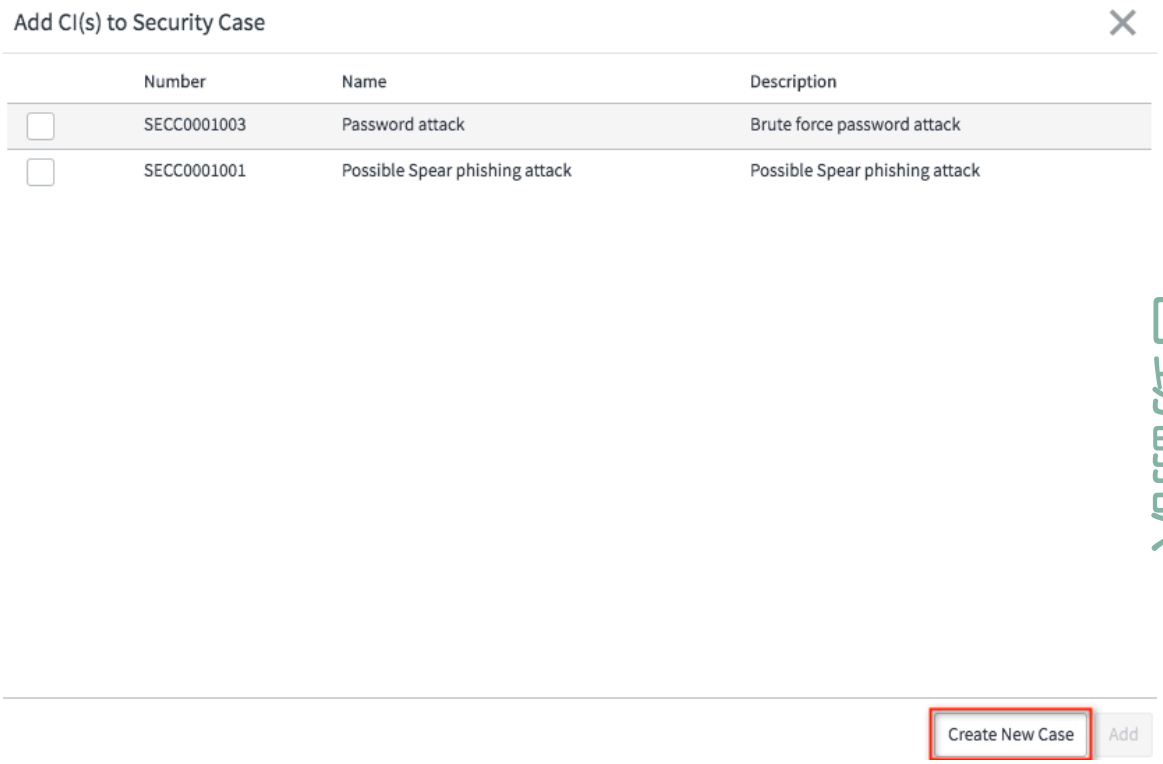
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 構成 > ベースアイテム > コンピュータ をクリックしてコンピューターの CI を表示します。
   選択した CI のリストが開きます。
2. リストで、既存のケースに追加する 1 つ以上の CI を選択します。

   注:
   複数の CI を選択すると、選択した CI が選択した各ケースに追加されます。

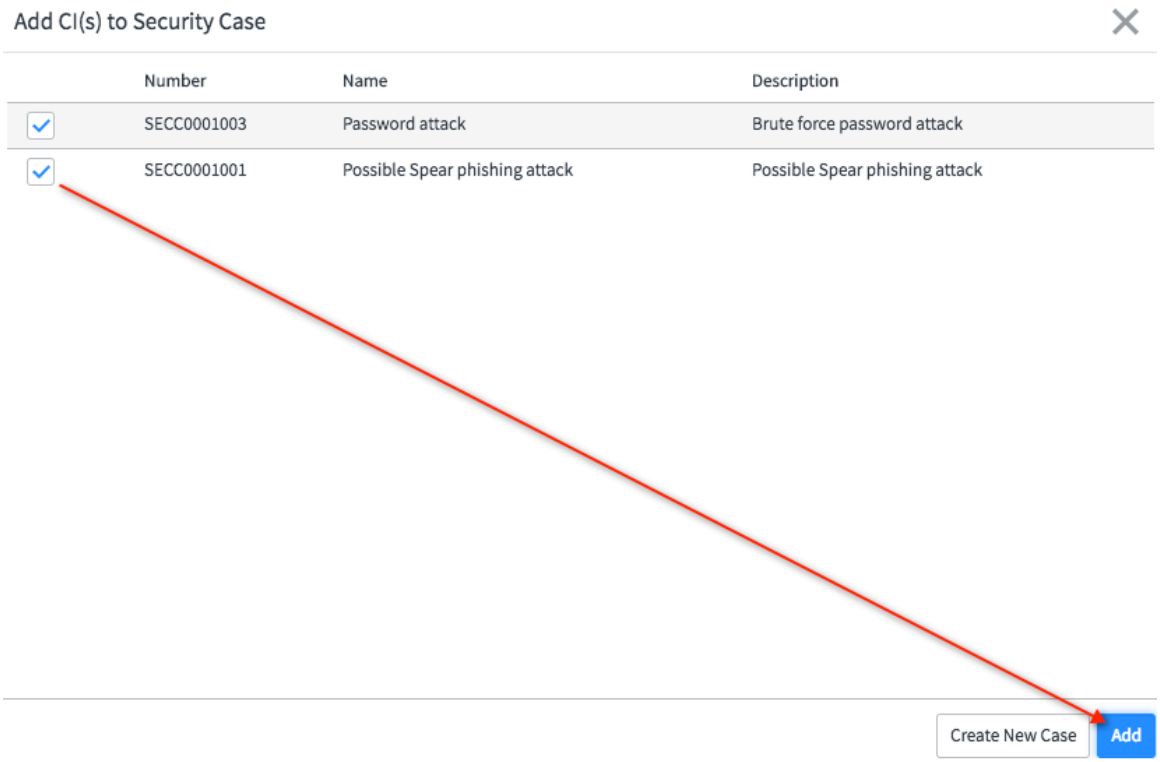
3. [選択したアイテムのアクション **(Actions on selected items)**] ドロップダウンリストから、[セキュリティケースに追加 **(Add to Security Case)**] を選択します。
   [セキュリティケースに追加 **(Add to Security Case)**] ダイアログボックスが開き、自分にアサインされたケースが表示されます。



4. 選択した CI を追加するケースを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. [追加] をクリックします。
   選択したレコードがケースに追加されたことを示すメッセージと、セキュリティケース管理 のケースへのリンクが表示されます。

ケースの影響を受けるユーザー

ユーザー [sys_user] テーブルの 1 人以上の影響を受けるユーザーから、新しいケースを作成できます。既存のケースにユーザーを追加することもできます。

影響を受けるユーザーからケースを作成する

ユーザー [sys_user] テーブル内の影響を受けるユーザーから、セキュリティケースを作成できます。影響を受けるユーザーを使用して新しいケースを作成した後、セキュリティケース管理 を使用してデータを分析できます。

始める前に
セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

必要なロール：sn_ti.case_user_write

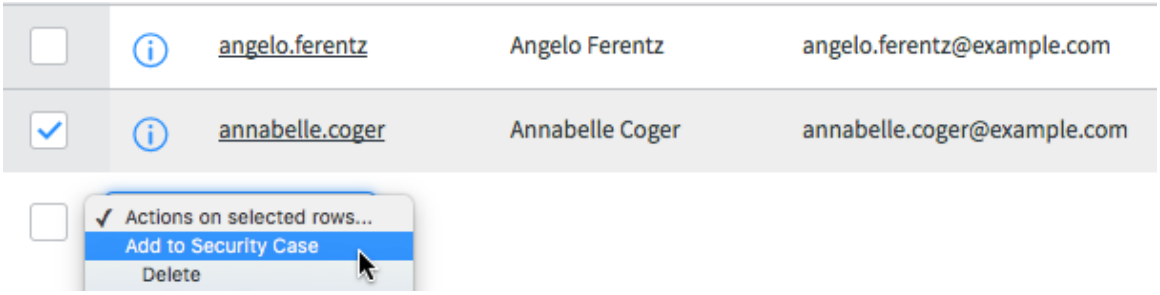
このタスクについて
ケースの作成に使用するユーザーに移動する必要があります。

手順

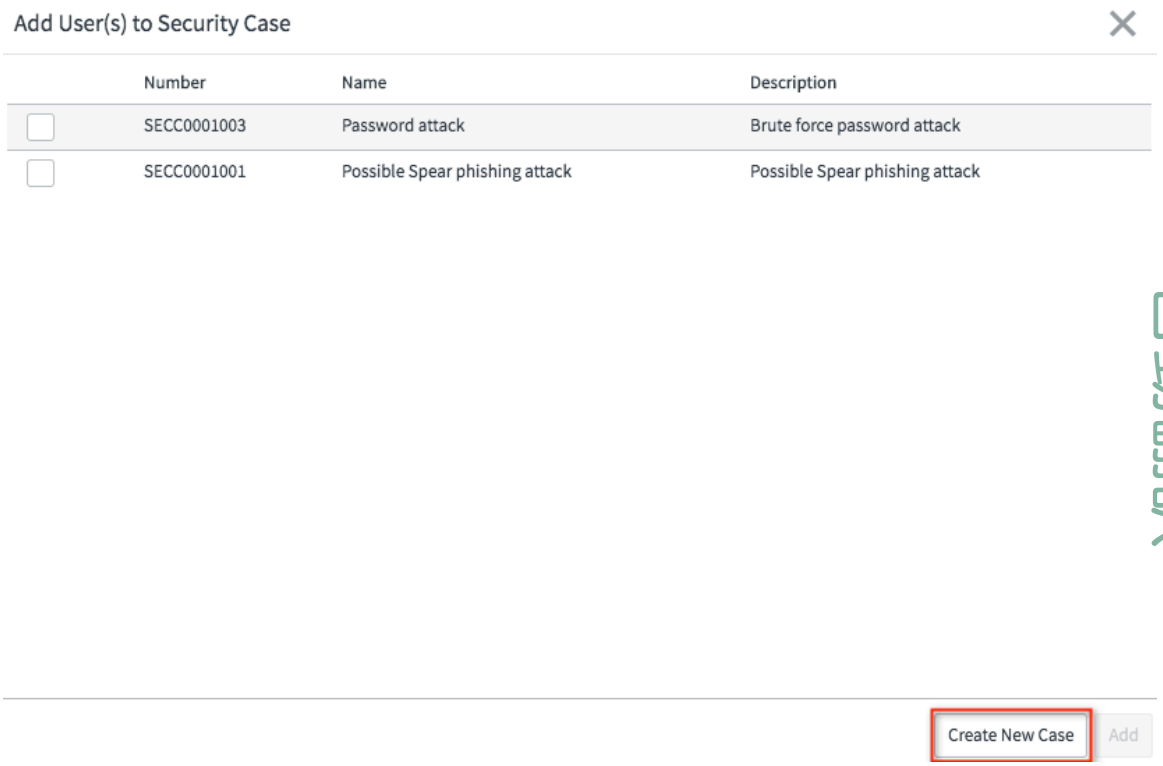
1. 次のように移動する。 **All** (すべて) > ユーザー管理 **(User Administration)** > ユーザー.
   選択したユーザーのリストが開きます。リストから、1 つ以上のユーザーレコードから新しいケースを作成するか、特定のユーザーレコードを選択してフォームから新しいケースを作成することができます。
2. リストから、新しいケースに追加するユーザーを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [選択したアイテムのアクション **(Actions on selected items)]** ドロップダウンリストから、[セキュリティケースに追加 **(Add to Security Case)]** を選択します。



[セキュリティケースに追加 **(Add to Security Case)]** ダイアログボックスが開きます。既にケースがアサインされている場合は、リストに表示されます。



4. [新規ケースの作成] をクリックします。
5. フィールドに入力します。

フィールド	説明
ケース名	このケースの名前を入力します。
説明	ケースアナリストに重要な説明を入力します。

6. **[Submit]** をクリックします。
リスト上部に、新しいケースが作成されたことを示すメッセージと、セキュリティケース管理 のケースへのリンクが表示されます。
7. リンクをクリックして新しいケースを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

既存のケースに影響を受けるユーザーを追加する

1 つ以上の既存のケースに影響を受けるユーザーを追加できます。ユーザーレコードがケースに追加された後、セキュリティケース管理 を使用してデータを分析できます。

始める前に

セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

必要なロール：sn_ti.case_user_write

このタスクについて

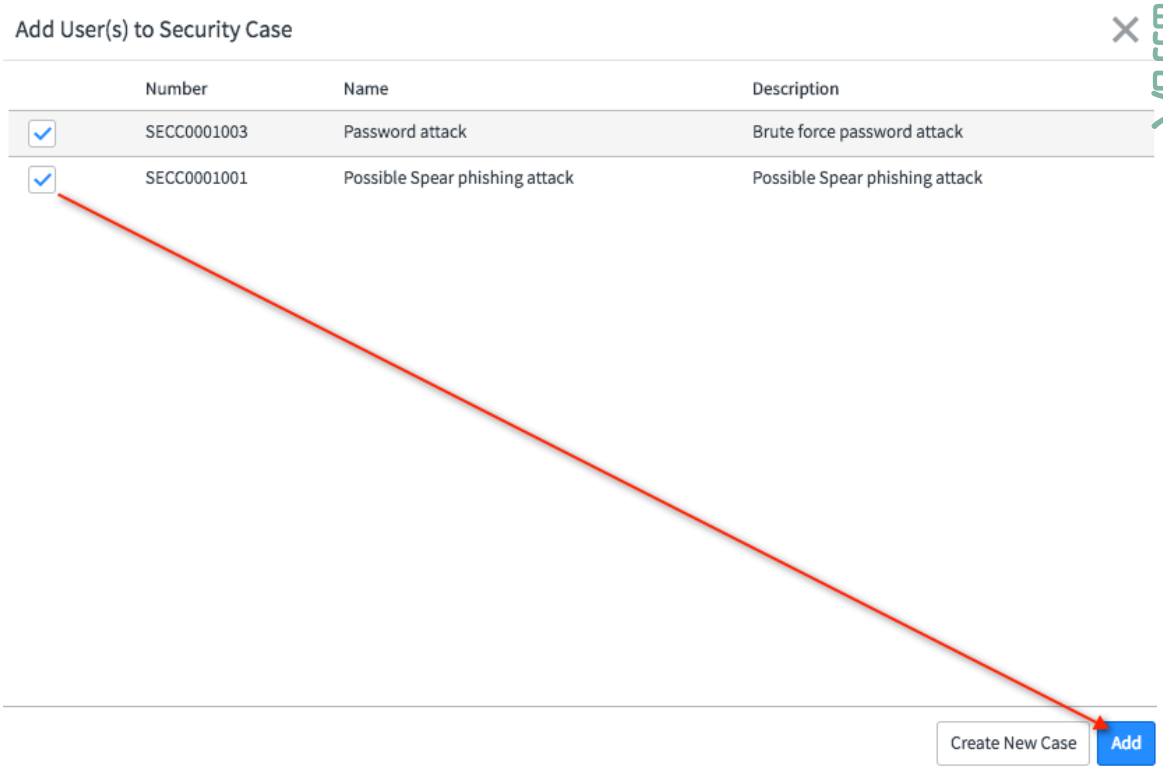
既存のケースに追加するユーザーレコードに移動する必要があります。

手順

1. 次のように移動する。 **All** (すべて) > ユーザー管理 **(User Administration)** > ユーザー.
   ユーザーレコードのリストが開きます。
2. リストで、既存のケースに追加する 1 つ以上のユーザーを選択します。

   注:
   複数のユーザーを選択すると、選択したユーザーレコードが選択した各ケースに追加されます。

3. [選択したアイテムのアクション **(Actions on selected items)**] ドロップダウンリストから、[セキュリティケースに追加 **(Add to Security Case)**] を選択します。
   [セキュリティケースに追加 **(Add to Security Case)**] ダイアログボックスが開き、自分にアサインされたケースが表示されます。



4. 選択したユーザーを追加するケースを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. [追加] をクリックします。
   選択したレコードがケースに追加されたことを示すメッセージと、セキュリティケース管理 のケースへのリンクが表示されます。

セキュリティアーティファクト分析

セキュリティケース管理 を使用するか、または IoC、観測事象、セキュリティインシデントなどのアーティファクトからケースを作成した後、識別された脅威の分析に役立つアーティファクトを追加し続けることができます。

ケースアーティファクトの関連する詳細

ケースにアーティファクトを追加すると、各アーティファクトのその他の関連する詳細も自動的に追加されます。たとえば、セキュリティインシデントを追加すると、影響を受ける CI やユーザーレコードが含まれる場合があります。アーティファクトのリストを離れなくても、選択したアーティファクトの関連する詳細をすばやく表示できます。

セキュリティインシデントのアーティファクトに関連する詳細を表示する

ケースにセキュリティインシデントのアーティファクトが含まれている場合は、ケースが参照する各セキュリティインシデントに含まれる関連する詳細を表示できます。

始める前に

- セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

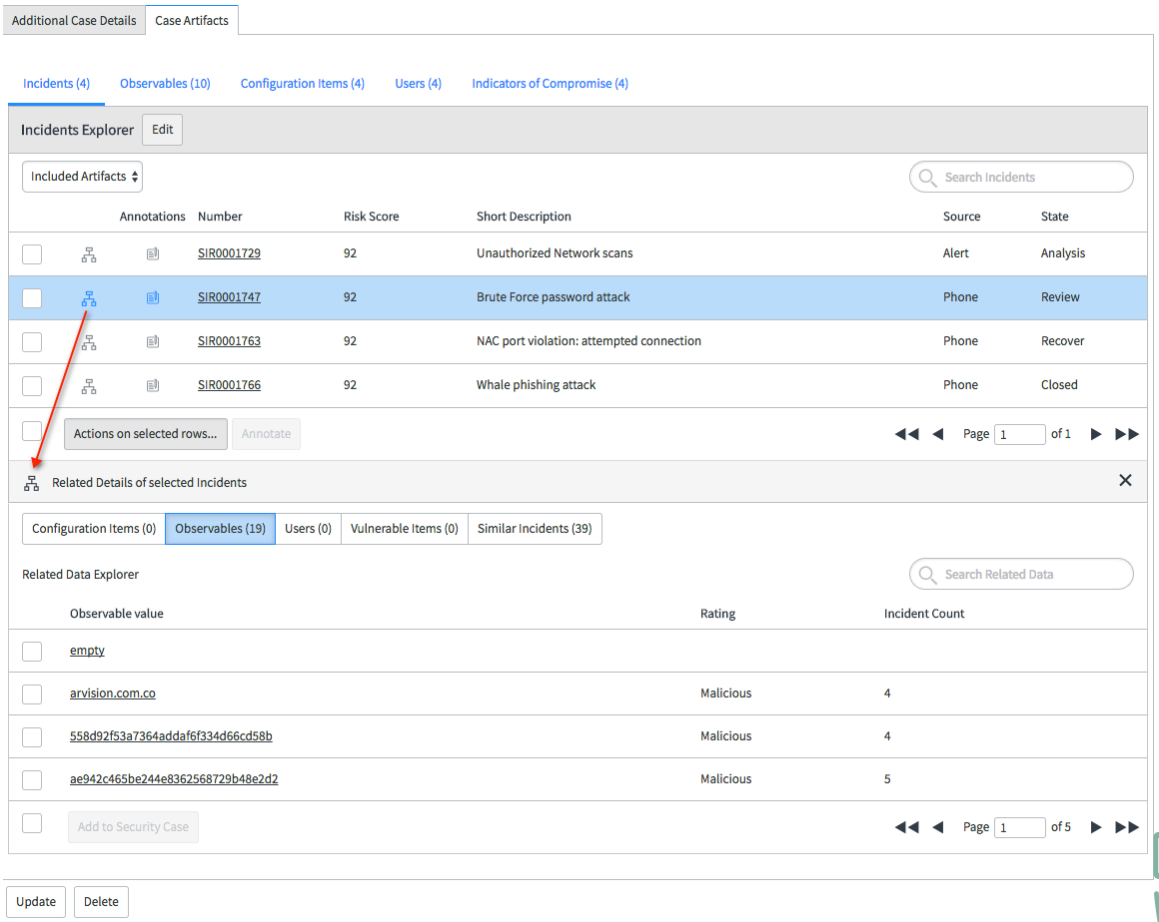
必要なロール：sn_ti.case_user_write

手順

1. セキュリティインシデントのアーティファクトを含んでいるケースを開きます。
2. [インシデント] タブをクリックします。
3. 関連する詳細を表示するセキュリティインシデントの [その他の詳細] アイコンをクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. いずれかのタブをクリックし、選択したアーティファクトの特定のタイプの詳細を表示します。
5. [セキュリティ注釈] タブをクリックして、選択したアーティファクトの注釈を表示することもできます。

構成アイテムのアーティファクトに関連する詳細を表示する

ケースに構成アイテムのアーティファクトが含まれている場合は、ケースが参照する各 CI に含まれる関連する詳細を表示できます。

始める前に

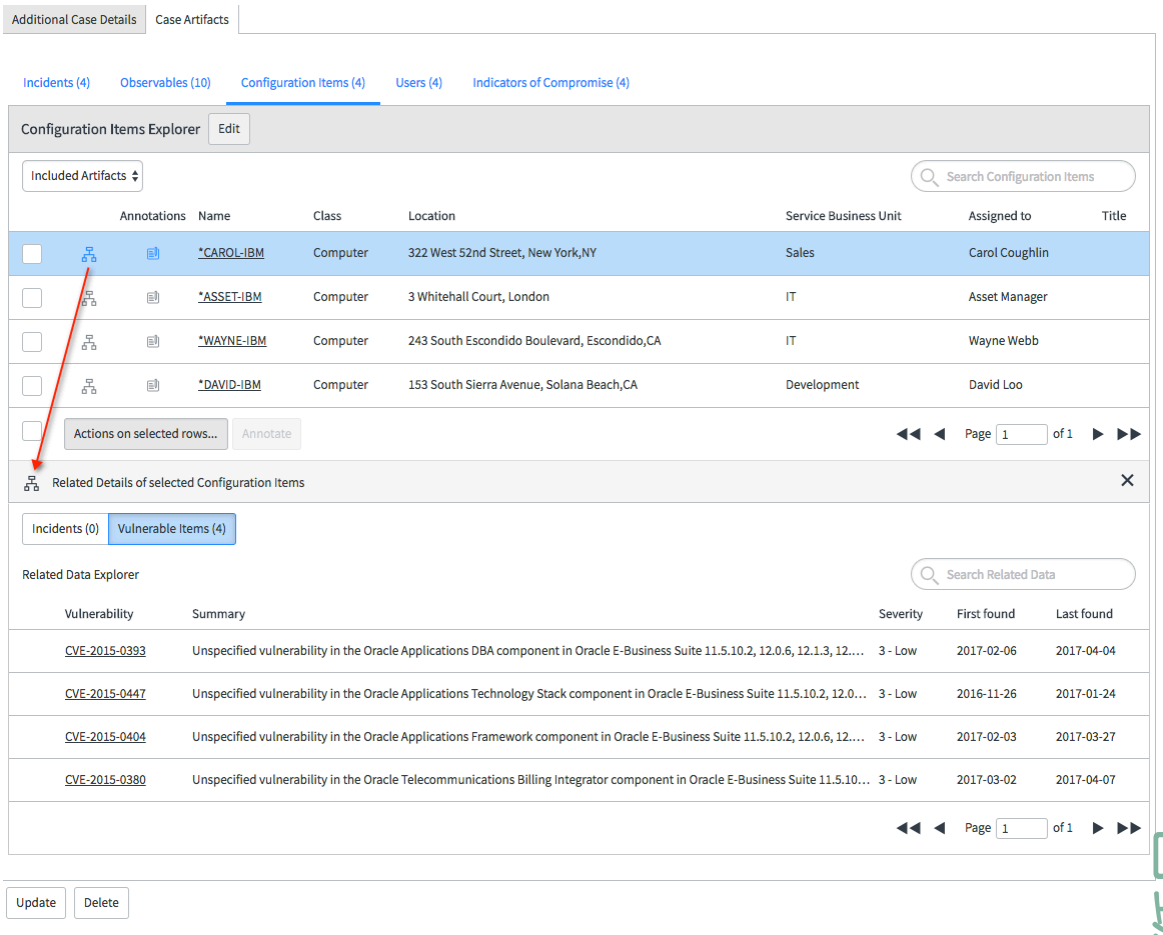
- セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

必要なロール：sn_ti.case_user_write

手順

1. CI のアーティファクトを含んでいるケースを開きます。
2. [構成アイテム] タブをクリックします。
3. 関連する詳細を表示する CI アーティファクトの [その他の詳細] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. いずれかのタブをクリックし、選択したアーティファクトの特定のタイプの詳細を表示します。
5. [セキュリティ注釈] タブをクリックして、選択したアーティファクトの注釈を表示することもできます。

IoC のアーティファクトに関連する詳細を表示する

ケースにセキュリティ侵害のインジケーター (IoC) のアーティファクトが含まれている場合は、ケースが参照する各 IoC に含まれる関連する詳細を表示できます。

始める前に

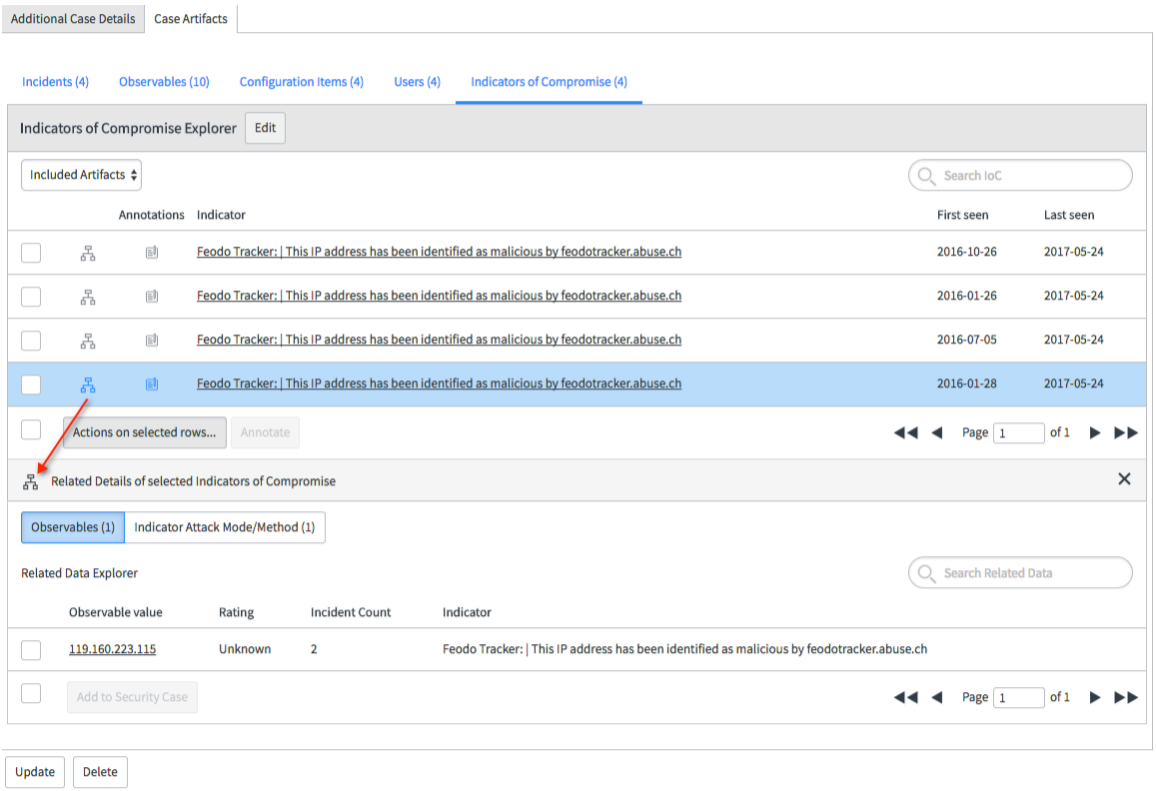
- セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

必要なロール：sn_ti.case_user_write

手順

1. IoC のアーティファクトを含んでいるケースを開きます。
2. [セキュリティ侵害のインジケーター] タブをクリックします。
3. 関連する詳細を表示する IoC アーティファクトの [その他の詳細] アイコンをクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. いずれかのタブをクリックし、選択したアーティファクトの特定のタイプの詳細を表示します。
5. [セキュリティ注釈] タブをクリックして、選択したアーティファクトの注釈を表示することもできます。

影響を受けるユーザーのアーティファクトに関連する詳細を表示する

ケースに影響を受けるユーザーのアーティファクトが含まれている場合は、ケースが参照する各影響を受けるユーザーに含まれる関連する詳細を表示できます。

始める前に

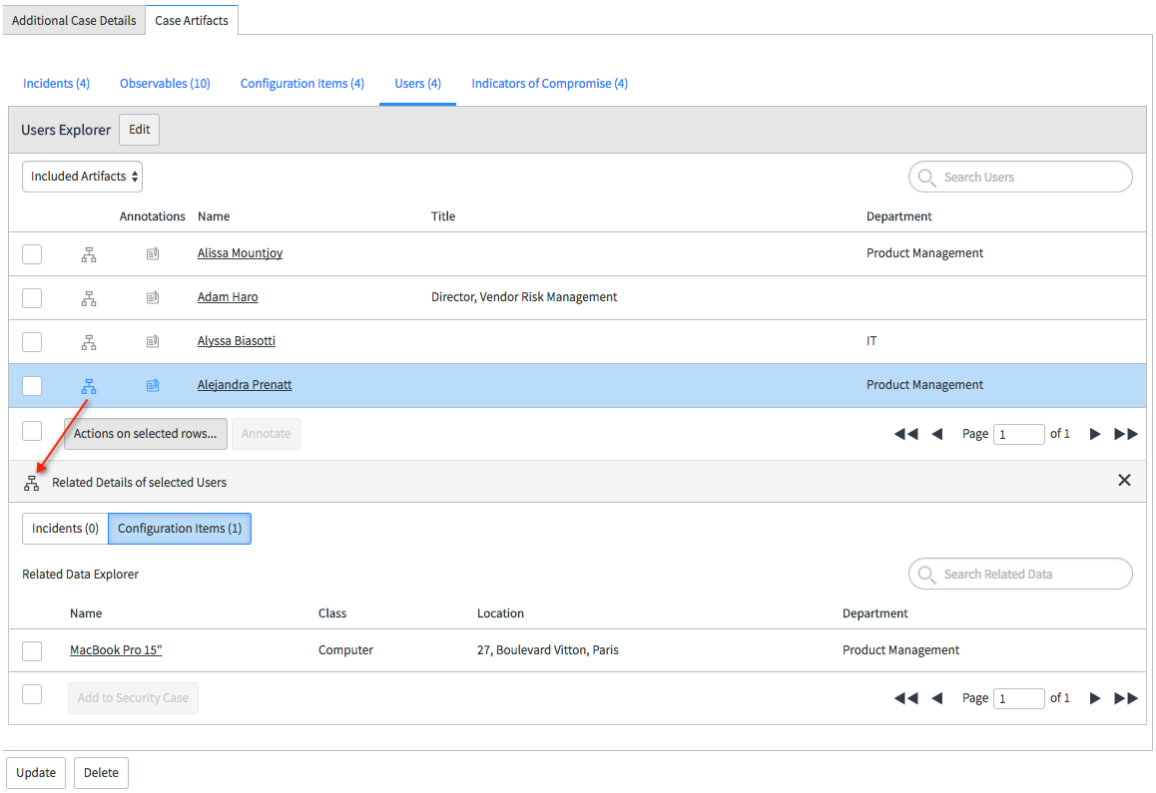
- セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

必要なロール：sn_ti.case_user_write

手順

1. 影響を受けるユーザーのアーティファクトを含んでいるケースを開きます。
2. [ユーザー] タブをクリックします
3. 関連する詳細を表示する影響を受けるユーザーのアーティファクトの [その他の詳細] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. いずれかのタブをクリックし、選択したアーティファクトの特定のタイプの詳細を表示します。
5. [セキュリティ注釈] タブをクリックして、選択したアーティファクトの注釈を表示することもできます。

観測事象のアーティファクトに関連する詳細を表示する

ケースに観測事象のアーティファクトが含まれている場合は、ケースが参照する各観測事象に含まれる関連する詳細を表示できます。

始める前に

セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

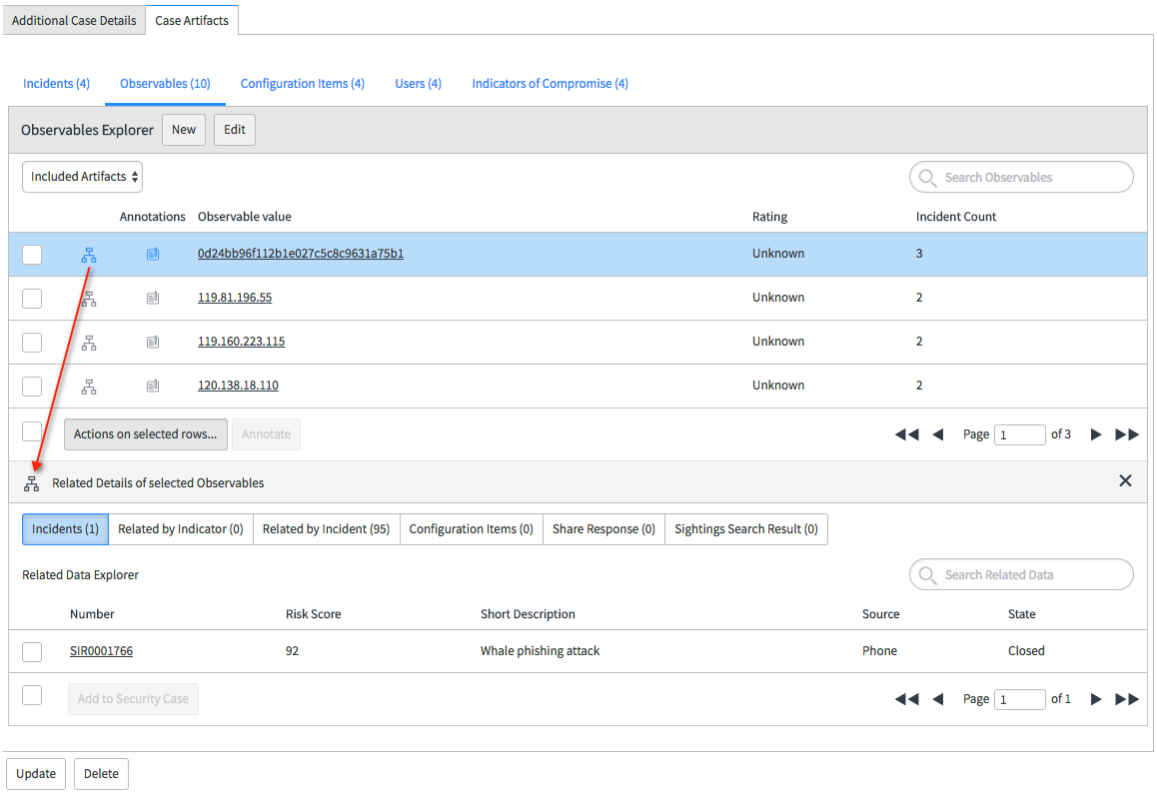
必要なロール：sn_ti.case_user_write

手順

1. 観測事象のアーティファクトを含んでいるケースを開きます。
2. [観測事象] タブをクリックします。
3. 関連する詳細を表示する観測可能アーティファクトの [その他の詳細] アイコンをクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. いずれかのタブをクリックし、選択したアーティファクトの特定のタイプの詳細を表示します。
5. [セキュリティ注釈] タブをクリックして、選択したアーティファクトの注釈を表示することもできます。

セキュリティアーティファクトの除外と包含

ケースにアサインされたサポートアーティファクトのリストは長くなることがあり、リストから特定のアーティファクトを削除する場合があります。アーティファクトを完全に削除するのではなく、リストから除外し、必要に応じて後でリストに戻すことができます。

ケースからセキュリティアーティファクトを除外する

サポートアーティファクトのリストからアーティファクトを削除できます。これらは完全に削除されるのではなく、必要に応じてケースに戻すことができます。

始める前に

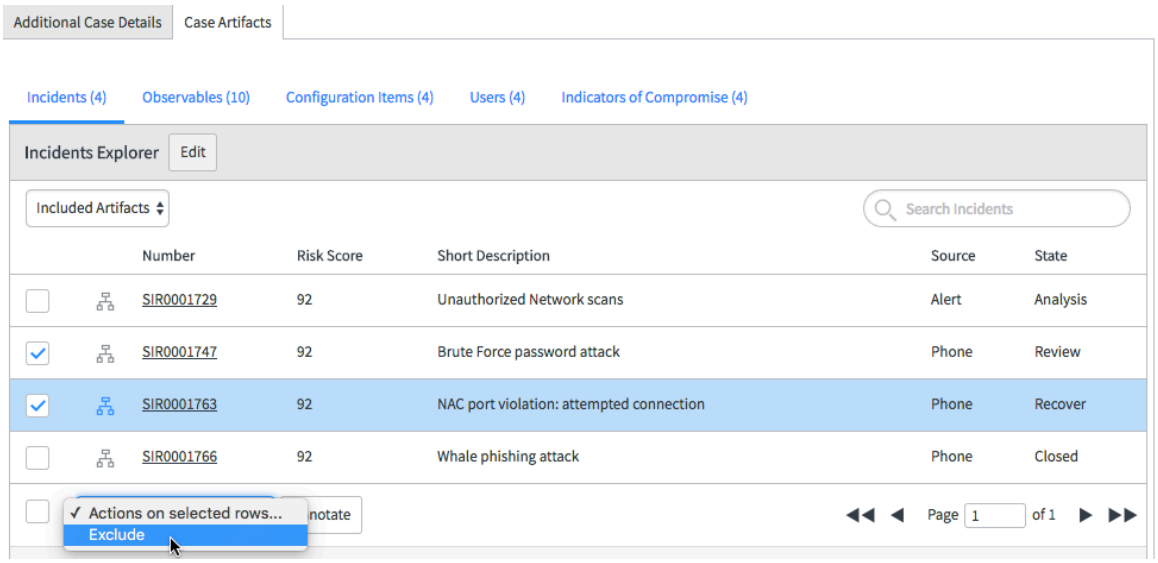
- セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

必要なロール：sn_ti.case_user_write

手順

1. リストから除外するアーティファクトを含んでいるケースを開きます。
2. [ケースアーティファクト] の関連リストをクリックします。
3. 除外するアーティファクトに関連するタブをクリックします。
   たとえば、[インシデント] をクリックして、リストからセキュリティインシデントを除外します。
4. 除外する 1 つ以上のアーティファクトレコードを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. [選択したアイテムのアクション **(Actions on selected items)]** ドロップダウンリストから、[除外] を選択します。
6. 確認ボックスで [除外] をクリックします。
   選択したアーティファクトがリストから削除されます。

除外されたセキュリティアーティファクトをケースに戻す

ケース内のリストからアーティファクトを除外した後、ケースに戻せば作業は続行できます。

始める前に

セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

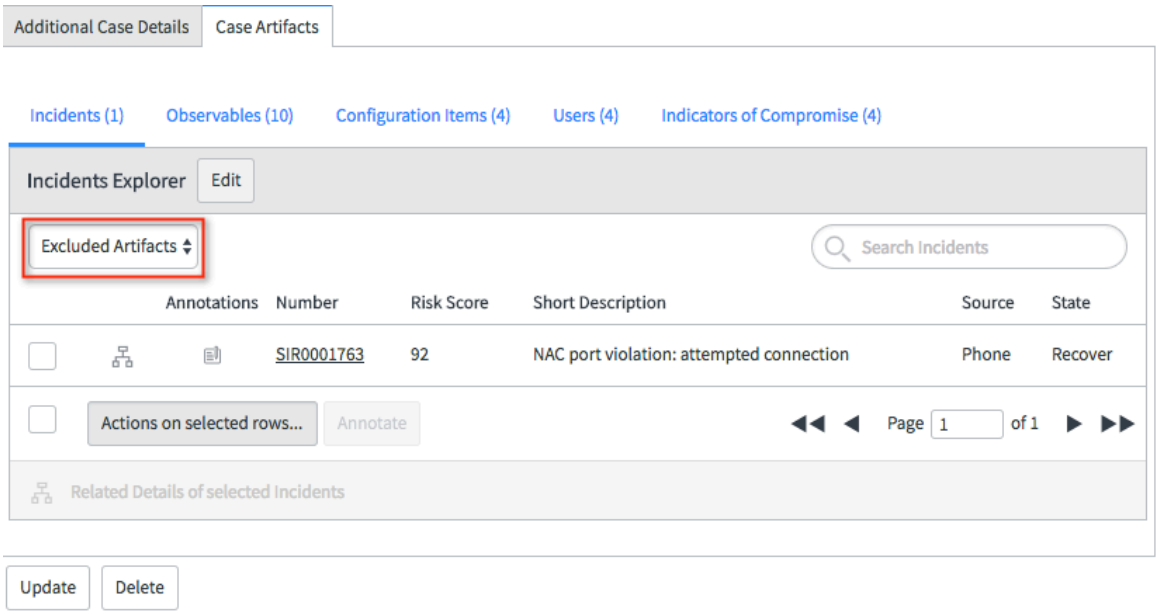
必要なロール：sn_ti.case_user_write

手順

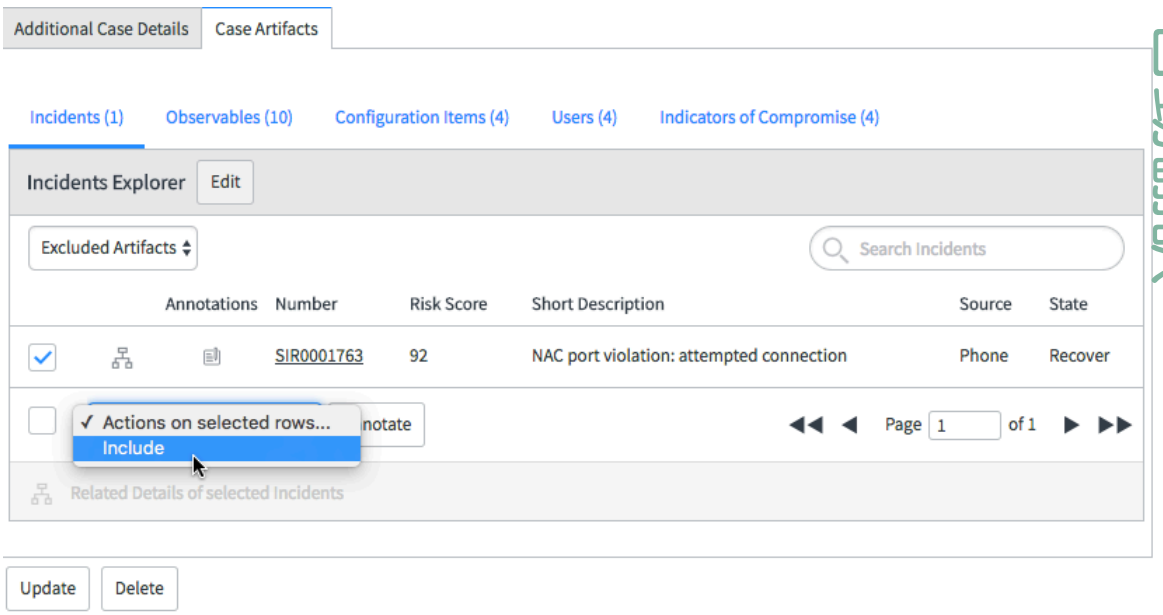
1. 前にリストから除外したアーティファクトの内、リストに戻すアーティファクトを含んでいるケースを開きます。
2. [ケースアーティファクト] の関連リストをクリックします。
3. リストに戻すアーティファクトに関連するタブをクリックします。
4. [アーティファクトフィルター] ドロップダウンリストをクリックし、[除外されたアーティファクト **(Excluded Artifacts)]** を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. 元のリストに戻す 1 つ以上のアーティファクトレコードを選択します。
6. [選択したアイテムのアクション **(Actions on selected items)]** ドロップダウンリストから、[包含] を選択します。



7. 確認ボックスで [包含] をクリックします。
   選択したアーティファクトが除外されたアーティファクトのリストから削除され、ケースに含まれるアーティファクトのリストに戻ります。

セキュリティアーティファクトに注釈を付ける

ケースを分析するときに、アーティファクトに注釈を追加できます。

始める前に

セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

必要なロール：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

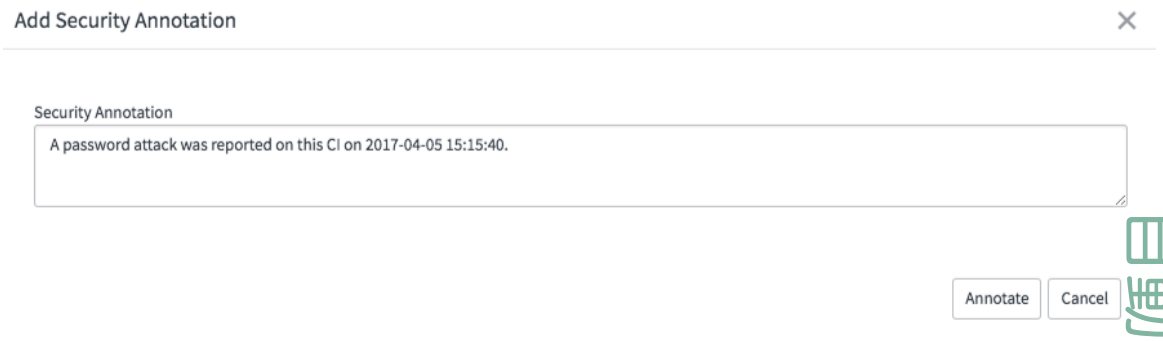
- 注釈を追加する場合、sn_ti.case_user_write
- 注釈を表示する場合、sn_ti.case_user_read

手順

1. 注釈を付けるアーティファクトを含んでいるケースを開きます。
2. [ケースアーティファクト] の関連リストをクリックします。
3. 注釈をつけるアーティファクトに関連するタブをクリックします。
   たとえば、[セキュリティ侵害のインジケーター] をクリックして、IoC に注釈を追加します。
4. 1 つ以上のアーティファクトに注釈を追加するには、次の手順を実行します。

   a. 注釈を追加するアーティファクトを選択します。

   b. [注釈] をクリックします。

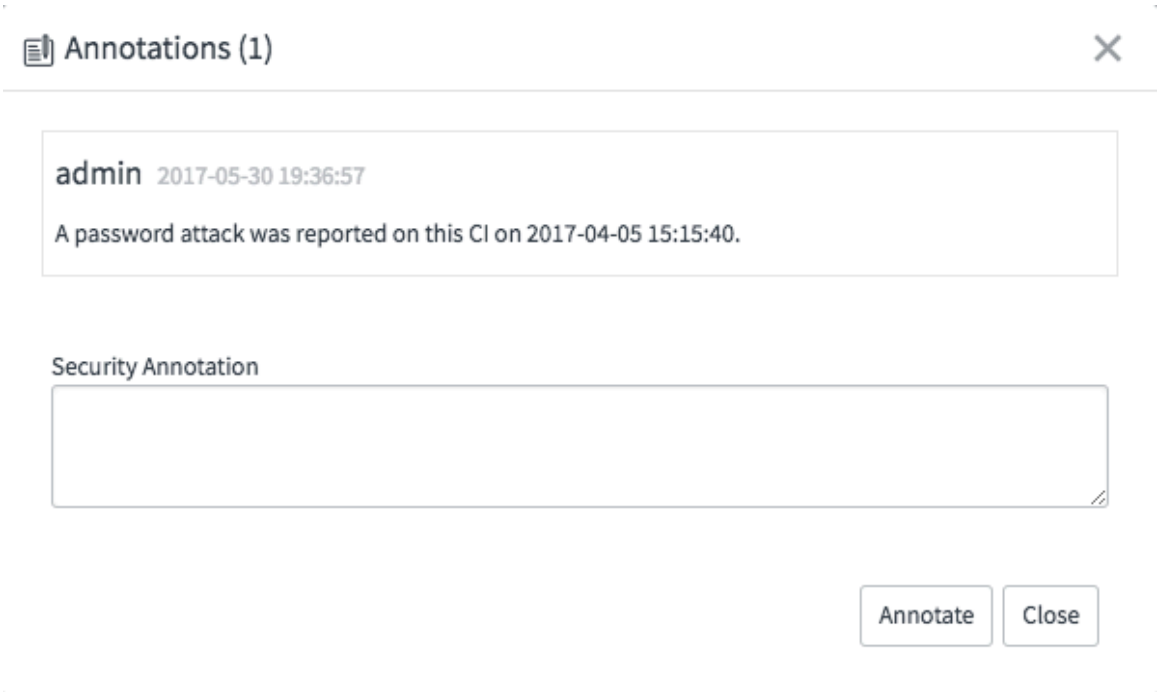


   c. 注釈を入力し、[注釈] をクリックします。
   選択したアーティファクトに注釈が追加されます。

5. アーティファクトの注釈を表示するには、[注釈を表示] ( ) アイコンをクリックします。
   既存の注釈が [注釈] ダイアログボックスに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



6. [セキュリティ注釈] ボックスにアーティファクトの新しい注釈を入力し、[注釈] をクリックすることもできます。

セキュリティアーティファクトの検索

セキュリティアーティファクトリストでキーワード検索を実行できます。

始める前に
セキュリティケース管理 を使用するには、脅威インテリジェンス プラグインをアクティブ化する必要があります。

必要なロール：sn_ti.case_user_write

手順

1. セキュリティアーティファクトを含んでいるケースを開きます。
2. キーワード検索を実行するセキュリティアーティファクトのタブをクリックします。
3. [キーワード検索] ボックスで、検索するアーティファクトの名前を入力します。
   入力と一致するアーティファクトが見つかると、表示されます。

セキュリティポスチャコントロール

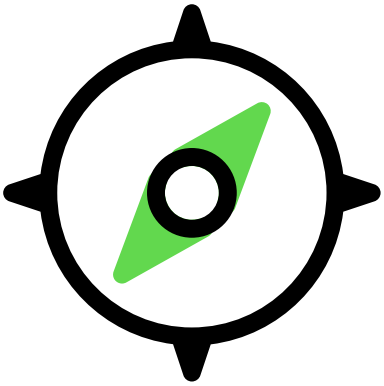
エンタープライズ資産在庫とセキュリティツール範囲を可視化します。製品で提供されるポリシーを使用するか、独自のポリシーを作成して、エンドポイント保護、構成管理、脆弱性スキャンなどの主要なセキュリティツールが不足している資産を特定します。環境に固有のセキュリティツール構成の資産を監視し、コンフィグレーションコンプライアンスアプリケーションのセキュリティギャップの修正ワークフローを自動化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

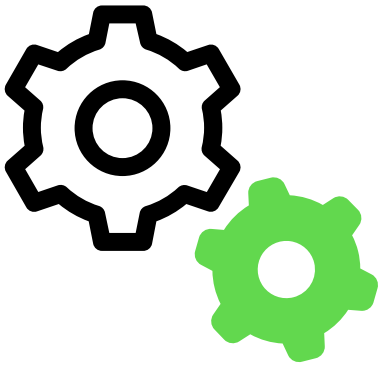
開始するには

探索



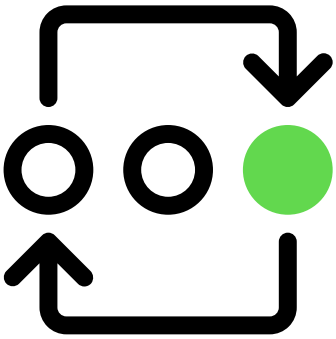
セキュリティポスチャコントロールの概念と機能について学ぶ

インストール



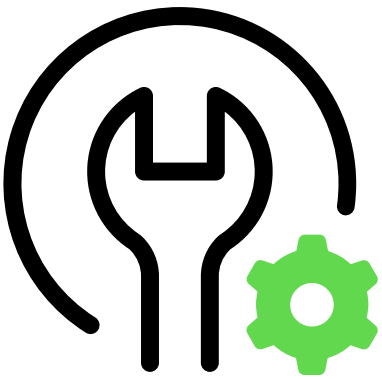
セキュリティポスチャコントロールアプリケーションのインストール

統合



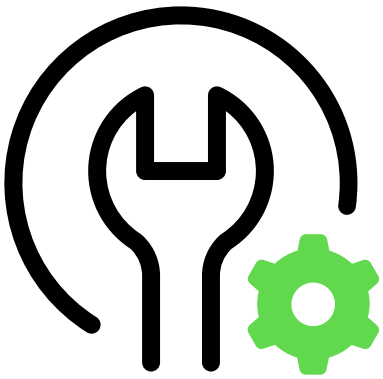
サービスグラフコネクタとセキュリティポスチャコントロールの統合

使用



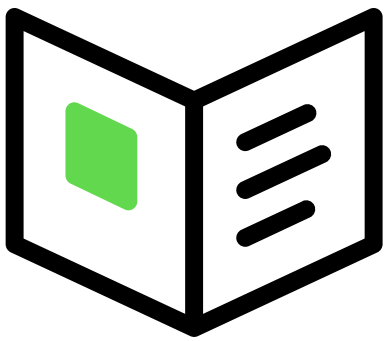
ワークスペースを使用して資産を検索し、セキュリティギャップを特定する方法について説明します

緩和コントロールモニタリング



利用可能な緩和コントロールによって資産に対するどの脅威が軽減されるかについてのインサイトを得る

Reference (参照)



特定のタイプのツール範囲のギャップを特定するのに役立つシナリオの詳細を取得します。基本ポリシー、子ポリシー、クローン作成されたポリシーの例と、サポートされているハードウェアおよびソフトウェアのサービスグラフコネクタのリストを参照してください。

自動翻訳

トラブルシューティングとサポート

- セキュリティオペレーションリソースライブラリ
- セキュリティオペレーションコミュニティ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 既知のエラーポータルで既知のエラー記事を検索する
- 連絡先 カスタマーサービス & サポート

セキュリティポスチャコントロール の詳細

セキュリティポスチャコントロール により、サイバーセキュリティチームはエンタープライズ資産インベントリ全体を可視化し、全体的なセキュリティポスチャを判断できるようになります。

セキュリティアナリストは、資産インベントリをはじめ、サービスグラフコネクタ、 ハードウェア資産管理 (HAM) 、ITOM ディスカバリーなどの ServiceNow 製品からのインポートデータに基づいて、セキュリティツールがどの程度適切に展開され、資産をカバーしているかについてのインサイトを得ることができます。

セキュリティアナリストは、カスタムポリシーを作成し、内部セキュリティ基準に対する資産のコンプライアンスを監視するためのインサイトを構成することもできます。脆弱性マネージャーは、セキュリティポスチャコントロール (SPC) からのインサイトを使用して、リスクの高い資産の脆弱性の修復に優先順位を付けることができます。

SPC 製品は、クラウドセキュリティポスチャ管理 (CSPM) とサイバーアセットハイジーンマネジメント (CAHM) に基づいています。セキュリティポスチャコントロールは、ServiceNow Store から別々のサブスクリプションで利用できる 2 つのアプリケーションで構成されています。

リリースバージョン	リリースノート
セキュリティポスチャコントロールコア:v 6.0、v5.0、v4.0、v3.0、v2.0	互換性情報については、「KB0856498 脆弱性対応互換性マトリクスおよびリリーススキーマの変更」を参照してください。 Security Posture Control release notes
資産セキュリティポスチャ管理:v5.3、v5.0、v4.0、v3.0、v2.0	
緩和コントロールモニタリング v3.0、v2.0	

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

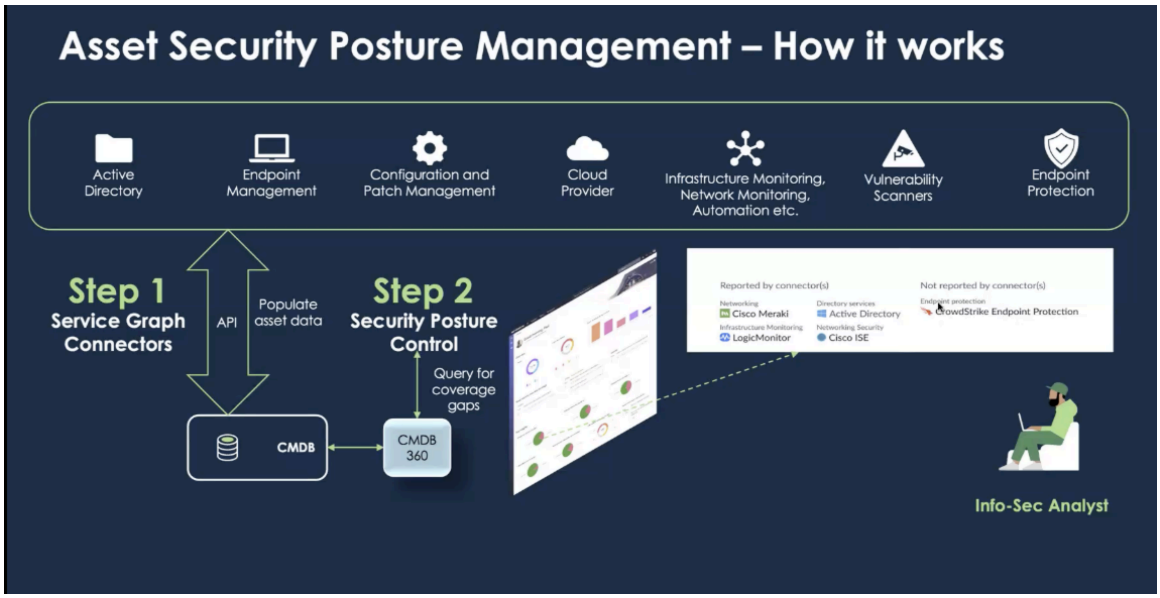
SPC 製品を使用すると、情報セキュリティチームは次のタスクを実行できます。

- オンプレミス資産とクラウド資産のセキュリティポスチャに関するインサイトを表示します。SPC は、情報セキュリティチームがエンドポイント保護が欠落している資産、管理されていない資産、インターネットに公開されている資産、脆弱性を含むリスクの高い組み合わせを特定するのに役立ちます。
- 資産が内部セキュリティツールの構成標準に準拠しているかどうか監視します。たとえば、最新バージョンのエンドポイント保護製品が使用されていることを確認します。
- ServiceNow コンフィグレーションコンプライアンスアプリケーションで検出されたセキュリティポスチャのギャップの修復ワークフローを自動化します。
- 資産メタデータ、セキュリティツール範囲データ、および脆弱性データに基づいて、カスタムポリシーとインサイトを作成します。
- さまざまなセキュリティツールが 緩和コントロールモニタリングでどのように構成されているかに基づいて、利用可能な緩和コントロールによって資産に対する脅威が緩和されるインサイトを得ることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

資産セキュリティポスチャ管理 の仕組み



資産セキュリティポスチャ管理 (ASPM) では、ServiceNow 製品と併せて、さまざまなサードパーティツール (サービスグラフコネクタ) との API 統合を使用して、資産のセキュリティツール範囲のギャップを特定します。

資産に関して ASPM は CMDB に入力されたデータに依存しています。資産データは、さまざまなカテゴリの監視ツールによってインポートされ、潜在的なセキュリティギャップを特定するために比較されます。

たとえば、インフラストラクチャ監視ツールやネットワークツールによって報告される、CMDB に入力された資産データがあるとします。ただし、この資産データはエンドポイント保護ツールからは入力されず、報告もされません。これらの異なるツールによって報告された資産データを比較すると、エンドポイント保護エージェントが欠落している資産があることがわかります。

資産セキュリティポスチャ管理 では、さまざまなツール (サービスグラフコネクタ) や ServiceNow 製品との API 統合を使用して、資産におけるセキュリティツール範囲のギャップを特定します。カテゴリには次のものが含まれますが、これらに限定されません。

- デジタル従業員エクスペリエンス
- ディスカバリー
- エンドポイント管理
- IT Asset Management
- インフラストラクチャモニタリング
- ネットワーク
- ネットワークセキュリティ
- ネットワークパフォーマンスモニタリング
- 構成とパッチ管理
- エンドポイント保護
- クラウドプロバイダー
- アプリケーションパフォーマンスモニタリング

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ディレクトリサービス
- 脆弱性アセスメント

セキュリティポスチャコントロール ワークフロー

セキュリティツールのギャップを特定するには、次の手順を実行します。

1. さまざまなカテゴリで使用しているいずれかのツールを使用して API 接続を設定し、アクティブ化します。必要な API 接続には、ServiceNow Store から入手できる製品にサービスグラフコネクタを使用できます。サポートされているサービスグラフコネクタの詳細については、「Service Graph Connectors」を参照してください。サポートされているサービスグラフコネクタは、個別のサブスクリプションで ServiceNow Store から入手できます。
2. セキュリティポスチャコントロールアプリケーションに備わるポリシーをアクティブ化します。セキュリティポスチャコントロール製品は、次のタスクを実行して、セキュリティツールのギャップを検出します。
   a. CMDB のさまざまなサービスグラフコネクタによって入力されたすべての一意の資産のリストを特定します。
   b. エンドポイント保護など、この資産プールから特定のカテゴリによって報告されていない資産を特定します。資産は、評価対象のアクティブなポリシーに基づいて特定されます。
   c. 特定のカテゴリで報告されていないと特定された資産は、コンフィグレーションコンプライアンスアプリケーションで「検出結果」または「テスト結果」として報告されます。
3. コンフィグレーションコンプライアンスアプリケーションで、修復のためにさまざまなチームに「検出結果」を自動的にアサインします。

高リスクの組み合わせ

資産セキュリティポスチャ管理 では、高リスクの組み合わせを有する資産を特定することもできます。高リスクの組み合わせの例としては、セキュリティツールがなく、重大な脆弱性があり、インターネット上に晒されている資産が挙げられます。

セキュリティポスチャコントロールアプリケーションに付属するポリシーの一部は、重大な脆弱性とセキュリティツール範囲とのギャップの高リスクの組み合わせを探します。ただし、これらの組み合わせポリシーを機能させるには、脆弱性対応 アプリケーションと、脆弱性スキャナー統合製品 (Qualys、Rapid7、Tenable 脆弱性統合 アプリケーション) が 1 つ以上インストールされている必要があります。これらのアプリケーションは ServiceNow Store の個別のサブスクリプションで利用できます。

軽減コントロールモニタリング

セキュリティポスチャコントロール (SPC) ワークスペース内から、さまざまなセキュリティツールの構成方法に基づいて、利用可能な緩和コントロールによって資産に対するどの脅威が軽減されるかを把握できます。詳細については、「 緩和コントロールの監視 」を参照してください。

セキュリティポスチャコントロールでサポートされるアプリケーションのインストール

この統合に必要なアプリケーションは、ServiceNow Store で入手できます。一部のアプリケーションには、個別にダウンロードしてインストールする必要がある依存関係があります。

始める前に

必要なロール：すべてのアプリケーションのダウンロード、インストール、およびアクティベーションを行うアドミン。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 必要なアプリケーションを ServiceNow Store から ServiceNow インスタンスにダウンロードします。

   セキュリティポスチャコントロール (SPC Core) アプリケーションは、コアフレームワークを提供し、資産セキュリティポスチャ管理 (ASPM) に必要です。コンフィグレーションコンプライアンスアプリケーションとその依存関係により、資産セキュリティポスチャ管理を使用して見つけたセキュリティコントロールのギャップの修復タスクを作成できます。

   資産セキュリティポスチャ管理 **(ASPM)** アプリケーション

アプリケーション	アプリ **ID**
資産セキュリティポスチャ管理	(プラグイン ID：sn_sec_caasm)
ITOM Discovery ライセンス	(プラグイン ID：com.snc.itom.discovery.license)
セキュリティポスチャコントロールコア	(プラグイン ID：sn_sec_spc_core)
軽減コントロールモニタリング	(プラグイン ID:sn_sec_mit_ctr)
コンフィグレーションコンプライアンス (子アプリ secops_shared_components を含む)	(プラグイン ID：sn_vulc)
脆弱性対応 Licensing and Usage	(プラグイン ID：sn_vul_licensing)

   クラウドセキュリティポスチャ管理 **(CSPM)** アプリケーション

アプリケーション	アプリ **ID**
ディスカバリープラグイン	(プラグイン ID：com.snc.discovery)
クラウドコンフィグレーションガバナンス	(プラグイン ID：sn_itom_ccg)
CCG Content Pack	(プラグイン ID：sn_itom_ccg_cp)
CMDB CI クラスモデル	(プラグイン ID：sn_cmdb_ci_class)
Cloud Action Library	(プラグイン ID：com.sn.itom.cal)

   アプリケーションのダウンロードとアクティブ化の詳細については、「」のトピックを参照してください。

   - ServiceNow Store からのアプリケーションの初回ダウンロード。
   - ServiceNow Store アプリケーションのアクティブ化.

2. アプリケーションをダウンロードしたら、 **All** (すべて) > システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて).

3. ダウンロードしたアプリケーションを見つけ、[インストール] を選択して、それぞれの依存関係とともにアクティブ化します。
   アプリケーションとともに自動的にインストールされる依存関係アプリケーションは、[アプリケーションのインストール] ダイアログに表示されます。ただし、インストール中に依存関係プラグインをインストールするように求められた場合は、表示されるプロンプトに従ってください。前のテーブルに記載されているすべてのアプリケーションと依存関係がインストールされ、アクティブ化されていることを確認します。

   アプリケーションが正常にアクティブ化されると、ダイアログが表示されます。

   ServiceNow Store からのアプリケーションのダウンロードとインストールの詳細については、以下を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ServiceNow製品にオプトインするには、Opt in to the ServiceNow Store products の手順に従います。
- ServiceNow Store から購入したアプリケーションをインストールするには、「Install a ServiceNow Store application 」の手順に従います。
- または、他の Now Platform インスタンスでアプリケーションのエンタイトルメントを管理する場合は、「 Manage entitlements from your ServiceNow instance 」の手順に従います。

4. アプリケーションをインストールしてアクティブ化したら、ユーザーを次のセキュリティポスチャコントロールグループに割り当てます。

   これらのグループは、SPC レコードの読み取りと編集に必要なすべてのロールを継承します。

   SPC アドミングループ

   このグループのユーザーは、ライセンス情報を含む製品のすべてのレコードに対する読み取り/書き込みのフルアクセス権を持ちます。このグループの詳細なロールには、[sn_sec_caasm.analyst、sn_sec_caasm.caasm_security_admin、および sn_sec_spc_core.configure] が含まれます。

   SPC アナリストグループ

   このグループのユーザーは、製品のすべてのレコードに対する読み取り/書き込みのフルアクセス権を有しますが、ライセンス情報を表示することはできません。このグループの詳細なロールには、[pa_power_user と sn_sec_spc_core.analyst] が含まれます。

   SPC アナリスト読み取り専用グループ

   このグループのユーザーは、製品のすべてのレコードに対する読み取りのフルアクセス権を有しますが、ライセンス情報を表示することはできません。このグループの詳細なロールには、[pa_power_user、sn_sec_spc_core.analyst_read、sn_sec_caasm.read、および cmdb_ms_user] が含まれます。

   アプリケーションロールのサポート

   SPC と資産セキュリティポスチャ管理をサポートするアプリケーション (前の表にリスト) には、次のロールが必要です。

   - コンフィグレーションコンプライアンスアドミン [sn_vulc.admin] - コンフィグレーションコンプライアンスアプリケーションを設定し、すべてのレコードを表示し、プロパティを変更できます。コンフィグレーションコンプライアンス アプリケーションでロールをアサインします。
   - 脆弱性対応 アドミン [sn_vulc.admin] - 脆弱性対応アプリケーションと脆弱性リスク算出を構成します。
   - MID サーバー [mid_server] - MID サーバーを構成します。

5. オプション: **ignoreCIClass** [sn_sec_cmn.ignoreCIClass] システムプロパティを設定することで、CI ルックアップルールの実行時に一部の構成アイテム (CI) クラスを無視できるようになります。

   (Optional) SPC アドミンおよび SPC アナリストは、特定のハードウェアや仮想クラスを無視して、管理したくない資産に関する情報を取り込まないようにすることが必要になる場合があります。詳細については、「脆弱性対応 CI ルックアップルールの作成」と「CI クラスの無視」を参照してください。

6. 調整を変更し、CMDB データソースを再計算して、属性値の信頼できる情報源を設定します。

   CMDB 360 ダッシュボードは、CMDB 360 データのアグリゲーションと分析結果を表示します。CMDB 360 は、CI の属性値を報告するすべてのディスカバリーソースに関するデータを収

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

集します。構成管理データベース (CMDB) ワークスペースの CMDB 360 ビューを使用して、アクティビティを追跡し、ディスカバリーソースの潜在的な問題を特定します。詳細については、「CMDB 360 view in CMDB Workspace」を参照してください。

セキュリティポスチャコントロール のサービスグラフコネクタ

セキュリティポスチャコントロール は、セキュリティギャップの特定に使用される資産データのキーソースとして、API 統合またはサービスグラフコネクタに依存しています。

現在、セキュリティポスチャコントロール はサービスグラフコネクタ (SGC) をサポートし、資産に関するさまざまなデータを提供することができます。これらの統合アプリケーションは ServiceNow Store で入手できます。

使用するコネクタを選択し、アプリケーションをダウンロードしてアクティブ化します。セキュリティポスチャコントロール でサポートされるコネクタが増えるにつれ、ストアでサポートされるコネクタの一覧も増えていきます。

セキュリティポスチャコントロール機能を最大限に活用するには、以下のカテゴリをサポートするサービスグラフコネクタ製品をダウンロードしてアクティブ化することをお勧めします。

現在、セキュリティポスチャコントロール でサポートされているサービスグラフコネクタには、次のカテゴリがあります。

- デジタル従業員エクスペリエンス
- ディスカバリー
- エンドポイント管理：Microsoft Intune または Jamf デバイスとエンドポイントの管理。
- IT Asset Management
- インフラストラクチャモニタリング
- ネットワーク
- ネットワークセキュリティ
- ネットワークパフォーマンスモニタリング
- 構成とパッチ管理：MicrosoftSCCM または IBM Bigfix。
- エンドポイント保護：CrowdStrike または SentinelOne。
- クラウドプロバイダー：Amazon AWS クラウド、Microsoft Azure、GCP。

  注:
  クラウドディスカバリーがアクティブ化されている場合、これらのサービスグラフコネクタ製品は必要ありません。

- アプリケーションパフォーマンスモニタリング
- ディレクトリサービス (Active Directory) Microsoft Active Directory
- 脆弱性アセスメント：Qualys、Rapid7、または Tenable。

これらをインストールすると、インスタンスのコネクタテーブル [sn_sec_spc_core_connector] でコネクタやカテゴリを表示できるようになります。

[sn_sec_spc_core_asset_type_connector] テーブルでは、資産タイプと、CI クラスやコネクタへのマッピングを確認することができます。

これらのテーブルの詳細や例については、セキュリティポスチャコントロールでサポートされているハードウェアサービスグラフコネクタ および セキュリティポスチャコントロールでサポートされて

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

いるソフトウェアサービスグラフコネクタ を参照してください。広範なリストではありませんが、サポートされているコネクタがさまざまなデータを提供する仕組みを確認することができます。

セキュリティポスチャコントロール では、ソフトウェア資産管理 (SAM) や ハードウェア資産管理 (HAM) などの ServiceNow 製品がサポートされます。これらをサービスグラフコネクタと併用することで、脆弱性スキャナー製品から報告されたインストール済みソフトウェアと、スキャナーより報告されたソフトウェア (SAM などの ServiceNow 製品で既に構成されている) の間に存在する不一致を検索することができます。

サービスグラフコネクタのサポート対象アプリケーションのダウンロード、構成、アクティブ化の詳細については、以下のトピックを参照してください。

- Service Graph Connectors 。
- ServiceNow Store からのアプリケーションの初回ダウンロード。
- ServiceNow Store アプリケーションのアクティブ化。

セキュリティポスチャコントロール のポリシー

ポリシーを用いることで、サービスグラフコネクタからのインポートデータに基づいて資産を監査し、潜在的な違反を見つけることができるようになります。

ポリシー

セキュリティポスチャコントロール ポリシーは、「資産 - 関係性 - プロパティ」のデータモデルに基づいてビルドされています。アプリケーションにはポリシーが含まれているので、独自のポリシーを作成して特定の基準を検索することができます。

ポリシー基準は、資産や関連するエンティティのプロパティ条件の形式で指定できます。ワークスペースの [ポリシーと結果] モジュールのポリシービルダーから、ポリシーを定義して資産タイプ (ハードウェア、ソフトウェア)、接続 (レポートがあるもの、レポートがないもの)、エンティティ (資産ソース、サービスグラフコネクタ製品、CMDB メタデータ) を検索したり、他のタイプの特定の基準を照合したりすることができます。

ポリシーの変更や作成でできること：

- [資産検索] モジュールに条件を設定し、資産を特定のサービスグラフコネクタ製品で検索、またはレポートされている特定のデータを有する資産をコネクタで検索。検索はポリシーとして保存することができます。
- アプリケーションに含まれているポリシーをクローン作成して、より広範なポリシーを作成。既存ポリシーの条件をコピーして改良するだけで、再入力する必要はありません。
- 新しいポリシーの足掛かりとして選択した基本ポリシーを使用して、新しいポリシー (子ポリシー) を作成。

資産タイプとポリシー

これらのプライマリまたはトップレベルの資産タイプを、ポリシー定義の足掛かりとして使用します。

ハードウェア資産

ハードウェア資産とは、パーソナルコンピューティングデバイス、サーバー、ネットワークデバイス、クラウド仮想マシン、その他のハードウェアなどのあらゆるデバイスを示す抽象概念を指します。ポリシーでは、サービスグラフコネクタ製品およびソフトウェア資産管理 (SAM) や ITOM Discovery などの ServiceNow 製品からのインポートデータに基づいて、資産の潜在的な違反を監査します。

ソフトウェア資産

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ソフトウェア資産を使用すると、サービスグラフコネクタからのインポートデータによってレポートされたインストール済みソフトウェア、脆弱性スキャナー製品、スキャナーよりレポートされたソフトウェア (ソフトウェア資産管理 (SAM) などの ServiceNow 製品で既に構成済み) の間に存在する不一致を検索することができます。

エンティティおよびそのセカンダリエンティティとの関係性

エンティティ	関係	ターゲットエンティティ	説明
ハードウェア資産	報告者	資産ソース	この資産を CMDB に報告したソースを表します。
ハードウェア資産	報告者のみ	資産ソース	この資産を CMDB に報告する唯一のソースを表します。
ハードウェア資産	次を報告元としない	資産ソース	この資産を CMDB に報告しなかったソースを表します。
ハードウェア資産	IRM 例外あり	IRM 例外	Integrated Risk Management の例外レコードを表します。
ハードウェア資産	脆弱性あり	脆弱性	この資産で見つかった脆弱性を表します。
ハードウェア資産	構成結果あり	構成	この資産で見つかった構成とコンプライアンスの問題を表します。
ハードウェア資産	CMDB メタデータあり	CMDB メタデータ	この資産の CMDB CI プロパティのコレクションを表します。
ハードウェア資産	コネクタデータあり	サービスグラフコネクタ	この資産に対して選択したサービスグラフコネクタによって報告されるプロパティのコレクションを表します。
ハードウェア資産	集計データあり	集計データ	特定の資産についてさまざまなソースから報告された集計値を含むプロパティのコレクション。たとえば、OS です。
ハードウェア資産	CI クラスから	CMDB CI クラス	特定の CI クラスプロパティの条件を定義するために使用されます。
ハードウェア資産	クラウドメタデータあり	クラウドメタデータ	クラウドメタデータを表します (クラウド VM に適用)。
ハードウェア資産	インターネットに開かれているポートがある	OpenPort	インターネットに対してオープンなポート

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エンティティおよびそのセカンダリエンティティとの関係性 (続く)

エンティティ	関係	ターゲットエンティティ	説明
			を表します (クラウド VM に適用)。
ソフトウェア	報告者	資産ソース	このソフトウェアを報告したソースを表します。
ソフトウェア	報告者のみ	資産ソース	このソフトウェアを報告する唯一のソースを表します。
ソフトウェア	次を報告元としない	資産ソース	このソフトウェアを報告しなかったソースを表します。
ソフトウェア	ソフトウェア詳細情報あり	ソフトウェア	たとえば、パブリッシャーやバージョンなどのソフトウェアプロパティのコレクションを表します。

ポリシー監査とデータ入力の例：**CMDB** の **CI** クラス

ポリシーが、特定のサービスグラフコネクタによって報告されたまたは報告されなかった資産クラスを取得しようとすると、セキュリティポスチャコントロールは、サービスグラフコネクタやコネクタカテゴリによって入力されているまたは入力されていない CMDB 内の資産クラスに関連するすべての関連構成アイテム (CI) クラスをマップします。

たとえば、ポリシーがサービスグラフコネクタ Jamf Pro によって報告されるすべてのハードウェア資産を検索するとします。次のロジックが適用されます。

1. セキュリティポスチャコントロールは、Jamf Pro の「ハードウェア資産」クラスにマッピングされている CMDB 内の CI クラスを特定します。

   注:
   サービスグラフコネクタが異なれば CMDB で入力される CI クラスも異なり、「ハードウェア資産」から CI クラスへのマッピングはサービスグラフコネクタごとに異なります。

2. セキュリティポスチャコントロール により、CMDB 内の CI クラス、コンピューター、サーバー、およびプリンターが、サービスグラフコネクタ Jamf Pro の「ハードウェア資産」資産クラスにマッピングされていることが確認されます。
3. 次に、セキュリティポスチャコントロールは、CMDB 内でサービスグラフコネクタ Jamf Pro によってサーバー、コンピューター、プリンターの 3 つの CI クラスのいずれかに入力された資産レコードを照会し、それらの資産を返します。

   次のテーブルの [SPC でサポートされている CI クラス (CI classes supported by SPC)] 列は、ポリシー評価の一環として、セキュリティポスチャコントロール製品による照会中に考慮される CI レコードのクラスを示します。このテーブルは包括的なリストではありませんが、さまざまなカテゴリやソースから取り込まれたデータが一般的にどのようにマッピングされ、照会されるかを確認するために使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

独自のポリシーの作成

独自のポリシーを作成する方法について、詳しくは「セキュリティポスチャコントロール アプリケーションで独自のポリシーを作成」を参照してください。

ポリシーの例については、「セキュリティポスチャコントロール における基本ポリシー、子ポリシー、クローンポリシーの例」を参照してください。

ポリシーの作成に必要な手順の詳細については、「セキュリティポスチャコントロール のカスタムポリシーを作成してアクティブ化」を参照してください。

サポートされている **SGC**

サポートされているサービスグラフコネクタのリストについては、セキュリティポスチャコントロールでサポートされているハードウェアサービスグラフコネクタ および セキュリティポスチャコントロールでサポートされているソフトウェアサービスグラフコネクタ を参照してください。

緩和コントロールポリシー

セキュリティポスチャコントロール (SPC) ワークスペース内から、さまざまなセキュリティツールの構成方法に基づいて、利用可能な緩和コントロールによって資産に対するどの脅威が軽減されるかを把握できます。詳細については、「の緩和コントロールとポリシー セキュリティポスチャコントロール」を参照してください。

セキュリティポスチャコントロール アプリケーションに含まれているポリシー

セキュリティポスチャコントロールアプリケーションには、重要なユースケースに関連付けられ、最終的にSPCワークスペースのランディングページ (ホームモジュール) のダッシュボードに主要なインサイトとして表示されるポリシーがいくつかあります。

ポリシーの表示

これらのポリシーを表示するには、 ワークスペース > セキュリティポスチャコントロール > ポリシーと検出結果 > **All** (すべて).

これらのポリシーはデフォルトで非アクティブ化されています。返された結果 (検索結果) を表示するには、これらをアクティブ化する必要があります。これらのポリシーは編集できませんが、足掛かりとしてポリシー条件をクローン作成すると、他のポリシーを作成できるようになります。詳細については、「セキュリティポスチャコントロールでポリシーのクローンを作成するか、子ポリシーを作成する」を参照してください。

これらのポリシーをクローン作成することで独自のカスタムポリシーを作成できますが、クローン作成したポリシーは、アプリケーションに含まれる重要インサイトとともにホームランディングページのダッシュボードに重要インサイトとして反映されません。ただし、これらのクローンポリシーの検索結果を構成し、これらのポリシーから返された結果を確認することはできます。

クローン作成されたポリシーのカスタムインサイトまたはレポートを構成したり、これらのクローン作成されたポリシーの結果を構成して修復を管理したりすることもできます。独自のカスタムポリシーを最初から作成し、内部要件に従ってセキュリティコントロール範囲を監視することもできます。

アプリケーションに付属するポリシーには、次のカテゴリが含まれます。

- セキュリティコントロールの範囲を監視するポリシー (エンドポイント保護と脆弱性スキャナー)。
- 管理対象外のデバイスを識別するポリシー。
- セキュリティコントロールの欠落、インターネットへの露出などの重要な組み合わせを含む有害な組み合わせを監視するポリシー。
- 緩和コントロールモニタリングのための SPC API 統合のポリシー。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

作成したポリシーをクローン作成してアクティブ化したら、ワークスペースのカスタムインサイトビルダーモジュール (ナビゲーターパネルの最後のモジュール) に独自のカスタムインサイトレコードを作成する必要があります。これを作成して初めて、カスタムインサイトダッシュボード (ワークスペースの上から 2 番目のアイコン) でポリシーのデータを表示できるようになります。

独自のポリシーの作成

独自のポリシーを作成する方法について、詳しくは「セキュリティポスチャコントロール アプリケーションで独自のポリシーを作成」を参照してください。

ポリシーの例については、「セキュリティポスチャコントロール における基本ポリシー、子ポリシー、クローンポリシーの例」を参照してください。

ポリシーの作成に必要な手順の詳細については、「セキュリティポスチャコントロール のカスタムポリシーを作成してアクティブ化」を参照してください。

緩和コントロールの監視に使用されるポリシーの詳細については、 の緩和コントロールとポリシー セキュリティポスチャコントロール を参照してください。

セキュリティポスチャコントロール アプリケーションで独自のポリシーを作成

独自のカスタムポリシーを作成して、環境内の資産固有のデータを監視することができます。これらのポリシーは、インストールしてアクティブ化したさまざまなサービスグラフコネクタからのインポートデータをベースにして作成することができます。

はじめに

既存のポリシーをクローン作成してさらに条件を追加するか、ポリシーを最初から作成することができます。カスタムポリシーには、さまざまなサービスグラフコネクタによって入力される共通の CMDB プロパティの基準を含めることができます。

また、ベースポリシーを足掛かりにして、承認済みの例外の条件を [ガバナンス、リスク、コンプライアンス (GRC)] アプリケーションなどのポリシーに含めることもできます。これらの例外は、監視を行わないものの、資産として計上される資産に適用されます。

カスタムポリシーには、たとえば古いソフトウェアで資産を監視するために、OS、OS バージョン、FQDN などのメタデータの条件を含めることができます。これらのプロパティは、任意の資産のさまざまなサービスグラフコネクタによって入力される共通の CMDB プロパティであることに注意してください。

ポリシーのポリシー条件ビルダーにおけるトップレベルの資産タイプやその関係の詳細については、セキュリティポスチャコントロール アプリケーションに含まれているポリシー を参照してください。

ポリシーの例については、「セキュリティポスチャコントロール における基本ポリシー、子ポリシー、クローンポリシーの例」を参照してください。

ポリシーの作成に必要な手順の詳細については、「セキュリティポスチャコントロール のカスタムポリシーを作成してアクティブ化」を参照してください。

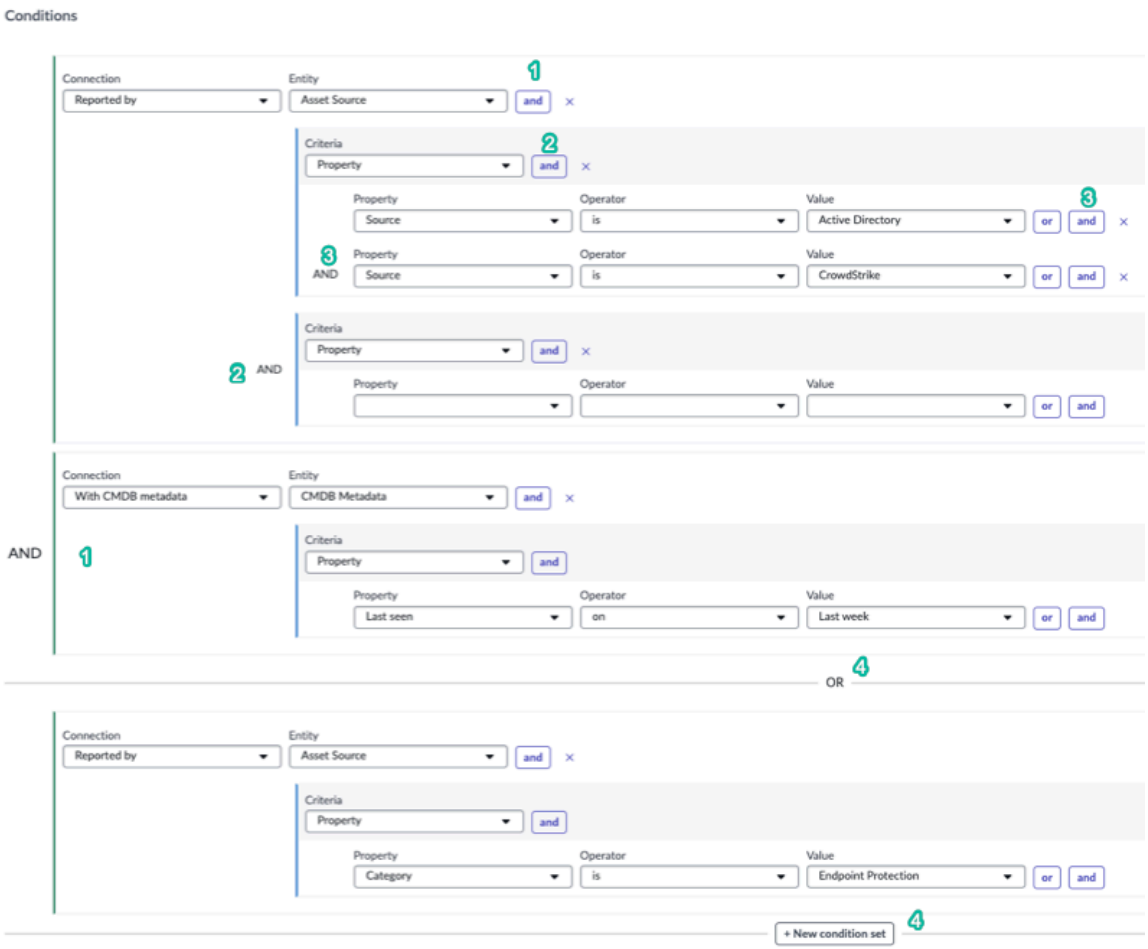
条件ビルダーで **AND / OR** のデコレータを使用する

ワークスペースのポリシーおよび検索結果モジュールにある条件ビルダーを使用すると、ハードウェアやソフトウェアのトップレベルの資産タイプからセカンダリエンティティまで移動することができます。選択内容に応じてフィールドが表示され、クライテリアを変更または追加することができます。

条件ビルダーの AND、OR デコレータを使用すると、ポリシーに対して返されるデータのロジックを設定できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

デコレータ	説明	画像で参照されている番号
新規の条件セットは、最上部の [接続] フィールドや [エンティティ] フィールドの横にある **[AND]** を選択します。	論理 AND を「接続 - エンティティ」のクライテリアと、別の「接続 - エンティティ」の新たなクライテリア間に追加します。	1
新規のクライテリアやプロパティ条件のセットは [クライテリア] または [プロパティ] フィールドの右側にある **[AND]** を選択します。	論理 AND を「接続 - エンティティ」のクライテリアと、同じ「接続 - エンティティ」の新たなクライテリア間に追加します。	2
新規のプロパティ条件のセットは [プロパティ] フィールドの右側にある **[OR] / [AND]** を選択します。	論理 OR/AND を現行のプロパティと、同じ「接続 - エンティティ - クライテリア」の新たなプロパティ間に追加します。	3
新規の条件セットは、**[+** 新規の条件セット (+ New condition set)] を選択します。	論理 OR を、現行のすべてのクライテリアにおける条件セットと新たな条件セット間に追加します。	4



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

基本ポリシー、クローン作成、子ポリシーの使用

複数のポリシーで資産を評価し、独自のカスタムインサイトを作成することができます。次のオプションを使用すると、カスタムポリシーの作成や既存のポリシーの編集をすばやくできるようになります。

- ポリシーのクローン作成：ポリシーのコピーを作成します。ポリシー名や条件と併せて「copy」の文字がタイトルに表示されます。条件が表示され、編集することができます。「セキュリティポスチャコントロール でアクティブ化されたポリシーを編集する」を参照してください。
- 子ポリシーの作成：元のポリシーの名前が「基本ポリシー」として新しいレコードに表示されます。基本ポリシーの条件は新しいポリシーに継承され、新規の条件セットが空白の状態で表示されます。「セキュリティポスチャコントロールでポリシーのクローンを作成するか、子ポリシーを作成する」を参照してください。
- 除外ポリシー：カスタムポリシーにポリシーを追加して、選択したポリシーで資産が見つかっても、これらが結果に含まれないようにします。「セキュリティポスチャコントロール のカスタムポリシーを作成してアクティブ化」を参照してください。

メタデータと **CMDB** フィルタリング

セキュリティチームが古いソフトウェアを使用して資産を監視することが重要であるという場合があります。ハードウェア資産タイプの後に「CMDB メタデータあり」の接続から開始するポリシー基準を指定して、以下にリストされている共通プロパティを含めることができます。このリストはすべてを網羅していません。このメタデータを収集するには、サービスグラフコネクタによって入力される CMDB メタデータ接続からプロパティが利用できる必要があります。

- RAM
- ホスト名
- シリアル番号
- OS ドメイン
- OS バージョン
- ディスクスペース
- 最終確認日
- OS
- 初回確認日
- CPU カウント
- MAC メーカー
- NIC
- IP アドレス
- 場所
- FQDN
- ネットマスク
- IP バージョン
- シリアル番号タイプ
- OS サービスパック

セキュリティポスチャコントロール v3.0 以降：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

「CMDB メタデータあり」の接続では、ホスト名のプロパティを追加し、matches regex 演算子を使用することで、ハードウェア資産タイプの条件に正規表現を入力することができます。たとえば、「lp」と入力すると、ホスト名の 2 文字目と 3 文字目が「lp」となるノート PC をすべて検索することができます。

「初回確認」：任意のソースで、「初回確認」のタイムスタンププロパティで選択した期間内で初めて検出された資産。

「最終確認」：任意のソースで「過去 n 日以内で最後に確認された」資産。[値] には 30 までの日数を入力します。たとえば、過去 3 日間において Active Directory からの「最終ログオン」で資産を監視する場合、[値] には 3 を入力します。

ソフトウェア資産タイプ：「ソフトウェア詳細情報あり」の接続から開始する場合、ソフトウェア公開者を検索するか、インストール済みの SGC を使用して必要なソフトウェアデータやメタデータをインポートします。

ハードウェア資産タイプにおいて、デバイスが特定のモデルやモデル情報に基づく場合、「モデル情報あり」の接続と「CMDB メタデータあり」の接続を併用することができます。

また、Qualys などのソースで報告されている資産のうち、ServiceNow ITOM ディスカバリーで報告されていない資産をすべて検索することもできます。

セキュリティポスチャコントロール ポリシースキーマの詳細については、セキュリティポスチャコントロール のポリシー を参照してください。

ガバナンス、リスク、コンプライアンス (GRC) アプリケーションでの例外

Integrated Risk Management (IRM) 例外は、ガバナンス、リスク、コンプライアンス (GRC) 製品での承認された例外を含む資産です。ポリシーには、例外の条件を追加して、これらの資産を監視してカウントに含めないようにするオプションがあります。

たとえば、一部の資産には、IRM での特定のコントロール目標に対する承認された例外がある場合があります。返される一致を減らすために、情報セキュリティチームは、既に承認されている IRM 例外があるセキュリティコントロールの監視からこれらの資産を除外できます。

セキュリティポスチャコントロール の重要インサイトおよび構成済みインサイト

重要インサイトや構成済み（カスタム）インサイトにより、レポートに視覚性がもたらされ、資産と一致するアセスメント基準に準じた作成および更新が実現します。インサイトは、ダッシュボードのセキュリティコントロール測定基準を監視するのに役立ちます。

主要なインサイト

資産のアセスメントに使用される基準は、アプリケーションに含まれているポリシーによって提供されます。

- 主要なインサイトは、アプリケーションに含まれているポリシーを使用します。
- 構成済みインサイトは、アプリケーションに含まれるポリシー、独自のカスタムポリシー、またはその両方の組み合わせを使用して作成することができます。

セキュリティポスチャコントロールワークスペースのホーム (ランディングページ) の [概要] の下にある [主要なインサイト] セクションには、アプリケーションに含まれるポリシーによって作成および更新されるビジュアルレポートが表示されます。これらのインサイトはアプリケーションにも含まれており、次の情報が表示されます。

- インストールされているエンドポイント保護エージェント：エンドポイント保護がある資産またはない資産の合計数。
- 管理対象デバイスのカバー範囲：管理対象資産と非管理対象資産との比較。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 脆弱性スキャンのカバー範囲：スキャンされた資産の合計数。サードパーティの脆弱性スキャナーによって既知の脆弱性がスキャンされなかった資産と比較されます。
- 重大な脆弱性がある資産：重大な脆弱性がある資産の合計数に対する資産の数。
- 重要度別の脆弱性一致アイテム：重大度別に分類された脆弱性一致アイテムの合計数。既知の脆弱性が CMDB 内の資産と一致すると、脆弱性一致アイテムになります。このインサイトを使用するには、脆弱性対応アプリケーションと、少なくとも 1 つのスキャナー統合 (Qualys、Rapid7、または Tenable 脆弱性統合) をインストールする必要があります。すべてのアプリケーションは ServiceNow Store から入手可能です。
- 検索結果別の上位 3 つのポリシー：資産で最も多くの検出結果 (一致) を返すポリシー。

構成済みインサイト

主要なインサイトにはない詳細情報が必要な場合は、独自のインサイトを作成できます。アセスメント用に構成済みインサイトを作成したり、既存のポリシーや独自のカスタムポリシーを使用したりすることができます。構成済みインサイトは、構成済みインサイトのダッシュボードモジュール (ワークスペースの上から 2 番目のアイコン) に表示されます。

次のタイプのインサイトを構成できます。

- 比較グラフ：複数のポリシー間の結果を棒グラフで比較します。
- ポリシー一致数ウィジェット：ポリシーに一致するデバイスの数を表示します。
- ポリシー一致率グラフ：ポリシーに一致するデバイスの割合を円グラフで表示します。SPC によって監視されるすべての資産、または現在選択されているポリシーの作成元である基本ポリシーに一致する資産として、総資産プールを選択できます。
- ポリシー傾向グラフ：さまざまなポリシーに一致する資産の傾向を表示します。

構成済みインサイトを作成する手順の詳細については、「セキュリティポスチャコントロールの構成済みインサイトを作成してアクティブ化する」を参照してください。

グループ

[カスタムインサイトビルダー] モジュールで新しいレコードを作成する場合、グループを作成するか、グループを構成済みインサイトにアサインする必要があります。構成済みインサイトのダッシュボードでレポートを整理できるようになります。

インサイトはグループ分けできます。各グループには、21 個のウィジェットまたはインサイトを含めることができます。

セキュリティポスチャコントロール ワークスペースの使用

セキュリティポスチャコントロール ワークスペースには、資産に関するインポートデータの構成、使用、監視で使用するモジュールが含まれています。

ロール

SPC アドミングループ

このグループのユーザーは、ライセンス情報を含む製品のすべてのレコードに対する読み取り/書き込みのフルアクセス権を持ちます。このグループの詳細なロールには、[sn_sec_caasm.analyst、sn_sec_caasm.caasm_security_admin、および sn_sec_spc_core.configure] が含まれます。

SPC アナリストグループ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このグループのユーザーは、製品のすべてのレコードに対する読み取り/書き込みのフルアクセス権を有しますが、ライセンス情報を表示することはできません。このグループの詳細なロールには、[pa_power_user と sn_sec_spc_core.analyst] が含まれます。

SPC アナリスト読み取り専用グループ

このグループのユーザーは、製品のすべてのレコードに対する読み取りのフルアクセス権を有しますが、ライセンス情報を表示することはできません。このグループの詳細なロールには、[pa_power_user、sn_sec_spc_core.analyst_read、sn_sec_caasm.read、および cmdb_ms_user] が含まれます。

アプリケーションロールのサポート

SPC と資産セキュリティポスチャ管理をサポートするアプリケーションには、次のロールが必要です。

- コンフィグレーションコンプライアンスアドミン [sn_vulc.admin] - コンフィグレーションコンプライアンスアプリケーションを設定し、すべてのレコードを表示し、プロパティを変更できます。コンフィグレーションコンプライアンス アプリケーションでロールをアサインします。
- 脆弱性対応 アドミン [sn_vulc.admin] - 脆弱性対応アプリケーションと脆弱性リスク算出を構成します。
- MID サーバー [mid_server] - MID サーバーを構成します。

ワークスペースのモジュール

ワークスペースにアクセスするには、次に移動します: ワークスペース > セキュリティポスチャコントロール ホーム (ランディング) ページが表示されます。セキュリティポスチャコントロール ワークスペースには、次のモジュールが含まれています。

モジュール

モジュール	説明
ホーム	[概要]、[主要なインサイト]、[主要なユースケース範囲] のセクションでデータの可視化などの情報を表示して、資産を監視することができます。 このページで提供される情報により、全体的なセキュリティ体制のステータスを IT 部門、IT およびセキュリティマネージャー、その他の主要ステークホルダーに報告できるようになります。 「セキュリティポスチャコントロール の重要インサイトおよび構成済みインサイト」および「セキュリティポスチャコントロール のポリシー」を参照してください。
構成済みインサイト	作成、構成、アクティブ化した資産に関するデータを可視化して表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール (続く)

モジュール	説明
	「セキュリティポスチャコントロール の重要インサイトおよび構成済みインサイト」を参照してください。
資産検索	設定した条件に基づいて、環境内の資産をすばやく検索します。 これらの条件をポリシーにコミットする前に、その条件のセットを持つ資産を見つけられることを確認します。これらの検索を絞り込んで、検索条件を満たす資産のプレビューを表示できます。準備が整ったら、条件をポリシーとして保存できます。 「セキュリティポスチャコントロールでの資産検索の作成」を参照してください。
ポリシーと検索結果	ポリシーを作成、クローン作成、編集、アクティブ化します。アプリケーションにはポリシーが含まれているので、独自のポリシーを作成することができます。 ポリシーは資産を監査して、潜在的な違反の一致を見つけます。インサイト、可視化、ユースケースはポリシーに依存します。「セキュリティポスチャコントロール のポリシー」を参照してください。 ポリシー条件に一致する資産は検索結果として報告され、修復の コンフィグレーションコンプライアンス アプリケーションにマッピングされます。「セキュリティポスチャコントロールの検索結果を表示」を参照してください。
コネクタとユースケースのセットアップ	インストールされているサービスグラフコネクタ (SGC) と API 統合のステータスをアクティブ化して表示します。サービスグラフコネクタと API 統合は、資産データのインポートで使用するソースとなります。さまざまな (SGC) がサポートされ、 ServiceNow Store で入手することができます。 主要なユースケースを設定して監視します。ユースケースは、特定タイプのツール範囲のギャップを識別するために構成するさまざまなシナリオです。各ユースケースには、潜在的な違反について資産を監査するためのポリシーが必要です。 「セキュリティポスチャコントロール におけるユースケース、ポリシー例、サポートされるサービスグラフコネクタ」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール (続く)

モジュール	説明
カスタムインサイトビルダー	独自のデータ可視化を作成します。カスタムインサイトでは、ポリシーやインポートデータの監査結果によって更新されるレポートを視覚的なかたちで提供します。 これらがアクティブ化されると、カスタムインサイトが [構成済みインサイト] モジュールのダッシュボードに表示されます。[グループ] を使用すると、ダッシュボードでのインサイトデータの表示場所を決めることができます。 「セキュリティポスチャコントロールの構成済みインサイトを作成してアクティブ化する」を参照してください。

ワークスペースのモジュールでツール範囲のギャップを特定

セキュリティツールのギャップを特定するには、次の手順を実行する必要があります。

1. さまざまなカテゴリで使用しているいずれかのツールを使用して API 接続を設定し、アクティブ化します。必要な API 接続には、ServiceNow Store から入手できる製品にサービスグラフコネクタを使用できます。サポートされているサービスグラフコネクタの詳細については、「セキュリティポスチャコントロール のサービスグラフコネクタ」と「Service Graph Connectors」を参照してください。サポートされているサービスグラフコネクタは、個別のサブスクリプションで ServiceNow Store から入手できます。
2. 特定の基準に基づいて 1 つ以上の資産検索を実行して、インベントリを取得します。
3. セキュリティポスチャコントロールアプリケーションに備わるポリシーをアクティブ化します。また、独自のポリシーを作成して、資産検索の結果に基づきアクティブ化することもできます。
4. 独自の構成済みインサイトを作成してアクティブ化すると、資産を監視できるようになります。
5. さまざまなセキュリティツールの構成方法に基づいて、利用可能な緩和コントロールによって資産に対するどの脅威が軽減されるかを把握するには、「 での緩和コントロールモニタリングの使用セキュリティポスチャコントロール」を参照してください。
6. コンフィグレーションコンプライアンスアプリケーションの修正ワークフローを自動化するルールを設定します。

セキュリティツールのギャップを特定するには、次の手順を実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. セキュリティポスチャコントロールアプリケーションに備わるポリシーをアクティブ化します。セキュリティポスチャコントロール製品は、次のタスクを実行して、セキュリティツールのギャップを検出します。
   a. CMDB のさまざまなサービスグラフコネクタによって入力されたすべての一意の資産のリストを特定します。
   b. エンドポイント保護など、この資産プールから特定のカテゴリによって報告されていない資産を特定します。資産は、評価対象のアクティブなポリシーに基づいて特定されます。
   c. 特定のカテゴリで報告されていないと特定された資産は、コンフィグレーションコンプライアンスアプリケーションで「検出結果」または「テスト結果」として報告されます。
2. コンフィグレーションコンプライアンスアプリケーションで、修復のためにさまざまなチームに「検出結果」を自動的にアサインします。

独自のポリシーの作成

独自のポリシーを作成する方法について、詳しくは「セキュリティポスチャコントロール アプリケーションで独自のポリシーを作成」を参照してください。

ポリシーの作成に必要な手順の詳細については、「セキュリティポスチャコントロール のカスタムポリシーを作成してアクティブ化」を参照してください。

ポリシーの例については、「セキュリティポスチャコントロール における基本ポリシー、子ポリシー、クローンポリシーの例」を参照してください。

セキュリティポスチャコントロールアプリケーションに含まれているポリシーをアクティブ化する

アプリケーションに含まれるポリシーは、セキュリティポスチャコントロールでそのポリシーに一致する資産を監視する前にアクティブ化しておく必要があります。デフォルトでは、アプリケーションに含まれているポリシーはいずれもアクティブになっていません。

始める前に
アプリケーションに含まれるポリシーをアクティブ化する前に、必要なすべての前提条件が満たされていることを確認する必要があります。

- 必要なサービスグラフコネクタがアクティブ化されていることを確認します。
- 該当する場合は、脆弱性対応などの必要なアプリケーションがインストールされ、アクティブ化されていることを確認します。
- 緩和コントロールの監視に使用されるポリシーの詳細については、「 の緩和コントロールとポリシー セキュリティポスチャコントロール」を参照してください。

注:

アプリケーションに含まれるポリシーを編集することはできませんが、[ポリシーのクローン作成 **(Clone policy)**] 機能と [子ポリシーを作成 **(Create child policy)**] 機能を使用して、基準に基づいて新しいポリシーを作成できます。これらの機能は、[その他のオプション] メニュー (縦に並んだ 3 つのドット) で利用できます。

必要なロール：SPC アドミングループまたは SPC アナリストグループ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > セキュリティポスチャコントロール > ポリシーと検出結果 > **All** (すべて).

   ポリシーがアクティブ化されているかどうかを判断するには、[アクティブ] 列でそのステータス (True または False) を確認します。

2. ポリシーレコードを選択して開きます。
3. アプリケーションに含まれるポリシーレコードには、次のオプションがあります。

オプション	説明
ポリシーをアクティブ化	ポリシー条件に一致する資産を監視し、結果を生成する場合は、ポリシーをアクティブ化します。 使用可能な場合は、[ポリシーを非アクティブ化] を選択して、このポリシーの資産評価と結果の生成を停止します。
検索結果を構成	モーダルで [はい] を選択して、ポリシーの検索結果を生成します。 [アサインルールを構成] リンクを選択して、コンフィグレーションコンプライアンスアプリケーションでアサインルールを設定し、解決のためにポリシーの検索結果を割り当てます。 **注:** 資産タイプが「ソフトウェア」のポリシーを作成する場合、ポリシーを保存してカスタムインサイトを作成することはできますが、ポリシーレコードから結果を構成することはできません。
Clone policy (ポリシーのクローン作成)	表示されたポリシーのすべての条件を開始点として、新しいポリシーを作成します。 詳細については、「セキュリティポスチャコントロール のカスタムポリシーを作成してアクティブ化」を参照してください。
子ポリシーを作成 (Create child policy)	現在のポリシーの条件を継承する子ポリシーを作成します。現在のポリシー条件が新しいレコードの [基本ポリシー] フィールドに表示され、さらに条件を追加します。
ポリシーを非アクティブ化 (アクティブ化されたポリシーにのみ表示)	ポリシーを用いて資産を監視したり評価したりしない場合、アクティブなポリシーを非アクティブ化します。この編集オプションは、アク

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
	ティブ化されたポリシーレコードでのみ表示されます。
検索結果を表示	新しいタブを開き、一致する資産がある場合は表示します。検索結果は、ポリシーの CTR またはテスト結果レコードでも参照されます。

セキュリティポスチャコントロール のカスタムポリシーを作成してアクティブ化

独自のカスタムポリシーを作成して、ツール範囲やその他の高リスクの組み合わせについて資産を監視します。

始める前に

ポリシーの作成に必要な手順の詳細については、「セキュリティポスチャコントロール における基本ポリシー、子ポリシー、クローンポリシーの例」を参照してください。この例では、基本ポリシーの作成、基本ポリシーを使用した子ポリシーの作成、ポリシーのクローン作成に必要な手順について説明します。

ポリシーの例については、「セキュリティポスチャコントロール における基本ポリシー、子ポリシー、クローンポリシーの例」を参照してください。

必要なロール：SPC アドミングループまたは SPC アナリストグループ

手順

1. 次のように移動する。 ワークスペース > セキュリティポスチャコントロール > リスト > ポリシー > **All** (すべて).
2. [新しいポリシー] を選択します。
3. 上部の名前の横にある鉛筆アイコンを選択して、メタデータを変更します。

   フィールドに入力します。

フィールド	説明
名前	一意のポリシー名です。
重要度	リストから 1 つ選択します。
簡単な説明	一意のポリシーの説明です。

4. [メタデータを保存 **(Save Metadata)]** を選択します。
5. 資産のタイプをリストから選択します。
6. オプション: 「なし」「どちらか 1 つ」「両方」のいずれかを選択します。

   (Optional) [接続] フィールドと [エンティティ] フィールドが表示されます。
7. [接続] フィールドのリストから 1 つ選択します。
   ターゲットの [エンティティ] フィールドは、選択に応じて自動入力されます。新規の [クライテリア] フィールドが [プロパティ]、[演算子]、[値] のフィールドとともに表示されます。資産タイプや関係のスキーマの詳細については「セキュリティポスチャコントロール のポリシー」を参照してください。
8. [プロパティ] のリストから 1 つ選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

9. [カテゴリ] または [ソース] を選択します。
10. 演算子を選択し、コネクタのカテゴリ (エンドポイント管理など) またはカテゴリの製品名 (ソース) を入力します。
11. オプション: 条件ビルダーで条件や条件セットを追加します。

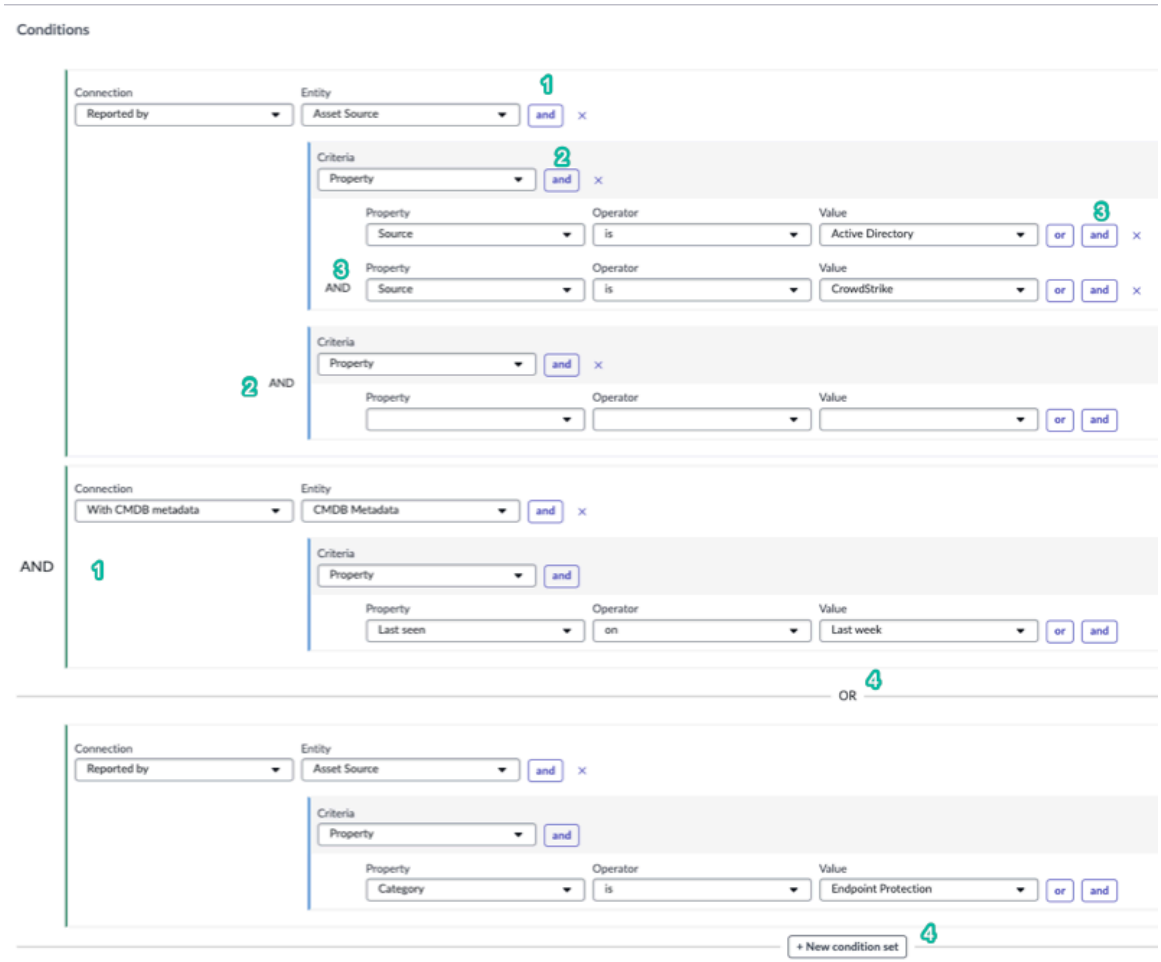
    (Optional) 条件ビルダーで、ハードウェアやソフトウェアのトップレベルの資産タイプからセカンダリエンティティに移動することができます。選択内容に応じてフィールドが表示され、クライテリアを変更または追加することができます。

    条件ビルダーの AND、OR デコレータを使用すると、ポリシーに対して返されるデータのロジックを設定できます。詳細については、次のテーブルおよび画像を参照してください。

デコレータ	説明	画像で参照されている番号
新規の条件セットは、最上部の [接続] フィールドや [エンティティ] フィールドの横にある **[AND]** を選択します。	論理 AND を「接続 - エンティティ」のクライテリアと、別の「接続 - エンティティ」の新たなクライテリア間に追加します。	1
新規のクライテリアやプロパティ条件のセットは [クライテリア] または [プロパティ] フィールドの右側にある **[AND]** を選択します。	論理 AND を「接続 - エンティティ」のクライテリアと、同じ「接続 - エンティティ」の新たなクライテリア間に追加します。	2
新規のプロパティ条件のセットは [プロパティ] フィールドの右側にある **[OR] / [AND]** を選択します。	論理 OR/AND を現行のプロパティと、同じ「接続 - エンティティ - クライテリア」の新たなプロパティ間に追加します。	3
新規の条件セットは、**[+** 新規の条件セット (+ New condition set)] を選択します。	論理 OR を、現行のすべてのクライテリアにおける条件セットと新たな条件セット間に追加します。	4

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



12. 編集が完了したら、[ポリシーを保存] を選択します。
ポリシーが保存されます。今すぐアクティブ化するか、後でアクティブ化するかを選択できます。
13. [ポリシーを保存] の横にある [その他のオプション] メニューから、[検索結果を構成] を選択します。
14. フィールドに入力します。

オプション	説明
このポリシーの検出結果を生成しますか？	一致する資産の検索結果を生成する場合は、[はい] を選択します。データがインポートされると、選択した [検索結果を表示] がポリシーレコードに表示されます。 検索結果を生成しない場合は、[いいえ] を選択します。
アサインルールを構成	リンクを選択してアサインルールを設定し、コンフィグレーションコンプライアンスアプリケーションで修復のために検索結果をアサインします。[sn_vulc_assignment_rule_list] テーブルには、コンフィグレーションコンプライアンスで使用できるデフォルトのアサインルールがあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

15. [構成を保存] を選択します。

    ポリシーを保存してアクティブ化すると、次回の実行時にスケジュールされているサービスグラフコネクタからのインポートデータが評価されます。ワークスペースの構成済みインサイトのダッシュボードにデータを表示する場合は、カスタムインサイト構成モジュールで新しいインサイトを作成する必要があります。構成済みインサイトをアクティブ化すると、データがワークスペースの構成済みインサイトのダッシュボード に表示されます。

セキュリティポスチャコントロール でアクティブ化されたポリシーを編集する

アクティブ化されたポリシーを編集することで、条件をカスタマイズして資産との一致性を高めることができます。

始める前に

アプリケーションに含まれているポリシーは編集できませんが、ポリシーをクローン作成して子ポリシーを作成することはできます。「セキュリティポスチャコントロールでポリシーのクローンを作成するか、子ポリシーを作成する」を参照してください。

ポリシーを編集して変更内容を公開すると、バージョンが追跡され、ポリシーレコードと関連のテスト結果にバージョン番号が表示されます。

アクティブ化されたポリシーを編集する場合は、予めポリシーを非アクティブ化して、編集中はポリシーによる資産評価が行われないようにしておいた方がよいでしょう。

必要なロール：SPC アドミングループまたは SPC アナリストグループ

手順

1. 次のように移動する。 ワークスペース > セキュリティポスチャコントロール > リスト > ポリシー > **All** (すべて).
2. ポリシーレコードを選択して開きます。
3. **[** ポリシーを編集] を選択します。
   初めて編集する場合は、アクティブな [編集モードを終了 **]** ボタンの横に非アクティブボタンが 2 つ ([変更を保存] と [変更を公開]) 表示されます。前回、ポリシーを編集してドラフト保存している場合は、「未公開の編集があります」という通知も表示されます。
4. 編集を行い、いずれかを選択して続行します。

オプション	説明
変更内容を保存	変更内容を「ドラフト」として保存し、編集モードに戻ります。この時点では変更内容が公開されていないため、ポリシーに戻って後で編集を続行することができます。
変更を公開	変更内容を新しいバージョンのポリシーとして公開します。編集モードは自動的に終了します。 ポリシーの [検索結果を表示] ボタンにおいて、検索結果が新しいバージョンのポリシーで表示されるまで、少し時間がかかる場合があります。 新しいバージョンのポリシーを公開する場合、オプションにより、変更したポリシーに関する既存の検索結果をすべてクローズすることがで

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
	きます。変更したポリシーの検索結果のみを表示する場合は、元のポリシーによる既存の検索結果はクローズすることをお勧めします。 この時点でキャンセルしたり、編集モードを終了したりすると、ポリシーに未公開の編集があることを示すメッセージが表示されます。 既存の関連テスト結果 (検索結果) をクローズする場合、テスト結果や修復タスクのステータスは、コンフィグレーションコンプライアンスアプリケーションのステータス移行プロセスに従って移行します。詳細については、「セキュリティポスチャコントロール アプリケーションのテスト結果と修復タスクのステータス移行」を参照してください。
バージョン履歴を表示	変更内容を公開すると、バージョンが追跡され、ポリシーレコードと関連のテスト結果にバージョン番号が表示されます。
編集モードを終了	変更内容を保存せずに終了する、または変更内容を保存して公開せずに終了します。変更内容を保存して公開しない場合、検索結果の作成は新しいバージョンを公開してから行う必要があります。
ポリシーを非アクティブ化 (アクティブ化されたポリシーにのみ表示)	ポリシーを用いて資産を監視したり評価したりしない場合、アクティブなポリシーを非アクティブ化します。この編集オプションは、アクティブなポリシーレコードでのみ表示されます。
検索結果を表示	新しいタブを開き、一致する資産がある場合は表示します。検索結果は、ポリシーの CTR またはテスト結果レコードでも参照されます。

5. ポリシーをドラフトとして保存し、編集モードを終了したら、次のオプションを選択します。

オプション	説明
ポリシーを編集	編集モードに戻ります。
ポリシーを非アクティブ化 (アクティブ化されたポリシーにのみ表示)	ポリシーを用いて資産を監視したり評価したりしない場合、アクティブなポリシーを非アクティブ化します。 このオプションは、アクティブなポリシーレコードでのみ表示されます。
その他のオプションメニュー	
検索結果を構成	モーダルで [はい] を選択して、ポリシーの検索結果を生成します。「セキュリティポスチャコントロールの検索結果を表示」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
Clone policy (ポリシーのクローン作成)	ポリシーレコードのコピーを作成します。「セキュリティポスチャコントロールでポリシーのクローンを作成するか、子ポリシーを作成する」を参照してください。
子ポリシーを作成	このポリシーをベースにして、新しいポリシーを作成します。「セキュリティポスチャコントロールでポリシーのクローンを作成するか、子ポリシーを作成する」を参照してください。
ポリシーを削除します	ポリシーリストからポリシーレコードを削除します。
検索結果を表示	新しいタブを開き、一致する資産がある場合は表示します。検索結果は、ポリシーのテスト結果レコード (CTR) でも参照されます。
リンクされたレコードを表示	公開ポリシーの場合、カスタムインサイトが表示されます (使用可能な場合)。「セキュリティポスチャコントロールの構成済みインサイトを作成してアクティブ化する」を参照してください。

セキュリティポスチャコントロールでポリシーのクローンを作成するか、子ポリシーを作成する

既存のポリシーのクローンを作成し、それに条件を追加して、独自のカスタムポリシーを作成します。既存のポリシーから子ポリシーを作成することもできます。

始める前に

ポリシーのクローンを作成して、独自のカスタムポリシーを作成できます。ポリシーのクローンを作成したり、任意のポリシーを基本として使用して子ポリシーを作成したりして、条件を再度入力することなく既存のポリシーを拡張できます。基本ポリシーのすべての条件は、子ポリシーでも継承されます。詳細については、「セキュリティポスチャコントロールのポリシーのクローンを作成する (例)」を参照してください。

アプリケーションに含まれる任意のポリシーのクローンを作成できますが、ポリシーの一致は、ホームランディングページのダッシュボードに重要なインサイトとして反映されません。ホームランディングページには、アプリケーションに含まれるポリシーの主要なインサイトのみが表示されます。

作成したポリシーのクローンを作成してアクティブ化したら、ワークスペースのカスタムインサイトビルダーモジュール (ナビゲーターパネルの最後のモジュール) に独自の構成済みインサイトレコードを作成する必要があります。これを作成して初めて、構成されたインサイトダッシュボード (ワークスペースの上から 2 番目のアイコン) でポリシーのデータを表示できるようになります。

必要なロール：SPC アドミングループまたは SPC アナリストグループ

手順

1. 次のように移動する。 ワークスペース > セキュリティポスチャコントロール > リスト > ポリシー > **All** (すべて).
2. クローンを作成するポリシーレコードを選択します。
3. [ポリシーのアクティブ化] の横にあるその他のオプションメニューから 1 つを選択します。
4. オプション: [基本ポリシー] を選択し、新しいポリシーのベースとなるポリシーを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(Optional) このオプションは、既存のポリシーの条件を新しいポリシーの開始点として継承する場合に選択できます。

5. オプション: [除外ポリシー] を選択し、このポリシーの検索結果から除外するポリシーを選択します。
除外されたポリシーに一致する新しいポリシーの検索結果は、検索結果に含まれません。
6. クローン作成されたポリシーの場合は、条件を編集します。
条件ビルダーの資産 - 接続 - エンティティ関係の詳細については、「セキュリティポスチャコントロール のポリシー」を参照してください。条件ビルダーのデコレーターの詳細については、「セキュリティポスチャコントロール アプリケーションで独自のポリシーを作成」を参照してください。
7. [変更を保存] をクリックして、ポリシーを編集して保存します。
ポリシーは、ワークスペースのリストモジュールの [すべて] リストに表示されます。
8. ポリシーをアクティブ化するには、「セキュリティポスチャコントロール のカスタムポリシーを作成してアクティブ化」で説明されている手順に従います。
9. オプション: [ポリシーを削除] を選択して、ポリシーを削除します。
削除オプションは、アプリケーションにあるポリシーや検索結果を生成しているポリシーではサポートされません。ポリシーは、検索結果がある場合にのみ非アクティブ化できます。

セキュリティポスチャコントロールの構成済みインサイトを作成してアクティブ化する

独自のインサイトを作成できます。構成済みインサイトとは、既存のポリシーや独自のカスタムポリシーを使用して作成できるインサイトを指します。

始める前に

構成済みインサイトのダッシュボードでデータを表示するには、インサイトレコードを作成してアクティブ化しておく必要があります。ワークスペースの構成済みインサイトのダッシュボードモジュールには、最大 6 個のインサイトと 21 個のチャートを含めることができます。

カスタムインサイトに使用するポリシーはすべてアクティブ化する必要があります。

資産タイプが「ソフトウェア」のポリシーを作成する場合、ポリシーを保存してカスタムインサイトを作成することはできますが、ポリシーレコードから結果を構成することはできません。

必要なロール：SPC アドミングループまたは SPC アナリストグループ

手順

1. 次のように移動する。 ワークスペース > セキュリティポスチャコントロール > カスタムインサイトビルダー (ワークスペースの最後のアイコン)

このランディングページには、次の 3 つのタブがあります。

有効

アクティブ化されたカスタムインサイト。アクティブ化されたカスタムインサイトは、構成済みインサイトのランディングページ (ワークスペースの上から 2 番目のアイコン) に表示されます。

非アクティブ

非アクティブなカスタムインサイト。非アクティブ化されたインサイトは、インサイトとそれをサポートするサポートポリシーがアクティブ化されるまで、構成済みインサイトのランディングページに表示されません。

すべて

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクティブおよび非アクティブなすべての構成済みインサイト。

2. ページの右側にある [新しいインサイト] を選択して、新しいレコードを作成します。
3. [タイプ] フィールドで、選択リストからインサイトを選択します。

オプション	説明
比較表	最大 5 つのポリシーの一致する資産の数を比較します。
ポリシー一致数ウィジェット	ポリシーに一致する資産の合計数。
ポリシー一致率グラフ	総資産に占める、ポリシーと一致する、または一致しない割合。
ポリシー一致トレンドチャート	ポリシーに一致する資産の履歴傾向。

4. 一方を選択します。
   - ハードウェア資産
   - ソフトウェア
5. インサイトのグループを選択します。
   インサイトは少なくとも 1 つのグループに属している必要があります。[カスタムインサイトビルダー] モジュールで新しいレコードを作成する場合、グループを作成するか、グループを構成済みインサイトにアサインする必要があります。構成済みインサイトのダッシュボードでレポートを整理できるようになります。
6. インサイトデータに必要なポリシーとインサイトラベルを選択します。
7. [保存] を選択します。
   インサイトは [非アクティブなインサイト (Inactive insight)] タブに保存されます。
8. 新しいインサイトをアクティブ化するには、非アクティブリストでレコードを開き、[アクティブ化 **(Activate)]** を選択します。
   インサイトのポリシーに関連付けられているサービスグラフコネクタの次のスケジュール済みインポートからデータが収集され、ワークスペースのカスタムインサイトダッシュボードモジュールにデータが表示されます。

セキュリティポスチャコントロールの検索結果を表示

セキュリティポスチャコントロール ワークスペースで、セキュリティポスチャコントロール のポリシー評価によって生成された検索結果を表示できます。

結果

ポリシーの実行から検索結果が生成されるように構成して、これらの検索結果を修正のためにさまざまなチームにアサインしたり、レポートに使用したりすることができます。ポリシーから直接結果を生成する方法の詳細については、「セキュリティポスチャコントロールアプリケーションに含まれているポリシーをアクティブ化する」を参照してください。

セキュリティポスチャコントロールは、これらの検索結果をコンフィグレーションコンプライアンスモジュールで「テスト結果」として公開します。セキュリティポスチャコントロールによって生成される検索結果では、アサイン、グループ化 (修復タスクの生成)、修復ターゲット、および例外に関連するコンフィグレーションコンプライアンスアプリケーションのすべての管理コントロールがサポートされます。

検索結果で使用されるラベル：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ツール範囲

このタイプは、セキュリティツール範囲のギャップを表します。この検索結果タイプは、「報告者 (Reported by)」および「報告なし (Not reported)」コネクタ関係を使用するポリシーに適用できます。

インターネットエクスポージャー

このタイプは、クラウド資産のインターネットエクスポージャーを表します。この検索結果タイプは、「インターネットに開かれているポートがある」という関係性または接続を使用するポリシーに適用できます。

高リスクの組み合わせ

このタイプは、資産に重大な脆弱性があったりエンドポイント保護エージェントが欠落したりしているなど、複数の関連するリスク要因がある問題を表します。

Integrated Risk Management (IRM) の例外

このタイプは、ガバナンス、リスク、コンプライアンス (GRC) 製品での承認された例外がある資産を表します。指定されている場合、これらの例外は検索結果数に含まれません。

脆弱性あり

このタイプは、既知の脆弱性を有する脆弱性一致アイテム (VIT) と関連付けられている資産となります。

セキュリティポスチャラベルが生成され、テスト結果に添付されます。たとえば、該当するタイプのラベルが「ツール範囲」の場合、ポリシーのタイプに基づいてテスト結果に自動的に割り当てられます。複数のラベルを有する資産の場合、複数のラベルがレコードに表示されます。

検索結果に関連付けられたセキュリティポスチャラベルを使用することで、コンフィグレーションコンプライアンスにアサインルールを記述し、これらの問題を修復のためにチームにルーティングすることができます。たとえば、「ツール範囲」の検索結果を IT 運用チームに送信し、「インターネットエクスポージャー」をアプリケーションチームに送信できます。

自動翻訳

検索結果を表示する場所

これらのオプションを使用して、ポリシーの評価によって生成された検索結果を表示します。

必要なロール：SPC アドミングループまたは SPC アナリストグループ

- 次のように移動する。 セキュリティポスチャコントロールワークスペース > ポリシーと検出結果 > 実行内容の詳細 > すべての。
- ポリシーレコードで、[検索結果を表示] を選択します。リストには、「高リスクの組み合わせ」、「インターネットエクスポージャー」などの一般的なカテゴリに分類された検索結果のグループが表示されますが、これらのグループは修復に使用できる正式なグループではありません。検索結果を得るには、コンフィグレーションコンプライアンスで修復ルールとアサインルールを設定する必要があります。
- コンフィグレーションコンプライアンスアプリケーションで、[テスト結果] を選択し、[ソースは **ServiceNow SPC (Source is ServiceNow SPC)]** でレコードをフィルタリングします。

ダッシュボード

セキュリティポスチャコントロールワークスペースのホーム (ランディングページ) には、次の可視化データが表示されます。

概要

- 資産：オンプレミスおよびクラウドで監視されている資産の数。
- 重要度別の検索結果：総資産のうちの重要な検索結果の数。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 上位 5 つのソースによって監視される資産：資産についてレポートする上位 5 つのサービスグラフコネクタ。
- クラウドアカウント：AWS および Azure によって監視されているクラウドアカウントの数。
- オープンとクローズ済みの検索結果の比較：まだ処理中または解決待ちのレコードと解決済みのレコードの比較。

主要なインサイト

- インストールされているエンドポイント保護エージェント：エンドポイント保護がある資産またはない資産の合計数。
- 管理対象デバイスのカバー範囲：管理対象資産と非管理対象資産との比較。
- 脆弱性スキャンのカバー範囲：スキャンされた資産の合計数と、サードパーティの脆弱性スキャナーでスキャンされなかった既知の脆弱性の数の比較。
- 重大な脆弱性がある資産：重大な脆弱性がある資産の合計数に対する資産の数。
- 重要度別の脆弱性一致アイテム：重大度別に分類された脆弱性一致アイテムの合計数。既知の脆弱性が CMDB 内の資産と一致すると、脆弱性一致アイテムになります。
- 検索結果別の上位 3 つのポリシー：資産で最も多くの検出結果 (一致) を返すポリシー。

主要なユースケース範囲

ユースケースを選択し、[ヘルプのアクティブ化 **(Help activate)]** または [ヘルプの改善 **(Help improve)]** を選択して、主要なユースケースに対してアクティブ化する必要があるサービスグラフコネクタとポリシーを表示します。

セキュリティポスチャコントロール アプリケーションのテスト結果と修復タスクのステータス移行

セキュリティポスチャコントロールアプリケーションでポリシーを変更すると、検索結果 (構成テストレコード) のステータスや関連付けられている修復タスクが影響を受けます。

テスト結果と修復タスク間のステータス移行シナリオ

セキュリティポスチャコントロールでは、一部の例外を除き、検索結果 (テスト結果) と関連の修復タスクの間でステータスが移行するのが一般的です。コンフィグレーションコンプライアンス アプリケーションでステータスがテスト結果と修復タスクの間を移行するのと同じ要領です。ただし、セキュリティポスチャコントロールでポリシーを変更した場合、検索結果と関連の修復タスクのステータス移行に影響が及びます。

ポリシーの編集、編集に伴う新しいバージョンの公開、ポリシーの非アクティブ化または削除に伴う検索結果でのステータス移行については、次のテーブルのとおりです。

コンフィグレーションコンプライアンス におけるステータス変更の詳細については、「コンフィグレーションコンプライアンスアプリケーションのテスト結果と修復タスクのステータス移行」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
コンフィグレーションコンプライアンス の v14.9 以降では、次の用語が変更されました。

用語の変更

v14.9 より前の用語	**v14.9** 以降の用語
テスト結果グループ	修復タスク
グループルール	修復タスクルール
ポリシー	テストグループ

ポリシー監査の機能拡張により、廃止された資産がアクティブ化されたポリシーによって評価されなくなります。資産のステータスが [廃止] から [アクティブ] に戻ると、次回のポリシー評価の対象となります。

ポリシーが次の場合	既存の検索レコードのフィールド値となる対象	移行先
非アクティブ化済み	結果	元の値を保持
	ステータス	クローズ済み
	解決	古い

ポリシーが次の場合	既存の検索レコードのフィールド値となる対象	移行先
選択した既存の結果をクローズするオプションで編集が行われました	結果	元の値を保持
	ステータス	クローズ済み
	解決	結果が無効

ポリシーが次の場合	既存の検索レコードのフィールド値となる対象	移行先
選択した既存の結果を保持するオプションで編集が行われました	結果	有効なテストケース (合格) では元の値が保持され、無効なテストケース (失敗) はクローズされます。
	ステータス	クローズ済み
	解決	結果が無効

ポリシーが次の場合	既存の検索レコードのフィールド値となる対象	移行先
削除済み	結果	元の値を保持
	ステータス	クローズ済み
	解決	結果が無効

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティポスチャコントロールでの資産検索の作成

条件を設定し、特定のサービスグラフコネクタ製品による資産、またはコネクタによって報告された特定のデータを持つ資産を検索します。

始める前に

検索の例として、Windows サーバーと CrowdStrike メタデータの詳細で見つかった特定のバージョンを持つ資産を特定するとします。

必要なロール：SPC アドミングループまたは SPC アナリストグループ

手順

1. 次のように移動する。 ワークスペース > セキュリティポスチャコントロール > 資産検索.
2. いずれかを選択します。
   この例では、[資産タイプ] に [ハードウェア資産] を選択します。
3. オプション: 既存のポリシーの条件を出発点として使用し、既存のポリシーに一致する資産をそれぞれ除外する場合は、[基本ポリシー] と [除外ポリシー] を選択します。
   選択したポリシーが表示されます。
4. [接続 (Connection)] フィールドで [コネクタデータあり **(With connector data)]** を選択します。
5. エンティティの **[CrowdStrike** デバイスの詳細 **(CrowdStrike Device Details)]** を選択します。
6. [プロパティ]、[演算子]、および [値] で「[エージェントのバージョン **(Agent Version)]**[次と等しい **(is)]**」を選択し、バージョン (**6.26.14003.0** など) を入力します。
7. 別の条件の値として CrowdStrike デバイスの詳細を含むエンティティフィールドの右側にある「AND」演算子を選択します。
8. [接続 (Connection)] フィールドで **[CMDB** メタデータあり **(With CMDB metadata)]** を選択します。
   [エンティティ] フィールドに、CMDB メタデータが入力されます。
9. [基準] フィールドで [プロパティ] を選択します。
10. [プロパティ]、[演算子]、および [値] で「**[OS]**[次を含む **(contains)]**」を選択し、「**Windows Server**」と入力します。
11. [資産を表示 **(View assets)]** を選択します。
    しばらくすると、[一致する資産 (Matching assets)] タブに結果が表示されます。一致するものが見つからない場合は、検索を絞り込むことができます。条件を正しく設定したことを確認したら、検索をポリシーとして保存してアクティブ化できます。他のポリシーと同様に、アクティブ化した後、バックグラウンドジョブで資産を継続的に検索します。

での緩和コントロールモニタリングの使用 セキュリティポスチャコントロール

セキュリティポスチャコントロール (SPC) ワークスペース内から、さまざまなセキュリティツールの構成方法に基づいて、利用可能な緩和コントロールによって資産に対するどの脅威が軽減されるかを把握できます。

緩和コントロールモニタリング

セキュリティポスチャコントロールアプリケーションは、次の 3 つの主要な問題領域に焦点を当てています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 資産インベントリ - 管理されていない資産や不明な資産を含むすべてのエンタープライズ資産を特定します。
- セキュリティコントロールの範囲と健全性 - セキュリティコントロールとのカバレッジのギャップを特定します
- 脅威の軽減の可視化 - 資産に対するどの脅威が、該当する軽減コントロールによって軽減されるかを特定します。

緩和コントロールモニタリングでは、脅威緩和の可視化に該当する セキュリティポスチャコントロール の機能について説明します。この点に関して、 MITRE-ATT&CK™ には、さまざまな手法に使用できる一連の利用可能な緩和策がリストされています。以下に例を示します。

1. この手法の緩和策としての Web アプリケーションファイアウォール 初期 初期アクセス > 公開されているアプリケーションを悪用.
2. 次のようなテクニックの緩和策としてのエクスプロイト保護 実行 > クライアント実行のエクスプロイト.
3. テクニックの緩和策としてのマルチファクター認証 権限のエスカレーション > アカウント操作.

必要なロール：

- アドミン: ServiceNow® Store からアプリケーションをインストールし、プラグインをアクティブ化します (ITOM ディスカバリー)。
- SPC アドミングループと SPC アナリストグループ:このグループのユーザーは、製品とワークスペースのすべてのレコードに対する読み取り/書き込みのフルアクセス権を持ちます。
- SPC アナリスト読み込み専用グループ:このグループのユーザーには、製品のすべてのレコードへのフル読み取りアクセス権があります。

緩和コントロール:ユーザーと福利厚生の監視

ユーザー

ユーザー	説明
サイバーセキュリティチーム、セキュリティアナリスト、マネージャー	• 管理されていない資産や不明な資産を含むすべてのエンタープライズ資産を可視化します。 • セキュリティコントロールの範囲のギャップ、資産の重大な脆弱性やインターネットエクスポージャーなどの問題の有害な組み合わせ、および内部セキュリティ標準からの逸脱を特定します。 • セキュリティツールの構成方法に基づく緩和コントロールによって、資産に対するどの脅威が軽減されるかについてのインサイトを得ることができます。

セキュリティポスチャコントロール と緩和コントロールモニタリング ワークフロー

セキュリティポスチャコントロール は、Web アプリケーションファイアウォールやエンドポイント保護ツールなどのセキュリティツールとの API 統合を使用して、資産に関する追加の構成データをインポートして分析し、特定の資産に適用可能な緩和コントロールを特定します。これらの API 統合は、 SPC でサポートされているサービスグラフコネクタ統合とは別のものであり、異なるデータをインポートします。これらの API 統合は、 SPC ワークスペース内から構成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

緩和コントロールのモニタリングには、サービスグラフコネクタ統合または ITOM ディスカバリーが引き続き必要です。たとえば、CrowdStrike エンドポイント保護構成によって有効になっている緩和コントロールに関する追加のインサイトをインポートするには、SPC でサポートされている CrowdStrike サービスグラフコネクタと CrowdStrike API 統合の両方をアクティブ化する必要があります。

の緩和コントロールとポリシー セキュリティポスチャコントロール

ポリシーと緩和コントロールは、エンタープライズ資産の緩和コントロールを検出できる セキュリティポスチャコントロール 製品に含まれています。これらのポリシーとコントロールは、 セキュリティポスチャコントロール ワークスペースで表示できます。

緩和コントロールポリシー

SPCで緩和コントロールと緩和コントロールポリシーを表示するには、セキュリティポスチャコントロール アプリケーションと緩和コントロールアプリケーションが必要です。どちらのアプリケーションも ServiceNow Store から入手できます。

ServiceNow® Store からのアプリケーションのダウンロードとインストールの詳細については、次のトピックを参照してください。

- ServiceNow Store からのアプリケーションの初回ダウンロード
- セキュリティオペレーション 統合のインストール

緩和コントロールポリシーを表示するには、SPC アドミングループと SPC アナリストグループのユーザーが次の場所に移動できます ワークスペース > セキュリティポスチャコントロール > ポリシーと検出結果 > **All** (すべて) (SPC ワークスペースのナビゲーションパネル)

次の緩和コントロールポリシーはアプリケーションに含まれており、他の SPC ポリシーとともに表示されます。

- SEH 上書き
- ヒープスプレー
- CrowdStrike NULL ページの割り当て
- CrowdStrike DEP を強制
- CrowdStrike ASLR を強制
- Microsoft Defender コントロールフローガード
- Microsoft Defender force ASLR
- Microsoft Defender 必須 ASLR とボトムアップ ASLR
- SentinelOne アプリケーションコントロール
- SentinelOne データファイル
- SentinelOne 実行可能ファイル
- SentinelOne エクスプロイト
- SentinelOne IDR
- SentinelOne インタラクティブな脅威の検出
- SentinelOneの横方向の動きの検出
- SentinelOne 静的 AI
- SentinelOne 静的 AI - 不審

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- SentinelOne 望ましくない可能性があるアプリケーション
- SentinelOne リモートシェル
- SentinelOne 評判

ワークスペースでの緩和コントロールの表示

緩和コントロールのリストを表示するには、SPC アドミングループと SPC アナリストグループが次の場所に移動できます: ワークスペース > セキュリティポスチャコントロール > 緩和コントロール (SPC ワークスペースのナビゲーションパネル)

サポートされている緩和コントロールのリストには、資産の SPC によって検出できるさまざまなタイプの緩和が含まれています。レコードを選択します。各緩和コントロールには、次の情報が含まれています。

- 名前:緩和コントロールの名前。
- ソース:特定の資産でこの緩和コントロールのステータスをインポートするために使用されるソース。この統合でサポートされているソースは、 CrowdStrike、 Microsoft SCCM、SentinelOne、および F5 BIG-IP セキュリティツールとの API ベースの統合です。
- カテゴリ:エクスプロイト保護 (EDR) などの緩和コントロールのカテゴリ。
- MITRE™ テクニック:この緩和コントロールが適用される MITRE テクニック。
- ポリシー:この緩和コントロールの存在を識別するために使用される、製品に含まれる SPC ポリシー。1 つの緩和コントロールに複数のポリシーが必要な場合があります。

緩和コントロールには、複数のポリシーを使用した評価が必要なものもあれば、1 つのポリシーのみが必要なものもあります。また、特定の緩和コントロールではすべてのポリシーが一致する必要がありますが、他のコントロールでは、緩和コントロールのステータスが特定の資産でアクティブであると判断するために必要なポリシーは 1 つだけです。

緩和コントロールカテゴリ

現在、次のカテゴリの緩和コントロールが SPC でサポートされています。

- Exploit Protection (EDR) に必要な軽減コントロールとポリシー.
- Exploit Protection (WAF) に必要な軽減コントロールとポリシー。

Exploit Protection (EDR) に必要な軽減コントロールとポリシー

Exploit Protection Endpoint Detection and Response (EDR) の監視に必要な軽減コントロールとポリシーは、 セキュリティポスチャコントロール 製品に含まれています。

エクスプロイト保護 **(EDR)**

必要なロール: SPC アドミングループと SPC アナリストグループ。

このカテゴリの緩和コントロールは、エンドポイント保護エージェント構成の形式で資産で利用可能な緩和をカバーします。これは、 CrowdStrike や Microsoft SCCM、 Microsoft Defender Mitigation Control Integration や SentineOne などのエンドポイント保護エージェントに適用されます。

[アドレススペースレイアウトのランダム化を強制する] や [DEP を強制する] などのエクスプロイト緩和設定は、 CrowdStrike などのエンドポイント保護ツールで有効にできます。 SPC は、アプリケーションに含まれるポリシーとエンドポイント保護ツールとの API 統合を利用して、デバイスでこの構成を自動的に検出します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

を使用した **Exploit Protection (EDR)** 検出の前提条件 **CrowdStrike**

1. CrowdStrike サービスグラフコネクタがアクティブ化されていることを確認します。このアプリケーションは ServiceNow Store で入手できます。インストールと構成に関する情報は、アプリのリストに含まれています。詳細については、「緩和コントロールモニタリングのための CrowdStrike 統合をインストールして構成します」を参照してください。
2. セキュリティポスチャコントロールワークスペースで CrowdStrike API 統合が有効になっていることを確認します。

Exploit Protection (EDR) の軽減コントロールとポリシー **CrowdStrike**

- CrowdStrike – エクスプロイト緩和 – ASLR を強制する
  - ソース: CrowdStrike API
  - MITRE 対処される戦術:初期アクセス、実行、認証情報アクセス、防御回避、特権エスカレーション、ラテラルムーブメント
  - MITRE この緩和策で対処される手法:ドライブバイ侵害 (初期アクセス)、クライアント実行のエクスプロイト (実行)、認証情報アクセスのエクスプロイト (認証情報アクセス)、防御回避のためのエクスプロイト (防御回避)、特権エスカレーションのエクスプロイト (防御回避)、リモートサービスのエクスプロイト (ラテラルムーブメント)
  - ポリシー - この緩和コントロールを識別するには、 CrowdStrike Force ASLR ポリシーをアクティブ化する必要があります。オプションで、他の緩和コントロールポリシーをアクティブ化できます。
- CrowdStrike – エクスプロイト緩和 – DEP を強制する
  - ソース: CrowdStrike API
  - MITRE 対処される戦術:初期アクセス、実行、認証情報アクセス、防御回避、特権エスカレーション、ラテラルムーブメント
  - MITRE この緩和策で対処される手法:ドライブバイ侵害 (初期アクセス)、クライアント実行のエクスプロイト (実行)、認証情報アクセスのエクスプロイト (認証情報アクセス)、防御回避のためのエクスプロイト (防御回避)、特権エスカレーションのエクスプロイト (防御回避)、リモートサービスのエクスプロイト (ラテラルムーブメント)
  - ポリシー:この緩和コントロールを識別するには、 CrowdStrike 強制 DEP ポリシーをアクティブ化する必要があります。オプションで、他の緩和コントロールポリシーをアクティブ化できます。
- CrowdStrike –エクスプロイト緩和–ヒープスプレーの事前割り当て
  - ソース: CrowdStrike API
  - MITRE 対処される戦術:初期アクセス、実行、認証情報アクセス、防御回避、特権エスカレーション、ラテラルムーブメント
  - MITRE この緩和策で対処される手法:ドライブバイ侵害 (初期アクセス)、クライアント実行のエクスプロイト (実行)、認証情報アクセスのエクスプロイト (認証情報アクセス)、防御回避のためのエクスプロイト (防御回避)、特権エスカレーションのエクスプロイト (防御回避)、リモートサービスのエクスプロイト (ラテラルムーブメント)
  - ポリシー:この緩和コントロールを特定するには、ヒープスプレー事前割り当てポリシーをアクティブ化する必要があります。オプションで、他の緩和コントロールポリシーをアクティブ化できます。
- CrowdStrike エクスプロイト緩和:NULL ページ割り当て
  - ソース: CrowdStrike API
  - MITRE 対処される戦術:初期アクセス、実行、認証情報アクセス、防御回避、特権エスカレーション、ラテラルムーブメント

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- MITRE この緩和策で対処される手法:ドライブバイ侵害 (初期アクセス)、クライアント実行のエクスプロイト (実行)、認証情報アクセスのエクスプロイト (認証情報アクセス)、防御回避のためのエクスプロイト (防御回避)、特権エスカレーションのエクスプロイト (防御回避)、リモートサービスのエクスプロイト (ラテラルムーブメント)
- ポリシー:この緩和コントロールを識別するには、 CrowdStrike NULL ページ割り当てポリシーを有効にする必要があります。オプションで、他の緩和コントロールポリシーをアクティブ化できます。

- CrowdStrike – エクスプロイト緩和 – SEH 上書き
  - ソース: CrowdStrike API
  - MITRE 対処される戦術:初期アクセス、実行、認証情報アクセス、防御回避、特権エスカレーション、ラテラルムーブメント
  - MITRE この緩和策で対処される手法:ドライブバイ侵害 (初期アクセス)、クライアント実行のエクスプロイト (実行)、認証情報アクセスのエクスプロイト (認証情報アクセス)、防御回避のためのエクスプロイト (防御回避)、特権エスカレーションのエクスプロイト (防御回避)、リモートサービスのエクスプロイト (ラテラルムーブメント)
  - ポリシー:この緩和コントロールを特定するには、少なくとも、CrowdStrike SEH 上書き保護ポリシーをアクティブ化する必要があります。オプションで、他の緩和コントロールポリシーをアクティブ化できます。
- CrowdStrike – エクスプロイト緩和 – すべての設定オン
  - ソース: CrowdStrike API
  - MITRE 対処される戦術:初期アクセス、実行、認証情報アクセス、防御回避、特権エスカレーション、ラテラルムーブメント
  - MITRE この緩和策で対処される手法:ドライブバイ侵害 (初期アクセス)、クライアント実行のエクスプロイト (実行)、認証情報アクセスのエクスプロイト (認証情報アクセス)、防御回避のためのエクスプロイト (防御回避)、特権エスカレーションのエクスプロイト (防御回避)、リモートサービスのエクスプロイト (ラテラルムーブメント)
  - ポリシー:この緩和コントロールを特定するには、CrowdStrike Force ASLR、 CrowdStrike Force DEP、ヒープスプレー事前割り当て、CrowdStrike NULL ページ割り当て、および CrowdStrike SEH 上書き保護のすべてのポリシーをアクティブ化する必要があります。

Microsoft SCCM と **Microsoft Defender** 緩和コントロール統合による **Exploit Protection (EDR)** 検出の前提条件

Microsoft スクリプト作成者ロールを含む SCCM 認証情報。スクリプト作成者ロールは、SCCM サーバーに緩和情報をインポートするために必要なスクリプトを作成するために必要な権限を提供します。

詳細については、「Microsoft SCCM のサービスグラフコネクタと Microsoft Defender 緩和コントロール統合のインストールと構成」を参照してください。

Exploit Protection (EDR) with Microsoft SCCM および Microsoft Defender Mitigation Control Integration の軽減コントロールとポリシー:

- Defender – エクスプロイト緩和 – CFG

  Microsoft Defender Control Flow Guard。

- Defender – エクスプロイト緩和 – DEP

  Microsoft Defender データ実行防止。

- Defender – エクスプロイト緩和 – 必須 ASLR とボトムアップ ASLR

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Microsoft ディフェンダーフォースASLR。

- MITRE 対処される戦術:初期アクセス、実行、認証情報アクセス、防御回避、特権エスカレーション、ラテラルムーブメント。
- MITRE この緩和策で対処される手法:ドライブバイ侵害 (初期アクセス)、クライアント実行のためのエクスプロイト (実行)、認証情報アクセスのエクスプロイト (認証情報アクセス)、防御回避のためのエクスプロイト (防御回避)、特権エスカレーションのためのエクスプロイト (防御回避)、リモートサービスのエクスプロイト (ラテラルムーブメント)。

SentinelOne Mitigation Control Integration を使用した **Exploit Protection (EDR)** 検出の前提条件

1. SentinelOne サービスグラフコネクタがアクティブ化されていることを確認します。

   このアプリケーションは ServiceNow Store で入手できます。インストールと構成に関する情報は、アプリのリストに含まれています。詳細については、「SentinelOne のサービスグラフコネクタ と SentinelOne 緩和コントロール統合のインストールと構成」を参照してください。

2. セキュリティポスチャコントロールワークスペースで SentinelOne API 統合が有効になっていることを確認します。
3. アプリケーションに含まれる SentinelOne 緩和コントロールポリシーを確認します。
   - SentinelOne アプリケーションコントロール
   - SentinelOne データファイル
   - SentinelOne 実行可能ファイル
   - SentinelOne エクスプロイト
   - SentinelOne IDR
   - SentinelOne インタラクティブな脅威の検出
   - SentinelOneの横方向の動きの検出
   - SentinelOne 静的 AI
   - SentinelOne 静的 AI - 不審
   - SentinelOne 望ましくない可能性があるアプリケーション
   - SentinelOne リモートシェル
   - SentinelOne 評判

緩和コントロールモニタリングのための **CrowdStrike** 統合をインストールして構成します

CrowdStrike サービスグラフコネクタと API 統合には、別々の構成手順が必要です。資産の詳細をインポートするように CrowdStrike サービスグラフコネクタを構成します。CrowdStrike API 統合を構成して、CrowdStrike によって監視される資産に関する緩和データを収集します。

始める前に

- インスタンスにセキュリティポスチャコントロールおよび緩和コントロールモニタリングアプリケーションがインストールされ、アクティブ化されていることを確認します。これらのアプリケーションは ServiceNow Store で入手できます。
- CrowdStrike API 統合を構成する前に、CrowdStrike サービスグラフコネクタをインストールして構成する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

必要なロール:プラグインのインストールの場合は admin、ワークスペースでの統合の構成の場合は SPC アドミングループと SPC アナリストグループ。

手順

1. CrowdStrike サービスグラフコネクタ統合をインストールして構成するには、次の手順を実行します。

   注:
   CrowdStrike のサービスグラフコネクタをインストールした場合は、ステップ 2 で CrowdStrike API 統合の構成方法に進んでください。

   a. 次のように移動する。 コネクタとユースケースのセットアップ > [サービスグラフコネクタ] タブ.
   b. CrowdStrike Endpoint Protection サービスグラフコネクタを見つけます。
   c. ServiceNow® Store にある CrowdStrike のサービスグラフコネクタのアプリリストに移動するリンクを選択します。
   d. プロンプトに従ってアプリケーションをインストールします。
   e. 終了する前に、アプリリストの [サポートリンクとドキュメント] セクションからインストールガイドをダウンロードして、構成とアクティブ化を支援します。
   f. 次のように移動する。 **CrowdStrike** > セットアップ インスタンス内にあります
   g. ガイド付きセットアップのプロンプトに従い、ドキュメントを参照して SGC を構成してアクティブ化します。
2. 次のように移動する。 コネクタとユースケースのセットアップ > **SPC API** 統合.

   このタブには緩和コントロールソース (CrowdStrike、F5 Big IP、および SCCM) が一覧表示され、このタブは緩和コントロールモニタリングアプリケーションをインストールしている場合にのみワークスペースに表示されます。

   ソースカードでは、緩和ソースのステータス (アクティブ または 非アクティブ) と、CrowdStrike (6) によって監視されている緩和コントロールと関連ポリシーの数を表示できます。番号を選択すると、リストが表示されます。

   [Sources] の [Active] 列に [Active] と表示されます。これは、ソース (SGC CrowdStrike) がアクティブであることを示しますが、緩和コントロールを監視するには、 CrowdStrike API 統合を設定する必要があります。

3. [**Next**] を選択します。
4. [名前] 列で [CrowdStrike] を選択します。
5. [編集] を選択し、フィールドに入力します。

   注:
   CrowdStrike サービスグラフコネクタに指定したのと同じ CrowdStrike アカウント情報とサーバーの詳細を API 統合に入力します。この情報により、サービスグラフコネクタでインポートした資産データと一致する緩和データをインポートできます。

フィールド	説明
名前	インスタンス名この名前を変更すると、認証情報をテストせずに保存することができます。[名前] フィールドの下のフィールドを変更する場

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	合は、保存して終了する前に接続をテストする必要があります。
資産サイズ制限	監視された資産の数。
クライアント ID	CrowdStrike ID
クライアントシークレット	CrowdStrike 秘密
API URL	API URL (例:https://api.crowdstrike.com)

6. 準備ができたら、[テスト接続] を選択します。
   接続に成功すると、メッセージが表示されます。
7. **[Save and Exit** (保存して終了)] を選択します。
8. [SPC API 統合] タブの CrowdStrike カードで [詳細を表示] を選択し、ソースと API がアクティブ化され、構成の進行状況バーが完了していることを確認します。
9. オプション: 資格情報テストが成功しなかった場合は、[以前の資格情報に戻す] を選択して、以前に検証した資格情報を挿入できます。
10. CrowdStrike統合を実行するには、次の手順に従います。

    a. 次のように移動する。 **CrowdStrike** 緩和コントロール > 統合.
    次の 3 つの統合があります。
    - CrowdStrike 防止ポリシーの統合
    - CrowdStrike デバイスコントロールポリシーの統合
    - CrowdStrike 資産インサイト統合

    統合は連結され、特定の順序で実行されます。1 つの統合が正常に完了すると、次の統合が開始されます。

    b. [名前] 列で [CrowdStrike 防止ポリシー統合] を選択して、統合の実行を開始します。

    c. レコードで、[アクティブ] チェックボックスをオンにして、[今すぐ実行] を選択します。

    統合レコードの [統合実行] タブで統合実行状況を表示できます。

    統合は、デフォルトで毎日実行されるようにスケジュールされています。

    CrowdStrike資産インサイト統合は、前回の統合実行以降に変更された資産に関する情報のみをインポートします。CrowdStrikeデバイスコントロールポリシー統合とCrowdStrike防止ポリシー統合は、実行ごとにすべてのデータをインポートします。

Microsoft SCCM のサービスグラフコネクタと **Microsoft Defender** 緩和コントロール統合のインストールと構成

SCCM のサービスグラフコネクタと Microsoft Defender 緩和コントロール統合には、別々の構成手順が必要です。資産の詳細をインポートするには、SCCM のサービスグラフコネクタをインストールして構成します。Microsoft Defender 緩和コントロール統合を構成して、SCCM のサービスグラフコネクタによって監視される資産に関する緩和データを収集します。

始める前に

必要なロール：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- プラグインのインストールとアクティブ化のためのアドミン
- ワークスペースでの統合の構成のための SPC アドミングループと SPC アナリストグループ
- スクリプト作成者ロールを含む Microsoft SCCM 認証情報。スクリプト作成者ロールは、SCCM サーバーに緩和情報をインポートするために必要なスクリプトを作成するために必要な権限を提供します。

  注:
  このロールを作成し、次の権限でアサインする必要があります。

  スクリプト作成者ロール

Category (カテゴリ)	権限	状況
コレクション	スクリプトを実行	いいえ
拠点	読み込み	要
SMS スクリプト	作成/挿入	要
SMS スクリプト	読み込み	要
SMS スクリプト	削除	要
SMS スクリプト	変更	要

- スクリプト承認者ロールを含む Microsoft SCCM 認証情報。緩和情報をインポートするために作成されたスクリプトでは、スクリプト承認者ロールを持つユーザーが Microsoft SCCM コンソールで承認する必要があります。

  注:
  このロールを作成し、次の権限でアサインする必要があります。

  スクリプト承認者

Category (カテゴリ)	権限	状況
コレクション	スクリプトを実行	いいえ
拠点	読み込み	要
SMS スクリプト	読み込み	要
SMS スクリプト	承認	要
SMS スクリプト	変更	要

手順

1. Microsoft SCCM のサービスグラフコネクタ統合をインストールして構成するには、次の手順を実行します。

   注:
   Microsoft SCCM のサービスグラフコネクタ統合をインストールしている場合は、ステップ 2 に進み、Microsoft Defender 緩和コントロール統合を構成します。

   a. 次のように移動する。 コネクタとユースケースのセットアップ > [サービスグラフコネクタ] タブ.

   b. Microsoft SCCM のサービスグラフコネクタ統合を見つけます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

c. ServiceNow® Store内のアプリケーションのアプリリストに移動するリンクを選択します。

d. プロンプトに従ってアプリケーションをインストールします。

e. 終了する前に、アプリリストの [サポートリンクとドキュメント] セクションからインストールガイドをダウンロードして、構成とアクティブ化を支援します。

f. 次のように移動する。 セットアップ インスタンス内にあります

g. ガイド付きセットアップのプロンプトに従い、ドキュメントを参照して SGC を構成してアクティブ化します。

2. 次のように移動する。 コネクタとユースケースのセットアップ > **SPC API** 統合 Microsoft Defender 緩和コントロール統合を構成します。

   このタブには緩和コントロールソース (CrowdStrike、F5 Big Ip、および Defender) が一覧表示され、このタブは緩和コントロールモニタリングアプリケーションをインストールしている場合にのみワークスペースに表示されます。

   ソースカードでは、緩和ソースのステータス (アクティブ または 非アクティブ) を表示できます。

   [Sources] の [Active] 列に [Active] と表示されます。これは、ソース (Microsoft SCCM のサービスグラフコネクタ) が資産データを取得するためにアクティブであることを示しますが、緩和コントロールを監視するには、Microsoft Defender 緩和コントロール統合を構成する必要があります。

3. [**Next**] を選択します。
   [SCCM 構成] ページに、1 つの Microsoft SCCM 緩和コントロールインスタンスリンクが表示されます。

4. [名前] 列に表示されるインスタンスリンクを選択します。

5. SCCM 認証情報構成 Microsoft SCCM 緩和コントロール統合モーダルのフィールドに入力します。

フィールド	説明
名前	フィールドにはインスタンス名が自動的に入力されます。
接続	接続情報が自動的に入力されるフィールド。
ホスト	前のフィールドで提供された接続情報内の SCCM サーバーのホスト名。
ユーザー名	SCCM サーバーにアクセスするためのユーザー名。
Password (パスワード)	SCCM サーバーにアクセスするためのパスワード。
MID Server	リストから ServiceNow 管理対象の MID サーバーを選択します。
検証ステータス	検証の試行後に入力されるフィールド。接続が成功すると、統合インスタンスのステータスは [有効] になります。
SG コネクタ接続	Microsoft SCCM のサービスグラフコネクタのリストから、接続および資格情報エイリアスのオプションを 1 つ選択します。この接続は、Microsoft SCCM SGC のガイド付きセットアップステップで設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
検証の詳細	検証試行の詳細。

6. [認証情報を保存してテスト] を選択します。
   次のステップに進むには、正常な接続に対する 有効な 応答が必要です。
7. [**Next**] を選択します。
   緩和の詳細を取得するための PowerShell スクリプトが自動的に作成されます。スクリプト承認を検証するオプションを含むモーダルが表示されます。
8. スクリプトを承認するには、スクリプト承認者ロールで Microsoft SCCM コンソールにログインします。

   緩和の詳細を取得するための PowerShell スクリプトが SCCM 構成マネージャーで生成されています。スクリプトを承認するには、スクリプト承認者権限を持つユーザーロールを持つ適切な認証情報でログインする必要があります。承認後、Now Platform インスタンスで検証できます。

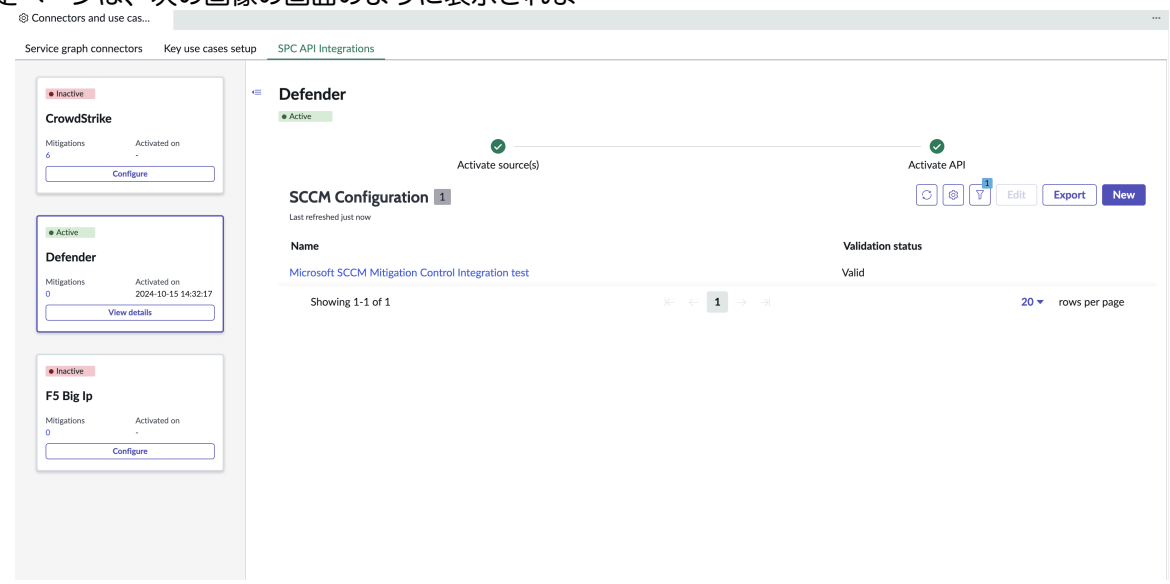
9. コンソールで、[**ServiceNow Secops]:**システム緩和策を取得 スクリプトを見つけて承認します。

   注:
   SCCM 構成マネージャーでは、[スクリプト] セクションはソフトウェアライブラリの下にあります。場所:[Servicenow Secops]:システム緩和スクリプトを取得して承認します。

   このスクリプトは、承認するまで [承認待ち] ステータスのままになります。

   上記のように承認せずに Now Platform インスタンスでスクリプトを検証できますが、「スクリプトは承認されていません」というエラーメッセージが表示されます。

10. 承認を検証するには、Now Platform インスタンスに戻り、[PowerShell スクリプトを承認] モーダルで [スクリプトの承認を検証] を選択します。
11. **[Done** (完了)] を選択します。
    設定ページは、次の画像の画面のように表示されます。



Microsoft Defender 緩和コントロール統合用に複数のインスタンスを作成する

Microsoft Defender 緩和コントロール統合のために複数のインスタンスを構成できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：

- ワークスペースで新しい統合インスタンスを構成するための SPC アドミングループと SPC アナリストグループ
- スクリプト作成者ロールを含む Microsoft SCCM 認証情報。スクリプト作成者ロールは、SCCM サーバーに緩和情報をインポートするために必要なスクリプトを作成するために必要な権限を提供します。

  注:
  このロールを作成し、次の権限でアサインする必要があります。

  スクリプト作成者ロール

Category (カテゴリ)	権限	状況
コレクション	スクリプトを実行	いいえ
拠点	読み込み	要
SMS スクリプト	作成/挿入	要
SMS スクリプト	読み込み	要
SMS スクリプト	削除	要
SMS スクリプト	変更	要

- スクリプト承認者ロールを含む Microsoft SCCM 認証情報。緩和情報をインポートするために作成されたスクリプトでは、スクリプト承認者ロールを持つユーザーが Microsoft SCCM コンソールで承認する必要があります。

  注:
  このロールを作成し、次の権限でアサインする必要があります。

  スクリプト承認者

Category (カテゴリ)	権限	状況
コレクション	スクリプトを実行	いいえ
拠点	読み込み	要
SMS スクリプト	読み込み	要
SMS スクリプト	承認	要
SMS スクリプト	変更	要

手順

1. 次のように移動する。 コネクタとユースケースのセットアップ > **SPC API** 統合.
2. **[New** (新規)] を選択します。
   [新しい Defender インスタンス (New Defender instance)] モーダルが表示されます。
3. 新しいインスタンスの名前を入力し、[インスタンスを作成] を選択します。
   [SPC API 統合] ページに、アプリケーションで提供されたインスタンスと新しいインスタンスが表示されます。
4. 新しいインスタンスのリンクを選択します。
5. 新しいインスタンスの SCCM 認証情報構成モーダルのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
名前	フィールドにはインスタンス名が自動的に入力されます。
接続	新しい接続を作成します。 **a.** モーダルの上部にある [接続とエイリアスを作成] を選択します。 **b.** [接続および資格情報エイリアス] フォームで、必須フィールドに入力します。 ▪ 名前 :一意の名前 ▪ タイプ :接続と認証情報 ▪ 接続タイプ - 基本 注: この時点で は [送信] を選択しないでください。 **c.** 灰色のヘッダーの任意の場所を右クリックし、[保存] を選択します。 保存すると、ページが更新され、関連リンクとタブがページの下部に表示されます。 **d.** [接続] タブを選択した状態で、タブの右側にある [新規] を選択します。 接続フォームが表示されます。フィールドに入力します。 ▪ 名前 :一意の名前 ▪ 認証情報:検索アイコンを選択します。Windows 認証情報を見つけて、リンクを選択します。[Windows 認証情報] フォームで、フィールドに入力します。 ▪ 名前 :一意の名前 ▪ ユーザー名:認証情報のユーザー名。これは、このページに保存した後に、SCCM 認証情報構成モーダルの [ユーザー名] フィールドで参照されるユーザー名です。 ▪ パスワード:認証情報のパスワード。これは、このページに保存した後に、SCCM 認証情報構成モーダルのパスワードフィールドで参照されるパスワードです。 ▪ ホスト:これは、このページに保存した後に SCCM 認証情報構成モーダルの [ホスト] フィールドで参照される SCCM サーバーのホストです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	e. [**MID** サーバーを使用] チェックボックスをオンにします。**[MID** 選択用に特定の MID サーバー] を選択し、[MID サーバー] リストから 1 つを選択します。 f. 灰色のヘッダーの任意の場所を右クリックし、[保存] を選択します。これらは、上記のステップ d で説明した接続フォームに入力した認証情報です。
ホスト	これは、上記のように [接続] ページで保存した後、[ホスト] フィールドから参照される SCCM サーバーのホストです。
ユーザー名	これは、前述のように [接続] ページで保存した後、[ユーザー名] フィールドから参照されるユーザー名です。
Password (パスワード)	これは、上記のように [接続] ページで保存した後に [パスワード] フィールドから参照されるパスワードです。
MID Server	これは、上記のように [接続] ページで保存した後、[MID サーバー] フィールドから参照される MID サーバーです。
検証ステータス	検証の試行後に入力されるフィールド。接続が成功すると、統合インスタンスのステータスは [有効] になります。
SG コネクタ接続	Microsoft SCCM のサービスグラフコネクタのリストから、接続および資格情報エイリアスのオプションを 1 つ選択します。この接続は、Microsoft SCCM SGC のガイド付きセットアップステップで設定します。
検証の詳細	検証試行の詳細。

6. 次のように移動する。 コネクタとユースケースのセットアップ > **SPC API** 統合.
7. 新しいインスタンスのリンクを選択します。
8. SCCM 認証情報構成モーダルで、[接続] フィールドのステップ 5 で作成したリストから接続を選択します。

   以下にリストされているフィールドは、新しい接続のために入力した情報に基づいて自動入力されることに注意してください。

ホスト	これは、上記のように [接続] ページで保存した後、[ホスト] フィールドから参照される SCCM サーバーのホストです。
ユーザー名	これは、前述のように [接続] ページで保存した後、[ユーザー名] フィールドから参照されるユーザー名です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Password (パスワード)	これは、上記のように [接続] ページで保存した後に [パスワード] フィールドから参照されるパスワードです。
MID Server	これは、上記のように [接続] ページで保存した後、[MID サーバー] フィールドから参照される MID サーバーです。
検証ステータス	検証の試行後に入力されるフィールド。接続が成功すると、統合インスタンスのステータスは [有効] になります。
SG コネクタ接続	リストから [接続および資格情報エイリアス] オプションを 1 つ選択します。
検証の詳細	検証試行の詳細。

9. [認証情報を保存してテスト] を選択します。
   次のステップに進むには、正常な接続に対する 有効な 応答が必要です。
10. [**Next**] を選択します。
    PowerShell スクリプトは、「 Microsoft SCCM のサービスグラフコネクタと Microsoft Defender 緩和コントロール統合のインストールと構成」で説明されているように作成されます。そのトピックの手順に従って、新しいインスタンスのスクリプトを承認します。

SentinelOne のサービスグラフコネクタ と **SentinelOne** 緩和コントロール統合のインストールと構成

緩和コントロール統合のための SentinelOne のサービスグラフコネクタ と SentinelOne 統合には、別々の構成手順が必要です。資産の詳細をインポートする SentinelOne のサービスグラフコネクタ をインストールして構成します。緩和コントロール統合用の SentinelOne 統合を設定して、SentinelOne のサービスグラフコネクタ によって監視される資産に関する緩和データを収集します。

始める前に

必要なロール：

- プラグインのインストールとアクティブ化のためのアドミン。
- ワークスペースでの統合を構成するための SPC アドミングループと SPC アナリストグループ。
- SentinelOne 認証情報。

手順

1. SentinelOne のサービスグラフコネクタ 統合をインストールして構成するには、次の手順を実行します。

   注:
   SentinelOne のサービスグラフコネクタをインストールした場合は、ステップ 2 に進み、緩和コントロール統合のための SentinelOne 統合を構成します。

   a. 次のように移動する。 コネクタとユースケースのセットアップ > [サービスグラフコネクタ] タブ.
   b. SentinelOne® のサービスグラフコネクタ 統合を見つけます。
   c. ServiceNow Store内のアプリケーションのアプリリストに移動するリンクを選択します。
   d. プロンプトに従ってアプリケーションをインストールします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

e. 終了する前に、アプリリストの [サポートリンクとドキュメント] セクションからインストールガイドをダウンロードして、構成とアクティブ化を支援します。

f. 次のように移動する。 セットアップ インスタンス内にあります

g. ガイド付きセットアップのプロンプトに従い、ドキュメントを参照して SGC を構成してアクティブ化します。

2. 次のように移動する。 コネクタとユースケースのセットアップ > **SPC API** 統合 緩和コントロール統合のために SentinelOne 統合を構成します。

   このタブには、緩和コントロールソース (CrowdStrike、F5 Big IP、Defender、SentinelOne) が一覧表示されます。このタブは、緩和コントロールモニタリングアプリケーションをインストールしている場合にのみワークスペースに表示されます。

   ソースカードでは、緩和ソースのステータス (アクティブ または 非アクティブ) を表示できます。

   [Sources] の [Active] 列に [Active] と表示されます。これは、ソース (この場合は SentinelOne のサービスグラフコネクタ) が資産データを取得するためにアクティブであることを示しますが、インポートされた資産の緩和コントロールを監視する前に、緩和コントロール統合のために SentinelOne 統合を構成する必要があります。

3. [**Next**] を選択します。
   [SentinelOne 構成] ページに、緩和コントロールインスタンスの 1 つの SentinelOne 統合リンクが表示されます。
4. [名前] 列に表示されるインスタンスリンクを選択します。
5. 緩和コントロール統合のための SentinelOne 統合のフィールドに入力します。

   注:

   緩和コントロール統合用の SentinelOne 統合に対して、 SentinelOne のサービスグラフコネクタ に指定したのと同じ SentinelOne アカウント情報とサーバーの詳細を入力します。この情報により、サービスグラフコネクタでインポートした資産データと一致する緩和データをインポートできます。

   フィールドを編集する必要がある場合は、ペンアイコンを選択します。

フィールド	説明
インスタンス名	フィールドにはインスタンス名が自動的に入力されます。
API キー	API キー情報が自動的に入力されるフィールド。
API URL	SentinelOne サーバーのホスト名 (例:https://usea1-na.sentinelone.net)

6. [認証情報を保存してテスト] を選択します。
   次のステップに進むには、正常な接続に対する 有効な 応答が必要です。
7. [保存して終了] を選択します。
8. [SPC API 統合] タブの SentinelOne カードで [詳細を表示] を選択します。
   ソースと API が有効になり、構成の進捗状況バーが完成していることを確認します。
9. オプション: [以前の認証情報に戻す] を選択して、以前に検証した認証情報を挿入します。
10. SentinelOne 資産インポート統合を実行するには、次の手順に従います。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

a. 次のように移動する。 **SentinelOne** 緩和コントロール > 統合.
統合は 1 つ、SGC SentinelOne Asset Import です。

b. [名前] 列で **[SentinelOne Prevention Policy Integration**] を選択して、統合を開始します。

c. レコードで、[アクティブ] チェックボックスをオンにして、[今すぐ実行] を選択します。

統合レコードの [統合実行] タブで統合実行状況を表示できます。

統合は、デフォルトで毎日実行されるようにスケジュールされています。

SentinelOne 資産インポート統合は、前回の統合実行以降に変更された資産に関する情報のみをインポートします。

Exploit Protection (WAF) に必要な軽減コントロールとポリシー

Exploit Protection Web アプリケーション ファイアウォール (WAF) の監視に必要な軽減コントロールとポリシーは、SPC 製品に含まれています。

エクスプロイト保護 **(WAF)**

このカテゴリの緩和コントロールは、Web アプリケーションファイアウォールの形式で利用可能な緩和をカバーしています。SPC は、必要に応じて、 F5 BIG-IP (F5) などの WAF ツールとの API 統合と ITOM IP ベースのディスカバリーからのネットワークトラフィックデータを使用して、Web アプリケーションファイアウォール (WAF) の背後で実行されているサーバーを検出します。

必要なロール: SPC アドミングループと SPC アナリストグループ。

を使用した **Exploit Protection (WAF)** の前提条件 **F5 BIG-IP**

1. F5 WAF および関連するアプリケーションサーバーがセットアップされている環境で、ITOM IP ベースのディスカバリーが有効になっていることを確認しますF5 BIG-IP
2. セキュリティポスチャコントロールワークスペースで F5 BIG-IP F5 の API 統合が有効になっていることを確認します。

Exploit Protection (WAF) の軽減コントロールとポリシー

F5 WAF保護:

- ソース: F5 および ITOM
- 対処された MITRE 戦術:初期アクセス
- 対処された MITRE テクニック:公開されているアプリケーションのエクスプロイト
- ポリシー:ポリシーは必要ありません。

緩和コントロールモニタリングのための **F5 BIG-IP** 統合の構成

ITOM IP ベースのディスカバリーアプリケーションと F5 BIG-IP API の統合には、別々の構成手順が必要です。資産の詳細をインポートするように ITOM IP ベースのディスカバリーアプリケーションを設定します。F5 BIG-IP API 統合を設定して、ITOM IP ベースのディスカバリーによって監視される資産に関する緩和データを収集します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に

- ITOM IP ベースのディスカバリーは、 F5 BIG-IP および関連するアプリケーションサーバーがセットアップされる環境で稼働している必要があります。
- オンプレミス資産の場合は、MID サーバーを指定する必要があります。
- ソース (ITOM) を有効にして、監視対象の資産に関するデータを収集します。
- API 統合をアクティブ化して、資産に関する緩和データを収集します。

必要なロール:プラグインのインストールとシステムプロパティの作成のためのアドミン、およびワークスペースでの統合の構成のためのアドミングループとSPCアナリストグループSPC。

手順

1. 統合をインストールして構成するには、次の手順を実行します。

   注:
   ITOM をインストールしてアクティブ化した場合は、ステップ 2 に進み、 F5 BIG-IP (F5) API 統合の構成方法を確認してください。

   a. 次のように移動する。 コネクタとユースケースのセットアップ > [サービスグラフコネクタ] タブ.
   b. F5 BIG-IPカードを選択します。
   c. [**ITOM** プラグイン] リンクを選択して、ITOM プラグインをアクティブ化します。
   d. プロンプトに従います。
2. 次のように移動する。 コネクタとユースケースのセットアップ > **SPC API** 統合.

   このタブには緩和コントロールソース (CrowdStrike と F5 Big IP、および SCCM) がリストされ、このタブは緩和コントロールモニタリングアプリケーションをインストールしている場合にのみワークスペースに表示されます。

   ソースカードでは、緩和ソースのステータス (アクティブ または 非アクティブ。
3. [**Next**] を選択します。

   ソース (ITOM) はアクティブですが、緩和コントロールを監視するには、 F5 BIG-IP API 統合を設定してアクティブ化する必要があります。
4. [名前] 列で [F5 BIG-IP] を選択します。
5. [編集] を選択し、フィールドに入力します。

フィールド	説明
名前	インスタンス名この名前を変更すると、認証情報をテストせずに保存することができます。[名前] フィールドの下のフィールドを変更する場合は、保存して終了する前に接続をテストする必要があります。
ユーザー名	F5 BIG-IP ユーザー名
Password (パスワード)	F5 BIG-IP パスワード。
MID Server	リストから MID サーバーを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
API URL	ポート 8443 の API URL (例:https://bigip.example.com:8443)。

6. 準備ができたら、[テスト接続] を選択します。
   接続に成功すると、メッセージが表示されます。

   構成手順中に接続をテストした結果、次のエラーが発生した場合: セッションに 証明書が含まれていません - 信頼できません: セッションに証明書が含まれていません - 信頼できない場合は、次のシステムプロパティを false に設定します。

   - com.glide.communications.httpclient.verify_hostname
   - com.glide.communications.httpclient.verify_revoked_certificate

   システムプロパティ [sys_properties] テーブルにリストされていない場合、アドミンロールを持つユーザーは、これらのシステムプロパティをグローバルスコープで作成する必要があります。システムプロパティは、タイプ、True/False (ブール) です。

7. **[Save and Exit** (保存して終了)] を選択します。
8. [SPC API 統合] タブの F5 BIG-IP カードで、ソースと API がアクティブ化され、構成の進捗状況バーが完了していることを確認します。
9. オプション: 資格情報テストが成功しなかった場合は、[以前の資格情報に戻す] を選択して、以前に検証した資格情報を挿入できます。
10. API 統合を実行するには、次の手順を実行します。

    a. 次のように移動する。 **F5 Big Ip** 緩和コントロール > 統合

       統合は 5 つあります。統合は連結され、特定の順序で実行されます。1 つの統合が正常に完了すると、次の統合が開始されます。

       - F5 Big IP デバイス統合
       - F5 Big IP ポリシー統合
       - F5 Big IP 攻撃署名統合
       - F5 Big IP 仮想サーバー統合
       - F5 Big IP プールメンバー統合

    b. 統合チェーンを開始するには、[名前] 列で **[F5 Big IP** デバイス統合] を選択します。

    c. レコードで、[アクティブ] チェックボックスをオンにして、[今すぐ実行] を選択します。

    d. 統合レコードの [統合実行] タブで統合実行のステータスを表示します。
       統合は、デフォルトで毎日実行されるようにスケジュールされています。

緩和コントロールポリシーをアクティブ化し、検出された緩和を表示する

利用可能な緩和コントロールによって軽減される資産に対する脅威を表示するには、ポリシーをアクティブ化する必要があります。

始める前に
Exploit Protection (EDR) に必要な軽減コントロールとポリシーを確認し、「緩和コントロールモニタリングのための CrowdStrike 統合をインストールして構成します」、「Microsoft SCCM の

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

サービスグラフコネクタと Microsoft Defender 緩和コントロール統合のインストールと構成」、および「緩和コントロールモニタリングのための F5 BIG-IP 統合の構成」に記載されている要件を完了していることを確認します。

必要なロール:SPC アドミングループと SPC アナリストグループ。

手順

1. 次のように移動する。 ワークスペース > セキュリティポスチャコントロール > ポリシーと検出結果 > **All** (すべて).
2. 次のポリシーをアクティブ化します。
   - SEH 上書き
   - ヒープスプレー
   - CrowdStrike NULL ページの割り当て
   - CrowdStrike DEP を強制
   - CrowdStrike ASLR を強制
   - Microsoft Defender コントロールフローガード
   - Microsoft Defender force ASLR
   - Microsoft Defender 必須 ASLR とボトムアップ ASLR
3. ダッシュボードの [MITRE 緩和策のある資産 (Assets with MITRE mitigations)] ウィジェットを使用して、セキュリティポスチャコントロールによって検出された緩和策のある資産を表示するには、次の手順を実行します。

   a. 次のように移動する。 ワークスペース > セキュリティポスチャコントロール > ホーム.

   b. [主要なインサイト] セクションで、[MITRE 緩和策を含む資産 (Assets with MITRE mitigations)] ウィジェットを確認します。

   c. ウィジェットで緩和カテゴリ、 エクスプロイト保護 **(EDR)** または エクスプロイト保護 **(WAF)** を選択します。

   d. その緩和カテゴリで緩和が検出された資産のリストを表示できます。

   e. 資産を選択します。

   f. [緩和コントロール] タブを選択して、検出された緩和コントロールの詳細を表示します。

   g. [緩和された脆弱性一致アイテム] タブを選択して、この緩和コントロールによって緩和される脆弱性一致アイテムのリストを表示します。

   > **注:**
   > このタブを設定するには、 脆弱性対応 アプリケーションをインストールしてアクティブ化する必要があります。

緩和コントロールから脆弱性一致アイテムへのマッピング

緩和コントロールデータは脆弱性一致アイテムにマッピングされます。脆弱性一致アイテムに関連付けられた脆弱性と根底にある共通脆弱性識別子 (CVE) を緩和するために使用される緩和コントロールのリストを表示できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティポスチャコントロールは、資産の特定の緩和コントロールを特定した後、そのコントロールによって緩和される脆弱性一致アイテムを自動的に識別します。たとえば、Web アプリケーションファイアウォール (WAF) ポリシーの署名の一部である CVE を持つ脆弱性一致アイテムは、緩和された脆弱性一致アイテムとしてマークされます。この識別は、脆弱性管理チームが、緩和された脆弱性一致アイテムのリスクスコアを自動的に削減するのに役立ちます。

脆弱性一致アイテム緩和コントロールテーブル

緩和コントロールデータを緩和された脆弱性一致アイテム (VIT) にマッピングするために、脆弱性一致アイテム緩和コントロール [sn_vul_vulnerable_item_mitigation_control] テーブルが作成されました。この表には、脆弱性一致アイテムに関連付けられた脆弱性とその基礎となる CVE を軽減するために使用された、緩和された VIT と検出された緩和コントロールがリストされています。軽減された CVE レコードには、資産に使用される緩和コントロール (Exploit Protection (EDR) など) への参照が含まれています。

サンプルデータを次の表に示します。

脆弱性一致アイテムの緩和コントロールデータ

緩和コントロールが存在します	緩和コントロール有効性	検出された緩和コントロールタイプ	**CVE** の緩和	脆弱性一致アイテム
はい/いいえ	中	エクスプロイト保護 (EDR)	CVE-2009-3373	VIT0018323

テーブルで緩和コントロールレコード (検出された緩和コントロールタイプ) を開き、CVE および関連する共通脆弱性タイプ一覧 (CWE) の脆弱性が、資産に関連付けられた緩和コントロールによってどのように緩和されるかの詳細を確認します。緩和コントロールレコードには、緩和された CWE に関する詳細 (緩和設定が CWE で指定された脆弱性をどのように満たすかなど) が含まれています。

リスク算出とリスク算出ルール

緩和情報を使用すると、カスタマイズされたリスク算出ルールを設定して、特定のタイプの脆弱性と緩和コントロールが関連付けられている VIT のリスクスコアを再計算できるようになります。前のテーブルに基づくこのルール例では、デフォルトのリスク算出では、検出された資産の緩和コントロールタイプが [エクスプロイト保護 (EDR)] の VIT のリスクスコアを 60 として計算します。この計算スコアは、この緩和策が実施されている脆弱性に関連付けられている中リスクによるものです。

次の条件を含むリスク算出ルールの例:

[緩和コントロールの詳細] [ではない] [空] かつ [緩和コントロールの詳細、検出された緩和コントロールタイプ] [次の値に等しい] [エクスプロイト保護 **(EDR)]**。

値:

[リスクスコア][次の値に等しい]**[60]**

詳細については、「脆弱性対応リスク算出のリスクルールのフィールドと重み付けの定義」を参照してください。

セキュリティポスチャコントロールにおけるユースケース、ポリシー例、サポートされるサービスグラフコネクタ

ユースケースは、特定タイプのツール範囲のギャップを識別するために構成するさまざまなシナリオです。各ユースケースには、潜在的な違反について資産を監査するためのポリシーが必要です。また、独自のポリシーを定義して、特定の内部セキュリティ標準の要件を満たすこともできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ユースケース

セキュリティポスチャコントロールアプリケーションは、アプリケーションに含まれるさまざまなユースケースをサポートします。ユースケースは、資産における特定タイプのツール範囲のギャップ、クラウド資産のインターネットエクスポージャー、および脆弱性との組み合わせを特定するのに役立ちます。サポートされているユースケースに必要なポリシーも製品に含まれています。

一部の主要なユースケースのカバレッジステータスは、次のセキュリティポスチャコントロールワークスペースのホーム (ランディング) ページで確認できます。 ワークスペース > セキュリティポスチャコントロール > ホーム ホームモジュール (ランディングページ) で。

または、一部の主要なユースケースでサポートされているサービスグラフコネクタとカバレッジステータスは、次の [サービスグラフコネクタに対応] タブと [主要なユースケースのセットアップ] タブで表示できます。 **All** (すべて) > ワークスペース > セキュリティポスチャコントロール > コネクタとユースケースのセットアップ (歯車のアイコン)。

注:

ホームランディングページの [主要なユースケース (Key use cases)] タブに、考えられるすべてのユースケースがリストされているわけではありません。そこにはセキュリティポスチャコントロール製品の展開を開始する際に役立つ、いくつかの重要なユースケースが示されています。

アプリケーションで提供されている、サポートされているユースケースのポリシーを有効にする前に、次のタスクを完了していることを確認してください。

- 「セキュリティポスチャコントロールでサポートされるアプリケーションのインストール」で説明されている必要なすべてのアプリケーションをインストールして構成済みである。
- ユースケースごとに、次の前提条件の 1 つ以上を満たしている。

1. 現在、さまざまなカテゴリのサービスグラフコネクタを使用しているか、インストールしてアクティブ化している。

   ユースケースのカテゴリには、初期インサイトを取得するためにアクティブ化する必要があるサービスグラフコネクタと、セキュリティポスチャコントロールが監視している資産のカバー範囲を改善するためにアクティブ化を選択できるサービスグラフコネクタが含まれます。

2. 脆弱性対応アプリケーションを現在使用しているか、インストールしてアクティブ化している。
3. 現在、クラウドセキュリティポスチャ管理 (CSPM) で AWS および Azure アカウントのクラウドアカウントスキャンを使用しているか、構成している。

サポートされている各ユースケースの特定の要件については、次のセクションで説明します。さらに、ユースケースのセキュリティポスチャコントロールに付属する 1 つ以上のポリシーをアクティブ化する必要があります。この概念については、以降のセクションでも説明します。

基本ポリシー、子ポリシー、クローンポリシーの例

セキュリティポスチャコントロール における基本ポリシー、子ポリシー、クローンポリシーの例 を参照して、他のポリシーの作成時に基本ポリシーの条件を再利用する方法を確認してください。これらは、基本ポリシーや子ポリシーの作成例および既存ポリシーのクローン作成例となります。これらの例では、ポリシーや検索結果のモジュールでポリシービルダーが機能する仕組みがわかります。

サポートされているサービスグラフコネクタ

サポートされているサービスグラフコネクタ、ツールカテゴリ、セキュリティポスチャコントロールでサポートされているハードウェアサービスグラフコネクタ および セキュリティポスチャコント

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロールでサポートされているソフトウェアサービスグラフコネクタ でインポートされるデータのタイプについてはテーブルを参照してください。

セキュリティポスチャコントロール のユースケース：エンドポイント保護が欠落している資産の検出

エンドポイント保護エージェントが欠落している資産を検出するには、次の前提条件が必要です。

ユースケースに応じて、必要なコネクタのみをアクティブ化することを選択できます。

1. [エンドポイント保護] カテゴリから少なくとも 1 つのサービスグラフコネクタを有効にします。
2. 次のいずれかのカテゴリに対してサービスグラフコネクタを少なくとも 1 つアクティブ化します。
   a. ディレクトリサービス (Microsoft Active Directory)。
   b. エンドポイント管理：Microsoft Intune または Jamf デバイスとエンドポイントの管理。
   c. 構成とパッチ管理：MicrosoftSCCM または IBM Bigfix。
   d. クラウドプロバイダー：Amazon AWS クラウド、Microsoft Azure、GCP。

   > **注:**
   > クラウドディスカバリーがアクティブ化されている場合、これらのサービスグラフコネクタ製品は必要ありません。

3. [オプション] 次のいずれかのカテゴリのサービスグラフコネクタをアクティブ化して、全体的なカバー範囲、つまりセキュリティポスチャコントロールによって報告および監視される資産の数を向上させることができます。
   a. ネットワークセキュリティ
   b. インフラストラクチャモニタリング
   c. ネットワーク
   d. アプリケーションパフォーマンスモニタリング。

これらの前提条件を満たしていることを確認したら、次のポリシー「エンドポイント保護が欠落している資産」をアクティブ化する必要があります。 ポリシーの詳細については、「セキュリティポスチャコントロール のポリシー」を参照してください。

セキュリティポスチャコントロール のユースケース：脆弱性アセスメントツールによって見落とされた資産の検出

脆弱性評価ツールによって見落とされた資産を検出するには、次の前提条件が必要です。

リスト内のサービスグラフコネクタごとに、オンプレミス資産またはクラウド資産の監視にそのコネクタが必要かどうかを確認できます。ユースケースに応じて、必要なコネクタのみをアクティブ化することを選択できます。

1. [脆弱性アセスメント] カテゴリから少なくとも 1 つのサービスグラフコネクタを有効にします。
2. 次のいずれかのカテゴリに対してサービスグラフコネクタを少なくとも 1 つアクティブ化します。
   a. ディレクトリサービス (Microsoft Active Directory)。
   b. エンドポイント管理：Microsoft Intune または Jamf デバイスとエンドポイントの管理。
   c. 構成とパッチ管理：MicrosoftSCCM または IBM Bigfix。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

d. クラウドプロバイダー：Amazon AWS クラウド、Microsoft Azure、GCP。

> **注:**
> クラウドディスカバリーがアクティブ化されている場合、これらのサービスグラフコネクタ製品は必要ありません。

3. [オプション] 次のいずれかのカテゴリのサービスグラフコネクタをアクティブ化して、全体的なカバー範囲、つまりセキュリティポスチャコントロールによって報告および監視される資産の数を向上させることができます。

a. ネットワークセキュリティ。

b. ネットワーク。

c. インフラストラクチャモニタリング。

d. アプリケーションパフォーマンスモニタリング。

これらの前提条件を満たしていることを確認したら、「資産の脆弱性がスキャンされていません」ポリシーを有効にする必要があります。ポリシーの詳細については、「セキュリティポスチャコントロール のポリシー」を参照してください。

セキュリティポスチャコントロール のユースケース：管理対象外資産の検出

このユースケースには、構成が欠落している資産の検出とパッチ管理エージェントの 2 つの部分が含まれています。

構成ツールとパッチ管理ツールがない資産を検出するには、次の前提条件が必要です。

リスト内のサービスグラフコネクタごとに、オンプレミス資産またはクラウド資産の監視にそのコネクタが必要かどうかを確認できます。

ユースケースに応じて、必要なコネクタのみをアクティブ化することを選択できます。

1. [構成とパッチ管理] カテゴリから少なくとも 1 つのサービスグラフコネクタをアクティブ化します。

2. 次のいずれかのカテゴリに対してサービスグラフコネクタを少なくとも 1 つ有効にする必要があります。

a. ディレクトリサービス (Microsoft Active Directory)。

b. エンドポイント保護：CrowdStrike または SentinelOne。

c. 脆弱性アセスメント：Qualys、Rapid7、または Tenable。

d. 構成とパッチ管理：MicrosoftSCCM または IBM Bigfix。

3. [オプション] 次のいずれかのカテゴリのサービスグラフコネクタをアクティブ化して、全体的なカバー範囲、つまりセキュリティポスチャコントロールによって報告および監視される資産の数を向上させることができます。

a. ネットワーク。

b. インフラストラクチャモニタリング

c. ネットワークセキュリティ

d. アプリケーションパフォーマンスモニタリング。

これらの前提条件を満たしていることを確認したら、少なくとも 1 つのポリシーを有効にする必要があります。先頭が「クラウド資産」のポリシーの場合は、「クラウドプロバイダー」カテゴリのサービスグラフコネクタを有効にする必要があります。ポリシーの詳細については、「セキュリティポスチャコントロール のポリシー」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 構成とパッチ管理が欠落している資産。
- 構成とパッチ管理が欠落しているクラウド資産。

セキュリティポスチャコントロール のユースケース：エンドポイント管理ソリューションが欠落している資産の検出

エンドポイント管理ソリューションがない資産を検出するには、次の前提条件が必要です。

ユースケースに応じて、必要なコネクタのみをアクティブ化することを選択できます。

1. [エンドポイント管理] カテゴリから少なくとも 1 つのサービスグラフコネクタを有効にします。
2. 次のいずれかのカテゴリに対してサービスグラフコネクタを少なくとも 1 つ有効にする必要があります。
   a. ディレクトリサービス (Microsoft Active Directory)。
   b. エンドポイント保護：CrowdStrike または SentinelOne。
   c. 脆弱性アセスメント：Qualys、Rapid7、または Tenable。
   d. 構成とパッチ管理：MicrosoftSCCM または IBM Bigfix。

これらの前提条件を満たしていることを確認したら、次のポリシー「資産にエンドポイント管理ソリューションがありません」を有効にする必要があります。ポリシーの詳細については、「セキュリティポスチャコントロール のポリシー」を参照してください。

セキュリティポスチャコントロール のユースケース：脆弱性とセキュリティツール範囲とのギャップがある資産の検出

重大な脆弱性がある資産や、エンドポイント保護などの重要なセキュリティツールが欠落している資産を特定して、修復対象の資産に優先順位を付けることができます。セキュリティポスチャコントロールには、このユースケースをサポートするいくつかのポリシーが製品に付属しています。

このユースケースでは、脆弱性対応アプリケーションをインストールすることと、少なくとも脆弱性アセスメント製品 (Qualys、Rapid7、Tenable など) との統合が必要です。

以下のポリシーはセキュリティポスチャコントロール製品に含まれており、重大な脆弱性がありセキュリティツールの対象範囲にもなっていない資産に対するこのユースケースをサポートしています。

1. 重大な脆弱性があり、エンドポイント保護が欠落している資産。
2. 重大な脆弱性があり、構成とパッチ管理が欠落している資産。
3. 重大な脆弱性があり、エンドポイント管理が欠落している資産。

セキュリティポスチャコントロール のユースケース：クラウド資産と高リスクの組み合わせによるインターネットエクスポージャーの検出

さまざまなポートでクラウド資産 (仮想マシン) の潜在的なインターネットエクスポージャーを監視して、これらの資産の脆弱性がリモートで悪用されないようにすることが重要です。このユースケースは、これらの資産を特定するのに役立ちます。

セキュリティポスチャコントロールを使用すると、クラウド資産の構成を評価して、インターネットに接続されている資産、つまり、インターネット上のあらゆるところからアクセスできるようになっている資産や、資産が晒されているポートを特定することができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティポスチャコントロールは、これらのインサイトを、セキュリティツール範囲のギャップや、Qualys、Rapid7、Tenable などのサードパーティスキャナーからの脆弱性データと組み合わせて、高リスクの組み合わせを特定します。

現在、このユースケースは AWS をサポートしており、次の前提条件が必要です。

1. AWS のサービスグラフコネクタが、構成した同じ AWS アカウントに対してアクティブ化されている。
2. セキュリティポスチャコントロールで製品に含まれている 1 つ以上のポリシーがアクティブになっている。
   - SSH ポート 22 がインターネットに開かれているクラウド資産。
   - SSH ポート 22 がインターネットに開かれており、エンドポイント保護が欠落しているクラウド資産。
   - HTTP ポート 80 がインターネットに開かれており、エンドポイント保護が欠落しているクラウド資産。
   - 重大な脆弱性があり、SSH ポート 22 がインターネットに開かれているクラウド資産 (脆弱性対応が必要)。
   - 重大な脆弱性があり、エンドポイント保護が欠落しており、SSH ポート 22 がインターネットに開かれているクラウド資産 (脆弱性対応が必要)。
   - インターネットに対してオープンな HTTP ポート、重大な脆弱性、およびエンドポイント保護がないクラウド資産 (脆弱性対応が必要)。

セキュリティポスチャコントロールでサポートされているハードウェアサービスグラフコネクタ

サポートされている CI クラス、ソース (製品)、およびツールカテゴリを含むハードウェアサービスグラフコネクタ。このリストは完全ではなく、製品の追加に伴って変更される可能性があります。

リストされているコネクタのディスカバリーソースの場合、SG-AWS、SGO-Datadog、SGC-AD (Active Directory) などのサードパーティ製品の製品名の前に「SG」、「SGO」または「SGC」が付きます。ServiceNow 製品の場合、製品名の前に「SN」または「ServiceNow」が付きます。たとえば、ServiceNow ハードウェア資産管理の場合は SNAssetManagement になります。

これらをインストールすると、インスタンスのコネクタテーブル [sn_sec_spc_core_connector] でコネクタやカテゴリを表示できるようになります。

[sn_sec_spc_core_asset_type_connector] テーブルでは、資産タイプと、CI クラスやコネクタへのマッピングを確認することができます。

ハードウェアサービスグラフコネクタ

資産タイプ	CI クラス	資産ソース	コネクタのカテゴリ
ハードウェア資産	cmdb_ci_computer	Active Directory	ディレクトリサービス
ハードウェア資産	cmdb_ci_server	AppDynamics	アプリケーションパフォーマンスモニタリング
ハードウェア資産	cmdb_ci_server	オートモックス	構成とパッチ管理
ハードウェア資産	cmdb_ci_computer	オートモックス	構成とパッチ管理
ハードウェア資産	cmdb_ci_computer	BigFix	構成とパッチ管理
ハードウェア資産	cmdb_ci_server	BigFix	構成とパッチ管理

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ハードウェアサービスグラフコネクタ (続く)

資産タイプ	CI クラス	資産ソース	コネクタのカテゴリ
ハードウェア資産	cmdb_ci_printer	Cisco Meraki	ネットワーク
ハードウェア資産	cmdb_ci_server	Cisco Meraki	ネットワーク
ハードウェア資産	cmdb_ci_iot	Cisco Meraki	ネットワーク
ハードウェア資産	cmdb_ci_hc_device	Cisco Meraki	ネットワーク
ハードウェア資産	cmdb_ci_netgear	Cisco Meraki	ネットワーク
ハードウェア資産	cmdb_ci_computer	Cisco Meraki	ネットワーク
ハードウェア資産	cmdb_ci_server	CrowdStrike	エンドポイント保護
ハードウェア資産	cmdb_ci_server	Datadog	インフラストラクチャモニタリング
ハードウェア資産	cmdb_ci_server	Dynatrace	アプリケーションパフォーマンスモニタリング
ハードウェア資産	cmdb_ci_computer	Dynatrace	アプリケーションパフォーマンスモニタリング
ハードウェア資産	cmdb_ci_computer	ExtraHop Reveal(x)	ネットワークセキュリティ
ハードウェア資産	cmdb_ci_hc_device	ExtraHop Reveal(x)	ネットワークセキュリティ
ハードウェア資産	cmdb_ci_server	ExtraHop Reveal(x)	ネットワークセキュリティ
ハードウェア資産	cmdb_ci_iot	ExtraHop Reveal(x)	ネットワークセキュリティ
ハードウェア資産	cmdb_ci_printer	ExtraHop Reveal(x)	ネットワークセキュリティ
ハードウェア資産	cmdb_ci_iot	Forescout	ネットワークセキュリティ
ハードウェア資産	cmdb_ci_hc_device	Forescout	ネットワークセキュリティ
ハードウェア資産	cmdb_ci_computer	Forescout	ネットワークセキュリティ
ハードウェア資産	cmdb_ci_server	Forescout	ネットワークセキュリティ
ハードウェア資産	cmdb_ci_printer	Forescout	ネットワークセキュリティ
ハードウェア資産	cmdb_ci_server	Intune	エンドポイント管理
ハードウェア資産	cmdb_ci_computer	Intune	エンドポイント管理
ハードウェア資産	cmdb_ci_printer	Jamf Pro	エンドポイント管理
ハードウェア資産	cmdb_ci_server	Jamf Pro	エンドポイント管理

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ハードウェアサービスグラフコネクタ (続く)

資産タイプ	CI クラス	資産ソース	コネクタのカテゴリ
ハードウェア資産	cmdb_ci_computer	Jamf Pro	エンドポイント管理
ハードウェア資産	cmdb_ci_server	Lansweeper	IT Asset Management
ハードウェア資産	cmdb_ci_computer	Lansweeper	IT Asset Management
ハードウェア資産	cmdb_ci_printer	Lansweeper	IT Asset Management
ハードウェア資産	cmdb_ci_hc_device	LogicMonitor	インフラストラクチャモニタリング
ハードウェア資産	cmdb_ci_printer	LogicMonitor	インフラストラクチャモニタリング
ハードウェア資産	cmdb_ci_server	LogicMonitor	インフラストラクチャモニタリング
ハードウェア資産	cmdb_ci_vm_instance	LogicMonitor	インフラストラクチャモニタリング
ハードウェア資産	cmdb_ci_iot	LogicMonitor	インフラストラクチャモニタリング
ハードウェア資産	cmdb_ci_computer	LogicMonitor	インフラストラクチャモニタリング
ハードウェア資産	cmdb_ci_netgear	LogicMonitor	インフラストラクチャモニタリング
ハードウェア資産	cmdb_ci_server	Microsoft Defender	エンドポイント保護
ハードウェア資産	cmdb_ci_server	New Relic	アプリケーションパフォーマンスモニタリング
ハードウェア資産	cmdb_ci_computer	Nexthink	デジタル従業員エクスペリエンス
ハードウェア資産	cmdb_ci_computer	Netskope	データ損失防止
ハードウェア資産	cmdb_hardware_product_model	Netskope	データ損失防止
ハードウェア資産	cmdb_ci_network_adapter	Netskope	データ損失防止
ハードウェア資産	cmdb_software_instance	Netskope	データ損失防止
ハードウェア資産	cmdb_sam_sw_install	Netskope	データ損失防止
ハードウェア資産	sn_sec_sgc_netskop_client_attribute	Netskope	データ損失防止
ハードウェア資産	cmdb_ci_server	テレメトリを開く	アプリケーションパフォーマンスモニタリング
ハードウェア資産	cmdb_ci_computer	パペット	構成とパッチ管理
ハードウェア資産	cmdb_ci_server	パペット	構成とパッチ管理
ハードウェア資産	cmdb_ci_computer	Qualys	脆弱性アセスメント

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ハードウェアサービスグラフコネクタ (続く)

資産タイプ	CI クラス	資産ソース	コネクタのカテゴリ
ハードウェア資産	cmdb_ci_server	Qualys	脆弱性アセスメント
ハードウェア資産	cmdb_ci_vm_instance	Qualys-ServiceNow	脆弱性アセスメント
ハードウェア資産	cmdb_ci_server	Qualys-ServiceNow	脆弱性アセスメント
ハードウェア資産	cmdb_ci_hardware	Rapid7	脆弱性アセスメント
ハードウェア資産	cmdb_ci_computer	SCCM	構成とパッチ管理
ハードウェア資産	cmdb_ci_server	SCCM	構成とパッチ管理
ハードウェア資産	cmdb_ci_printer	ScienceLogic	インフラストラクチャモニタリング
ハードウェア資産	cmdb_ci_iot	ScienceLogic	インフラストラクチャモニタリング
ハードウェア資産	cmdb_ci_server	ScienceLogic	インフラストラクチャモニタリング
ハードウェア資産	cmdb_ci_computer	ScienceLogic	インフラストラクチャモニタリング
ハードウェア資産	cmdb_ci_hc_device	ScienceLogic	インフラストラクチャモニタリング
ハードウェア資産	cmdb_ci_vm_instance	ScienceLogic	インフラストラクチャモニタリング
ハードウェア資産	cmdb_ci_hardware	ServiceNow HAM	ハードウェア資産管理
ハードウェア資産	cmdb_ci_hardware	ServiceNow ITOM ディスカバリー	ディスカバリー
ハードウェア資産	cmdb_ci_aws_datacenter	センチネルワン	エンドポイント保護
ハードウェア資産	cmdb_ci_azure_datacenter	センチネルワン	エンドポイント保護
ハードウェア資産	cmdb_ci_availability_zone	センチネルワン	エンドポイント保護
ハードウェア資産	cmdb_ci_google_datacenter	センチネルワン	エンドポイント保護
ハードウェア資産	cmdb_ci_cloud_service_account	センチネルワン	エンドポイント保護
ハードウェア資産	cmdb_ci_cloud_subnet	センチネルワン	エンドポイント保護
ハードウェア資産	cmdb_ci_compute_template	センチネルワン	エンドポイント保護
ハードウェア資産	cmdb_ci_network	センチネルワン	エンドポイント保護
ハードウェア資産	cmdb_ci_vm_instance	センチネルワン	エンドポイント保護
ハードウェア資産	cmdb_key_value	センチネルワン	エンドポイント保護
ハードウェア資産	cmdb_ci_os_template	センチネルワン	エンドポイント保護
ハードウェア資産	cmdb_ci_server	センチネルワン	エンドポイント保護
ハードウェア資産	cmdb_ci_computer	センチネルワン	エンドポイント保護
ハードウェア資産	sn_sec_sgc_sntlone_asset_tags	センチネルワン	エンドポイント保護
ハードウェア資産	cmdb_ci_ip_address	センチネルワン	エンドポイント保護

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ハードウェアサービスグラフコネクタ (続く)

資産タイプ	CI クラス	資産ソース	コネクタのカテゴリ
ハードウェア資産	cmdb_ci_network_adapter	センチネルワン	エンドポイント保護
ハードウェア資産	sn_sec_sgc_sntlone_additional_attributes	センチネルワン	エンドポイント保護
ハードウェア資産	cmdb_ci_server	Tanium 資産	エンドポイント管理
ハードウェア資産	cmdb_ci_computer	Tanium 資産	エンドポイント管理
ハードウェア資産	cmdb_ci_ups	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ot_industrial_sensor	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ot_cnc	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_hardware	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_netgear	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ot_industrial_actuator	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ip_switch	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_hub_network	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_security	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_server	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ot_rtu	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ot_ews	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ot_plc	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ot_control	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ot_dcs	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_storage_server	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ot_hmi	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ot_control_module	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ot_industrial_robot	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ot_historian	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ot_industrial_drive	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_iot	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ip_firewall	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_computer	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_unclassed_hardware	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ids_network	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_ot_ied	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_printer	Tenable	脆弱性アセスメント
ハードウェア資産	cmdb_ci_computer	VMWare Workspace ONE UEM	エンドポイント管理

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ハードウェアサービスグラフコネクタ (続く)

資産タイプ	CI クラス	資産ソース	コネクタのカテゴリ
ハードウェア資産	cmdb_ci_server	VMWare Workspace ONE UEM	エンドポイント管理
ハードウェア資産	cmdb_ci_printer	VMWare Workspace ONE UEM	エンドポイント管理
ハードウェア資産	cmdb_ci_vm_instance	Wiz	クラウドネイティブアプリケーション保護プラットフォーム
ハードウェア資産	cmdb_ci_server	Wiz	クラウドネイティブアプリケーション保護プラットフォーム
ハードウェア資産	cmdb_ci_linux_server	Wiz	クラウドネイティブアプリケーション保護プラットフォーム
ハードウェア資産	cmdb_ci_win_server	Wiz	クラウドネイティブアプリケーション保護プラットフォーム

セキュリティポスチャコントロールでサポートされているソフトウェアサービスグラフコネクタ

サポートされている CI クラス、ソース (製品)、およびツールカテゴリを含むソフトウェアサービスグラフコネクタ。このリストは完全ではなく、製品の追加に伴って変更される可能性があります。

これらをインストールすると、インスタンスのコネクタテーブル [sn_sec_spc_core_connector] でコネクタやカテゴリを表示できるようになります。

[sn_sec_spc_core_asset_type_connector] テーブルでは、資産タイプと、CI クラスやコネクタへのマッピングを確認することができます。

ソフトウェアサービスグラフコネクタ

資産タイプ	CI クラス	資産ソース	コネクタのカテゴリ
ソフトウェア	cmdb_ci_spkg	BigFix	構成とパッチ管理
ソフトウェア	cmdb_ci_spkg	Dynatrace	アプリケーションパフォーマンスモニタリング
ソフトウェア	cmdb_ci_spkg	Forescout	ネットワークセキュリティ
ソフトウェア	cmdb_ci_spkg	Intune	エンドポイント管理
ソフトウェア	cmdb_ci_spkg	Jamf Pro	エンドポイント管理
ソフトウェア	cmdb_ci_spkg	New Relic	アプリケーションパフォーマンスモニタリング
ソフトウェア	cmdb_ci_spkg	Nexthink	デジタル従業員エクスペリエンス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ソフトウェアサービスグラフコネクタ (続く)

資産タイプ	CI クラス	資産ソース	コネクタのカテゴリ
ソフトウェア	cmdb_ci_spkg	Netskope	データ損失防止
Software (ソフトウェア)	cmdb_ci_spkg	Qualys-ServiceNow	脆弱性アセスメント
ソフトウェア	cmdb_ci_spkg	SCCM	構成とパッチ管理
ソフトウェア	cmdb_ci_spkg	ServiceNow ITOM ディスカバリー	ディスカバリー
ソフトウェア	cmdb_ci_spkg	Tanium 資産	エンドポイント管理
ソフトウェア	cmdb_ci_spkg	VMWare Workspace ONE UEM	エンドポイント管理

セキュリティポスチャコントロール における基本ポリシー、子ポリシー、クローンポリシーの例

幅広い条件セットを有する独自の基本ポリシーを作成することが、より複雑なポリシーを作成するうえでの足掛かりとなります。

例

子ポリシーの作成や既存ポリシーのクローン作成で他のポリシーを作成するうえで、基本ポリシーの条件をどのように再利用したらよいのか、次の例で説明します。これらの例では、ポリシーや検索結果のモジュールでポリシービルダーが機能する仕組みがわかります。

まず、基本ポリシーの例から見ていきます。基本ポリシーが、他の例の足掛かりとなります。

注:
これらの例では、CrowdStrike サービスグラフコネクタがサービスグラフコネクタとして使用されていますが、実際にはインストールした任意のコネクタを使用して構いません。これらの例では、ポリシーを作成およびアクティブ化して、一致する資産を検索します。これらのポリシーは、アクティブ化した後でも [ポリシーと検索結果] モジュールでいつでも削除することができます。

セキュリティポスチャコントロールの基本ポリシーの作成 (例)

他のポリシーの作成に使用できる基本ポリシーの作成方法の例を示します。

始める前に
必要なロール：SPC アドミングループまたは SPC アナリストグループ

手順

1. 次のように移動する。 **All** (すべて) > セキュリティポスチャコントロールワークスペース > ポリシーと検出結果.
2. [新しいポリシー] を選択します。
3. 左上のペンアイコンを選択し、[メタデータを編集] モーダルでフィールドに入力します。
4. [メタデータを保存 **(Save Metadata)]** を選択します。
5. 条件ビルダーで、[資産タイプ] として [ハードウェア資産] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このポリシーでは、[基本ポリシー] オプションと [除外ポリシー] オプションをデフォルトの (オフ) 設定のままにします。

6. [接続] で [集計データあり **(With aggregated data)]** を選択します。

   このポリシーの場合、集計データは、Windows 10 がインストールされている CMDB 内の資産を見つけるのに役立ちます。たとえば、一部のレコードでは、スキャナーが「Windows 10」を報告する方法がわずかに異なる場合があります。集計されたデータにより、「Windows 10」のこれらすべてのわずかなバリエーションがこのポリシーに一致することが保証されます。

   [エンティティ] フィールドと [基準] フィールドは、[接続] フィールドの選択に基づいて自動的に入力されます。

7. [プロパティ] で **[OS]** を選択します。
8. Windows 10 の値タイプの場合。
9. [変更内容を保存] を選択します。
   基本ポリシーは [ポリシーと結果 (Policies and findings)] モジュールの [すべて] リストに表示されますが、アクティブ化されていません。
10. [ポリシーのアクティブ化] を選択すると、基本ポリシーでポリシーの条件に一致する資産が監視され、結果が生成されます。

セキュリティポスチャコントロールの基本ポリシーからの子ポリシーの作成 (例)

基本ポリシーの条件を使用して子ポリシーを作成する方法の例。

始める前に

この子ポリシーは基本ポリシーの条件を継承し、子ポリシーにさらに条件を追加して、より具体的な資産の詳細に集中できるようにします。CrowdStrike サービスグラフコネクタによって報告される Windows 10 がインストールされているすべてのデバイスを監視する新しいポリシーが必要であり、別のポリシーに一致するデバイスを除外します。この例では、Integrated Risk Management (IRM) の例外に対して承認された資産を結果から除外します。

> **注:**
> CrowdStrike サービスグラフコネクタがインストールされていない場合は、インストールされているものを使用できます。

必要なロール：SPC アドミングループまたは SPC アナリストグループ

手順

1. 次のように移動する。 **All** (すべて) > セキュリティポスチャコントロールワークスペース > ポリシーと検出結果.
2. [アクティブ] リストから、最初の例で作成した [基本ポリシー - Windows 10 デバイス] を見つけて選択し、レコードを開きます。
3. その他のオプションメニュー (縦に並んだ 3 つのドット) を選択し、[子ポリシーを作成 **(Create child policy)]** を選択します。
   新しいタブが開き、新しいレコードと [基本ポリシー - Windows 10 デバイス] が [基本ポリシー (Base policy)] フィールドに表示されます。
4. 左上のペンアイコンを選択し、[メタデータを編集] モーダルでフィールドに入力します。
5. [メタデータを保存 **(Save Metadata)]** を選択します。
6. 条件ビルダーで、[資産タイプ] として [ハードウェア資産] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. [基本ポリシー (Base policy)] トグルを選択します。
8. 例 1 の [基本ポリシー **- Windows 10** デバイス] で作成したポリシーをリストから選択します。

   この子ポリシーは、基本ポリシーの条件を自動的に継承します。
9. [除外ポリシー] トグルを選択します。
10. リストから [IRM 例外が承認された資産 (Assets with IRM exception approved)] を選択します。

    注:
    このポリシーがない場合は、このポリシーから除外する別のポリシーをリストから選択できます。

    このポリシーに一致する資産は、子ポリシーから除外されます。さらにポリシーを追加できることに注意してください。
11. [報告者] を選択します。
12. リストから **[CrowdStrike]** を選択します。
13. [変更内容を保存] を選択します。
    新しいポリシーは [ポリシーと結果 (Policies and findings)] モジュールの [すべて] リストに表示されますが、アクティブ化されていません。
14. [ポリシーのアクティブ化] を選択すると、基本ポリシーでポリシーの条件に一致する資産が監視され、結果が生成されます。

セキュリティポスチャコントロールのポリシーのクローンを作成する (例)

別のポリシーから条件をコピーするポリシーを作成する方法の例。

始める前に

例 2 で作成したポリシーから条件をコピーしてポリシーを作成し、再入力しなくて済むようにします。これらの条件のクローンを作成し、作成した子ポリシーのコピーにさらに条件を追加します。この例では、このポリシーで CrowdStrike を搭載した Windows 10 デバイスを検索し、過去 7 日間に確認されていない IRM 例外のある資産を除外します。

必要なロール：SPC アドミングループまたは SPC アナリストグループ

手順

1. 次のように移動する。 **All** (すべて) > セキュリティポスチャコントロールワークスペース > ポリシーと検出結果.
2. [アクティブ] リストから、2 番目の例で作成した子ポリシー - CrowdStrike を搭載した Windows デバイスを見つけ、それを選択してレコードを開きます。
3. その他のオプションメニュー (縦に並んだ 3 つのドット) を選択し、[ポリシーのクローン作成 **(Clone policy)]** を選択します。
   新しいタブが開き、タイトルに「copy」が含まれる新しいレコードにポリシー名 (CrowdStrike を搭載した Windows デバイス-copy) が表示されます。
4. 左上のペンアイコンを選択し、[メタデータを編集] モーダルでフィールドに入力します。
5. [メタデータを保存 **(Save Metadata)]** を選択します。
6. 最初の [接続] フィールドと [エンティティ] フィールドの右側で、新しいフィールドの **[AND]** 演算子を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

これにより、論理 AND が「接続 - エンティティ」の基準と、別の「接続 - エンティティ」の新たな基準の間に追加されます。この場合、「過去 7 日間に CrowdStrike によって認識されなかった資産のコネクタデータ」を指定します。

7. [接続] で [コネクタデータあり **(With connector data)]** を選択します。
8. [エンティティ] で [CrowdStrike：**CrowdStrike** デバイスの詳細 **(CrowdStrike: CrowdStrike Device Details)]** を選択します。
   この基準フィールドは、選択内容に基づいて自動的に入力されます。
9. [プロパティ] で [最終確認時間] を選択します。
10. [値] で [今週] を選択します。
11. [変更内容を保存] を選択します。
12. [ポリシーのアクティブ化] を選択します。
    これらのポリシーは、[ポリシーと結果 (Policies and Findings)] モジュールからいつでも削除できます。

[store-future: BEGIN review]

Cloud Security Posture Management と Amazon Web サービスの統合

ServiceNow によって開発されたクラウドセキュリティポスチャ管理 (CSPM) アプリケーションは、クラウド環境を継続的にスキャンして、CIS などのコンプライアンスフレームワークに対する非準拠または構成違反を特定します。

主要な用語と概念

現在、ServiceNow の CSPM は CIS AWS Foundations Benchmark v1.4.0 をサポートしています。このモジュールは、AWS 環境のクラウド資産の構成データをクラウドから直接収集し、Now Platform インスタンスにインポートして、コンプライアンスを監査します。

リージョン

リージョンとは、AWS クラウドサービスがサポートする地理的領域のことです。リージョンには、そのリージョンでサポートされているサービスにアクセスできるデフォルトのエンドポイントがあります。リージョンの例には、米国のバージニアやオハイオ、または米国外の他のデータセンター があります。

リソース

リソースは、AWS 資産とその構成設定を説明する AWS 環境で使用される用語です。リソースは AWS 環境のサービスです。Now Platform インスタンスでは、リソースは資産または構成アイテム (CI) と呼ばれます。

インターネットセキュリティセンター (CIS)

CIS は、IT システムとデータを保護するための世界的に認められたプロセスである CIS Controls および CIS Benchmarks を担当するコミュニティ主導型の非営利団体です。現在、ServiceNow CSPM アプリケーションは、CIS AWS Foundations 1.4.0 で公開されているガイドラインを使用して、クラウド資産のコンプライアンスを監査します。

ポリシー (設定ポリシー)

ポリシーはガバナンスのガイドラインです。Now Platform では、ポリシーは構成ポリシーと呼ばれます。ServiceNow によって開発された CSPM アプリケーションは、CIS などのベンチマーク標準に対してクラウド環境を評価するためのベースライン構成ポリシーを提供します。構成ポリシーとコンプライアンスフレームワークで提供されるガイドラインの間には 1 対 1 のマッピングがあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ポリシーセット (設定ポリシーグループ)

ポリシーセットは個々のポリシーのグループです。Now Platform では、ポリシーセットは設定ポリシーグループと呼ばれます。

Cloud Security Posture Management

ポリシー (構成ポリシー) とポリシーセット (構成ポリシーグループ) は、この統合のためにインスタンスに作成された **Cloud Security Posture Management** モジュールにあります。

テスト

テストは、資産のスキャンを整理するデータレコードのライブラリです。構成テストでは、コンプライアンスを満たすためにテクノロジー資産のクラスを管理する方法を定義します。テストは、修復の際に資産をグループ化するために コンフィグレーションコンプライアンス アプリケーションで使用されます。

テスト結果

クラウド環境のリソースがコンプライアンス違反であることが監査によって検出された場合、インスタンスにテスト結果 (TR) が作成されます。テスト結果は、Now Platform の コンフィグレーションコンプライアンス アプリケーションに保存されます。これらのレコードには、リソースで実行された監査の結果 (合格/不合格) が表示されます。

テスト結果グループ

テスト結果グループは、テスト結果を論理グループに整理し、修復タスクの優先順位を付けるのに役立ちます。

必要な **Now Platform** ロール

sn_vul.cspm_security_admin ロールを持つセキュリティアドミンは、この製品を使用できます。クラウドアカウントスキャンは、sn_vul.cspm_cloud_account_admin ロールを持つユーザーが設定することもできます。

この統合に必要なロールの完全なリストについては、「」を参照してください。

ワークフロー

- アプリケーションに含まれるポリシーセット (構成ポリシーグループ) によって、インポートするデータが定義されます。
- インポートされたリソース構成データは、Now Platform インスタンスの一時テーブルに格納されます。この保存されたデータは、CIS Amazon Web Services Foundations Benchmark v1.4.0 に記載されているポリシーに準拠しているかどうか監査されます。
- 監査の結果は、プラットフォームインスタンスの コンフィグレーションコンプライアンス アプリケーションにテスト結果およびテスト結果グループとして作成されます。
- テスト結果、テスト結果グループ、およびその他の コンフィグレーションコンプライアンス データをダッシュボードと コンフィグレーションコンプライアンス アプリケーションのレコードで表示できます。セキュリティマネージャー、脆弱性マネージャー、および脆弱性アナリストは、このデータを使用して、資産の構成関連の脆弱性を特定し、それらに対応することができます。

データコレクション

環境内の AWS クラウド構成データを収集するには、Now Platform® インスタンスから MID サーバーを介して AWS クラウド API を呼び出します。エンタープライズ環境の AWS リソースのデータをプルします。リソースのデータには、監査のためにインポートできる次の幅広い情報が含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ID とアクセス管理 (IAM)
- ストレージ
- ログ記録
- 監視
- ネットワーク

インポートされたデータのセキュリティおよび構成の非準拠の例

次のリストには、非準拠リソースの例、または資産構成における健全なセキュリティ慣行からの逸脱が含まれています。

- 公開されている S3 バケットを確認します。
- 暗号化されていない S3 バケットを確認します。
- IAM ユーザーキーはローテーションされません。
- 特定のベンダーからの仮想マシン (VM) イメージへのアクセスが制限されていることを確認します。
- どの IP アドレスが公開されているかを確認します。
- S3 バケットに対してマルチファクター認証 (MFA) が有効になっているかどうかを確認します。

ポリシーとベンチマーク標準

CIS Amazon Web Services Foundations Benchmark v1.4.0 では、58 個のポリシーが定義されています。これらのポリシーのうち 47 個は、このアプリケーションの一部としてインスタンスにコーディングされています。ベンチマークにもリストされている 11 個の手動ポリシーは、このアプリケーションではサポートされていません。

[End]
[store-future: BEGIN review]

AWS 向け CSPM Innovation Lab アプリケーションのインストールとアクティブ化

この統合に必要なアプリケーションは、ServiceNow® Store で入手でき、アプリリストページの [依存関係とライセンスを表示] リンクの下に表示されます。一部のアプリケーションには、個別にダウンロードしてインストールする必要がある依存関係があります。

始める前に
必要なロール：すべてのアプリケーションのダウンロード、インストール、およびアクティベーションを行うアドミン。

アドミニストレーターは次のロールをアサインします。アプリケーションにはこれらの Now Platform® ロールが必要です。

アプリケーションのダウンロードとアクティブ化の詳細については、「」のトピックを参照してください。
•

- ServiceNow Store アプリケーションのアクティブ化

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 受信したメールに記載されているリンクをクリックして、ServiceNow Store でこの統合用のアプリケーションにアクセスします。

   アプリケーションの依存関係を表示するには、ServiceNow Store のアプリケーションページの [依存関係およびライセンス] で [依存関係とライセンス要件を表示] をクリックします。

   注:
   Cloud Security Posture Management アプリケーションは ServiceNow Store の **Innovation Lab** リンクの下にあります。他のアプリケーションは [アプリとソリューション] の下にあります。

2. 次の順序でアプリケーションをインストールします。

アプリケーション	アプリのバージョンと依存関係プラグイン
プラットフォームバージョン	San Diego vx.xx
脆弱性対応 (依存関係)	v x.xx
コンフィグレーションコンプライアンス (依存関係)	v x.xx
CMDB CI クラスモデル	CMDB CI クラスモデル 、分岐マスターをインストールする
Security Support Common	リポジトリ (branch feature/EPIC1037528_native_cspm) から Security Support Common (プラグイン ID：com.snc.security_support.common) をインストールする
Security Integration Framework	リポジトリ (branch feature/EPIC1037528_native_cspm) から Security Integration Framework (プラグイン ID：com.snc.sec.int.framework) をインストールする
セキュリティサポートオーケストレーション	リポジトリ (branch secops-dev) からセキュリティサポートオーケストレーション (プラグイン ID：com.snc.secops.orchestration) をインストールする
脆弱性対応 (コアアプリケーション)	リポジトリ (branch feature/EPIC1037528_native_cspm) から脆弱性対応 (プラグイン ID：com.snc.vulnerability) をインストールする
Configuration Compliance (コアアプリケーション)	リポジトリ (branch feature/EPIC1037528_native_cspm) から Configuration Compliance (プラグイン ID：com.snc.vulc) をインストールする
Vulnerability Response and Configuration Compliance for Cloud	リポジトリ (branch scratch/STRY53500471_overview) から Vulnerability Response and Configuration Compliance for Cloud (プラグイン ID：com.snc.vul_cloud) をインストールする

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション	アプリのバージョンと依存関係プラグイン
脆弱性対応のパフォーマンスアナリティクス	リポジトリ (branch feature/EPIC1037528_native_cspm) から脆弱性対応のパフォーマンスアナリティクス (プラグイン ID：com.snc.vulnerability.analytics) をインストールする
ServiceNow IntegrationHub Enterprise Pack Installer	ServiceNow IntegrationHub Enterprise Pack Installer (プラグイン ID：com.glide.hub.integrations.enterprise) をインストールする
Cloud Provisioning and Governance Core	Cloud Provisioning and Governance Core (com.snc.cloud.core) をインストールする
クラウドアクションライブラリ	リポジトリ 、分岐マスターからクラウドアクションライブラリ (プラグイン ID：com.sn.itom.cal) をインストールする
クラウドコンフィグレーションガバナンス	クラウドコンフィギュレーションガバナンス (プラグイン ID：com.sn.itom.ccg) 、分岐マスターをインストールする
Cloud Security Posture Management	リポジトリ (branch scratch/develop) から Cloud Security Posture Management (プラグイン ID：com.snc.secops.cspm) をインストールする

3. ServiceNow Storeからアプリケーションをダウンロードしたら、Now Platformインスタンスで **All** (すべて) > システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて).
4. 前のテーブルに記載されているアプリケーションを見つけ、[インストール] をクリックしてアクティブ化します。
   アプリケーションとともに自動的にインストールされる依存関係アプリケーションは、[アプリケーションのインストール] ダイアログに表示されます。ただし、インストール中に依存関係プラグインをインストールするように求められた場合は、表示されるプロンプトに従ってください。前のテーブルに記載されているすべてのアプリケーションと依存関係がインストールされ、アクティブ化されていることを確認します。

   アプリケーションが正常にアクティブ化されると、ダイアログが表示されます。
5. アプリケーションをインストールしてアクティブ化した後、まだ割り当てられていない場合は、次のロールをアサインします。

   統合のさまざまなワークフローアクティビティには、次のロールが必要です。

   - discovery_admin または sn_cmmp.cloud_admin - 対応する AWS サービスアカウントの Now Platform でクラウドサービスアカウントを設定します。
   - cspm_security_admin。このロールは、次のロールも継承します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- sn_itom_ccg.governor - 新しいポリシー、ポリシーセット、およびコレクターを作成します。ガバナーロールは「テストポリシー」を実行し、スケジューリングアドミニストレーターが使用する新しいエンティティを作成します。
- sn_itom_ccg.operator - クラウドコンフィグレーションガバナンス オペレーターはポリシーをテストし、結果をチェックします。オペレーターは、テスト結果とテスト結果グループも修正します。
- sn_itom_ccg.scheduling_admin - AWS サービスアカウントの クラウドコンフィグレーションガバナンス を設定します。スキャン設定とスキャンスケジュールを作成します。インポートされたエンティティとポリシーを表示するためのスキャン結果へのアクセス権があります。

◦ cspm_cloud_account_admin。このロールは、sn_itom_ccg.scheduling_admin ロールも継承します。

◦ mid_server - MID サーバーを設定します。

◦ sn_vulc.admin - コンフィグレーションコンプライアンス アプリケーションを設定し、すべてのレコードを表示し、プロパティを変更できます。コンフィグレーションコンプライアンス アプリケーションでロールをアサインします。コンフィグレーションコンプライアンス アプリケーションのロールの詳細については、「コンフィグレーションコンプライアンスと一緒にインストールされるコンポーネント」を参照してください。

◦ sn_vuln.admin - 脆弱性対応のパフォーマンスアナリティクス アプリケーションを設定します。

AWS 環境で資産をスキャンするためのスキャンレコードを作成するには、次のステップを実行します。

6. まだ完了していない場合は、AWS のサービスアカウントと認証情報、および認証情報エイリアスを設定します。
discovery_admin または sn_cmmp.cloud_admin を持つユーザーが Amazon Web サービス (AWS) サービスアカウントを設定します。詳細については、「」を参照してください。作成したクラウドサービスアカウントレコードの [ディスカバリー認証情報] 列にこれらの認証情報が表示されます。

7. Cloud Discovery および Cloud Provisioning and Governance の AWS リソースへのアクセスに必要なレベルの権限を持つポリシーを設定します。
次の JSON を付録に配置して、権限を作成します。テキストをコピーし、必要な編集を行います。このファイルを使用して、ポリシー権限を作成します。少なくとも、これらの権限はこのアプリケーションに必要な権限です。詳細については、「」を参照してください。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "iam:GenerateCredentialReport",
    "access-analyzer:ListAnalyzers",
    "iam:GetPolicyVersion",
    "iam:GetAccountPasswordPolicy",
    "iam:ListServerCertificates",
    "s3:GetBucketLogging",
    "cloudtrail:GetTrailStatus",
    "ec2:DescribeFlowLogs",
    "ec2:DescribeRegions",
    "logs:DescribeMetricFilters",
    "cloudtrail:GetEventSelectors",
    "iam:ListVirtualMFADevices",
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
        "s3:GetEncryptionConfiguration",
        "kms:GetKeyRotationStatus",
        "iam:ListAttachedUserPolicies",
        "rds:DescribeDBInstances",
        "iam:GetCredentialReport",
        "ec2:DescribeNetworkAcls",
        "iam:ListPolicies",
        "sns:ListSubscriptionsByTopic",
        "iam:ListEntitiesForPolicy",
        "iam:ListUserPolicies",
        "s3:GetBucketVersioning",
        "config:DescribeConfigurationRecorderStatus",
        "cloudtrail:DescribeTrails",
        "ec2:DescribeSecurityGroups",
        "kms:ListKeys",
        "config:DescribeConfigurationRecorders",
        "ec2:DescribeVpcs",
        "cloudwatch:DescribeAlarms",
        "iam:GetLoginProfile",
        "iam:GetAccountSummary"
      ],
      "Resource": "*"
    }
  ]
}
```

8. sn_itom_ccg.scheduling_admin ロールを持つユーザーが、前のステップで作成した Amazon Web サービス サービスアカウント用の クラウドコンフィグレーションガバナンス の AWS 認証情報を使用してクラウドサービスアカウントを設定します。

   必要なステップの詳細については、「」を参照してください。

9. まだ完了していない場合は、mid_server ロールを持つユーザーが Now Platform MID サーバーをセットアップして、 インスタンスを AWS アカウントに接続します。

   詳細については、「」を参照してください。

10. MID サーバーをセットアップすると、sn_itom_ccg.scheduling_admin を持つユーザーがデータセンター検出を実行してサービスアカウントのあるデータセンターを識別します。

    詳細については、「」を参照してください。

    注:
    クラウドサービスアカウントのテーブルに入力しないと、統合が正しく実行されません。

11. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > グループルール をクリックし 、[アサイン先グループ、テストルール] を選択してレコードを開き、[アクティブ] フィールドを **true** に設定します。

    コンフィグレーションコンプライアンス では、アプリケーションに含まれるグループルールとアサインルールはデフォルトで無効になっています。sn_vulc.admin を持つユーザーがこれらのルールをアクティブ化します。

    このルールは、監査中に作成されたテスト結果をグループ化します。false のテスト結果が返された特定のポリシーのすべてのテスト結果が 1 つのテスト結果グループにグループ化されます。

    デフォルトでは、テスト結果グループは CI サポートユーザーグループにアサインされます。デフォルトでは、このアサインルールは非アクティブです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

12. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > アサインルール をクリックし、[CI サポートグループにアサイン] レコードを選択して開き、[アクティブ] チェックボックスをクリックしてアクティブ化します。

    このルールは、CI サポートグループのユーザーにテスト結果グループをアサインします。これらのテスト結果で作業するユーザーをこのグループにアサインします。

    これはデフォルトのアサインルールであり、組織内のプラクティスによっては、組織のクラウド構成の問題をアサインするのに役に立たない可能性があります。代わりに、要件に適したアサインルールを作成することもできます。クラウドアカウントのメタデータを使用するには、[テスト結果] テーブルから [検出されたアイテム] テーブルをドット連結して、アサインルールを定義します。

13. 次のように移動する。 パフォーマンスアナリティクス > データコレクター > ジョブ PA CC 日次コレクタージョブを見つけて、これらのジョブがアクティブ化されていることを確認します。

    脆弱性対応のパフォーマンスアナリティクス ダッシュボードで監査結果を表示するには、sn_vuln.admin ロールを持つユーザーがアプリケーションを有効にし、データコレクタをアクティブ化します。

    統合のセットアップが完了しました。CSPM アプリケーションでスキャン設定レコードを作成する準備ができました。

[End]

[store-future: BEGIN review]

ServiceNow CSPM アプリケーションと AWS を使用したクラウドアカウントのスキャン

このセクションでは、クラウドアカウントのセキュリティスキャンを設定して、ベンチマークフレームワークに対するリソースのコンプライアンスを確認する方法について説明します。サンプルポリシーを使用して、このプロセスを示します。

始める前に

必要な設定：この例では、まずスキャンレコードを作成します。AWS サービスアカウントの情報を設定または確認する場合は、 のセットアップステップを参照してください。

必要なロール：sn_vul.cspm_cloud_account_admin

手順

1. 次のように移動する。 **All** (すべて) > クラウドセキュリティポスチャ管理 **(CSPM)** > アドミニストレーション > クラウドアカウントスキャン をクリックして、CSPM アプリケーションでスキャン設定レコードを作成します。
   [ポリシー評価ルール] ページが表示されます。
2. [新規] をクリックします。
3. フィールドに入力します。

   a. スキャン構成の一意の名前を入力します。

   b. 後でレコードを見つけることができるように、簡単な説明を入力します。

   c. [クラウドサービスアカウント] を選択し、必要なターゲットサービスアカウントを選択します。これらは、AWS アカウントに対して作成して設定し、クラウドコンフィグレーションガバナンス に入力したレコードです。

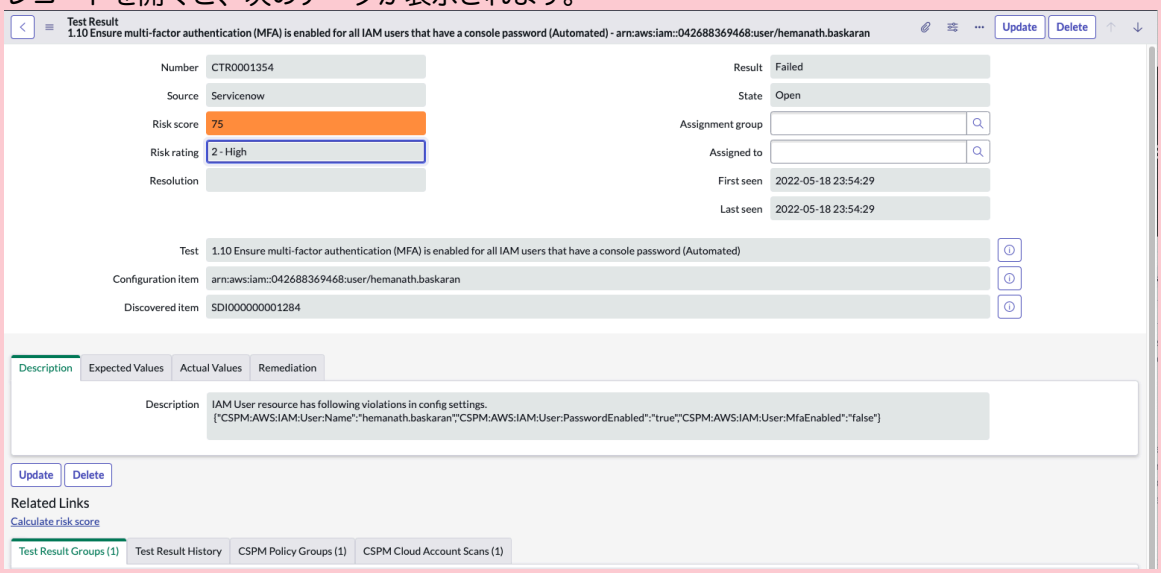
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [バックグラウンドスキャン] チェックボックスをオンにしてアクティブ化します。
スキャンを 1 時間ごとに実行する場合は、[バックグラウンドスキャン] チェックボックスをオンにしてアクティブ化します。チェックボックスが選択されていない場合は、スキャンをオンデマンドで起動する必要があります。
5. リンクされた子アカウントを自動スキャンするには、[リンクされた子アカウントを自動的にスキャン] チェックボックスをオンにします。
6. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > テスト結果 > **All** (すべて).
ポリシー監査から作成されたテスト結果グループ (CTR#) のリストが表示されます。

   コンプライアンス違反のクラウドリソースのテスト結果レコードが作成されます。違反が修正されると、テスト結果レコードがクローズされます。

7. レコードを開くと、次のデータが表示されます。



テストフィールド

このフィールドには、監査に使用されるポリシーと コンフィグレーションコンプライアンス の監査テストレコード間の 1 対 1 のマッピングが表示されます。クリックしてテストレコードをプレビューして開き、引用、つまり信頼できるソースを表示します。この例では、信頼できるソースは CIS AWS Foundations Benchmark v1.4.0 で、引用されたセクション (ポリシー) は 1.10 です。このポリシーが属する各ポリシーグループが表示されます。ポリシーは複数のポリシーグループに含めることができます。また、監査によって生成されたテスト結果の数も表示されます。

[構成アイテム] フィールド

このデータは AWS のリソースを参照しています。

検出されたアイテムフィールド

Now Platform で検出されたアイテムは AWS リソースに関連付けられています。リージョン、クラウドアカウント、リソースタイプなど、AWS リソースについてインポートされたすべてのクラウドメタデータは、検出されたアイテムレコードに保存されます。

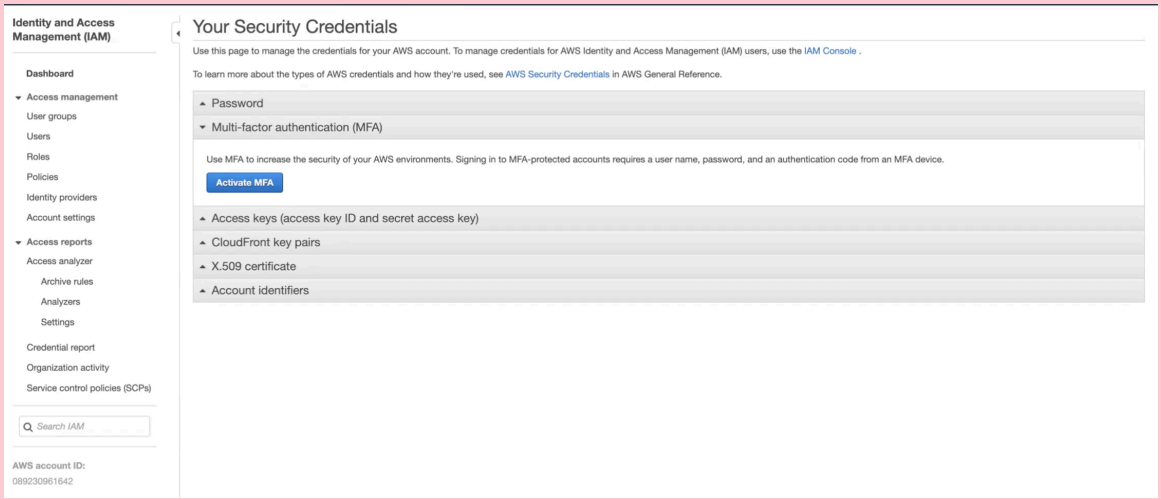
テスト結果のグループタブ

デフォルトでは、コンフィグレーションコンプライアンス アプリケーションは、監査での誤検出に基づいてテスト結果をテスト結果グループにグループ化します。1 つのリソースに対してテスト結果ごとに 1 つのレコードのみが作成され、データのインポート後に更新されます。スキャンとスキャンの間に AWS 環境のリソースの構成設定が変更されると、Now Platform インスタンスでレコードが更新されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

8. インポートされたデータを確認するには、AWS ユーザーアカウントに戻ります。

   この例では、このアカウントのチェックはマルチファクター認証が有効にされていないことを示しています (**[MFA** のアクティブ化 **(Activate MFA)]**)。このステータスは、クラウドからインポートされたリソースとリソースグループに関するセキュリティデータと一致します。設定を変更してリソースが準拠すると、変更は次のデータインポートに反映されます。次の例では、テスト結果レコードを閉じる前に、このリソースに対して AWS で MFA をアクティブ化する必要があります。



[End]

脆弱性対応のパフォーマンスアナリティクス ダッシュボードでの **AWS CSPM** 監査データの表示

この統合には、脆弱性対応のパフォーマンスアナリティクス アプリケーションのダッシュボードが含まれます。

始める前に

必要なロール：pa_viewer

手順

1. ダッシュボードを表示するには、次に移動します: コンフィグレーションコンプライアンス > 概要.

   ダッシュボードのデータは毎日収集されます。設定を変更するには、次に移動します: パフォーマンスアナリティクス > データコレクター > ジョブ.

   > **注:**
   > 他のサードパーティの脆弱性統合を実行している場合、すべての脆弱性データと監査結果データが一緒にダッシュボードに視覚的に表示されます。フィルターを設定して、CSPM データを除外することができます。

   ダッシュボードには次の 3 つのタブがあります。

   - 資産カテゴリ
   - 修復
   - 承認

2. データを表示するには、タブをクリックします。
3. データの可視化の下に、データに含まれる信頼できるソースが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CSPM での AWS のカスタムポリシーの作成

カスタマイズされたコンプライアンス標準を実装するためのポリシーを作成します。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > クラウドセキュリティポスチャ管理 **(CSPM)** > 設定ポリシー.
2. **[New** (新規)] を選択します。
3. フォームのフィールドに入力します。

CSPM カスタムポリシー作成フォーム

フィールド	説明		
ポリシー名	一意のポリシー名。		
説明	ポリシーの詳細。		
リソースタイプ			
クラウドプロバイダ	ポリシーのクラウド提供プラットフォーム。		
リソースタイプ	クラウド環境でのリソースのタイプ。リソースタイプが存在しない場合は、AWS または Azure の規則を使用してリソースタイプを作成します。		
ポリシー条件			
タイプ			
条件	テスト結果を作成する条件。次のシナリオを考えてみましょう。		
	構成キーが存在しますか？	リソースタイプが存在しますか？	次のステップ
	はい	はい。リソースタイプとメタデータを取得するためのフローが存在します。サブフローの例：CSPM：Azure サブスクリプションリソースコレクター	ポリシーの条件を指定します。
	いいえ	はい	**a.** 構成キーを作成します。 **b.** リソースコレクターを作成します。 **c.** 構成コレクターを作成します。 **d.** ポリシーの条件を指定します。
重大度	ポリシーの重大度。		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [送信] を選択してカスタムポリシーを作成します。

Microsoft Azure を使用した Cloud Security Posture Management

ServiceNow® によって開発された Cloud Security Posture Management (CSPM) アプリケーションは、クラウド環境を継続的にスキャンして、CIS などのコンプライアンスフレームワークに対する非準拠または構成違反を特定します。

主要な用語と概念

ServiceNow によって開発されたこの CSPM 統合は、CIS をサポートしています Microsoft Azure. この統合は、Microsoft Azure 環境のクラウド資産の構成データをクラウドから直接収集し、Now Platform インスタンスにインポートして、コンプライアンスに準拠しているか資産を監査します。

この CSPM 統合の概念を理解するために、次の用語が用意されています。Azure 製品の詳細については、Azure.com を参照してください。

リージョン

リージョンとは、Microsoft Azure クラウドサービスがサポートする地理的領域のことです。リージョンには、そのリージョンでサポートされているサービスにアクセスできるデフォルトのエンドポイントがあります。リージョンの例には、米国のバージニアやオハイオ、または米国外の他のデータセンター があります。

リソース

リソースは、Microsoft Azure 資産とその構成設定を説明する Microsoft Azure 環境で使用される用語です。リソースは Microsoft Azure 環境のサービスです。仮想マシン、ストレージアカウント、Web アプリ、データベース、および仮想ネットワークは、一般的なリソースの例です。Now Platform インスタンスでは、リソースは資産または構成アイテム (CI) と呼ばれます。

リソースグループ

Microsoft Azure アカウントのリソースはリソースグループに整理できます。グループは、特定の Microsoft Azure ソリューションまたは製品の関連リソースを保持します。リソースグループ内のリソースはさまざまなリージョンに配置でき、グループ自体の外部のリージョンに配置できます。リソースグループには、そのリソースに関するメタデータが格納されます。リソースグループの場所を指定するときは、そのメタデータが格納される場所を指定します。コンプライアンスのため、データが特定のリージョンに保存されていることを把握しておく必要があります。

インターネットセキュリティセンター (CIS)

CIS は、IT システムとデータを保護するための世界的に認められたプロセスである CIS Controls および CIS Benchmarks を担当するコミュニティ主導型の非営利団体です。現在、ServiceNow CSPM アプリケーションは、Microsoft Azure (CIS Microsoft Azure Foundations Benchmark バージョン 1.4.0 で公開されているガイドラインを使用して、クラウド資産のコンプライアンスを監査します。

オートメーション

この用語は、完全に自動化され、合格/不合格ステータスによって検証できる、資産または技術的コントロールの監査の結果として得られる推奨事項を指します。この統合では自動アセスメントがサポートされています。

ポリシー (設定ポリシー)

ポリシーはガバナンスのガイドラインです。Now Platform では、ポリシーは構成ポリシーと呼ばれます。ServiceNow によって開発された CSPM アプリケーションは、CIS などのベンチマーク標準に対してクラウド環境を評価するためのベースライン

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

構成ポリシーを提供します。構成ポリシーとコンプライアンスフレームワークで提供されるガイドラインの間には 1 対 1 のマッピングがあります。

ポリシーセット (設定ポリシーグループ)

ポリシーセットは個々のポリシーのグループです。Now Platform では、ポリシーセットは設定ポリシーグループと呼ばれます。

Cloud Security Posture Management

ポリシー (構成ポリシー) とポリシーセット (構成ポリシーグループ) は、この統合のためにインスタンスに作成された **Cloud Security Posture Management** モジュールにあります。

テスト

テストは、構成ポリシー用に作成された記述子レコードです。CSPM モジュールのすべての構成ポリシーには、Configuration Compliance モジュールで自動的に作成された同等の構成テストがあります。構成テストは、テスト結果、つまりスキャンからの構成検出結果によって参照され、特定のクラウドリソースで評価されたテストまたはポリシーを識別するのに役立ちます。

テスト結果

クラウド環境のリソースがコンプライアンス違反であることが監査によって検出された場合、インスタンスにテスト結果 (TR) が作成されます。テスト結果は、Now Platform の コンフィグレーションコンプライアンス アプリケーションに保存されます。これらのレコードには、リソースで実行された監査の結果 (合格/不合格) が表示されます。

テスト結果グループ

テスト結果グループは、テスト結果を論理グループに整理し、修復タスクの優先順位を付けるのに役立ちます。

必要な **Now Platform** ロール

sn_vul.cspm_security_admin ロールを持つセキュリティアドミンは、この製品を使用できます。クラウドアカウントスキャンは、sn_vul.cspm_cloud_account_admin ロールを持つユーザーが設定することもできます。

この統合に必要なロールの完全なリストについては、「」を参照してください。

ワークフロー

- アプリケーションに含まれるポリシーセット (構成ポリシーグループ) によって、インポートするデータが定義されます。
- インポートされたリソース構成データは、Now Platform インスタンスの一時テーブルに格納されます。この保存されたデータは、次にリストされているポリシーに準拠しているかどうか監査されます。 Microsoft Azure. . この統合でサポートされている自動化ポリシーは 56 個あります。手動ポリシーと 9 個の自動ポリシーはサポートされていません。
- 監査の結果は、プラットフォームインスタンスの コンフィグレーションコンプライアンス アプリケーションにテスト結果およびテスト結果グループとして作成されます。
- テスト結果、テスト結果グループ、およびその他の コンフィグレーションコンプライアンス データをダッシュボードと コンフィグレーションコンプライアンス アプリケーションのレコードで表示できます。セキュリティマネージャー、脆弱性マネージャー、および脆弱性アナリストは、このデータを使用して、資産の構成関連の脆弱性を特定し、それらに対応することができます。

データコレクション

環境内の Microsoft Azure クラウド構成データを収集するために、ServiceNow は Now Platform インスタンスから MID サーバーを介して Microsoft Azure クラウド API を呼び出します。構成ポ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リシーを評価するために、Microsoft Azure リソースの構成データが取得されます。構成データが取得されるサービスまたはリソースには、次のものが含まれます。

- ID とアクセス管理 (IAM)
- ストレージ
- データベースサービス
- ログ記録と監視
- ネットワーク
- 仮想マシン
- キーの有効期限などのセキュリティに関する考慮事項
- AppService

インポートされたデータのセキュリティおよび構成の非準拠の例

次のリストには、非準拠リソースを特定するために Microsoft Azure クラウドリソースで評価される構成ポリシーのいくつかの例が含まれています。

- BLOB ストレージのアクセスレベルが「プライベート」に設定されているかどうかを確認します。
- 重要なデータの BLOB ストレージが暗号化されているかどうかを確認します。
- ストレージアクセスキーが定期的に再生成されるようにします。
- すべての仮想マシン (VM) のエンドポイント保護がインストールされているかどうかを確認します。
- ストレージアカウントのデフォルトアクセスが「拒否」に設定されているかどうかを確認します。
- 標準 MySQL データベースサーバーの [SSL 接続を強制] が [有効] に設定されているかどうかを確認します。

ポリシーとベンチマーク標準

約 123 のポリシーが定義されています Microsoft Azure. .これらのポリシーまたは推奨事項のうち 56 件は、デフォルトで CSPM アプリケーションに含まれています。

Microsoft Azure 向け CSPM Innovation Lab アプリケーションのインストールとアクティブ化

この統合に必要なアプリケーションは、ServiceNow® Store で入手でき、アプリリストページの [依存関係とライセンスを表示] リンクの下に表示されます。一部のアプリケーションには、個別にダウンロードしてインストールする必要がある依存関係があります。

始める前に
必要なロール：すべてのアプリケーションのダウンロード、インストール、およびアクティベーションを行うアドミン。

アドミンは、ステップ 5 にリストされている Now Platform® ロールをアサインします。これらの Now Platform® ロールはアプリケーションに必要です。

アプリケーションのダウンロードとアクティブ化の詳細については、「」のトピックを参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 受信したメールに記載されているリンクをクリックして、ServiceNow Store でこの統合用のアプリケーションにアクセスします。

   アプリケーションの依存関係を表示するには、ServiceNow Store のアプリケーションページの [依存関係およびライセンス] で [依存関係とライセンス要件を表示] をクリックします。

   > **注:**
   > Microsoft Azure 向け Cloud Security Posture Management アプリケーションは ServiceNow Store の **Innovation Lab** リンクの下にあります。他のアプリケーションは [アプリとソリューション] の下にあります。

2. 次のテーブルにリストされている順序でアプリケーションをインストールします。
3. ServiceNow Storeからアプリケーションをダウンロードしたら、Now Platformインスタンスで **All** (すべて) > システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて). アプリケーションを見つけて、テーブルにリストされている順序でアクティブ化します。
4. [インストール] をクリックしてアクティブ化します。

   > **注:**
   > これらのアプリケーションは、インストールに 2 ～ 3 時間かかる場合があります。

アプリケーション	アプリのバージョンと依存関係プラグインをインストールする
プラットフォームバージョン	San Diego、Tokyo
脆弱性対応 (依存関係)	プラグイン ID：com.snc.vul_dep
Configuration Compliance (依存関係)	プラグイン ID：com.snc.vulc_dep
CMDB CI クラスモデル	CMDB CI クラスモデル：com.sn_cmdb_ci_class - 1.39.0 をインストールする
Security Support Common	プラグイン ID：com.snc.security_support.common - 13.3.3
Security Integration Framework	プラグイン ID：com.snc.sec.int.framework - 13.2.2
セキュリティサポートオーケストレーション	プラグイン ID：com.snc.secops.orchestration - 12.3.0
脆弱性対応 (コアアプリケーション)	プラグイン ID：sn_vul - 17.0.2
コンフィギュレーションコンプライアンス (コアアプリケーション)	プラグイン ID：sn_vulc - 14.4.4
脆弱性対応のパフォーマンスアナリティクス	プラグイン ID：com.snc.vulnerability.analytics - 12.4.4
ServiceNow IntegrationHub Enterprise Pack Installer	プラグイン ID：com.glide.hub.integrations.enterprise
Cloud Provisioning and Governance Core	プラグイン ID：com.snc.cloud.core
クラウドアクションライブラリ	プラグイン ID：com.sn.itom.cal - 1.3.6
クラウドコンフィグレーションガバナンス	プラグイン ID：com.sn.itom.ccg - 1.3.7

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション	アプリのバージョンと依存関係プラグインをインストールする
CCG Content Pack	プラグイン ID：com.sn.itom.ccg_cp - 1.3.7
Cloud Security Posture Management	プラグイン ID：com.snc.secops.condor - 1.1.1

アプリケーションとともに自動的にインストールされる依存関係アプリケーションは、[アプリケーションのインストール] ダイアログに表示されます。ただし、インストール中に依存関係プラグインをインストールするように求められた場合は、表示されるプロンプトに従ってください。

前のテーブルに記載されているすべてのアプリケーションと依存関係がインストールされ、アクティブ化されていることを確認してから、次のステップに進みます。

アプリケーションが正常にアクティブ化されると、ダイアログが表示されます。

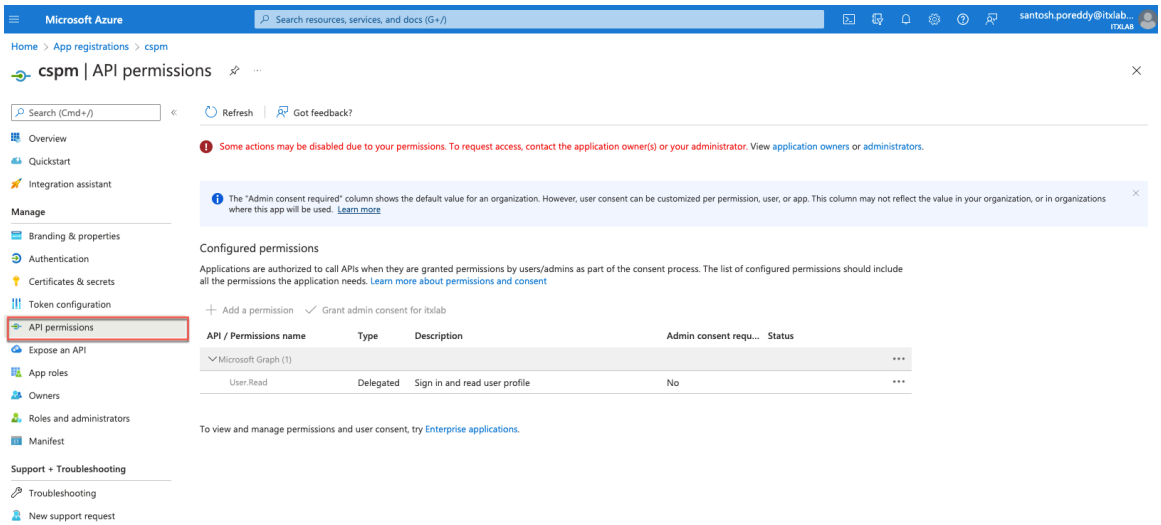
5. まだアサインされていない場合は、次のロールをアサインします。
統合のさまざまなワークフローアクティビティには、次のロールが必要です。
   - discovery_admin または sn_cmmp.cloud_admin - 対応する Microsoft Azure サービスアカウントの Now Platform でクラウドサービスアカウントを設定します。
   - cspm_security_admin。このロールは、次のロールも継承します。
     - sn_itom_ccg.governor - ポリシー、ポリシーセット、およびコレクターを作成します。ガバナーロールは「テストポリシー」を実行し、スケジューリングアドミニストレーターが使用する新しいエンティティを作成します。
     - sn_itom_ccg.operator - クラウドコンフィグレーションガバナンス オペレーターはポリシーをテストし、結果をチェックします。オペレーターは、テスト結果とテスト結果グループも修正します。
     - sn_itom_ccg.scheduling_admin - Microsoft Azure アカウントに クラウドコンフィグレーションガバナンス を設定します。スキャン設定とスキャンスケジュールを作成します。インポートされたエンティティとポリシーを表示するためのスキャン結果へのアクセス権があります。
   - cspm_cloud_account_admin。このロールは、sn_itom_ccg.scheduling_admin ロールも継承します。
   - mid_server - MID サーバーを設定します。
   - sn_vulc.admin - コンフィグレーションコンプライアンス アプリケーションを設定し、すべてのレコードを表示し、プロパティを変更できます。コンフィグレーションコンプライアンス アプリケーションでロールをアサインします。コンフィグレーションコンプライアンス アプリケーションのロールの詳細については、「コンフィグレーションコンプライアンスと一緒にインストールされるコンポーネント」を参照してください。
   - sn_vuln.admin - 脆弱性対応のパフォーマンスアナリティクス アプリケーションを設定します。

   Microsoft Azure 環境で資産をスキャンするためのスキャンレコードを作成するには、次のステップを実行します。

6. Azure アカウントで、クラウドディスカバリーおよび Cloud Provisioning and Governance の Microsoft Azure リソースへのアクセスに必要なレベルの権限を持つポリシーを設定します。
次の画像に示すページを使用して、ポリシー権限を作成します。これらの権限はこのアプリケーションに必要です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



コンフィグレーションコンプライアンス アプリケーションでは、そのアプリケーションに含まれるグループルールとアサインルールはデフォルトで非アクティブになっています。sn_vulc.admin を持つユーザーがこれらのルールをアクティブ化します。

7. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > グループルール.
8. [アサイン先グループ、テスト] ルール をクリックしてレコードを開き、 [アクティブ] フィールドを **true** に設定します。

   このルールは、監査中に作成されたテスト結果をグループ化します。false のテスト結果が返された特定のポリシーのすべてのテスト結果が 1 つのテスト結果グループにグループ化されます。

   デフォルトでは、テスト結果グループは CI サポートユーザーグループにアサインされます。デフォルトでは、このアサインルールは非アクティブです。
9. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > アドミニストレーション > アサインルール.
10. [CI サポートグループに割り当て] レコードをクリックして開き、 [アクティブ] チェックボックスをクリックしてアクティブ化します。

    このルールは、CI サポートグループのユーザーにテスト結果グループをアサインします。これらのテスト結果で作業するユーザーをこのグループにアサインします。

    これはデフォルトのアサインルールであり、組織内のプラクティスによっては、組織のクラウド構成の問題をアサインするのに役に立たない可能性があります。代わりに、要件に適したアサインルールを作成することもできます。クラウドアカウントのメタデータを使用するには、[テスト結果] テーブルから [検出されたアイテム] テーブルをドット連結して、アサインルールを定義します。

    注:

    コンフィグレーションコンプライアンスの使用の詳細については、servicenow.com/docs に関するコンフィグレーションコンプライアンスドキュメントを参照してください。

11. 脆弱性対応のパフォーマンスアナリティクス ダッシュボードで監査結果を表示するには、sn_vuln.admin ロールを持つユーザーがアプリケーションを有効にし、データコレクタをアクティブ化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

12. 次のように移動する。 パフォーマンスアナリティクス > データコレクター > ジョブ 日次コレクタージョブを見つけて、アクティブ化されていることを確認します。
統合のセットアップが完了しました。CSPM アプリケーションを使用して Azure 環境をスキャンする準備ができました。

ServiceNow CSPM アプリケーションを使用したクラウドアカウントのスキャン

このセクションでは、クラウドアカウントのセキュリティスキャンを設定して、ベンチマークフレームワークに対するリソースのコンプライアンスを確認する方法について説明します。サンプルポリシーを使用して、このプロセスを示します。

始める前に

必要な設定：この例では、まずスキャンレコードを作成します。Microsoft Azure サービスアカウントの情報を設定または確認する場合は、Microsoft Azure 向け CSPM Innovation Lab アプリケーションのインストールとアクティブ化 のセットアップステップを参照してください。

必要なロール：sn_vul.cspm_cloud_account_admin

手順

1. 次のように移動する。 **All** (すべて) > クラウドセキュリティポスチャ管理 **(CSPM)** > アドミニストレーション > クラウドアカウントスキャン をクリックして、CSPM アプリケーションでスキャン設定レコードを作成します。
[クラウドアカウントスキャン] ページが表示されます。
2. [新規] をクリックします。
3. フィールドに入力します。
   a. スキャン構成の一意の名前を入力します。
   b. 後でレコードを見つけることができるように、簡単な説明を入力します。
   c. [クラウドサービスアカウント] を選択し、必要なターゲットサービスアカウントを選択します。これらのレコードを Microsoft Azure アカウントに対して作成し、クラウドコンフィグレーションガバナンス に入力しました。
4. [バックグラウンドスキャン] チェックボックスをオンにします。
これにより、1 時間ごとにスキャンが実行されます。チェックボックスが選択されていない場合は、スキャンをオンデマンドで起動する必要があります。
5. 次のように移動する。 **All** (すべて) > コンフィグレーションコンプライアンス > テスト結果 > **All** (すべて).
ポリシー監査から作成されたテスト結果グループ (CTR#) のリストが表示されます。

   コンプライアンス違反のクラウドリソースのテスト結果レコードが作成されます。違反が修正されると、テスト結果レコードがクローズされます。

6. レコードを開くと、次のデータが表示されます。

   テストフィールド

   このフィールドには、監査に使用されるポリシーと コンフィグレーションコンプライアンス の監査テストレコード間の 1 対 1 のマッピングが表示されます。クリックしてテストレコードをプレビューして開き、引用、つまり信頼できるソースを表示します。この例では、信頼できるソースは Microsoft Azure (CIS Microsoft Azure Foundations Benchmark バージョン 1.4.0) で、引用されたセクション、つまりポリシーは 3.1.2 Ensure the "Minimum TLS version" is set to "Version 1.2" (Automated) です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このポリシーが属する各ポリシーグループが表示されます。ポリシーは複数のポリシーグループに含めることができます。また、監査によって生成されたテスト結果の数も表示されます。

[構成アイテム] フィールド

このデータは Microsoft Azure のリソースを参照しています。

検出されたアイテムフィールド

Now Platform で検出されたアイテムは Microsoft Azure リソースに関連付けられています。リージョン、クラウドアカウント、リソースタイプなど、Microsoft Azure リソースについてインポートされたすべてのクラウドメタデータは、検出されたアイテムレコードに保存されます。

テスト結果のグループタブ

デフォルトでは、コンフィグレーションコンプライアンス アプリケーションは、監査での誤検出に基づいてテスト結果をテスト結果グループにグループ化します。1 つのリソースに対してテスト結果ごとに 1 つのレコードのみが作成され、データのインポート後に更新されます。スキャンとスキャンの間に Microsoft Azure 環境のリソースの構成設定が変更されると、Now Platform インスタンスでレコードが更新されます。

7. インポートされたデータを確認するには、Microsoft Azure ユーザーアカウントに戻ります。

この例では、このアカウントのチェックで最小 TLS バージョンが 1.0 であることを示しています。このステータスは、クラウドからインポートされたリソースとリソースグループに関するセキュリティデータと一致します。設定を変更してリソースが準拠すると、変更は次のデータインポートに反映されます。次の例では、テスト結果レコードを閉じる前に、このリソースに対して最小 TLS バージョンに更新する必要があります。

脆弱性対応のパフォーマンスアナリティクスダッシュボードの **Azure CSPM** 監査データの表示

この統合には、脆弱性対応のパフォーマンスアナリティクス アプリケーションのダッシュボードが含まれます。

始める前に

必要なロール：pa_viewer

手順

1. ダッシュボードを表示するには、次に移動します: コンフィグレーションコンプライアンス > 概要.

ダッシュボードのデータは毎日収集されます。設定を変更するには、次に移動します: パフォーマンスアナリティクス > データコレクター > ジョブ.

> **注:**
> 他のサードパーティの脆弱性統合を実行している場合、すべての脆弱性データと監査結果データが一緒にダッシュボードに視覚的に表示されます。フィルターを設定して、CSPM データを除外することができます。

ダッシュボードには次の 3 つのタブがあります。

- 資産カテゴリ
- 修復
- 承認

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. データを表示するには、タブをクリックします。
3. データの可視化の下に、データに含まれる信頼できるソースが表示されます。

CSPM での Azure のカスタムポリシーの作成

カスタマイズされたコンプライアンス標準を実装するためのポリシーを作成します。

始める前に
必要なロール：sn_sec_cspm.cspm_security_admin

手順

1. 次のように移動する。 **All** (すべて) > クラウドセキュリティポスチャ管理 **(CSPM)** > 設定ポリシー.
2. **[New** (新規)] を選択します。
3. フォームのフィールドに入力します。

CSPM カスタムポリシー作成フォーム

フィールド	説明		
ポリシー名	一意のポリシー名。		
説明	ポリシーの詳細。		
リソースタイプ			
クラウドプロバイダ	ポリシーのクラウド提供プラットフォーム。		
リソースタイプ	クラウド環境でのリソースのタイプ。リソースタイプが存在しない場合は、AWS または Azure の規則を使用してリソースタイプを作成します。		
ポリシー条件			
タイプ			
条件	テスト結果を作成する条件。次のシナリオを考えてみましょう。		
	構成キーが存在しますか？	リソースタイプが存在しますか？	次のステップ
	はい	はい。リソースタイプとメタデータを取得するためのフローが存在します。サブフローの例：CSPM：Azure サブスクリプションリソースコレクター	ポリシーの条件を指定します。
	いいえ	はい	**a.** 構成キーを作成します。 **b.** リソースコレクターを作成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明		
			c. 構成コレクターを作成します。 d. ポリシーの条件を指定します。
重大度	ポリシーの重大度。		

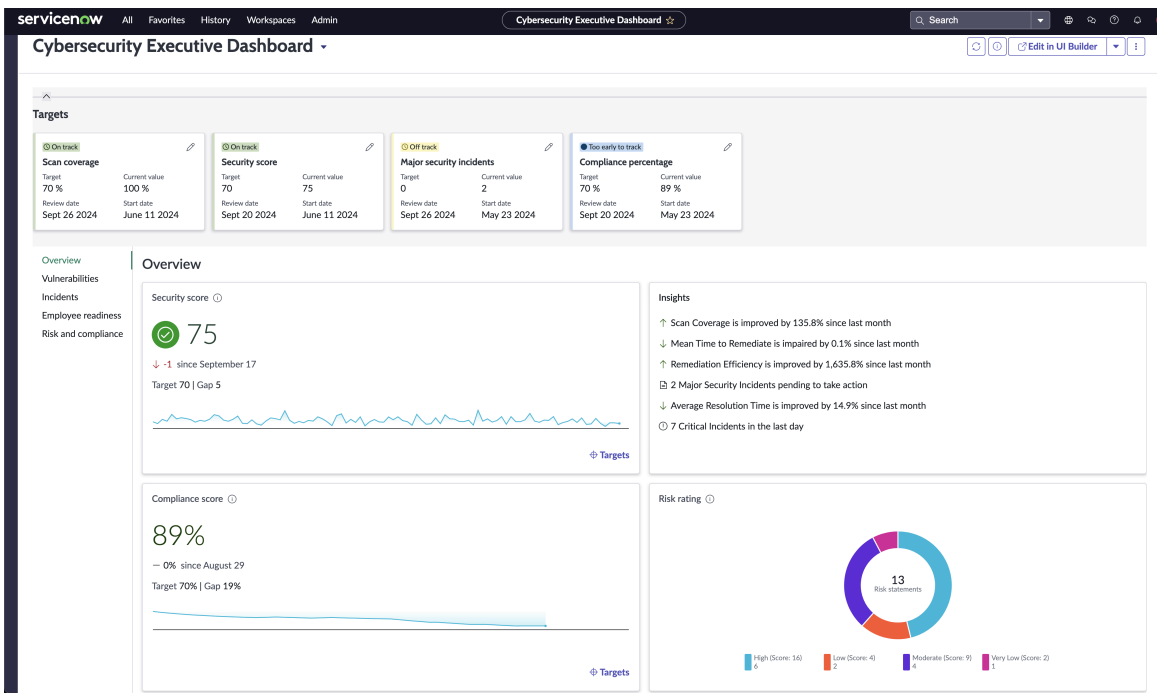
4. [送信] を選択してカスタムポリシーを作成します。

サイバーセキュリティエグゼクティブダッシュボード

サイバーセキュリティエグゼクティブダッシュボードは、最高情報セキュリティ責任者 (CISO) とサイバーセキュリティ担当役員が組織のセキュリティ体制とイニシアチブを可視化できるようにする包括的なソリューションです。ダッシュボードでは、ServiceNow の「Security Operations スイート」や「ガバナンス、リスク、コンプライアンス (GRC)」のさまざまな製品データが統合されます。

ダッシュボードには、次の機能があります。

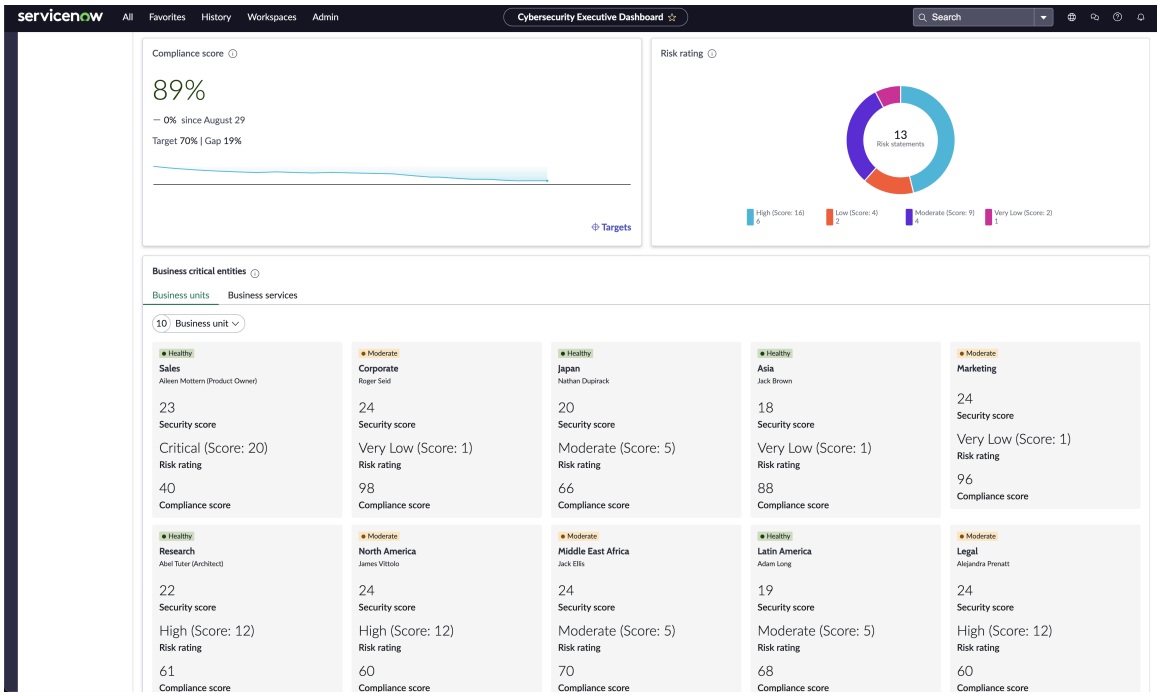
- 組織全体のセキュリティ体制のスコアリング
- 事業部門別のセキュリティ、リスク、コンプライアンススコア
- カスタマイズ可能な監視
- 組織のセキュリティランドスケープの統一されたビュー
- ベンチマーキング
- 分かりやすいインターフェイス
- KnowBe4 および Microsoft Defender for Office 365 からのフィッシングシミュレーションメトリクスのヴィジビリティ



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

これらの機能により、重要なセキュリティメトリクスにすばやくアクセスできるため、プロアクティブな意思決定が可能になります。したがって、このダッシュボードは全体的なセキュリティのレジリエンスと準備を強化するために不可欠なツールになります。



必要な **Now Platform** ロール

- CISO (sn_bod.ciso) でダッシュボードを表示および共有します。
- sn_bod.ciso_admin を使用して、ダッシュボードを表示、共有し、セキュリティ体制評価の重み付けを設定します。
- GRC CISO ユーザー (sn_grc_dashboards.grc_ciso_user) でリスクやコンプライアンスレポートを表示します。

サイバーセキュリティエグゼクティブダッシュボードへのアクセス

ダッシュボードを開くには、次の場所に移動します。 **All** (すべて) > サイバーセキュリティエグゼクティブダッシュボード > サイバーセキュリティエグゼクティブダッシュボード.

ユースケース

組織内のさまざまなユーザーがこのダッシュボードをどのように使用するかの例については、次のユースケースを参照してください。

ユーザー	ダッシュボードの使用法
最高情報セキュリティ責任者 (CISO)	CISO は、組織の脆弱性管理、インシデント管理、組織のセキュリティ体制、フィッシングシミュレーションメトリクスなどに関するインサイトを得ることができます。

データの可視化

注:

ウィジェットの詳細については、[情報] アイコン (ⓘ) を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ターゲット

メトリクス	タイプ	説明
ターゲット	パーセンテージ	メトリクスを対象に設定されたターゲットを表示します。 ターゲットのステータスは、色分けして表示されます。レビュー日が過去 30 日以内または未来日のターゲットがすべて表示されます。*sn_bod.show_targets_from* システムプロパティでターゲットを表示する日数を設定することができます。また、これらのターゲットを編集することもできます。 詳細については、「ターゲットを設定」を参照してください。

メトリクス	タイプ	説明
セキュリティスコア	単一スコア	脆弱性一致アイテム、セキュリティインシデント、重大なセキュリティインシデント、および構成ミスを考慮した、組織のセキュリティ体制の全体的なスコア。
インサイト	ハイライト	ダッシュボード全体のハイライト。
コンプライアンススコア	単一スコア	コントロールの合計数に対するコンプライアンス率に基づいて計算されたコンプライアンススコアを活用して、組織のコンプライアンス体制を提示します。
リスクスコア	単一スコア	リスク評価に基づいてリスクステートメントの数を提示します。これは、組織がさまざまなリスクの潜在的な影響と可能性を理解し、これらのリスクに優先順位を付けて管理するのに役立ちます。
事業上の重要エンティティ		
事業部門	単一スコア	脆弱性、構成ミス、オペレーショナルテクノロジー (OT) の脆弱性、セキュリティインシデント、重大なセキュリティインシデントに関連するリスクを考慮した、事業部門全体のセキュ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

メトリクス	タイプ	説明
		リティスコア。事業部門の健全性ラベルは、セキュリティスコアにのみ基づいています。 ラベルの割り当て状況を確認するには、リスクスコアの重み付け [sn_sec_cmn_risk_score_weight_list.do] テーブルに移動し、ビジネスエンティティを検索します。「正常」などのラベルは、事前定義された値の範囲に基づいて割り当てられます。たとえば、0～39 の範囲のセキュリティスコアは [正常] とラベル付けされます。ラベルの色分けは、「UnifiedCISOutils」スクリプトインクルードで指定されます。値の範囲だけでなくラベルの色も設定できます。 事業部門および事業部門長の名前の割り当て方法については、次の場所に移動します **All** (すべて) > 組織 > 事業部門. **注:** 有効化したプラグインに応じて、コンプライアンススコア、リスクスコア、セキュリティスコアにアクセスできます。コンプライアンスおよびリスクスコアを表示するには、GRC プラグインをアクティブ化する必要があります。セキュリティスコアを表示するには、Security Operations 関連のプラグインをアクティブ化する必要があります。詳細は、「アクティブ化するアプリケーション」セクションを参照してください。
ビジネスサービス	単一スコア	脆弱性、構成ミス、オペレーショナルテクノロジー (OT) の脆弱性、セキュリティインシデント、重大なセキュリティインシデントに関連するリスクを考慮した、ビジネスサービス全体のセキュリティスコア。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

メトリクス	タイプ	説明
		ラベルの割り当て状況を確認するには、リスクスコアの重み付け [sn_sec_cmn_risk_score_weight_list.do] テーブルに移動し、ビジネスエンティティを検索します。「正常」「中」「重大」などのラベルは、事前定義された値の範囲に基づいて割り当てられます。たとえば、0～39 の範囲のセキュリティスコアは [正常] とラベル付けされます。ラベルの色分けは、「UnifiedCISOutils」スクリプトインクルードで指定されます。値の範囲だけでなくラベルの色も設定できます。 事業部門と事業部門長の割り当て状況を確認するには、次の場所に移動します **All** (すべて) > 組織 > 事業部門. **注:** 有効化したプラグインに応じて、コンプライアンススコア、リスクスコア、セキュリティスコアにアクセスできます。コンプライアンスおよびリスクスコアを表示するには、GRC プラグインをアクティブ化する必要があります。セキュリティスコアを表示するには、Security Operations 関連のプラグインをアクティブ化する必要があります。詳細は、「アクティブ化するアプリケーション」セクションを参照してください。

自動翻訳

脆弱性

メトリクス	タイプ	説明
平均修復時間 (月次)	線	すべての資産 (ホスト、コンテナ、アプリケーション) の脆弱性と失敗したテスト結果のクローズにかかった 1 か月の平均時間。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

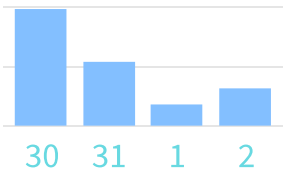
脆弱性 (続く)

メトリクス	タイプ	説明
		また、次のメトリクスも提供します。 • ターゲット：脆弱性を修復するために設定されたターゲット (日数)。 • ギャップ：脆弱性の修正に要したターゲット時間と実際の時間との差 (日数)。 • 業界ベンチマーク：同じ業界の同業他社のメトリクスの平均。 • グローバルベンチマーク：グローバル市場の同業他社からのメトリクスの平均 ベンチマークスコアの表示方法については、「ベンチマークスコアのオプトイン」を参照してください。
アクティブな脆弱性の平均経過時間 (月次)	単一スコア	3 つのタイプすべての脆弱性一致アイテムの月次平均経過時間。また、当月の経過時間と前月の比較も表示されます。 また、次のメトリクスも提供します。 • 業界ベンチマーク：同じ業界の同業他社のメトリクスの平均。 • グローバルベンチマーク：グローバル市場の同業他社からのメトリクスの平均 • ターゲット：脆弱性を修復するために設定されたターゲット (日数)。
修復効率 (月次)	単一スコア	月次のアクティブな脆弱性一致アイテムに対する月次のクローズ済み脆弱性一致アイテムのパーセンテージ。 また、次のメトリクスも提供します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

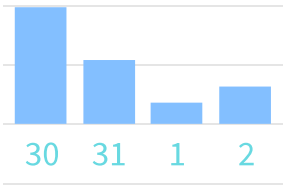
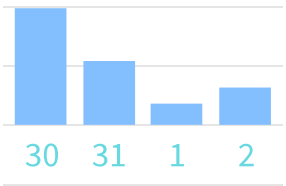
脆弱性 (続く)

メトリクス	タイプ	説明
		• 前のスコアからのパーセンテージの変更を表示します。 • ターゲット：脆弱性を修復するために設定されたターゲット (パーセンテージ)。 • ギャップ：ターゲットスコアと現在のスコアのギャップ。 • 業界ベンチマーク：同じ業界の同業他社のメトリクスの平均。 • グローバルベンチマーク：グローバル市場の同業他社からのメトリクスの平均
アサイン先グループ別のアクティブな脆弱性の平均経過時間	複数折れ線グラフ	各アサイン先グループのアクティブな脆弱性の平均経過時間。
リスク評価と経過時間別の脆弱性	ヒートマップ	リスク評価と経過時間別の、ホスト、コンテナ、およびアプリケーション全体のアクティブな脆弱性のブレークダウン。
アサイン先グループによる修復ターゲット遵守	垂直  バー	クローズされた脆弱性と構成ミスの総数に対する、修復ターゲット内でクローズされた脆弱性と構成ミスの数の比率。
スキャン範囲	パーセンテージ	CMDB のすべての資産のうち、過去 90 日間にスキャンされた資産の割合。
スキャンされた資産とスキャンされなかった資産	水平バー	過去 90 日間にスキャンされた資産のブレークダウンと CI クラス別の CMDB 内の総資産
スキャンされた資産	水平バー	脆弱性とコンフィグレーションコンプライアンスについて過去 90 日間にスキャンされた資産。
アクティブな「重大」および「高」の結果のトレンド	複数折れ線グラフ	リスク評価が「重大」「高」の脆弱性や構成ミスに関する日次傾向。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性 (続く)

メトリクス	タイプ	説明
資産カテゴリとリスク評価別の脆弱性	垂直  バー	資産カテゴリとリスク評価 (「重大」「高」「中」) 別のアクティブな脆弱性と構成ミスのブレークダウン。
理由とアサイン先グループによる保留結果	垂直  バー	保留理由とアサイン先グループによって保留されたアクティブな脆弱性と構成ミスのブレークダウン。
オペレーショナルテクノロジー (OT)		
アクティブな「重大」および「高」の脆弱性のトレンド	線グラフ	リスク評価が「重大」「高」のアクティブな OT 脆弱性に関する日次傾向。
平均修復時間 (月次)	単一スコア	OT 脆弱性がクローズするまでの平均時間。OT 脆弱性の合計数に対するクローズ済み OT 脆弱性の合計経過時間の比率。 また、次のメトリクスも提供します。 • 前のスコアからのパーセンテージの変更を表示します。 • ターゲット：脆弱性を修復するために設定されたターゲット (日数)。 • 業界ベンチマーク：同じ業界の同業他社のメトリクスの平均。 • グローバルベンチマーク：グローバル市場の同業他社からのメトリクスの平均 ベンチマークスコアの表示方法については、「ベンチマークスコアのオプトイン」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性 (続く)

メトリクス	タイプ	説明
リスク評価と経過時間別の脆弱性	ヒートマップ	アクティブな OT 脆弱性のブレークダウン (リスク評価別、経過時間別)。
アクティブな脆弱性の平均経過時間 (月次)	線グラフ	OT 脆弱性一致アイテムの月次平均経過時間。また、当月の経過時間と前月の比較も表示されます。
状況と経過時間別の脆弱性	ヒートマップ	アクティブな OT 脆弱性のブレークダウン (状況別、経過時間別)。

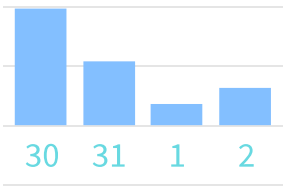
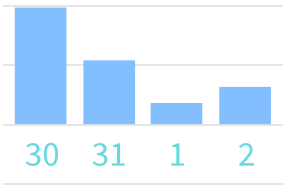
インシデント

メトリクス	タイプ	説明
重大なセキュリティインシデント	単一スコア	現在アクティブである重大なセキュリティインシデントの数
セキュリティインシデントの平均解決時間 (月次)	単一スコア	クローズ済みセキュリティインシデントの月次平均解決時間 (日数)。 また、次のメトリクスも提供します。 • 前のスコアからのパーセンテージの変更を表示します。 • ターゲット：セキュリティインシデントを修復するために設定されたターゲット (日数)。 • ギャップ：解決にかかった実際の日数と修復に設定されたターゲットとのギャップ。 • 業界ベンチマーク：同じ業界の同業他社のメトリクスの平均。 • グローバルベンチマーク：グローバル市場の同業他社からのメトリクスの平均
平均除去時間 (月次)	線グラフ	セキュリティインシデントを除去するための月次平均解決時間 (日数)。
平均識別時間 (月次)	単一スコア	セキュリティインシデントを識別するための月次平均解決時間 (日数)。

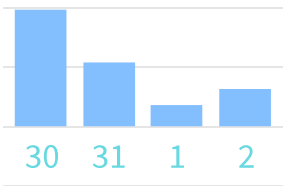
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インシデント (続く)

メトリクス	タイプ	説明
平均封じ込め時間 (月次)	単一スコア	セキュリティインシデントを封じ込めるための月次平均解決時間 (日数)。
優先度とカテゴリ別のアクティブなインシデント	ヒートマップ	優先度とカテゴリ別に分類された、アクティブなセキュリティインシデントの数。
クローズ済みインシデントとオープンインシデントの傾向	垂直  バー	クローズ済みインシデントとオープンインシデントのブレークダウン。
状況別のアクティブなインシデント	垂直  バー	ステータスに基づくアクティブなインシデントのブレークダウン。

従業員の準備

メトリクス	タイプ	説明
毎月のフィッシングシミュレーション概要	垂直  バー	フィッシングシミュレーションでオープン、クリック、レポートなどのアクションを実行したユーザーの総計と、過去 6 か月における各シミュレーションの合計ユーザーの総計。

リスクとコンプライアンス

リスクやコンプライアンスのウィジェットを表示するには、GRC プラグインをアクティブ化する必要があります。GRC プラグインについて、詳細は「アクティブ化するアプリケーション」セクションを参照してください。GRC ヴィジェットに関する詳細については、「GRC：メトリクス のリスクとコンプライアンスダッシュボード」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インジケーター

ホスト SLA - クローズ済み

このインジケーターは毎日計算されます。計算時、前日にクローズしたすべてのホスト脆弱性の合計経過時間が考慮されます。

コンテナ SLA - クローズ済み

このインジケーターは毎日計算されます。計算時、前日にクローズしたすべてのコンテナ脆弱性が考慮されます。

アプリケーション SLA - クローズ済み

このインジケーターは毎日計算されます。計算時、前日にクローズしたすべてのアプリケーション脆弱性の合計経過時間が考慮されます。

テスト結果 SLA - 合格

このインジケーターは毎日計算されます。計算時、前日に合格したすべてのテスト結果脆弱性が考慮されます。

ホスト SLA：クローズ済み数

このインジケーターは毎日計算されます。計算時、前日にクローズしたすべてのホスト脆弱性の数が考慮されます。

コンテナ SLA：クローズ済み数

このインジケーターは毎日計算されます。計算時、前日にクローズしたすべてのコンテナ脆弱性の数が考慮されます。

アプリケーション SLA：クローズ済み数

このインジケーターは毎日計算されます。計算時、前日にクローズしたすべてのアプリケーション脆弱性の数が考慮されます。

テスト結果 SLA - 合格数

このインジケーターは毎日測定されます。計算時、前日に最後に合格したすべてのテスト結果脆弱性の数が考慮されます。

スキャンされた資産

このインジケーターは毎日計算されます。すべての CMDB CI クラスにおいて、「sn_vul_analytics_scan_coverage_config」テーブルのスキャン済み CI の合計が考慮されます (過去 90 日間で最後にスキャンされた CI を含む)。

スキャンが可能な資産

このインジケーターは毎日計算されます。現存するすべての CMDB CI クラスにおいて、「sn_vul_analytics_scan_coverage_config」テーブルの合計 CI の総計が考慮されます。

脆弱性一致アイテム

このインジケーターは毎日計算されます。計算時にアクティブな脆弱性一致アイテムの数が考慮されます。

アプリケーション脆弱性一致アイテム

このインジケーターは毎日計算されます。計算時にアクティブなアプリケーション脆弱性一致アイテムの数が考慮されます。

コンテナ脆弱性一致アイテム

このインジケーターは毎日計算されます。計算時にアクティブなコンテナ脆弱性一致アイテムの数が考慮されます。

脆弱なアイテムの合計経過時間

このインジケーターは毎日計算されます。計算時にアクティブな脆弱性一致アイテムの合計経過時間が考慮されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション脆弱性一致アイテムの合計経過時間

このインジケーターは毎日計算されます。計算時にアクティブなアプリケーション脆弱性一致アイテムの合計経過時間が考慮されます。

オープンな脆弱性一致アイテム

このインジケーターは毎日計算されます。計算時にオープンな脆弱性一致アイテムが考慮されます。

オープンなコンテナ脆弱性一致アイテム

このインジケーターは毎日計算されます。計算時にオープンなコンテナ脆弱性一致アイテムが考慮されます。

オープンなアプリケーション脆弱性一致アイテム

このインジケーターは毎日計算されます。計算時にオープンなアプリケーション脆弱性一致アイテムが考慮されます。

アクティブなテスト結果

このインジケーターは毎日計算されます。計算時にオープンなテスト結果が考慮されます。

保留 VIT

このインジケーターは毎日計算されます。ホスト脆弱性一致アイテムとしてのインジケーターソースがあります。

保留 AVIT (Deferred AVITs)

このインジケーターは毎日計算されます。アプリケーション脆弱性一致アイテムとしてのインジケーターソースがあります。

保留 CVIT (Deferred CVITs)

このインジケーターは毎日計算されます。コンテナ脆弱性一致アイテムとしてのインジケーターソースがあります。

保留されたテスト結果

このインジケーターは毎日計算されます。保留ステータスのテスト結果が考慮されます。

オープンな構成の問題 - テスト結果

このインジケーターは毎日計算されます。統一脆弱性対応ダッシュボードのテスト結果としてのインジケーターソースがあります。

SI - 平均識別時間

このインジケーターは毎日計算されます。計算時に識別時間が定義されているセキュリティインシデントが考慮されます。

SI：平均期間

このインジケーターは毎日計算されます。計算時にインシデント状況期間が定義されているセキュリティインシデントが考慮されます。

オープンで重大なセキュリティインシデントの数

このインジケーターは毎日計算されます。計算時にオープンな重大セキュリティインシデントが考慮されます。

クローズ済みセキュリティインシデントの数

このインジケーターは毎日計算されます。計算時にクローズされたセキュリティインシデントが考慮されます。

クローズされたアプリケーション脆弱性一致アイテム

このインジケーターは毎日計算されます。計算時にクローズされたアプリケーション脆弱性一致アイテムが考慮されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

クローズされたコンテナ脆弱性一致アイテム

このインジケーターは毎日計算されます。計算時にクローズされたコンテナ脆弱性一致アイテムが考慮されます。

クローズされた脆弱なアイテム

このインジケーターは毎日計算されます。計算時にクローズされた脆弱性一致アイテムが考慮されます。

脆弱性一致アイテムの最大リスクスコアを取得

このインジケーターは毎日計算されます。計算時に脆弱性一致アイテムの最大リスクスコアが考慮されます。

コンテナ脆弱性一致アイテムの最大リスクスコアを取得

このインジケーターは毎日計算されます。計算時にコンテナ脆弱性一致アイテムの最大リスクスコアが考慮されます。

アプリケーション脆弱性一致アイテムの最大リスクスコアを取得

このインジケーターは毎日計算されます。計算時にアプリケーション脆弱性一致アイテムの最大リスクスコアが考慮されます。

VIT の合計リスクスコア

このインジケーターは毎日計算されます。計算時に脆弱性一致アイテムの合計リスクスコアが考慮されます。

AVI の合計リスクスコア

このインジケーターは毎日計算されます。計算時にアプリケーション脆弱性一致アイテムの合計リスクスコアが考慮されます。

CVI の合計リスクスコア

このインジケーターは毎日計算されます。計算時にコンテナ脆弱性一致アイテムの合計リスクスコアが考慮されます。

構成ミスの合計リスクスコア

このインジケーターは毎日計算されます。計算時にテスト結果のリスクスコアの合計が考慮されます。

SI インシデントの最大リスクスコアを取得

このインジケーターは毎日計算されます。計算時にセキュリティインシデントの最大リスクスコアが考慮されます。

構成ミステスト結果の最大リスクスコアを取得

このインジケーターは毎日計算されます。計算時にテスト結果の構成ミスの最大リスクスコアが考慮されます。

構成ミステスト結果の平均リスクスコアを取得

このインジケーターは毎日計算されます。計算時にテスト結果の構成ミスの平均リスクスコアが考慮されます。

オープンセキュリティインシデントの数

このインジケーターは毎日計算されます。計算時にオープンなセキュリティインシデントが考慮されます。

フィッシングの概要

このインジケーターは毎日計算されます。計算時にセキュリティシミュレーションメトリクスの数が考慮されます。

集計 MTTR (Aggregate MTTR)

脆弱性 (ホスト、コンテナ、およびアプリケーション) のクローズに要する平均時間と、テスト結果のクローズに要する時間 (日数) を計算します。[[ホスト SLA - クロー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ズ済み]] + [[アプリケーション SLA - クローズ済み]] + [[コンテナ SLA - クローズ済み]] + [[テスト結果 SLA - 合格]]) / ([[ホスト SLA - クローズ済み数]] + [[アプリケーション SLA - クローズ済み数]] + [[テスト結果 SLA - 合格数]] + [[コンテナ SLA - クローズ済み数]])

現在のスキャン範囲

同期間におけるスキャン済みアイテムの数とスキャン対象アイテムの合計数との比率を利用して、割合を計算します。var scannedItems =[[スキャン済み資産]];var scannableItems = [[スキャン可能資産]];var res;if (scannedItems == 0)res = 0;elseres = scannedItems / scannableItems * 100;if (res > 100)res = 100;res;

アクティブな脆弱性一致アイテムの平均経過時間

すべての有効な脆弱性一致アイテム (ホスト、コンテナ、およびアプリケーション) の平均経過時間 (日数) を計算します。([[脆弱性一致アイテムの合計経過時間]] + [[アプリケーション脆弱性一致アイテムの合計経過時間]] + [[コンテナ脆弱性一致アイテムの合計経過時間]]) / ([[脆弱性一致アイテム]] + [[アプリケーション脆弱性一致アイテム]] + [[コンテナ脆弱性一致アイテム]])

経過時間とリスク評価別のアクティブな VIT

経過時間とリスクアセスメントのレベルによって分類された、すべてのアクティブな脆弱性一致アイテム (ホスト、コンテナ、およびアプリケーション) の合計数を計算します。[[オープンな脆弱性一致アイテム]] + [[オープンなコンテナ脆弱性一致アイテム]] + [[オープンなアプリケーション脆弱性一致アイテム]]

保留された問題

ステータスが「保留」となっているすべての脆弱性一致アイテム (ホスト、コンテナ、アプリケーション、テスト結果) の合計数を計算します。[[保留 VIT]] + [[保留 AVIT]] + [[保留テスト結果]] + [[保留 CVIT]]

クローズ済みセキュリティインシデントの平均解決時間

セキュリティインシデントのクローズに要した平均時間 (日数) を計算します。([[クローズされたセキュリティインシデントの所要時間合計]] / [[クローズされたセキュリティインシデントの数]]) /24

セキュリティスコア

全体的なセキュリティ評価を毎日計算します。ロールアップされたリスクスコアに基づいて計算されます。var secPostureRating = 100 - [[セキュリティスコア]]; secPostureRating;

セキュリティスコア (事業部門)

脆弱性一致アイテム、構成ミス、セキュリティインシデント、および重大なセキュリティインシデントのロールアップリスクスコアに、セキュリティ体制ロールアップテーブルからフェッチされたそれぞれの重み付けが乗算された、最終的なロールアップリスクスコアを計算します。var numMajorIncidents = [[オープンな重大セキュリティインシデントの数]], majorSIRiskScore, rollUpRiskScore; if(numMajorIncidents > 0) majorSIRiskScore = 100; else majorSIRiskScore = 0; rollUpRiskScore = ([[脆弱性と構成ミスがロールアップされたリスクスコア]] * 20 + [[OT 脆弱性がロールアップされたリスクスコア]] * 20 + [[SI インシデントの最大リスクスコアを取得]] * 20 + majorSIRiskScore * 40)/100; rollUpRiskScore;

セキュリティスコア (ビジネスサービス)

脆弱性一致アイテム、構成ミス、セキュリティインシデント、重大セキュリティインシデントのロールアップリスクスコアに、セキュリティ体制ロールアップテーブルからフェッチされたそれぞれの重み付けが乗算された、最終的なロールアップリスクスコアを計算します。var numMajorIncidents = [[オープンな重大セキュリティインシデントの数 - サービス]], majorSIRiskScore, rollUpRiskScore; if(numMajorIncidents > 0) majorSIRiskScore = 100; else majorSIRiskScore = 0; rollUpRiskScore = ([[脆弱性と構成ミスがロールアップされたリスクスコア - サービス]] * 20 + [[OT 脆弱性が

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロールアップされたリスクスコア - サービス]] * 20 + [[SI インシデントの最大リスクスコアを取得 - サービス]] * 20 + majorSIRiskScore * 40)/100; rollUpRiskScore;

脆弱性がロールアップされたリスクスコア

最大リスクスコア、脆弱性一致アイテムの平均リスクスコア、および脆弱性一致アイテムの数にそれぞれの重み付けを乗じた、脆弱性がロールアップされたリスクスコアを計算します。var maxRiskScore = 100; var count = [[経過時間とリスク評価別のアクティブ VIT]]; var countRiskScore; if (0 == count) countRiskScore = 0; else if (count > 10000) countRiskScore = maxRiskScore; else if (count > 1000) countRiskScore = (maxRiskScore * 0.80); else if (count > 100) countRiskScore = (maxRiskScore * 0.60); else if (count > 10) countRiskScore = (maxRiskScore * 0.40); else countRiskScore = (maxRiskScore * 0.20); var vulRiskScore = ([[すべての脆弱性一致アイテムから最大スコアを取得]] * 0 + [[すべての脆弱性一致アイテムの平均リスクスコア]] * 100 + countRiskScore * 0)/100; vulRiskScore;

すべての脆弱性一致アイテムから最大スコアを取得

最大リスクスコア、脆弱性一致アイテムの平均リスクスコア、および脆弱性一致アイテムの数にそれぞれの重み付けを乗じた、脆弱性がロールアップされたリスクスコアを計算します。var maxScoreForVI = [[脆弱性一致アイテムの最大リスクスコアを取得]], maxScoreForCVI = [[コンテナ脆弱性一致アイテムの最大リスクスコアを取得]], maxScoreForAVI = [[アプリケーション脆弱性一致アイテムの最大リスクスコアを取得]], maxScore; if (maxScoreForVI >= maxScoreForCVI && maxScoreForVI >= maxScoreForAVI) maxScore = maxScoreForVI; else if (maxScoreForCVI >= maxScoreForVI && maxScoreForCVI >= maxScoreForAVI) maxScore = maxScoreForCVI; else maxScore = maxScoreForAVI; maxScore;

すべての脆弱性一致アイテムの平均リスクスコア

すべての脆弱性一致アイテム (ホスト、コンテナ、およびアプリケーション) から平均リスクスコアを計算します。var summedRiskScore = [[VIT の合計リスクスコア]] + [[AVI の合計リスクスコア]] + [[CVI の合計リスクスコア]], avgRiskScore; var totalVulCount = [[オープンな脆弱性一致アイテム]] + [[オープンなアプリケーション脆弱性一致アイテム]] + [[オープンなコンテナ脆弱性一致アイテム]]; if(summedRiskScore == 0) avgRiskScore = 0; else if(totalVulCount .=0) avgRiskScore = summedRiskScore / totalVulCount; avgRiskScore;

構成ミスがロールアップされたリスクスコア

失敗、エラー、または不明として分類されたテスト結果を使用して、構成ミスがロールアップされたリスクスコアを計算します。var maxRiskScore = 100; var count = [[オープンな構成の問題 - テスト結果]]; var countRiskScore; if (0 == count) countRiskScore = 0; else if (count > 10000) countRiskScore = maxRiskScore; else if (count > 1000) countRiskScore = (maxRiskScore * 0.80); else if (count > 100) countRiskScore = (maxRiskScore * 0.60); else if (count > 10) countRiskScore = (maxRiskScore * 0.40); else countRiskScore = (maxRiskScore * 0.20); var misRiskScore = ([[構成ミステスト結果の最大リスクスコアを取得]] * 0 + [[構成ミステスト結果の平均リスクスコアを取得]] * 100 + countRiskScore * 0)/100; misRiskScore;

平均除去時間

セキュリティインシデントの除去に要する平均時間 (日数) を計算します。[[SI - 平均期間 > セキュリティインシデント状況 = 除去]] / 1440

平均識別時間

セキュリティインシデントの識別に要した平均時間 (日数) を計算します。[[SI - 平均識別時間]] / 1440

平均封じ込め時間

セキュリティインシデントの封じ込めに要した平均時間 (日数) を計算します。[[SI - 平均期間 > セキュリティインシデント状況 = 封じ込め]] / 1440

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

修復ターゲット遵守

テスト結果、脆弱性一致アイテム、コンテナ脆弱性一致アイテム、およびアプリケーション脆弱性一致アイテムから、修復ターゲット遵守率の月次割合を計算します。ターゲットの遵守率は、設定されたターゲットを達成したアイテムの数によって決まります。([[テスト結果 SLA - 合格数 > 修復ステータス (統一) = ターゲット達成]] + [[コンテナ SLA - クローズ済み数 > 修復ステータス (統一) = ターゲット達成]] + [[アプリケーション SLA - クローズ済み数 > 修復ステータス (統一) = ターゲット達成]] + [[ホスト SLA - クローズ済み数 > 修復ステータス (統一) = ターゲット達成]]) / ([[テスト結果 SLA - 合格数]] + [[コンテナ SLA - クローズ済み数]] + [[アプリケーション SLA - クローズ済み数]] + [[ホスト SLA - クローズ済み数]]) * 100

月次修復効率（すべての脆弱性一致アイテム）

新たに特定された脆弱性一致アイテムに対する、クローズ済み脆弱性一致アイテム、コンテナ脆弱性一致アイテム、アプリケーション脆弱性一致アイテムの割合を月次で計算します。var closedItems = [[ホスト SLA - クローズ済み数]] + [[コンテナ SLA - クローズ済み数]] + [[アプリケーション SLA - クローズ済み数]] + [[テスト結果 SLA - 合格数]];

var newItems = [[昨日オープン / 再オープンされたホスト VIT]] + [[昨日オープン / 再オープンされたコンテナ VIT]] + [[昨日オープン / 再オープンされたアプリケーション VIT]] + [[昨日オープン / 再オープンされたテスト結果]];

var res = 0;if (closedItems == 0) res = 0;else if (newItems .=0)res = closedItems / newItems * 100;if (res > 1000) res = 1000; res;

昨日オープン/再オープンされたホスト VIT

このインジケーターは毎日計算されます。計算時、前日に最後にオープンされたホスト脆弱性一致アイテムが考慮されます。

昨日オープン/再オープンされたアプリケーション VIT

このインジケーターは毎日計算されます。計算時、前日に最後にオープンされたアプリケーション脆弱性一致アイテムが考慮されます。

昨日オープン/再オープンされたコンテナ VIT

このインジケーターは毎日計算されます。計算時、前日に最後にオープンされたコンテナ脆弱性一致アイテムが考慮されます。

昨日オープン/再オープンされたテスト結果

このインジケーターは毎日計算されます。計算時、前日に最後に確認されたテスト結果が考慮されます。

OT 脆弱性一致アイテム

このインジケーターは毎日計算されます。計算時に存在するアクティブな OT 脆弱性一致アイテムが考慮されます。

クローズ済み脆弱性一致の OT 合計期間

このインジケーターは毎日計算されます。計算日にクローズしたすべての OT 脆弱性の合計経過時間が考慮されます。

クローズ済み OT 脆弱性一致アイテム

このインジケーターは毎日計算されます。計算日にクローズした OT 脆弱性一致アイテムが考慮されます。

アクティブな OT 脆弱性一致アイテムの平均経過時間

OT 脆弱性一致アイテムの平均経過時間を計算します ([[OT 脆弱性一致アイテムの合計経過時間]] / [[OT 脆弱性一致アイテム]])

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ブレークダウン

- 事業部門
- ビジネスサービス
- リスク評価
- 年齢範囲
- アサイン先グループ (統一)
- 修復ターゲットステータス (クローズ済み)
- 資産クラス
- 資産カテゴリ
- リスク評価 (統一)
- 保留理由 (統一) (Deferred Reason (unified))
- セキュリティインシデントのステータス
- セキュリティインシデント優先度
- セキュリティインシデントカテゴリ
- フィッシングイベント
- 保留理由「クローズされていない」(統一)

アクティブ化するアプリケーション

ウィジェットにスコアを入力するには、次のアプリケーションをアクティブ化する必要があります。使用しているアプリケーションによっては、依存アプリケーションのアクティブ化が必要になります。

以下を使用している場合	アクティブ化
脆弱性対応	• 脆弱性対応のパフォーマンスアナリティクス • 脆弱性対応 Common • 脆弱性対応 • コンテナの脆弱性対応とコンフィグレーションコンプライアンス • コンフィグレーションコンプライアンス
オペレーショナルテクノロジー	オペレーショナルテクノロジーに対する脆弱性対応
フィッシング統合	• SecOps のセキュリティシミュレーションとトレーニングの統合 • SecOps 用 KnowBe4 統合 • SecOps 用 Microsoft Defender for Office365 統合

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

以下を使用している場合	アクティブ化
セキュリティインシデントレスポンス	• セキュリティインシデント対応のパフォーマンスアナリティクス • セキュリティインシデントレスポンス • 重大セキュリティインシデント管理
Governance, Risk, and Compliance (ガバナンス、リスク、コンプライアンス)	• GRC：共通ダッシュボード要素 • GRC：リスク管理ワークスペース • GRC：高度なリスク • GRC：コンプライアンス管理ワークスペース

データ収集スケジュール済みジョブ

新しいデータのスコアを自動的に収集するために、次のスケジュール済みジョブが実行されます。

スケジュール済みジョブ	頻度	説明
ベンチマークスコアをアップロードする	オンデマンド	インスタンスからスコアを収集し、セントラルインスタンスに投稿します。ベンチマークアルゴリズムは、業界最高のスコアを計算します。
ベンチマークスコアをダウンロードする	オンデマンド	ベンチマークスコアをダウンロードします。これは、ベンチマークスコア [sn_bm_client_score_list] テーブルにあります。

ベンチマークスコアのオプトイン

インスタンスを ServiceNow セントラルインスタンスに登録して、ベンチマークスコアを取得します。後者は、ベンチマークスコアを提供するために複数の業界の情報を維持します。

始める前に
必要なロール：admin

このタスクについて
ベンチマーキングの詳細については、「 Benchmarks overview 」を参照してください。

手順

1. インスタンスをセントラルインスタンスに登録するには、次の手順を実行します。

   a. 次のように移動する。 **All** (すべて) > システムプロパティ > すべてのプロパティ.

   b. *sn_bm_client.central_instance_url* システムプロパティを選択します。

   c. [値]フィールドに、ベンチマークセントラルインスタンスの URL を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> インスタンスがプロビジョニングされると、詳細がセントラルインスタンスに自動的にプッシュされます。

d. ウィジェットから [オプトイン] を選択し、セントラルインスタンスとの接続を検証して確立します。

2. スコアをセントラルインスタンスにアップロードするには、次の手順を実行します。

   a. 次のように移動する。 **All** (すべて) > システムスケジューラ > スケジュール済みジョブ

   b. *`Upload the benchmark scores`* スケジュール済みジョブを選択します。

   c. [更新] を選択します。
   スコアがセントラルインスタンスにアップロードされます。ただし、セントラルインスタンスによるスケジュール済みジョブは、ダッシュボードウィジェットのスコアを更新するために月に 1 回実行されます。

3. セントラルインスタンスからスコアをダウンロードするには、次の手順を実行します。

   a. 次のように移動する。 **All** (すべて) > システムスケジューラ > スケジュール済みジョブ

   b. *`Download the benchmark scores`* スケジュール済みジョブを選択します。

   c. [今すぐ実行] を選択します。
   スコアは、ダッシュボードウィジェットに反映されるベンチマークスコア [sn_bm_client_score_list] テーブルから入手できます。

ターゲットを設定

脆弱性、セキュリティインシデント、および構成ミスを修復するためのターゲットを日数で設定します。

始める前に

必要なロール：admin

手順

1. ウィジェットで [ターゲット] を選択するか、[KPI 詳細] ページで [ターゲット] アイコンを選択します。
2. [全員用] ボタンを選択します。
3. [新しい値] フィールドに、ターゲットを達成する日数を入力します。
4. ターゲット開始日を選択します。
5. ターゲットレビュー日を選択します。
6. [更新] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Security Operations のためのセキュリティシミュレーションとトレーニングの統合

サイバーセキュリティエグゼクティブダッシュボードにフィッシング統合を組み込むことで、重大なサイバーセキュリティの脅威に対する組織の防御を強化します。フィッシング統合は、KnowBe4 や Microsoft Defender for Office 365 などのサードパーティのフィッシングシミュレーションツールからのデータをシームレスに組み込むことで、サイバーセキュリティエグゼクティブダッシュボードを強化します。

次の統合により、サイバーセキュリティエグゼクティブダッシュボードの機能が向上し、組織のセキュリティ体制、従業員の準備、フィッシング攻撃に対する脆さに関する統一された視点が提供されます。

- KnowBe4 統合
- Microsoft Defender for Office 365 統合

Knowbe4 統合の構成

主要なサイバーセキュリティ意識向上トレーニングプラットフォームである KnowBe4 と統合することで、スタッフはフィッシング攻撃の脆弱性に関するインサイトをすぐに得ることができます。KnowBe4 の統合を通じて、サイバーセキュリティトレーニングプログラムの傾向と改善領域を特定し、全体的なフィッシングのレジリエンスを監視し、組織のセキュリティ対策を積極的に強化します。

始める前に

必要なロール：sn_sec_phish.admin および sn_sec_phish_kb4.kb4_admin

手順

1. 次のように移動する。 **All** (すべて) > **KnowBe4** 統合 > **KnowBe4** 構成.
2. **[New** (新規)] を選択します。
3. フォームで、次の詳細を入力します。

[Knowbe4 構成] フォーム

フィールド	説明
統合インスタンス	統合インスタンスの名前。[ルックアップ] アイコンを使用して統合インスタンスを選択します。
ベース URL	KnowBe4 と統合するための URL。
API キー	KnowBe4 アカウントから取得した API キー。
ページ	シミュレーションをフェッチするページ番号。
ページサイズ	含める必要があるシミュレーションの数。

   a. 利用可能な統合インスタンスがない場合は [新規] を選択します。

   b. フォームで、次の詳細を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

「統合インスタンス」フォーム

フィールド	説明
名前	統合インスタンスの名前。
アプリケーション	アプリケーションの名前 (SecOps 向け KnowBe4 統合)。
データ連携	デフォルトは KnowBe4 です。
有効	デフォルトで有効にされています (オン)。オフにすると、インスタンスはアクティブになりません。
説明	統合インスタンスの簡単な説明。

4. [**Submit** (送信)] を選択します。
5. 次のように移動する。 **All** (すべて) > セキュリティシミュレーションとトレーニング > 統合.
6. KnowBe4 統合を選択します。
7. [今すぐ実行] を選択して、KnowBe4 からデータを収集して実行します。

Microsoft Defender for Office 365 統合の構成

Microsoft Defender for Office 365 とのシームレスな統合により、サイバーセキュリティエグゼクティブダッシュボード内で、フィッシングシミュレーションメトリクスに関する貴重なインサイトを直接得ることができます。

始める前に

必要なロール：sn_sec_phish_msatk.ms_admin

このタスクについて

フィッシング攻撃のシミュレーションとテナントの設定の詳細については、以下を参照してください。

- 攻撃シミュレーショントレーニングによるフィッシング攻撃のシミュレーション
- 攻撃シミュレーショントレーニングの使用を開始する
- テナントの設定

手順

1. 次のように移動する。 **All** (すべて) > **Microsoft** 攻撃統合 > **Microsoft** 攻撃構成.
2. **[New** (新規)] を選択します。
3. フォームで、次の詳細を入力します。

[Microsoft 攻撃構成] フォーム

フィールド	説明
統合インスタンス	統合インスタンスの名前。[ルックアップ] アイコンを使用して統合インスタンスを選択します。
テナント ID	Microsoft Azure ポータルで作成されたアプリケーションのテナント ID。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
クライアント ID	Microsoft Azure ポータルで作成されたアプリケーションのクライアント ID。
クライアントシークレット	Microsoft Azure ポータルで作成されたアプリケーションのクライアントシークレット。
ブックマーク	シミュレーションをフェッチする必要がある日付。
トークン URL	Microsoft Simulations API にアクセスするためのトークンが作成されるベース URL。
すべてのシミュレーション URL	Microsoft Simulations API のベース URL。

a. 利用可能な統合インスタンスがない場合は [新規] を選択します。

b. フォームで、次の詳細を入力します。

「統合インスタンス」フォーム

フィールド	説明
名前	統合インスタンスの名前。
アプリケーション	アプリケーションの名前 (Microsoft Defender for Office 365)。
データ連携	サードパーティ統合の参照 (Microsoft 攻撃統合)。
有効	デフォルトで有効にされています (オン)。オフにすると、インスタンスはアクティブになりません。
説明	統合インスタンスの簡単な説明。

4. [**Submit** (送信)] を選択します。

5. 次のように移動する。 **All** (すべて) > セキュリティシミュレーションとトレーニング > 統合.

6. [Microsoft 攻撃統合] を選択します。

7. [今すぐ実行] を選択して、Microsoft からデータを収集して実行します。

GRC：メトリクス のリスクとコンプライアンスダッシュボード

[リスクとコンプライアンス (Risk and compliance)] ダッシュボードは、コンプライアンスとリスクのユーザーに、リスクとコンプライアンス情報の包括的な概要を単一のダッシュボードで提供し、重要な意思決定を支援するものです。

単一の統合されたサイバーセキュリティエグゼクティブダッシュボードから [リスクとコンプライアンス (Risk and compliance)] ダッシュボードに移動して、ガバナンス、リスク、コンプライアンスアプリケーションのリスクとコンプライアンスのメトリクスを表示できます。

ダッシュボードには、次の機能があります。

- コンプライアンスの概要
- リスクの概要

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- プライバシーの概要
- 事業継続性の概要
- サードパーティリスク
- 監査の概要

[リスクとコンプライアンス **(Risk and compliance)**] ダッシュボードにアクセスするための前提条件

> **重要:**
> [リスクとコンプライアンス (Risk and compliance)] ダッシュボードにアクセスできる Cybersecurity and risk functional プラグインをアクティブにするには、サイバーセキュリティエグゼクティブダッシュボードへのプライマリアクセス権が必要です。

サイバーセキュリティとリスク関連のデータを分離するために、新しい機能ドメインが導入されました。UI アクションの [アクティブ化 **(Activate)**] ボタンを選択して、Cybersecurity and risk プラグインをアクティブにできます。デフォルトでは、この機能ドメインは非アクティブです。

必要な **Now Platform** ロール

主要な GRC ユーザーロールは、[リスクとコンプライアンス (Risk and compliance)] ダッシュボードにレポートを表示できる sn_grc_dashboards.grc_ciso_user です。このロールには以下が含まれます。

- sn_compliance.reader
- sn_risk.reader

> **注:**
> ただし、[リスクとコンプライアンス (Risk and compliance)] ダッシュボードに移動できる [サイバーセキュリティエグゼクティブダッシュボード] にログインして表示および共有するには、sn_bod.ciso ロールが必要です。

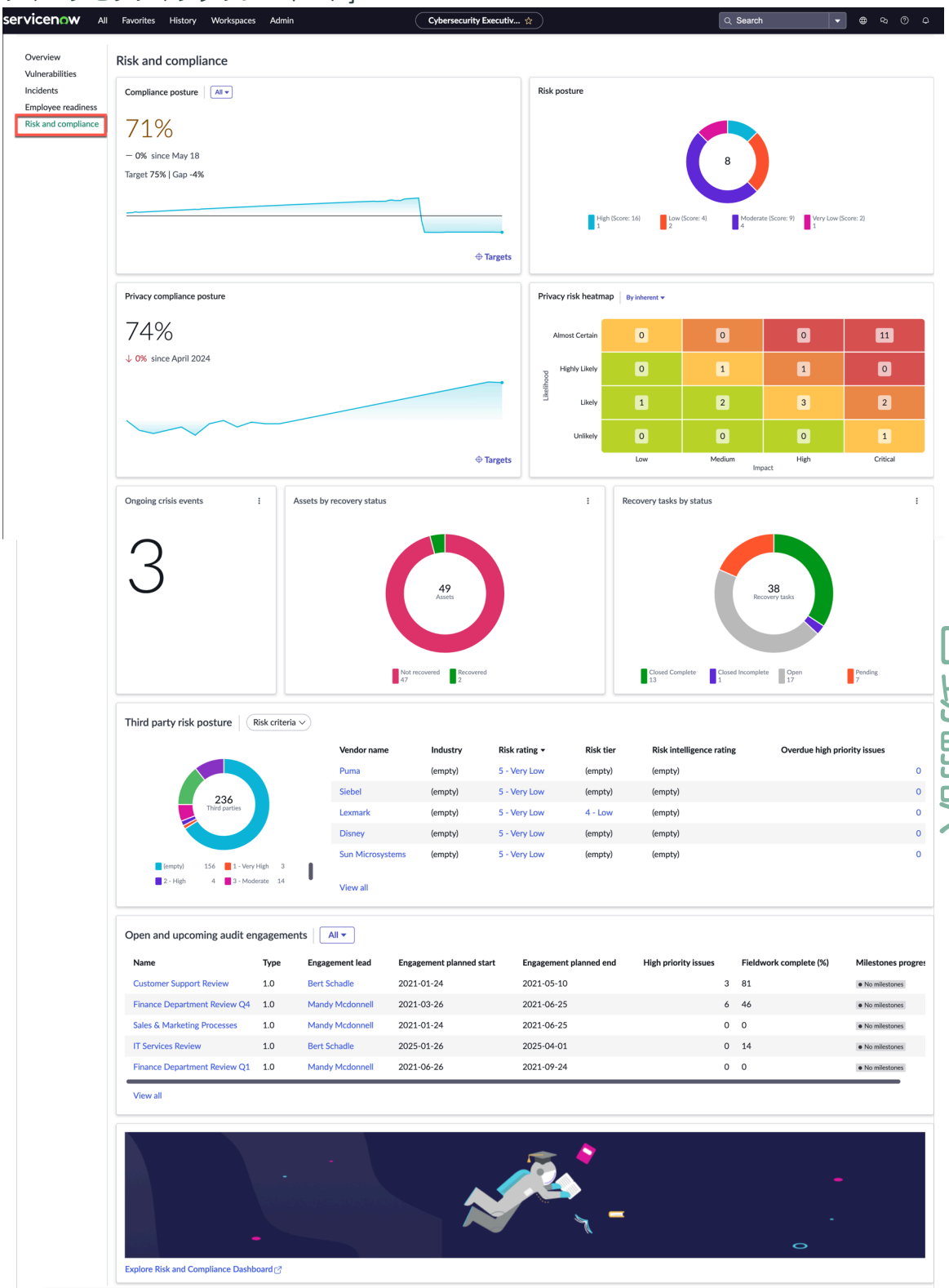
[リスクとコンプライアンス **(Risk and compliance)**] ダッシュボードにアクセスする

1. [リスクとコンプライアンス (Risk and compliance)] ダッシュボードにアクセスするには、次に移動します: **All** (すべて) > サイバーセキュリティエグゼクティブダッシュボード > サイバーセキュリティエグゼクティブダッシュボード.
2. ダッシュボードの左側にあるリストで、[リスクとコンプライアンス **(Risk and compliance)**] ラベルを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リスクおよびコンプライアンスのメトリクスのための統合された [サイバーセキュリティエグゼクティブダッシュボード]



3. データを可視化し、ユーザー向けに設計されたダッシュボードで利用可能なレポートとソリューションを表示するには、[リスクとコンプライアンスダッシュボードの探索 (Explore Risk and Compliance Dashboard label)] ラベルを選択します。

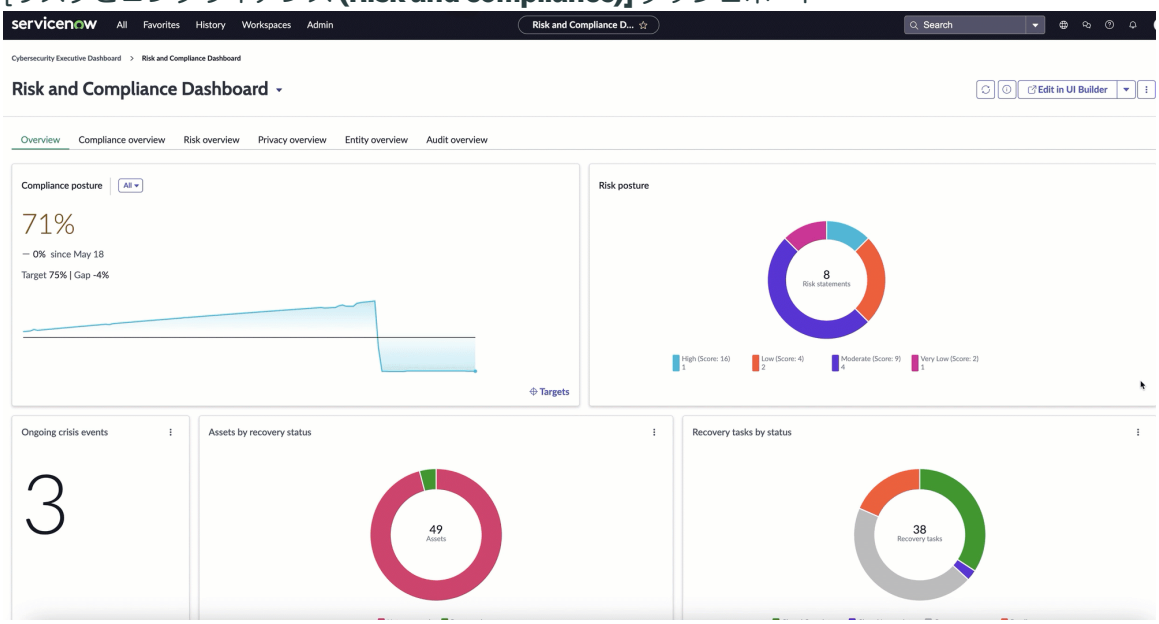
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リスクとコンプライアンスダッシュボードのレポートとソリューション

[リスクとコンプライアンス (Risk and compliance)] ダッシュボードは、最高情報セキュリティ責任者が組織のコンプライアンスとリスク体制を理解するための主要な GRC アプリケーションから利用可能なレポートの包括的な分析データを提供する統合ダッシュボードです。ダッシュボードは、ServiceNow GRC アプリケーションのスイート内のさまざまな製品のデータを統合します。

注:
すべてのレポートは、対応するワークスペースがインストールされている場合にのみ使用できます。

[リスクとコンプライアンス **(Risk and compliance)**] ダッシュボード



必要な **Now Platform** ロール

コンプライアンス関連レポートの場合

ユーザーには sn_grc_dashboards.grc_ciso_user ロールと sn_bod.ciso ロールが必要です。

リスク関連レポートの場合

ユーザーには sn_grc_dashboards.grc_ciso_user ロールと sn_bod.ciso ロールが必要です。

事業継続性管理関連レポートの場合

ユーザーには sn_bcm.viewer ロールと sn_bod.ciso ロールが必要です。

サードパーティリスク関連レポートの場合

ユーザーには sn_vdr_risk_asmt.vendor_assessment_reviewer ロールと sn_bod.ciso ロールが必要です。

プライバシー関連レポートの場合

ユーザーには sn_privacy.analyst ロールと sn_bod.ciso ロールが必要です。

監査関連レポートの場合

ユーザーには sn_audit_ws.auditor ロールと sn_bod.ciso ロールが必要です。

リスクとコンプライアンスダッシュボードにアクセスする

ダッシュボードを開くには、次の場所に移動します。 **All** (すべて) > サイバーセキュリティエグゼクティブダッシュボード > サイバーセキュリティエグゼクティブダッシュボード.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インジケーター

コンプライアンス体制

- コンプライアンスの割合 (%)：コンプライアンス体制を表す式インジケーター。
- すべてのコントロール：式インジケーターをサポートする自動インジケーター。
- 準拠コントロール：式インジケーターをサポートする自動インジケーター。

プライバシーコンプライアンスの体制

PA インジケーター：処理アクティビティのコンプライアンススコア (%)

ブレークダウン

機能ドメイン

レポート

注:
すべてのレポートは、対応するワークスペースがインストールされている場合にのみ使用できます。

[概要] タブ

タイトル	タイプ	ソーステーブル	説明
コンプライアンス体制	線グラフ	コントロール [sn_compliance_control]	コンプライアンスマネージャーに、データ分析に基づいてサイバーセキュリティとリスク、および IT リスクとコンプライアンスの体制を提供します。
リスク体制	ドーナツグラフ	ソーステーブルは次のとおりです。 • リスク [sn_risk_risk] • 詳細に集計されたリスク [sn_risk_advanced_risk_assessment_result] (高度なリスク アプリケーションがインストールされ、高度なリスクアセスメントが有効になっている場合)	リスク評価に基づいてリスク数を提供します。
進行中の危機イベント	単一スコア 。	復旧イベント [sn_recovery_event] (イベントタイプは実際)	承認もクローズもされていない進行中の危機イベントの合計数を表示します。
復旧ステータス別の資産	ドーナツグラフ	資産 [sn_recovery_event_asset]	復旧済みの資産と復旧していない資産を含む、復旧ステータス別

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[概要] タブ (続く)

タイトル	タイプ	ソーステーブル	説明
			にグループ化された進行中の危機イベントの資産の合計数を提供します。
ステータス別の復旧タスク (Recovery tasks by status)	ドーナツグラフ	復旧タスク [sn_recovery_event_task]	進行中の危機イベントのさまざまなステータスの復旧タスクのステータスを提供します。

[コンプライアンスの概要] タブ

タイトル	タイプ	ソーステーブル	説明
各種法令・基準等	ドーナツグラフ	各種法令・基準等 [sn_compliance_authority_document]	準拠および非準拠の各種法令・基準等のデータをチャートで提供します。このリストには、各種法令・基準等の詳細、個々のコンプライアンススコア (%)、各種法令・基準等の高優先度の問題と高リスクの例外の数、および準拠ケースの数が表示されます。
ポリシー	ドーナツグラフ	ポリシー [sn_compliance_policy]	チャート内の準拠ポリシーと非準拠ポリシーの数を示します。このリストには、ポリシーの詳細、個々のコンプライアンススコア (%)、各ポリシーで発生した高優先度の問題とリスク例外の数、および準拠ケースの数が表示されます。

[リスク概要] タブ

タイトル	タイプ	ソーステーブル	説明
リスク体制	ドーナツグラフ	ソーステーブルは次のとおりです。 • リスク [sn_risk_risk] • 詳細に集計されたリスク [sn_risk_advanced_risk_assessment_result]	リスク評価に基づいてリスク数を提供します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[リスク概要] タブ (続く)

タイトル	タイプ	ソーステーブル	説明
		(高度なリスク アプリケーションがインストールされ、高度なリスクアセスメントが有効になっている場合)	
リスク体制	リスト	GRC コンテンツステータス [sn_grc_content_reports]	全体的なリスクアセスメント結果を把握するために、各組織リスクのリスク評価を提供します。これらの評価は、組織がさまざまなリスクの潜在的な影響と可能性を理解し、これらのリスクに優先順位を付けて管理するのに役立ちます。リスク体制カードでは、各リスクに関する次の情報も強調表示されます。 • リスク選好度：定義されたリスク選好度値。 • 高優先度の問題：優先度が「高」と定義されている問題の数。 • 期限切れのリスク応答タスク：期限切れのリスク応答タスクの数。 • **KRI** 違反 **%**：事前定義されたしきい値または制限を超えた重要リスク指標 (KRI) の割合。
サードパーティのリスク体制	ドーナツグラフ	サードパーティリスク [sn_grc_dashboards_third_party_risk]	各サードパーティのリスク評価を提供します。リスク評価は、サードパーティまたはベンダーに対して実施されたすべてのアセスメントのスコアと評価を考慮した総合的なアセスメント評価になります。サードパーティのリスク体制カードでは、各サードパーティ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[リスク概要] タブ (続く)

タイトル	タイプ	ソーステーブル	説明
			またはベンダーの次の情報も強調表示されます。 • リスク基準：特定のタイプのサードパーティに適用されるリスクドメイン (他のプラットフォーム機能ではリスク領域とも呼ばれる) のグループです。 • リスク階層：固有リスクアセスメント (IRQ) の完了後に収集された応答に基づいて決定される値。 • リスクインテリジェンス評価：リスクインテリジェンスプロバイダーから収集されたすべてのスコアの集計。 • 期限切れのリスク応答タスク：期限切れのリスク応答タスクの数。

[プライバシーの概要] タブ

タイトル	タイプ	ソーステーブル	説明
プライバシーコンプライアンスの体制	線グラフ	PA インジケーター：処理アクティビティのコンプライアンススコア (%) [pa_indicators]	月別のコンプライアンス体制を提供し、すべての処理アクティビティの全体的なコンプライアンススコアを参照してプロットされます。
期限切れの高優先度の問題 (Overdue high priority issues)	単一スコア	問題 [sn_grc_issue]	すべての期限切れの高優先度のプライバシー関連の問題について焦点を絞った概要を提供し、コンプライアンスとデータ保護を確保するための重要なタスクの迅速な特定と解決を可能にします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[プライバシーの概要] タブ (続く)

タイトル	タイプ	ソーステーブル	説明
プライバシーリスクヒートマップ (Privacy risk heatmap)	ヒートマップ	リスクアセスメント方法論 [sn_risk_advanced_risk_assessment_methodology]	プライバシーリスクアセスメントデータをヒートマップフォームで提供します。プライバシーリスクアセスメントは、重要度スコアが高い場合に実施される詳細なアセスメントです。処理アクティビティに関連付けられている各リスクを評価し、処理アクティビティの集計リスクスコアを把握します。プライバシーリスクを評価した後、リスクヒートマップでプライバシーリスク体制を表示できます。

[エンティティの概要] タブ

タイトル	タイプ	ソーステーブル	説明
エンティティ	リスト	エンティティのコンプライアンスステータス [sn_compliance_entities_reports]	エンティティの全体的なリスク評価に寄与するエンティティに直接関連付けられたリスクのサマリーを提供します。このリストには、エンティティのコンプライアンススコア、およびエンティティに関連付けられた非準拠コントロールの結果として発生した高優先度の問題とリスク例外も表示されます。

監査の概要タブ

タイトル	タイプ	ソーステーブル	説明
オープンおよび今後の監査エンゲージメント	リスト	エンゲージメント [sn_audit_engagement]	オープンおよび今後の監査エンゲージメントのリストを提供します。このリストには、各種法令・基準等のエンゲージメントリード、各エンゲージメントの開始予定日と終了予定日、高優先度の

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

監査の概要タブ (続く)

タイトル	タイプ	ソーステーブル	説明
			問題、完了したフィールドワークの割合、および進行中のマイルストーンの詳細も記載されています。

フィルター

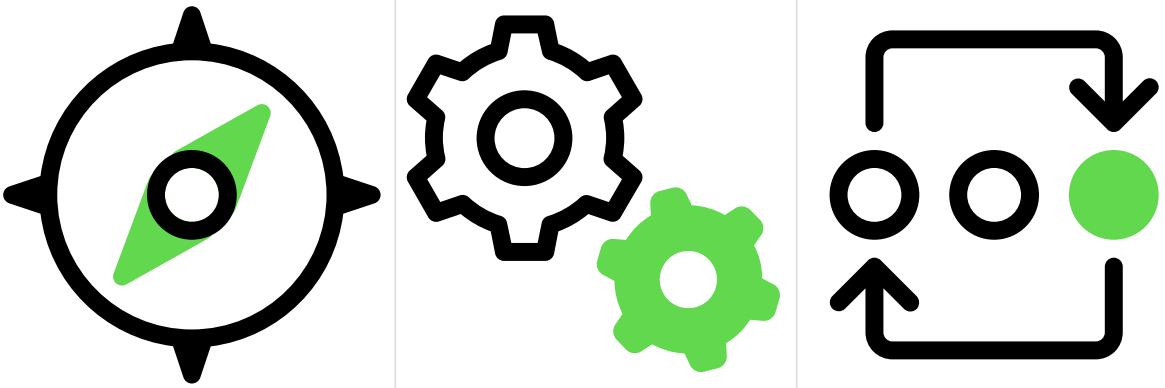
名前	タイプ	説明
リスク基準	レポート	選択したリスク基準に応じて、ドーナツグラフとリストには、それらのリスク領域にあるサードパーティまたはベンダーが表示されます。

脅威インテリジェンスセキュリティセンター

脅威インテリジェンスセキュリティセンター (TISC) プラットフォームは、脅威インテリジェンスの集計、管理、運用化のためのテクノロジーソリューションです。

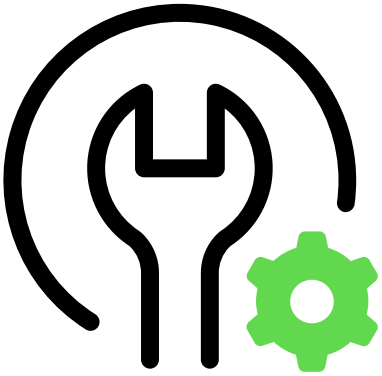
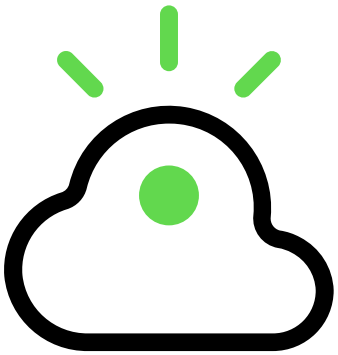
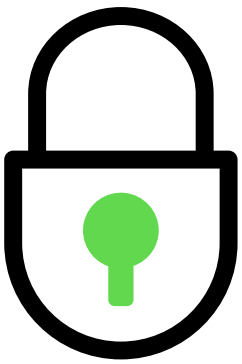
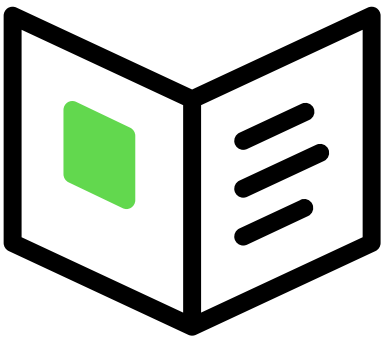
開始

タイルをクリックして開始します。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

管理	使用	レポートテンプレート
		
脅威インテリジェンスセキュリティセンターを管理およびカスタマイズします。	脅威インテリジェンスセキュリティセンターのライブラリとオブジェクトを管理します。	ケース管理レポートを管理およびカスタマイズします。
MITRE ATT&CK リポジトリ	**アーカイブ**	**Reference (参照)**
		
MITRE ATT&CK リポジトリデータを管理します。	データのアーカイブと破棄のルールを管理します。	脅威インテリジェンスセキュリティセンターに関する追加情報を取得します。

ストアでアプリを要求

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアに要求を送信する方法について確認してください。リリースされたすべてのアプリのリリースメモ情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

脅威インテリジェンスセキュリティセンター (sn_sec_tisc) をインストールすると、ServiceNow Store から依存アプリケーションがすべて自動的にインストールされます。

その他のリソース

ServiceNow コミュニティ で、セキュリティインシデントレスポンス のフォーラム にアクセスしてください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

トラブルシューティングとサポート

- 既知のエラーポータルで既知のエラー記事を検索する
- 連絡先 カスタマーサービス & サポート

脅威インテリジェンスセキュリティセンター の詳細

脅威インテリジェンスセキュリティセンター (TISC) を使用すると、脅威インテリジェンスチームと共同作業を行うことができます。さまざまな脅威インテリジェンスフィードを収集して処理する複数の機能と、必要な情報を分析、共同作業、アクション、共有できるワークスペースがあります。

脅威インテリジェンスセキュリティセンター アプリケーションの概要をご覧ください。

https://player.vimeo.com/video/1020328039?h=33e58d6e14&badge=0&autopause=0&player_id=0&app_id=58479

脅威インテリジェンスセキュリティセンターは、データ収集、データ処理 (重複排除、正規化、集計など)、脅威インテリジェンスの分析、脅威インテリジェンスの配布、および管理タスクを提供するワークスペースを管理する機能によって強化されています。

主要な機能

以下は脅威インテリジェンスセキュリティセンター (TISC) の主な機能になります。詳細については以降のセクションで説明します。

- 異なるソースからさまざまな形式でデータ収集。
- STIX、XML、JSON、OpenIOC などの多様なフィードでデータ集計。
- 誤検出の削除、インジケーターの信頼性 / スコアリング、インジケーターの検証、コンテキスト情報の追加など、強化された機能。
- 判断し難い脅威アセスメントにも対応できるカスタム脅威スコア算出。
- VR、SIR、資産、サービス、CMDB を包括する内部インテリジェンスの統合。
- ケース管理やタスク機能による脅威ハンティング。
- 脅威インテリジェンスのペルソナに合わせたユーザー固有のダッシュボード。
- 脅威インテリジェンスデータを把握できるグラフィカルな可視化ツール。
- 合理化された運用を実現する専用の脅威インテリジェンスアナリストワークスペース。
- 観測事象間の関係を自動的に確立できる相関ルール。
- システムには、アップロードファイルの観測事象をすべて自動的に識別して抽出する機能が搭載されています。
- 脅威インテリジェンスを強化するプレミアムフィードの統合。
- MITRE ATT&CK 情報を脅威インテリジェンスライブラリやケース管理のレコードに関連付けられるようになります。
- SIR との統合と、脅威インテリジェンスから脅威インテリジェンスセキュリティセンターへのデータ移行機能。

TISC の主要な用語

以下に定義する用語は、脅威インテリジェンスセキュリティセンター (TISC) 全体で使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

用語の定義

用語	定義
データ処理	脅威インテリジェンスプラットフォーム (TIP) は、さまざまなソースやパターンから脅威インテリジェンスデータを収集、集計、整理するテクノロジーソリューションです。脅威インテリジェンスは、攻撃者のターゲットや攻撃動作を把握するために収集、処理、分析されるデータです。
観測事象	観測事象は、コンピューターやネットワークの操作に関連するステートフルなプロパティ (ファイルの MD5 ハッシュやレジストリキーの値など) または測定可能なイベント (レジストリキーの作成やファイルの削除など) を表します。詳細については、「観測事象」を参照してください。
インジケーター	インジケーターにはパターンがあり、疑わしいまたは悪意のあるサイバーアクティビティの検出に使用されます。たとえば、インジケーターで一連の悪意のあるドメインを表し、STIX パターン言語でこれらのドメインを指定することができます。 インジケーター SDO には、単純なテキストによる説明、動作を検出するキルチェーンフェーズ、インジケーターが有効または有益となる期間、構造化された検出パターンのキャプチャに必要なパターンプロパティが含まれています。詳細については、「インジケーター」を参照してください。
オブジェクト	STIX ドメインオブジェクト (SDO) のセットを定義します。各 SDO は、サイバー脅威インテリジェンス (CTI) で一般的に表される固有の概念に対応しています。 SDO や STIX 関係オブジェクト (SRO) を構成要素として使用することで、広範かつ包括的なサイバー脅威インテリジェンスを個人で作成および共有できるようになります。詳細については、「TISC ライブラリリポジトリ」を参照してください。
関係性	関係性は、2 つの観測事象や 2 つの SDO、あるいは観測事象と SDO をリンクさせ、オブジェクトがどのように関連しているのかを説明するものとなります。 外部 STIX 関係オブジェクト (SRO) で表したり、深く根付いた関係を構成する識別子参照を格納する特定のプロパティで表したりする場合もあります。詳細については、「関係オブジェクト」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドメインセパレーションと脅威インテリジェンスセキュリティセンター

脅威インテリジェンスセキュリティセンター ではドメインセパレーションがサポートされています。ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル：標準

- ベーシックレベルのサポートのすべての側面が含まれています。
- アプリケーションプロパティは、必要に応じてドメイン対応です。
- ビジネスロジック：サービスプロバイダー (SP) によって顧客ごとにプロセスを作成または変更できます。ユースケースには、単一のインスタンスでの複数のサービスプロバイダー顧客によるアプリケーションの正しい使用が反映されています。
- インスタンスのオーナーは、特定のアプリケーションに期待される通りに、テナントごとに MVP ビジネスロジックとデータパラメーターを設定できる必要があります。

サンプルユースケース：アドミンは、レコードを他のテナントに対してはクローズしないが、1 つのテナントに対してクローズする場合、コメントを必須にすることができる必要があります。

サポートレベルの詳細については、「アプリケーションでのドメインセパレーションのサポート)」を参照してください。

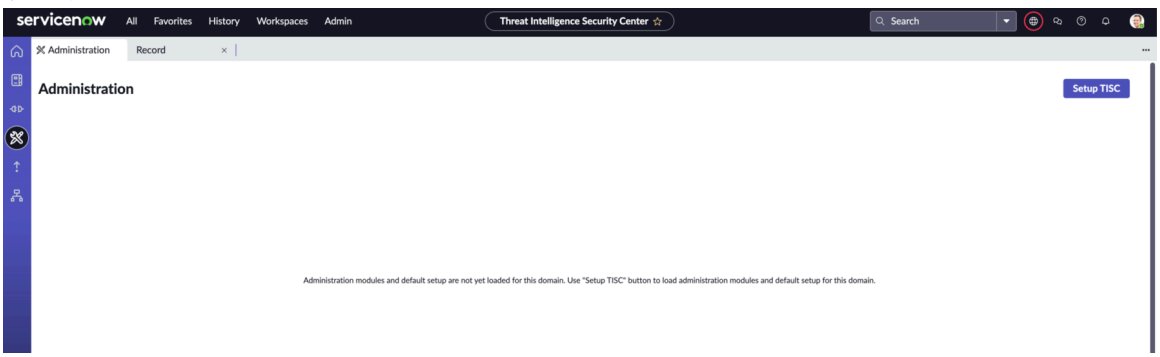
概要

ドメインセパレーションは 脅威インテリジェンスセキュリティセンター のすべての機能で有効になっています。

におけるドメインセパレーションの仕組み 脅威インテリジェンスセキュリティセンター

- ベースシステムでプロビジョニングされた構成関連のレコードはすべてグローバルドメインで提供されます。インスタンスがドメインセパレーションとなる場合は、TISC ワークスペースの管理モジュールに **[TISC** のセットアップ] ボタンが明確に表示されます。このボタンをクリックすると、ベースシステムでプロビジョニングされたグローバルドメイン構成が各ドメインにクローン作成されます。

ドメインセパレーション



注:
ユーザーは、ドメイン固有の構成レコードのみを有効化または変更する必要があり、グローバルドメイン内の構成レコードを有効化または変更することはできません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ベースシステムにはプラットフォームの通知ルール (sysevent_email_action) がいくつかプロビジョニングされています。これらの通知ルールは必要なドメインにクローン作成し、ドメイン固有の通知ルールのみを有効化する必要があります。

  注:
  ルール通知の詳細については、 システム通知 > 通知 をクリックし、名前 *sn_sec_tisc* で始まるテーブルで定義されているすべてのグローバルドメイン通知ルールをフィルタリングして、ベースシステムでプロビジョニングされた基本通知ルールをユーザーが識別する方法を理解します。

- 取り込まれる構成やデータはすべて各ドメイン固有となるため、あるドメインのユーザーが他のドメインのデータにアクセスすることはできません。
- [ドメインサポート – ドメイン拡張インストーラー] プラグインをインストールして、このアプリケーションでドメインセパレーション環境を構成します。
- すべてのベースシステムアプリケーションテーブルにドメイン列が追加されています。
- プラットフォームが提供する機能で、テナントドメインが独自のアプリケーションデータを管理します。
- インスタンスオーナーによってドメインセパレーションになるビジネスロジックやプロセスは、プラットフォームでも同じようにサポートされます。
- テナントドメインによって管理されるビジネスロジックやプロセスは、プラットフォームでも同じようにサポートされます。
- [管理] セクションから [セットアップ] ページにアクセスできます。[管理] セクションの下にあるリンクをクリックして、[ドメインセパレーション] ビューを表示します。
- TISC ホームダッシュボードで、パフォーマンスアナリティクス (PA) インジケーターを使用してウィジェットのドメインセパレーションをサポートするには、 KB 記事「KB1647990」 を参照して、詳細な手順を確認してください。

ドメインセパレーションテーブル

すべてのテーブルはドメインセパレーションされています。

ユースケース

このアプリケーションの機能はすべてドメインセパレーションとなります。

関連情報

サービスプロバイダーのドメインセパレーション

脅威インテリジェンスセキュリティセンターの設定

脅威インテリジェンスセキュリティセンターを使用する前に、ServiceNow Store からダウンロードする必要があります。

インストールされるロール

次の情報を確認し、スムーズな統合のためのすべてのタスクを完了したことを確認します。以下は、アプリケーションにアクセスして操作するために定義されたさまざまなユーザーペルソナのリストです。

- 脅威インテリジェンスアナリスト (sn_sec_tisc.analyst)
- 脅威インテリジェンスの管理 (sn_sec_tisc.admin)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

TISC ロールに適用されるエンタイトルメント

セットアップ	説明
必要な Now Platform および脅威インテリジェンスセキュリティセンターのロールをアサインして確認します。	期待される結果を構成および検証するには、次のロールが必要です。 • 管理者は、ServiceNow Store から TISC アプリケーションをインストールし、sn_sec_tisc.admin としてロールをアサインする必要があります。 • 次のタスクを実行するには、sn_sec_tisc.admin ロールが必要です。 ○ データを取り込むようにデータソースを構成します。詳細については、「脅威インテリジェンスフィード」を参照してください。 ○ TISC で観測事象データを拡張するために必要な統合を構成します。詳細については、「TISC 拡張統合」を参照してください。 ○ インポートアシスタントを使用して、データをインポートするためのデータインポート承認ロールを構成します。詳細については、「データインポートの使用」を参照してください。 ○ 観測事象の脅威スコアの自動計算に必要な基準を使用して、脅威スコア算出を構成します。詳細については、「脅威スコア算出の定義」を参照してください。 ○ 必要な分類と分類値を設定します。詳細については、「分類の作成」を参照してください。 ○ 組織に関連する MITRE ATT&CK リポジトリを構成します。詳細については、「MITRE-ATT&CK リポジトリ」を参照してください。 **注:** sn_sec_tisc.admin として、sn_sec_tisc.analyst ロールをアサインすることもできます。 • 次のタスクを実行するには、sn_sec_tisc.analyst ロールが必要です。 ○ 製品ホームページを使用して、システム内のデータの概要を表示します。詳細については、「脅威インテリジェンスセキュリティセンターホームページの表示」を参照してください。 ○ 脅威ライブラリページの [インテリジェンスのインポート (Import Intelligence)] ボタンを使用して、システムにデータをインポー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

TISC ロールに適用されるエンタイトルメント (続く)

セットアップ	説明
	トします。詳細については、「脅威インテリジェンスセキュリティセンター ライブラリ」を参照してください。 ○ ▪ [脅威ライブラリ (Threat Library)] ページで提供される検索を使用して、アプリケーションに存在するデータ全体を検索します。 ▪ 脅威ライブラリのさまざまなソースから取り込まれたデータを管理します。 ▪ 観測事象に対してさまざまな拡張アクションを実行します。 ▪ ケースを作成および管理します。詳細については、「脅威アナリストワークベンチを使用したケースを作成する」を参照してください。

依存プラグイン

プラグイン	説明
このアプリケーションのインストールには、次のアプリケーションが必要です。 • Security Case Management common workspace components [com.snc.escm.ws_commons]。 • 脅威インテリジェンス Support Common [com.snc.threat]。	この統合を構成する前に、統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。

脅威インテリジェンスセキュリティセンターホームページの表示

ランディングページである TISC ホームページを使用して、脅威インテリジェンス関連のデータを可視化します。

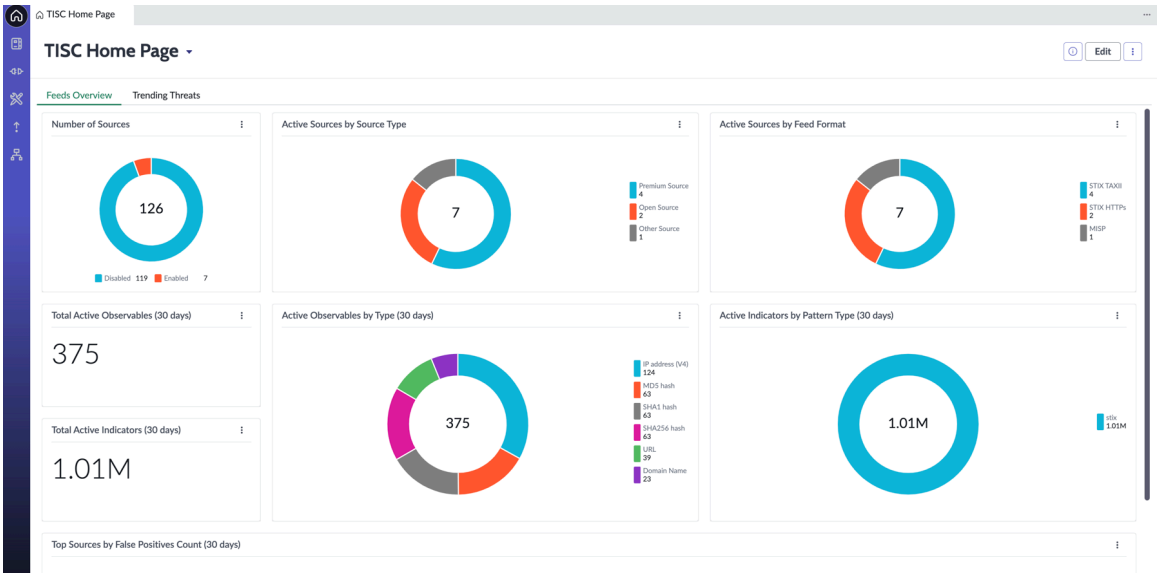
始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 **All** (すべて) > ワークスペース > 脅威インテリジェンスセキュリティセンター.
   TISC ホームページが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



2. さまざまなウィジェットデータを有する TISC ホームページを表示します。
ホームページビューは、[フィードの概要 **]** と [増加傾向の脅威] の 2 つの異なるタブで構成されています。ホームページのコンテンツは、観測事象、インジケーター、データフィードなどのさまざまなソースから提供されています。

a. フィードの概要：このタブには、データが取り込まれるさまざまなソースや、データの取り込み用に構成されたソースに関する概要が表示されます。

フィードの概要

ウィジェット名	説明	アクション
ソースの数	システム内のソースの数を「ドラフト」「有効」「無効」などのステータス別に表示します。	このウィジェットをクリックすると、リストページが開き、フィルタリングされたレコードが表示されます。
ソースタイプ別のアクティブなソース	アクティブなソースの分布をソースタイプ別に表示します。	このウィジェットをクリックすると、リストページが開き、フィルタリングされたレコードが表示されます。
フィード形式別のアクティブなソース	フィードタイプ別に有効なソースの数を表示します。	このウィジェットをクリックすると、リストページが開き、フィルタリングされたレコードが表示されます。
アクティブな観測事象の合計数 (30 日間)	過去 30 日間に作成されたインテリジェンスレコード数で、上位 10 個のソースを表示します。	このウィジェットをクリックすると、選択したフィルターのウィジェットの KPI 詳細ページが新しいタブで開きます。
タイプ別のアクティブな観測事象	過去 30 日間に作成された観測事象集計のうち、最も多い合計数を表示します。	このウィジェットをクリックすると、選択したフィルターのウィジェットの KPI 詳細ページが新しいタブで開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ウィジェット名	説明	アクション
パターンタイプ別のアクティブなインジケーター	過去 30 日間に作成されたパターンタイプ別にインジケーター集計の合計数を表示します。	このウィジェットをクリックすると、選択したフィルターのウィジェットの KPI 詳細ページが新しいタブで開きます。
アクティブなインジケーターの合計数 (30 日間)	過去 30 日間に作成されたインジケーター集計の合計数を表示します。	このウィジェットをクリックすると、選択したフィルターのウィジェットの KPI 詳細ページが新しいタブで開きます。
誤検出数の上位ソース (30 日間)	過去 30 日間に作成された誤検出の観測事象の合計数を表示します。	このウィジェットをクリックすると、リストページが開き、フィルタリングされたレコードが表示されます。

b. 増加傾向の脅威：このタブには、増加傾向の脅威の概要が表示されます。

フィードの概要

ウィジェット名	説明	アクション
最新のレポート (上位 10 個)	レポートとリンクのリストを表示します - 公開日別の上位 10 個。	このウィジェットをクリックすると、リストページが開き、フィルタリングされたレコードが表示されます。
最新の RSS フィード (上位 10 件)	RSS フィードとリンクのリストを表示します - 公開日順の上位 10 件。	このウィジェットをクリックすると、リストページが開き、フィルタリングされたレコードが表示されます。
脅威スコア範囲別のアクティブな観測事象 (30 日間)	過去 30 日間に作成された観測事象の数を脅威スコア範囲別に表示します。	このウィジェットをクリックすると、選択したフィルターのウィジェットの KPI 詳細ページが新しいタブで開きます。
評判別のアクティブな観測事象 (30 日間)	過去 30 日間に作成された観測事象の数を評判別に表示します。	このウィジェットをクリックすると、選択したフィルターのウィジェットの KPI 詳細ページが新しいタブで開きます。
上位タグ (30 日間)	使用頻度に基づいて、過去 30 日間に作成されたレコードの上位タグを表示します。	このウィジェットをクリックすると、選択したフィルターのウィジェットの KPI 詳細ページが新しいタブで開きます。
最も狙われたセクター (30 日間)	過去 30 日間に作成されたとされるアクティビティ別の上位 10 セクターを表示します。	このウィジェットをクリックすると、選択したフィルターのウィジェットの KPI 詳細ページが新しいタブで開きます。

脅威インテリジェンスセキュリティセンターの統合

このセクションを使用して、脅威インテリジェンスセキュリティセンター統合を理解します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[統合] セクションには、次のサブモジュールが含まれています。

統合

モジュール名	説明
カタログ	利用可能なすべての脅威インテリジェンスフィードと拡張統合が、タイル/カードとしてここに表示されます。ユーザーは、このセクションから新しいフィードまたは統合を作成することはできません。
脅威フィード	このセクションには脅威インテリジェンスフィードに関連する詳細のみが含まれており、ユーザーはこのセクションから新しい脅威インテリジェンスフィードを構成できます。
拡張統合	このセクションには、拡張統合に関連する詳細のみが含まれており、ユーザーはこのセクションから利用可能な拡張統合を構成できます。 **注:** [拡張統合] セクションは、少なくとも 1 つの拡張統合プラグインがインストールされている場合にのみ表示されます。

脅威インテリジェンスセキュリティセンター カタログ

脅威インテリジェンスセキュリティセンター カタログは、アプリケーションで利用可能な脅威インテリジェンスフィードや拡張統合のキュレーション済みリストとなります。必要な情報を追加して有効化し、フィードをスケジュール設定すると、設定された頻度で脅威インテリジェンスデータを自動的に取り込めるようになります。

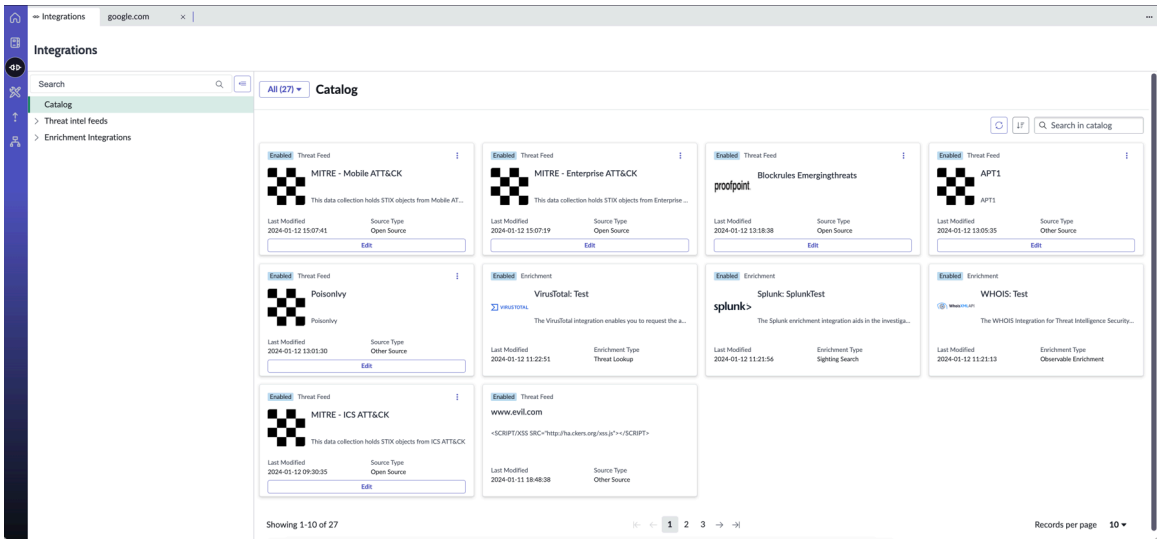
「sn_sec_tisc.admin」であれば、既存のソース構成を検索したり編集したりすることや、カタログの構成を有効化、無効化、削除することもできます。新規のデータソースはカタログに追加され、カタログには新しい構成カードとして表示されます。

必要なロール：

- sn_sec_tisc.admin (作成/更新)
- sn_sec_tisc.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
カタログのカードを見分けるには、 カード [脅威フィード/拡張] の上部にあるラベルを確認します。

[カタログ] ビューのアクション

[カタログ] ビューでは、次のアクションを実行できます。

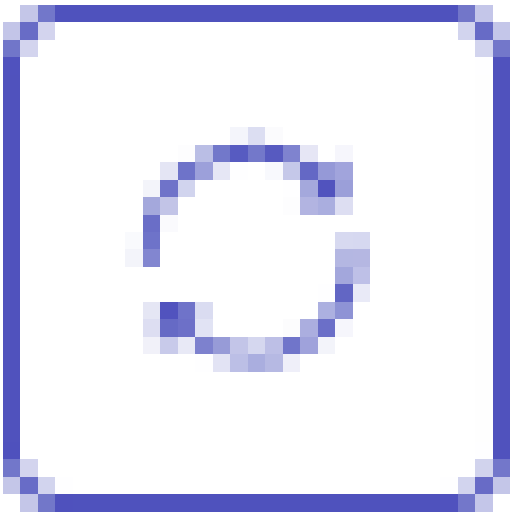
[カタログ] ビューのアクション

アクション	説明
すべて	現在のステータスに応じて、ドロップダウンメニューでフィードや統合をフィルタリングします。フィルタリングは次のステータスに基づいて実行することができます。 • すべて：ページ上のフィードや統合がすべて表示されます。これはデフォルトのオプションです。 • 有効：有効ステータスのフィードや統合がすべて表示されます。 • 無効：無効ステータスのフィードや統合がすべて表示されます。 • ドラフト：ドラフトステータスのフィードや統合がすべて表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[カタログ] ビューのアクション (続く)

アクション	説明
	このアクションで、カタログが更新されます。
	このアクションで、次の内容に基づいてフィードや統合がすべてソートされます。 • 最終変更日 (最新) • 最終変更日 (古い順) • 名前 **(A** から **Z)** • 名前 **(Z** から **A)**
カタログで検索	このアクションで、カタログ内の名前や説明に基づいてフィードや統合を検索します。

脅威インテリジェンスフィード

脅威インテリジェンスフィードを使用して脅威インテリジェンスフィードのデータソースを追加、編集、削除します。

データソースのフィードは、[統合] セクションの [脅威インテリジェンスカタログ (Threat Intel Catalog)] で利用できます。

脅威インテリジェンスフィードのカタログでは、利用可能なフィードのデータソースがタイル形式で表示されるようになっています。また、ソース構成の詳細情報をフィルタリング、検索、操作したり、さまざまなアクションを実行したりすることができます。

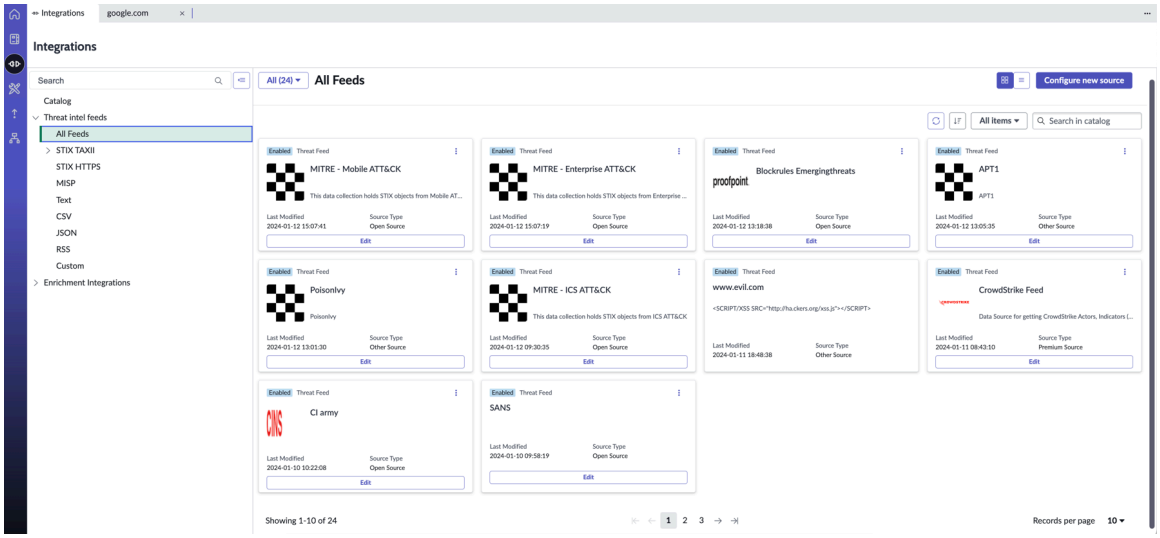
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

すべてのフィード

ベースシステムには各フィードに対する一連のカードがあり、これらを有効化して使用することができます。

フィードを表示するには、 ワークスペース > 脅威インテリジェンスセキュリティセンター > 統合 > 脅威インテルフィード > すべてのフィード.



[すべてのフィード] ビューのアクション

[すべてのフィード] セクションでは、次のアクションを実行できます。

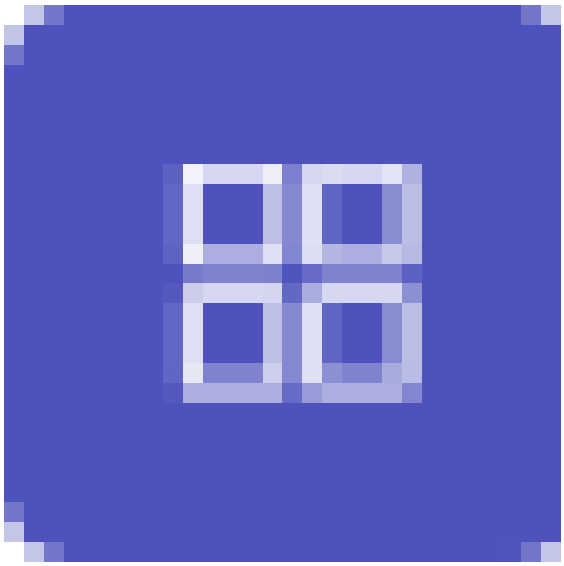
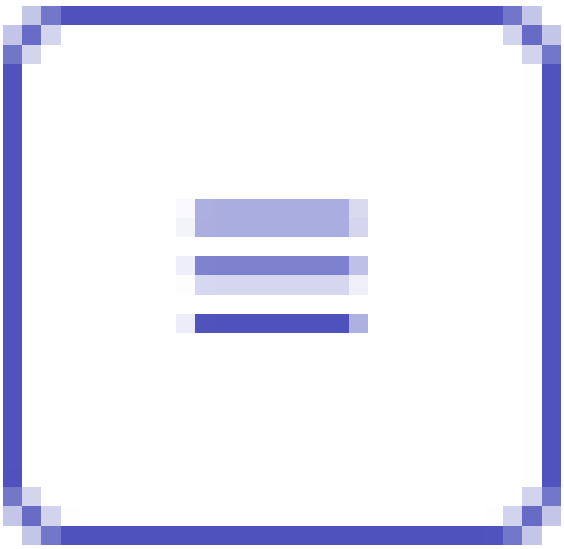
[すべての統合 **(All Integrations)**] ビューのアクション

アクション	説明
すべて	現在のステータスに応じて、このドロップダウンメニューでフィードをフィルタリングします。フィルタリングは次のステータスに基づいて実行することができます。 • すべて：ページ上のすべてのフィードを表示。これはデフォルトのオプションです。 • 有効：有効ステータスのフィードをすべて表示。 • 無効：無効ステータスのフィードをすべて表示。 • ドラフト：ドラフトステータスのフィードをすべて表示。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

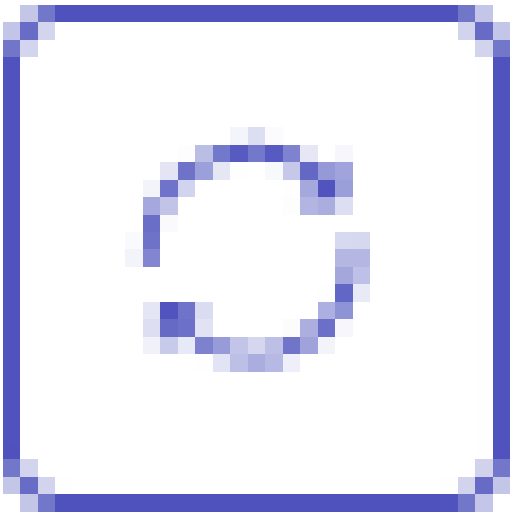
[すべての統合 **(All Integrations)**] ビューのアクション (続く)

アクション	説明
	このアクションで、すべてのフィードがカード形式で表示されます。
	このアクションで、すべてのフィードがリストビュー形式で表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[すべての統合 **(All Integrations)**] ビューのアクション (続く)

アクション	説明
	このアクションで、ページが更新されます。
	このアクションで、統合が次の内容に基づいてすべてソートされます。 • 最終変更日 (最新) • 最終変更日 (古い順) • 名前 **(A** から **Z)** • 名前 **(Z** ～ **A)**
すべてのアイテム	このアクションで、脅威インテリジェンスフィードをソースタイプやフィードタイプでフィルタリングしたりリスト表示したりすることができます。 ソースタイプ： • オープンソース • その他のソース • プレミアムソース フィードタイプ： • CSV • カスタムフィード

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

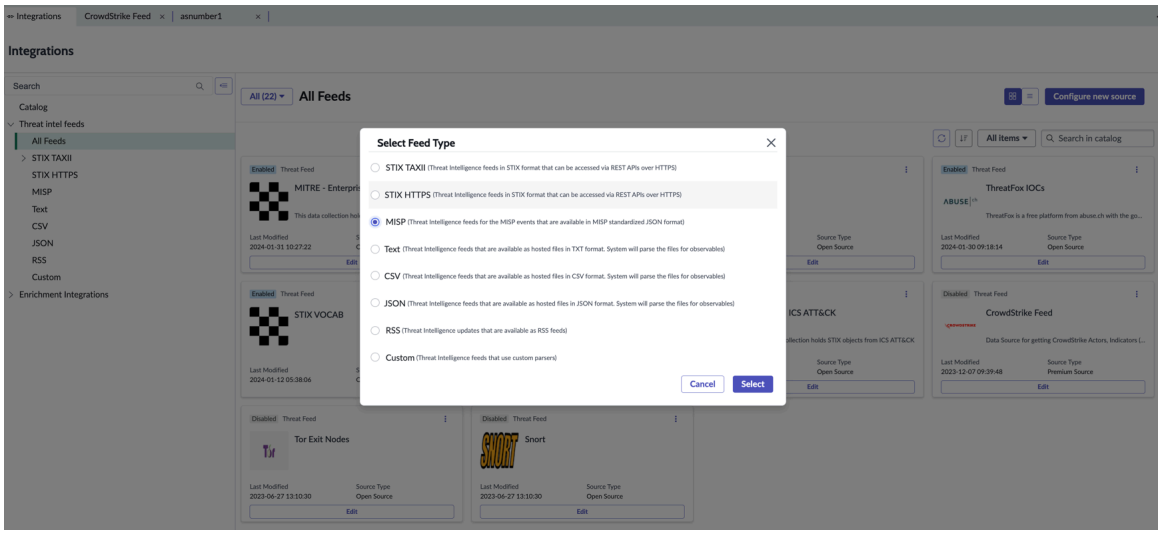
[すべての統合 **(All Integrations)**] ビューのアクション (続く)

アクション	説明
	• JSON • MISP • RSS • STIX HTTPS • テキスト
カタログで検索	このアクションで、カタログ内の名前や説明に基づいてフィードを検索します。

新規で脅威インテリジェンスフィードのデータソースを構成

新規で脅威インテリジェンスフィードのデータソースを構成するには、次の手順に従います。

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. 統合アイコンをクリックします。
3. 選択 脅威インテルフィード > すべてのフィード.
4. [新しいデータソースを構成 **(Configure new source)**] をクリックします。さまざまなフィードタイプが表示されます。



5. 各フィードタイプを選択します。MISP など。
6. [選択] をクリックします。
7. フォームのフィールドに入力します。

新しいデータソースを作成

フィールド	説明
名前	フィードの名前を入力します。
説明	フィードの説明。
フィードタイプ	フィードのタイプ。MISP など。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	デフォルトでは、この値はカタログで選択したフィードのタイプに基づいて表示されます。
ロゴ	ソースフィードのロゴを添付します。
業種	フィードのデータソースが適用される産業カテゴリ (航空宇宙、農業など) を選択します。
ソースタイプ	利用可能なソースタイプのリストからソースタイプを選択します。利用可能なソースのリストは次のとおりです。 ○ 政府 ○ ISAC ○ オープンソース ○ プレミアムソース ○ その他のソース

必要に応じて、[構成] セクションのフィールドに入力します。

構成

フィールド	説明
有効期限 (日数) (Expiry Period (days))	フィードの有効期間を日単位で入力します。例：「180 日」など。 **注:** ソースから取り込まれたデータはすべて、取り込みから 180 日後に有効期限が切れます。
REST メッセージを使用	Now Platform の REST メッセージ / REST メソッド機能を使用する必要がある場合は、**[REST** メッセージを使用] チェックボックスをオンにします。 このチェックボックスがオンになっていない場合、アプリケーションは **REST** エンドポイント **URL** のエンドポイントを使用してフィードからデータを取得します。詳細については、Now Platform ドキュメントの「送信 REST Web サービス」を参照してください。 **注:** REST メッセージを選択する場合は、[REST メッセージ] フィールドと [REST メソッド] フィールドが必須です。
REST メッセージ	インスタンスで既に構成されている REST メッセージレコードのリストから、REST メッセージレコードを選択します。詳細については、Now Platform ドキュメントの「送信

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	REST Web サービス」を参照してください。 注: 特定のヘッダーを表示する必要がある場合はこの値を選択して、[REST メッセージ] オプションで REST 関連のレコードを定義します。
REST メソッド	選択した REST メッセージに対して構成されている利用可能な REST メソッドのリストから REST メソッドを選択します。詳細については、Now Platform ドキュメントの「送信 REST Web サービス」を参照してください。
信頼性	この特定のフィードから取り込まれた適用可能なすべてのレコードに対する信頼度を設定します。 注: このソースの信頼度を 0 ～ 100 の範囲で設定します。
REST エンドポイント URL	データソースによってデータがホストされている REST エンドポイント URL を入力します。
認証が必要	新規のデータソースに認証が必要な場合は、このチェックボックスをオンにします。 注: 「REST エンドポイント URL がデータの取得で使用されている場合にのみ適用」というステートメントを追加します。
認証タイプ	ソースフィードの認証タイプ。ユーザーにおいてベースシステム内で構成およびプロビジョニングされる認証タイプは次のとおりです。 ○ API ID / API キー ○ API ID / API シークレット ○ API キー ○ API キー / API シークレット ○ API ユーザー名 / API パスワード / API キー ○ ベーシック認証

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: カスタムソースフィードタイプにおけるベースシステムの認証タイプは、クライアント ID とクライアントシークレットです。
要求とともに渡されるヘッダー	要求とともに渡されるヘッダーは、要求ヘッダーマッピングで指定できます。ヘッダーはキーと値のペアで指定され、コロン (:) で区切る必要があります。ヘッダーの各キー値のペアは、新しい行で指定する必要があります。認証パラメーターをヘッダー値として指定する場合、必要な認証ラベルを「${」と「}$」で囲みます。例：「x-api-key:${API キー}$」など。
詳細	カスタム統合スクリプトやレポートプロセッサスクリプトを定義する場合、このチェックボックスをオンにします。 注: チェックボックスをオンにすると、[統合スクリプト] フィールドと [レポートプロセッサ] フィールドが表示され、カスタムスクリプトを選択できます。
統合スクリプト	統合スクリプトは、フィードで構成されている認証パラメーターやヘッダーを使用して REST エンドポイント URL への呼び出しを起動し、特定のフィードから利用可能なデータを取得します。 以下は、ベースシステム内のカスタムスクリプトインクルードです。これらが、統合スクリプト用にアプリケーション内でプロビジョニングされます。 ○ FeedDatasourceIntegrationBase ○ MITRESourceIntegration ○ RSSFeedDatasourceIntegration ○ SimpleFeedDatasourceIntegration ○ SimpleMISPFeedDatasourceIntegration デフォルトの統合スクリプトは、選択したフィードタイプに基づいています。たとえば、データ処理および取得の標準形式である「MISP フィードタイプ」を選択した場合、統合スクリプトは「SimpleFeedDatasourceIntegration」になります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: カスタム統合スクリプトの場合、「FeedDatasourceIntegrationBase」を拡張してスクリプトインクルードを作成し、必要なメソッドを上書きすることができます。
プロセッサをレポート	レポートプロセッサスクリプトは、統合スクリプトを使用してフィードから取得したデータを処理します。 以下は、ベースシステム内のカスタムスクリプトインクルードです。これらが、統合スクリプト用にアプリケーション内でプロビジョニングされます。 ○ FeedDatasourceResponseProcessor ○ MITRECollectionDataProcessor ○ RSSFeedDatasourceResponseProcessor ○ SimpleFeedDatasourceResponseProcessor ○ SimpleMISPFeedDatasourceResponseProcessor ○ TAXIIV2CollectionDataProcessor STIX HTTPS のデフォルトのレポートプロセッサは「TAXIIV2CollectionDataProcessor」です。デフォルトでは、このオプションが表示されます。他のレポートプロセッサへの変更や選択はできません。

必要に応じて、[スケジュール] セクションのフィールドに入力します。

スケジューリング

フィールド	説明
ラン	レコードを取り込む頻度を設定します。フィードは、ジョブのスケジュール間隔に基づいて実行されます。使用可能なジョブ間隔は、以下のとおりです。 ○ 日次 ○ 週次 ○ 月次 ○ 定期的 ○ 1 回 ○ オンデマンド

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ ビジネスカレンダー: エントリー開始 ○ ビジネスカレンダー: エントリー終了 **注:** デフォルトでは、頻度は [オンデマンド] に設定されています。 詳細については、「スケジュール済みジョブ」および「選択したスクリプトを自動的に実行する方法」を参照してください。
データのフェッチ元	開始日は、データフェッチが必要になる最初の日となります。このフィールドでは時刻を設定する必要があります。この時刻は、該当のソースからデータを取り込む必要がある時刻となります。このフィールドが設定されると、次の取り込み実行では設定された時刻にデータがフェッチされ、取り込み実行が継続的に行われる場合は増分のデータが取得されることになります。 たとえば、1 時間ごとにデータを取り込むようにソースをスケジュール設定します。ユーザーが 1 月 12 日午前 9 時 30 分に **[**データフェッチの開始日時] を 1 月 12 日午前 6 時 00 分に設定し、取り込みのトリガーが 1 月 12 日午前 10 時に行われると、1 月 12 日午前 6 時～ 1 月 12 日午前 10 時までのデータが取得されます。次の取り込みのトリガーは午前 11:00 になり、1 月 12 日午前 10 時～ 1 月 12 日午前 11 時までの増分データのみがフェッチされます。 **注:** つまり、スケジュールされた実行では、指定された日時以降にデータが追加的にフェッチされることになります。

タグ

フィールド	説明
タグを選択	タグを使用して、ソースからシステムに取り込まれたレコードに注釈や目印を付けます。[検索] バーにタグ名を入力して、アプリケーションで使用可能なタグを選択するか、新しいタグ名を入力して [追加] をクリックし、ソースに割り当てます。

8. [保存] アクションをクリックして、フィードを保存および作成します。

   指定された詳細情報が検証されます。デフォルトではフィードのステータスが無効になっています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

9. (オプション) [下書きとして保存する] アクションをクリックすると、フィード構成がドラフトとして保存されるだけとなります。ドラフトとして保存されたフィードは有効化できません。

   構成の詳細が不明な場合は、[下書きとして保存する] のオプションを利用して構いません。構成の詳細を取得したら、残りの情報をドラフトバージョンに入力して作成できます。

10. フィードを有効化するには、[有効化] をクリックします。

    フィードが正常に有効化されました。[カタログ] または [脅威インテリジェンスフィード] ページでは、必要なフィードのタイルのアクションメニューから特定のフィードを有効化、無効化、削除することもできます。

    注:
    データソースフォームのページの [スケジュール] セクションで実行頻度が [オンデマンド] に設定されている場合、統合を有効化するたびに、ソースが正常に有効化されたことをユーザーにアラートするメッセージプロンプトが表示されます。ソース構成でデータを自動的に取り込むには、実行頻度を変更する必要があります。

11. [有効化] をクリックしてレコードを有効化します。

    フィードデータソースのレコードが有効化されたら、レコードを実行して、統合を実行します。

    注:
    データソースのレコードにラベルが付けられ、有効であることが示されます。同様に、[無効化] ボタンをクリックすると、データソースのフィードが無効化されます。

12. [削除] をクリックして、フィードデータソースのレコードを削除します。
13. [統合実行] セクションを選択して、実行の詳細情報を確認します。

    注:
    上記のフィードデータソースの構成手順は、他のあらゆるフィードデータソースタイプに対しても同様です (STIX TAXII を除く)。STIX TAXII の構成方法について、詳細は「新しい TAXII フィードを構成する」を参照してください。

脅威インテリジェンスフィードのタイプ

脅威インテリジェンスフィードのタイプは次のとおりです。これらは構成して有効化することができます。

脅威インテリジェンスフィード

タイプ	説明
TAXII フィード	STIX/TAXII の収集形式で利用可能なフィード。
STIX HTTPS	STIX 形式の脅威インテリジェンスフィード。HTTPS プロトコルで REST API を介してアクセスできます。
MISP	MISP 形式のフィードです。
テキスト	テキスト形式のホストファイルとして利用できるフィード。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威インテリジェンスフィード (続く)

タイプ	説明
	注: システムで URL、ドメイン、ファイル名、ハッシュのファイルを解析します。IP アドレスのみが抽出され、他の観測可能タイプは抽出されません。
CSV	CSV 形式でホストファイルとして利用できるフィード。 注: システムで URL、ドメイン、ファイル名、ハッシュのファイルを解析します。IP アドレスのみが抽出され、他の観測可能タイプは抽出されません。
JSON	JSON 形式でホストファイルとして利用できるフィード。 注: システムで URL、ドメイン、ファイル名、ハッシュのファイルを解析します。IP アドレスのみが抽出され、他の観測可能タイプは抽出されません。
RSS	RSS 形式で利用できるフィード。アプリケーションで、データが RSS フィードレコードとして保存されます。
カスタム	カスタムパーサーで構成されたフィード。 注: システムで URL、ドメイン、ファイル名、ハッシュのファイルを解析します。IP アドレスのみが抽出され、他の観測可能タイプは抽出されません。

手順の次のステップについては、固有の各フィードタイプの構成に関するセクションをそれぞれ参照してください。 脅威インテリジェンスフィード。

脅威インテリジェンスフィードを表示する

このセクションでは、ベースシステムで構成されている脅威インテリジェンスフィードについて説明します。

STIX TAXII フィードを表示

ベースシステムで構成されている STIX TAXII フィードを表示します。

始める前に
必要なロール：sn_sec_tisc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. 統合アイコンをクリックします。
3. **STIX TAXII** を選択します。
   ベースシステム内の MISP フィードについては、次の表のとおりです。

脅威フィード	説明	URL
Cyware TAXII	Cyware Threat Intelligence eXchange (CTIX) は、組織間でのサイバー脅威インテリジェンスの共有を促進するために設計されたプラットフォームです。	https://threatfeed.cyware.com/ctixapi/ctix21/
RecordedFuture TAXII	Recorded Future は、サイバー、サプライチェーン、物理、不正の領域における脅威の特定および緩和を実現する独立型の脅威インテリジェンスクラウドプラットフォームです。	https://api.recordedfuture.com/taxii2
Pulsedive TAXII	Pulsedive は、幅広いサイバー脅威インテリジェンスのサービスやツールを組織に提供する脅威インテリジェンスプラットフォームです。	https://pulsedive.com/taxii2/api/

4. [編集] をクリックして、フィードを編集します。

STIX HTTPS フィードを表示

ベースシステムで構成されている STIX HTTPS フィードを表示します。

始める前に
必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. 統合アイコンをクリックします。
3. **[STIX HTTPS]** を選択します。
   ベースシステム内の STIX HTTPS フィードについては、次の表のとおりです。

ThreatFeed	説明	URL
MITRE - モバイル ATT&CK	このデータコレクションでは、モバイル ATT&CK からの STIX オブジェクトを保持します。	https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json
MITRE - ICS ATT&CK	このデータコレクションでは、ICS ATT&CK からの	https://raw.githubusercontent.com/

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ThreatFeed	説明	URL
	STIX オブジェクトを保持します。	mitre/cti/master/ics-attack/ics-attack.json
MITRE - エンタープライズ ATT&CK	このデータコレクションは、エンタープライズ ATT&CK からの STIX オブジェクトを保持します。	https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json

4. [編集] をクリックし、フィードを編集して必要な更新を行います。

MISP フィードを表示

ベースシステムで構成されている MISP フィードを表示します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. 統合アイコンをクリックします。
3. **MISP** を選択します。
   ベースシステム内の MISP フィードについては、次の表のとおりです。

脅威フィード	説明	URL
DigitalSide 脅威インテリジェンス OSINT フィード	DigitalSide 脅威インテリジェンス OSINT フィードからオープンソースのサイバー脅威インテリジェンス情報をフェッチするデータソースです。主にマルウェア分析をはじめ、侵害された URL、IP、ドメインがベースとなります。	https://osint.digitalside.it/Threat-Intel/digitalside-misp-feed/manifest.json
URLhaus IOC	URLhaus は、マルウェアの配布で使用されている悪意のある URL を共有することを目的とした abuse.ch のプロジェクトです。	https://urlhaus.abuse.ch/downloads/misp/manifest.json
MalwareBazaar	MalwareBazaar は、マルウェアサンプルを情報セキュリティコミュニティ、AV ベンダー、脅威インテリジェンスプロバイダーと共有することを目的とした abuse.ch のプロジェクトです。	https://bazaar.abuse.ch/downloads/misp/manifest.json
ThreatFox IOC	ThreatFox は、マルウェアと関連付けられているセキュリティ侵害のインジケーター (IOC) を情報セキュリティコミュニティ、AV ベンダー、脅	https://threatfox.abuse.ch/downloads/misp/manifest.json

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威フィード	説明	URL
	威インテリジェンスプロバイダーと共有することを目的とした abuse.ch の無料プラットフォームです。	

4. [編集] をクリックして、フィードを編集します。

テキストフィードの表示

ベースシステムで構成されているテキストフィードを表示します。

始める前に
必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. 統合アイコンをクリックします。
3. [テキスト] オプションを選択します。
   ベースシステム内で構成されたテキストフィードは、次の一覧のとおりです。

脅威フィード	説明	URL
Haley のブルートフォース IP	IP アドレスでソートされた、過去 2 年間の攻撃マシンの IP アドレスリストを提供します	http://charles.the-haleys.org/ssh_dico_attack_hdeny_format.php/hostsdeny.txt
Blockrules Emergingthreats	Emerging Threat (ET) Intelligence では、疑わしいアクティビティや悪意のあるアクティビティに関与する IP を特定するための実用的な脅威インテリジェンスフィードを提供します。	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
Nuug Pop3 Groper Web	bsdly.net で POP3 サービスへのログオンを試行して失敗したホストのリスト。	https://home.nuug.no/%7Epeter/pop3gropers.txt
Tor 出口ノード	Tor 出口ノードを使用して、TOR ネットワークからのトラフィックを検出することができます。	https://www.dan.me.uk/torlist/?exit
Talos インテリジェンス IP ブラックリスト	Talos は、SourceFire の Vulnerability Research Team (脆弱性調査チーム)、Cisco の Threat Research and Communications (脅威調査およびコミュニケーション) グループ、Cisco Secure Applications Group (セキュアアプリケーショングループ) を統合して設立されました。	https://www.talosintelligence.com/documents/ip-blacklist

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威フィード	説明	URL
	統合された専門知識は、高度なインフラストラクチャをはじめ、ネットワーク、エンドポイント、クラウド環境、仮想システム、日常的な Web やメールのトラフィックに及ぶ Cisco の比類のないテレメトリデータによって支えられています。	
SANS	ISC では、何千ものインターネットユーザーや組織に分析および警告サービスを無料で提供しています。	https://isc.sans.edu/feeds/topips.txt
Snort	Snort は、世界最高クラスのオープンソース侵入防止システム (IPS) です。Snort IPS では、悪意のあるネットワークアクティビティの定義に役立つ一連のルールが用いられます。	https://snort.org/downloads/ip-block-list
CI Army	CINS Army リストは CINS Active Threat Intelligence ルールセットのサブセットとなり、次の 2 つの基本基準のいずれかを満たす IP アドレスで構成されています：1) 最近における IP の Rogue Packet スコア係数が非常に低い。2) IP が、世界中に展開されている一定数の Sentinel において、指定された数の「信頼性の高い」アラートを作動させた。	https://cinsscore.com/list/ci-badguys.txt
Proofpoint	ファイアウォールブロックリストの生 IP。リストのソース：Spamhaus (www.spamhaus.org) によって識別された Spam nets、DShield (www.dshield.org) によってリストされた Top Attackers、Abuse.ch	https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt
ブロックリスト - GreenSnow	GreenSnow は、コンピューターセキュリティの最も優れたスペシャリストで構成されるチームです。GreenSnow では世界中のさまざまなコンピューターから大量の IP を収集しています。GreenSnow は、スパム以外のあらゆる種類の攻撃において	https://blocklist.greensnow.co/greensnow.txt

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威フィード	説明	URL
	SpamHaus.org に匹敵すると言えます。	
CI Army	CINS Army リストは CINS Active Threat Intelligence ルールセットのサブセットとなり、次の 2 つの基本基準のいずれかを満たす IP アドレスで構成されています：1) 最近における IP の Rogue Packet スコア係数が非常に低い。2) IP が、世界中に展開されている一定数の Sentinel において、指定された数の「信頼性の高い」アラートを作動させた。	https://cinsscore.com/list/ci-badguys.txt
ブロックリスト	www.blocklist.de は、詐欺 / 悪用に関するスペシャリストがボランティアで提供する無料サービスです。このサーバーは SSH、メールログイン、FTP、Web サーバーなどのサービスを介して攻撃される傾向があります。	https://lists.blocklist.de/lists/all.txt
Tor 出口ノード	Tor 出口ノードを使用して、TOR ネットワークからのトラフィックを検出することができます。	https://www.dan.me.uk/torlist/?exit
Botscout ボットの IP	BotScout は、「ボット」と呼ばれる Web の自動化スクリプトによるフォーラム登録、データベースの汚染、スパムの拡散、Web サイトでのフォームの悪用を防止するのに役立ちます。	http://botscout.com/last_caught_cache.txt
データプレーン - VNC RFB	VNC リモートフレームバッファセッションの開始と識別された IP アドレス。	https://dataplane.org/signals/vncrfb.txt
データプレーン - TELNET ログイン	TELNET パスワード認証を介したログイン試行と識別された IP アドレス。	https://dataplane.org/signals/telnetlogin.txt
データプレーン - SSH パスワード認証	SSH パスワード認証を介したログイン試行と識別された IP アドレス。	https://dataplane.org/signals/sshpwauth.txt
データプレーン - SSH クライアント接続	SSH クライアントプロトコルネゴシエーションの実行と識別された IP アドレス。	https://dataplane.org/signals/sshclient.txt
Blockrules Emergingthreats	Emerging Threat (ET) Intelligence では、疑わしいアクティビティや悪意のあるアクティビティに関与する IP を特	https://rules.emergingthreats.net/blockrules/compromised-ips.txt

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威フィード	説明	URL
	定するための実用的な脅威インテリジェンスフィードを提供します。	
データプレーン - SMTP グリーティング	SMTP クライアントによる一方的な HELO または EHLO コマンド発行と識別された IP アドレス。	https://dataplane.org/signals/smtpgreet.txt
データプレーン - SIP クエリ	SIP OPTIONS クエリの送信と識別された IP アドレス。	https://dataplane.org/signals/sipquery.txt
データプレーン - IP プロトコル 41	オープン IPv4 プロトコル 41 のリレー (IPv6 over IPv4 など) と識別された IP アドレス。	https://dataplane.org/signals/proto41.txt
データプレーン - SIP 招待	SIP INVITE のオペレーション送信と識別された IP アドレス。	https://dataplane.org/signals/sipinvitation.txt
データプレーン - DNS CH TXT version.bind	DNS CH TXT VERSION.BIND クエリを送信していると識別された IP アドレス。	https://dataplane.org/signals/dnsversion.txt
データプレーン - DNS TCP	DNS over TCP ポート 53 クエリを送信していると識別された IP アドレス。	https://dataplane.org/signals/dnstcp.txt
データプレーン - DNS 再帰要求 の IN ANY	再帰 DNS の IN ANY クエリを送信していると識別された IP アドレス。	https://dataplane.org/signals/dnsrdany.txt
データプレーン - DNS 再帰が必要	再帰 DNS クエリを送信していると識別された IP アドレス。	https://dataplane.org/signals/dnsrd.txt
GitHub のフィッシングデータベース - アクティブなフィッシングリンク	Github で利用可能なフィッシングデータベースからアクティブなフィッシングリンクをフェッチするためのデータソース。	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-links-ACTIVE.txt
GitHub のフィッシングデータベース - アクティブドメイン	Github で利用可能なフィッシングデータベースからアクティブドメインをフェッチするためのデータソース。	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-domains-ACTIVE.txt
GitHub のフィッシングデータベース - アクティブ IP	Github で利用可能なフィッシングデータベースからアクティブ IP をフェッチするためのデータソース。	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-IPs-ACTIVE.txt
ブロックリスト - ボット	過去 48 時間以内に、攻撃 (RFI 攻撃、REG-Bot、IRC-Bot、BadBot) の実行が報告されたすべての IP アドレス。	https://lists.blocklist.de/lists/bots.txt

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威フィード	説明	URL
ブロックリスト - Apache 攻撃	過去 48 時間以内に、攻撃 (Apache サービス、Apache-DDOS、RFI 攻撃) の実行が報告されたすべての IP アドレス。	https://lists.blocklist.de/lists/apache.txt
Scopserv による VoIP ブラックリスト	VoIP ブラックリストからブロックリスト登録された IP のリストを取得します。	http://voipbl.org/update/?dm=bl
Threatview ドメインブロックリスト	フィッシング / マルウェアの供給 / コマンドアンドコントロールにおいて識別された悪意のあるドメイン。	https://threatview.io/Downloads/DOMAIN-High-Confidence-Feed.txt
Threatview MD5 ハッシュブロックリスト	悪意のあるファイルや、マルウェア、ランサムウェア、ハッキングツール、ボットなどと関連付けられている MD5 ハッシュ。	https://threatview.io/Downloads/MD5-HASH-ALL.txt
Threatview URL ブロックリスト	マルウェア、フィッシング、ボットネット、C2 を供給する悪意のある URL。	https://threatview.io/Downloads/URL-High-Confidence-Feed.txt
Threatview SHA ファイルハッシュのブロックリスト	マルウェアを実行する既知のファイルまたはマルウェアの実行とリンクされているファイルの SHA ハッシュ。	https://threatview.io/Downloads/SHA-HASH-FEED.txt
Threatview IP ブロックリスト	既知の不正な IP アドレスに関する悪意のある IP ブロックリスト。	https://threatview.io/Downloads/IP-High-Confidence-Feed.txt
Threatview C2 ハントフィード	Threatview.io が Proactive Hunt (プロアクティブハント) 中に検出したコマンドアンドコントロールサーバーをホストするインフラストラクチャ	https://threatview.io/Downloads/High-Confidence-CobaltStrike-C2%20-Feeds.txt
Threatview OSINT 脅威フィード	OSINT ソース (X および Pastebin) から収集された悪意のあるセキュリティ侵害のインジケーター。	https://threatview.io/Downloads/Experimental-IOC-Tweets.txt

4. [編集] をクリックして、フィードを編集します。

CSV フィードを表示

ベースシステムで構成されている CSV フィードを表示します。

始める前に

必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. 統合アイコンをクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. **[CSV]** を選択します。
   ベースシステム内の CSV フィードについては、次の表のとおりです。

ThreatFeed	説明	URL
Abuse.ch SSL 認証のブラックリスト	SSL 認証のブラックリスト (CSV) は、SSLBL でブラックリストに登録されているすべての SSL 認証の SHA1 フィンガープリントを含む CSV です。	https://sslbl.abuse.ch/blacklist/sslblacklist.csv
ボットネット C2 IP のブラックリスト	SSL 認証は、1 つ以上のサーバーに関連付けることができます (IP アドレス：ポートの組み合わせ)。SSLBL では、SSLBL でブラックリスト登録された SSL 認証で実行されている IP アドレスを収集します。通常、これらはボットネットのコマンド & コントロールサーバー (C&C) です。こうした IP のブラックリストが SSLBL で公開されているので、これらを活用して、感染したマシンからインターネットへのボットネット C2 トラフィックを検出し、ネットワークから切り離すことができます。	https://sslbl.abuse.ch/blacklist/sslipblacklist.csv
Phishtank オンライン	NA	https://data.phishtank.com/data/online-valid.csv

4. [編集] をクリックして、フィードを編集します。

カスタムフィードの表示

ベースシステム内で送出されるカスタムフィードを表示します。

始める前に

必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. 統合アイコンをクリックします。
3. [カスタム] を選択します。
   すぐに利用できるカスタムフィードは、次のテーブルのとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ThreatFeed	説明	URL
CrowdStrike フィード	CrowdStrike アクター、観測事象、レポートのデータを取得するソース。	https://api.crowdstrike.com

4. [編集] をクリックして、フィードを編集します。

CrowdStrike のプレミアム脅威フィードの表示

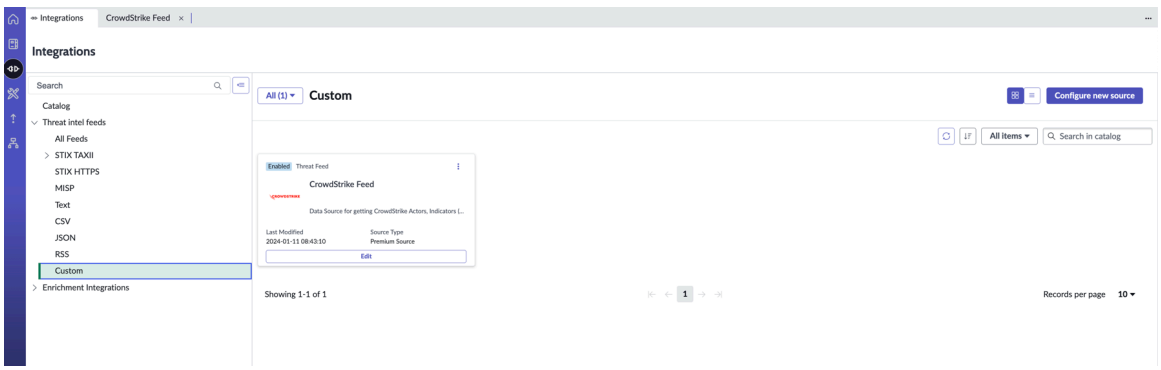
[カスタム] タイプのフィードに新しく追加されたプレミアム脅威フィードを表示します。データソースマネージャーを使用するすべてのプレミアムフィードには、ポイント統合が必要です。

始める前に
必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. 統合アイコンをクリックします。
3. [カスタム] を選択します。
4. **[CrowdStrike フィード (CrowdStrike feed)]** カードをクリックします。

> 注:
> デフォルトでは、CrowdStrike フィードは無効になっています。フィードを有効にするには構成を編集する必要があります。



5. [構成の詳細] セクションにドリルダウンします。
6. [ベース **URL**]、[クライアント **ID**]、[クライアントシークレット] を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

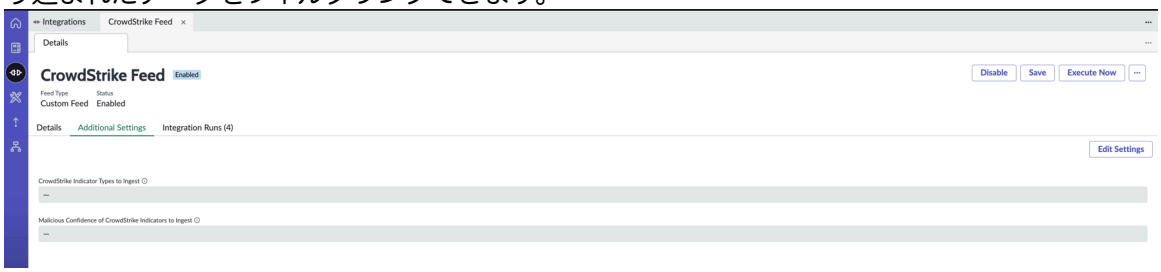
a. [ベース **URL**]：各 CrowdStrike クラウドには異なるベース URL があります。CrowdStrike API に要求を行う場合は、CrowdStrike がホストされているクラウドに対応するベース URL を使用します。

b. ベース URL がない場合は、クライアント ID とクライアントシークレットを生成する必要があります。クライアント ID とクライアントシークレットの詳細については、「Defining your first API Client (最初の API クライアントの定義)」セクションを参照してください。

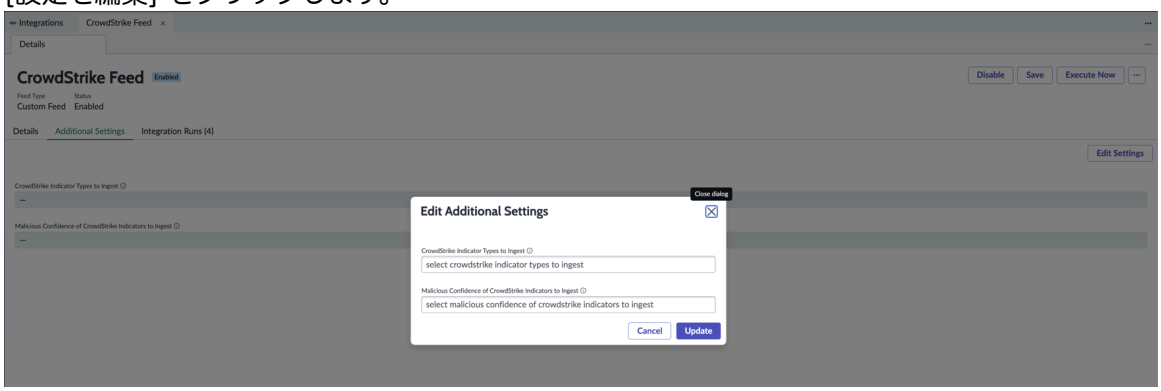
c. 必要なスコープのクライアント ID とクライアントシークレットを CrowdStrike から取得します。以下は、Crowdstrike からのクライアント ID およびクライアントシークレットに必要なスコープです。

- インジケーター (Falcon Intelligence)
- アクター (Falcon Intelligence)
- レポート (Falcon Intelligence)

7. CrowdStrike 脅威フィード統合固有の [追加設定] に移動します。これを使用して、ソースから取り込まれたデータをフィルタリングできます。



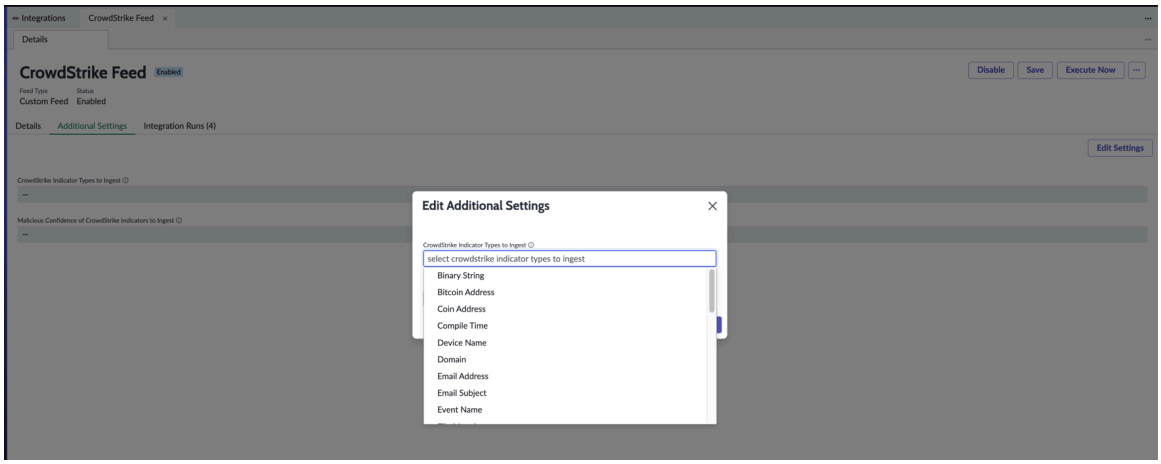
8. [設定を編集] をクリックします。

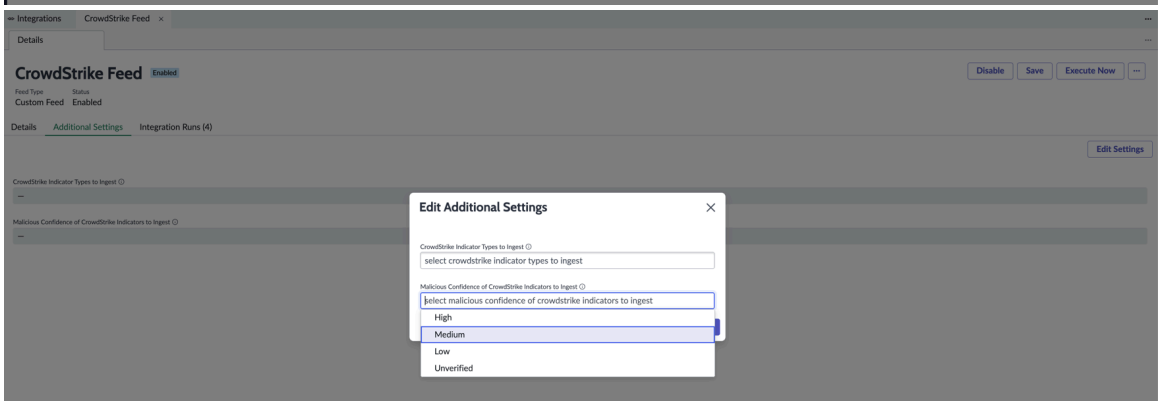


9. [取り込む **CrowdStrike** インジケータータイプ **(Crowd Strike Indicator Types to Ingest)**] または [取り込む **CrowdStrike** インジケーターの悪意のある信頼度 **(Malicious Confidence of CrowdStrike Indicators to Ingest)**] のいずれかのオプションを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。





注:

a. 取り込む **CrowdStrike** インジケータータイプ **(Crowd Strike Indicator Types to Ingest)**：更新されたインジケーターのフェッチ中に、選択したインジケータータイプのみが CrowdStrike から取り込まれます (CrowdStrike のインジケーターは TISC の観測事象にマッピングされます)。空白のままにすると、すべてのタイプのインジケーターが取り込まれます。

b. 取り込む **CrowdStrike** インジケーターの悪意のある信頼度 **(Malicious Confidence of CrowdStrike Indicators to Ingest)**：更新されたインジケーターのフェッチ中に、選択された悪意のある信頼性を持つ選択されたインジケーターのみが CrowdStrike から取り込まれます (CrowdStrike のインジケーターは TISC の観測事象にマッピングされます)。空白のままにすると、すべての悪意のある信頼のインジケーターが取り込まれます。

10. 各オプションに必要な値を選択します。これに基づいて一致インジケーターが取り込まれます。
11. [更新] をクリックします。
12. [有効化] をクリックします。

注:
プレミアムフィードは、構成中に解析される応答を除き、他のフィードと同じです。特定の応答は、クライアント ID とクライアントシークレットを追加することで CrowdStrike に対して解析されます。

CrowdStrike からフェッチされるデータのタイプ：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. 設定された取り込み時間の後に更新される CrowdStrike からのインジケーター。CrowdStrike からのこれらのインジケーターは、TISC の観測事象にマッピングされます。以下は、TISC に取り込まれるインジケータータイプです。
   - SHA256 ハッシュ
   - MD5 ハッシュ
   - SHA1 ハッシュ
   - URL
   - ドメイン
   - IP アドレス
   - ミューテックス名
   - ファイル名
   - メールアドレス
   - ユーザー名
   - IP アドレスブロック

b. 設定された取り込み時間の後に更新された CrowdStrike の攻撃者。CrowdStrike のこれらのアクターは、システム内の攻撃者にマッピングされます。

c. 設定された取り込み時間の後に更新される CrowdStrike からのレポート。CrowdStrike からのこれらのレポートは、システム内の脅威レポートにマッピングされます。

d. また、上記のエンティティに加えて、以下のデータもフェッチします。
   i. 上記で取り込まれたインジケーターに関連する攻撃者/レポート/インジケーター。
   ii. 現在の取り込みの一部として取り込まれたすべてのレポートに関連する攻撃者/インジケーター。

CrowdStrike のシステムプロパティ

以下では、CrowdStrike のシステムプロパティについて詳しく説明します。

1. sn_sec_tisc.crowdstrike_actor_batch_size：1 回の API 呼び出しでプルされるアクターの数を示します。注：統合によってシステム内に必要なものが見つからない場合にのみ適用されます。
   - タイプ：整数
   - 値：250
2. sn_sec_tisc.crowdstrike_api_limit：CrowdStrike から一度にフェッチするレコードの数。数値が大きいほど、ペイロードの処理で消費されるメモリが多くなります。
   - タイプ：整数
   - 値：1,000
3. sn_sec_tisc.crowdstrike_indicator_batch_size：1 回の API 呼び出しでプルされるインジケーターの数を示します。注：統合によってシステム内に必要なものが見つからない場合にのみ適用されます。
   - タイプ：整数
   - 値：150
4. sn_sec_tisc.crowdstrike_offset_limit_total：CrowdStrike API からのオフセットと制限の許容合計。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- タイプ：整数
- 値：50,000

5. sn_sec_tisc.crowdstrike_report_batch_size：1 回の API 呼び出しでプルされるレポートの数を示します。注：統合によってシステム内に必要なものが見つからない場合にのみ適用されます。
   - タイプ：整数
   - 値：50

STIX TAXII について

構造化脅威情報表現 (STIX) とは、サイバー脅威インテリジェンス (CTI) の交換で使用される言語およびシリアル化形式です。TAXII (Trusted Automated Exchange of Intelligence Information) は、HTTPS 経由でのサイバー脅威インテリジェンス (CTI) の交換で使用されるプロトコルです。

STIX を使用して、疑い、侵害、属性のあらゆる側面をオブジェクトや記述的関係として表します。STIX 情報は、アナリスト向けに視覚的に表現したり、JSON で保存して素早く機械可読化したりすることができます。

サイバー脅威インテリジェンス (CTI) とは、一連の情報表現やプロトコルを定義して、サイバー脅威インテリジェンスのモデル化、分析、共有のニーズに対応する認められた概念です。CTI では主に、構造化脅威情報表現 (STIX) と検知指標情報自動交換手順 (TAXII) の開発や標準化に重点を置いています。

新しい TAXII フィードを構成する

STIX 形式の情報を共有するために、TAXII フィードを管理できます。各 TAXII フィードには、1 つ以上の TAXII 収集が含まれています。

始める前に

必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. 統合アイコンをクリックします。
3. 選択 脅威インテルフィード > **STIX TAXII** > **TAXII** フィード.

   注:
   TAXII フィードがすべての TAXII 収集のプロファイルとして機能するように構成します。

4. [新しいデータソースを構成 **(Configure new source)**] をクリックします。
   [新しい TAXII フィードを構成する] ページが表示されます。
5. フォームのフィールドに入力します。

新しいデータソースを作成

フィールド	説明
名前	フィードの名前を入力します。
説明	フィードの説明。
ソースタイプ	フィードに提供されるソースのタイプ (オープンソース、プレミアムソースなど)。利用可能なソースタイプは、次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ 政府 ○ ISAC ○ オープンソース ○ プレミアムソース ○ その他のソース
ロゴ	ソースフィードのロゴを添付します。
業種	フィードのデータソースが適用される産業カテゴリ (航空宇宙、農業など) を選択します。

必要に応じて、[構成] セクションのフィールドに入力します。

構成

フィールド	説明
TAXII バージョン	構成が必要な TAXII サーバーの TAXII バージョンを選択します。サポートされているバージョンは 2.0 と 2.1 です。
構成タイプ	TAXII 収集をフェッチする構成タイプを指定します。使用可能な値： ○ ディスカバリーサービス **URL**：ディスカバリーサービス URL を選択して、TAXII サーバーのディスカバリーサービスで使用可能なすべての API ルートからコレクションをフェッチします。 ○ **API** ルート **URL**：API ルート URL を選択して、TAXII サーバーの特定の API ルートからコレクションをフェッチします。
認証	認証が必要な場合、ドロップダウンリストから必要なオプションを選択します。使用可能なオプションは、次のとおりです。 ○ なし：認証が不要な場合は、このオプションを選択します。 ○ 基本：ユーザー名とパスワードを指定するには、このオプションを選択します。 ○ **API** キー：API キーを指定するには、このオプションを選択します。 ○ **REST** メッセージを選択：その他のタイプの認証には、このオプションを選択します。REST メッセージのオプションは次のとおりです。 ▪ **REST** メッセージを使用：構築済み REST メッセージを作成する REST メッセージが必要な場合は、このボックスを選択します。選択されていない場合は、エンドポイントフィールドの値が使用されます。ルッ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	クアップアイコンをクリックして、リストから REST メッセージを選択します。 ▪ **REST** メソッド：REST メソッドが必要な場合は、このボックスを選択します。ルックアップアイコンをクリックして、リストから REST メソッドを選択します。 **注:** REST メッセージのオプションが選択されていると、[REST メッセージ] および [REST メソッド] フィールドが使用できるようになります。
URL	選択した構成タイプに応じて、TAXII サーバーのディスカバリーサービス URL または特定の API ルート URL を入力します。
[詳細設定] セクション	
詳細	別の統合スクリプトやレポートプロセッサを選択するには、このチェックボックスをオンにします。選択したスクリプトが、選択した TAXII バージョンと互換性があることを確認してください。デフォルトでは、TAXII バージョンと認証に応じてこれらのスクリプトが 自動入力されます。
統合スクリプト	認証タイプ (ユーザー名 / パスワード / API キー) や要求とともに渡されるヘッダーなどの認証パラメーターを使用して REST エンドポイント URL API の呼び出しを起動します。その後、スクリプトが、特定のフィードで利用可能な観測事象やインジケーター STIX データをフェッチします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: フェッチされるデータは生データのみとなります (レコードは作成されません)。データは統合プロセスに添付され、[統合実行] セクションで表示できるようになります。 以下は、ベースシステム内のカスタムスクリプトインクルードです。これらが、統合スクリプト用にアプリケーション内でプロビジョニングされます。 ○ TAXIIV2_0QueryParamAPIKeyIntegrationScript ○ TAXIIV2_0BasicAuthIntegrationScript ○ TAXIIV2_1QueryParamAPIKeyIntegrationScript ○ TAXIIV2_1BasicAuthIntegrationScript デフォルトの統合スクリプトは、選択したフィードタイプに基づいています。スクリプトインクルードは、簡単な REST コールを実行し、応答を添付ファイルとして保存してから、添付ファイルをプロセッサに返します。
プロセッサをレポート	レポートプロセッサは、REST エンドポイント URL の呼び出しを起動します。 以下のベースシステム内にはカスタムスクリプトインクルードがあります。これが、統合スクリプト (**TAXIIV2CollectionDataProcessor**) 用にアプリケーション内でプロビジョニングされます。

必要に応じて、[スケジュール] セクションのフィールドに入力します。

スケジューリング

フィールド	説明
コレクションの実行頻度	TAXII 収集レコードに適用されるスケジュール間隔。TAXII 収集の実行頻度は、必要に応じて TAXII 収集のフォームビューで変更できます。 注: この設定は、フェッチされるすべての TAXII 収集にデフォルトで適用されます。必要に応じて、TAXII 収集の設定を上書きすることができます (オプション)。 詳細については、「スケジュール済みジョブ」および「選択したスクリプトを自動的に実行する方法」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
データのフェッチ元	開始日は、データフェッチが必要になる最初の日となります。このフィールドでは時刻を設定する必要があります。この時刻は、該当のソースからデータを取り込む必要がある時刻となります。このフィールドが設定されると、次の取り込み実行では設定された時刻にデータがフェッチされ、取り込み実行が継続的に行われる場合は増分のデータが取得されることになります。 たとえば、1 時間ごとにデータを取り込むようにソースをスケジュール設定します。ユーザーが 1 月 12 日午前 9 時 30 分に **[**データフェッチの開始日時] を 1 月 12 日午前 6 時 00 分に設定し、取り込みのトリガーが 1 月 12 日午前 10 時に行われると、1 月 12 日午前 6 時～ 1 月 12 日午前 10 時までのデータが取得されます。次の取り込みのトリガーは午前 11:00 になり、1 月 12 日午前 10 時～ 1 月 12 日午前 11 時までの増分データのみがフェッチされます。 **注:** つまり、スケジュールされた実行では、指定された日時以降にデータが追加的にフェッチされることになります。

6. [接続を検証] をクリックします。
   TAXII フィード接続に成功したことを示す情報メッセージが表示されます。コレクションをフェッチするには、次のステップに進みます。
7. **[TAXII** 収集を取得] をクリックします。

   注:
   エラーが発生した場合は、TAXII 収集のフェッチ中にエラーが発生したことを示すエラーメッセージが表示されるので、ログで詳細を確認してください。

   TAXII 収集は [TAXII 収集] セクションの下に表示されます。デフォルトでは無効になっています。
8. TAXII 収集で使用可能な STIX オブジェクトを取得するには、TAXII 収集を有効化します。

TISC 統合

このセクションでは、脅威インテリジェンス統合の構成や有効化に関する手順について説明します。

観測項目の拡張

観測事象を拡張 WhoIs ワークフローは、選択された観測事象に対して拡張を実行します。観測事象が WhoisXML API 統合で認識されるタイプであれば、拡張できます。

注:
脅威インテリジェンスセキュリティセンターは WHOIS 統合に対してのみ観測事象の拡張をサポートしています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Whois 統合

Whois 統合を使用すると、ドメイン名と URL の Whois ルックアップを送信して、URL 観測事象のコンテキストを取得し、脅威をより適切に判断することができます。

Whois 統合の構成と有効化

Whois 統合を使用するにあたり、ServiceNow Store からのダウンロードが必要です。また、Whois の有効アカウントも必要になります。

始める前に
必要なロール：sn_sec_tisc.admin

脅威インテリジェンスセキュリティセンターと Whois 観測事象の統合プラグインが必要です。

手順

1. 自身のインスタンスを使用して、脅威インテリジェンスセキュリティセンターにアクセスします。
2. から統合をダウンロードします ServiceNow Store.
3. インストールが完了したら、次に移動します: ワークスペース > 脅威インテリジェンスセキュリティセンター.
4. 選択 統合 > 拡張統合 > すべての統合.
5. または、 統合 > 拡張統合 > すべての統合 > 観察事項の拡張.
6. **WHOIS** カードで、[新しい拡張の構成] をクリックして、**WHOIS** 統合を構成します。
7. [新しい拡張を構成 (Configure New Enrichment)] フォームのフィールドに入力します。

拡張統合

フィールド	説明
名前	新しい拡張統合の名前を入力します。例：WHOIS。
ベンダー名	ベンダーの名前。選択したベンダーの詳細がデフォルトで入力されます。例：WHOIS。
統合タイプ	選択した統合のタイプ。例：「脅威のルックアップ」。
説明	新しい拡張統合の説明を入力します。例：WHOIS 統合の説明として「脅威インテリジェンスセキュリティセンターの WHOIS 統合を使用すると、ドメイン名と URL の Whois ルックアップを送信して、URL 観測事象のコンテキストを取得し、脅威をより適切に判断することができます」など。

8. [統合構成] セクションにドリルダウンします。
9. WHOIS サイトから取得した **API** キーを入力 (またはペースト) します。
10. [保存] をクリックします。
    統合の詳細が検証されます。WHOIS 統合のステータスはデフォルトで無効になっています。
11. [有効化] をクリックして、WHOIS 統合を有効化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスクの結果
構成が完了すると、脅威インテリジェンスセキュリティセンターで観測事象の拡張を実行する際に [WHOIS] を選択できるようになります。

Shodan 統合

Shodan は、世界中の接続されたデバイスからのサービスバナー情報を分析する検索エンジンです。

Shodan 統合は、次の観測事象で拡張を実行します。

- IP アドレス
- URL
- ドメイン

Shodan 統合の構成と有効化

Shodan 統合を使用する前に、ServiceNow Store からダウンロードする必要があります。

始める前に
必要なロール：sn_sec_tisc.admin

手順

1. 自身のインスタンスを使用して、脅威インテリジェンスセキュリティセンターにアクセスします。
2. から統合をダウンロードします ServiceNow Store.
3. インストールが完了したら、次に移動します: ワークスペース > 脅威インテリジェンスセキュリティセンター.
4. 選択 統合 > 拡張統合 > すべての統合.
5. または、 統合 > 拡張統合 > すべての統合 > 観察事項の拡張.
6. **Shodan** カードで、[新しい拡張を構成 **(Configure New Enrichment)]** をクリックして、統合を構成します。
7. [新しい拡張を構成 (Configure New Enrichment)] フォームのフィールドに入力します。

拡張統合

フィールド	説明
名前	新しい拡張統合の名前を入力します。例：Shodan。
ベンダー名	ベンダーの名前。選択したベンダーの詳細は自動入力され、デフォルトではこのフィールドは読み取り専用です。例：Shodan。
統合タイプ	選択した統合のタイプ。例：観測事象の拡張。
説明	新しい拡張統合の説明を入力します。たとえば、Shodan 統合の説明では「Shodan は世界中の接続されたデバイスからのバナー情報を分析するのに役立ちます。」と記載されています。

8. [統合構成] セクションにドリルダウンします。
9. Shodan ポータルから取得した **API** キーを入力します (または貼り付けます)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

10. [保存] をクリックします。
    統合の詳細が検証され、デフォルトではステータスは無効になっています。
11. [有効化] をクリックして、統合を有効化します。

サイティング検索

このセクションでは、TISC サイティング検索と Elasticsearch 統合について説明します。

ElasticSearch Integration の開始

Elasticsearch 拡張統合ではログを検索し、関連するサイティング情報を観測事象に追加します。

ElasticSearch Integration の構成と有効化

Elasticsearch は、Security Operations と簡単に統合できる分散型の RESTful 検索および分析エンジンです。

始める前に
Elasticsearch を利用する前に、ServiceNow Store でのダウンロードが必要です。

必要なロール：sn_sec_tisc.admin

- ElasticSearch Integration を利用する前に、脅威インテリジェンスセキュリティセンターのプラグインをインストールしてアクティブ化する必要があります。
- Elasticsearch プロファイルで Elasticsearch API ベース URL、Kibana ベース URL、ユーザー名、パスワードを取得します。

手順

1. 自身のインスタンスを使用して、脅威インテリジェンスセキュリティセンターにアクセスします。
2. から統合をダウンロードします ServiceNow Store.
3. インストールが完了したら、次に移動します: ワークスペース > 脅威インテリジェンスセキュリティセンター.
4. 選択 統合 > 拡張統合 > すべての統合.
5. または、 統合 > 拡張統合 > すべての統合 > サイティング検索

   注:
   構成済みの統合が一連のカードとして表示されます。

6. **Elasticsearch** のカードで、[新しい拡張の構成] をクリックして **Elasticsearch** Integration を構成します。
7. [新しい拡張を構成 (Configure New Enrichment)] フォームのフィールドに入力します。

拡張統合

フィールド	説明
名前	サイティング検索構成の名前を入力します。
ベンダー名	ベンダーの名前。選択したベンダーの詳細がデフォルトで入力されます。例：「Elasticsearch」など。
統合タイプ	選択した統合のタイプ。例：「脅威のルックアップ」。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
説明	ElasticSearch Integration の説明を入力します。例：「Elasticseaarch 拡張統合は、Elasticseaarch 展開でログのクエリをサポートし、観測事象の調査に役立つ」など。
データ連携の構成	
Elasticsearch API のベース URL	Elasticsearch のサイトから取得したベース URL。
Kibana ベース URL	Kibana ベース URL。(オプション) 利用可能な場合、Kibana インスタンスへのリンク。
ユーザー名	Intel Elasticsearch のユーザー名。
パスワード	Intel Elasticsearch のパスワード。
Elasticsearch インデックス	Elasticsearch インデックス。これらは、各インデックス固有のドキュメントを保持します。インデックスは、検索や削除などの動作を示すアクション名 (小文字)で識別されます。
[日付範囲] フィールド	構成のタイムスタンプ。
最大行数	検索する行の最大行数。
最も早い結果 (日数)	表示する最も早い結果 (日数単位)。
検索結果に生データサンプルを含める	サイティング検索結果に生データのサンプルを含めるには、これを選択します。返されるデータの量は、[セキュリティインシデントレスポンス] プロパティの [生データの行数] プロパティの設定によって異なります。
MID サーバー	[任意] を選択して、 任意のアクティブな MID サーバーを使用するか、特定の MID サーバー名を選択します。

注:
この統合を設定すると、ワークフローが有効になります。ワークフローを管理するには、[ワークフローエディター] に移動します。

8. [保存] をクリックします。
   統合の詳細が検証されます。ElasticSearch Integration のステータスはデフォルトで無効になっています。
9. [有効化] をクリックして、ElasticSearch Integration を有効化します。

タスクの結果
構成が完了すると、脅威インテリジェンスセキュリティセンターで観測事象のサイティング検索を実行する際に [Elasticsearch] を選択できるようになります。

Splunk 検索統合の開始

Splunk ソフトウェアは、マシンで生成されたビッグデータを検索、監視、および分析し、Security Operations と簡単に統合できます。Splunk サイティング検索統合を利用する前に、ServiceNow Store からダウンロードする必要があります。

Splunk Integration の構成と有効化

Splunk Enrichment Integration ではログを検索し、関連するサイティング情報を追加します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
Splunk 検索を利用する前に、ServiceNow Store でのダウンロードが必要です。

必要なロール：sn_sec_tisc.admin

- Splunk 検索統合を利用する前に、脅威インテリジェンスセキュリティセンターのプラグインをインストールしてアクティブ化する必要があります。
- Splunk や Splunk 検索を取得し、さらに Splunk インスタンスから API ベース URL、リンク URL、ユーザー名、パスワードを取得します。

手順

1. 自身のインスタンスを使用して、脅威インテリジェンスセキュリティセンターにアクセスします。
2. から統合をダウンロードします ServiceNow Store.
3. インストールが完了したら、次に移動します: ワークスペース > 脅威インテリジェンスセキュリティセンター.
4. 選択 統合 > 拡張統合 > すべての統合.
5. または、 統合 > 拡張統合 > すべての統合 > サイティング検索
   構成済みの統合が一連のカードとして表示されます。
6. **[Splunk** 検索] カードで、[新しい拡張の構成] をクリックして **Splunk** 検索統合を構成します。
7. [新しい拡張を構成 (Configure New Enrichment)] フォームのフィールドに入力します。

拡張統合

フィールド	説明
名前	サイティング検索構成の名前を入力します。
ベンダー名	ベンダーの名前。選択したベンダーの詳細がデフォルトで入力されます。例：Splunk。
統合タイプ	選択した統合のタイプ。例：「脅威のルックアップ」。
説明	Splunk Integration の説明を入力します。たとえば、「Splunk Enrichment Integration は、悪意のある可能性があるインジケーターとの関連において Splunk 展開内でログのクエリをサポートすることで、観測事象の調査をサポートします」など。
データ連携の構成	
Splunk API のベース URL	Splunk サイトから取得したベース URL。
リンク URL	(オプション) 利用可能な場合、Splunk Web インターフェイスにリンクするリンク URL。
ユーザー名	Intel Elasticsearch のユーザー名。
パスワード	Intel Elasticsearch のパスワード。
最大行数	検索する行の最大行数。
最も早い結果 (日数)	表示する最も早い結果 (日数単位)。
検索結果に生データサンプルを含める	サイティング検索結果に生データのサンプルを含めるには、これを選択します。返されるデー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	タの量は、[セキュリティインシデントレスポンス] プロパティの [生データの行数] プロパティの設定によって異なります。
オンプレミス展開	オンプレミス展開環境。
MID サーバー	[任意] を選択して、 任意のアクティブな MID サーバーを使用するか、特定の MID サーバー名を選択します。

注:
この統合を設定すると、ワークフローが有効になります。ワークフローを管理するには、[ワークフローエディター] に移動します。

8. [保存] をクリックします。
   統合の詳細が検証されます。Splunk Integration のステータスはデフォルトで無効になっています。
9. [有効化] をクリックして、Splunk Integration を有効化します。

タスクの結果
構成が完了すると、脅威インテリジェンスセキュリティセンターで観測事象のサイティング検索を実行する際に [Splunk] を選択できるようになります。

脅威のルックアップ

脅威のルックアップ：VirusTotal と CrowdStrike Falcon Intelligence ワークフローでは、選択された観測事象に対してルックアップを実行します。観測事象が VirusTotal や CrowdStrike で認識されるタイプである場合、観測事象でマルウェアがスキャンされ、結果が返されます。

TISC の VirusTotal 統合

TISC の VirusTotal 統合を使用すると、不審な IP アドレス、ファイル、ファイルハッシュ、URL アドレスの分析をリクエストして、調査において悪意の有無を判断できるようになります。

VirusTotal 統合の構成および有効化

VirusTotal 統合を使用する前に、ServiceNow Store からダウンロードする必要があります。

始める前に
必要なロール：sn_sec_tisc.admin

VirusTotal 統合をアクティブ化するには、脅威インテリジェンスセキュリティセンターのプラグインが必要です。

手順

1. 自身のインスタンスを使用して、脅威インテリジェンスセキュリティセンターにアクセスします。
2. から統合をダウンロードします ServiceNow Store.
3. インストールが完了したら、VirusTotal にアクセスし、VirusTotal プロファイルから API キーを取得します。
4. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
5. 選択 統合 > 拡張統合 > すべての統合.
6. または、 統合 > 拡張統合 > すべての統合 > 脅威情報ルックアップ
7. [新しい拡張の構成] をクリックして、**VirusTotal** 統合を構成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

8. [新しい拡張を構成 (Configure New Enrichment)] フォームのフィールドに入力します。

拡張統合

フィールド	説明
名前	新しい拡張統合の名前を入力します。例：VirusTotal。
ベンダー名	ベンダーの名前。選択したベンダーの詳細がデフォルトで入力されます。例：VirusTotal。
統合タイプ	選択した統合のタイプ。例：「脅威のルックアップ」。
説明	新しい拡張統合の説明を入力します。

9. [統合構成] セクションにドリルダウンします。
10. VirusTotal サイトから取得した **API** キーを入力します (または貼り付けます)。
11. [保存] をクリックします。
    統合の詳細が検証されます。VirusTotal 統合のステータスはデフォルトで無効になっています。
12. [有効化] をクリックして、VirusTotal 統合を有効化します。

タスクの結果
構成が完了すると、脅威インテリジェンスセキュリティセンターで観測事象のルックアップを実行する際に [VirusTotal] を選択できるようになります。

TISC の CrowdStrike Falcon Intelligence 統合

CrowdStrike Falcon Intelligence では、Security Operations と簡単に統合できるサイバーセキュリティインテリジェンスを提供します。

注:

CrowdStrike Falcon Intelligence 統合を実装するには、脅威インテリジェンスセキュリティセンターのプラグインが必要です。

CrowdStrike Falcon Intelligence 統合を構成して有効にする

CrowdStrike Falcon Intelligence を使用する前に、ServiceNow Store からダウンロードし、適切なクライアント ID とクライアントシークレットを追加する必要があります。

始める前に
必要なロール：sn_sec_tisc.admin

- 脅威インテリジェンスセキュリティセンターアプリケーションをインストールしてアクティブ化する必要があります。
- CrowdStrike Falcon Intelligence プロファイルで API クライアント ID と API クライアントシークレットを取得します。
- CrowdStrike Falcon Intelligence ポータル API スコープで、インジケーター (Falcon Intelligence) の読み取り設定を有効にします。

手順

1. 自身のインスタンスを使用して、脅威インテリジェンスセキュリティセンターにアクセスします。
2. から統合をダウンロードします ServiceNow Store.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
4. 選択 統合 > 拡張統合 > すべての統合.
5. または、 統合 > 拡張統合 > すべての統合 > 脅威情報ルックアップ.
6. [新しい拡張の構成] をクリックして、**CrowdStrike Falcon Intelligence** 統合を構成します。
7. [新しい拡張を構成 (Configure New Enrichment)] フォームのフィールドに入力します。

拡張統合

フィールド	説明
名前	新しい拡張統合の名前を入力します。例：CrowdStrike Falcon Intelligence
ベンダー名	ベンダーの名前。選択したベンダーの詳細がデフォルトで入力されます。例：CrowdStrike Falcon Intelligence
統合タイプ	選択した統合のタイプ。例：「脅威のルックアップ」。
説明	新しい拡張統合の説明を入力します。
データ連携の構成	
クライアント ID	CrowdStrike から取得したクライアント ID。
クライアントシークレット	CrowdStrike から取得したクライアントシークレットキー。

8. [保存] をクリックします。
   統合の詳細が検証され、デフォルトでは CrowdStrike Falcon Intelligence 統合のステータスは無効になっています。
9. CrowdStrike Falcon Intelligence 統合を有効にするには、[有効] をクリックします。

タスクの結果

構成が完了すると、脅威インテリジェンスセキュリティセンターで観測事象のルックアップを実行する際に CrowdStrike Falcon Intelligence を選択できるようになります。

TISC 拡張統合

脅威インテリジェンスセキュリティセンター のベースシステムには、事前構成された統合は含まれていません。このセクションでは、ServiceNow とサードパーティの統合を構成する手順について説明します。

重要:

必要なサードパーティアプリ統合がインストールされていることを確認します。観測事象、サイティング検索、脅威のルックアップの詳細は、インストールされているサードパーティアプリについてのみ確認できます。

すべての統合構成

統合はすべて、インストールが必要な単独のアプリケーションになります。TISC では、サードパーティベンダーとの統合をサポートしています。インストール済みの統合は、ここで構成できます。

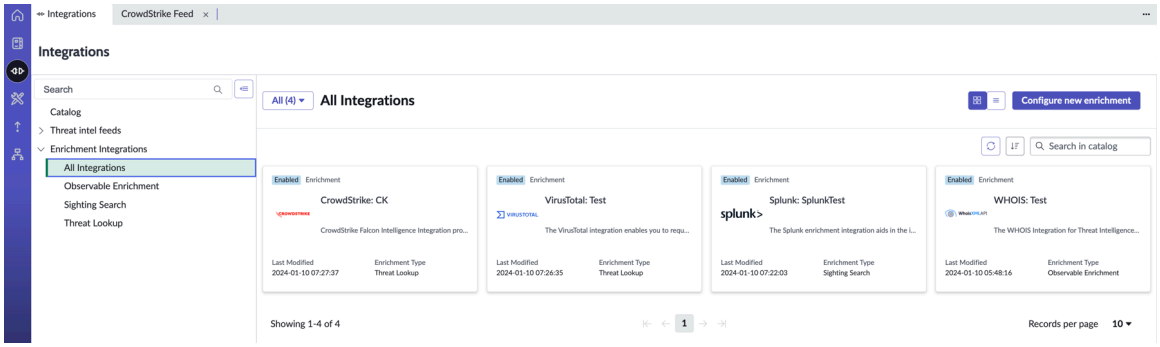
このセクションには、アクティブ化して使用できる構成済みの各統合実装のカードが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

各拡張タイプのセクションは、拡張タイプに対応する統合が 1 つ以上インストールされている場合にのみ表示されます。たとえば、[脅威の ルックアップ] セクションは、「脅威のルックアップ統合」が 1 つ以上インストールされている場合にのみ、[拡張統合] に表示されます。

構成された統合カードは、次に移動して表示できます: ワークスペース > 脅威インテリジェンスセキュリティセンター > 統合 > 拡張統合 > すべての統合.



[すべての統合 **(All Integrations)**] ビューのアクション

[すべての統合 (All Integrations)]ビューでは、次のアクションを実行できます。

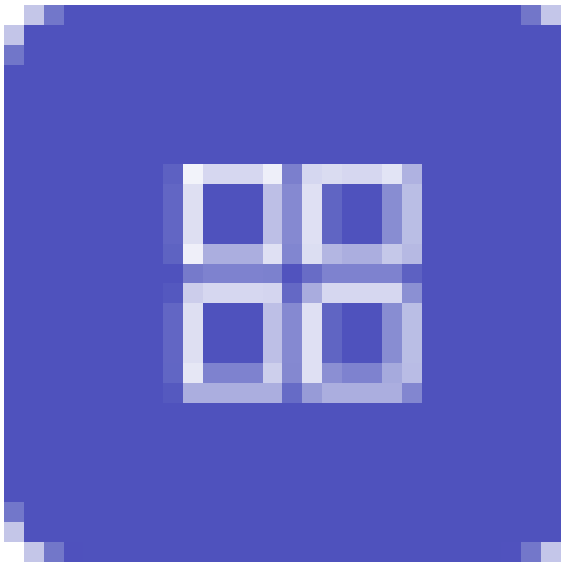
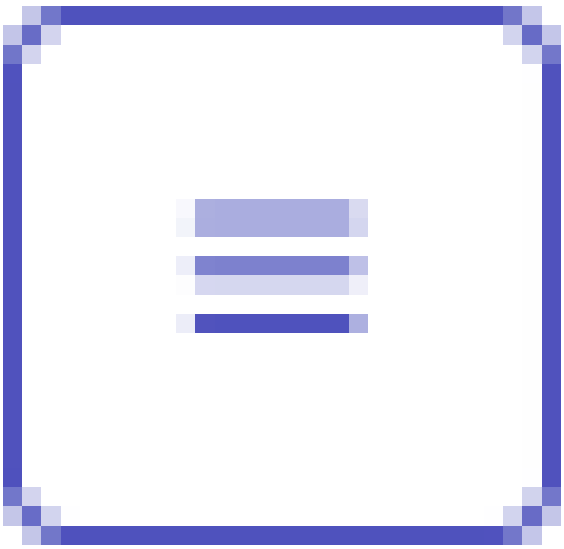
[すべての統合 **(All Integrations)**] ビューのアクション

アクション	説明
すべて	現在のステータスに応じて、ドロップダウンメニューで統合をフィルタリングします。フィルタリングは次のステータスに基づいて実行することができます。 • すべて：ページ上の統合をすべて表示。これはデフォルトのオプションです。 • 有効：有効ステータスの統合をすべて表示。 • 無効：無効ステータスの統合をすべて表示。 • ドラフト：ドラフトステータスの統合をすべて表示。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

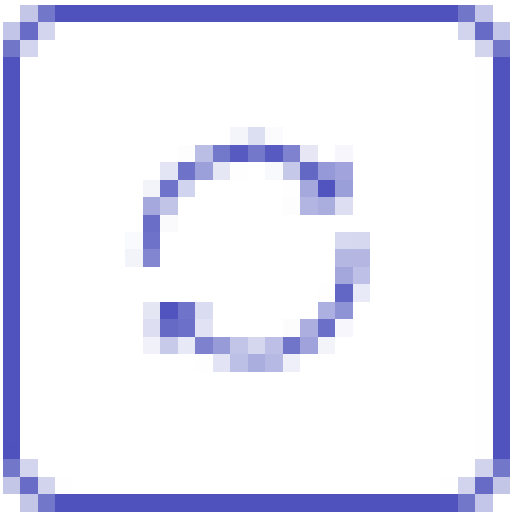
[すべての統合 **(All Integrations)**] ビューのアクション (続く)

アクション	説明
	このアクションで、すべての統合がカード形式で表示されます。
	このアクションで、すべての統合がリスト形式で表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[すべての統合 **(All Integrations)**] ビューのアクション (続く)

アクション	説明
	このアクションで、[すべての統合] ページが更新されます。
	このアクションで、統合が次の内容に基づいてすべてソートされます。 • 最終変更日 (最新) • 最終変更日 (古い順) • 名前 **(A** から **Z)** • 名前 **(Z** から **A)**
カタログで検索	このアクションで、カタログ内の名前や説明に基づいて構成済みの統合を検索します。

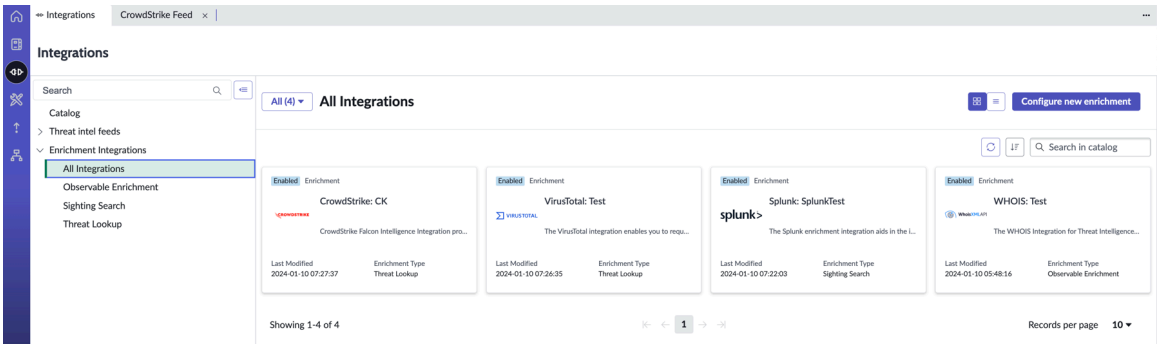
[すべての統合] ビューから新しい拡張統合を構成

新しい拡張は、[すべての統合] ビューから構成できます。または、[観測事象の拡張]、[サイティング検索]、[脅威のルックアップ] セクションから直接構成しても構いません。あらゆる [すべての統合] ビューから新しい拡張を構成するには、次の手順を実行します。

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.

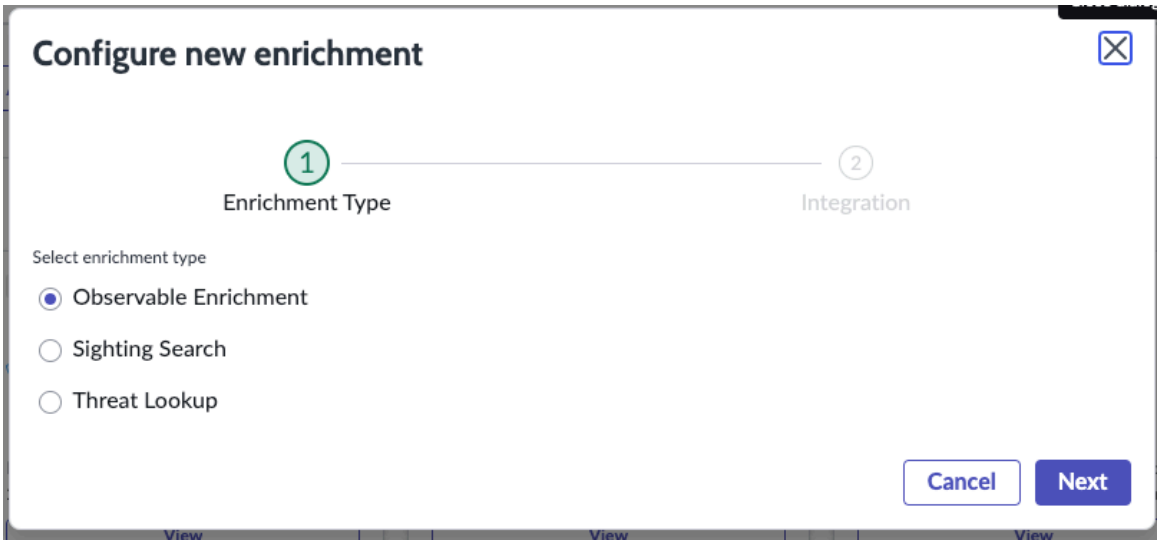
2. [統合] アイコンをクリックし、[すべての統合] セクションを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. [新しい拡張を構成 **(Configure new enrichment)**] アクションをクリックします。

   [新しい拡張の構成] ポップアップに、[観測事象の拡張]、[サイティング検索]、[脅威のルックアップ] の 3 つの拡張タイプが表示されます。構成する拡張タイプを選択する必要があります。



4. 拡張タイプを選択して、 [次へ **(Next)**] をクリックします。

   これにより、利用可能な統合を表示するポップアップが表示されます。構成する統合を選択する必要があります。

5. 利用可能な統合のリストから統合を選択し、[選択] をクリックします。

   これにより、選択した統合の [新しい拡張統合を作成] ページが表示されます。このページには、選択した統合の詳細がデフォルトで事前入力されています。例：WHOIS 統合。

6. [新しい統合を作成] フォームでフィールドに入力します。

   新しい拡張統合フォームの構成

フィールド	説明
名前	新しい拡張統合の名前を入力します。 例：WHOIS1。
ベンダー名	ベンダーの名前。選択したベンダーの詳細は、デフォルトで事前に入力されています。 例：WHOIS。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
統合タイプ	選択した統合のタイプ。例：観測事象の拡張。選択した統合タイプの詳細は、デフォルトで事前に入力されています。 次の統合タイプがサポートされています。 ○ 観測項目の拡張 ○ サイティング検索 ○ 脅威のルックアップ
説明	新しい拡張統合の一意の説明を入力します。

7. [統合構成] セクションで、要件に基づいて統合の詳細を構成します。

   [統合構成] セクションには、API キー、API クライアント ID またはシークレット、ユーザー名、パスワードなどの構成の詳細が含まれており、それらを入力する必要があります。構成の詳細は、統合によって異なります。

8. [保存] アクションをクリックして、拡張統合構成を保存および作成します。

   指定された詳細が検証され、拡張統合のステータスはデフォルトで無効になっています。

9. (オプション) [下書きとして保存する] アクションをクリックすると、フィード構成がドラフトとして保存されるだけとなります。ドラフトとして保存された統合は有効化できません。

   構成の詳細が不明な場合は、[下書きとして保存する] のオプションを利用して構いません。構成の詳細を取得したら、残りの情報をドラフトバージョンに入力して作成できます。

10. 拡張統合を有効にするには、[有効化] をクリックします。

    拡張統合が正常に有効化されました。

11. [カタログ] ページまたは [拡張統合] ページで必要な統合タイルの [アクション] メニューを使用して、特定の拡張統合を有効、無効、または削除することもできます。

観測事象の拡張を構成する

脅威インテリジェンスの拡張を 1 つ以上の観測事象で実行し、既知のセキュリティ上の脅威に関連するかどうかを判断します。実行される実装は、アクティブ化した実装によって異なります。

始める前に

必要なロール：sn_sec_tisc.admin

現在、脅威インテリジェンスセキュリティセンターは WHOIS 統合に対してのみ観測事象の拡張をサポートしています。詳細については、「Whois 統合の構成と有効化」を参照してください。

> **注:**
> 拡張統合モジュールは、いずれかの機能をサポートする統合の少なくとも 1 つがアプリケーションにインストールされている場合にのみ表示されます。

このタスクについて

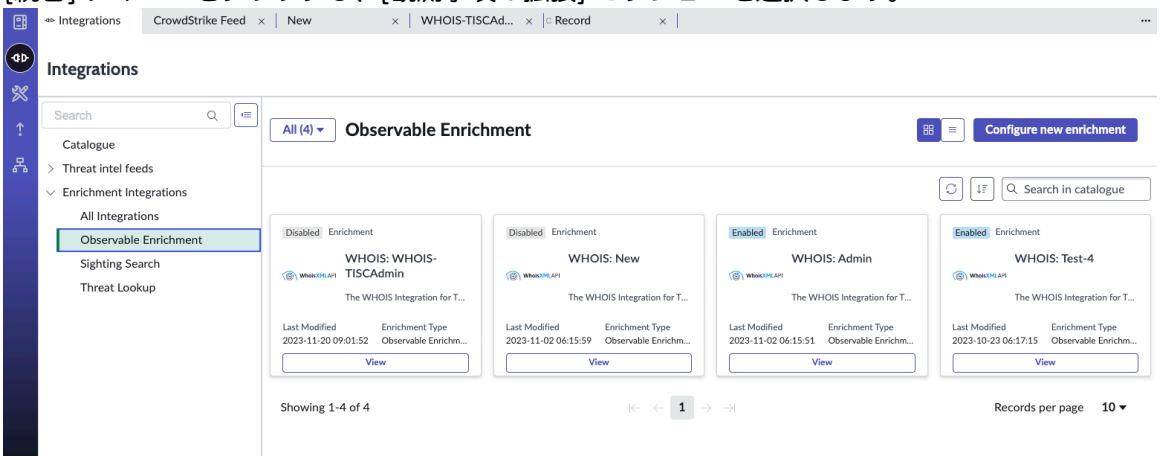
[観測事項の拡張] セクションには、統合タイプが観測事象の拡張である統合のみが含まれます。このセクションには、アクティブ化して使用できる構成済みの各統合実装のカードが表示されます。

自動翻訳

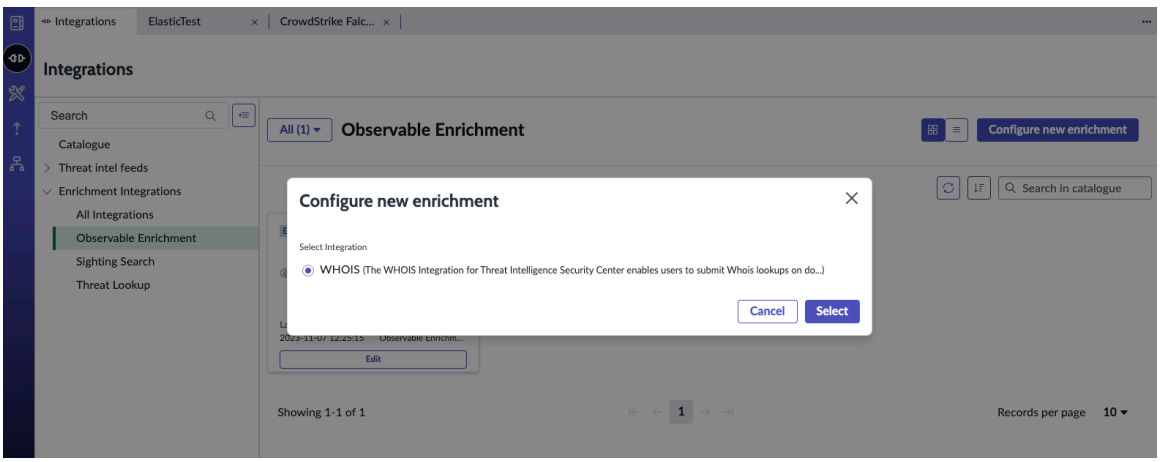
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

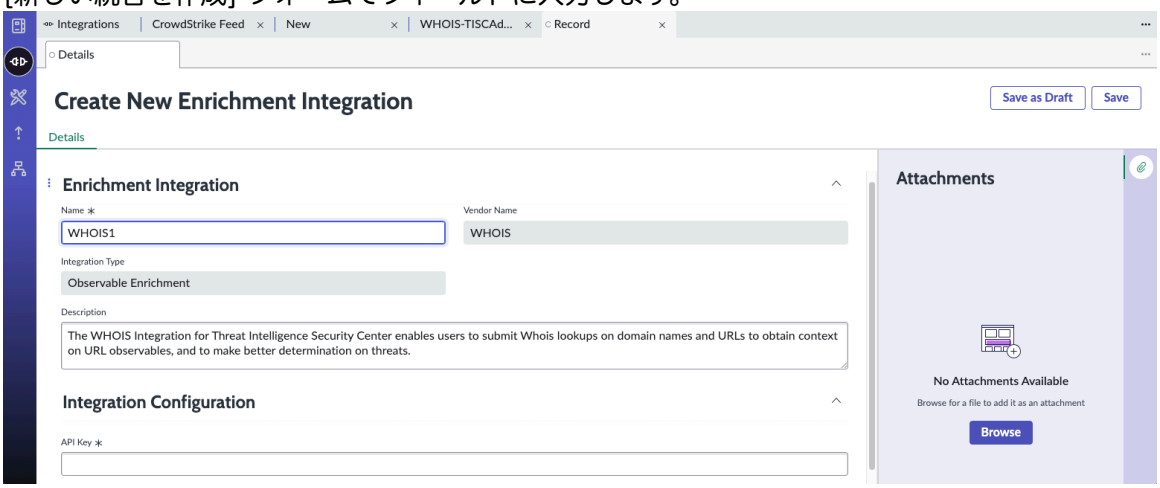
1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [統合] アイコンをクリックし、[観測事項の拡張] セクションを選択します。



3. [新しい拡張を構成 **(Configure new enrichment)]** アクションをクリックします。
これにより、利用可能な統合を表示するポップアップが表示されます。構成する必要がある統合を選択する必要があります。
4. 利用可能な統合のリストから統合を選択し、[選択] をクリックします。
これにより、選択した統合の [新しい拡張統合を作成] ページが表示されます。このページには、選択した統合の詳細がデフォルトで事前入力されています。例：WHOIS 統合。



5. [新しい統合を作成] フォームでフィールドに入力します。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [統合構成] セクションで、要件に基づいて統合の詳細を構成します。
   [統合構成] セクションには、API キー、API クライアント ID またはシークレット、ユーザー名、パスワードなどの構成の詳細が含まれており、それらを入力する必要があります。これらの構成の詳細は、アプリによって異なります。
7. [保存] アクションをクリックして、新しい拡張統合構成を保存および作成します。
   [保存] または [有効化] のアクションをクリックすると、提供された統合構成を使用して統合が検証されます。デフォルトでは、拡張統合のステータスは無効に設定されています。
8. [下書きとして保存する] アクションをクリックすると、拡張構成に加えられた更新のみが保存され、作成はされません。
   構成の詳細が不明な場合は、[下書きとして保存する] オプションを使用できます。構成の詳細を取得したら、残りの情報をドラフトバージョンに入力して作成できます。
9. 拡張統合を有効にするには、[有効化] をクリックします。
   拡張統合が正常に有効化されました。[カタログ] ページまたは [拡張統合] ページで必要な統合タイルの [アクション] メニューを使用して、特定の拡張統合を有効、無効、または削除することもできます。

サイティング検索を構成する

1 つまたは複数の観測事象でサイティング検索を実行し、組織のログで観測事象が観測された回数を判断できます。選択した日数または日付範囲内の観測事象でサイティング検索を実行できます。

始める前に
必要なロール：sn_sec_tisc.admin

> **注:**
> 拡張統合モジュールは、いずれかの機能をサポートする統合の少なくとも 1 つがアプリケーションにインストールされている場合にのみ表示されます。

脅威インテリジェンスセキュリティセンター は、次の統合に対してのみサイティング検索をサポートしています。

- Splunk 検索
- ElasticSearch

このタスクについて
[サイティング検索] セクションには、統合タイプがサイティング検索である統合のみが含まれます。

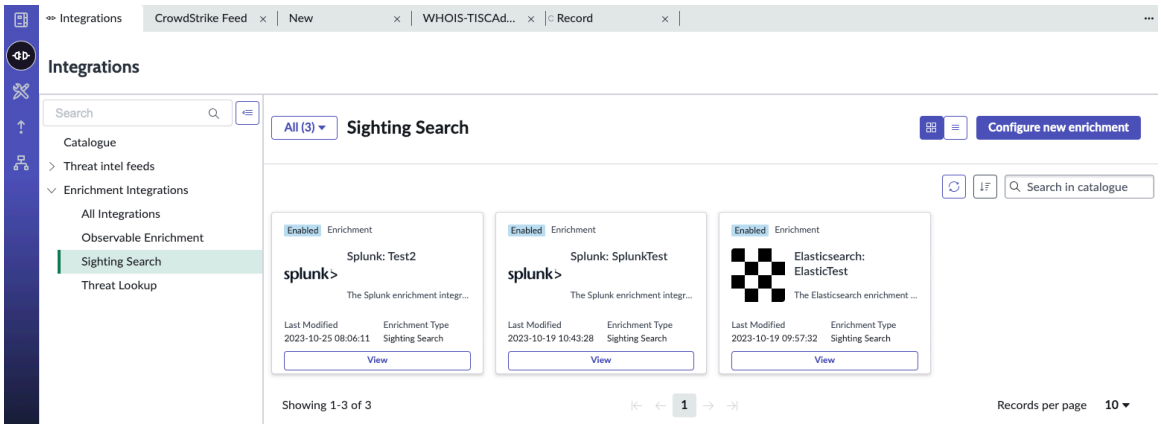
このセクションには、アクティブ化して使用できる構成済みの各統合実装のカードが表示されます。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [統合] アイコンをクリックし、[サイティング検索] セクションを選択します。

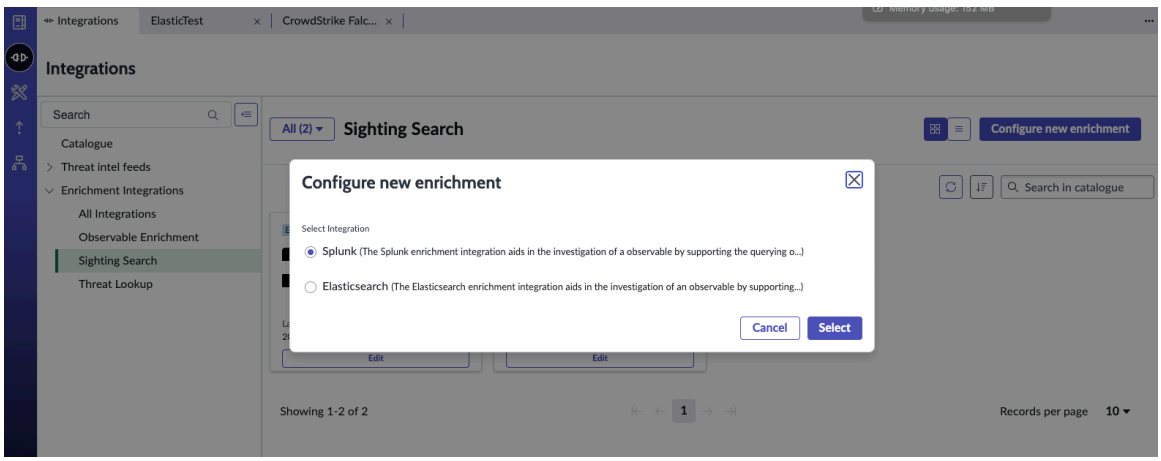
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

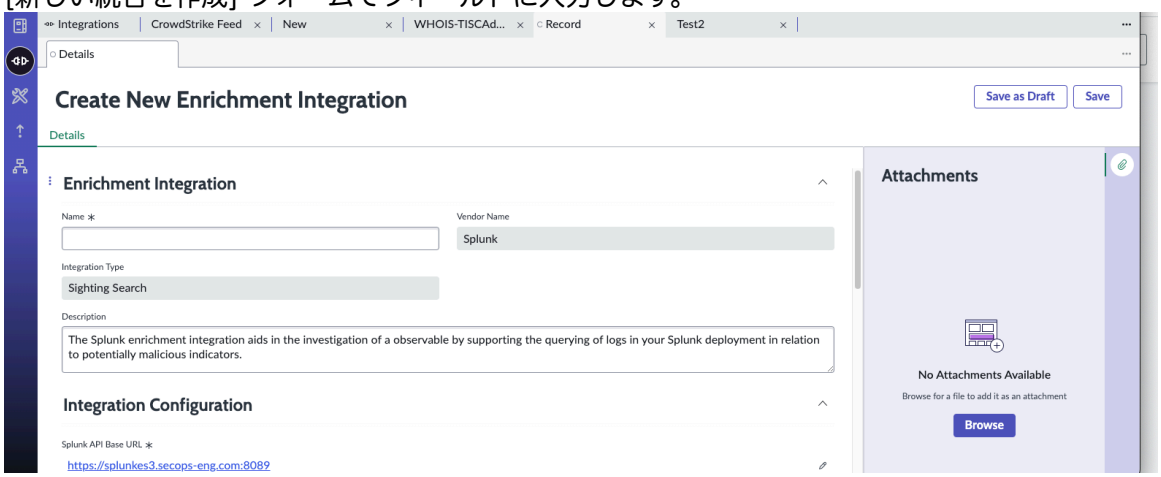


3. [新しい拡張を構成 **(Configure new enrichment)]** アクションをクリックします。
これにより、利用可能な統合を表示するポップアップが表示されます。構成する必要がある統合を選択する必要があります。

4. 利用可能な統合のリストから統合を選択し、[選択] をクリックします。
これにより、選択した統合の [新しい拡張統合を作成] ページが表示されます。このページには、選択した統合の詳細がデフォルトで事前入力されています。次の例は Splunk Integration です。



5. [新しい統合を作成] フォームでフィールドに入力します。



6. [統合構成] セクションで、要件に基づいて統合の詳細を構成します。
[統合構成] セクションには、API キー、API クライアント ID またはシークレット、ユーザー名、パスワードなどの構成の詳細が含まれており、それらを入力する必要があります。これらの構成の詳細は、アプリによって異なります。

7. [保存] アクションをクリックして、新しい拡張統合構成を保存および作成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

指定された詳細が検証され、拡張統合のステータスはデフォルトで無効になっています。

8. [下書きとして保存する] アクションをクリックすると、拡張構成に加えられた更新のみが保存され、作成はされません。
   構成の詳細が不明な場合は、[下書きとして保存する] オプションを使用できます。構成の詳細を取得したら、残りの情報をドラフトバージョンに入力して作成できます。
9. 拡張統合を有効にするには、[有効化] をクリックします。
   拡張統合が正常に有効化されました。[カタログ] ページまたは [すべての統合] ページで必要な統合タイルの [アクション] メニューを使用して、特定の拡張統合を有効にすることもできます。

サイティング検索のクエリの定義

観測事象調査の一環として、環境内の観測事象のまん延を見つけるために使用されるクエリを定義するために、サイティング検索構成を使用できます。

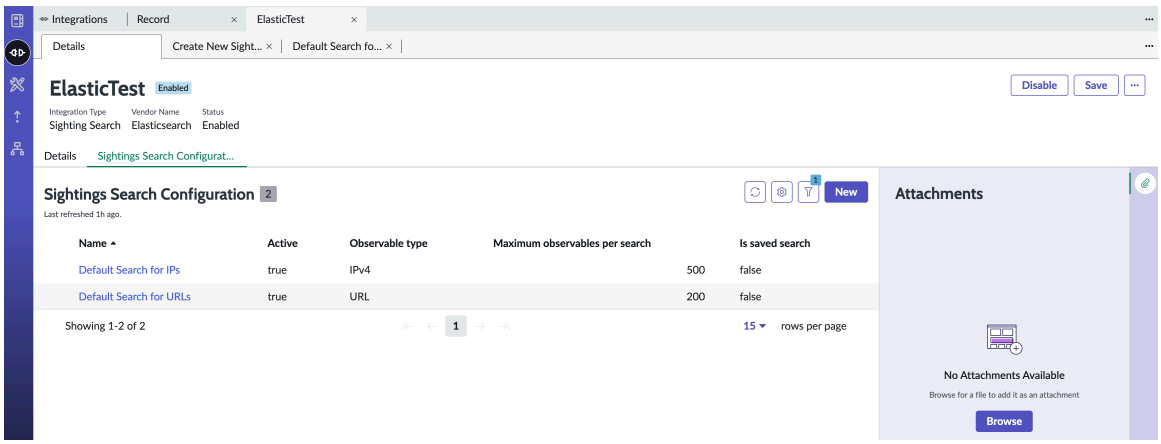
サイティング検索のクエリを表示

必要なロール：sn_sec_tisc.admin

サイティング検索構成を表示するには、次の手順を実行します。

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > 統合.
2. [統合] ページから、 拡張統合 > サイティング検索.
3. サイティング検索構成を表示する統合を探し、[編集] をクリックします。
4. [サイティング検索構成] タブを選択します。

   サイティング検索構成のリストを表示できます。



タブ

5. 必要なサイティング検索構成をクリックして、構成の詳細を表示します。
6. テストサイティング検索クエリを生成するには、[テストサイティング検索クエリを生成] アクションをクリックします。

   注:
   [テストサイティング検索クエリを生成] アクションは、サイティング検索クエリパラメーターを設定した場合にのみ機能します。詳細については、「サイティング検索パラメーターの使用」を参照してください。

7. [テストサイティング検索クエリを生成] ポップアップで、カンマ、改行、タブ、またはパイプ区切り文字を使用して、複数の観測事象を入力または貼り付け、テストクエリを生成します。
8. [生成] をクリックして、テストサイティング検索クエリを生成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

9. [サイティング検索構成] タブでは、次のアクションを実行することもできます。

   a. サイティング検索構成のリストを更新するには、 アイコンをクリックします。

   b. サイティング検索構成でリストアクションを実行するには、 アイコンをクリックします。

      次の 2 つのリストアクションを実行できます。

      - 列の編集：このアクションを実行すると、既存の列を追加または削除し、要件に応じて順序を変更することができます。
      - 幅をリセット：このアクションを実行すると、列の幅をリセットすることができます。

   c. 条件に基づいてサイティング検索構成をフィルタリングするには、 アイコンをクリックします。

      値 1 は、フィルタリングに 1 つの条件が使用されることを示します。

サイティング検索構成を作成する

必要なロール：sn_sec_tisc.admin

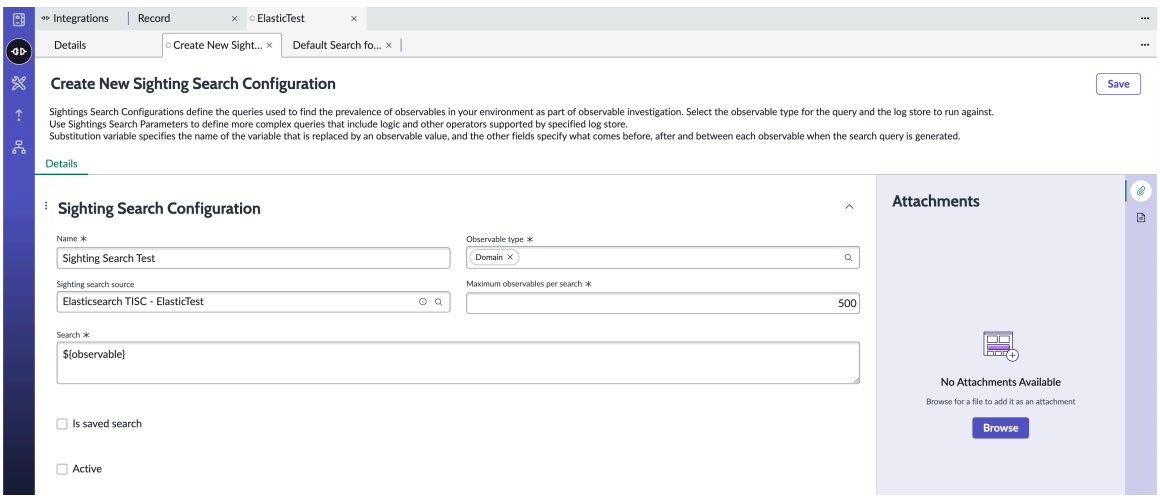
Maximum observables per search = "maximum number of observables that can be substituted in a single search query"
Search = "Search query that should be executed in sighting search source. Search query can contain substitution variables that would be substituted with observables of specific type as configured in sighting search parameters when sighting search query is formed"

サイティング検索構成を作成するには、次の手順を実行します。

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > 統合.
2. [統合] ページから、 拡張統合 > サイティング検索.
3. サイティング検索構成を表示する統合を探し、[編集] をクリックします。
4. [サイティング検索構成] タブを選択します。

   サイティング検索構成のリストを表示できます。

5. サイティング検索構成を作成するには、[新規] をクリックします。



6. フォームの各フィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

サイティング検索構成を作成する

フィールド	説明
名前	サイティング検索構成の名前。
観測事象タイプ	観測事象カテゴリのタイプを定義します。
サイティング検索ソース	統合用に構成されたソースを定義します。
検索あたりの最大観測事象数	検索クエリが複数のクエリに分割される前の観測事象の数。この統合では、この値を 500 に設定します。
検索	クエリを形成するネイティブ検索文字列を追加します。例：${observable}。
保存された検索	保存された検索を実行します。つまり、[名前] フィールドは保存された検索の名前と一致している必要があります。
アクティブ	クエリは、アクティブオプションが選択されている場合にのみ実行されます。

7. [保存] をクリックします。

サイティング検索パラメーターの使用

サイティング検索パラメーターを使用して、指定されたログストアでサポートされているロジックやその他の演算子を含む、より複雑なクエリを定義します。

サイティング検索パラメーターの表示

必要なロール：sn_sec_tisc.admin

サイティング検索パラメーターを表示するには、次の手順を実行します。

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > 統合.

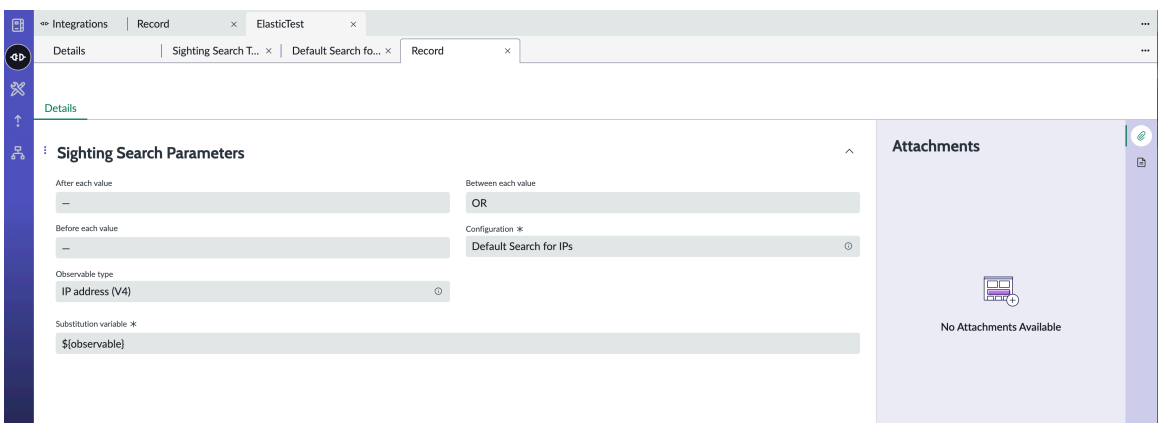
2. [統合] ページから、 拡張統合 > サイティング検索.

3. サイティング検索構成を表示する統合を探し、[編集] をクリックします。

4. [サイティング検索構成] タブを選択します。

サイティング検索構成のリストを表示できます。

5. 必要なサイティング検索構成をクリックして、構成の詳細を表示します。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

6. [サイティング検索パラメーター] タブを選択します。

   サイティング検索パラメーターのリストを表示できます。

7. パラメーターの詳細を表示するには、必要なサイティング検索パラメーターをクリックします。
8. [サイティング検索パラメーター] タブでは、次のアクションを実行することもできます。

   a. サイティング検索パラメーターのリストを更新するには、 アイコンをクリックします。

   b. サイティング検索パラメーターでリストアクションを実行するには、 アイコンをクリックします。

      列の編集：このアクションを実行すると、既存の列を追加または削除し、要件に応じて順序を変更することができます。

   c. 条件に基づいてサイティング検索パラメーターをフィルタリングするには、 アイコンをクリックします。

      値 1 は、フィルタリングに 1 つの条件が使用されることを示します。

サイティング検索パラメーターの作成

クエリ生成の例

```
Configured Query: ${Observable}

Observables Substitutes for Sightings search: Obs1 , Obs2

Query: {Before each Value}Obs1{After each Value}{Between each value}{Before each
 Value}Obs2{After each Value}


Let observables are: 172.32.31.41 & 192.168.10.12

Query Formed with below configuration will be: “ip_address = 172.32.31.41 OR ip_address =
 192.168.10.12”
```

サイティング検索パラメーターを作成するには、次の手順を実行します。

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > 統合.
2. [統合] ページから、 拡張統合 > サイティング検索.
3. サイティング検索構成を表示する統合を探し、[編集] をクリックします。
4. [サイティング検索構成] タブを選択します。

   サイティング検索構成のリストを表示できます。

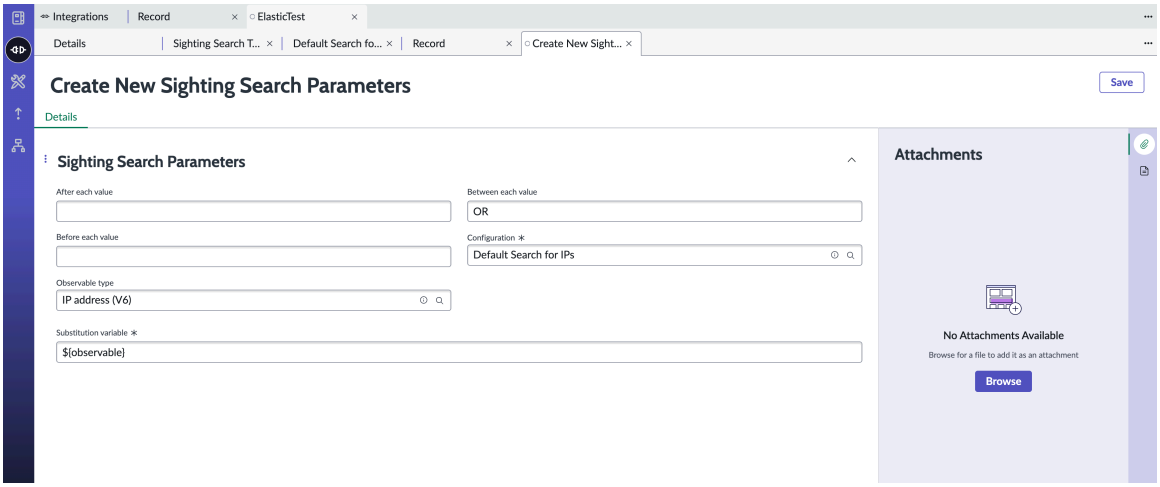
5. 必要なサイティング検索構成をクリックして、構成の詳細を表示します。
6. [サイティング検索パラメーター] タブを選択します。

   サイティング検索パラメーターのリストを表示できます。

7. サイティング検索パラメーターを作成するには、[新規] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



8. フォームの各フィールドに入力します。

サイティング検索パラメーターの作成

フィールド	説明
各値の後	検索クエリが生成される際の各観測事象の後のサイティング検索パラメーター。
各値の間	検索クエリが生成される際の各観測事象間のサイティング検索パラメーター。例：OR。
各値の前	検索クエリが生成される際の各観測事象の前のサイティング検索パラメーター。
構成	検索パラメーターの構成の詳細。
観測事象タイプ	観測事象カテゴリのタイプを定義します。
代替変数	観測事象値に置き換えられる変数の名前を指定します。

9. [保存] をクリックします。

脅威のルックアップを構成する

選択した観測事象に対してルックアップを実行するように脅威のルックアップを構成できます。観測事象が脅威インテリジェンスによって認識されるタイプである場合、観測事象でマルウェアがスキャンされ、結果が返されます。1 つ以上の観測事象で脅威のルックアップを実行して、観測事象の悪意を判断できます。

始める前に

必要なロール：sn_sec_tisc.admin

注:
拡張統合モジュールは、いずれかの機能をサポートする統合の少なくとも 1 つがアプリケーションにインストールされている場合にのみ表示されます。

脅威インテリジェンスセキュリティセンターは、次の統合に対してのみ脅威のルックアップをサポートしています。

- VirusTotal
- CrowdStrike Intelligence

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

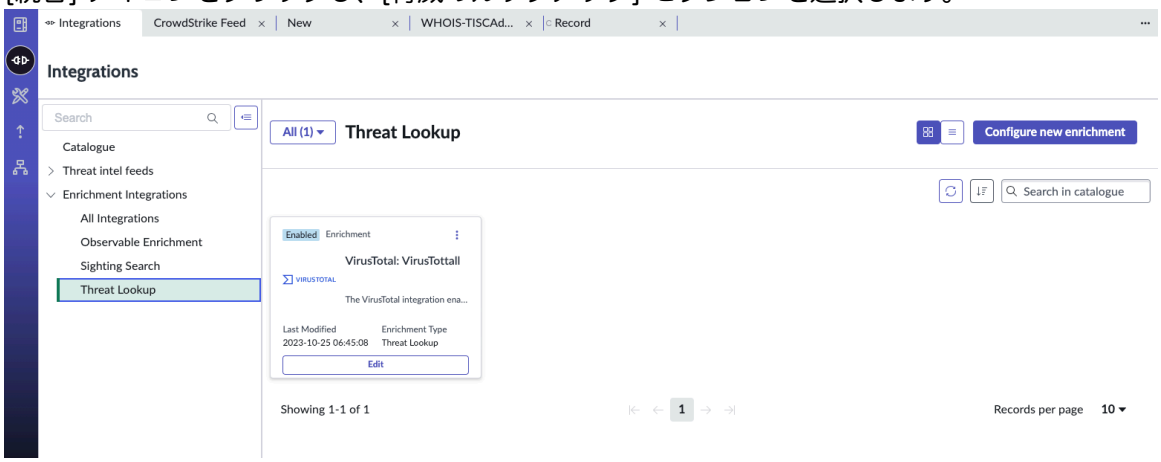
詳細については、「脅威のルックアップ」を参照してください。

このタスクについて
[脅威のルックアップ] セクションには、統合タイプが脅威のルックアップである統合のみが含まれます。

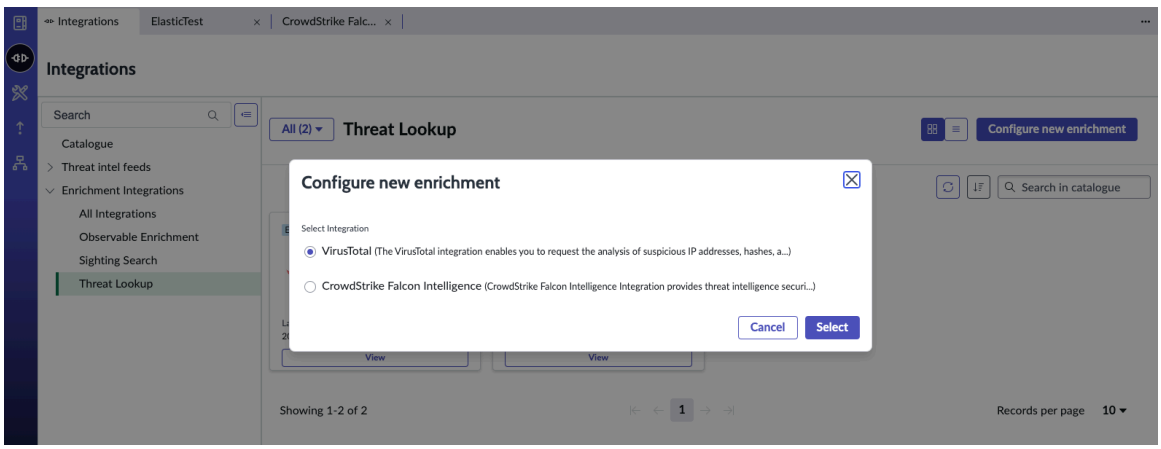
このセクションには、アクティブ化して使用できる構成済みの各統合実装のカードが表示されます。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [統合] アイコンをクリックし、[脅威のルックアップ] セクションを選択します。

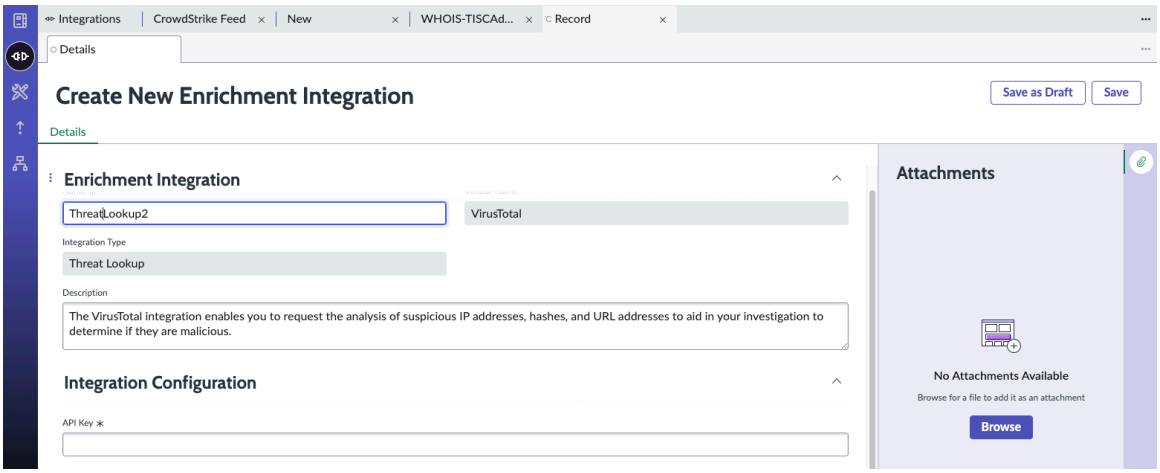


3. [新しい拡張を構成 **(Configure new enrichment)]** アクションをクリックします。
これにより、利用可能な統合を表示するポップアップが表示されます。構成する必要がある統合を選択する必要があります。
4. 利用可能な統合のリストから統合を選択し、[選択] をクリックします。
これにより、選択した統合の [新しい拡張統合を作成] ページが表示されます。このページには、選択した統合の詳細がデフォルトで事前入力されています。例：VirusTotal 統合。



5. [新しい統合を作成] フォームでフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



6. [統合構成] セクションで、要件に基づいて統合の詳細を構成します。
   [統合構成] セクションには、API キー、API クライアント ID またはシークレット、ユーザー名、パスワードなどの構成の詳細が含まれており、それらを入力する必要があります。これらの構成の詳細は、アプリによって異なります。
7. [保存] アクションをクリックして、新しい拡張統合構成を保存および作成します。
   指定された詳細が検証され、拡張統合のステータスはデフォルトで無効になっています。
8. [下書きとして保存する] アクションをクリックすると、拡張構成に加えられた更新のみが保存され、作成はされません。
   構成の詳細が不明な場合は、[下書きとして保存する] オプションを使用できます。構成の詳細を取得したら、残りの情報をドラフトバージョンに入力して作成できます。
9. 拡張統合を有効にするには、[有効化] をクリックします。
   拡張統合が正常に有効化されました。[カタログ] ページまたは [拡張統合] ページで必要な統合タイルの [アクション] メニューを使用して、特定の拡張統合を有効、無効、または削除することもできます。

脅威のルックアップ評価計算ツールの表示

脅威のルックアップ検索計算ツールを表示して、統合の観測事象結果を計算することができます。

始める前に

必要なロール：sn_sec_tisc.admin

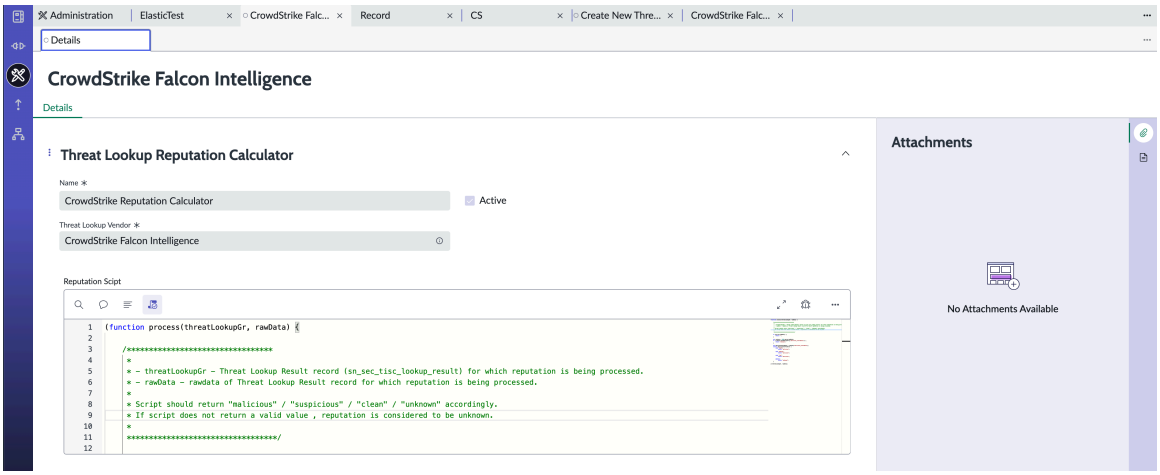
脅威のルックアップ評価計算ツールについて、詳細は「脅威のルックアップ評価計算ツールの管理」を参照してください。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. [脅威のルックアップ評価計算ツール] セクションを選択します。
   脅威のルックアップ評価計算ツールのリストを表示することができます。
3. 必要な脅威のルックアップ評価計算ツールをクリックして、計算ツールの詳細を表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [脅威のルックアップ評価計算ツール] セクションでは、次のアクションを実行することもできます。

   a. 脅威のルックアップ評価計算ツールのリストをリフレッシュするには、をクリックします。

   b. 脅威のルックアップ評価計算ツールでリストアクションを実行するには、 アイコンをクリックします。

      次の 2 つのリストアクションを実行できます。

      - 列の編集：このアクションを実行すると、既存の列を追加または削除し、要件に応じて順序を変更することができます。
      - 幅をリセット：このアクションを実行すると、列の幅をリセットすることができます。

   c. 条件に基づいて脅威のルックアップ評価計算ツールをフィルタリングするには、 アイコンをクリックします。

      値 1 は、フィルタリングに 1 つの条件が使用されることを示します。

TISC セキュリティツール - EDR

TISC Endpoint Detection and Response (EDR) 統合は、エンドポイントレベルでのセキュリティ脅威の特定と対処に重点を置いています。

EDR ネットワークソリューションは、新たな脅威を予測して未然に防ぎ、組織全体のセキュリティ体制の強化を支援します。

TISC は、EDR などの他のセキュリティツールと統合することで、エンドポイントでプロアクティブな脅威監視を可能にし、進化する脅威に対する全体的なセキュリティ体制とレジリエンスを強化します。

関連情報

CrowdStrike Falcon EDR 統合

CrowdStrike Falcon EDR 統合

CrowdStrike Falcon EDRとの統合により、TISCのインテリジェンスに基づく継続的な監視とリアルタイムのアラートが可能になります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

この統合により、セキュリティ運用を簡素化し、組織のビジネスに対する潜在的なリスクを軽減できます。

Crowdstrike Falcon EDR 統合の構成

CrowdStrike Falcon EDR 統合を使用する前に、ServiceNow Store Store からダウンロードし、適切なクライアント ID とクライアントシークレットを追加する必要があります。

始める前に
必要なロール：sn_sec_tisc.admin

- 脅威インテリジェンスセキュリティセンターアプリケーションをインストールしてアクティブ化する必要があります。
- Falcon コンソールから API クライアント ID と API クライアントシークレットを取得しますCrowdStrike
- CrowdStrike Falcon ポータル API スコープで、**IOC** 管理:読み取りおよび書き込みアクセスを有効にします。

手順

1. 自身のインスタンスを使用して、脅威インテリジェンスセキュリティセンターにアクセスします。
2. から統合をダウンロードします ServiceNow Store.
3. 選択 統合 > セキュリティツール > **EDR**.
4. [新しいセキュリティツールを構成] をクリックして CrowdStrike Falcon EDR 統合を構成します。
5. **[CrowdStrike Falcon EDR]** オプションを選択します。
6. [新しいセキュリティツールを構成 (Configure new security tool)] フォームのフィールドに入力します。

新しい拡張統合を作成

フィールド	説明
名前	新しいセキュリティツール統合の名前を入力します。例: CrowdStrike Falcon EDR。
ベンダー名	ベンダーの名前。選択したベンダーの詳細がデフォルトで入力されます。例: CrowdStrike Falcon EDR。
説明	新しいセキュリティツール統合の説明を入力します。
統合タイプ	統合タイプを表示するオプション。
統合カテゴリ	統合カテゴリを表示するオプション。
データ連携の構成	
ベース URL	ベース URL は CrowdStrike API のベース URL です。デフォルト値は https://api.crowdstrike.com です。詳細については、「https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis#k9578c40」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
クライアント ID	CrowdStrike から取得したクライアント ID。詳細については、「https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis」を参照してください。
クライアントシークレット	CrowdStrike から取得したクライアントシークレットキー。詳細については、「https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis」を参照してください。
すべてのタイプの観測事象の有効期間 (日数)	任意のタイプの観測事象が CrowdStrike EDR に送信されるときに適用される有効期限 (日数)。 注: このオプションは、特定の観測事象タイプに有効期限が設定されていない場合の代替有効期間です。
IP 観察事項の有効期限	観測事象の IP タイプが CrowdStrike EDR に送信されるときに適用される有効期限 (日数)。
ドメイン観測事象の有効期限	観測事象のドメインタイプが CrowdStrike EDR に送信されるときに適用される有効期限 (日数)。
ハッシュ観測事象の有効期限	観測事象が CrowdStrike EDR に送信されるときにハッシュタイプの観測事象に適用される有効期限 (日数)。

7. **[Save** (保存)] をクリックします。
   統合の詳細が検証されます。デフォルトでは、 CrowdStrike EDR 統合のステータスは無効になっています。
8. [有効化] をクリックして、 CrowdStrike EDR 統合を有効にします。

   注:
   CrowdStrike Falcon EDR 統合では、複数の構成が許可されています。

観測事象を **EDR** に送信

観測事象を EDR セキュリティツールに送信します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

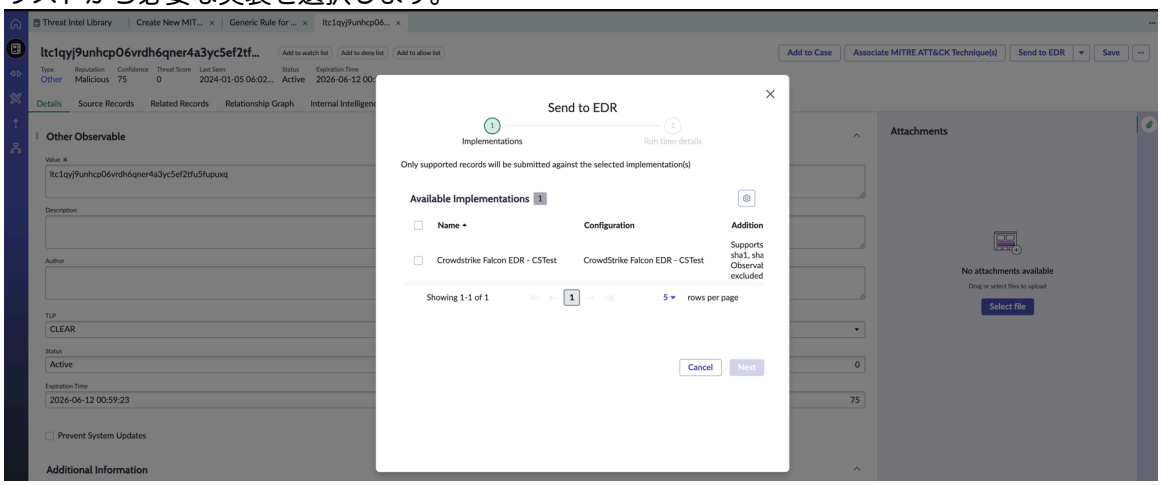
1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. 脅威インテリジェンスライブラリアイコンをクリックします。
3. 検索項目 観察事項 > すべての観察事項.
4. 任意の観測事象レコードを開きます。
5. **[EDR** に送信] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

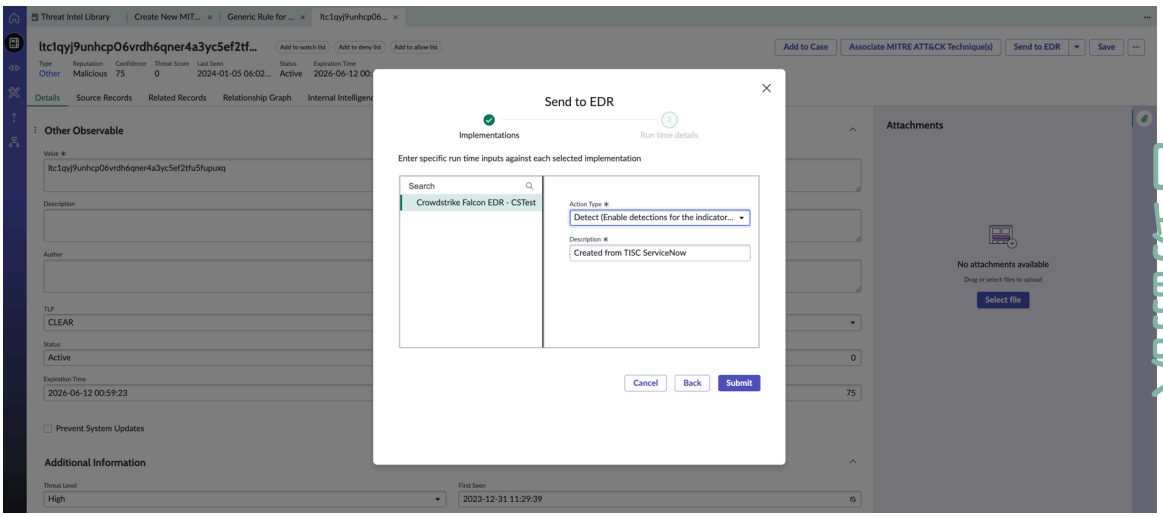
[EDR 実装に送信] モーダル画面が表示されます。

6. リストから必要な実装を選択します。



7. [次へ] をクリックします。

8. 実装の [アクションタイプ] や [説明] などの実行時の詳細を選択します。



実装実行時の詳細時に CrowdStrike に使用可能なオプションは次のとおりです。

- アクションなし (後で使用するためにインジケーターを保存しますが、アクションは実行しません):観測事象フォームビューでは、観測事象の脅威の重大度は CrowdStrike Falcon EDR ではオプションです。
- 検出 (レコードの脅威の重大度でインジケーターの検出を有効にする):観測事象フォームビューでは、 CrowdStrike Falcon EDR に脅威の重大度が必須です。観測事象の脅威の重大度は、選択した観測事象について空にすることはできません。

9. [**Submit** (送信)] を選択します。
選択したアクションが実行され、観測事象の EDR への送信の実行が開始されたという情報メッセージが表示されます。

注:

- 実行が開始または完了すると、作業メモがフォームビューのアクティビティストリームにポストされます。
- **EDR** に送信 アクションは、ケースレコードの [アーティファクト] タブの [観測事象] リストでも使用できます。詳細については、「ケースまたはケースタスクにアーティファクトを追加する」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

TISC セキュリティツール - ファイアウォール

TISC Security Tools - ファイアウォールは、ネットワークへの不正アクセスを防止します。Palo Alto と TISC の統合により、外部動的リスト (EDL) 機能と ServiceNow 脅威インテリジェンスデータを使用して、悪意のある IP アドレス、URL、およびドメインをブロックできます。

TISC 内では、 Palo Alto Networks などの他のセキュリティツールと統合することで、組織全体のネットワークセキュリティを強化します。

Palo Alto Networks 統合

Palo Alto Networks 統合を構成すると、脅威アナリストは、悪意のある IP アドレス、URL、ドメインを外部動的リスト (EDL) に追加したり、悪意がないまたはクリーンであることが確認された後にこれらのエントリを EDL から削除したりできます。

EDL は、外部 Web サーバーでホストされるテキストファイルです。この統合では、この Web サーバーは Now Platform インスタンスです。これにより、Palo Alto Networks ファイアウォールは、リストに含まれるオブジェクト、IP アドレス、URL、およびドメインをインポートできます。

Palo Alto Networks の新しい EDL を作成

Palo Alto Networks の新しい外部動的リスト (EDL) を作成します。EDL を作成したら、その EDL のエントリーの作成を開始できます。

始める前に
必要なロール：sn_sec_tisc.admin

手順

1. 新しく構成した Palo Alto NGFW 構成を保存したら、[**EDL**] セクションに移動します。
2. [新規] をクリックして、新しい外部動的リスト (EDL) を作成します。
3. フォームのフィールドに入力します。

Palo Alto Networks ファイアウォール外部動的リストフォーム

フィールド	説明
名前	Palo Alto Networks ファイアウォール動的リスト名。
観察事項タイプ	この EDL が受け付ける観測事象タイプ (IP (CIDR を含む)、URL、またはドメイン) を選択します。
有効期限（日数）	EDL の有効期間。 0 (デフォルト) は、EDL エントリーが無期限であることを示します。この値を変更すると、このエントリーは入力した日数の間有効になります。入力できる最小値は 1 で、最大値はありません。 たとえば、11 月 1 日の午後 2 時 1 分に 30 日と入力すると、EDL は 11 月 30 日の午後 2 時 1 分に期限切れになります。 この EDL のすべてのエントリーは、個々のエントリー単位で値を上書きしない限り、デフォルトでこの値を継承します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
変更要求を作成	このチェックボックスはデフォルトでオンになっており、Now Platform インスタンスに変更要求と変更タスクが自動的に作成され、EDL レコードに添付されます。 変更要求は、Palo Alto Networks 次世代ファイアウォールサーバーで EDL リスト取得 URL を設定するために使用されます。 ファイアウォールアドミニストレーターがファイアウォールポリシーまたはルールの変更に Now Platform も使用している場合は、このオプションをお勧めします。要求を作成して、要求がクローズされると、EDL リストは自動的に有効になります。
説明	Palo Alto Networks ファイアウォール動的リストの説明。名前には通常、この EDL にあると予想されるサイトと観測事象のタイプが含まれており、このフィールドを使用して詳細を確認できます。
変更要求	[変更要求を作成] チェックボックスをオンにすると、EDL が保存された後、変更要求番号が Now Platform インスタンスに表示されます。 [変更要求の作成] チェックボックスをオフにすると、このフィールドは表示されません。
IP アドレスとサブネットアドレスを 1 つのエントリに結合する	IP アドレスとサブネットアドレスの両方を 1 つのエントリに結合するオプション。 このチェックボックスをオンにし、CIDR タイプの IP が追加されると、CIDR 範囲内にある既存のエントリーが自動的に削除されます。例:EDL に値が 192.168.1.1 のエントリーがあり、CIDR 値 192.168.1.0/24 が同じ EDL に追加された場合、最初の IP アドレスエントリーは新しいエントリーの CIDR 範囲内にあるため、削除されます。 **注:** このオプションは、[観測事象タイプ] で [IP] を選択した場合にのみ表示されます。
EDL 取得 URL	Palo Alto Networks ファイアウォールアドミニストレーターが Palo Alto Networks ファイアウォールの構成に使用する URL リンクが自動的に生成され、表示されます。

4. 必要に応じて、さらに EDL を作成して追加します。
   EDL が [Palo Alto Networks 外部動的リスト] リストに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連情報

Palo Alto EDL 承認ルール

Palo Alto EDL 承認ルール

承認ルールを使用すると、ユーザーは EDL エントリーを承認または却下するために必要な承認ワークフローをアクティブ化できます。

始める前に
必要なロール：sn_sec_tisc.admin

このタスクについて
TISC アドミニストレーターは、これらの承認ルールを定義して、承認要求に同意します。TISC アドミニストレーターは、ここから複数レベルの承認を定義することもできます。

手順

1. 新しく構成した Palo Alto NGFW 構成を保存したら、[**EDL** 承認ルール] セクションに移動します。
2. [新規] をクリックして、新しい承認ルールを作成します。
   次のルールは、Palo Alto NGFW 統合のベースシステムで事前設定されたルールです。

事前設定された **EDL** 承認ルール

名前	説明	EDL アクション
EDL に追加するための承認ルール	この承認ルールにより、ユーザーは EDL にエントリーを追加するための承認ワークフローをアクティブ化できます。	EDL へ追加
EDL から削除する承認ルール	この承認ルールにより、ユーザーは EDL からエントリーを削除するための承認ワークフローをアクティブ化できます。	EDL から削除

3. 必要に応じて、フォームのフィールドに入力します。

新しい **EDL** 承認ルールを作成

フィールド	説明
名前	承認ルールの名前。
EDL アクション	EDL エントリーを追加または削除するオプション。
EDL	承認が必要な EDL を選択します。これを空のままにすると、すべての EDL が含まれます。
説明	承認ルールの説明を入力します。
承認が必要なユーザーまたはグループを選択	
ユーザー	承認が必要なユーザーを選択します。
グループ	承認が必要なグループを選択します。
承認者を選択	
ユーザー	承認するユーザーを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
グループ	承認するグループを選択します。
通知	
承認時に要求者に通知	EDL の承認時に要求者に通知するには、このチェックボックスをオンにします。
却下時に要求者に通知	EDL の却下について要求者に通知するには、このチェックボックスをオンにします。

4. [保存] をクリックして、承認ルールを検証して保存します。
5. [有効化] をクリックして、承認ルールを有効にします。

観測事象を **EDL** に追加

IP、ドメイン、ハッシュなどの観測事象を外部動的リスト (EDL) に追加します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順
1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [脅威アナリストワークベンチ **(Threat Analyst Workbench)]** アイコンをクリックします。
3. 検索項目 観察事項 > すべての観察事項.
4. 任意の観測事象レコードを開きます。
5. **[EDL** に追加] をクリックします。
   [EDL に追加] モーダル画面が表示されます。

EDL から観測項目を削除

EDL から観測事象を削除します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順
1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [脅威アナリストワークベンチ **(Threat Analyst Workbench)]** アイコンをクリックします。
3. 検索項目 観察事項 > すべての観察事項.
4. 任意の観測事象レコードを開きます。
5. 「EDL から削除」をクリックします。
   [EDL から削除] モーダル画面が表示されます。

Palo Alto Networks の **EDL** エントリーの承認

外部動的リスト (EDL) エントリーの承認は、事前設定の一部です。EDL エントリーを承認してから、ファイアウォールで EDL エントリーを取得してセキュリティポリシーを適用するために、EDL エントリーをアクティブ化する必要があります。

始める前に
必要なロール：sn_sec_tisc.admin

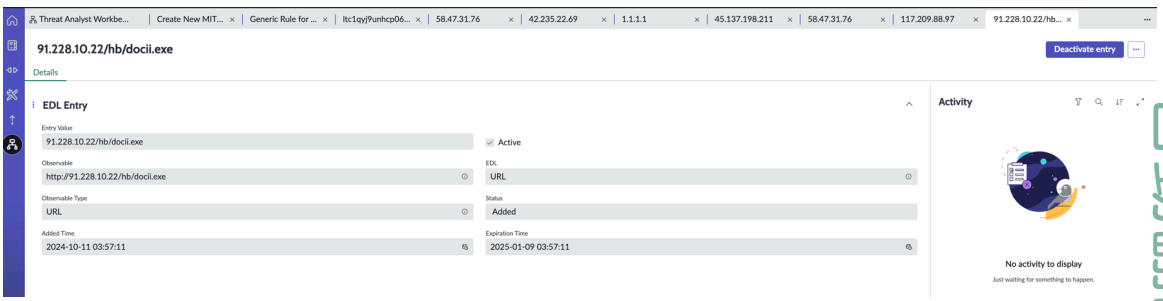
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
承認プロセスが有効になっている場合、EDL エントリーは承認されるまで EDL でアクティブ化または非アクティブ化されません。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > 脅威アナリストワークベンチ.
2. **[PAN NGFW]** セクションにドリルダウンし、承認する EDL レコードを選択します。
3. [自分の承認] に移動します。
4. 承認する EDL レコードを選択します。
5. [承認] をクリックします。
6. [自分の承認要求] で、[ステータス] 列のアイテムをクリックして開きます。
7. EDL エントリーを承認するオプションを選択します。
   EDL エントリーを承認してアクティブ化すると、Palo Alto Networks は次の取得間隔の後に EDL エントリーを取得します。エントリーが取得されると、その時点から観測事象がブロックされます。次の図では、[アクティブ] チェックボックスがオンで、ステータスが [追加] になっており、作業メモに要求が承認されたことが示されています。



TISC API リファレンス

次のテーブルでは、拡張に役立つ API エンドポイントのリファレンスを確認できます。

TISC API

API	説明
TISC API - POST /sn_sec_tisc/threat_intel_data/observables	この API は、観測事象と他の関連する脅威インテリジェンスデータとの関係性などの観測事象データを取得します。
TISC API - POST /sn_sec_tisc/threat_intel_data/add_observables	この API は、観測事象ソースレコードを作成して、有効な観測事象を脅威インテリジェンスセキュリティセンターアプリケーション (TISC) に追加します。

TISC API エンドポイントの詳細については、 API 実装に関する REST API リファレンスセクションにある TISC API および servicenow.com/docs のリファレンスを参照してください。

TISC Add-on for Splunk の概要

脅威インテリジェンスセキュリティセンター (TISC) for Splunk アプリでは、TISC と Splunk が統合され、ユーザーは TISC から最新の脅威インテリジェンスを Splunk にシームレスにインポートして、アラートを監視および強化できます。ユーザーはインジケーターコレクションを構成し、検索を

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

実行し、ダッシュボードを利用して検索一致とインジケーターコレクションを効果的に分析できます。

TISC と Splunk の統合

脅威インテリジェンスセキュリティセンター (TISC) と Splunk の統合により、ユーザーは関連する脅威インテリジェンスの観測事象データをフィルタリングしてSplunkに取り込むことができます。Splunk内で、ユーザーはこのデータを使用してセキュリティアラートを生成できます。

必要なロール:Splunk アドミン

TISC アドオンアプリケーションを使用すると、TISC インスタンスから観測事象をプルできる間隔を設定できます ServiceNow 。

この間隔は、アプリケーションが観測事象データを ServiceNow して取得するための要求を行うことができる頻度を決定します。また、フィルターを定義して適用し、 ServiceNow TISC インスタンスからプルする観測事象を指定することもできます。

観測事象が ServiceNow からプルされると、観測事象データは Splunk の KV ストア (Key-Value ストア) に保存され、プルされた観測事象のセットに対して相関ルールをさらに書き込むことができます。

ServiceNow TISC インスタンスでのユーザーの作成

有効なユーザーロール (sn_sec_tisc.api_obs_read_access) を使用して、 ServiceNow TISC インスタンスにユーザーを作成できます。

TISC アドオンアプリを Splunk にインストール

詳細については、「ユーザーへのロールのアサイン」を参照してください。

必要なロール:Splunk admin

1. Splunk にログインし ます。
2. 次のように移動する。 アプリ > アプリケーションを管理 または、[管理] 歯車アイコンをクリックします。
3. **Splunk** の脅威インテリジェンスセキュリティセンターアプリを検索してインストールします。
4. インストールすると、アプリケーションがアプリのリストの下に表示されます。

での TISC アドオンの構成 Splunk

以下の手順に従って、アプリケーションを構成します。

始める前に
必要なロール:Splunk アドミン

このタスクについて
次の手順では、 Splunk での TISC アドオンの構成について説明します。

手順

1. 左側のナビゲーションから **Splunk** 向け脅威インテリジェンスセキュリティセンター アプリを検索します。
2. [アクション] 列の [設定] をクリックします。
   [構成] ページが表示され、ServiceNow TISC アカウントを設定できます。
3. [**Add**] を選択します。
4. フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
口座の追加	
名前	アカウントの一意の名前。
ユーザー名	ServiceNow アカウントのユーザー名を入力します。上記の手順でロールの作成時に作成された sn_sec_tisc.api_obs_read_access と同じユーザー名を使用できます。
Password (パスワード)	アカウントのパスワード ServiceNow 入力します。
インスタンス URL	ServiceNowインスタンスの URL アドレスを入力します。

5. [追加] をクリックします。
ServiceNowインスタンスアカウントがSplunkに追加されます。
6. [入力] ページに移動してコレクションを作成し、ServiceNowアカウントのデータ入力を管理します。
7. [新規入力を作成] をクリックします。
ServiceNowアカウントに入力を追加するための [入力を追加] ダイアログボックスが表示されます。

   入力セットが定義されると、アプリケーションはその情報を TISC インスタンスに送信して、基準を満たす特定の数の観測事象を取得します。
8. 必要に応じて入力の詳細を入力します。

フィールド	説明
名前	入力の一意の名前。例:悪意のある IP リスト。
アカウント	ServiceNow アカウントのユーザー名を入力します。上記の手順で sn_sec_tisc.api_obs_read_access ロールで作成されたユーザーに使用されるのと同じユーザー名を使用できます。
間隔	TISC からデータを取得する時間間隔を秒単位で設定します。
有効期限 (日数)	有効期限を日数で設定するオプション。 **注:** サンプルの有効期限は 30 日に設定されています。たとえば、特定の日付にデータをプルすると、10,000 件のレコードセットが取得される場合があります。これらのレコードは、 Splunk 内の KV (キー値) ストアに格納されます。取り込み日から、レコードは 30 日間保持されます。31日目になると、KVストアから自動的に削除されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
無期限	取り込まれたレコードを期限切れにしない場合は、このオプションを選択します。
フィルター	インポートするデータをフィルタリングする条件を定義します。 フィルター条件を設定するには、脅威スコア、信頼性レベル、タイプなどのフィールドに基づいて基準を定義します。 単純なフィルター条件の場合は、このフィルタリングオプションを使用できます。ただし、フィルター条件がより複雑で、高度なフィルタリングの場合は、JSON フィルターを追加することを選択できます。 ○ 使用できる整数演算子は次のとおりです。 "=", "!=", ">", "<", ">=", "<=" ○ 使用できる文字列演算子は次のとおりです。 "="、"!="、"IN" 以下は、単純なフィルターの例です。 {Sample filter format: Allowed Tokens: "threat_score", "confidence", "reputation", "type", "value". Allowed Integer Operators: "=", "!=", ">", "<", ">=", "<=". Allowed String Operators: "=", "!=", "IN". Example: reputation IN ("clean","suspicious","malicious") AND threat_score > 90 AND confidence > 90 AND type = "ip_v4_address"}
JSON	JSON ベースのフィルターを使用すると、より複雑な条件を定義できます。JSON オブジェクトのステータスがアクティブである必要があります。 [**JSON** フィルター] チェックボックスをオンにすると、JSON を使用してフィルター条件を適用できる詳細フィルターに切り替わります。

詳細フィルターの例:

```
{"boolean_operator":"AND","filters":[{"field_name":"reputation","operator":"IN","field_value":"clean,suspicious,malicious"},{"field_name":"threat_score","operator":">","field_value":"90"},{"field_name":"confidence","operator":">","field_value":"90"},{"field_name":"type","operator":"=","field_value":"ip_v4_address"}]}
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> アカウントはデフォルトでアクティブになっていますが、入力はデフォルトでは非アクティブになっているため、データのインポートを開始するにはアカウントを有効にする必要があります。可能なフィルターについては、「脅威 インテリジェンスセキュリティセンター (TISC) アプリケーションに観測事象ソースレコードを追加する 」のObservable_filters セクションを参照してください。

9. [追加] をクリックして入力を追加します。
10. [クローンまたはコピー] をクリックして、既存のアカウントに基づいて新しいアカウントをコピーして作成します。
同じ基準を使用してデータをインポートするときに重複エントリが作成されないように、クローンを作成する前に入力が非アクティブ化されていることを確認してください。
11. データがプルされると、次の情報が取得され、TISC からプルされたレコードとともに Splunk 内の KV ストアに保存されます。

フィールド	説明
脅威スコア	レコードに関連付けられた脅威のレベルを示すスコア。
信頼性	脅威スコアの精度に関連付けられた信頼性レベルを示します。
有効期限	有効期限が切れる前にアプリケーションでレコードが有効な期間。
脅威レベル	脅威の重大度レベルを示します。
評判	関連するエンティティの評判を示します。
更新者	レコードを最後に更新したユーザーに関する情報を提供します。
更新時間	レコードが最後に更新されたタイムスタンプを示します。
作成時刻	レコードの作成時刻を示します。
Days_till_expiry	レコードが KV ストアから削除されるまでの日数を示します。
Source_reported_score	TISC から報告されたソーススコア。
Sys_id	TISC を介して受信されるレコードの Sys ID。
脅威の重大度	観測事象の脅威の重大度を示します。
値	レコードの値。たとえば、IP、ハッシュなどです。

これらのフィールドは、条件で定義された他のフィールドとともに Splunk で利用可能になり、[検索] タブを使用して表示、検索、および分析できます。

Splunk でのデータストレージ

このセクションでは、TISC が Splunk の Key-Value ストア内のデータストレージとの連携時にルックアップをどのように利用するかについて説明します。これらのルックアップが Splunk 内でどのように構成および取得されるかについて詳しく説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ルックアップ	ルックアップの説明
tisc_store_lookup	受信レコードの検索に使用される KV ルックアップの名前。
tisc_kv_store	データが存在する KV ストアの名前。
inputlookup <lookup_name>" example : | inputlookup tisc_store_lookup	KV ストア内のレコードを検索するクエリ。

TISC - Microsoft Sentinel 統合

脅威インテリジェンスセキュリティセンター for Microsoft Sentinel には、 TISC から Sentinel への観測事象のインポート、関連する観測事象の詳細による Sentinel インシデントの拡張、Sentinel から TISC への観測事象のエクスポートなど、いくつかの機能があります。

注:
Microsoft Sentinel では、観測事象はエンティティと呼ばれます。

前提条件

依存関係

Microsoft Sentinel Content Hub の脅威 インテリジェンス ソリューションをインストールする必要があります。

ロールと権限

アプリケーション	ロールおよび権限	説明
Microsoft Sentinel 固有のロール	1. ロジック アプリ共同作成者 2. Microsoft Sentinel 共同作成者	1. 必要なプレイブックをリソースグループレベルでインストールします。 2. Microsoft Sentinel プレイブックを操作します。 詳細については、「Microsoft Sentinel の役割 とアクセス許可 」を参照してください。
脅威インテリジェンスセキュリティセンター	sn_sec_tisc.api_azure_sentinel_tisc_API	TISC API へのアクセスを許可するには、TISC カスタムコネクタで構成されたユーザーにこのロールが必要です。

TISC プレイブックテンプレート

このセクションでは、TISC Sentinel ソリューションに付属するプレイブックテンプレートについて説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プレイブックのユースケース
次の表で、プレイブックのさまざまなユースケースについて説明します。

ユースケース	プレイブック	説明
TISC から Sentinel への観測事象のインポート	Batch_Indicator_Uploader	Microsoft Sentinel が提供するインジケーターのアップロード API を使用して、TISC から観測事象をエクスポートするためのバッチ処理メカニズムを提供します。
	Import_Observables_Batch	TISC からの観測事象のスケジュール済みエクスポートを有効にします。
Sentinel から TISC へのエンティティのエクスポート	Export_Incident_Entities	Sentinel インシデントのすべてのエンティティをエクスポートします。
	Export_Hash_Entity	Sentinel インシデントのファイルハッシュエンティティをエクスポートします。
	Export_Domain_Entityエンティティ	Sentinel インシデントのドメインエンティティをエクスポートします。
	Export_IP_Entity	Sentinel インシデントの IP エンティティをエクスポートします。
	Export_URL_Entity	Sentinel インシデントの URL エンティティをエクスポートします。
Sentinel インシデントを拡張	Incident_Enrichment	Sentinel インシデントに関連付けられているエンティティに関連する詳細をフェッチし、インシデントに関するコメントの形式で情報を投稿することで、Sentinel インシデントの拡張を有効にします。

注:
すべてのプレイブックは、内部で TISC カスタムコネクタを使用して TISC API を使用します。

テンプレートからプレイブックを作成

1. **Sentinel** ワークスペースのコンテンツハブから**[ISC** ソリューション] コンテンツページに移動します。
2. コンテンツページに表示されるプレイブックごとに、次の操作を行います。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. プレイブックテンプレートを選択すると、画面の右側にコンテキストペインが表示されるので、[構成] をクリックします。

b. プレイブックテンプレートの説明を読み、説明に記載されている 前提条件 と 展開後の 手順を実行します。

c. [カスタムコネクタの展開] をクリックします (カスタムコネクタをまだ展開していない場合)。

[展開構成] ページで **ServiceNow** インスタンスの **URL** を追加します。

d. [**Create Playbook**] をクリックすると、展開構成画面に移動します

e. [プレイブック構成を作成] 画面で、次の操作を行います。

- 適切なリソースグループを選択します。
- プレイブック名を変更するか、デフォルト名を使用します。
- [パラメーター] セクションに カスタムコネクタの名前を入力します(前のステップで展開したコネクタの名前と一致していることを確認してください)。
- [レビューおよび作成] をクリックします。

Import_Observables_Batchプレイブックの構成

Import_Observables_Batch プレイブックを作成する前にBatch_Indicator_Uploaderプレイブックを作成してください。

1. 次のように移動する。 ロジック アプリ デザイナー プレイブックを編集します。
2. 必要に応じて繰り返し時間 (時間) を更新します。
3. プレイブック内の TISC カスタムコネクタコンポーネントから、TISC API に送信されるパラメーターを更新します。

パラメーター名	説明
観察事項タイプ	サポートされているタイプは次のとおりです。1 つ以上を選択してください。 ○ IP ○ ファイルハッシュ ○ ドメイン ○ URL
脅威スコア	観測事象の脅威スコアを入力します。脅威スコア値は、0～100 の範囲の数値でなければなりません。
信頼性	観測事象の信頼度を入力します。 信頼度値は 0～100 の範囲にする必要があります。
評判	サポートされている値は次のとおりです。1 つ以上を選択します。 ○ クリーン ○ 悪意がある

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

パラメーター名	説明
	○ 不審 ○ 不明
脅威の重大度	サポートされている重大度レベルは次のとおりです。1 つ以上を選択してください。 ○ クリティカル ○ 高 ○ 中 ○ Low (低)
脅威レベル	サポートされている脅威レベルは次のとおりです。1 つ以上を選択してください。 ○ High (高) ○ 中 ○ Low (低)
最終更新日デルタ (時間単位)	観測事象の最終更新時間 (時間)。

プレイブック**Export_Incident_Entities**構成

このプレイブックでは、TISC 観測事象追加 API を使用しています。ロジック アプリ デザイナーを使用すると、プレイブックから API に送信されるパラメーターを編集できます。詳細については、「 TISC API - POST /sn_sec_tisc/threat_intel_data/add_observables 」を参照してください。

さまざまなタイプのエンティティをエクスポートする以下にリストされているすべてのプレイブックについて、同じ手順を実行できます。

- Export_Hash_Entity
- Export_Domain_Entity
- Export_IP_Entity
- Export_URL_Entity

プレイブック**Incident_Enrichment**構成

このプレイブックでは、TISC 観測事象 API を使用しています。ロジック アプリ デザイナーを使用すると、プレイブックから API に送信されるパラメーターを編集できます。詳細については、「 TISC API - POST /sn_sec_tisc/threat_intel_data/observables 」を参照してください。

プレイブックを実行

次の表では、次のプレイブックを実行する方法について説明します。

プレイブック	アクション
Import_Observables_Batch	このプレイブックは、繰り返しトリガーに記載されているスケジュール時刻に基づいて自動的に実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プレイブック	アクション
Export_Incident_Entities	Sentinelインシデントで、 インシデントアクション > プレイブックを実行 実行のために。
Export_Hash_Entity	Sentinelインシデントで、 ファイルハッシュエンティティ > プレイブックを実行 実行のために。
Export_Domain_Entity	Sentinelインシデントで、 ドメインエンティティ > プレイブックを実行 実行のために。
Export_IP_Entity	Sentinelインシデントで、 **IP** エンティティ > プレイブックを実行 実行のために。
Export_URL_Entity	Sentinelインシデントで、 **URL** エンティティ > プレイブックを実行 実行のために。
Incident_Enrichment	Sentinelインシデントで、 インシデントアクション > プレイブックを実行 実行のために。

SIR ワークスペースとの TISC 統合

SIR との TISC 統合により、セキュリティアナリストのセキュリティインシデントワークスペース内での観測事象にコンテキストが自動的に加えられます。SIR からの新しい観測事象は、画面に表示される UI アクションで CTI チームが TISC に送信して、分析をさらに進めることができるようになります。

さらに、SIR でのみ利用可能な統合から生成されたエンリッチメント結果は、ワークスペースで提供される UI アクションでプッシュすることもできます。

管理

左側のナビゲーションで脅威インテリジェンスセキュリティセンター内の [管理] モジュールに移動し、TISC データ管理に関する以下のモジュールを表示して、フィルタリングルールや承認ルールの詳細設定、脅威スコアの定義、通知の管理を行います。

データ管理

モジュール	説明
ルールエンジン	このセクションは以下のルールで構成されています。これらはデータ管理の際に必要になります。 **1.** データのインポート承認ルール：承認ルールを定義し、データインポートの送信後に [インポートインテリジェンス] セクション内で承認フローを統合します。 **2.** 受信フィルタリングルール：受信ソースレコードのデータをフィルタリングするフィルタリングルールを作成します。 **3.** 脅威採点ルール：観測事象に脅威スコアを割り当てる脅威スコア算出ツールをカスタマイズします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データ管理 (続く)

モジュール	説明
セキュリティコントロールリスト	このモジュールは、次のセキュリティ制御に役立ちます。 **1.** 許可リスト **2.** 拒否リスト **3.** ウォッチリスト
分類	このモジュールで、データソースレコードの分類を作成することができます。
通知	このモジュールで、メール通知の管理方法を定義します。
テンプレート	このモジュールでは、設計時や実行時の環境でレポートのテンプレートを作成する方法が簡潔にまとめられています。

データのインポート承認ルールの定義

このセクションを使用して承認ルールを定義し、データインポートを送信した後に [インテリジェンスをインポート (Import Intelligence)] セクション内で承認フローを統合します。

始める前に
必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.

2. ワークスペースの [管理] アイコンをクリックします。

3. 検索項目 ルールエンジン > データのインポート承認ルール.

4. [データのインポート承認ルール **(Data Imports Approval Rules)]**を選択します。

ベースシステム内では、[データのインポート承認ルール **(Data Imports Approval Rules)]** は、ユーザーが承認ワークフローをアクティブ化できるようにプロビジョニングされたデフォルトの承認ルールです。

5. [承認が必要なユーザーまたはグループを選択 **(Select User or Groups requiring approval)]** セクションと [承認者を選択] セクションのそれぞれに、少なくとも 1 つのユーザー名またはユーザーグループを入力します。

6. [有効化] ボタンをクリックして、データインポートの承認フローを有効にします。

有効にすると、データインポートは承認キューに入り、承認者がデータ処理を承認または却下できるようになります。承認者は、アナリストが行った変更をレビューし、データインポート要求を承認または却下します。

注:
インポートジョブが処理され、承認または却下されたことを示すメール通知がユーザーまたはユーザーグループに送信されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

有効期限ルールの定義

TISC で作成されたさまざまな観測事象、さまざまなソースオブジェクトやインジケーターソースの組み合わせに関するに有効期限ルールを定義します。

始める前に

アプリケーションで作成されたソースにはすべて有効期限があります。データフィードにおいては、有効期限を時間ベースとするなどの手段でデータの取り込みを促します。TISC では、有効期限ルールにおいて、特定のデータソースセット、オブジェクトタイプや観測事象タイプのセットに対する有効期限を定義します。

必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. 選択 有効期限ルール.
   [有効期限ルール] ページが表示されます。
3. [新規] をクリックします。
4. 新しいルールを作成したら、[有効化] をクリックして有効期限ルールを有効化します。
   有効期限ルールが有効化されていないと、ルールがソースレコードに適用されません。

   注:

   - 有効期限ルールを有効化すると重複チェックがバックグラウンドで行われ、データソースとレコードタイプの組み合わせが同じ重複ルールがシステムに存在しないか検証されます。存在する場合、アプリケーションから「データソースとオブジェクトカテゴリの同じ組み合わせがルールに既に含まれているため、ルールを有効化するには既存の組み合わせを変更する必要があります」という内容の情報メッセージが表示されます。
   - ユーザーに対してサンプルの有効期限ルールがベースシステムにプロビジョニングされています。ただし、観測事象の場合はサンプルの有効期限がデフォルトで無効になっているため、ルールを有効化およびアクティブ化する必要があります。
5. [保存] をクリックします。
6. 有効期限ルールを削除する場合は、[削除] をクリックします。

ソースレコードの有効期限ルール

ソースレコードの有効期限を設定する際、基本的に有効期限ルールがあると便利です。集計レコードでは、対応するソースレコードの中で最長の有効期限が継承されます。

ルールの適用方法

Example: 受信ソースレコードタイプが、データソースタイプ「CrowdStrike」からのマルウェアである

ソースレコードに有効期限を適用するために定められたルールに基づくルール評価プロセス：

1. 有効なルールをすべてフェッチ： アプリケーションでは、最初に現在有効なルールをすべて検証します。
2. 特定のルールの組み合わせを確認：

   次の組み合わせと明確に一致するルールを検索：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- データソースタイプ：CrowdStrike
- レコードのタイプ：マルウェア

3. 一致ルールの組み合わせに基づく優先度：

   データソースタイプが「CrowdStrike」で、レコードタイプが「マルウェア」のルールが存在する場合、このルールが優先されます。このルールで指定された有効期限が適用されます。

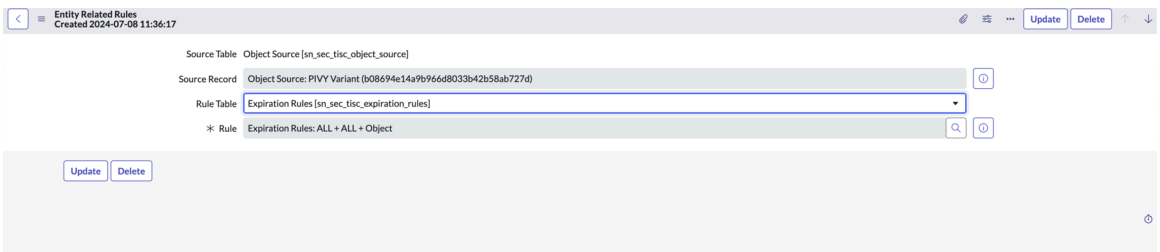
4. フォールバックルール：

   a. 「CrowdStrike」と「マルウェア」の組み合わせと一致するルールがない場合、システムでは、データソースタイプが「CrowdStrike」、レコードタイプが「すべて」のルールを確認します。

   b. それでもルールが見つからない場合は、データソースタイプが「すべて」、レコードタイプが「マルウェア」のルールを検索します。

   c. 最終的に、上記のいずれのルールも存在しない場合は、データソースタイプとレコードタイプのいずれも「すべて」のルールが既定の設定になります。

5. これらのルールがシステムに存在しない場合は、ソースレコードに有効期限ルールが適用されません。その場合は、以下のテーブル (スクリーンショットを参照) に移動して、オブジェクトに適用されたルールの組み合わせを確認します。



6. データソースの削除：

   たとえば、有効期限ルールが関連付けられているデータソースを削除するときにこれらのルールに対応していないと、削除に制限がかかったり、許可されなくなったりする場合があります。これにより、有効期限ポリシーの適用に不整合がなくなります。

フィルタリングルールの定義

あらゆるタイプのデータまたはあらゆる種類の受信ソースレコードデータをフィルタリングするために、フィルタリングルールを作成します。データソースマネージャーを使用して、STIX データ、RSS フィードなどの複数のフィードを構成します。構成されたフィードからのデータをフィルタリングするには、特定のフィルタリングルールを定義する必要があります。

始める前に

フィルタリングルールを定義する場合、データの取り込みおよびデータのインポート中にレコードをフィルタリングするためにルールが適用されるソースデータのセットにのみ、そのルールが適用されます。

必要なロール：sn_sec_tisc.admin

このタスクについて

フィルタリングルールが作成され、以降のステップを処理するためにソースレコードに適用されます。ベースシステムは、取り込まれた観測事象、インジケーターデータ、またはエンティティ/オブジェクトをフィルタリングするための事前定義されたルールを使用して、ユーザーにサンプルフィルタリングルールを提供します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. ドリルダウン先 ルールエンジン > 受信フィルタリングルール.
3. [新規] をクリックしてフィルタリングルールを定義します。
   [新しい受信フィルタリングルールの作成 (Create New Inbound Filter Rules)] ページが表示されます。
4. フォームのフィールドに入力します。

フィルタリングルールの定義

フィールド	説明
名前	新しいフィルタリングルールの名前。
説明	フィルタリングルールの簡単な説明。
順序	フィルタリングルールの優先度。このフィールドは、2 つ以上のルールがトリガー条件を共有する場合にフィルタリングルールが実行される順序を示します。番号が最も小さいフィルタリングルールの優先度が最も高くなります。 操作の順序を設定するには、値を入力します。たとえば、100、200、300 などです。 ベースシステムのフィルタリングルールのデフォルト値は 100 です。
データソース	ルックアップリストからデータソースタイプを選択します。
テーブル	フィルターを適用するテーブルのタイプを選択します。たとえば、観測事象ソース、インジケーターソース、オブジェクトソースなどです。
フィルタータイプ (選択したテーブルが [観測事象ソース] の場合のみ)	フィルタータイプには、フィルターを適用できる対象に基づいて 2 つのオプションがあります。 ○ 条件に基づいてフィルター (Filter based on Condition) ○ リストに基づいてフィルター
フィルタータイプ (条件に基づいてフィルター)	条件ビルダーのフィルター条件。この条件はソーステーブルに基づいて決まります。たとえば、インジケーターソースとオブジェクトソースのフィルタータイプは、[条件に基づいてフィルター] のみです。 条件を追加するには、**[AND]** または **[OR]** をクリックします。[**AND**] を選択した場合は、すべての条件に一致する必要があります。**[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。2 つ目のフィルター条件を設定

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	するには、[新しい条件セット] をクリックします。
フィルタータイプ (リストに基づいてフィルター)	受信観測事象が選択したリスト内のエントリーと一致する場合、フィルタリングされます。 注: これらのフィルタリングルールは、インポートインテリジェンスを使用したデータインポートには適用されません。使用可能なオプションは、[許可リスト]、[拒否リスト]、および [ウォッチリスト] です。

取り込まれたデータでフィルタリングルールを有効にすると、その結果は、フィルタリングされたさまざまなレコードとして次のタブに表示されます。

a. フィルター済みの観測事象レコード：観測事象レコードをフィルタリングして一覧表示します。

b. フィルター済みのインジケーターレコード：インジケーターレコードをフィルタリングして一覧表示します。

c. フィルター済みのオブジェクトレコード：オブジェクトレコードをフィルタリングして一覧表示します。

注:
ソースレコードに追加されたタグに基づいてフィルタリングルールを適用するには、フィルター条件ビルダーで **[TISC** タグ **(TISC tags)]** オプションを選択します。

TISC のカスタム脅威スコア算出

カスタム脅威スコア算出を使用すると、ユーザー定義の基準に基づいて観測事象における脅威の重大度スコアを定義および計算できます。これにより、観測事象の透過的なインテリジェンススコアリングが実現します。観測事象レコードの脅威スコアは自動計算されます。

脅威スコア算出の定義

ユーザー定義のパラメーターに基づいて生成された観測事象レコードの脅威スコアを定義します。ベースシステムには脅威スコアルール が 1 つプロビジョニングされており、それに応じてカスタマイズして有効化することができます。

始める前に

必要なロール：sn_sec_tisc.admin

注:
デフォルトでは、脅威スコアルールが非アクティブになっています。観測事象のスコアを表示するには、ルールを有効化する必要があります。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. 検索項目 脅威採点ルール.
   [脅威スコア算出] ページが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

重要:

- アプリケーションのベースシステム内には、プロビジョニングされているスコアルールが 1 つあり、ユーザーは脅威スコアを表示、編集、変更することができます。ただし、新しいルールを作成したり、事前定義された脅威スコアルールを削除したりすることはできません。
- 変更は新たな観測事象に対して適用 (更新内容は変更後の観測事象に対して適用) されます。履歴のスコアを再計算するには、再計算オプションを使用する必要があります。

3. フォームの下記フィールドには事前定義された値が含まれています。

脅威スコア算出

フィールド	説明
名前	脅威スコア値の名前。例：「脅威スコア算出ツール」など。
説明	脅威スコアレコードの説明。例：「事前定義された基準スコアの重み付けに基づいて脅威スコアを算出」など。
全体的な重み付け（基準ビルダーに適用）	このフィールドは編集できません。有効な基準に対応する重み付けに基づいて計算された全体的な重み付けが表示されます。
採点基準	観測事象の採点基準を示します。 脅威スコアの基準を定義するには、次の 2 つのオプションが利用できます。 ○ 基準ビルダー： このオプションを使用すると、脅威スコアの計算に寄与する基準を追加、編集、削除、有効化 / 無効化して、重み付けの合計が 100% になるようにすることができます。 ○ スクリプトを使用 (高度)： スクリプト機能は、0～100 の範囲の脅威スコアを返すカスタムスクリプトを構築できる高度な機能です。

採点基準の定義で利用できるオプションは次のとおりです。

○ 基準ビルダー

○ スクリプト (詳細) を使用
基準ビルダーの手順は次のとおりです。

注:
既存の基準を編集または変更したり、新規の基準を追加したりすることができます。

a. 基準のタイプを選択します。
例：[新しい基準を追加] など。

b. 基準を構成するテーブルを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドロップダウンリストの値のリストには、[観測事象]、[攻撃者]、[キャンペーン]、[場所]、[ID]、[脆弱性]、[脅威イベント]、[セキュリティインシデント]、[集計] があります。ドロップダウンリストでいずれかのオプションを選択すると、条件が適用されます。その条件に基づき、選択した値に関連するレコードのみが表示または計算されます。

注:

- 観測事象が選択されている場合、脅威スコアが算出される観測事象レコードに条件が適用されます。選択したテーブルが観測事象でない場合、脅威スコアが算出される観測事象とレコードが関連している場合にのみ条件が適用されます。
- 観測事象と関連付けられている数に基づいてスコアを定義するには、集計テーブルを新たに追加します。たとえば、テーブルを [集計]、フィールド値を [攻撃者] で選択したときに、観測事象において複数の攻撃者がいる場合、スコアを設定して、必要に応じて条件を適用します。
- また、観測事象に関連する複数の攻撃者に対してスコアを設定する場合は、フィールドに [攻撃者の数] を選択して適切なスコアを設定し、必要に応じて条件を適用します。

c. 選択したテーブルからフィールドを選択します。

d. 基準の重み付けを 0～100 の範囲で入力します。
すべての基準の全体的な重み付けが 100% になるようにする必要があります。

e. 基準の名前と簡単な説明を入力します。

f. [採点基準を有効にする **(Enable scoring criteria)]** チェックボックスをオンにして、採点基準を有効にします。

g. 条件を定義し、条件のスコアを設定します。

h. [新しい条件 **(New Condition)]** ボタンで新しい条件を追加したり、[基準を削除]アイコンで条件を削除したりすることもできます。

i. [追加 **]** をクリックして、構成した基準を追加します。

脅威スコアに対する条件の定義については、次の例のとおりです。

```
Table: Vulnerability

Field: CVSS2.0

Weightage: 30%

Condition-1: CVSS2.0 > 7, Score = 80

Condition-2: CVSS2.0 > 4 AND CVSS2.0 < 7, Score = 50

Condition-3: CVSS2.0 < 4, Score = 10
```

4. [履歴を再計算] ボタンをクリックして、脅威スコアを再計算します。
脅威採点ルールが変更されている場合、過去に脅威スコアを計算した観測事象に対して採点ルールを再適用する必要があります。[履歴を再計算] ボタンで再計算のジョブをトリガーします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

- アクションを実行する確認メッセージが表示されます。このアクションは、バックグラウンドで実行される長時間実行プロセスとなります。プロセスが完了するまで、変更を加えることはできません。このアクションを実行してもよろしいですか？
- [履歴を再計算] の一環で観測事象に対して生成を行っている更新イベントの場合、Webhook の処理が無効になります。有効化する場合は、このシステムプロパティ「webhook_ignore_threat_score_reapply」を変更します。

5. [**OK**] をクリックします。

重要:
このアクションにより長時間実行ジョブがトリガーされ、ジョブが完了するまで脅威採点ルールに新たな変更を加えることができなくなります。バックグラウンドジョブ構成の構成方法について、詳細は「脆弱性対応のバックグラウンドジョブフレームワーク構成 (Vulnerability Response background job framework configuration)」を参照してください。

以下は、[スクリプトを使用 (高度)]のスクリプトとなります。このスクリプトで、0～100 の範囲の脅威スコアを返すカスタムスクリプトを構築することができます。

高度なスクリプトのフィールドには、**current** パラメーターと **aggregate** パラメーターを受け取る関数が自動的に入力されます。この関数が、0～100 の範囲の脅威スコアを返すことになります。

current パラメーターは、脅威スコアが計算されるエンティティ (観測事象) の GlideRecord オブジェクトとなります。観測事象の場合は、sn_sec_tisc_observable テーブルの GlideRecord に該当します。aggregate パラメーターは、sn_sec_tisc_aggregates テーブルレコードの GlideRecord オブジェクトとなります。これにより、メインエンティティ (観測事象) に関連するさまざまなレコードタイプ (キャンペーンや ID など) のレコード数にアクセスすることができます。

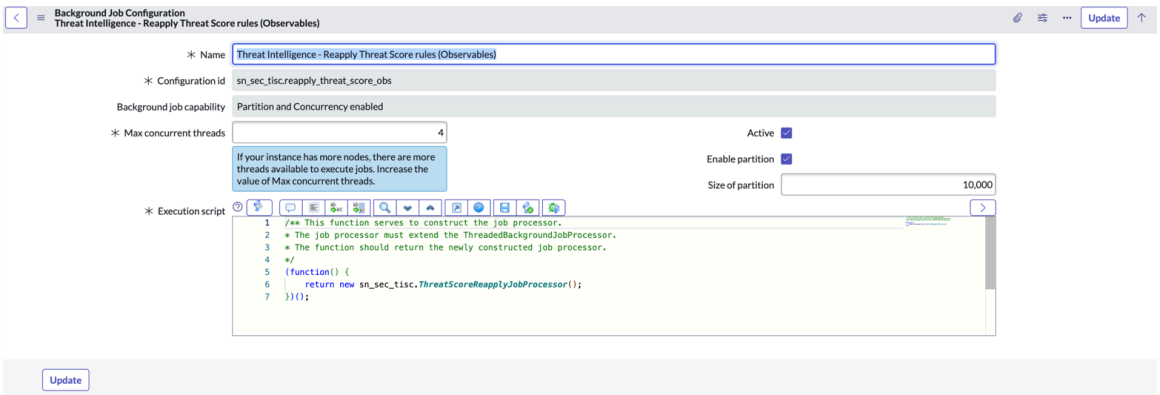
高度なオプションのスクリプト例：

```
answer = (function threatScoreCalculator(current, aggregates) {

   // return the threat score in the range of 0-100
   var threatSeverity = current.getValue("threat_severity");
   if(threatSeverity == "high")
    return 80;
   else {
      let associatedCampaigns = aggregates.getValue("num_of_campaigns");
      if(associatedCampaigns > 0)
         return 50;
   }
   return 0;

})(current, aggregates);
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

参考までに、脅威スコアのバックグラウンドジョブ構成プロセスのスクリーンショットを以下に紹介します。



MITRE ATT&CK テクニック抽出ルール

さまざまなデータソースから取り込まれた観測事象またはオブジェクトから MITRE テクニックを自動的に抽出し、観測事象レコードの脅威のルックアップ結果から MITRE テクニックを抽出します。

始める前に

必要なロール：sn_sec_tisc.admin

> **注:**
> 使用しているインスタンスで MITRE ATT&CK リポジトリデータが利用可能であることを確認してください。データが利用できない場合、アプリケーションは抽出を実行しません。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. 検索項目 ルールエンジン > **MITRE ATT&CK** テクニック抽出ルール.
   [MITRE ATT&CK テクニック抽出ルール] ページが表示されます。
3. [**New**] をクリックします。
4. 新しいルールを作成した後、[有効化] をクリックして MITRE ATT&CK テクニック抽出ルールを有効にします。
   MITRE ATT&CK テクニック抽出ルールを有効にしないと、ルールはレコードに適用されません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

a. データソース:抽出ルールを有効にするたびに、データソースと統合タイプの組み合わせが既存の有効な抽出ルールのいずれにも一致しない必要があり、一致する場合は、既存の組み合わせを変更してルールを再度有効にするように求めるエラーメッセージが表示されます。

b. 脅威のルックアップ:抽出ルールを有効にするたびに、ベンダー名が既存の有効な抽出ルールのいずれとも一致していてはなりません。一致する場合は、ベンダー名を変更してルールを再度有効にするように求めるエラー メッセージがアプリケーションに表示されます。

c. ベースシステムのユーザーに対してサンプルの MITRE ATT&CK テクニック抽出ルールがプロビジョニングされます。これらのルールはデフォルトで無効ステータスになるため、ルールを有効にしてアクティブ化する必要があります。

フィールド	説明
データソース取り込みの汎用ルール	これは、インポートインテリジェンスと手動作成を含むすべてのタイプのデータソースからの取り込みに関する汎用ルールです。
脅威情報ルックアップの汎用ルール	これは、脅威のルックアップの統合の汎用ルールです。

5. [複製] をクリックして、抽出ルールのコピーを作成します。
6. [無効化] をクリックして、抽出ルールを無効にします。

注:
無効にすると、このルールは MITRE データの抽出で考慮されなくなります。

7. **[Save** (保存)] をクリックします。
8. MITRE ATT&CK テクニック抽出ルールを削除する場合は、[削除] をクリックします。

MITRE ATT&CK テクニック抽出メソッド

MITRE ATT&CK テクニック抽出メソッドでは、抽出メソッドの実行方法と関連するテクニックの検証方法について説明します。

1. データソース (脅威のルックアップは適用されません) の抽出ルールは、エンティティ (観測事象ソースやオブジェクトソースなど) のソースレコードが作成されるたびに処理されます。
2. ルールは、エンティティソースレコード内のすべてのフィールドに適用されます (日付、数値フィールド、使用率カテゴリと攻撃フェーズを除く)。
3. 抽出された MITRE テクニックは対応するエンティティレコードに関連付けられ、[関連レコード] タブの [MITRE テクニック] 関連リストでレコードを表示できます。

注:
MITRE テクニックが最初に抽出され、エンティティソースレコードに関連付けられ、次にテクニックの関連付けが除外され、親エンティティレコードに集計されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MITRE テクニックを表示

1. 次のように移動する。 脅威インテリジェンスライブラリを使用する任意のエンティティ (観測事象またはオブジェクト) レコード。
2. [関連レコード] タブをクリックします。
3. **[MITRE** テクニック] を選択し、抽出された関連テクニックを表示します。
4. MITRE テクニック ID をクリックして、MITRE テクニック関連付けレコードを表示してアクセスします。[ソース] 列には、MITRE 抽出が実行されるエンティティソースレコードに関連付けられているすべてのソース (1 つ以上のソースがある場合はカンマで区切って) が表示されます。

   注:
   複数のソースから同じ戦術とテクニックの ID が抽出された場合、戦術とテクニックの関連付けレコードが 1 つだけ表示され、[ソース] 列には抽出されたすべてのソースが表示されます。

5. トラブルシューティングを行う場合は、[テクニックソース関係 **(Technique Source Relations**)] に移動して、戦術とテクニックの関連付けの抽出に関与した MITRE 抽出ルールを表示できます。

   注:
   [抽出ルール] 列が表示されない場合は、[リストアクション] アイコンを使用して [抽出ルール] 列を追加してください。

脅威のルックアップの抽出ルールは、[脅威のルックアップを実行] アクションがトリガーされた観測事象に対して脅威のルックアップの結果レコードが作成されるたびに処理され、脅威のルックアップの結果レコードで利用可能な生データ (raw_dataフィールド) ペイロードに対してのみ抽出が実行されます。

注:

- MITRE ATT&CK テクニックの抽出されたエンティティ (観測事象またはオブジェクト) ソースまたは脅威のルックアップの結果に戦術 ID が存在しない場合、MITRE リポジトリ内の対応するテクニックに関連付けられているすべての戦術に対してテクニックの関連付けが作成されます。
- MITRE ATT&CK テクニックの抽出されたエンティティ (観測事象またはオブジェクト) ソースまたは脅威のルックアップ結果に戦術 ID が存在する場合、テクニックの関連付けは、MITRE リポジトリ内の対応するテクニックに関連付けられているすべての抽出された戦術に対してのみ特別に作成されます。

セキュリティコントロールリストの定義

この機能を使用して、観測事象を一括で追加または削除します。

始める前に
必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. 検索項目 セキュリティコントロールリスト.
   たとえば、観測事象を許可リストに追加してから、[許可リスト] オプションに移動します。
3. [許可リスト] を選択します。
4. IP アドレスやファイルなどの観測事象タイプを選択して、許可リストに追加します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

5. [追加] をクリックします。
[許可リスト用の観測事象を選択 **(Select Observables For Allow list)]** が表示されます。
6. 許可リストに追加する必要があるすべての観測事象を選択します。
7. [許可リストに追加] をクリックします。
選択した観測事象が追加されます。
8. 同様に、[拒否リストに追加 **(Add to Deny list)]** を選択して、削除済みリストに観測事象を追加します。
9. [ウォッチリストに追加 **(Add to Watch list)]** を選択して、観測事象をウォッチリストに追加します。

   注:
   フォームバナーの上にある [観測事象] フォームビューページから、許可リスト、拒否リスト、またはウォッチリストに観測事象を直接追加できます。

10. 確認するには、[脅威インテリジェンスライブラリ **(Threat Intel Library)]** に移動します。
11. 許可リストに追加された観測事象タイプを選択します。
観測事象が許可リストに追加されたと示されます。

   注:
   許可リストと拒否リストは相互に排他的であり、許可リスト内の観測事象が拒否リストに含まれていないことがシステムによって自動的に確認されます。その逆も同様です。

分類の作成

データソースレコードの分類を作成します。

始める前に

必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > アドミニストレーション > 分類.
2. [**New**] をクリックします。
3. 名前を入力します。
4. フォームアクションの [有効] または [無効] を使用して、分類のステータスを有効または無効にします。

   注:
   無効化された分類は、分類が適用可能なレコードでは選択できません。

5. [分類値] セクションに移動して、分類値を追加します。
6. [新規] をクリックして新しい分類値フォームビューを開き、分類と値を入力します。
7. **[Save** (保存)] をクリックします。
8. たとえば、 脅威インテリジェンスライブラリ > 観察事項 して、観測事象レコードの分類を検証します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

9. 観測事象フォームページの [タグと分類] セクションに移動し、新しく作成された分類を選択します。

   注:
   脅威インテリジェンスライブラリのリストビューからタグと分類を追加することもできます。

分類の一括インポート

分類レコードをインポートします。

始める前に
必要なロール：sn_sec_tisc.admin

このタスクについて
スプレッドシートのデータを使用して分類をインポートできます。これにより、複数のレコードを一括でインポートできます。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > アドミニストレーション > 分類.
2. [インポート] ボタンを選択します。
   このアクションにより、XLSX または CSV 形式でデータファイルをインポートするアクションが開きます。サンプルファイルをダウンロードして、インポートする形式を理解することもできます。このファイル形式には、[分類] と [分類値] の 2 つの値が含まれています。
3. [ファイルリンクを追加] をクリックします。
4. ファイルを選択して アップロードします。
5. [完了] をクリックします。
   添付されたファイルのデータが正常にインポートされたことを示す確認メッセージが表示されます。リンクをクリックすると、インポートの概要を表示できます。リンクをクリックすると、レコードが新しいタブで開きます。作成された分類と分類値の数を表示できます。ログに記録されたエラーがある場合は、[インポートエラー] セクションに記録されます。

   注:
   デフォルトでは、これらすべての分類と分類値は、有効のステータスで作成されます。無効にする場合は、いつでもリストビューから行うことができます。

6. [分類] ページでは、任意のレコードをクリックできます。このアクションにより、分類値が別のタブとして表示され、正常にインポートされた 2 つの分類値を確認できます。これらの分類値は [有効] ステータスになります。
7. また、分類のインポートを表示するには、いつでも [インポート] セクションに移動すると、インポートされた分類が [分類インポート] セクションに表示されます。
8. [すべてのインポート] をクリックすると、アプリケーションのさまざまなユーザーによって作成されたすべての分類インポートが表示されます。
9. [自分のインポート] をクリックして、現在ログインしているユーザーの分類インポートを表示します。

脅威のルックアップ評価計算ツールの管理

脅威のルックアップ検索計算ツールを使用すると、脅威のルックアップベンダーから受信した応答に基づいて観測事象の検出結果を計算できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統合用に脅威のルックアップ検索計算ツールを作成し、スクリプトを使用してさまざまな観測事象の検出結果をどのよう識別するかを決定できます。脅威のルックアップ検索計算ツールには、ベースシステムに付属するサンプルスクリプトが含まれています。これを使用して観測事象の結果を特定したり、要件に従ってこのスクリプトを変更したりできます。

脅威のルックアップ検索計算ツールでは、計算された結果を提供するサードパーティ統合の場合、ベースシステム内のサポートされている検出結果に結果をマッピングします。

脅威のルックアップ結果のロールアップ

さまざまな統合ベンダーから観測事象に対して複数の脅威のルックアップ結果がある場合は、すべてのベンダーからの最新の脅威のルックアップ結果が考慮され、全体的な観測事象結果が次のようにマークされます。

脅威のルックアップ検索結果のロールアップ

最新の観測事象結果	全体的な観測事象結果
悪意がある	統合ベンダーの 1 つが観測事象を「悪意がある」と報告した場合、全体的な観測事象結果は [悪意がある] とマークされます。
不審	観測事象を「悪意がある」と報告した統合ベンダーはいないが、統合ベンダーの 1 つが「不審」と報告した場合、全体的な観測事象結果は [不審] とマークされます。
クリーン	すべての統合ベンダーが観測事象を「クリーン」と報告した場合、全体的な観測事象結果は [クリーン] とマークされます。
不明	観測事象を「悪意がある」と報告した統合ベンダーはいないが、統合ベンダーの 1 つが「不明」と報告した場合、全体的な観測事象結果は [不明] とマークされます。

脅威のルックアップ評価計算ツールの表示

脅威のルックアップ検索計算ツールを表示して、特定の脅威のルックアップベンダーからの応答に基づいて観測事象の評判を計算する方法を決定できます。

必要なロール：sn_sec_tisc.admin

脅威のルックアップ評価計算ツールを表示するには、次の手順を実行します。

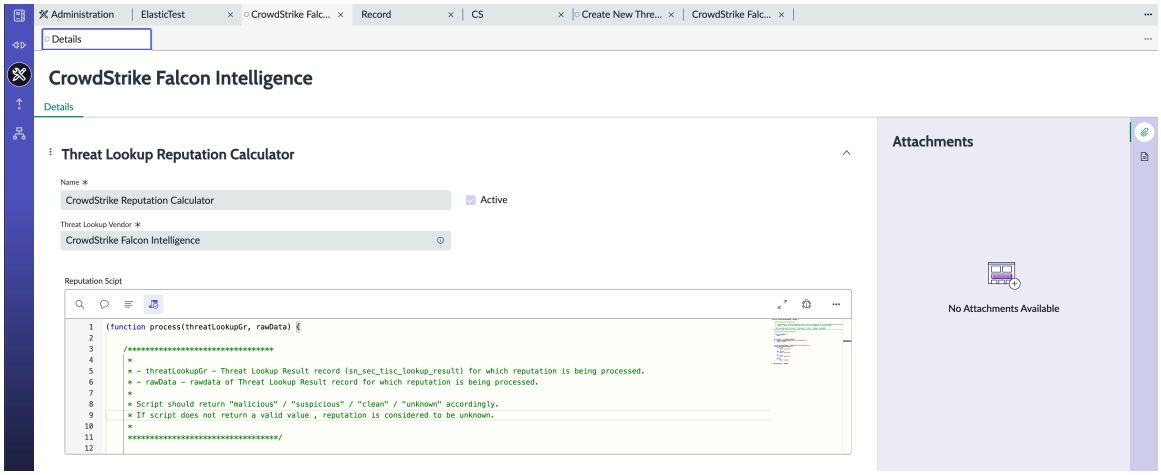
1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. [脅威のルックアップ評価計算ツール] セクションを選択します。

   脅威のルックアップ評価計算ツールのリストを表示することができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 必要な脅威のルックアップ評価計算ツールをクリックして、計算ツールの詳細を表示します。



脅威のルックアップ評価計算ツールの作成

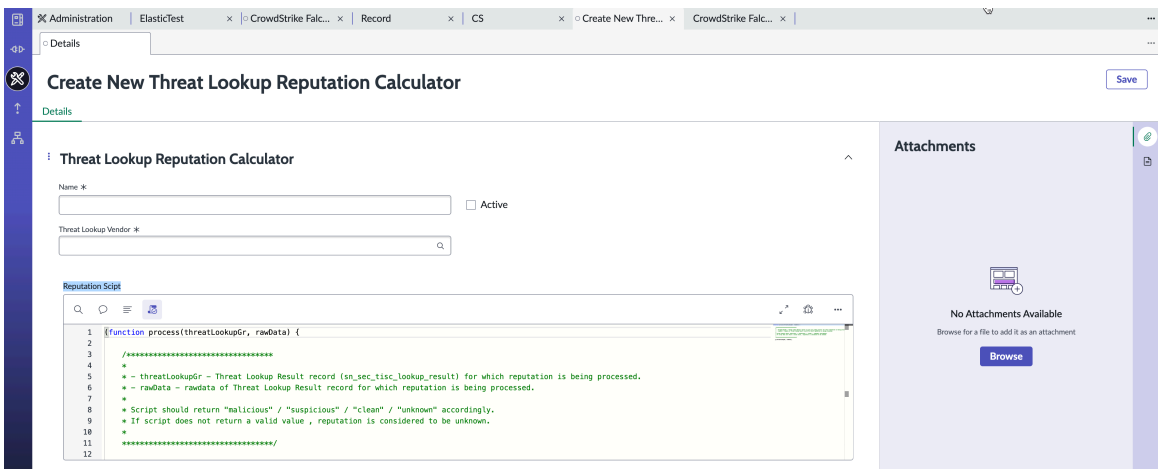
必要なロール：sn_sec_tisc.admin

> **注:**
> 脅威のルックアップベンダーごとに、一度にアクティブにできる脅威のルックアップ計算ツールは 1 つのみです。

脅威のルックアップ評価計算ツールを作成するには、次の手順を実行します。

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. [脅威のルックアップ評価計算ツール] セクションを選択します。

   脅威のルックアップ評価計算ツールのリストを表示することができます。
3. 脅威のルックアップ評価計算ツールを作成するには、[新規] をクリックします。



4. フォームの各フィールドに入力します。

脅威のルックアップ評価計算ツールの作成

フィールド	説明
名前	脅威のルックアップ評価計算ツールの名前。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
アクティブ	脅威のルックアップの計算は、[アクティブ] オプションが選択されている場合にのみ実行されます。
脅威のルックアップベンダー	脅威のルックアップのベンダー名。 例：CrowdStrike Falcon Intelligence
評価スクリプト	さまざまな観測事象結果を識別する方法を決めるためのスクリプトエディター。すべての脅威のルックアップの統合には、脅威のルックアップの評価を計算するための基本スクリプトが付属しています。

5. [保存] をクリックします。

メール通知の管理

ServiceNow の通知を使用して、システムのメール通知を作成および管理し、メールログを表示します。

メール通知

メール通知を使用すると、選択したユーザーに対して観測事象 / インジケーター / その他のさまざまなオブジェクトの更新など、アプリケーション内の特定のタスクに関するメール通知を送信できます。

必要なロール：admin

注:
システムアドミニストレーターは、アプリケーションのクラシックビューでメール通知ルールの詳細を表示、作成、編集することができます。

脅威インテリジェンスセキュリティセンター ではルール主導のメール通知を提供し、個々のメールアドレスやメールアドレスのリストに送信することができます。内部ユーザーに対する脅威インテリジェンス情報は、メール形式で送信して周知されるのが一般的です。このプロセスでは、指定された形式とタイムラインに従って脅威インテリジェンスデータをユーザーに配信します。

メール通知では、アドミニストレーターは次のことを指定できます。

- 通知の送信時期
- 通知の受信者
- 通知の内容

注:
変更する場合は、要件に基づいてベースシステムのルールを変更して、メールの送信先を設定する必要があります。

詳細については、Now Platform 管理 ドキュメントの「メール通知を作成する」を参照してください。

ベースシステムにプロビジョニングされているメール通知ルールの詳細は、以下のテーブルのとおりです。

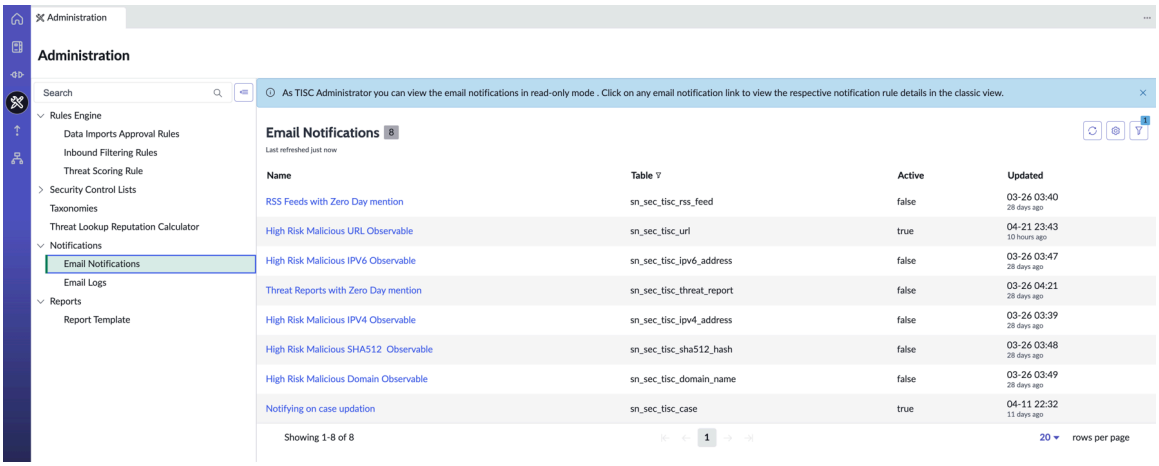
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

メール通知

名前	テーブル
ゼロデイのメンションがある RSS フィード	sn_sec_tisc_rss_feed
高リスクで悪意のある URL の観測事象	sn_sec_tisc_url
高リスクで悪意のある IPV6 の観測事象	sn_sec_tisc_ipv6_address
ゼロデイのメンションを含む脅威レポート	sn_sec_tisc_threat_report
高リスクで悪意のある IPV4 の観測事象	sn_sec_tisc_ipv4_address
高リスクで悪意のある SHA512 の観測事象	sn_sec_tisc_sha512_hash
高リスクで悪意のあるドメインの観測事象	sn_sec_tisc_domain_name
ケース更新時に通知	sn_sec_tisc_case

メール通知



注:
各メール通知をクリックするとクラシック UI が表示され、通知の表示、編集、作成などの必要なアクションを実行することができます。

メールログ

このセクションでは、構成済みのメール通知ルールで送信されるメールにおいて、TISC 管理者に明確な可視性を提供します。

メール通知とログの権限範囲

TISC では、さまざまなペルソナに応じて、メール通知とログのアクセス、表示、変更に対するさまざまな権限を提供しています。

注:

ペルソナ	アクセスレベル
TISC 管理者 (sn_sec_tisc.admin)	sn_sec_tisc.admin は、TISC 用に構成されたメール通知のみを表示できます。☒

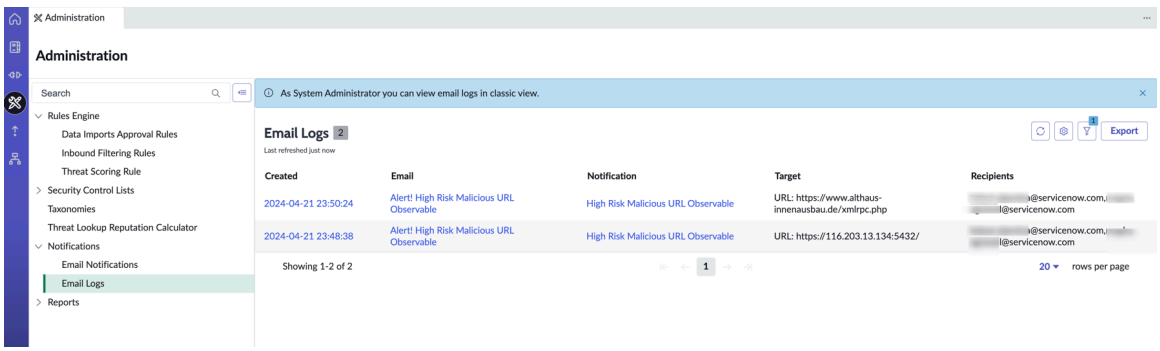
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ペルソナ	アクセスレベル
	注: メールログのハイパーリンクをクリックしてクラシック UI に移動すると、これらの通知を表示できます。
システム管理者 (admin)	管理者は、クラシック UI で通知を作成、表示、編集することができます。 注: メールログのハイパーリンクをクリックしてクラシック UI に移動すると、これらの通知を表示および作成することができます。

注:
TISC の管理者とシステム管理者は、フィルターを使用してメールログを検索できます。

メールログ



レポートテンプレート

ユーザーのグループ内で共有できるレポートテンプレートを再利用して、迅速かつ一貫性のあるレポートを生成する機能を定義します。

この機能を使用して、さまざまなタイプのレポートテンプレートを作成します。これは、組織の脅威に関する進行中の調査のステータスを報告するケースや、同じレポートを生成するうえで役立つケースに適用できます。

このセクションでは、ケースレベルで CTI レポートを実装する方法について説明し、管理者 (テンプレートデザイン) およびアナリスト (ランタイム) エクスペリエンスを提供します。

ドット連結が可能なカスタムケースタスクフォームフィールドや関連リストをレポートテンプレートに追加できます。また、さまざまなレポート要素を使用して、要件に基づくレポートを書式設定および構成できます。

必要なロール：sn_sec_tisc.admin

ベースシステム内でプロビジョニングされるいくつかのレポートテンプレートについては、次のテーブルのとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レポートテンプレート

名前	説明
ケースステータスレポート：攻撃者プロファイル	このレポートは、脅威アクターに関連する進行中のケース調査に関するステータスを提供することを目的としています。脅威アクターは、組織に対する脅威のコンテキストと関連性、攻撃者の行動と潜在的な目標、IOC 拡張、関連するマルウェアとツール、観測された TTP、既存の TTP との違い (新機能、わずかな変更など) を理解しようとしています。
エグゼクティブサマリー	また、特定のリスクについて上級意思決定者に情報を提供できるようにもなっています。上級管理者に理解してもらうことに重点を置き、戦略的な問題については「何が」「いつ」ではなく「なぜ」「どのように」を明らかにします。長文の物語を書くための技術的な詳細や付録は、このレポートには含まれません。
事後調査のサマリー：攻撃者プロファイル	このレポートは、組織に対する脅威のコンテキストと関連性を提供するように設計されています。敵対者の行動と潜在的な目標。IOCエンリッチメント;関連するマルウェアとツール。観測されたTTP;既存の TTP との違い – 新機能、わずかな変更など。

注:
デフォルトでは、これらのレポートのステータスは「公開済み」で、読み取り専用モードになります。レポートテンプレートは読み取り専用モードのため、ユーザーはテンプレートを編集できません。また、レポートテンプレートが無効になるため、アナリストはレポートを生成できません。

自動翻訳

新しいレポートテンプレートの作成

組織のビジネスニーズに応じて、新しいケースレポートテンプレートを作成します。

始める前に

必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. 選択 レポート > レポートテンプレート.
   このセクションには、ベースシステムで利用可能なテンプレートや公開テンプレートが表示されます。レポートの作業に必要なテンプレートを選択できます。

   注:
   必要に応じて、テンプレートの削除もこのセクションで行うことができます。

3. [新規] をクリックします。
4. テンプレートの名前と説明を入力します。
5. [保存] をクリックします。
   [テンプレートのコンテンツ] セクションが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
新しいレポートテンプレートを作成するときは、テンプレートのステータスが「ドラフト」になります。このとき、テンプレートは作成中の状態となり、作業が完了するまで他のユーザーはレポートテンプレートを表示できません。

6. [テンプレートのコンテンツ] を展開して、目的のフィールドをテンプレート本文に挿入します。

注:

- 編集中のテンプレートでは、テンプレート本文を定義し、必要な変数を選択して、[テンプレートエディター] セクションに追加することができます。テンプレートはリッチテキストエディター (RTE) でサポートされているため、インデント、フォントサイズ、テーブル作成、画像の追加、他のさまざまな書式設定機能など、さまざまな機能が利用および制御できます。
- レポートテンプレートに画像を挿入することもできます。その場合は、画像をコピーしてテンプレートに直接ペーストする必要があります。画像を追加すると、その画像は添付ファイルとしてアップロードされます。
- 画像のアップロードまたは添付は最大 698 ピクセルまで可能です。画像が規定のサイズを超えた場合は、自動的にサイズ調整されます。このピクセルサイズの制限により、適切な形式で表示されるように PDF レポートが生成されるので、レポートの画像が切れてしまうこともありません。

7. ケースの必要な要素を追加します。
8. [コンテンツを保存する] をクリックして、新しいレポートテンプレートのコンテンツを保存します。
9. [プレビュー] をクリックして、レポート形式をプレビューし、ケースレポートを生成したときのレポートの仕上がりを確認します。

注:

- ケースフィールド：レポートテンプレートを変更したときは、テンプレートに追加されたコンテンツをプレビューします。たとえば、ケースレポートの生成時に [簡単な説明] フィールドを追加する場合、[ケース] フィールドから当該のフィールドを選択することができます。その後、当該のフィールドが変数としてレポートテンプレートに追加されます。レポートがアナリスト向けに生成されると、[簡単な説明] がレポートに常に表示されます。
- レコード：レポートテンプレート内で、ケースのアーティファクトとして表示される特定のケースの関連レコードを追加することもできます。たとえば、観測事象関連のリストから悪意のある観測事象をレポートに表示する場合は、レポートテンプレートに追加することができます。これらの関連レコードは、テーブル形式で表示されます
- スクリプト：レポートの日時を表示する場合、[現在の日時] スクリプトをレポートテンプレートに追加できます。これにより、レポートの作成日時が追加されます。
- **MITRE ATT&CK**：MITRE カード関連のテクニックがレポートに表示されます。

必要なケース関連のフィールドをすべてレポートテンプレートに追加した後、レポートテンプレートを公開する必要があります。

10. テンプレートを公開するには、[公開] をクリックします。
レポートテンプレートを公開するかどうかを確認するメッセージが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
レポートテンプレートを公開すると、テンプレートがすべてのユーザーに対して有効になります。レポートテンプレートが古くなり、ユーザーに対するレポート表示を制限する場合は、公開レポートを無効化することができます。これにより、レポートテンプレートはユーザーに対して非表示になります。ユーザーが表示および使用できるようにするには、公開レポートを再度有効化する必要があります。有効化されない限り、レポートは表示されません。

11. レポートテンプレートが不要な場合は、[削除] をクリックしてレポートテンプレートを削除します。
レポートテンプレートの名前を変更する場合は、[編集] をクリックして、目的のフィールドを変更します。

レポートのシステムプロパティ

レポートのシステムプロパティについて、以下で説明します。

プロパティ	説明	値
sn_sec_reporting.max_list_columns_allowed	レポート PDF でリストをレンダリングするときに追加できる列の数を制限します。これにより、最初からビューから許容される制限までの列が使用されます。	5.0
sn_sec_reporting.report_default_style_object	このプロパティを使用して、フリーフォームフィールド、左パネル、レポートリストの css を制御します。	(JSON オブジェクト)
sn_sec_reporting.load_all_records	テンプレートから作成されたレポートにリストのすべてのレコードをロードします。true：すべてのレコードをロードします。false：sn_sec_reporting.reporting_list_records_count プロパティで定義された特定の数のレコードをロードします。	False
sn_sec_reporting.reporting_list_records_count	特定の数のレコードをレポートエディターにロードします。	20
sn_sec_tisc.sn_sec_tisc_case.defang_record_list_urls	リストの URL をデフラグするかどうかを制御します。	True
sn_sec_tisc.show_all_tactics_reporting	true の場合、レポートに表示される MITRE リストのすべての戦術 (ケースに関連付けられたテクニックがない戦術を含む) を表示します。	False
sn_sec_tisc.reporting_email_template_sn_sec_tisc_case	共有レポートで使用されるケース (sn_sec_tisc_case) テーブルのメールクライアントテンプレートの Sys ID。	b55e22c54324021060eee0ea78b8f2df

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明	値
sn_sec_tisc.sn_sec_tisc_case.excluded_ctx_menu	フィールドを置き換えるためのレポート/テンプレートメニューオプション内のケースの除外フィールド。	(すべての除外ケースフィールドのリスト)
sn_sec_tisc.sn_sec_tisc_case.ctx_menu_field_header	このプロパティは、レポート/テンプレートメニューオプションのケースフィールドラベルに対応する UI メッセージレコードを取得するために使用されます。	sn_sec_tisc_case_reporting_ctx_menu_field_h

公開されたレポートテンプレートの編集

レポートテンプレートを編集します。

始める前に

必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンスセキュリティセンター > > アドミニストレーション.
2. 選択 レポート > レポートテンプレート.
3. 必要なレポートテンプレートを選択します。
4. レポートテンプレートに表示される [編集] ボタンをクリックします。

   注:

   「公開されたテンプレートを編集しています。[ケースレポート] で使用できるようにするには、テンプレートを再公開する必要があります。編集を続行しますか？」という確認メッセージが表示されます。つまり、必要な変更を加えた後、編集したテンプレートを再公開する必要があります。

5. 確認ダイアログボックスで [編集] をクリックします。
6. 必要なコンテンツフィールドまたは関連リストを追加して、必要な変更を行います。
7. [コンテンツを保存] をクリックします。
8. [公開] ボタンをクリックして、変更を公開します。

   注:

   a. レポートテンプレートを公開する前に、レポートテンプレートの内容をプレビューすることもできます。
   b. 「このテンプレートを公開してもよろしいですか？」という確認メッセージが表示されます。[公開] をクリックして、レポートテンプレートの公開を続行します。
   c. レポートテンプレートを削除する場合は、[削除] をクリックしてレポートテンプレートを削除できます。

レポートテンプレートの複製

増分の更新を追加する場合はレポートを複製します。これにより、レポートテンプレートのコピーを作成できるようになります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンスセキュリティセンター > > アドミニストレーション.
2. 選択 レポート > レポートテンプレート.
3. テンプレートを選択します。
4. [複製] をクリックします。
   選択したテンプレートのコンテンツが複製され、テンプレートのコピーが表示されます。テンプレートのステータスが再び [ドラフト] になり、コンテンツをカスタマイズできるようになります。必要に応じてテンプレート名も変更できます。
5. コピーしたテンプレートのコンテンツを編集または変更します。

> **注:**
> 不要になった場合はレポートテンプレートを削除し、新たにテンプレートを作成することもできます。

Webhook の使用

Webhook は、ソースシステム (TISC) のイベントによってトリガーされ、イベントデータのペイロードとともに宛先システム (エンドポイント URL が存在する) に送信される HTTP 要求です。

脅威インテリジェンスセキュリティセンターで Webhook を使用すると、イベントが発生するたびに宛先アプリケーションに通知することができ便利です。

TISC では、次のことができます。

- Webhook の構成
- トリガーの管理
- 再試行のメカニズム
- 検証の実行
- サブスクリプションの管理

Webhook のシステムプロパティ

Webhook のシステムプロパティについて、以下で説明します。

プロパティ名	説明	タイプ	値
sn_sec_tisc.webhook_ignore_threat_score	脅威スコアの再計算履歴でトリガーされた Webhook イベントは無視します。	True/False	True
sn_sec_tisc.webhook_max_event_batch_size	1 つの Webhook 要求の一部として送信できる最大イベント数。このプロパティで大きな値を設定しても、バッチサイズは 2000 に制限されます。	整数	1000 以上

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

プロパティ名	説明	タイプ	値
sn_sec_tisc.webhook_retry_count	失敗した要求をエラーとしてマークして、次のイベントバッチに進むまでに要求を再試行する必要回数。このプロパティで大きな値を設定しても、再試行回数は 10 に制限されます。	整数	5
sn_sec_tisc.webhook_retry_interval	失敗したバッチを再試行するまでの待機秒数。 再試行回数に応じて指数関数的に増加します。たとえば、「retry_count」が 3 で「retry_interval」が 30 の場合、再試行は 30、60、120 秒後に実行されます。 このプロパティで大きな値を設定しても、初回の再試行間隔は 300 秒 に制限されます。	整数	30

自動翻訳

Webhook の構成

脅威インテリジェンスセキュリティセンターのイベントを登録する Webhook を構成します。

始める前に
必要なロール：sn_sec_tisc.admin

このタスクについて
TISC Webhook は、SIEM などのセキュリティツールと統合する機能を提供します。ユーザーは、観測事象やインジケーター、マルウェア、攻撃者などのさまざまなアーティファクトに関連するさまざまなイベントを登録できます。新しい脅威インテリジェンスが利用可能になったとき、または TISC で既存の脅威インテリジェンスデータが更新または削除されたときに、TISC はセキュリティツール (SIEM など) に通知します。

たとえば、脅威インテリジェンスに新しい観測事象が追加されるたびに、ペイロード要求が Webhook URL 構成に送信されます。このペイロード要求は通常、観測事象の情報を収集し、セキュリティツール (SIEM など) に追加情報として提供します。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. 選択 **Webhook** 構成 > **Webhook**.
   [Webhook] ページが表示されます。
3. [新規] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [検証して保存] をクリックします。
   構成の詳細が正しくない場合、構成の詳細が変更されると、システムは自動的に接続を検証し、アプリケーションは [Webhook の検証に失敗したため、構成の詳細を確認してそれに応じて変更する必要があります。(the validation of the webhook is failed and you need to check the configuration details and modify it accordingly)] という警告メッセージを表示します。

   注:
   - Webhook の検証では、空の要求ペイロードがエンドポイントに送信され、ユーザーは、空の要求が構成された Webhook エンドポイントに渡されたときに、エンドポイントが成功応答コード (200) を送信することを確認する必要があります。
   - デフォルトでは、作成された Webhook はすべて無効ステータスになるため、Webhook を有効にしてアクティブ化する必要があります。サンプル Webhook は、ユーザーへの参照としてベースシステムにプロビジョニングされます。

トリガーを登録

現行の Webhook に登録されているすべての Webhook トリガーのリストを表示します。

始める前に
必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. 選択 **Webhook** 構成 > **Webhook**.
   [Webhook] ページが表示されます。
3. Webhook を選択します。
   [登録済みトリガー] セクションが表示されます。
4. [登録済みトリガー] セクションの [登録] ボタンをクリックします。
   リストビューに、インスタンス内の有効な Webhook トリガーがすべて表示されます。
5. 目的の Webhook トリガーを選択し、[Webhook トリガー] ダイアログボックスで [登録] をクリックします。
   選択したトリガーに Webhook が正常に登録されたことを示す確認メッセージが表示されます。
   ここから直接新しいトリガーを作成して、Webhook を登録することもできます。

   注:
   選択したトリガーから Webhook を登録解除することもできます。

Webhook エラーログの表示

このエラーログセクションを使用して、特定の Webhook でのステータスが「エラー」としてマークされている監査エントリーを表示します。

始める前に
必要なロール：sn_sec_tisc.admin

このタスクについて
監査ログを使用すると、ユーザーは実行の調査やデバッグをさらに行い、実行エラーの根本原因を特定することができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. 選択 **Webhook** 構成 > **Webhook**.
   [Webhook] ページが表示されます。
3. Webhook を選択します。
4. [エラーログ] に移動します。
5. エラーログを表示します。
   リストビューには、特定の Webhook でのエラーログがすべて表示されます。
6. [バッチ] 列に移動します。
7. 任意のバッチ **ID** をクリックします。

   注:
   各エラーログはバッチに関連付けられているので、([バッチ] 列 の) バッチ ID を使用して、関連付けられているバッチレコードを表示することができます。バッチ ID をクリックすると、別のタブで開きます。各バッチ ID には、Webhook のバッチ番号、エラーメッセージ、応答ステータスコード、再試行回数、実際のペイロードデータ、Webhook に送信されるイベントのリストが含まれています。

8. [バッチの再試行 **(Retry batch)**] をクリックして、失敗したバッチを再試行します。
   このボタンをクリックすると、(特定のバッチ情報の) 要求ペイロードが、構成済みの Webhook エンドポイントに送信されます。

   注:
   このアクションは、実行エラーがあるバッチレコードや正常に完了したバッチレコードに対してのみ有効となります。また、[再試行] ステータスのレコードは自動的に再試行されます。

Webhook バッチを表示

Webhook の実行ごとに Webhook バッチレコードが作成されます。

始める前に
必要なロール：admin

このタスクについて
Webhook エンドポイントに送信される API 呼び出しの数を減らすために、イベントのバッチ処理が Webhook に実装されています。各 Webhook で、ほぼ同時に複数のイベントがトリガーされた場合、これらのイベントはすべて同じ要求の一部として Webhook エンドポイントに送信されます。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. 選択 **Webhook** 構成 > **Webhook**.
   [Webhook] ページが表示されます。
3. Webhook を選択します。
4. [エラーログ] に移動します。
5. エラーログを表示します。
   リストビューには、特定の Webhook でのエラーログがすべて表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [バッチ] 列に移動します。
7. 任意のバッチ **ID** をクリックします。
   [Webhook バッチ (Webhook Batch)] ページが表示されます。

   注:
   バッチはすべてテーブル「sn_sec_tisc_webhook_batch」に保存されます。

   以下は、Webhook エンドポイントが受信するペイロード形式のサンプルです。


```
{
   "batch_id": "06eeb3693b6bca10f6f82a60c5e45a7b",
   "events": [
      {
         "record": "Observable",
         "record_fields": {
            "is_false_positive": "false",
            "reputation": "malicious",
            "sys_updated_on": "2024-07-22T14:31:26.000Z",
            "type": "url",
            "sys_updated_by": "admin",
            "sys_created_on": "2024-07-04T06:45:20.000Z",
            "id": "url--1e77adb7eb8b06107750fa86cad0cd70",
            "is_defanged": "false",
            "sys_created_by": "SecCommon.System",
            "tags": "Enriched",
            "taxonomies": "T1: V1",
            "domain": "urlhaus.abuse.ch",
            "status": "active",
            "source_count": "1",
            "threat_score": "20",
            "sys_id": "da77adb7eb8b06107750fa86cad0cd70",
            "value": "https://urlhaus.abuse.ch/url/2578255/",
            "confidence": "89",
            "expiration_time": "2025-10-07T07:13:18.000Z",
            "tlp": "CLEAR"
         },
         "trigger": {
            "name": "Observable Update",
            "type": "UPDATE",
            "trigger_time": "2024-07-22T14:31:26.000Z",
            "trigger_fields": [
               {
                  "field_name": "reputation",
                  "previous_value": null,
                  "current_value": "malicious"
               }
            ]
         }
      },
      {
         "record": "Observable",
         "record_fields": {
            "is_false_positive": "false",
            "reputation": "malicious",
            "sys_updated_on": "2024-07-22T14:31:19.000Z",
            "type": "url",
```


自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
            "sys_updated_by": "admin",
            "sys_created_on": "2024-07-04T06:45:20.000Z",
            "id": "url--9a77adb7eb8b06107750fa86cad0cd6f",
            "is_defanged": "false",
            "sys_created_by": "SecCommon.System",
            "tags": "Enriched",
            "taxonomies": "T1: V1",
            "domain": "urlhaus.abuse.ch",
            "status": "active",
            "source_count": "1",
            "threat_score": "20",
            "sys_id": "5a77adb7eb8b06107750fa86cad0cd6f",
            "value": "https://urlhaus.abuse.ch/url/2578264/",
            "confidence": "89",
            "expiration_time": "2025-10-07T07:13:18.000Z",
            "tlp": "CLEAR"
        },
        "trigger": {
            "name": "Observable Update",
            "type": "UPDATE",
            "trigger_time": "2024-07-22T14:31:19.000Z",
            "trigger_fields": [
                {
                    "field_name": "reputation",
                    "previous_value": null,
                    "current_value": "malicious"
                }
            ]
        }
    }
  ]
}
```


次のテーブルは、Webhook ペイロードとしてユーザーに送信されるバッチペイロード構造と属性の一覧です。

バッチペイロードのパラメーター	タイプ	説明
batch_id	文字列	バッチの一意の識別子を指定します。
イベント	オブジェクトのアレイ	Webhook の一部としてトリガーされる一連のイベントが含まれます。各イベントには、イベント生成時のフィールド値のスナップショットやトリガー情報が含まれます。 **注:** イベントオブジェクトのパラメーター表示について、詳細は Webhook トリガー を参照してください。

注:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

8. [バッチの再試行 **(Retry batch)**] ボタンをクリックして、失敗したバッチを再試行します。

   注:
   完了済みのバッチで再試行バッチをトリガーすることもできます。

Webhook トリガー

Webhook トリガーは、作成、更新、削除などのイベント変更について追跡する必要がある脅威インテリジェンスエンティティをフィルタリングするために使用されます。

始める前に
必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. 選択 **Webhook** 構成 > トリガー.
   [Webhook トリガー] ページが表示されます。
3. [新規] をクリックします。
4. [保存] をクリックします。
   デフォルトでは、トリガー作成時のステータスは「無効」です。
5. [有効化] をクリックしてトリガーを有効にすると、トリガーが Webhook で登録できるようになります。

   注:
   [無効化] をクリックして有効なトリガーを無効化すると、Webhook に関連付けられている登録がトリガーからすべて解除されます。

6. [サンプルペイロードを表示 **(View Sample Payload)**] をクリックしてレコードを選択します。
   特定の Webhook トリガーのサンプルペイロードを表示します。選択したテーブルに基づいて、指定したテーブルのレコードが [レコードを選択] ドロップダウンリストに入力されます。サンプルペイロードを表示するレコードを選択します。サンプル ペイロードが JSON 形式で表示されます。ペイロードのフィールドが以下のように一覧表示されます。
7. ドロップダウンリストからレコードのタイプを選択します。
   ペイロードは、選択したレコードに応じて自動的に変更されます。


```
{
   "record": "Observable",
   "record_fields": {
      "additional_context": "This could be a potential malicious IP. ",
      "attack_phases": "Lockheed Martin: Command and Control",
      "author": "Anomali",
      "confidence": "50",
      "description": "This could be a potential malicious IP. ",
      "expiration_time": "2024-12-01T00:00:00.000Z",
      "first_observed": "2024-01-01T00:00:00.000Z",
      "first_seen": "2024-01-01T00:00:00.000Z",
      "id": "ipv4-addr--70526b0a436a02102164e0ea78b8f210",
      "is_defanged": "false",
      "is_false_positive": "false",
      "last_observed": "2024-01-01T00:00:00.000Z",
      "last_seen": "2024-01-01T00:00:00.000Z",
```


自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
      "reputation": "suspicious",
      "source_count": "1",
      "status": "active",
      "sys_created_by": "SecCommon.System",
      "sys_created_on": "2024-06-04T00:00:00.000Z",
      "sys_id": "30526b0a436a02102164e0ea78b8f210",
      "sys_updated_by": "system",
      "sys_updated_on": "2024-06-15T00:00:00.000Z",
      "tags": "critical",
      "taxonomies": "MITRE: T121",
      "threat_level": "medium",
      "threat_score": "24",
      "threat_severity": "medium",
      "tlp": "CLEAR",
      "type": "ip_v4_address",
      "usage_categories": "APT",
      "value": "116.98.170.70"
   },
   "trigger": {
      "name": "Observable Update",
      "type": "UPDATE",
      "trigger_time": "2024-07-26T07:27:29.000Z",
      "trigger_fields": [
         {
            "field_name": "confidence",
            "previous_value": "30",
            "current_value": "50"
         }
      ]
   }
}
```


トリガーペイロードのパラメーターのリスト

トリガーペイロードのパラメーター	タイプ	説明
レコード	文字列	「観測事象」や「インジケーター」などのレコードタイプを指定します。
record_fields	オブジェクト	イベント生成時のレコードフィールドのスナップショットを指定します。サポートされているフィールドのリストについては、以下のセクションのテーブルを参照してください。
トリガー	オブジェクト	一致したトリガー情報を指定します。
trigger.name	文字列	トリガーの名前を指定します
trigger.type	文字列	トリガーのタイプを指定します。有効な値は、「CREATE」「UPDATE」「DELETE」となります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

トリガーペイロードのパラメーター	タイプ	説明
trigger.trigger_time	日付 (UTC タイムゾーンの ISO 形式)	レコードのイベント発生時刻を指定します。
trigger_fields	オブジェクトのアレイ	UPDATE トリガータイプでのみ使用できます。イベント発生時に変更されたトリガーフィールドのリストを指定します。**trigger_fields** 内のパラメーターは次のとおりです。 ○ **field_name**：変更されたフィールド名を提供します。 ○ **previous_value**：フィールドの以前の値を提供します。 ○ **current_value**：フィールドの現在の値を提供します。

[作成] および [更新] トリガーでサポートされているフィールドのリスト

テーブル	列名	列ラベル
キャンペーン	aliases	エイリアス
キャンペーン	description	説明
キャンペーン	first_seen	初回確認日
キャンペーン	last_seen	最終確認日
キャンペーン	name	名前
キャンペーン	objective	目的
インジケーター	additional_context	追加コンテキスト
インジケーター	attack_phases	攻撃フェーズ
インジケーター	author	作成者
インジケーター	信頼性	信頼性
インジケーター	description	説明
インジケーター	expiration_time	有効期限
インジケーター	first_detected	初回検出日
インジケーター	first_observed	初回観測日
インジケーター	first_seen	初回確認日
インジケーター	id	ID
インジケーター	indicator_types	インジケータータイプ
インジケーター	ioc_classification	IOC 分類
インジケーター	last_observed	最終観測日
インジケーター	last_seen	最終確認日
インジケーター	name	名前

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	列名	列ラベル
インジケーター	pattern	パターン
インジケーター	pattern_type	パターンタイプ
インジケーター	pattern_version	パターンバージョン
インジケーター	platforms	プラットフォーム
インジケーター	revoked	取り消し
インジケーター	source_count	ソースの数
インジケーター	spec_version	仕様バージョン
インジケーター	status	ステータス
インジケーター	tags	TISC タグ
インジケーター	taxonomies	分類
インジケーター	threat_level	脅威レベル
インジケーター	threat_severity	脅威の重大度
インジケーター	tlp	TLP
インジケーター	usage_categories	使用率カテゴリ
インジケーター	valid_from	有効期間開始日
インジケーター	valid_until	有効期限
マルウェア	aliases	エイリアス
マルウェア	attack_phases	攻撃フェーズ
マルウェア	description	説明
マルウェア	executable_process_architectures	プロセスアーキテクチャ
マルウェア	first_seen	初回確認日
マルウェア	implementation_languages	実装言語
マルウェア	is_family	ファミリ
マルウェア	last_seen	最終確認日
マルウェア	malware_capabilities	マルウェア機能
マルウェア	malware_types	マルウェアタイプ
マルウェア	name	名前
オブジェクト ([一般的なオブジェクト(Common Object)] フィールド)	additional_context	追加コンテキスト
オブジェクト ([一般的なオブジェクト(Common Object)] フィールド)	信頼性	信頼性
オブジェクト ([一般的なオブジェクト(Common Object)] フィールド)	expiration_time	有効期限

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	列名	列ラベル
オブジェクト ([一般的なオブジェクト(Common Object)] フィールド)	id	ID
オブジェクト ([一般的なオブジェクト(Common Object)] フィールド)	revoked	取り消し
オブジェクト ([一般的なオブジェクト(Common Object)] フィールド)	source_count	ソースの数
オブジェクト ([一般的なオブジェクト(Common Object)] フィールド)	spec_version	仕様バージョン
オブジェクト ([一般的なオブジェクト(Common Object)] フィールド)	status	ステータス
オブジェクト ([一般的なオブジェクト(Common Object)] フィールド)	tags	TISC タグ
オブジェクト ([一般的なオブジェクト(Common Object)] フィールド)	taxonomies	分類
オブジェクト ([一般的なオブジェクト(Common Object)] フィールド)	threat_level	脅威レベル
オブジェクト ([一般的なオブジェクト(Common Object)] フィールド)	threat_severity	脅威の重大度
オブジェクト ([一般的なオブジェクト(Common Object)] フィールド)	tlp	TLP
観測事象	additional_context	追加コンテキスト
観測事象	attack_phases	攻撃フェーズ
観測事象	author	作成者
観測事象	信頼性	信頼性
観測事象	description	説明
観測事象	expiration_time	有効期限
観測事象	first_observed	初回観測日
観測事象	first_seen	初回確認日
観測事象	id	ID
観測事象	is_defanged	無力化済み
観測事象	is_false_positive	誤検出
観測事象	last_observed	最終観測日

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	列名	列ラベル
観測事象	last_seen	最終確認日
観測事象	reputation	評判
観測事象	source_count	ソースの数
観測事象	status	ステータス
観測事象	tags	TISC タグ
観測事象	taxonomies	分類
観測事象	threat_level	脅威レベル
観測事象	threat_score	脅威スコア
観測事象	threat_severity	脅威の重大度
観測事象	tlp	TLP
観測事象	type	タイプ
観測事象	usage_categories	使用率カテゴリ
観測事象	value	値
攻撃者	aliases	エイリアス
攻撃者	description	説明
攻撃者	first_seen	初回確認日
攻撃者	goals	ゴール
攻撃者	last_seen	最終確認日
攻撃者	name	名前
攻撃者	personal_motivations	個人の動機
攻撃者	primary_motivation	プライマリ動機
攻撃者	resource_level	リソースレベル
攻撃者	secondary_motivations	セカンダリ動機
攻撃者	sophistication	洗練
攻撃者	threat_actor_roles	攻撃者ロール
攻撃者	threat_actor_types	攻撃者タイプ
脅威レポート	description	説明
脅威レポート	name	名前
脅威レポート	published	公開
脅威レポート	report_types	レポートタイプ
脆弱性	affected_software	影響を受けるソフトウェア
脆弱性	description	説明
脆弱性	exploitation_status	エクスプロイトステータス
脆弱性	exploit_exists	エクスプロイト有無
脆弱性	name	名前

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	列名	列ラベル
脆弱性	published	公開
脆弱性	record_last_modified	最後に変更されたレコード
脆弱性	重大度	重大度

以下は、すべてのエンティティに共通する適用可能なシステムフィールドのリストです。これらは作成トリガーと更新トリガーの Webhook トリガーペイロードでサポートされています。

- sys_id (Sys ID)
- sys_created_on (作成済み)
- sys_created_by (作成者)
- sys_updated_on (更新済み)
- sys_updated_by (更新者)

注:
削除の場合、sys_id (Sys ID) のみがペイロードの一部として Webhook エンドポイント URL に送信され、他のシステムフィールドはサポートされていません。

[削除] トリガーでサポートされているフィールドのリスト

テーブル	列名	列ラベル
観測事象	type	タイプ
観測事象	value	値
インジケーター	name	名前
インジケーター	pattern	パターン
インジケーター	pattern_type	パターンタイプ
インジケーター	valid_from	有効期間開始日
キャンペーン	name	名前
マルウェア	is_family	ファミリ
マルウェア	name	名前
攻撃者	name	名前
脅威レポート	name	名前
脅威レポート	published	公開
脆弱性	name	名前
脆弱性	重大度	重大度

自動翻訳

自動フローでの作業

これらの定義された手順で、TISC や関連機能の自動フローをどのように活用できるのか説明します。

TISC のロールで実行するフローを作成します。TISC では、次のフローが作成されます。

- 自動 IOC エンリッチメント
- 脅威に関連する IoC の分析、評価、周知

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 分析を実行し、脅威に関連する IoC を評価して、インシデントを作成します。
- 脆弱性管理サポート。
- ゼロデイ脆弱性追跡。

注:
フローはすべてテンプレートとしてドラフトの状態で提供されるので、ユーザーのニーズに応じてカスタマイズしたりコピーしたりすることができます。

再利用可能アクション

フローアクション	説明
エンティティにタグを追加	サポートするエンティティにタグを追加します (観測事象 / インジケーター / オブジェクト)。
エンティティからタグを削除	サポートするエンティティのタグを削除します (観測事象 / インジケーター / オブジェクト)。
IP アドレスが CIDR の範囲内にあるかどうかを確認	IP アドレスが CIDR 範囲内にあるかどうかを確認します。
IP アドレスが範囲内にあるかどうかを確認	IP アドレスが開始範囲と終了範囲の間にあるかどうかを確認します。

自動 **IOC** エンリッチメント

特定の基準に一致したときに、フローを使用して IOC の拡張を自動化する方法について説明します。

始める前に

必要なロール：

- システム管理者 (表示、作成、編集)
- sn_sec_tisc.admin (表示)

このタスクについて

次の場合にのみ、IOC 拡張のトリガーを自動化します。

- 観測事象のタイプがドメイン名、IPv4 アドレス、または IPv6 アドレスである。
- 観測事象のステータスが「処理済み」である。
- 観測事象に拡張済みのタグや [拡張をスキップ] タグがない。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. 選択 自動フロー.
3. [自動 **IOC** エンリッチメント] アクションのリンクを選択して、フローデザイナーで各ルールの詳細を表示します。
4. 次のトリガーのフローデザイナーアクションを表示します：

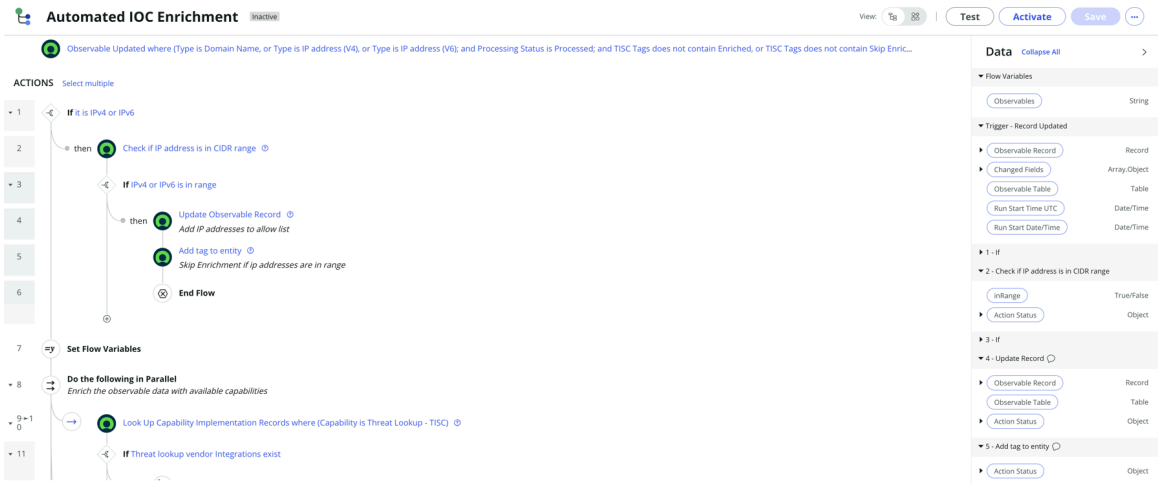
```
Observable Updated where (Type is Domain Name, or Type is IP address (V4), or Type is IP address (V6); and Processing Status is Processed; and TISC Tags does not contain Enriched,
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

or TISC Tags does not contain Skip Enrichment, or TISC Tags does not contain Potential New Threat)

5. 観測事象が **IPv4** または **IPv6** アドレスで、許可された **CIDR** 範囲内にある場合：
   a. 観測事象を許可リストに追加します。
   b. 観測事象のタグを [拡張をスキップ] に更新します。
   c. この観測事象のフローを終了します。
6. それ以外の場合は、利用可能な機能で観測事象データを拡張します。
   a. 脅威のルックアップとサイティング検索を実行して、観測事象に関する追加情報を収集します。
   b. 拡張データで観測事象を更新します。
   c. IOC が処理されたことを示す [拡張済み **(Enriched)]** タグを追加します。
7. また、観測事象の評判が「クリーン」の場合：
   a. 観測事象を「誤検出」としてマークし、非アクティブ化します。
8. その他、観測事象の評判が不明な場合：
   a. [潜在的な脅威で拡張済みというわけではない **(Not Potential Threat & Enriched)]** タグを追加して、脅威ではないことを示します。



観測事象の分析、評価、周知

脅威に関連する観測事象を分析および周知する方法について説明します。

始める前に

必要なロール：

- システム管理者 (表示、作成、編集)
- sn_sec_tisc.admin (表示)

このタスクについて

サイティング検索の拡張が要求されると、サイティングなしで返されます。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. 選択 自動フロー.

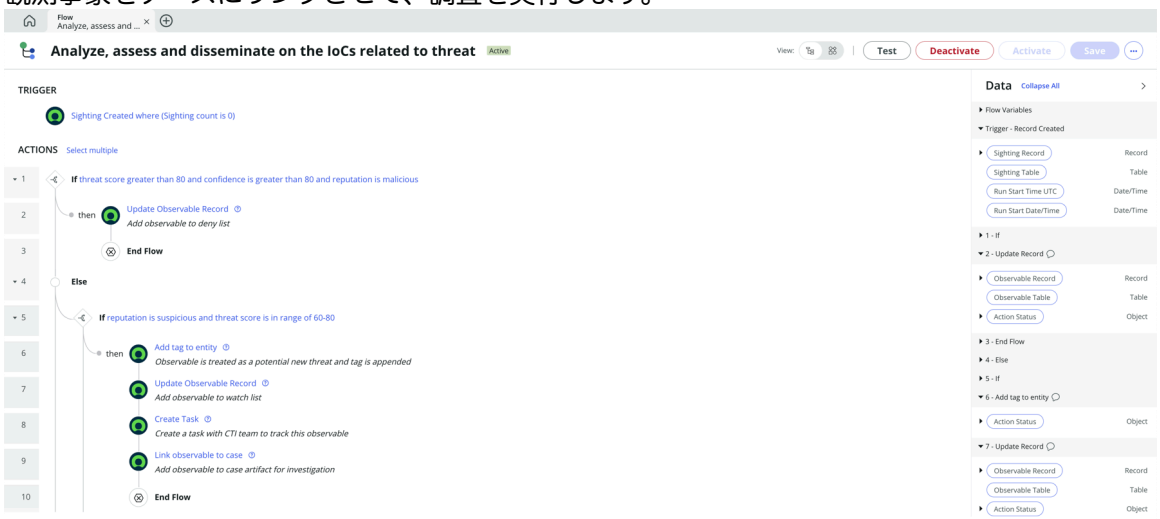
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. 「脅威に関連する **IoC** の分析、評価、周知」のアクションリンクを選択して、フローデザイナーで各ルールの詳細を表示します。
4. 次のトリガーのフローデザイナーアクションを表示します：

   Sighting Created where (Sighting count is 0)

5. 観測事象において脅威スコアが **80** 以上、信頼度が **80** 以上、評判が「悪意あり」：
   a. 観測事象を拒否リストに追加します。
   b. この観測事象のフローを終了します。
6. その他、観測事象の評価が「疑わしい」、脅威スコアが 60～**80** の範囲の場合：
   a. [新たな潜在的脅威 (Potential New Threat)] タグを追加します。
   b. 観測事象をウォッチリストに追加します。
   c. CTI チームとともにケースタスクを作成し、この観測事象を追跡して分析を続けます。
   d. 観測事象をケースにリンクさせて、調査を実行します。



脅威 **IoC** の分析とアセスメント

脅威となる IOC の分析方法と、セキュリティインシデントチームへの通知について説明します。

始める前に

必要なロール：

- システム管理者 (表示、作成、編集)
- sn_sec_tisc.admin (表示)

このタスクについて

サイティング検索の拡張が要求されたとき：

- 観測事象が観測されている場合 (数が 0 以上)、かつ
- 観測事象の評判が「悪意あり」、かつ
- 観測事象の脅威スコアが 80 以上、かつ
- 観測事象の信頼度が 80 以上の場合

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. 選択 自動フロー.
3. 「分析を実行し、脅威に関連する **IoC** を評価して、インシデントを作成する」アクションリンクを選択して、フローデザイナーで各ルールの詳細を表示します。
4. 次のトリガーのフローデザイナーアクションを表示します：

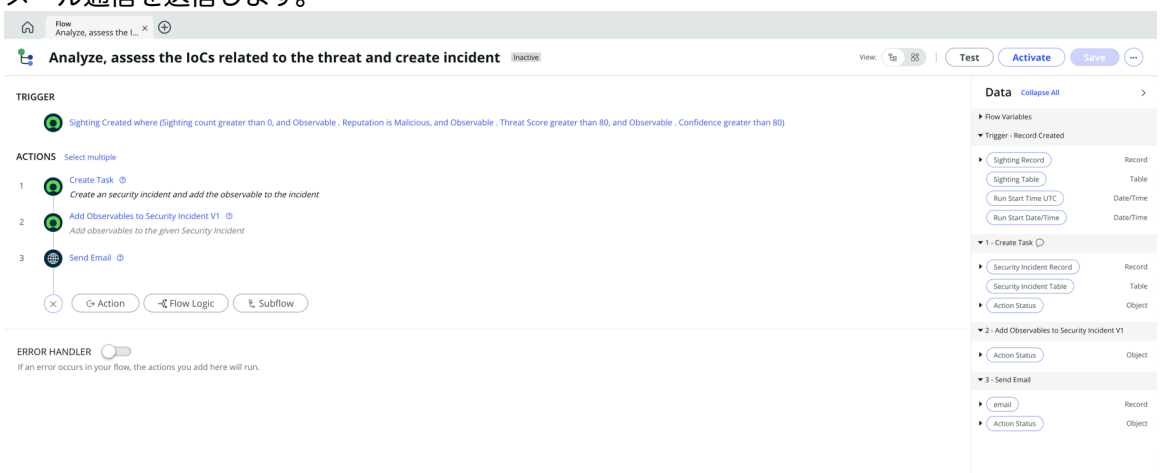
   Sighting Created where (Sighting count greater than 0, and Observable. Reputation is Malicious, and Observable. Threat Score greater than 80, and Observable. Confidence greater than 80)

5. サイティングが作成されたときに (サイティングの数が **0** 以上、かつ観測事象である。評判が「悪意あり」、かつ観測事象である。脅威スコアが **80** 以上、かつ観測事象である。信頼度が **80** 以上) の場合：

   a. セキュリティインシデントを作成し、観測事象をインシデントに追加します。

   b. 観測事象をセキュリティインシデント V1 に追加します。

   c. メール通信を送信します。



脆弱性管理サポート

VR 関連の脆弱性により TISC で新たな脆弱性が生じる仕組みについて説明します。

始める前に

必要なロール：

- システム管理者 (表示、作成、編集)
- sn_sec_tisc.admin (表示)

このタスクについて

TISC で新たな脆弱性が生じ、VR に関連の脆弱性が存在している場合。

- VR 脆弱性 (v2) スコアが 8 を超えているか、VR 脆弱性 (v3) スコアが 8 を超えている場合。
- 関連付けられている VI の合計が 0 超えになります。

自動翻訳

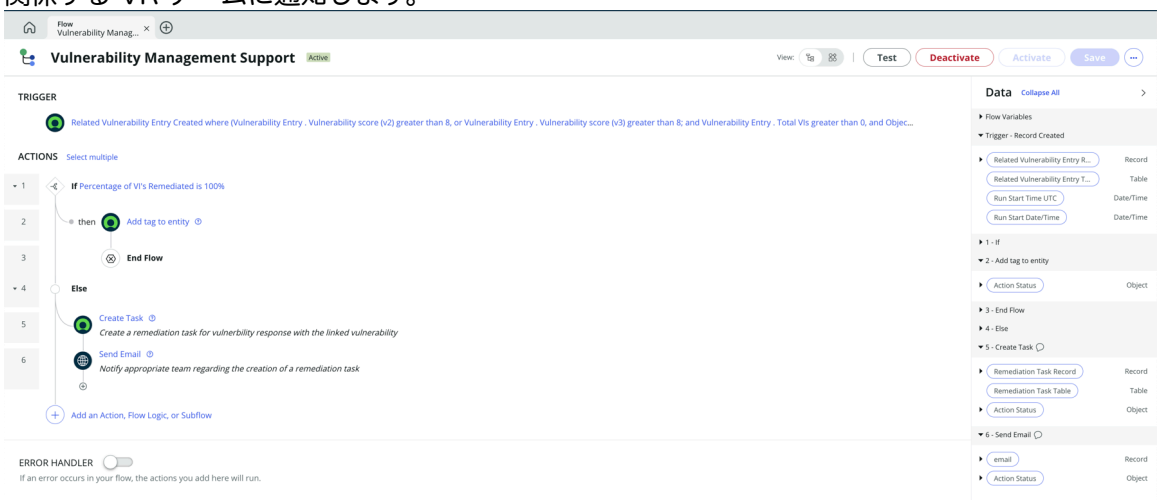
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. 選択 自動フロー.
3. [脆弱性管理サポート] アクションのリンクを選択して、フローデザイナーで各ルールの詳細を表示します。
4. 次のトリガーのフローデザイナーアクションを表示します：

   When new vulnerability is created in TISC and there is a related vulnerability in VR.

5. 修正された **VI** の合計のうち、当該の脆弱性に関連付けられている **VI** の割合が **100%** の場合：
   a. [修復済み (Remediated)] タグを観測事象に追加します。
6. それ以外の場合は、利用可能な機能で観測事象データを拡張します。
   a. VR の修正タスクを作成します。
   b. 関係する VR チームに通知します。



ゼロデイ脆弱性の追跡

システムに送られる RSS フィードの分析方法について説明します。

始める前に

必要なロール：

- システム管理者 (表示、作成、編集)
- sn_sec_tisc.admin (表示)

このタスクについて

新しい RSS フィードがシステムに作成されたときにタイトルや説明に「ゼロデイ」が含まれる場合。

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンスセキュリティセンター > アドミニストレーション.
2. 選択 自動フロー.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. [ゼロデイ脆弱性の追跡] リンクを選択して、フローデザイナーで各ルールの詳細を表示します。
4. 次のトリガーのフローデザイナーアクションを表示します：

   RSS Feed Created where (Title contains zero day, or Description contains zero day, or Title contains zero_day, or Description contains zero_day, or Title contains zero-day, or Description contains zero-day)

5. 観測事象が **IPv4** または **IPv6** アドレスで、許可された **CIDR** 範囲内にある場合：
   a. VR チームの修復タスクとともに、TISC チームのケースを作成します。
   b. 関係する TISC チームや VR チームに通知します。

自動フローのテーブル

次のテーブルは、自動フローで使用されるエンティティ間の関係テーブルや拡張テーブルを理解するうえで役立ちます。

エンティティ間の関係テーブル

テーブル	エンティティ
関連するインジケーター観測事象	sn_sec_tisc_m2m_indicator_observable
関連するインジケーター	sn_sec_tisc_m2m_indicator
関連する観測事象	sn_sec_tisc_m2m_observable
オブジェクトとオブジェクトのリレーションシップ	sn_sec_tisc_m2m_object
関連するインジケーターオブジェクト	sn_sec_tisc_m2m_object_indicator
オブジェクトと観測事象のリレーションシップ	sn_sec_tisc_m2m_object_observable

拡張テーブル

テーブル	エンティティ
脅威のルックアップの結果	sn_sec_tisc_lookup_result
サイティング	sn_sec_tisc_sighting
観測事象の拡張結果	sn_sec_tisc_observable_enrichment_result

Intelligence Exchange 構成の管理

データインポートの使用

データインポートでは、インポートジョブで処理されているレコードをすべて表示するだけでなく、承認待ちのインポートジョブを一覧表示することもできます。

すべてのインポートを表示

このセクションを使用して、すべてのユーザーのリストビューに表示されているインポート済みレコードをすべて表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > インポート.
2. 選択 データインポート > すべてのインポート
   このページには、インポートジョブで処理されているレコードがすべて表示されます。
3. 任意のレコードを開いて、インポートプロセスのステータスを表示します。

   注:
   [新しいインポート] をクリックして、新規のインポートレコードを作成することもできます。このボタンをクリックすると、直接 [インポートインテリジェンス] ページに移動します。新しいレコードの作成について、詳細は 脅威インテリジェンスのインポート セクションより各インポートタイプを参照してください。

自分のインポートを表示

このセクションを使用して、ログインしたユーザーが作成したインポートレコードを表示します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > インポート.
2. 選択 データインポート > 自分のインポート
   このページには、インポートジョブのプロセスを進めるために分類されたインポートレコードがすべて表示されます。
3. 任意のレコードを開いて、インポートプロセスのステータスを表示します。

   注:
   [新しいインポート] をクリックして、新規のインポートレコードを作成することもできます。このボタンをクリックすると、直接 [インポートインテリジェンス] ページに移動します。新しいレコードの作成について、詳細は 脅威インテリジェンスのインポート セクションより各インポートタイプを参照してください。

4. インポートレコードのサマリーを表示します。

   注:
   インポートジョブが送信されていない場合は、処理を進めるレコードを送信して、承認を要求することができます。特定のインポートジョブにおいて承認が不要な場合、レコードは自動的に処理されます。

自分の承認を表示

このセクションを使用して、インポートジョブレコードを確認および承認します。

始める前に
必要なロール：sn_sec_tisc.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > インポート.
2. 選択 データインポート > 自分の承認
   このページには、ログインしたユーザーの承認を待っているインポートレコードがすべて表示されます。
3. レコードを開き、インポートレコードを承認または却下します。
4. [承認] をクリックして、インポートジョブレコードを承認します。
   [インポートを承認] ダイアログボックスが表示され、選択したインポートを承認するかどうかの確認メッセージが表示されます。

   注:
   各ユーザーに、処理中のインポートジョブが承認されたことを示すメール通知が送信されます。承認ルールについての詳細は、「データのインポート承認ルールの定義」を参照してください。

5. ダイアログボックスから [承認] を選択します。
   インポートジョブを作成したユーザーにメール通知が送信され、処理中のインポートジョブが承認済みとなります。
6. [却下] をクリックしてレコードを却下します。

   注:
   - 却下されたインポートジョブは、見直しをして再送信することができます。却下のコメントを必ず加えてください。
   - 処理中のインポートジョブが却下されると、インポートジョブを作成したユーザーにメール通知が送信されます。
   - 承認要求のメール通知が承認者に送信されます。

脅威インテリジェンスのインポート

この機能を使用して、脅威インテリジェンスデータをリポジトリに手動で追加またはインポートします。

インテリジェンスデータのインポートプロセスでは、次のインポート形式がサポートされています。

1. 構造化ファイルからインポート
2. 標準形式でのインポート
3. 生のテキストからインポート
4. ファイル (非構造化) からインポート

構造化ファイルを使用したデータのインポート

CSV、XLSX、XLS などのサポートされているファイル形式で構造化データをアップロードします。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
   [脅威インテリジェンスライブラリ (Threat Intel Library)] ページが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. [インテリジェンスをインポート **(Import Intelligence)**]をクリックします。
3. [構造化ファイルからインポート **(Import from structured file)**] カードをクリックします。

> **重要:**
> サポートされているファイル形式 (TXT、CSV、STIX 2.x JSON、MISP JSON、または構造化ファイル) で脅威インテリジェンスデータをインポートします。ファイルサイズの制限は 5 MB です。生のテキストの文字数制限は 10,000 文字です。

4. フォームのフィールドに入力します。

フィールド	説明
オプションを選択	ドロップダウンリストから、[観測事象] や [インジケーター] などの必要なオプションを選択します。 ○ 観測事象：インポートする観測事象データを選択します。 **注:** 観測事象データをインポートする場合は、このオプションを選択します。また、ファイル内の列ヘッダーを変更しないでください。必須フィールドは [値] と [タイプ] で、その他のフィールドはオプションです。また、日付/時刻を YYYY-MM-DDThh:mm:ssZ 形式で入力します。 ○ インジケーター：インポートするインジケーターデータを選択します。 **注:** インジケーターデータをインポートする場合は、このオプションを選択します。また、ファイル内の列ヘッダーを変更しないでください。[インジケーター] の必須フィールドは [パターン]、[パターンタイプ]、および [有効開始日] で、その他のフィールドはオプションです。また、日付/時刻を YYYY-MM-DDThh:mm:ssZ 形式で入力します。
インジケーターのサンプルファイルをプレビューおよびダウンロードする (Preview and download sample file for Indicators)	[プレビュー] リンクを使用してサンプルファイルをダウンロードし、CSV、XLS、XLSX などの互換性のあるファイル形式で構造化データをアップロードするには、このリンクを使用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: 列ヘッダーはヘッダーと正確に一致する必要があります。ファイルの各観測事象に [値] フィールドと [タイプ] フィールドが必要です。その他のフィールドはオプションです。[初回確認日 (First Seen)] と [最終確認日 (Last Seen)] は数値で、エポック時間 (ミリ秒単位) である必要があります。
ファイルをアップロード	推奨される構造化ファイル形式でファイルデータをアップロードするには、このリンクをクリックします。 **注:** 一度にアップロードできるのは 1 ファイルのみです。新しいファイルを追加するには、既存のファイルを削除してから新しいファイルを追加する必要があります。
定義の設定 **(Set definitions)**	
TLP	インポートされたレコードに適用する Traffic Light Protocol (TLP) インジケーターをドロップダウンリストから選択します。 TLP は TISC にあり、目的のユーザーと機密データが共有されるようにするために、さまざまな色でラベル付けされています。 ○ クリア：情報を制限なく共有できます。 ○ 赤 ○ 琥珀色 + 厳格 (AMBER+STRICT) ○ 琥珀色 ○ 緑
信頼性 (0～100)	インポートされたレコードの信頼度値を 0～100 の範囲で設定します。
有効期限 (日数) (Expiry Period (days))	インポートされたレコードの有効期間を入力します。 **注:** このフィールドは必須です。
タグ	
タグを追加	タグを使用して、このソースからシステムに取り込まれたレコードに注釈を付けたり、耳のマークを付けたりします。検索バーにタグ名を入力してシステムで使用可能なタグを選択する

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	か、新しいタグ名を入力して [追加] をクリックし、ソースにアサインします。
分類	
分類を選択 (Select a Taxonomy)	インポートされたデータの分類を選択します。分類を使用して、脅威インテリジェンスレコードにアサインされた分類として使用できる辞書を定義します。例：CAPEC 命名法。詳細については、「分類の作成」を参照してください。 注: 分類値のオプションは、選択した分類に基づいて変更されます。
ソース値を上書き (Override source value)	構成された値で TLP、信頼性、有効期限、タグ、および分類のソース値を上書きする場合は、このチェックボックスをオンにします。このチェックボックスをオンにしない場合、空でなければ構成された値が適用されます。

5. [次へ] をクリックします。
6. データを処理のために送信する前に確認します。

   注:
   インポートされたレコードのレビューは、STIX オプションではサポートされていません。

   [次へ] をクリックすると、ユーザーが上記のセクションで提供したすべての情報の概要が表示され、下のセクションにはインポートする必要があるすべてのレコードが表示されます。

   ユーザーは任意のタイプのアクティビティを実行でき、複数のユーザーは右側のコンテキストメニューにあるコメントセクションを使用して共同作業を行うことができます。インポートされたレコードのリストは、ファイル全体または生のテキストが処理されるとレンダリングされます。大きなファイルのインポート処理には時間がかかりますが、処理中はインポートレコードページからもステータスの確認、レビュー、送信が可能です。

   注:
   検証に失敗したレコードはインポートプロセスからスキップされ、そのようなレコードはそれ以上の処理を行うために [レビューおよび送信] ページに表示されません。

7. [更新タイプ] をクリックし、インポートされたレコードの任意のタイプを更新するタイプを選択します。
8. インポートされたレコードのタイプを削除するには、[削除] をクリックします。
9. [送信] をクリックします。

   注:
   インポートレコードを送信すると、構成された承認ルールに基づいて対応するインポートレコードを承認するため、ユーザーは承認者に誘導されます。レコードを作成している現在のユーザーが承認プロセスを必要としない場合、レコードは自動承認プロセスを経て、要求の送信時にインポートジョブが自動承認されます。

10. [ステータスを表示] をクリックしてインポートレコードのステータスを表示するか、[完了] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レコードが処理のためにインポートされると、処理済みステータスが表示されます。

11. [キャンセル] をクリックして、インポートプロセスを中止します。
12. 必要に応じて、[戻る] をクリックして前のページに戻り、レコードを確認します。

標準形式を使用したデータのインポート

サポートされているファイル形式 (STIX 2.x JSON、MISP JSON など) で標準データをアップロードします。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
   [脅威インテリジェンスライブラリ (Threat Intel Library)] ページが表示されます。
2. [インテリジェンスをインポート **(Import Intelligence)**]をクリックします。
3. [標準ファイルからインポート **(Import from standard file)**] カードをクリックします。

> **重要:**
> サポートされているファイル形式 (TXT、CSV、STIX 2.x JSON、MISP JSON、または構造化ファイル) で脅威インテリジェンスデータをインポートします。ファイルサイズの制限は 5 MB です。生のテキストの文字数制限は 10,000 文字です。

4. フォームのフィールドに入力します。

フィールド	説明
ファイル形式	ドロップダウンリストから [STIX 2.x JSON] や [MISP JSON] などの必要なオプションを選択します。 ○ **STIX 2.x JSON**：インポートの形式として [STIX 2.x JSON] を選択します。 ○ **MISP JSON**：インポートの形式として [MISP JSON] を選択します。
ファイルをアップロード	標準ファイル形式でデータをアップロードするには、このリンクをクリックします。
定義の設定 **(Set definitions)**	
TLP	インポートされたレコードに適用する TLP インジケーターをドロップダウンリストから選択します。
信頼性 (0～100)	信頼性の値を定義します。
有効期限 (日数) (Expiry Period (days))	インポートされたレコードの有効期間を入力します。 **注:** このフィールドは必須です。
タグを追加	タグを使用して、このソースからシステムに取り込まれたレコードに注釈を付けたり、耳の

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	マークを付けたりします。検索バーにタグ名を入力してシステムで使用可能なタグを選択するか、新しいタグ名を入力して [追加] をクリックし、ソースにアサインします。
分類	
分類を選択 (Select a Taxonomy)	インポートされたデータの分類を選択します。分類を使用して、脅威インテリジェンスレコードにアサインされた分類として使用できる辞書を定義します。例：CAPEC 命名法。詳細については、「分類の作成」を参照してください。
分類値を選択 (Select Taxonomy values)	分類に関連付けられている分類値を示します。
ソース値を上書き (Override source value)	構成された値から TLP、信頼性、有効期限、タグ、および分類のソース値を上書きする場合は、このチェックボックスをオンにします。このチェックボックスをオンにしない場合にはデフォルト値が適用されます。

5. [次へ] をクリックします。
6. データを処理のために送信する前に確認します。

   注:
   インポートされたレコードのレビューは、STIX オプションではサポートされていません。

   [次へ] をクリックすると、ユーザーが上記のセクションで提供したすべての情報の概要が表示され、下のセクションにはインポートする必要があるすべてのレコードが表示されます。

   ユーザーは任意のタイプのアクティビティを実行でき、複数のユーザーは右側のコンテキストメニューにあるコメントセクションを使用して共同作業を行うことができます。

   注:
   検証に失敗したレコードはインポートプロセスからスキップされ、そのようなレコードはそれ以上の処理を行うために [レビューおよび送信] ページに表示されません。

7. [更新タイプ] をクリックし、インポートされたレコードの任意のタイプを更新するタイプを選択します。
8. インポートされたレコードのタイプを削除するには、[削除] をクリックします。
9. [送信] をクリックします。

   注:

   インポートレコードを送信すると、構成された承認ルールに基づいて対応するインポートレコードを承認するため、ユーザーは承認者に誘導されます。レコードを作成している現在のユーザーが承認プロセスを必要としない場合、レコードは自動承認プロセスを経て、要求の送信時にインポートジョブが自動承認されます。

10. [ステータスを表示] をクリックしてレコードのステータスを表示するか、[完了] をクリックします。
    レコードが処理されると、処理済みステータスが表示されます。
11. [キャンセル] をクリックして、インポートプロセスを中止します。
12. 必要に応じて、[戻る] をクリックして前のページに戻り、レコードを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

生のテキストを使用したデータのインポート

生のテキストをコピー & ペーストするか、フリーテキスト入力して、観測事象データをインポートします。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
   [脅威インテリジェンスライブラリ (Threat Intel Library)] ページが表示されます。
2. [インテリジェンスをインポート **(Import Intelligence)**]をクリックします。

   重要:
   - デファンジング文字は、観測事象の解析と抽出の一環として消去されます。
   - この貼り付けられたテキストを使用するオプションでは、URL、ドメイン、ファイル名、ハッシュ、および IP アドレスのみが抽出され、他の観測事象タイプはデータインポートで抽出されません。また、レジストリ、ディレクトリタイプなどの他の観測事象タイプは、インポート時にスキップされます。

3. [生のテキストからインポート **(Import from raw text)**] カードをクリックします。

   重要:
   生のテキスト形式で脅威インテリジェンスデータをインポートする場合、文字数が 10,000 文字に制限されます。[生のテキスト] オプションは、PDF から観測事象を抽出するための回避策として使用できます。

4. フォームのフィールドに入力します。

フィールド	説明
生データテキストボックス (Raw data text box)	生のテキストを入力するか、コピーしてこのテキストボックスに貼り付けます。 **注:** 生のテキストは 10,000 文字以内まで入力または貼り付けることができます。
定義の設定 **(Set definitions)**	
TLP	インポートされたレコードに適用する TLP インジケーターをドロップダウンリストから選択します。
信頼性 (0～100)	信頼性の値を定義します。
有効期限 (日数) (Expiry Period (days))	インポートされたレコードの有効期間を入力します。 **注:** このフィールドは必須です。
タグを追加	タグを使用して、このソースからシステムに取り込まれたレコードに注釈を付けたり、耳の

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	マークを付けたりします。検索バーにタグ名を入力してシステムで使用可能なタグを選択するか、新しいタグ名を入力して [追加] をクリックし、ソースにアサインします。
分類	
分類を選択 (Select a Taxonomy)	インポートされたデータの分類を選択します。分類を使用して、脅威インテリジェンスレコードにアサインされた分類として使用できる辞書を定義します。例：CAPEC 命名法。詳細については、「分類の作成」を参照してください。

5. [次へ] をクリックします。
6. データを処理のために送信する前に確認します。

   [次へ] をクリックすると、ユーザーが上記のセクションで提供したすべての情報の概要が表示され、下のセクションにはインポートする必要があるすべてのレコードが表示されます。

   ユーザーは任意のタイプのアクティビティを実行でき、複数のユーザーは右側のコンテキストメニューにあるコメントセクションを使用して共同作業を行うことができます。

   > **注:**
   > 検証に失敗したレコードはインポートプロセスからスキップされ、そのようなレコードはそれ以上の処理を行うために [レビューおよび送信] ページに表示されません。

7. [更新タイプ] をクリックし、インポートされたレコードの任意のタイプを更新するタイプを選択します。
8. インポートされたレコードのタイプを削除するには、[削除] をクリックします。
9. [送信] をクリックします。

   > **注:**
   > インポートレコードを送信すると、構成された承認ルールに基づいて対応するインポートレコードを承認するため、ユーザーは承認者に誘導されます。レコードを作成している現在のユーザーが承認プロセスを必要としない場合、レコードは自動承認プロセスを経て、要求の送信時にインポートジョブが自動承認されます。

10. [ステータスを表示] をクリックしてレコードのステータスを表示するか、[完了] をクリックします。
    レコードが処理されると、処理済みステータスが表示されます。
11. [キャンセル] をクリックして、インポートプロセスを中止します。
12. 必要に応じて、[戻る] をクリックして前のページに戻り、レコードを確認します。

非構造化ファイル形式を使用したデータのインポート

TXT、CSV、JSON、XLS、XLSX などのファイル形式を使用して、サポートされている非構造化形式のデータをアップロードします。

始める前に

必要なロール：sn_sec_tisc.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
   [脅威インテリジェンスライブラリ (Threat Intel Library)] ページが表示されます。
2. [インテリジェンスをインポート **(Import Intelligence)**]をクリックします。

> **重要:**
> - デファンジング文字は、観測事象の解析と抽出の一環として消去されます。
> - この非構造化ファイル形式オプションでは、URL、ドメイン、ファイル名、ハッシュ、および IP アドレスのみが抽出され、他の観測事象タイプはデータインポート用に抽出されず、レジストリ、ディレクトリタイプなどのそのようなタイプの観測事象の場合、それらはインポートからスキップされます。

3. [ファイル (非構造化) からインポート **(Import from file (unstructured))**] カードをクリックします。

> **注:**
> サポートされているファイル形式 (TXT、CSV、STIX 2.x JSON、MISP JSON、または構造化ファイル) で脅威インテリジェンスデータをインポートします。ファイルサイズの制限は 5 MB です。

4. フォームのフィールドに入力します。

フィールド	説明
ファイルをアップロード	標準ファイル形式でデータをアップロードするには、このリンクをクリックします。
定義の設定 **(Set definitions)**	
TLP	インポートされたレコードに適用する TLP インジケーターをドロップダウンリストから選択します。
信頼性 (0～100)	信頼性の値を定義します。
有効期限 (日数) (Expiry Period (days))	関連する観測事象の有効期限を入力します。 **注:** このフィールドは必須です。
タグを追加	タグを使用して、このソースからシステムに取り込まれたレコードに注釈を付けたり、耳のマークを付けたりします。検索バーにタグ名を入力してシステムで使用可能なタグを選択するか、新しいタグ名を入力して [追加] をクリックし、ソースにアサインします。
分類	
分類を選択 (Select a Taxonomy)	インポートされたデータの分類を選択します。分類を使用して、脅威インテリジェンスレコードにアサインされた分類として使用できる辞書を定義します。例：CAPEC 命名法。詳細については、「分類の作成」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. データを処理のために送信する前に確認します。

   [次へ] をクリックすると、ユーザーが上記のセクションで提供したすべての情報の概要が表示され、下のセクションにはインポートする必要があるすべてのレコードが表示されます。

   ユーザーは任意のタイプのアクティビティを実行でき、複数のユーザーは右側のコンテキストメニューにあるコメントセクションを使用して共同作業を行うことができます。

   注:
   データのインポートでサポートされている形式は TXT、CSV、JSON、XLS です。検証に失敗したレコードはインポートプロセスからスキップされ、それらのレコードは [レビューと送信] ページに表示されません。

6. [更新タイプ] をクリックし、インポートされたレコードの任意のタイプを更新するタイプを選択します。
7. インポートされたレコードのタイプを削除するには、[削除] をクリックします。
8. [送信] をクリックします。

   注:
   インポートレコードを送信すると、構成された承認ルールに基づいて対応するインポートレコードを承認するため、ユーザーは承認者に誘導されます。レコードを作成している現在のユーザーが承認プロセスを必要としない場合、レコードは自動承認プロセスを経て、要求の送信時にインポートジョブが自動承認されます。

9. [ステータスを表示] をクリックしてレコードのステータスを表示するか、[完了] をクリックします。
   送信が正常に完了すると、そのレコードの処理済みステータスが表示されます。
10. [キャンセル] をクリックして、インポートプロセスを中止します。
11. 必要に応じて、[戻る] をクリックして前のページに戻り、レコードを確認します。

自動翻訳

脅威アナリストワークベンチ

[脅威アナリストワークベンチ (Threat Analyst Workbench)] ページは、脅威アナリストおよびチームの管理下にあるケースやケースタスクで構成されています。

[ケース管理] 機能を使用して、脅威調査や分析アクティビティを作成および追跡します。

脅威調査では、アナリストが観測事象、攻撃者、キャンペーンなどの内部インテリジェンスレコードからデータを収集します。

ワークベンチの概要

[ワークベンチの概要] ページは、脅威アナリストおよびチームの管理下にあるケースタスクやケースで構成されています。

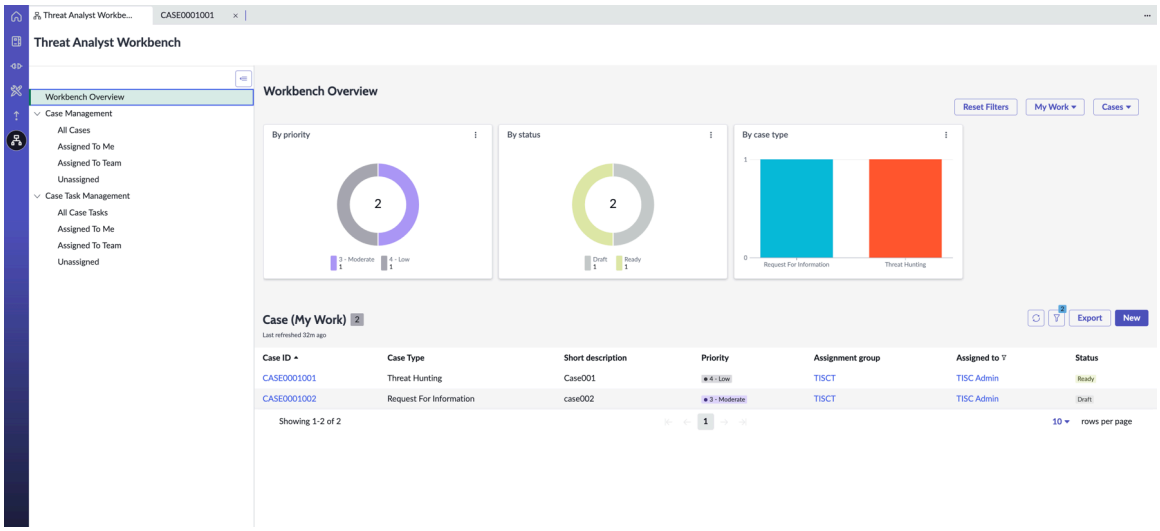
概要にはオープンケースとステータスが一覧表示され、アナリストは作業負荷を管理し、調査に優先順位を付けることができます。

必要なロール：sn_sec_tisc.analyst、sn_sec_tisc.admin

ケースが作成されると、アナリストはケースタスクを他のアナリストやチームにアサインして、調査をさらに進めることができます。さらに、彼らとコラボレーションして情報やインサイトを共有することもできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

各フィルターの下には、セキュリティアナリストやセキュリティアナリストチームのキューにある「優先度」「ステータス」「ケースタイプ」別にグループ化されたさまざまなウィジェットがあります。



ウィジェットでフィルターを適用すると、概要ページの下半分に、該当のケースやケースタスクがリストアイテムとして表示されます。適用されているフィルターを解除するには、[フィルターをリセット] をクリックして元のビューにリセットします。

脅威アナリストと管理者は、このページで自分の作業、チームの作業、未アサインの作業を表示することができます。ドロップダウンリストで操作ができます。使用可能なオプションは、次のとおりです。

- [自分の作業]：自分に割り当てられた作業を表示するには、このオプションを選択します。
- [自分のチームの作業]：自分が属しているすべてのグループにおいて、アサインされているチームの作業を表示するには、このオプションを選択します。
- [未アサインの作業]：アサインされていないケースやケースタスクを表示するには、このオプションを選択します。ケースやケースタスクをアサインするには、フォームビューに移動して、ユーザーやユーザーグループをケースやケースタスクにアサインする必要があります。

また、自分に割り当てられているケースやケースタスクは、[ワークベンチの概要] から直接表示することもできます。デフォルトではケースビューが表示されます。優先度やステータス別にケースタスクを表示する場合は、ドロップダウンでケースタスクを選択できるようになっています。

脅威アナリストワークベンチを使用したケースを作成する

ケースは、組織を脅かすキャンペーンまたは攻撃者に関する情報を追跡するために使用されます。ケースを作成した後、アーティファクトを追加することで、1 つのケースまたはケースタスクからすべての関連情報を確認および分析することができます。

始める前に

必要なロール：sn_sec_tisc.analyst、sn_sec_tisc.admin

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [脅威アナリストワークベンチ **(Threat Analyst Workbench)]** アイコンをクリックします。
3. 検索項目 ケースの管理 > すべてのケース.
   すべてのケースが表示されます。
4. [新規] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. 必要に応じてフィールドを入力します。

新規ケースの作成

フィールド	説明
ケース ID	ケースの一意の識別子。これはシステム生成 ID です。
簡単な説明	調査中の要求または問題の概要、または簡単な説明。
説明	バックグラウンド、必要な分析、期待される結果など、ケースの関連情報などの詳細な説明。
ケースのタイプ	調査対象のケースタイプを選択します。調査の可能なオプションは、次のとおりです。 ○ 脅威の検出 ○ 情報の要求 ○ 脆弱性管理ケース ○ コンプライアンスケース ○ インシデントレスポンスケース ○ コラボレーションケース ○ その他
優先度	要求または問題の重大度のアセスメント。
アサイン先グループ	ケースの作業を担当するアサイン先グループ。
ステータス	ケースの現在のステータス。
アサイン先	ケースの作業を担当するアナリスト。
期日	タスクが完了またはクローズとなる予定日時。
貢献者	タスクからロールアップされ、その上に追加できるアサイニーのリスト。
TLP	TLP に基づくデータの機密性の設定を示す一意の値。
ウォッチリスト	ユーザーがウォッチリストに追加されると、そのユーザーはステータスと優先度の変更に関するメール通知を受信します。
制限の適用	許可されたグループのメンバーと許可されたメンバーを変更するには、このチェックボックスをオンにします。詳細については、「ケースに適用される制限」を参照してください。

6. 必要に応じて、[インサイト] セクションのフィールドに入力します。

インサイト

フィールド	説明
メモ	脅威調査に関連する追加のメモ。

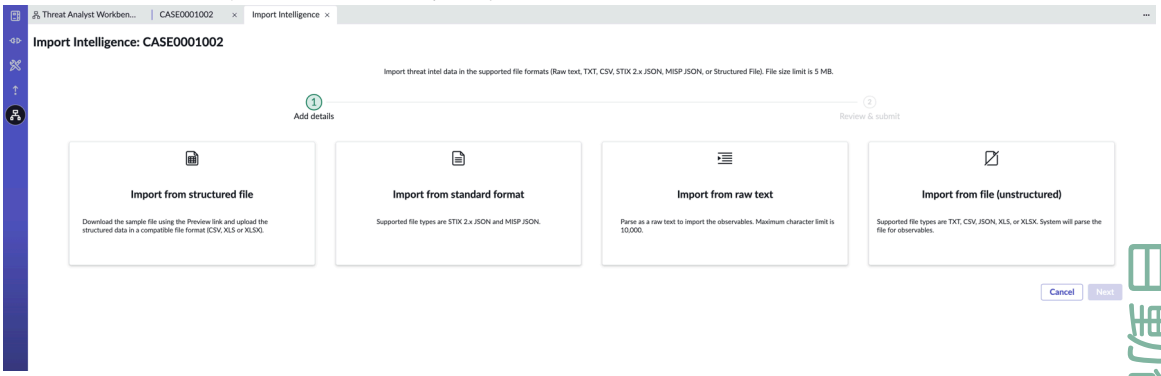
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
推奨またはアクション	脅威の調査に関連する推奨事項またはアクション。
分析と結果	脅威調査に関連する分析と結果を入力します。
クローズの概要	検索結果に関するクローズの概要を追加します。

7. [保存] をクリックします。
   レコードを保存した後、[インテリジェンスをインポート **(Import Intelligence)]** タブをクリックし、 インポートインテリジェンス機能を使用して脅威インテリジェンスデータをインポートできます。

   注:
   ケース管理からデータをインポートして処理する場合は、一意のものがインポートレコードに関連付けられます。



ケースに適用される制限

この機能を使用して、ケースに制限をかけ、アクセスできるグループやユーザーのリストを提供します。

必要なロール：

- sn_sec_tisc.analyst
- sn_sec_tisc.admin
- sn_sec_tisc.restriction_access_manager

主な考慮事項

1. ケースに制限をかけ、そのケースにアクセスできるグループ / ユーザーのリストを提供します。
2. [ケース] フォームページの [制限の適用] フィールドを有効にします。
3. 許可されたグループのメンバーや許可されたメンバーを変更します。
4. ケースが制限付きとしてマークされると、許可されたグループのメンバー、許可されたユーザーリストのメンバー、および sn_sec_tisc.admin ロールを持つユーザーのみがこのケースにアクセスできます。
5. [制限の適用] フィールドにアクセスする必要があるアナリスト (このロールを持つ sn_sec_tisc.restriction_access_manager) にアクセス権を付与します。
6. 既存のassigned_toアナリストと制限付きとしてマークしたアナリストも、許可されたグループまたはメンバーに追加されていない場合、アクセス権が失われます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. CTI チーム内でのケースの制限は、ケースごとに実装されます。許可されたメンバーは、許可リストに入っている場合、制限付きケースにアクセスできます。いずれかのケースの許可リストに入っていても、他の制限付きケースにすべてアクセスできるわけではありません。
8. ケースが制限付きとしてマークされ、許可されたメンバーまたは許可されたグループが空白の場合、制限付きケースにアクセスできるのは sn_sec_tisc.admin のみとなります。
9. アナリスト (sn_sec_tisc.analyst) ロールが割り当てられているグループのみが、[許可されたメンバー] および [許可されたグループ] リストに表示されます。

> **注:**
> ケースが制限付きとしてマークされている場合、作業メモがポストされます。

ケースのアクセス制御

ケースに固有のアクセス制御を許可します。

次の表では、ロールとアクセス制御について説明します。

ロール	アクセス	説明
sn_sec_tisc.restriction_access_manager	読み取りアクセス	ここで追加された外部ユーザーには、ケースフォームを表示できるアクセス権が付与されますが、ケースのフィールドを編集したり、アクションを実行したりすることはできません。
	特権アクセス	ここで追加された外部ユーザーには、ケースフォームのあらゆるフィールドを編集できるアクセス権が付与されますが、オーケストレーションを実行することはできません。
sn_sec_tisc.special_access_read_manager	読み取りアクセス	ここで追加された外部ユーザーには、ケースフォームを表示できるアクセス権が付与されますが、ケースのフィールドを編集したり、アクションを実行したりすることはできません。
sn_sec_tisc.special_access_write_manager	特権アクセス	ここで追加された外部ユーザーには、ケースフォームのあらゆるフィールドを編集できるアクセス権が付与されますが、オーケストレーションを実行することはできません。

ケースタスクの外部ユーザーアクセス

このセクションでは、ケースタスクの外部ユーザーアクセスについて説明します。

外部ユーザーへのケースタスクのアサイン

ケースタスクは、sn_sec_tisc.analyst ロールへのアクセス権がない場合でも、外部ロールを持つユーザーにアサインされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. ケースタスクがアサインされた外部ユーザーは、ケースタスクモジュールの表示のみが可能で、ケースタスクを編集する権限があります。
2. 外部ユーザーは、その特定のユーザーまたはユーザーが属するグループにアサインされたケースタスクのみを表示できます。
3. 外部ユーザーは、ユーザーが属するグループ内でタスクを再アサインできる必要があります。

MITRE テクニックをケースに関連付ける

1 つまたは複数の MITRE テクニックをケースに関連付けます。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [脅威アナリストワークベンチ **(Threat Analyst Workbench)]** アイコンをクリックします。
3. 検索項目 ケースの管理 > すべてのケース.
   すべてのケースが表示されます。
4. 任意のケースを選択します。
5. **[MITRE** テクニックを関連付ける] ボタンをクリックします。
6. [マトリクスを追加] をクリックして MITRE テクニックを関連付けます。
   [MITRE テクニックをケースに関連付ける **(Associate MITRE Technique to Case)]** ダイアログボックスが表示されます。
7. マトリクスを選択します。
   有効なマトリクスがすべて表示され、マトリクスを選択できるようになります。
8. ドロップダウンリストから戦術を選択します。
   マトリクスに関連付けられている戦術がすべて表示されます。

   注:
   さらに戦術を追加する場合は、[戦術を追加] をクリックします。戦術を新たに追加する場合、以前に選択した戦術はドロップダウンリストに表示されなくなります。

9. テクニックを選択します。
   選択した戦術に関連付けられているテクニックがすべて表示されます。戦術をさらに追加する場合、選択した戦術に関連付けられているテクニックを選択できます。
10. [保存] をクリックします。
    マトリクスに関連付けられているデータをすべて削除してから [マトリクスを削除] をクリックすると、関連付けられているマトリクスデータが削除されるだけで、マトリクスは MITRE ATT&CK リポジトリに残ります。

    関連付けられているマトリクスデータレコードは [MITRE ATT&CK カード] セクションに表示されます。カードビュー：

    注:
    [マトリクス] ドロップダウンリストから、複数のマトリクス間で切り替えることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. カードビューの最初の行には、現在選択されているマトリクスに関連する戦術がすべて表示されます。

b. 各戦術カードには、現在のケースレコードにマッピングされた戦術の名前とテクニックの数が表示されます。

c. ケースに関連するテクニックはすべて、各戦術の下に縦並びで表示されます。テクニックをクリックすると、テクニックのフォームビューが表示されます。

11. **[ID** を表示] をクリックすると、関連するすべてのテクニックの ID が表示されます。

> 注:
> 各テクニックカードには、**[ID** を表示] が有効になっている場合のみ、テクニック名とテクニック ID が表示されます。

12. [リフレッシュ] をクリックして、カードビューを更新します。
選択したマトリクスの前回の更新のタイムスタンプを表示できます。

> 注:
> ポップアウトアイコンをクリックして、関連するマトリクスカードをポップアウトし、新しいタブに表示します。

MITRE テクニックの関連付けのロールアップ

ケースレコードにリンクされている、またはリンク解除されている観測事象、インジケーター、オブジェクト、およびセキュリティインシデントからの MITRE テクニックの関連付けのロールアップ。

始める前に

> 注:

- セキュリティインシデントの MITRE テクニック関連付けのロールアップでは、セキュリティインシデントの MITRE テクニック関連データが TISC のケース管理にロールアップされます。
- デフォルトでは、このプロパティ sn_sec_tisc.auto_rollup_mitre_data は MITRE テクニックに対して有効になっており、関連するオブジェクトまたはセキュリティインシデントからケースに自動的にロールアップされます。
- MITRE テクニックの関連付けのオンデマンドロールアップを実行する場合は、[ケース] フォームビュー 内のその他のアクションに移動し、[**MITRE** テクニックをロールアップ] オプションを選択します。この操作は非同期に行われ、[アクティビティストリーム] セクションでロールアップアクティビティの更新を確認できます。

必要なロール：sn_sec_tisc.analyst

このタスクについて

- 観測事象やインジケーターなどのエンティティがケースにリンクされると、そのエンティティに存在するすべての MITRE テクニックの関連付けが自動的にケースにロールアップされます。
- 観測事象やインジケーターなどのエンティティがケースからリンク解除されて削除されると、そのエンティティに存在するケースからロールアップされたすべての MITRE テクニックの関連付けが自動的に削除され、ケースにロールアップされます。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [脅威の **Analyst Workbench]** アイコンをクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. 検索項目 ケースの管理 > すべてのケース.
すべてのケースが表示されます。
4. 任意のケースをオープンします。
5. [アーティファクト **(Artifacts)]** タブに移動します。
6. アーティファクト関連リストから [観測事象] を選択します。
7. [リンク] ボタンを選択します。
8. ケースにリンクできる観測事象を選択します。
9. [リンク] をクリックして観測事象をリンクします。
観測事象をケースにリンクすると、その特定の観測事象に関連付けられた MITRE テクニックが自動的にロールアップされ、[アーティファクト] セクションの [MITRE テクニック] リストの数が自動的に更新されます。
10. [リンクを解除] をクリックして、ケースから観測事象のリンクを解除します。
観測事象をケースにリンク解除すると、その特定の観測事象に関連付けられた MITRE テクニックが自動的に削除され、[アーティファクト] セクションの [MITRE テクニック] リストの数が自動的に更新されます。

脅威アナリストワークベンチでケースタスクを作成する

ケースタスクを作成してケースに関連付けます。

始める前に

必要なロール：sn_sec_tisc.analyst、sn_sec_tisc.admin

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [脅威アナリストワークベンチ **(Threat Analyst Workbench)]** アイコンをクリックします。
3. 検索項目 ケースタスク管理 > すべてのケースタスク.
ケースタスクがすべて表示されます。
4. [新規] をクリックします。
5. 必要に応じてフィールドを入力します。

新規のケースタスクを作成

フィールド	説明
タスク ID	ケースタスクの一意の識別子。これはシステム生成 ID です。
簡単な説明	調査中の要求または問題の概要、または簡単な説明。
説明	ケースタスクの関連情報などの詳細な説明 (バックグラウンド、必要な分析、期待される結果など)。
親ケース ID	ルックアップから親ケース ID を選択します。
優先度	要求または問題の重大度のアセスメント。
アサイン先グループ	ケースタスクの作業を担当するアサイン先グループ。
ステータス	ケースタスクの現在のステータス。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
アサイン先	ケースタスクの作業を担当するアナリスト。
期日	ケースタスクが完了またはクローズとなる予定日時。
TLP	TLP に基づくデータの機密性の設定を示す一意の値。
制限の適用	sn_sec_tisc_admin として、このチェックボックスをオンにして、許可グループのメンバーと許可メンバーを変更します。詳細については、「ケースに適用される制限」を参照してください。

6. 必要に応じて、[インサイト] セクションのフィールドに入力します。

インサイト

フィールド	説明
メモ	脅威調査に関連する追加のメモ。
クローズ	検索結果に関するクローズの概要を追加します。

7. [保存] をクリックします。
ケースタスクがケースに関連付けられます。

> **注:**
> ケースタスクを保存した後、タグと分類をタスクに追加することができます。詳細については、「分類の作成」を参照してください。7

ケースまたはケースタスクにアーティファクトを追加する

ケースを作成したら、セキュリティインシデント、CI、セキュリティ侵害のインジケーターなどのアーティファクトをケースに表示または追加できます。これらのアーティファクトは、ケースを解決する手掛かりとなるものです。

始める前に

必要なロール：admin

> **注:**
> アーティファクトは、既存のケースでのみ使用できます。観測事象およびインジケーターの場合は、[インテリジェンスをインポート] ボタンを使用して、インポートジョブからアーティファクトをケースに追加または関連付けることもできます。インポート方法の詳細については、「脅威インテリジェンスのインポート」を参照してください。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [脅威アナリストワークベンチ **(Threat Analyst Workbench)]** アイコンをクリックします。
3. 検索項目 ケースの管理 > すべてのケース.
すべてのケースが表示されます。
4. 任意のケースまたはケースタスクを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

5. [アーティファクト **(Artifacts)]** タブに移動します。
   関連するアーティファクトは、その特定のケースまたはケースタスクの関連リストとして表示されます。
6. ケースまたはケースタスクからレコードをリンクまたはリンク解除します。

   注:
   詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。

次の表に、ケースまたはケースタスクに関連するアーティファクト関連リストを示します。

関連レコード

関連リスト	説明
MITRE テクニック	ケースに関連する MITRE テクニックを一覧表示します。 MITRE テクニックでは、ケース内の関連するテクニックもすべて表示されます。
観察事項	このケースまたはケースタスクに関連する観測事象のリスト。
インジケーター	このケースまたはケースタスクに関連するインジケーターのリスト。
攻撃パターン	このケースまたはケースタスクに関連する攻撃パターンのリスト。
キャンペーン	このケースまたはケースタスクに関連するキャンペーンを一覧表示します。
対処措置	このケースまたはケースタスクに関連する対処措置を一覧表示します。
データコンポーネント	このケースまたはケースタスクに関連するデータコンポーネントのリスト。
脅威グループ化	このケースまたはケースタスクに関連する脅威グループ化を一覧表示します。
ID	このケースまたはケースタスクに関連する ID を一覧表示します。
インフラストラクチャ	このケースまたはケースタスクに関連するシステム、ソフトウェアサービス、および関連する物理リソースまたは仮想リソースなどのインフラストラクチャを一覧表示します。
侵入セット	このケースまたはケースタスクに関連する共通プロパティを持つ一連の攻撃者の行動やリソースなどの侵入セットを一覧表示します。
場所	このケースまたはケースタスクに関連する場所レコードを一覧表示します。
マルウェア	このケースまたはケースタスクに関連するマルウェアソースレコードを一覧表示します。
マーキング定義	このケースまたはケースタスクに関連するマーキング定義レコードを一覧表示します。
脅威メモ	このケースまたはケースタスクに関連するマーキング定義レコードを一覧表示します。
観測データ	このケースまたはケースタスクに関連する観測データを一覧表示します。
脅威に関する意見	このケースまたはケースタスクに関連する脅威に関する意見を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連リスト	説明
脅威レポート	このケースまたはケースタスクに関連する脅威レポートを一覧表示します。
サイティング	このケースまたはケースタスクに関連するサイティングのリスト。
攻撃者	このケースまたはケースタスクに関連する攻撃者を一覧表示します。
ツール	このケースまたはケースタスクに関連するツールを一覧表示します。
脆弱性	観測事象が IP アドレスの場合、このリストには、このケースまたはケースタスクに関連する、一致する IP アドレスを持つすべてのリソース (構成アイテム) が表示されます。
関連ケース	関連ケースを一覧表示します。
関連ケースタスク	関連ケースタスクを一覧表示します。
セキュリティインシデント	このケースまたはケースタスクに関連するセキュリティインシデントを一覧表示します。
影響を受ける構成アイテム	このケースまたはケースタスクに関連する、影響を受ける構成アイテムを一覧表示します。
影響を受けるサービス	このケースまたはケースタスクに関連する、影響を受けるサービスを一覧表示します。
影響を受ける資産	このケースまたはケースタスクに関連する、影響を受ける資産を一覧表示します。
脆弱性エントリー	このケースまたはケースタスクに関連する脆弱性エントリーを一覧表示します。

自動翻訳

ケース内で拡張アクションを実行

このセクションを使用して、拡張アクションがケースに対してどのように実行されるかを理解します。

始める前に

必要なロール：sn_sec_tisc.admin

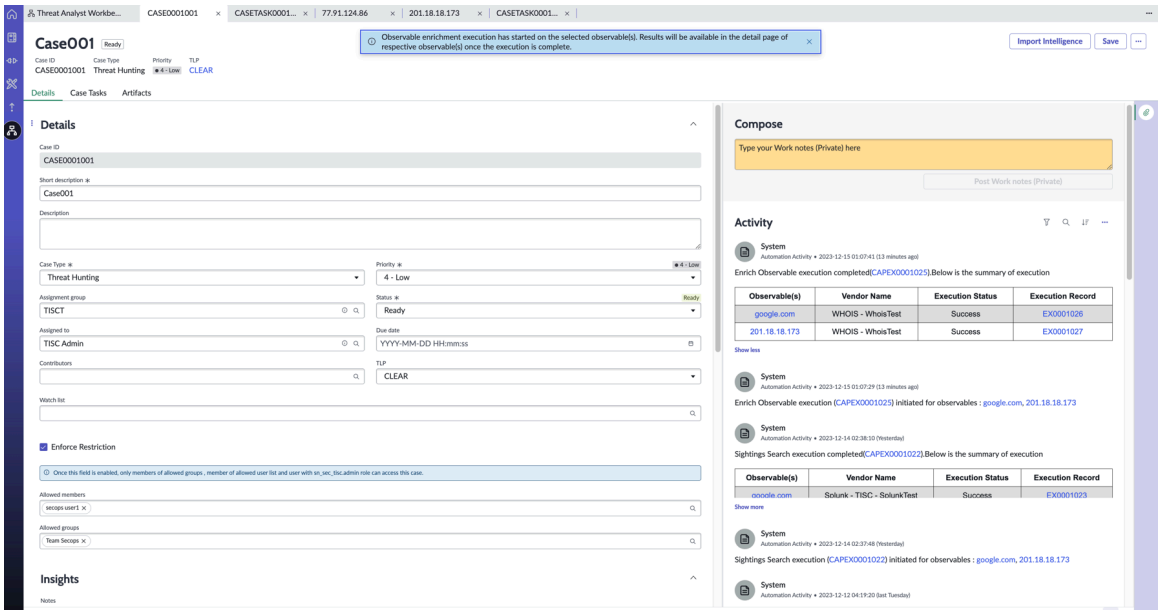
手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [脅威アナリストワークベンチ **(Threat Analyst Workbench)]** アイコンをクリックします。
3. 検索項目 ケースの管理 > すべてのケース.
   すべてのケースが表示されます。
4. 任意のケースまたはケースタスクを選択します。
5. [アーティファクト **(Artifacts)]** タブに移動します。
6. [観測事象] 関連リストを選択します。
7. 観測事象を 1 つ以上選択します。
8. ドロップダウンリストから任意の拡張アクションをクリックします。
9. 利用可能な実装を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

10. [送信] をクリックします。
    たとえば、[脅威のルックアップを実行] などです。選択した拡張アクションが実行され、[選択した観測事象で観測事象の拡張実行が開始されました。実行が完了すると、それぞれの観測事象の詳細ページで結果を確認できます。(Observable enrichment execution has started on the selected observable(s). Results will be available in the detail page of respective observable(s) once the execution is complete.)] という情報メッセージが表示されます。

    注:
    実行が開始または完了すると、作業メモがフォームビューのアクティビティストリームにポストされます。



ケースレポートの表示

ケースレポート機能を使用して、ケースに関連するレポートを生成します。これらのレポートには、調査後のレポートやエグゼクティブサマリーレポートが含まれます。

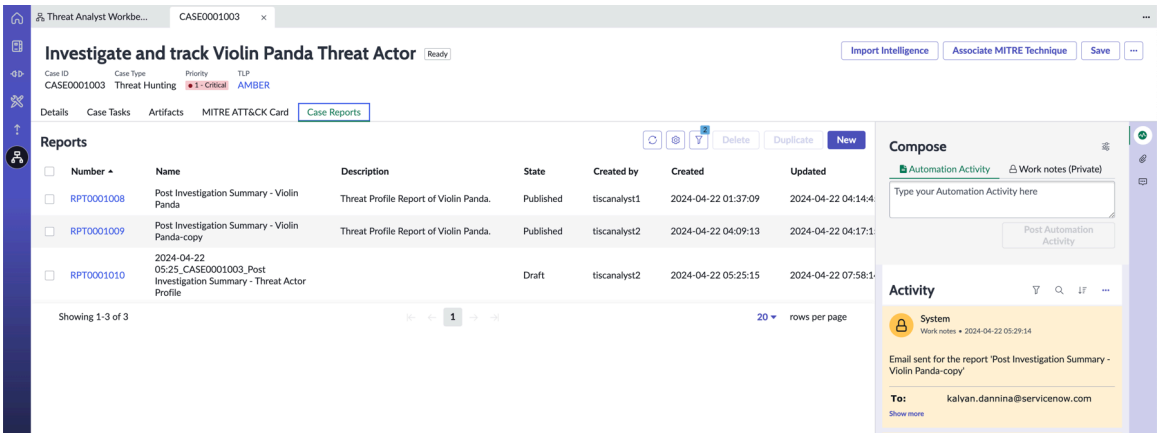
始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [脅威アナリストワークベンチ **(Threat Analyst Workbench)]** アイコンをクリックします。
3. 検索項目 ケースの管理 > すべてのケース.
   すべてのケースが表示されます。
4. 任意のケースを選択します。
5. [ケースレポート] に移動します。

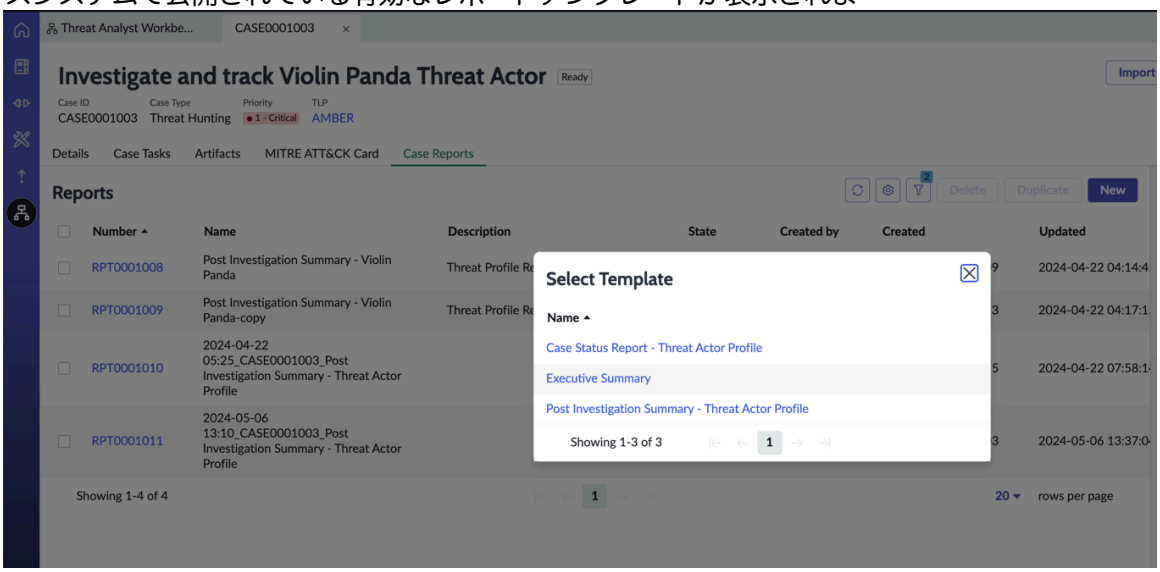
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
リストからレポートを削除したり、既存のレポートの複製を作成したり、独自のレポートにカスタマイズしたりできます。

6. [新規] をクリックします。
ベースシステムで公開されている有効なレポートテンプレートが表示されます。



7. 目的のレポートテンプレートを選択します。
レポートタイプに対して選択したレポートテンプレートが生成されます。また、レポートが公開されると大勢のユーザーがレポートを表示できるようになりますが、レポートのステータスが「ドラフト」の場合は、レポートがユーザーに表示されません。アナリストは公開されているレポートのみ表示でき、ドラフトステータスのレポートは表示できません。

注:

- さらにフィールドを追加する場合は、フィールドを選択してケースレポート内に直接追加します。
- 関連リストを追加する場合、観測事象のリストであれば [観測事象] を選択します。特定のケースに関連付けられている観測事象がすべて一覧表示されます。観測事象を 1 つ以上選択して、[追加] をクリックします。必要な観測事象をフィルタリングして、ケースに追加しても構いません。

8. [コンテンツを保存する] をクリックして、レポートのコンテンツを保存します。
9. [プレビュー] をクリックして、レポートをプレビューします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
次の操作を実行できます。

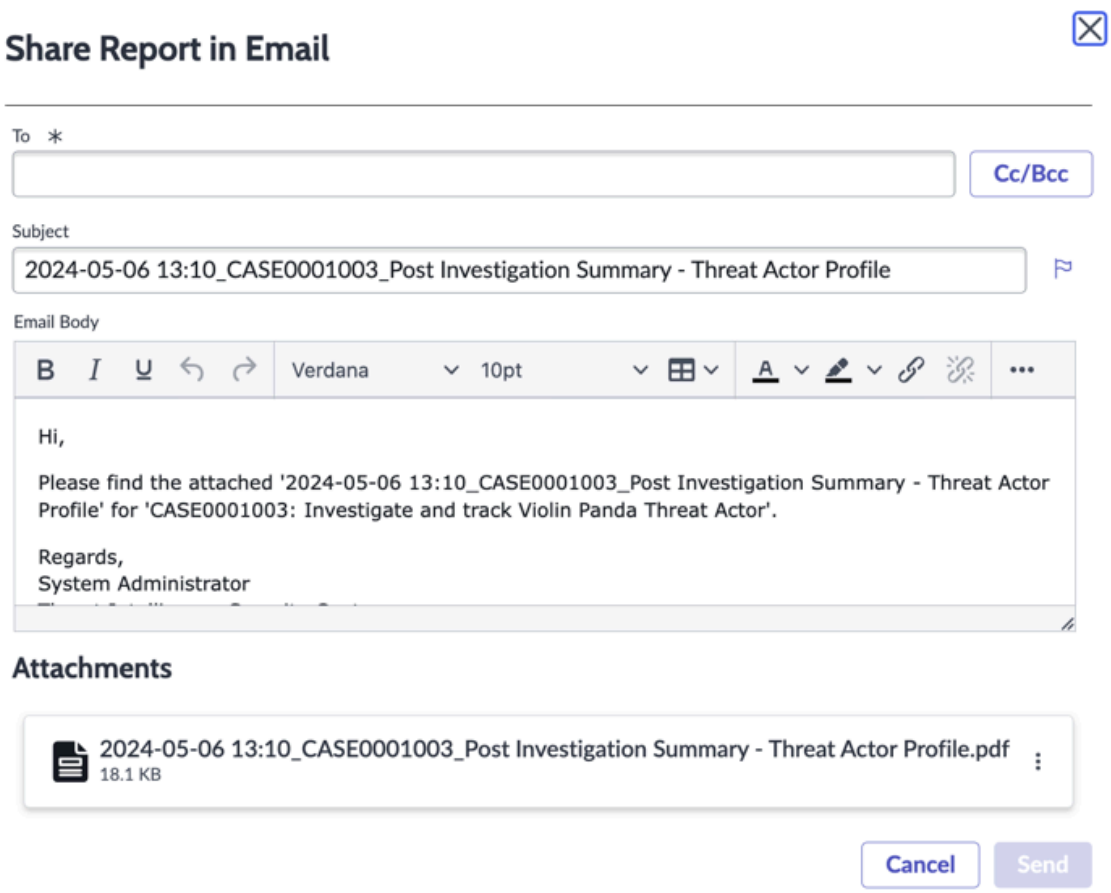
- レポートのウィンドウを最大化。
- [ダウンロード] アイコンでレポートをダウンロード。
- 長さや大きさのあるレポートを見やすくする場合は、レポートを新しいタブにポップアウト表示させます。
- [レポート名] と [レポートの説明] を編集します。
- レポートを公開します。

10. [コンテンツの編集] ボタンをクリックして、レポートを再公開します。

注:
レポートが共有されることを伝える警告メッセージが表示されます。

レポートをダウンロードまたは共有するには、変更した後にレポートを再公開する必要があります。編集を続行しますか?

11. [編集] をクリックします。
レポートを編集する場合は、説明に従ってレポートの編集を続行します。そうでなければ、レポートを公開することができます。公開されると、レポートは読み取り専用になります。
12. [レポートをメールで共有] をクリックして、レポートを共有します。
レポートを共有しているときは、生成された PDF レポートが添付ファイルとしてメールに添付されま



す。

13. To (レポートを共有する相手)、CC、BCC など、必要なメールフィールドを追加

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

14. 必要に応じて、メールに「重要」マークを付けます。
15. [送信] をクリックします。
    レポートが大勢のユーザーと共有されます。

安全な添付ファイルをアップロード

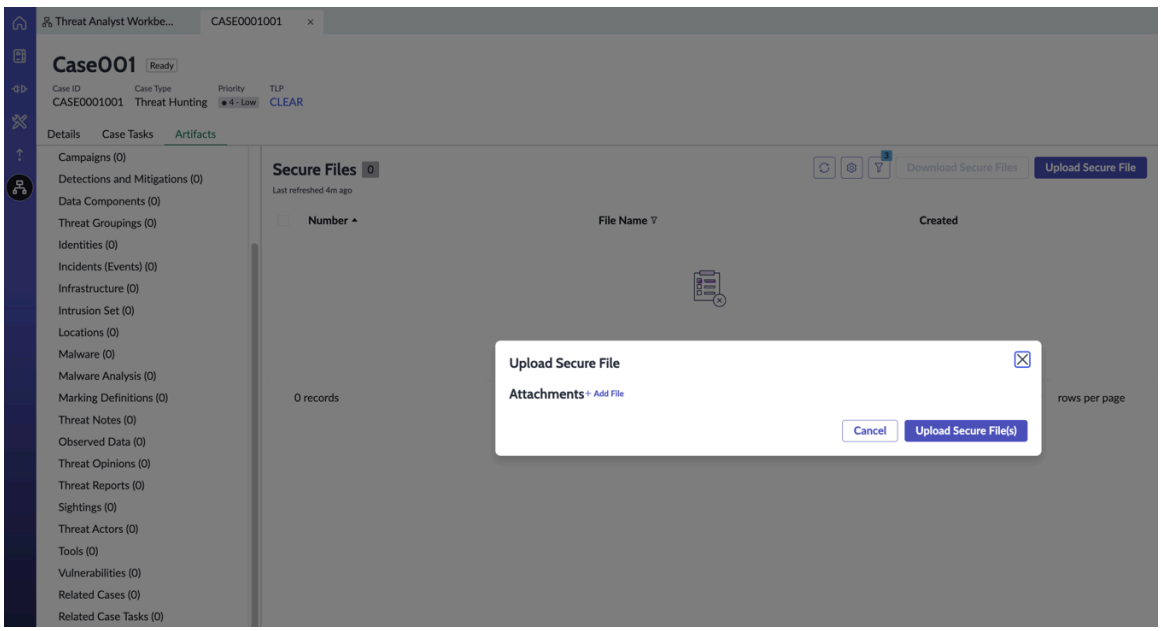
このセクションを使用して、安全な添付ファイルをケースにアップロードする方法を理解します。

始める前に
必要なロール：sn_sec_tisc_secure_file_access、sn_sec_tiscadmin

> **注:**
> [安全なファイル (Secure Files)] 関連リストは、ユーザーロール sn_sec_tisc.secure_file_access がある場合にのみ表示されます。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [脅威アナリストワークベンチ **(Threat Analyst Workbench)]** アイコンをクリックします。
3. 検索項目 ケースの管理 > すべてのケース.
   すべてのケースが表示されます。
4. 任意のケースを選択します。
5. 検索項目 アーティファクト > 安全なファイル 関連リスト。
6. [安全なファイルをアップロード **(Upload Secure File)]** ボタンをクリックします。
7. [ファイルを追加] をクリックして添付ファイルを追加します。
8. ファイルを選択し、[安全なファイルをアップロード **(Upload Secure File)]** ボタンをクリックします。
   添付ファイルがアップロードされます。



9. [安全なファイルをダウンロード **(Upload Secure File)]** をクリックして、添付ファイルをダウンロードします。
   添付ファイルは zip 形式で利用できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

10. または、安全なファイルレコードの詳細ページに移動してファイルをダウンロードすることもできます。

    注:

    - すべての安全な添付ファイルは暗号化され、キー管理フレームワーク (KMF) を使用してシステムに保存されます。詳細については、「添付ファイルの暗号化」を参照してください。
    - ユーザーが *ServiceNow* 統合ハブ**Professional Pack Installer** のサブスクリプションを持っている場合、安全なファイルは zip 形式で圧縮され、暗号化されて保存されます。

脅威インテリジェンスセキュリティセンター ライブラリ

脅威ライブラリは、構造化セキュリティ脅威情報と非構造化セキュリティ脅威情報を組織に提供する、体系的なオブジェクトとエンティティのグループとして定義されます。

脅威情報はフィードの形式で入手できます。フィードは、STIX や MISP などのソースからの貴重な脅威データを提供します。このデータには、脅威インテリジェンスのエンティティのリストが含まれています。

脅威インテリジェンスセキュリティセンターライブラリでは、データを使用した参照をはじめ、基本検索 / 詳細検索 / ルールのフィルタリングによる参照、インポートアシスタントの呼び出し、手動による脅威インテリジェンスレコードの追加、必要なアクション (許可リスト、拒否リスト、ウォッチリストへの追加など) の実行の方法について説明しています。

詳細なビューにより、インテリジェンスレコードに対するインサイトを利用したり、リストビューから複数のレコードで迅速にアクションを実行したりすることができます。

データモデルの概要

脅威インテリジェンスセキュリティセンターモジュールのデータモデルやアーキテクチャでは、脅威インテリジェンのスプラットフォーム機能や、脅威アナリストに詳細データを提供するさまざまなセキュリティビューをサポートできるようになっています。

データモデルのデータ構造は、脅威インテリジェンスリポジトリでオブジェクトとして表されます。

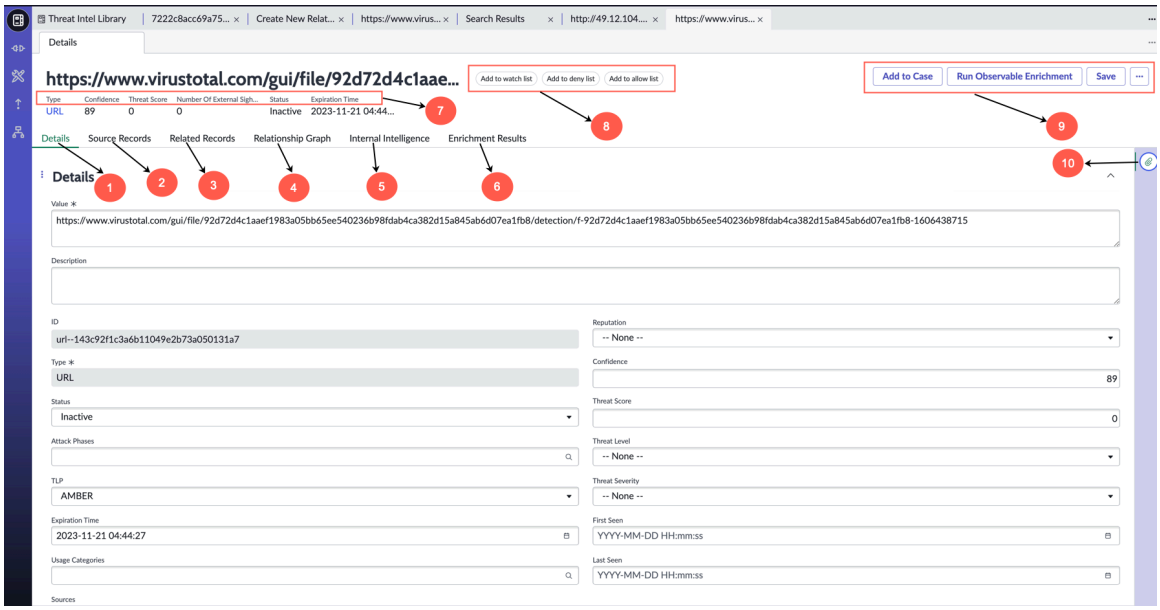
TISC ライブラリオブジェクトフォームビュー

脅威インテリジェンスセキュリティセンター オブジェクトのホームページは次の機能で構成されています。

以下のセクションを使用または移動して、各 SDO の詳細を確認してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



TISC ライブラリオブジェクトフォームビュー

順序	メニュー / タブ	説明
1	[詳細] タブ	このセクションを使用して、フォームビューで SDO を表示または編集します。
2	[ソースレコード] タブ	ソースレコードは、フォームビューに表示される集計レコードに寄与します。ソースレコードはフィードから自動作成されるか、ユーザーが手動で作成します。
3	[関連レコード] タブ	SDO に関連付けられている関連レコードをすべて一覧表示します。
4	[関係グラフ] タブ	関連オブジェクトの視覚的表現。
5	[内部インテリジェンス] タブ	関連付けられたオブジェクトの内部インテリジェンスレコードを一覧表示します。
6	[エンリッチメント結果] タブ	オブジェクトに関連付けられている拡張統合を一覧表示します。
7	フォームバナー	これは読み取り専用セクションです。[タイプ]、[信頼性]、[脅威スコア]、[サイティング数]、[ステータス]、[有効期限] などの主要なフィールドがあります。
8	フォームバナーの **UI** アクション	セキュリティコントロールリストとなります。観測事象に応じて許可リストへの追加、許可リスト (拒否リスト) からの削

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

TISC ライブラリオブジェクトフォームビュー (続く)

順序	メニュー / タブ	説明
		除、ウォッチリストへの追加が必要かどうかをチェックするときに有効です。クリックして以下を実行します： • ウォッチリストに追加 • 拒否リストに追加 • 許可リストに追加 **注:** フォームアクションは観測事象にのみ適用されます。
9	フォームの **UI** アクション	使用可能なフォーム UI アクションは次のとおりです。 **1.** ケースに追加：オブジェクトをケースに追加します。 **2.** 観測事象の拡張を実行：選択したオブジェクトに対して拡張を実行します。 **3.** 保存：レコードを保存します。 **4.** 削除：レコードを削除します。
10	右側のコンテキストメニュー	オブジェクトに関連付けられたタスクに応じて、添付ファイルやメモなどのクイックコントロールに簡単にアクセスできます。このオプションは、残っている 2 つのタブで使用でき、必要なときにいつでも脅威アナリストがアクセスできます。 コンテキストメニューを使用すると、次のリソースに簡単に移動できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

TISC ライブラリオブジェクトフォームビュー (続く)

順序	メニュー / タブ	説明
		1. 添付ファイル：オブジェクトに関連するファイルを添付します。 **注:** 観測事象、インジケーター、任意のオブジェクトを新規で作成したり、既存のオブジェクトを表示したりすると、デフォルトで [添付ファイル] ペインがそれぞれのフォームビューに表示されます。右側のコンテキストメニューの [添付ファイル] アイコンをクリックするか、 設定 > ワークスペース をクリックし、[サイドバーを表示] を無効にします。詳細については、「ネクストエクスペリエンスワークスペースの設定を構成する」を参照してください。 **2.** インサイト：オブジェクトに関連付けられている観測事象やインジケーターの関連情報を新たに追加します。
NA	ナビゲーターで検索	この検索機能で、脅威インテリジェンス (TI) ライブラリ内のさまざまなオブジェクトを検索できます。たとえば、TI ライブラリモジュール内の観測事象レコードをすべて検索できます。
NA	脅威インテリジェンスライブラリで検索	この検索機能で、検索条件に基づき複数のソースでソースレコードを検索できます。結果は別の [検索結果] タブに表示されます。たとえば、IP アドレス「104.227.137.35」の場合、レコードを検索する際に「104.*」と入力すると、検索によりレコードが絞り込まれ、「104」で始まる IP アドレスを含むレコードが別の [検索結果] タブに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

TISC ライブラリオブジェクトフォームビュー (続く)

順序	メニュー / タブ	説明
		• また、同じ [検索結果] ページの [検索条件] で既存の検索キーワードを変更することもでき、[脅威ライブラリ] ページに戻る必要もありません。 • 同様に、特定のレコード名や説明に基づいて検索することもできます。 • レコードが絞り込まれて一覧表示されたら、リストビューをクリックして、新しいタブの各レコードに移動することができます。

TISC ライブラリリポジトリ

IoC リポジトリには STIX オブジェクトが含まれており、これらの各オブジェクトには特定の情報が含まれています。

観測事象

観測事象は、コンピューターやネットワークの操作に関連するステートフルなプロパティ (ファイルの MD5 ハッシュやレジストリキーの値など) または測定可能なイベント (レジストリキーの作成やファイルの削除など) を表します。

アプリケーションで利用可能な観測事象のタイプは、次のとおりです。

- アーティファクト
- AS 番号
- ディレクトリ
- ドメイン名
- メールアドレス
- メールメッセージ
- メールの件名
- ファイル
- IPv4 アドレス
- IPv4 CIDR
- IPv6 アドレス
- IPv6 CIDR
- MAC アドレス
- MD5 ハッシュ
- ミューテックス名
- ネットワーク

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- その他の観測事象
- プロセス
- SHA1 ハッシュ
- SHA256 ハッシュ
- SHA512 ハッシュ
- ソフトウェア
- URL
- ユーザーアカウント
- Windows レジストリキー
- X.509 証明書

観測事象の定義

観測事象は、スケジュール済みフィードの取り込みから、またはインポートアシスタントから取得できます。ただし、必要に応じて観測事象を作成できます。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > 脅威インテリジェンスライブラリ > 観察事項 > すべての観察事項.
2. [**New**] をクリックします。
3. 観測可能タイプを選択します。
   [新しい観測事象レコードの作成 (Create New Observable record)] フォームが表示されます。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

4. フォームのフィールドに入力します。

   注:
   新しい観測事象を作成するか、既存の観測事象を表示するたびに、デフォルトで [添付ファイル] ペインがフォームビューに表示されます。右側のコンテキストメニューの [添付ファイル] アイコンをクリックするか、 設定 > ワークスペース をクリックし、[サイドバーを表示] を無効にします。詳細については、「ネクストエクスペリエンスワークスペースの設定を構成する」を参照してください。

   #### 詳細セクション

フィールド	説明
値	観測事象に関連付けられている値 (IP アドレスやハッシュなど)。
説明	観測事象レコードの説明。
作成者	名前を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
タイプ	IP アドレス、ドメイン名、アーティファクト、ディレクトリ、ファイル、ハッシュなどの観測事象の分類タイプ。 デフォルトでは、これは新しいレコードを選択したときに表示されます。
ステータス	観測事象のステータス (アクティブまたは非アクティブ)。
攻撃フェーズ	LM、MITRE ATT&CK などのキルチェーンの攻撃フェーズを表します。
TLP	TLP に基づくデータの機密性の設定を示す一意の値。
評判	観測事象の悪意のある評判を指定します。
ステータス	観測事象のステータス (アクティブまたは非アクティブ) を入力します。
脅威スコア	その観測事象の脅威スコアを示します。
有効期限	観測事象レコードの有効期限を指定します。
ソース	このレコードの作成元である脅威のソースを指定します。
信頼性	この観測事象レコードの信頼度を入力します。 信頼度プロパティは、作成者がデータの正確性に対して持っている信頼性を識別します。信頼度値は 0〜100 の範囲にする必要があります。
システムの更新を防止	このフラグを true に設定すると、レコードのフィールドの値が上書きされなくなります。
誤検出	観測事象が誤検出として識別されたかどうかを示すブールフラグ。

属性

フィールド	説明
解決先	ドメイン名が解決される 1 つ以上の IP アドレスまたはドメイン名への参照のリストを指定します。
FQDN である	完全修飾ドメイン名 (FQDN) は、インターネットホストまたはコンピューターの完全なアドレスです。ホスト名、ドメイン名、およびトップレベルドメイン (TLD) を指定することで、ドメインネームシステム (DNS) 内の正確な場所を提供します。

追加情報

フィールド	説明
脅威レベル	観測事象レコードの脅威レベルを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
初回確認日	この観測事象レコードが悪意のあるアクティビティを実行していることが最初に確認された時間。
脅威の重大度	観測事象レコードの脅威の重大度を示します。
最終確認日	この観測事象レコードが悪意のあるアクティビティを実行していることが最後に確認された時間。
使用率カテゴリ	ボットネットやフィッシングなど、観測事象が該当するカテゴリ。
攻撃フェーズ	LM、MITRE ATT&CK などのキルチェーンの攻撃フェーズを表します。
追加コンテキスト	追加コンテキストを追加します。
ソース	このレコードの作成元である脅威のソースを指定します。

重要:
ソースの報告済みスコア：このフィールドには、観測事象の取り込み元のソースによって報告された脅威スコアの集計値が含まれます。デフォルトでは利用できないため、このフィールドを観測事象レコードフォームに表示するには、手動で追加する必要があります。

属性

フィールド	説明
解決先	ドメイン名が解決される 1 つ以上の IP アドレスまたはドメイン名への参照のリストを指定します。
FQDN である	完全修飾ドメイン名 (FQDN) は、インターネットホストまたはコンピューターの完全なアドレスです。ホスト名、ドメイン名、およびトップレベルドメイン (TLD) を指定することで、ドメインネームシステム (DNS) 内の正確な場所を提供します。

注:
[解決先 **(Resolves To)]** および **[FQDN** である **(Is FQDN)]** 属性は、観測事象の [ドメイン名] タイプにのみ適用されます。

観測事象タイプ属性

属性名	属性タイプ
アーティファクト	○ 復号化キー ○ 暗号化アルゴリズム ○ MD5 ハッシュ ○ MIME タイプ ○ SHA1 ハッシュ ○ SHA256 ハッシュ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性名	属性タイプ
	○ SHA512 ハッシュ ○ URL
AS 番号	○ 名前 ○ RIR
ディレクトリ	○ ディレクトリ作成時刻 ○ ディレクトリの最終アクセス時刻 ○ ディレクトリの最終変更時刻 ○ エンコードパス
ドメイン名	○ FQDN である ○ 解決先
メールアドレス	○ 表示名 ○ メール本文 ○ Bcc でのメール受信者 ○ Cc でのメール受信者 ○ To でのメール受信者 ○ メール送信者 ○ メールの件名 ○ 送信日
ファイル	○ 追加情報 ○ エンコードされたファイル名 ○ ファイル作成時刻 ○ ファイルの最終アクセス時刻 ○ ファイルの最終変更時刻 ○ ファイル名マジックナンバー ○ MD5 ハッシュ ○ MIME タイプ ○ SHA1 ハッシュ ○ SHA256 ハッシュ ○ SHA512 ハッシュ
IPv4 アドレス	○ AS 番号 ○ MAC アドレス
IPv4 CIDR	○ AS 番号 ○ MAC アドレス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性名	属性タイプ
IPv6 アドレス	○ AS 番号 ○ MAC アドレス
IPv6 CIDR	○ AS 番号 ○ MAC アドレス
ネットワーク	○ 宛先バイト ○ 宛先パケット数をカウント ○ 宛先ポート ○ 終了時間 ○ HTTP メッセージ本文の長さ ○ HTTP 要求ヘッダー ○ HTTP 要求メソッド ○ HTTP 要求値 ○ HTTP 要求バージョン ○ ICMP コードバイト ○ ICMP タイプバイト ○ ネットワークがアクティブ ○ ソケットがブロック ○ ソケットがリッスン ○ ネットワークプロトコル ○ ソケットアドレスファミリ ○ ソケット記述子 ○ ソケットハンドル ○ ソケットオプション ○ ソースタイプのソースバイト数 ○ ソースパケット数 ○ ソースポート ○ 開始時間 ○ TCP 宛先フラグ ○ TCP ソースフラグ
プロセス	○ ASLR が有効 ○ コマンドライン ○ 現在の作業ディレクトリ（CWD） ○ DEP が有効 ○ 環境変数 ○ 非表示

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性名	属性タイプ
	○ 所有者 SID ○ プロセス ID ○ 優先度 ○ プロセス作成時刻 ○ サービスの説明 ○ サービスの表示名 ○ サービスのグループ名 ○ サービス名 ○ サービスの起動タイプ ○ サービスステータスサービスタイプ ○ スタートアップ情報 ○ Windows 完全性レベル ○ ウィンドウタイトル
ソフトウェア	○ 共通プラットフォーム一覧 (CPE) ○ サポート対象の言語 ○ ソフトウェア識別（SWID） ○ ベンダーバージョン
ユーザーアカウント	○ アカウント作成時刻 ○ アカウントの有効期限 ○ アカウントログイン ○ 口座種類 ○ 追加情報 ○ 特権のエスカレートが可能 ○ 認証情報の最終変更時刻 ○ 表示名 ○ 最初のログイン時刻 ○ アカウントが無効である ○ 特権付きである ○ サービスアカウントである ○ 前回のログイン時間 ○ ユーザー ID
Windows レジストリキー	○ キーの変更 ○ 時間レジストリ値 ○ サブキー数

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性名	属性タイプ
X.509 証明書	○ 追加情報 ○ 権限キー識別子 ○ 基本的な制約 ○ 証明書ポリシー ○ CRL 配布ポイント ○ 拡張キー使用率 ○ すべてのポリシーを禁止 ○ 発行者 ○ 発行者の代替名 ○ 自己署名である ○ キーの使用率 ○ 名前の制約 ○ ポリシーの制約 ○ ポリシーマッピング ○ 秘密鍵の使用の有効開始日 ○ 秘密鍵の使用の有効期限 ○ 署名アルゴリズム ○ 件名 ○ サブジェクトの代替名 ○ サブジェクトのディレクトリ属性 ○ サブジェクトキー識別子 ○ サブジェクトの公開鍵アルゴリズム ○ サブジェクトの公開鍵指数 ○ サブジェクトの公開鍵係数 ○ 有効期間開始日 ○ 有効期限 ○ バージョン

インサイト

フィールド	説明
メモ	観測事象レコードに関するメモを追加します。

5. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
6. [続行] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択 (Select Tags)	観測事象に関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択 (Select Taxonomy)	観測事象に関連付けられている分類を選択します。
分類値を追加 (Add Taxonomy Values)	観測事象に関連付けられている分類の値を追加します。

ソースレコード

フィールド	説明
観測事象のソースレコードの詳細が表示されます (存在する場合)。	

次のタスク

次の表に、観測事象に関連する関連レコードを示します。

関連レコード

関連リスト	説明
観測事象	この観測事象に関連する観測事象のリスト。 **注:** このセクションには、2 つの観測事象間の潜在的な関係も含まれています。詳細については、「観測事象と観測事象の潜在リレーションシップを確認する」および「観測事象と観測事象の関係を定義する」を参照して、2 つの観測事象間の確認済みの関係を確認してください。
インジケーター	この観測事象に関連するインジケーターのリスト。
攻撃パターン	この観測事象に関連する攻撃パターンのリスト。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコード (続く)

関連リスト	説明
キャンペーン	この観測事象に関連するキャンペーンを一覧表示します。
インフラストラクチャ	この観測事象に関連するシステム、ソフトウェアサービス、および関連する物理リソースまたは仮想リソースなどのインフラストラクチャを一覧表示します。
侵入セット	この観測事象に関連する共通のプロパティを持つ一連の攻撃者の行動やリソースなどの侵入セットを一覧表示します。
マルウェア	この観測事象に関連するマルウェアソースレコードを一覧表示します。
攻撃者	この観測事象に関連する攻撃者を一覧表示します。
脅威イベント	この観測事象に関連する脅威イベントを一覧表示します。
脆弱性	観測事象が IP アドレスの場合、このリストには、この観測事象に関連する、一致する IP アドレスを持つすべてのリソース (構成アイテム) が表示されます。

自動翻訳

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. また、[関連レコード] セクションで、[観測事象] フォームビューにある [潜在リレーションシップ **(Potential Relationships)]** セクションを使用して、2 つの観測事象間の関係を確認できます。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
3. ケースに観測事象を追加できます。詳細については、「ケースに追加する」を参照してください。
4. 観測事象に対して拡張アクションを実行することもできます。詳細については、「ケース内で拡張アクションを実行」を参照してください。

観測事象ソースレコード

ソースレコードは、フォームビューに表示される集計レコードに寄与します。ソースレコードはフィードから自動作成されるか、ユーザーが手動で作成します。

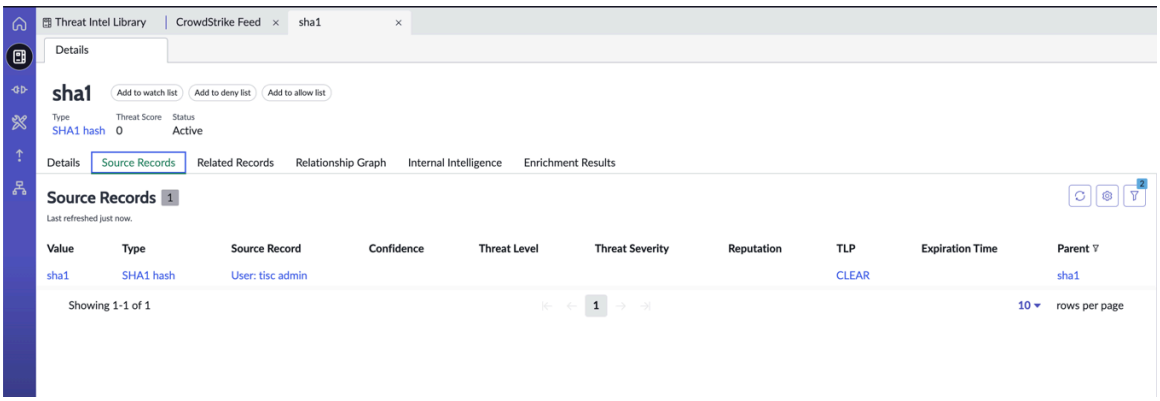
始める前に

必要なロール：sn_sec_tisc.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [脅威アナリストワークベンチ **(Threat Analyst Workbench)**] アイコンをクリックします。
3. 検索項目 観察事項 > すべての観察事項.
4. 観測事象を 1 つ以上選択します。
5. [ソースレコード] に移動します。
   集計レコードのソースレコードが表示されます。



6. レコードを表示します。

脅威インテリジェンス関連レコードへのリンク

対応する脅威インテリジェンスオブジェクトに関連する関連レコードをリンクします。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > 脅威インテリジェンスライブラリ > 観察事項 > すべての観察事項.
2. 一例として、任意の観測事象レコードを選択します。
3. [関連レコード] セクション移動します。
4. 任意の関連レコードを選択します。
5. [リンク] をクリックします。
   [リンクオブジェクト] ダイアログボックスが表示されます。
6. リストからオブジェクトを選択し、[リンク] ボタンをクリックします。
   観測事象レコードに関連付けられたオブジェクトはリンクされ、[関連レコード] リストビューに表示されます。
7. [保存] をクリックします。
   [リンク解除] ボタンをクリックして、オブジェクトのリンクを解除します。

観測事象データのフェッチ

観測事象関連レコードのデータをフェッチします。

始める前に
必要なロール：sn_sec_tisc.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [観測事象] に移動します。
   選択したオブジェクトに関連付けられている関連する観測事象が表示されます。
4. 任意の観測事象レコードを選択します。
   指定された観測事象に CVE が関連付けられている場合は、表示されたボタンを使用して脆弱性関連データを自動的にフェッチできます。これらの関連レコードは [脆弱性] の [ビジネスコンテキスト] セクションに表示されます。
5. 検索項目 内部インテリジェンス > 脆弱なエントリー.
   観測事象に関連する CVE レコードが表示されます。
6. 任意の CVE を選択し、[脆弱性関連データをフェッチ] ボタンをクリックします。

   注:

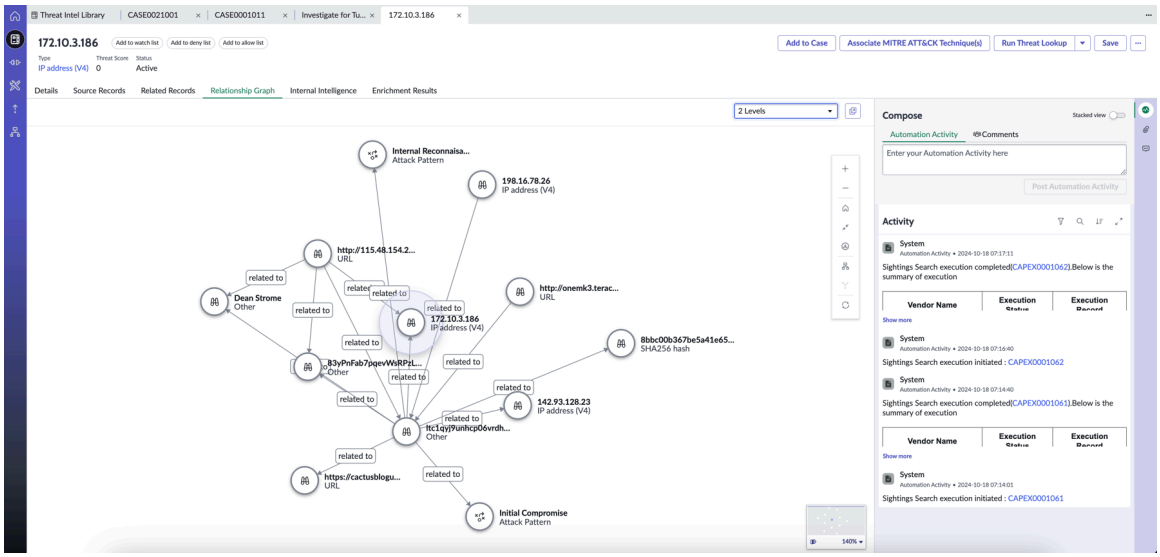
   - [この特定の脆弱性オブジェクトには、脆弱性エントリーが関連付けられていません。データをフェッチするには、オブジェクトを脆弱性エントリーに関連付ける必要があります。(This specific vulnerability object doesn't have any vulnerable entries associated with it. You must associate the object(s) with the vulnerable entries to fetch the data.)] という情報メッセージが表示されます。レコードをリンクし、スケジュール済みジョブを実行してデータをフェッチする方法の詳細については、「脆弱性データのフェッチ」を参照してください。スケジュール済みジョブの詳細については、「スケジュール済みジョブ」を参照してください。
   - このボタンをクリックすると、バックグラウンドのスケジュール済みジョブがトリガーされ、ジョブの開始と実行の詳細が [アクティビティストリーム] セクションに表示されます。たとえば、ジョブがトリガーされると、アクティビティストリームには、脆弱性エントリーに関連するデータのフェッチを開始したアクティビティが表示されます。バックグラウンドのスケジュール済みジョブは、観測事象に関連付けられた脆弱性エントリーがある観測事象を継続的にチェックして自動的に実行します。このスケジュール済みジョブは 1 時間ごとに実行されます。レコードがフェッチされない場合は、手動でレコードをリンクしてデータをフェッチできます。

ビジュアライザーでの詳細の表示

ビジュアライザーを使用すると、さらに調査するためのコンテキストを提供するオブジェクト、観測事象、インジケーター間の関係を表示できます。Visualizer は、色とアイコンを使用してオブジェクトに関するさまざまな情報を示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



次の操作を実行できます。

- オブジェクトをズームインしたり、画面を合わせたり、ノードをドラッグしたり、特定の関係に焦点を当てたりできます。
- 任意のオブジェクトをクリックして [詳細] ペインを開きます。詳細ペインでは、オブジェクトに関連付けられている詳細情報を確認できます。[オブジェクト]、[オブジェクト名]、[説明]、[ソース] などのノードプロパティを表示できます。デフォルトでは、各グラフノードの [詳細] セクションは表示されず、グラフ内の各ノードをクリックして、選択したノードの詳細を表示する必要があります。

  注:
  ビジュアライザーは、観測データオブジェクトを除くすべての STIX ドメインオブジェクト (SDO) で使用できます。[更新] ボタンをクリックして、ビジュアライザーを更新します。

- [ポップアウト] アイコンをクリックして、より大きなウィンドウでグラフを表示することもできます。

内部インテリジェンスレコードとの連携

この機能で、Configuration Database Management System (CMDB) から脅威インテリジェンスセキュリティセンターに収集された内部インテリジェンスデータと連携することができます。

内部インテリジェンスレコードを表示

CMDB、セキュリティインシデントレスポンス (SIR)、脆弱性対応 (VR) から収集された内部インテリジェンスレコードを表示します。

始める前に

[内部インテリジェンス] セクションでは、SIR、VR、CMDB などのアプリケーションからのコンテキストがプラットフォームに提供され、アナリストは脅威に対して幅広い視点が得られるようになります。

必要なロール：sn_sec_tisc.analyst

注:
[内部インテリジェンス] タブは、観測事象および脆弱性オブジェクトに対してのみ表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > 脅威インテリジェンスライブラリ > 観察事項 > すべての観察事項.
2. 任意の観測事象レコードを選択します。
3. [内部インテリジェンス] タブに移動します。
   [内部インテリジェンス] セクションは、「セキュリティインシデントレスポンス」「ビジネスコンテキスト」「脆弱性対応」の 3 つのサブセクションで構成されています。

   注:
   これらのセクションを [内部インテリジェンス] タブに表示するには、各アプリケーションがインスタンスにインストールされている必要があります。

   a. セキュリティインシデントレスポンス：関連付けられている観測事象や脆弱性一致アイテムとリンクされているインシデントをすべて表示します。

      注:
      観測事象の値は、SIR インシデント間だけでなく、TISC の範囲内で一致する必要もあります。その場合のみ、関連付けられている観測事象やインジケーターが [セキュリティインシデントレスポンス] セクションに一覧表示されます。また、ソースシステム内のレコードを検索して、レコードをリンクさせたりリンクを解除したりすることもできます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。

      - ソースシステムで任意のレコードを選択して、詳細情報に移動および表示します。例：関連付けられている観測事象レコードをフェッチするためにセキュリティインシデントレスポンスに関連付けられている観測事象など。
      - 現在のリリースの一環で、ソース (SIR) レコードからフェッチできるインテリジェンスデータは次のとおりです。
        - 関連する観測項目
        - 脆弱性一致アイテム

   b. ビジネスコンテキスト：影響を受けるユーザーや他の構成アイテム (CI) を表示します。現在のリリースの一環で、ソース (ビジネスコンテキスト) レコードからフェッチできるインテリジェンスデータは次のとおりです。
      - 構成アイテム
      - 影響を受けるサービス
      - 影響を受ける資産

   c. 脆弱性対応：脆弱性のインテリジェンスデータを表示します。

      脆弱性エントリー：このオプションでは脆弱性を照合し、関連レコードをフェッチします。

観測事象から拡張アクションを実行

このセクションを使用して、観測事象やその他のオブジェクトに対して拡張アクションがどのように実行されるかを理解します。

始める前に
必要なロール：sn_sec_tisc.admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [脅威アナリストワークベンチ **(Threat Analyst Workbench)]** アイコンをクリックします。
3. 検索項目 観察事項 > すべての観察事項.
4. 分割ボタンから任意の拡張アクションをクリックします。
5. 利用可能な実装を選択します。
6. [送信] をクリックします。
   たとえば、[脅威のルックアップを実行] などです。選択した拡張アクションが実行され、[選択した観測事象で観測事象の拡張実行が開始されました。実行が完了すると、それぞれの観測事象の詳細ページで結果を確認できます。(Observable enrichment execution has started on the selected observable(s). Results will be available in the detail page of respective observable(s) once the execution is complete.)] という情報メッセージが表示されます。

   注:
   実行が開始または完了すると、作業メモがフォームビューのアクティビティストリームにポストされます。

ケースに追加する

ケースに観測事象、インジケーター、またはその他のオブジェクトを追加します。

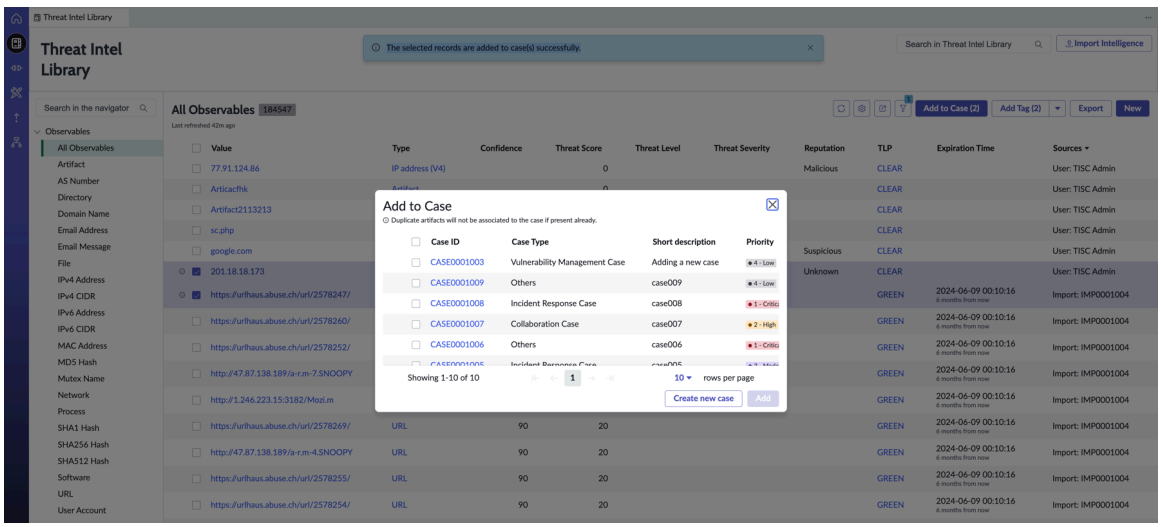
始める前に

必要なロール：sn_sec_tisc.analyst

観測事象レコードにケースを追加する手順は、次のとおりです。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > 脅威インテリジェンスライブラリ > 観察事項 > すべての観察事項.
2. 観測事象を選択します。
3. [ケースに追加 **(Add to Case)]** ボタンをクリックします。
   レコードがまだ関連付けられていないケースのみが表示されます。



4. 既存のケースにレコードを追加するかどうかを確認し、追加する場合は既存のケースを選択します。追加しない場合は、[新規ケースを作成] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

次の情報を入力して、新しいケースを作成します。

新規ケースの作成

フィールド	説明
ケース ID	ケースの一意の識別子。これはシステム生成 ID です。
簡単な説明	調査中の要求または問題の概要、または簡単な説明。
ケースのタイプ	調査対象のケースタイプを選択します。調査の可能なオプションは、次のとおりです。 ○ 脅威の検出 ○ 情報の要求 ○ 脆弱性管理ケース ○ コンプライアンスケース ○ インシデントレスポンスケース ○ コラボレーションケース ○ その他
優先度	要求または問題の重大度のアセスメント。
アサイン先グループ	ケースの作業を担当するアサイン先グループ。
アサイン先	ケースの作業を担当するアナリスト。

5. 新しいケースを作成する場合は、[作成] をクリックします。

   注:
   新しいケースが既存のケースリストに追加されます。

6. 新しく追加されたケースを選択します。
7. [追加] をクリックします。
   選択したレコードがケースに正常に追加されたことを示す情報メッセージが表示されます。

TISC での拡張操作の実行

次のテーブルでは、TISC でさまざまな拡張操作を実行する際のインタラクションについて説明します。

TISC モーダル画面

機能	UX フレームワークのインタラクション	サポートされる統合
脅威のルックアップを実行	画面 1 – 実装を選択して送信します。	• ウイルス合計 • Crowd Strike Falcon Intelligence

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

機能	UX フレームワークのインタラクション	サポートされる統合
	[脅威のルックアップの実行] に適用される共通入力または実装固有の入力はありません。	
サイティング検索を実行	画面 1 の [実装を選択 (Select Implementations)] および画面 2 の [共通入力 (Common Inputs)] が適用されます。 サイティング検索では、Splunk およびその他の統合の複数の実装に共通する入力として日付と時刻の頻度が使用されます。	• Elasticsearch • Splunk Sighting
観測事象の拡張を実行	画面 1 のみ – 実装を選択します。 [観測事象の拡張を実行] に適用される共通入力または実装固有の入力はありません。	• WHOIS • Shodan

脅威のルックアップを実行

実装を適宜 1 つ以上選択して、観測事象に対して脅威のルックアップを実行します。

始める前に
必要なロール：sn_sec_tisc.admin

手順

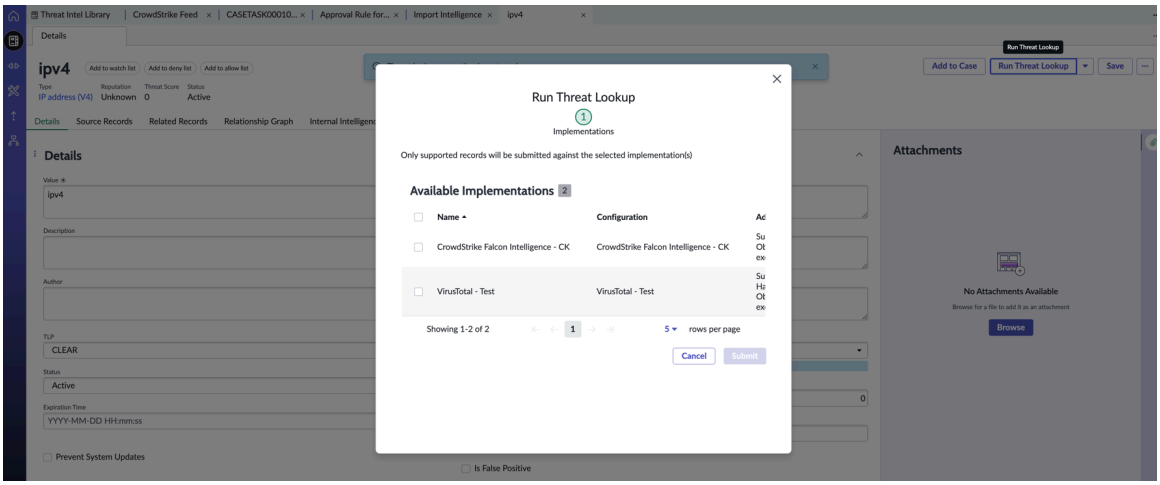
1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [脅威アナリストワークベンチ **(Threat Analyst Workbench)]** アイコンをクリックします。
3. 検索項目 観察事項 > すべての観察事項.
4. 任意の観測事象レコードを開きます。
5. [脅威のルックアップを実行] をクリックします。
   [脅威のルックアップを実行] の [実装の選択] モーダル画面が表示されます。

   注:
   [脅威のルックアップを実行] 機能では、脅威インテリジェンスのルックアップを実行し、観測事象が既知の脅威に関連するかどうかを判断します。

6. リストから必要な実装を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



7. [送信] をクリックします。
選択した拡張アクションが実行され、「脅威のルックアップ」が実行開始されたことを示す情報メッセージが表示されます。

注:

- 実行が開始または完了すると、作業メモがフォームビューのアクティビティストリームにポストされます。
- SIR ワークスペースからプッシュされたエンリッチメント結果は、TISC ワークスペースの対応する [観測事象の詳細 (Observables details)] ページの [エンリッチメント結果] タブで確認できます。
- SIR ワークスペースからプッシュされたエンリッチメント結果は、拡張結果テーブルの [ソース] フィールドを使用して特定することができます。

サイティング検索を実行

サイティング検索関連の統合を実行します。

始める前に

必要なロール：sn_sec_tisc.admin

このアクションを実行するには、実装を選択し、選択したすべての実装に適用される共通の実行時間入力を必要に応じて選択および追加します。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.

2. [脅威アナリストワークベンチ **(Threat Analyst Workbench)]** アイコンをクリックします。

3. 検索項目 観察事項 > すべての観察事項.

4. 任意の観測事象レコードを開きます。

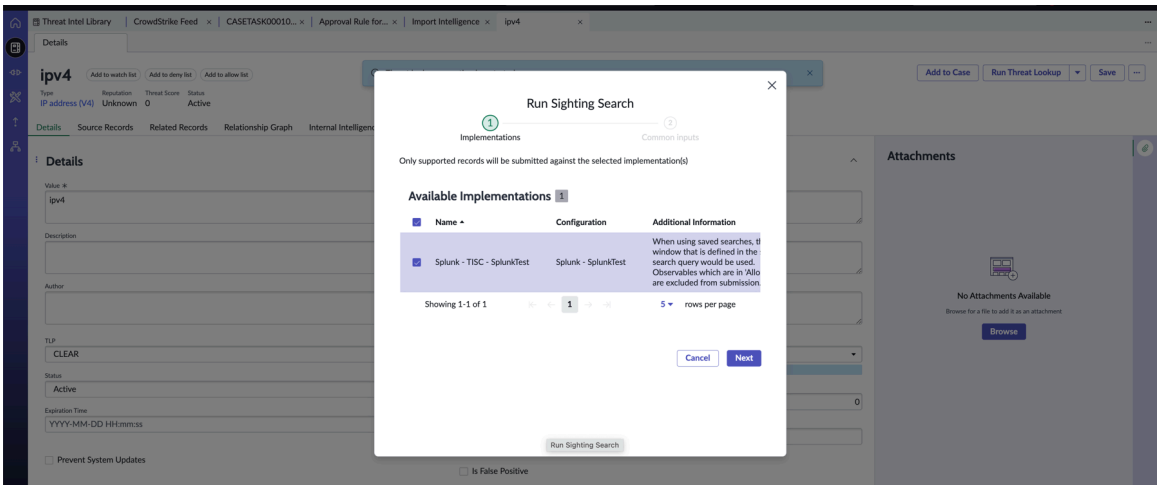
5. [サイティング検索を実行] をクリックします。
[サイティング検索を実行] の [実装の選択] モーダル画面が表示されます。

注:
[サイティング検索を実行] 機能では、脅威インテリジェンスのルックアップを実行し、観測事象が既知のセキュリティ上の脅威に関連するかどうかを判断します。

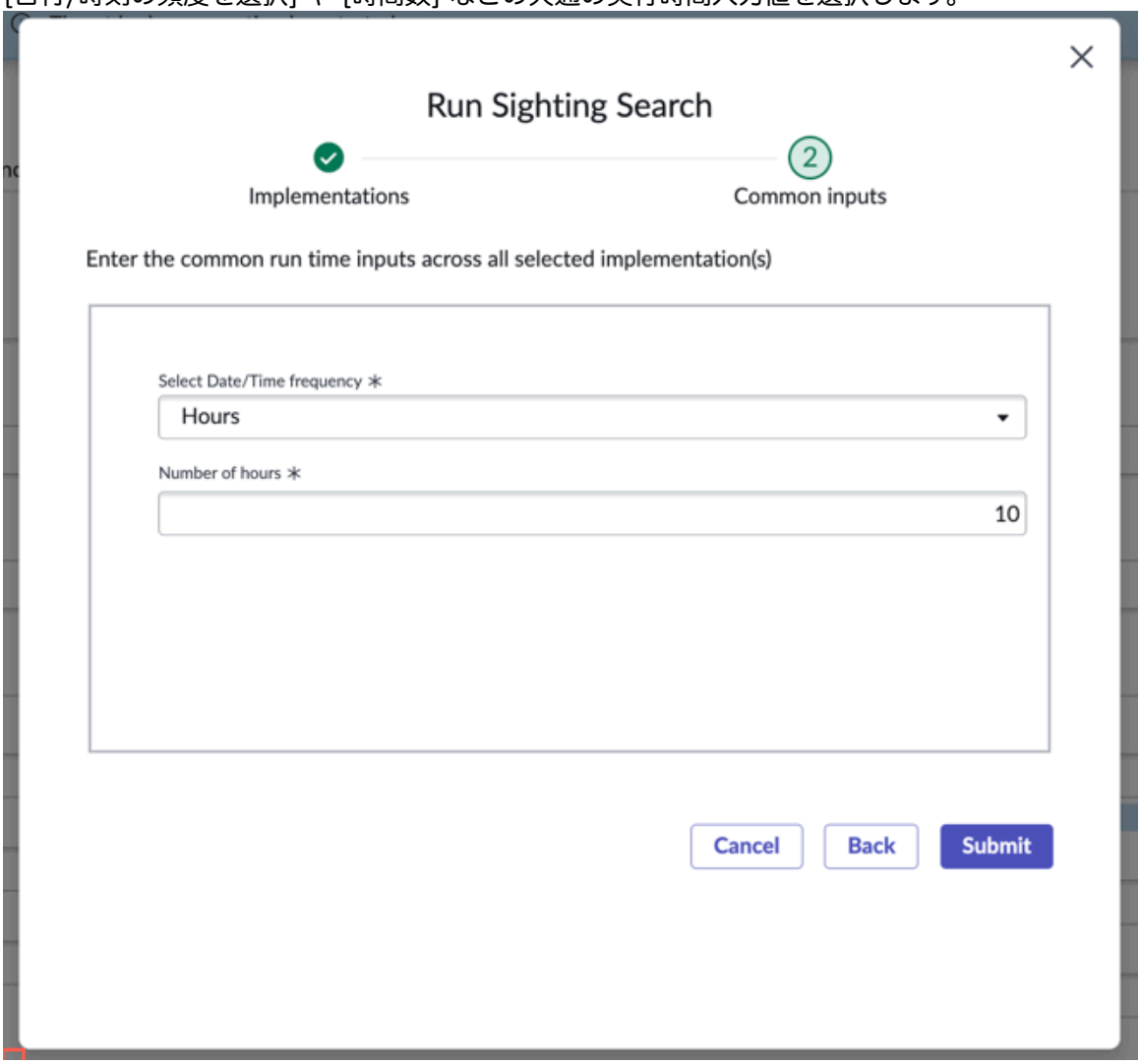
6. リストから必要な実装を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



7. [次へ] をクリックします。
8. [日付/時刻の頻度を選択] や [時間数] などの共通の実行時間入力値を選択します。



9. [送信] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

選択した拡張アクションが実行され、「サイティング検索を実行」が実行開始されたことを示す情報メッセージが表示されます。

注:

- 実行が開始または完了すると、作業メモがフォームビューのアクティビティストリームにポストされます。
- SIR ワークスペースからプッシュされたエンリッチメント結果は、TISC ワークスペースの対応する [観測事象の詳細 (Observables details)] ページの [エンリッチメント結果] タブで確認できます。
- SIR ワークスペースからプッシュされたエンリッチメント結果は、拡張結果テーブルの [ソース] フィールドを使用して特定することができます。

観測事象の拡張を実行

実装を適宜 1 つ以上選択して、観測事象に対して脅威のルックアップを実行します。

始める前に

必要なロール：sn_sec_tisc.admin

手順

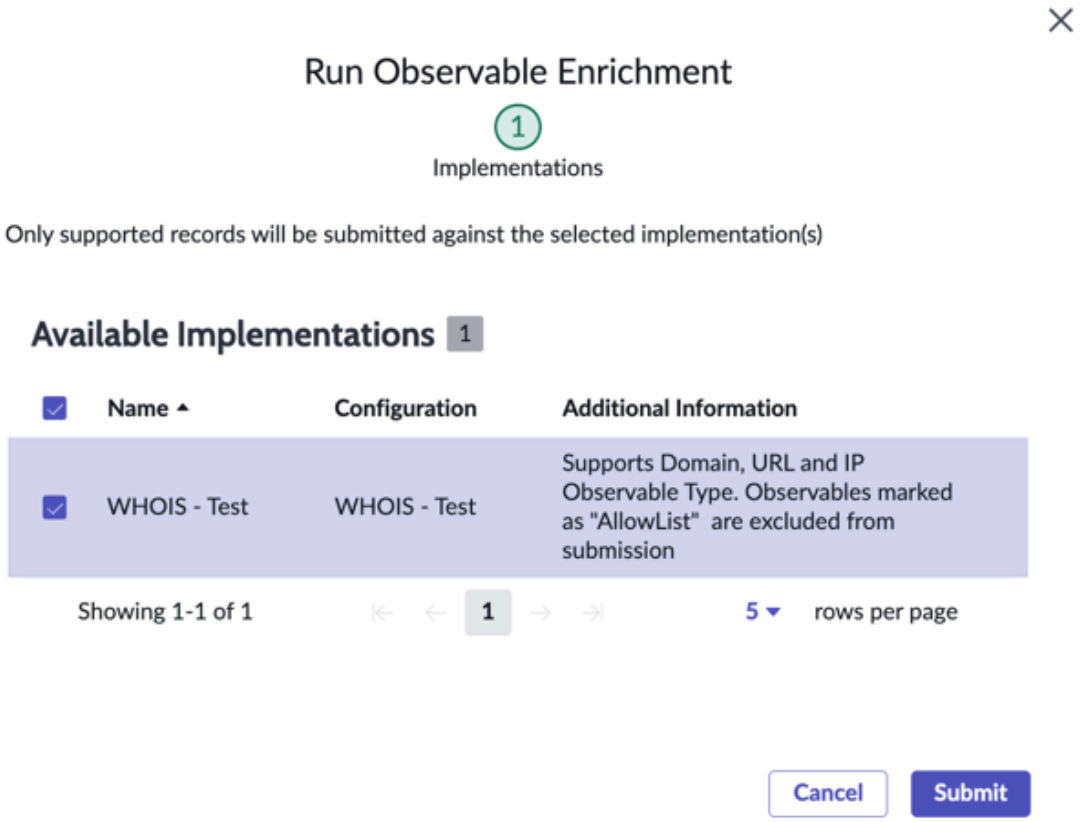
1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. [脅威アナリストワークベンチ **(Threat Analyst Workbench)]** アイコンをクリックします。
3. 検索項目 観察事項 > すべての観察事項.
4. 任意の観測事象レコードを開きます。
5. [観測事象の拡張を実行] をクリックします。
   [観測事象の拡張を実行] の [実装の選択] モーダル画面が表示されます。

   注:
   選択した実装に対してサポートされているレコードのみが送信されます

6. リストから必要な実装 (WHOIS など) を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

7. [送信] をクリックします。
選択した拡張アクションが実行され、「脅威のルックアップ」が実行開始されたことを示す情報メッセージが表示されます。

注:

- 実行が開始または完了すると、作業メモがフォームビューのアクティビティストリームにポストされます。
- SIR ワークスペースからプッシュされたエンリッチメント結果は、TISC ワークスペースの対応する [観測事象の詳細 (Observables details)] ページの [エンリッチメント結果] タブで確認できます。
- SIR ワークスペースからプッシュされたエンリッチメント結果は、拡張結果テーブルの [ソース] フィールドを使用して特定することができます。

エンリッチメント結果を表示

観測事象、インジケーター、さまざまなオブジェクトのエンリッチメント結果を表示します。

始める前に

必要なロール：sn_sec_tisc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > 脅威インテリジェンスライブラリ > 観察事項 > すべての観察事項.
2. 任意の観測事象レコードを選択します。
3. [エンリッチメント結果] タブに移動します。
   [エンリッチメント結果] には、TISC 統合のエンリッチメント結果が表示されます。

拡張名	説明
脅威のルックアップの結果	観測事象に関連する脅威のルックアップ結果をすべて一覧表示します。
サイティング	観測事象に関連するサイティングをすべて一覧表示します。
観測事象のエンリッチメント結果	観測事象に関連する観測事象のエンリッチメント結果をすべて一覧表示します。

インジケーター

インジケーターは、ネットワークまたはオペレーティングシステムで検出された、侵入を示す可能性のあるアーティファクトです。一般的な IoC は、ウイルス署名と IP アドレス、マルウェアファイルまたは URL の MD5 ハッシュ、またはドメイン名です。

インジケーターの定義

インジケーターを定義します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター > 脅威インテリジェンスライブラリ > インジケーター.
2. [インジケーター] を選択します。
3. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

4. フォームのフィールドに入力します。

詳細セクション

フィールド	説明
ID	インジケーターの一意の ID。
説明	インジケーターの説明。
名前	インジケーターの名前。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
パターン	このインジケーターの検出パターンは、STIX パターンとして表すことができます。
パターンタイプ	このインジケーターで使用されるパターン言語。
パターンバージョン	パターンプロパティに含まれるパターンデータのタイプと一致する必要がある、パターンプロパティ内のデータに使用されるパターン言語のバージョン。
有効期間開始日	このインジケーターが、関連する動作または表される動作の有効なインジケーターと見なされる時間。
有効期限	このインジケーターが、関連するまたは表す動作の有効なインジケーターと見なされなくなるまでの時間。
IOC 分類	インジケーターの IOC 分類。
インジケータータイプ	インジケーターのさまざまなカテゴリを示します。
ステータス	インジケーターのステータスを示します。
プラットフォーム	このインジケーターが適用されるプラットフォームを定義します。
TLP	TLP に基づくデータの機密性の設定を示す一意の値。
攻撃フェーズ	LM、MITRE ATT&CK などのキルチェーンの攻撃フェーズを表します。
信頼性	このインジケーターレコードの信頼度を入力します。 信頼度プロパティは、作成者がデータの正確性に対して持っている信頼性を識別します。信頼度値は 0～100 の範囲にする必要があります。
脅威レベル	インジケーターレコードの脅威レベルを示します。
有効期限	インジケーターレコードの有効期限を指定します。
脅威の重大度	インジケーターレコードの脅威の重大度を示します。
使用率カテゴリ	ボットネットやフィッシングなど、観測事象が該当するカテゴリ。
初回確認日	このインジケーターレコードが悪意のあるアクティビティを実行していることが最初に確認された時間。
最終確認日	このインジケーターレコードが悪意のあるアクティビティを実行していることが最後に確認された時間。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ソース	このレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	インジケーターに関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	このインジケーターのコンテキストを追加します。
仕様バージョン	このインジケーターを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
作成日時	システムでインジケーターが作成される時刻を指定します。
更新日時	システムでインジケーターが更新される時刻を指定します。
拡張	インジケーターの拡張を示します。
処理ステータス	このインジケーターの処理ステータスを表します。

5. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
6. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タグと分類

フィールド	説明
Tags	
タグを選択	インジケーターに関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	インジケーターに関連付けられている分類を選択します。
分類値を追加	インジケーターに関連付けられている分類値を追加します。

ソースレコード

フィールド	説明
インジケーターのソースレコードの詳細が表示されます (存在する場合)。	

次のタスク

次の関連リストのいずれかをクリックすると、インジケーターに関連するオブジェクトの追加情報が表示できます。

関連レコード

関連リスト	説明
インジケーターの参照	このインジケーターを説明する外部参照のリスト。
観測事象	このインジケーターに関連する関連する観測事象レコードを一覧表示します。
インジケーター	このインジケーターに関連するインジケーターを一覧表示します。 **注:** このセクションには、2 つのインジケーター間の潜在的な関係も含まれています。詳細については、「インジケーターとインジケーターの潜在リレーションシップを確認する」および「インジケーターとインジケーターの関係を定義する」を参照して、2 つの観測事象間の確認済みの関係を確認してください。
構成アイテム	このインジケーターに関連する構成アイテムを一覧表示します。
攻撃パ	攻撃者がこのインジケーターに関連するターゲットを侵害しようとする方法を記述する攻撃パターンソースを一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコード (続く)

関連リスト	説明
ターン	
キャンペーン	このインジケーターに関連する特定の標的に対して時間の経過とともに発生する一連の悪意のあるアクティビティまたは攻撃を記述するキャンペーンソースを一覧表示します。
検出と軽減	このインジケーターに関連する検出と軽減を一覧表示します。
ID	このインジケーターに関連する ID を一覧表示します。
インフラストラクチャ	このインジケーターに関連する攻撃の何らかの目的をサポートするためのシステム、ソフトウェアサービス、および関連する物理または仮想リソースを記述するインフラストラクチャソースを一覧表示します。
侵入セット	このインジケーターに関連する共通のプロパティを持つ一連の攻撃者の行動とリソースを一覧表示します。
所在地	オブジェクトに関連付けられた地理的な場所を一覧表示します。
マルウェア	このインジケーターに関連するマルウェアソースレコードを一覧表示します。
マーキング定義	このオブジェクトに関連付けられたマーキング定義を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングソースレコードを一覧表示します。
攻撃者	観測事象に関連する変更を一覧表示します。
脅威イベント	脅威のソースによって識別された、関連する観測事象を一覧表示します。
ツール	このオブジェクトに関連付けられているツールを一覧表示します。
脆弱性	観測事象が IP アドレスの場合、このリストには、一致する IP アドレスを持つすべてのリソース (構成アイテム) が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. また、[関連レコード] セクションで、[インジケーター] フォームビューにある [潜在リレーションシップ] セクションを使用して、2 つの観測事象間の関係を確認できます。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
3. ケースにインジケーターを追加できます。詳細については、「ケースに追加する」を参照してください。

攻撃パターン

攻撃パターンは、攻撃者がターゲットを侵害しようとする方法を記述する戦術、テクニック、手順 (TTP) の一種です。

攻撃パターンは、攻撃を分類するために使用されます。これらは、特定の攻撃をパターンに一般化し、攻撃がどのように実行されるかについての詳細な情報を提供します。

たとえば、スピアフィッシングは、リンクをクリックしたり、添付ファイルを開いてマルウェアに感染させることを目的に、入念に細工したメールメッセージを攻撃者が送信する一般的な攻撃です。攻撃パターンは具体的であり、特定の攻撃者によるスピアフィッシング (例：標的がコンテストに勝った) なども攻撃パターンになります。

攻撃パターンの定義

攻撃パターンを定義して脅威アナリストが攻撃を分類できるようにします。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. 攻撃パターンに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

[攻撃パターンの詳細] ビュー

フィールド	説明
ID	攻撃パターンの一意の ID。
名前	この攻撃パターンの名前を入力します。
説明	攻撃パターンの説明を入力します。
エイリアス	この攻撃パターンを識別する代替名。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	注: アプリケーションに存在しない新しいエイリアスを追加するには、[エイリアス] フィールド自体で使用できる [新しいエイリアスを追加] アイコンをクリックします。
攻撃フェーズ	LM、MITRE ATT&CK などのキルチェーンの攻撃フェーズを表します。
必要な権限	この攻撃パターンに対する必要な権限を選択します。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、オレンジ、赤) を使用して、さまざまな感度を示します。
信頼性	この攻撃パターンモードの信頼度を入力します。 信頼度プロパティは、作成者がデータの正確性に対して持っている信頼性を識別します。信頼度値は 0～100 の範囲にする必要があります。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。
システムの更新を防止	このフラグを true に設定すると、レコードのフィールドの値が上書きされなくなります。

重要:
新しいオブジェクトレコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

インサイト

フィールド	説明
メモ	攻撃パターンに関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	この攻撃パターンのコンテキストを追加します。
仕様バージョン	このオブジェクト (攻撃パターン) を表すために使用される STIX 仕様のバージョン。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
作成日時	システムでレコードが作成される時刻を指定します。
更新日時	システムでレコードが変更される時刻を指定します。
拡張	攻撃パターンの拡張を示します。
処理ステータス	このオブジェクト (攻撃パターン) の処理ステータスを表します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択 (Select Tags)	観測事象に関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	攻撃パターンに関連付けられている分類を選択します。
分類値を追加	攻撃パターンに関連する分類値を選択します。

次のタスク

次の関連リストのいずれかをクリックすると、攻撃パターンに関連するオブジェクトの追加情報が表示できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
ID	このオブジェクトに関連付けられた ID のリスト。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

自動翻訳

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

キャンペーン

キャンペーンは、攻撃者の行動のグループとして定義されます。一連の特定の標的に対して、時間の経過とともに発生する一連の悪意のあるアクティビティまたは攻撃 (波と呼ばれる場合もある) を表します。

キャンペーンの定義

キャンペーンを定義して攻撃者の行動をグループ化します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [キャンペーン] オブジェクトに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

[キャンペーン] ビュー

フィールド	説明
ID	攻撃者行動の一意の ID。
名前	攻撃者行動の名前を入力します。
説明	このキャンペーンの説明を入力します。
目的	キャンペーンの主要目標、目的、期待される結果、または意図した効果。攻撃者または侵入セットがこのキャンペーンで達成しようとしていること。
エイリアス	このキャンペーンを識別する代替名。 **注:** アプリケーションに存在しない新しいエイリアスを追加するには、[エイリアス] フィールド自体で使用できる [新しいエイリアスを追加] アイコンをクリックします。
TLP	TLP (Traffic Light Protocol)：機密情報が適切な対象者と共有されていることを示します。攻撃パターンの感度を 4 色 (白、緑、黄、赤) で示すことができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
信頼性	このキャンペーンの信頼度を入力します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	キャンペーンに関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	このキャンペーンのコンテキストを追加します。
初回確認日	このオブジェクトが敵対的な動作を実行していることが初めて確認された時間。
最終確認日	このオブジェクトが敵対的な動作を実行していることが最後に確認された時間。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
作成日時	ソースでオブジェクトが作成された日時を指定します。
拡張	攻撃パターンの拡張を示します。
更新日時	ソースでオブジェクトが更新された日時を指定します。
処理ステータス	このオブジェクト (キャンペーン) の処理ステータスを表します。

6. [保存] をクリックします。
   保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	キャンペーンに関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	キャンペーンに関連付けられている分類を選択します。
分類値を追加	キャンペーンに関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、キャンペーンに関連するオブジェクトの追加情報が表示できます。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
ID	このオブジェクトに関連付けられた ID のリスト。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコード (続く)

フィールド	説明
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

対処措置

対処措置は、攻撃を阻止するため、または進行中の攻撃に対処するために実行されるアクションです。

対処措置は、技術的または自動化された対応 (パッチの適用、ファイアウォールの再構成) を示しています。また、従業員のトレーニングやポリシーの変更など、高レベルのアクションを記述することもできます。

たとえば、脆弱性を緩和する対処措置には、それを修正するパッチの適用が含まれます。

対処措置を定義する

攻撃を阻止したり、進行中の攻撃に対処するための対処措置を定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)**] アイコンをクリックします。
3. [対処措置] オブジェクトに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

対処措置の詳細ビュー

フィールド	説明
ID	攻撃を防ぐ対処措置の一意の ID。
名前	この対処処置のわかりやすい名前を入力します。
説明	対処措置に関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。
アクション	構造化された、または自動化された一連のアクションをキャプチャします。
TLP	TLP (Traffic Light Protocol)：機密情報が適切な対象者と共有されていることを示します。攻撃パターンの感度を 4 色 (白、緑、黄、赤) で示すことができます。
信頼性	この対処措置の信頼度を入力します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	対処措置に関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	この攻撃パターンのコンテキストを追加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。
作成日時	ソースでオブジェクトが作成された日時を指定します。
更新日時	ソースでオブジェクトが更新された日時を指定します。
作成者参照	

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択 (Select Tags)	観測事象に関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	攻撃パターンに関連付けられている分類を選択します。
分類値を追加	攻撃パターンに関連する分類値を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のタスク
次の関連リストのいずれかをクリックすると、対処措置に関連するオブジェクトの追加情報が表示されます。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ID

ID は、実際の個人、組織、またはグループ、および個人、システム、またはグループのクラスを表します。ID は STIX 2.x に適用されます。

ID SDO は、基本的な識別情報、連絡先情報、および ID が属するセクターをキャプチャできます。ID は、攻撃の標的、情報ソース、オブジェクト作成者、および攻撃者の ID を表します。

ID の定義

実際の個人、組織、またはグループを表す ID を定義します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. **[ID]** オブジェクトに移動します。
4. [新規] をクリックします。

> **注:**
> 観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

ID の詳細ビュー

フィールド	説明
ID	ID の一意の ID。
名前	この ID の内容を端的に表す名前を入力します。 特定のエンティティ (個人または組織) を参照する場合、このプロパティには特定のエンティティの正規名を含める必要があります。
説明	対処措置に関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。
ロール	この ID が実行するロールのリスト。
ID クラス	この ID が表すエンティティのタイプ。たとえば、個人や組織などです。
セクター	この ID が属する業種のリスト。
連絡先	この ID の連絡先情報 (メールや電話番号など)。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。取り

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	扱いの注意レベルを 4 色 (白、緑、黄、赤) で示すことができます。
信頼性	この ID の信頼度を入力します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	ID に関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	この ID に関連するコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。
作成日時	ソースでオブジェクトが作成された日時を指定します。
更新日時	ソースでオブジェクトが更新された日時を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. [続行] をクリックします。

> **重要:**
> 新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。
>
> 観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	ID に関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	ID に関連付けられている分類を選択します。
分類値を追加	ID に関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、ID に関連するオブジェクトの追加情報が表示されます。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
キャンペーン	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコード (続く)

フィールド	説明
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

インフラストラクチャ

インフラストラクチャ SDO は、戦術、テクニック、手順 (TTP) の一種です。これらは、攻撃の何らかの目的をサポートするためのシステム、ソフトウェアサービス、および関連する物理または仮想リソースを表します。インフラストラクチャは STIX 2.x に適用されます。

攻撃の要素は、他の SDO または SCO によって表されます。これに対し、インフラストラクチャ SDO は、インフラストラクチャを構成するデータの名前付きグループを表します。

インフラストラクチャの例には、攻撃で使用される C2 サーバー、防御の一部であるデバイス (サーバー)、または攻撃の標的となるデータベースサーバーが含まれます。

インフラストラクチャの定義

攻撃の何らかの目的をサポートするためのシステム、ソフトウェアサービス、および関連する物理または仮想リソースであるインフラストラクチャを定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)**] アイコンをクリックします。
3. [インフラストラクチャ] オブジェクトに移動します。
4. [新規] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> 観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

[インフラストラクチャの詳細] ビュー

フィールド	説明
ID	攻撃を防ぐ対処措置の一意の ID。
名前	この対処処置のわかりやすい名前を入力します。 特定のエンティティ (個人または組織) を参照する場合、このプロパティには特定のエンティティの正規名を含める必要があります。
説明	インフラストラクチャに関する詳細とコンテキストの説明。これには、その目的、使用方法、関連するオブジェクトでキャプチャされた他のインテリジェンスアクティビティとの関連性、およびその主要な特性が含まれます。
インフラストラクチャタイプ	インフラストラクチャの分類について説明します。
エイリアス	このインフラストラクチャを識別する代替名。 **注:** アプリケーションに存在しない新しいエイリアスを追加するには、[エイリアス] フィールド自体で使用できる [新しいエイリアスを追加] アイコンをクリックします。
攻撃フェーズ	LM、MITRE ATT&CK などのキルチェーンの攻撃フェーズを表します。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、黄、赤) を使用して、さまざまな感度を示します。
初回確認日	このインフラストラクチャが悪意のあるアクティビティを実行していることが最初に確認された時間。
最終確認日	このインフラストラクチャが悪意のあるアクティビティを実行していることが最後に確認された時間。
信頼性	この対処措置の信頼度を入力します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	このインフラストラクチャに関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	このインフラストラクチャに関するコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。
作成日時	ソースでレコードが作成される時刻を指定します。
更新日時	ソースでレコードが変更される時刻を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
   保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	インフラストラクチャに関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	このインフラストラクチャに関連付けられている分類を選択します。
分類値を追加	このインフラストラクチャに関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、ID に関連するオブジェクトの追加情報が表示されます。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコード (続く)

フィールド	説明
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。
観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
観測データ	このオブジェクトに関連付けられた観測データを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

侵入セット

侵入セットは、共通のプロパティを持つ攻撃者の行動とリソースのグループ化されたセットです。通常、侵入セットには単一の組織が含まれます。侵入セットは STIX 2.x に適用されます。

侵入セットは、複数のキャンペーンまたはその他のアクティビティをキャプチャできます。これらのアクティビティは、既知または不明な攻撃者を示す属性を共有しています。

攻撃の背後にいる攻撃者が不明な場合でも、新しいアクティビティを侵入セットに関連付けることができます。攻撃者は、ある侵入セットから別の侵入セットのサポートに移行することも、複数の侵入セットをサポートすることもできます。

侵入セットは攻撃パッケージ全体であり、潜在的に複数の目的を達成するために複数のキャンペーンで長期間使用される可能性があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

侵入セットの定義

共通のプロパティを持つ攻撃者の行動とリソースのグループ化されたセットである侵入セットを定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. 侵入セットに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

[侵入セットの詳細] ビュー

フィールド	説明
ID	侵入セットの一意の ID。
名前	この侵入セットのわかりやすい名前を入力します。 特定のエンティティ (個人または組織) を参照する場合、このプロパティには特定のエンティティの正規名を含める必要があります。
説明	侵入セットに関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。
別名	この侵入セットを識別する代替名。 **注:** アプリケーションに存在しない新しいエイリアスを追加するには、[エイリアス] フィールド自体で使用できる [新しいエイリアスを追加] アイコンをクリックします。
Goals (最終目標)	この侵入セットの高レベルの目標 (何をしようとしているのか)。 たとえば、個人的な利益が動機の場合もありますが、その目的はクレジットカード番号を盗むことです。これを行うには、大規模な小売業の

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	POS システムの侵害などの詳細な目標を含む特定のキャンペーンを実行します。
初回確認日	この侵入セットが悪意のあるアクティビティを実行していることが最初に確認された時間。
最終確認日	この侵入セットが悪意のあるアクティビティを実行していることが最後に確認された時間。
プライマリ動機	この侵入セットの背後にある主な理由、動機、または目的。動機は、侵入セットが目標 (達成しようとしていること) を達成したい理由です。
セカンダリ動機	この侵入セットの背後にある副次的な理由、動機、目的。これらの動機は、主要な動機と同等またはほぼ等しい原因として存在できます。ただし、主要な動機に取って代わったり、必ずしも拡大したりするわけではありませんが、追加のコンテキストを示している可能性があります。リスト内の位置は重要ではありません。
リソースレベル	このプロパティは、この侵入セットが通常機能する組織レベルを指定します。これにより、この侵入セットに対して攻撃中に使用できるリソースが決まります。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、オレンジ、赤) を使用して、さまざまな感度を示します。
信頼性	この侵入セットの信頼度を入力します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	この侵入セットに関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	この侵入セットのコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでレコードが作成される時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。
作成日時	ソースでレコードが作成される時刻を指定します。
更新日時	ソースでレコードが変更される時刻を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	侵入セットに関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	この侵入セットに関連付けられている分類を選択します。
分類値を追加	この侵入セットに関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、侵入セットに関連するオブジェクトの追加情報が表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
ID	このオブジェクトに関連付けられた ID のリスト。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
所在地	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

場所

場所は地理的な場所を表します。場所は、主に他の SDO にコンテキストを提供するために使用されます。場所は STIX 2.x に適用されます。

場所には、地域 (北米)、住所 (米国、ニューヨーク)、緯度、経度の一部またはすべてを含めることができます。

場所 SDO は、ID または侵入セットに関連付けて、ID または侵入セットがその場所にあることを示すことができます。また、マルウェアまたは攻撃パターンに関連付けて、標的の被害者が特定の場所にいることを示すこともできます。

たとえば、関係で場所を使用して、Bourgeois Swallow 侵入セットが東ヨーロッパから発信されていることを説明できます。

次のプロパティまたはプロパティのセットのうち、少なくとも 1 つを指定する必要があります。

- region
- country
- latitude または longitude

場所の定義

地理的な場所を定義して、他の SDO に多くのコンテキストを提供します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [場所] オブジェクトに移動します。
4. [新規] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> 観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームでフィールドに入力します。

ID の詳細ビュー

フィールド	説明
ID	場所の一意の ID。
名前	場所を識別するわかりやすい名前を入力します。
説明	侵入セットに関する詳細とコンテキストの説明(目的や主要な特性を含む可能性があります)。
緯度	この場所の緯度 (10 進数の度数)。正の数は赤道より北の緯度を示し、負の数は赤道より南の緯度を示します。 このプロパティの値は、それぞれ -90.0 ～ 90.0 である必要があります。
経度	この場所の緯度 (10 進数の度数)。正の数は本初子午線より東の経度を示し、負の数は本初子午線より西の経度を示します。 このプロパティの値は、-180.0 ～ 180.0 である必要があります。
精度	緯度プロパティと経度プロパティで指定される座標の精度を定義します。これはメートル単位で測定されます。実際の位置は、定義されたポイントから正確なメートル地点までのどこかになる場合があります。 このプロパティが示されない場合、精度は未指定となります。 このプロパティが示される場合は、緯度と経度のプロパティが必ず示されます。
リージョン	この場所がある地域。
国	この場所がある国。
管理領域	この場所の州、都道府県、他の地方行政区域。
市区町村	この場所がある市区町村。
番地	この場所が示す住所。このプロパティには、住所のすべての要素または一部が含まれます。
郵便番号	この場所がある郵便番号。
信頼性	この対処措置の信頼度を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、黄、赤) を使用して、さまざまな感度を示します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	この場所に関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	この場所のコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	この場所に関する拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。
作成日時	ソースでレコードが作成される時刻を指定します。
更新日時	ソースでレコードが変更される時刻を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	場所に関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	この場所に関連付けられている分類を選択します。
分類値を追加	この場所に関連付けられている分類値を追加します。

次のタスク
次の関連リストのいずれかをクリックすると、場所に関連するオブジェクトの追加情報が表示されます。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
ID	このオブジェクトに関連付けられた ID のリスト。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコード (続く)

フィールド	説明
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

マルウェア

マルウェアは、悪意のあるコードを表す TTP の一種です。これは、システムに密かに挿入されるプログラムを指します。マルウェアは STIX 2.x に適用されます。

マルウェアの目的は、被害者のデータ、アプリケーション、またはオペレーティングシステム (OS) の機密性、完全性、または可用性を侵害することです。

マルウェア SDO は、分析から導出されたデータからマルウェアインスタンスとファミリを特徴付け、識別、分類します。この SDO は、マルウェアの仕組みと動作に関する詳細情報をキャプチャします。

マルウェアの定義

悪意のあるコードを表すマルウェアを定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [マルウェア] 脅威インテリジェンスオブジェクトに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

[マルウェアの詳細] ビュー

フィールド	説明
ID	マルウェアインスタンスを識別する一意の ID。
名前	SDO のプロデューサーによって指定された、マルウェアのインスタンスまたはファミリを識別する名前を入力します。マルウェアファミリの場合は、名前を定義する必要があります。
説明	マルウェアのインスタンスまたはファミリに関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。
マルウェアタイプ	マルウェアのさまざまなカテゴリを示します。
ファミリ	このチェックボックスをオンにして、オブジェクトがマルウェアファミリを表すのか、マルウェアインスタンスを表すのかを指定します。
エイリアス	このマルウェアまたはマルウェアファミリを識別するための代替名。 **注:** アプリケーションに存在しない新しいエイリアスを追加するには、[エイリアス] フィールド自体で使用できる [新しいエイリアスを追加] アイコンをクリックします。
攻撃フェーズ	LM、MITRE ATT&CK などのキルチェーンの攻撃フェーズを表します。
初回確認日	このマルウェアのインスタンスまたはファミリが悪意のあるアクティビティを実行していることが最初に確認された時間。
最終確認日	このマルウェアのインスタンスまたはファミリが悪意のあるアクティビティを実行していることが最後に確認された時間

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
プロセスアーキテクチャ	このマルウェアのプロセスアーキテクチャを示します。
実装言語	このマルウェアの実装言語を示します。
マルウェア機能	マルウェアのインスタンスまたはファミリによって表示される可能性がある機能。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、オレンジ、赤) を使用して、さまざまな感度を示します。
信頼性	このマルウェアの信頼度を入力します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	マルウェアレコードのメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	このマルウェアレコードのコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (マルウェア) の処理ステータスを表します。
作成日時	ソースでオブジェクトが作成された日時を指定します。
更新日時	ソースでオブジェクトが更新された日時を指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

> **重要:**
> 新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。
>
> 観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	マルウェアに関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	マルウェアに関連付けられている分類を選択します。
分類値を追加	マルウェアに関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、マルウェアに関連するオブジェクトの追加情報が表示されます。

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
検出と軽減	このマルウェアに関連する検出と軽減を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ID	このオブジェクトに関連付けられた ID のリスト。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア分析	このオブジェクトに関連付けられたマルウェア分析レポートを一覧表示します。
マルウェア	このオブジェクトに関連付けられたマルウェアレコードを一覧表示します。
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。

自動翻訳

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

マルウェア分析

マルウェア分析は、マルウェアのメタデータと結果をキャプチャします。マルウェア分析は STIX 2.x に適用されます。

マルウェア分析には、マルウェアのインスタンスまたはファミリに対して実行される静的分析または動的分析が含まれます。

マルウェア分析の定義

マルウェアのインスタンスまたはファミリで実行された特定の静的または動的分析のメタデータと結果をキャプチャするマルウェア分析を定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [マルウェア分析] オブジェクトに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

[マルウェア分析の詳細] ビュー

フィールド	説明
ID	マルウェア分析を識別する一意の ID。
製品	使用された分析エンジンまたは製品の名前。製品名は必ずすべて小文字で、単語はダッシュ「-」で区切ってください。 製品の名前を指定できない場合は、匿名値を使用する必要があります。
バージョン	分析の実行に使用された分析製品のバージョン。
ホスト VM	ゲストオペレーティングシステム (該当する場合、マルウェアインスタンスまたはファミリの動的分析に使用された OS) をホストするために使用された仮想マシン環境の説明。 この値が operating_system_ref プロパティと併せて含まれていない場合、動的解析がベアメタル (仮想化なしなど) で実行されたか、情報が編集された可能性があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	このプロパティの値は、SCO ソフトウェア オブジェクトの識別子でなければなりません。
オペレーティングシステム	マルウェアインスタンスまたはファミリの動的分析で使用されたオペレーティングシステム。これは、仮想化されたオペレーティングシステムとベアメタルで実行されているオペレーティングシステムに適用されます。 このプロパティの値は、SCO ソフトウェア オブジェクトの識別子でなければなりません。
構成バージョン	このマルウェアまたはマルウェアファミリを識別するための代替名。
モジュール	この分析の実行時に製品で使用および構成された特定の分析モジュール。
分析エンジンバージョン	分析の実行に使用された分析エンジンまたは製品 (AV エンジンを含む) のバージョン。
分析定義バージョン	AV ツールなどの分析ツールで使用された分析定義のバージョン。
分析が開始されました	マルウェア分析が開始された日時。
分析が終了しました	マルウェア分析が終了した日時。
結果	スキャナーまたはツール分析プロセスで確認された分類結果。
結果名	スキャナーツールによってマルウェアインスタンスに割り当てられた分類結果または名前。
送信済み	スキャンや分析の目的でマルウェアが初めて送信された日時。この値は、スキャンの日付が変わる可能性がある間は一定に保たれます。たとえば、マルウェアがウイルス分析ツールに送信された場合などが挙げられます。
分析された観測事象	分析された観測事象を選択します。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、オレンジ、赤) を使用して、さまざまな感度を示します。
信頼性	このマルウェア分析の信頼度を入力します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インサイト

フィールド	説明
メモ	マルウェアファミリレコードのメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	このマルウェアレコードのコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (マルウェア) の処理ステータスを表します。
作成日時	ソースでオブジェクトが作成された日時を指定します。
更新日時	ソースでオブジェクトが更新された日時を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タグと分類

フィールド	説明
Tags	
タグを選択	マルウェアに関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	マルウェアに関連付けられている分類を選択します。
分類値を追加	マルウェアに関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、マルウェアに関連するオブジェクトの追加情報が表示されます。

関連のレコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
マルウェア	このオブジェクトに関連付けられたマルウェアレコードを一覧表示します。
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。

自動翻訳

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オブジェクトのサイティング

サイティングは、オブジェクトが確認されたことを示します。オブジェクトには、マルウェア、ツール、攻撃者などがあります。

サイティングは、標的が誰であるか、どのように攻撃が実行されたかを追跡し、攻撃動作の傾向を追跡します。

サイティング関係オブジェクトには、汎用関係オブジェクトに存在しない追加のプロパティが含まれています。これらの追加プロパティは、サイティング関係に固有のデータを示します。

オブジェクトのサイティングの定義

オブジェクト (マルウェア、ツール、攻撃者など) が確認されたことを示すオブジェクトのサイティングを定義します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [オブジェクトのサイティング] オブジェクトに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

エンティティと値の選択

フィールド	説明
エンティティ	エンティティオブジェクトのサイティングレコードを選択します。 **注:** 新しいオブジェクトサイティングレコードの作成中に、関連する関係レコードが集計に必要です。
サイティング対象	潜在的な脅威の兆候となる可能性のある特定のエンティティまたはインジケーターが環境で観測されたことを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: [エンティティ] フィールドで選択したオブジェクトに関連付けられているサイティング関連レコードを選択します。これにより、関連レコードを作成してサイティングレコードを集計できます。

オブジェクトサイティングの詳細ビュー

フィールド	説明
ID	攻撃を防ぐ対処措置の一意の ID。
説明	サイティングの詳細とコンテキストを示す説明。
初回確認日	プロパティがサイティングされた SDO が参照する時間枠の開始。
最終確認日	プロパティがサイティングされた SDO の参照する時間枠の終了。
カウント	存在する場合、これは 0～999,999,999 までの整数である必要があり、プロパティがサイティングされた SDO が参照した回数を表します。
サマリー	サイティングをサマリーデータと見なすかどうかを示します。サマリーデータは以前のサイティングレポートの集計であり、プライマリソースデータと見なすべきではありません。
内部	サイティングが内部であるかどうかを示します。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、オレンジ、赤) を使用して、さまざまな感度を示します。
信頼性	この対処措置の信頼度を入力します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	この侵入セットに関するメモを追加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

追加情報

フィールド	説明
追加コンテキスト	この攻撃パターンのコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。
作成日時	ソースでオブジェクトが作成された日時を指定します。
更新日時	ソースでオブジェクトが更新された日時を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

自動翻訳

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	ID に関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
分類	
分類を選択	このインフラストラクチャに関連付けられている分類を選択します。
分類値を追加	このインフラストラクチャに関連付けられている分類値を追加します。

次のタスク
次の関連リストのいずれかをクリックすると、オブジェクトのサイティングに関連するオブジェクトの追加情報が表示されます。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
オブジェクト	サイティングに関連付けられたオブジェクトを一覧表示します。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

観測データ

観測データは、STIX サイバー観測可能オブジェクト (SCO) を使用して、ファイル、システム、ネットワークなどのサイバーセキュリティ関連エンティティに関する情報を伝えます。観測データは STIX 2.x に適用されます。

観測データは、単一のエンティティ (ファイル、ネットワーク接続) の単一の観測事象と、エンティティの複数の観測事象の集計の両方をキャプチャします。

観測データを単独で (関係なしで) 使用して、任意のソースから収集された生データを提供することができます。ソースには、アナリストレポート、サンドボックス、ネットワークおよびホストベースのディスカバリーツールが含まれます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

たとえば、観測データは、IP アドレス、ネットワーク接続、ファイル、またはレジストリキーに関する情報をキャプチャできます。観測データはインテリジェンスのアサーションではなく、意味を示すコンテキストがない生の情報です。

観測データの定義

STIX サイバー観測可能オブジェクト (SCO) を使用して、ファイル、システム、ネットワークなどのサイバーセキュリティ関連エンティティに関する情報を提供します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [観測データ] オブジェクトに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

観測データの詳細ビュー

フィールド	説明
ID	観測データを識別する一意の ID。
初回観測日	データが表示された最初の時刻。
最終観測日	データが表示された最後の時刻。
観測数	各サイバー観測可能オブジェクトが表示された回数。値は 1 ～ 999,999,999 の整数でなければなりません。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、オレンジ、赤) を使用して、さまざまな感度を示します。
信頼性	観測データの信頼度を入力します
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インサイト

フィールド	説明
メモ	この観測データに関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	この観測データのコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
作成日時	ソースでオブジェクトが作成された日時を指定します。
拡張	攻撃パターンの拡張を示します。
更新日時	ソースでオブジェクトが更新された日時を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	観測データに関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
分類を選択	この観測データに関連付けられている分類を選択します。
分類値を追加	この観測データに関連付けられている分類値を追加します。

次のタスク
次の関連リストのいずれかをクリックすると、観測データに関連するオブジェクトの追加情報が表示されます。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。

自動翻訳

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

攻撃者

攻撃者は、悪意を持って行動する個人、グループ、または組織です。攻撃者は STIX 2.x に適用されます。

攻撃者は侵入セットではありませんが、時間の経過とともにさまざまな侵入セット、グループ、または組織をサポートするか、それらと関係する可能性があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

攻撃者は、自身のリソースと侵入セットのリソースを使用して攻撃し、標的に対してキャンペーンを実行します。

攻撃者は、その動機、能力、目標、高度なレベル、過去のアクティビティ、アクセス可能なリソース、および組織内での役割によって特定できます。

攻撃者の定義

攻撃者 (悪意を持って行動する個人、グループ、または組織) を定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [攻撃者] オブジェクトに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

   攻撃者の詳細ビュー

フィールド	説明
ID	攻撃を防ぐ対処措置の一意の ID。
名前	場所を識別するわかりやすい名前を入力します。
説明	侵入セットに関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。
エイリアス	この攻撃者を識別する他の名前のリスト。 **注:** アプリケーションに存在しない新しいエイリアスを追加するには、[エイリアス] フィールド自体で使用できる [新しいエイリアスを追加] アイコンをクリックします。
Goals (最終目標)	この攻撃者の高レベルの目標 (何をしようとしているのか)。たとえば、個人的な利益が動機の場合もありますが、その目的はクレジットカード番号を盗むことです。
攻撃者タイプ	この攻撃者のタイプ。
攻撃者ロール	このオブジェクトのさまざまな攻撃者ロール。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
初回確認日	この攻撃者が最初に確認された時間。 このプロパティは、STIX で利用できるかどうかわからないサイティングからのデータやその他のデータのサマリープロパティです。最初に確認されたタイムスタンプよりも前の新しいサイティングを受信した場合、オブジェクトは新しいデータを考慮して更新される場合があります。
最終確認日	この攻撃者が最後に確認された時間。
プライマリ動機	この攻撃者の背後にある主な理由、動機、または目的。動機は、攻撃者が目標 (達成しようとしていること) を達成したい理由です。 たとえば、ある国のファイナンスセクターを混乱させることを目的とした攻撃者は、反資本主義などのイデオロギーが動機になっている可能性があります。
洗練	攻撃者が攻撃を実行するために必要なスキル、特定の知識、特別なトレーニング、または専門知識。
セカンダリ動機	このプロパティは、この攻撃者の背後にある二次的な理由、動機、または目的を指定します。 これらの動機は、主要な動機と同等またはほぼ等しい原因として存在できます。ただし、主要な動機に取って代わったり、必ずしも拡大したりするわけではありませんが、追加のコンテキストを示している可能性があります。リスト内の位置は重要ではありません。
リソースレベル	この攻撃者が通常機能する組織レベルを指定します。これにより、この攻撃者が攻撃に使用できるリソースが決まります。この属性は高度なプロパティにリンクされています。特定のリソースレベルは、攻撃者が少なくとも特定の高度なレベルにアクセスできることを意味します。
信頼性	この対処措置の信頼度を入力します。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、黄、赤) を使用して、さまざまな感度を示します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インサイト

フィールド	説明
メモ	この攻撃者に関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	この攻撃パターンのコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。
作成日時	ソースでオブジェクトが作成された日時を指定します。
更新日時	ソースでオブジェクトが更新された日時を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タグと分類

フィールド	説明
Tags	
タグを選択	攻撃者に関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	この攻撃者に関連付けられている分類を選択します。
分類値を追加	この攻撃者に関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、攻撃者に関連するオブジェクトの追加情報が表示されます。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
攻撃パターン	このオブジェクトに関連付けられた攻撃を分類するのに役立つ攻撃パターンを一覧表示します。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
ID	このオブジェクトに関連付けられた ID のリスト。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに関連付けられた場所のリスト。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコード (続く)

フィールド	説明
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

脅威イベント

望ましくない結果や影響を引き起こす可能性のあるイベントや状況。

ハッカーによる Web サイト攻撃は脅威イベントとなります。ハッカーが Web サイトに損害を与えたり、情報を盗んだりする行為は脅威イベントとして定義されます。

脅威イベントの定義

非公開情報への不正なアクセスや取得、あるいは情報システムの中断や誤用につながるイベントを、脅威イベントとして定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [脅威イベント] オブジェクトに移動します。
4. [新規] をクリックします。

注:
観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. フォームのフィールドに入力します。

攻撃者の詳細ビュー

フィールド	説明
ID	脅威イベントを防ぐための対処措置の一意の ID。
名前	脅威イベントを識別するわかりやすい名前を入力します。
説明	脅威イベントに関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。
信頼性	この対処措置の信頼度を入力します。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、黄、赤) を使用して、さまざまな感度を示します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	この攻撃者に関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	この攻撃パターンのコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。
作成日時	ソースでオブジェクトが作成された日時を指定します。
更新日時	ソースでオブジェクトが更新された日時を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	脅威イベントに関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	この脅威イベントに関連付けられている分類を選択します。
分類値を追加	この脅威イベントに関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、脅威イベントに関連するオブジェクトの追加情報が表示されます。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコード (続く)

フィールド	説明
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。
観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
観測データ	このオブジェクトに関連付けられた観測データを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

脅威グループ化

脅威グループ化オブジェクトは、参照される STIX オブジェクトに共有コンテキストがあることを明示的に示します。脅威グループ化は STIX 2.x に適用されます。

脅威グループ化オブジェクトは一連のデータを表しますが、十分に分析することで、データが成熟し、インシデントまたは脅威レポートを STIX レポートオブジェクトとして提供できます。たとえば、グループ化を使用して、進行中の調査の特徴を明らかにし、セキュリティイベントまたはインシデントにすることができます。

脅威グループ化オブジェクトを使用して、参照されている STIX オブジェクトが進行中の分析プロセスに関連していると判断することもできます。たとえば、脅威アナリストは、脅威コミュニティの他のユーザーと協力して一連のキャンペーンとインジケーターを調べることができます。

脅威グループ化 SDO には、SDO、SCO、および SRO への参照のリスト、コンテンツで共有されるコンテキストの明示、テキストによる説明、およびグループ化の名前が含まれています。

脅威グループ化の定義

脅威グループ化を、共有コンテキストを持つオブジェクトとして定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [脅威グループ化] オブジェクトに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威グループ化の詳細ビュー

フィールド	説明
ID	脅威グループタイプの攻撃の発生を防ぐための対処措置の一意の ID。
名前	脅威グループを識別するわかりやすい名前を入力します。
説明	脅威イベントに関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。
信頼性	この対処措置の信頼度を入力します。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、黄、赤) を使用して、さまざまな感度を示します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	この脅威グループ化に関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	この攻撃パターンのコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。
作成日時	ソースでオブジェクトが作成された日時を指定します。
更新日時	ソースでオブジェクトが更新された日時を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	脅威グループ化に関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	この脅威グループ化に関連付けられている分類を選択します。
分類値を追加	この脅威グループ化に関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、脅威グループ化に関連するオブジェクトの追加情報が表示されます。

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。
観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
観測データ	このオブジェクトに関連付けられた観測データを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
脅威イベント	このオブジェクトに関連付けられている脅威イベントの一覧を示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

脅威メモ

脅威メモは、そのメモが関連する STIX オブジェクト、マーク定義オブジェクト、または言語コンテンツオブジェクトに含まれていない追加の分析を提供するための情報テキストを提供します。脅威メモは STIX 2.x に適用されます。

たとえば、アナリストが別の組織によって作成されたキャンペーンオブジェクトにメモを追加する場合があります。そのメモには、ハッカーフォーラムでそのキャンペーンに関連する投稿を見たことを示すことができます。

メモは通常、人間のアナリストによって作成され、人間向けのテキストで構成されます。メモには、メモを作成した作成者をキャプチャするための追加のプロパティが含まれています。

脅威メモの定義

既存のオブジェクトでは利用できない詳細なコンテキストまたは分析を提供する脅威メモを定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)**] アイコンをクリックします。
3. [脅威メモ] に移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威メモの詳細ビュー

フィールド	説明
ID	脅威メモの一意の ID。
抽象	メモの内容の簡単な概要を指定します。
コンテンツ	メモの内容を指定します。
作成者	作成者の名前 (アナリストなど) を指定します。
信頼性	この対処措置の信頼度を入力します。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、黄、赤) を使用して、さまざまな感度を示します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	この脅威メモにメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	この攻撃パターンのコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
作成日時	ソースでオブジェクトが作成された日時を指定します。
更新日時	ソースでオブジェクトが更新された日時を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	脅威グループ化に関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	この脅威グループ化に関連付けられている分類を選択します。
分類値を追加	この脅威グループ化に関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、脅威メモに関連するオブジェクトの追加情報が表示されます。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコード (続く)

フィールド	説明
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。
観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
観測データ	このオブジェクトに関連付けられた観測データを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
脅威イベント	このオブジェクトに関連付けられている脅威イベントの一覧を示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

脅威に関する意見

意見は、別のエンティティによって生成された STIX オブジェクト内の情報の正確性を評価するものです。脅威に関する意見は STIX 2.x に適用されます。

意見プロパティは、固定スケールを使用して賛成または反対のレベルをキャプチャします。固定スケールは、複数の意見にまたがる一貫した統計操作を可能にする数値マッピングもサポートしています。

たとえば、消費組織のアナリストがキャンペーンオブジェクトに「強く反対」し、その理由を説明するとします。

意見は主観的なものであり、仕様にはそれらを解釈する最善の方法は記載されていません。

意見は人間のアナリストによって作成され、人間向けのテキストで構成されます。意見には、意見を作成した作成者をキャプチャするための追加のプロパティが含まれています。

脅威に関する意見の定義

STIX オブジェクト内の情報の正確性のアセスメントとして脅威に関する意見を定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [脅威に関する意見] オブジェクトに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威に関する意見の詳細ビュー

フィールド	説明
ID	脅威に関する意見の一意の ID。
意見	STIX オブジェクトに関するプロデューサーの意見。
説明	意見の内容を指定します。
作成者	作成者の名前 (アナリストなど) を指定します。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、オレンジ、赤) を使用して、さまざまな感度を示します。
信頼性	この対処措置の信頼度を入力します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	この脅威に関する意見にメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	この脅威に関する意見にコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
作成日時	ソースでレコードが作成される時刻を指定します。
更新日時	ソースでレコードが変更される時刻を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	脅威に関する意見に関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	この脅威に関する意見に関連付けられている分類を選択します。
分類値を追加	この脅威に関する意見に関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、脅威に関する意見に関連するオブジェクトの追加情報が表示されます。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコード (続く)

フィールド	説明
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。
観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
観測データ	このオブジェクトに関連付けられた観測データを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
脅威イベント	このオブジェクトに関連付けられている脅威イベントの一覧を示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

脅威レポート

脅威レポートは、1 つ以上のトピックに焦点を当てた脅威インテリジェンスのコレクションです。脅威レポートは STIX 2.x に適用されます。

脅威レポートには、コンテキストや関連する詳細を含む、攻撃者、マルウェア、攻撃手法の説明が含まれます。これらは、包括的なサイバー脅威ストーリーとして公開できるように、関連する脅威インテリジェンスをグループ化するために使用されます。

脅威レポート SDO には、レポートの説明と名前とともに STIX オブジェクトへの参照のリストが含まれています。

脅威レポートの定義

コンテキストや関連する詳細を含む、攻撃者、マルウェア、攻撃テクニックについて説明した脅威レポートを定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)**] アイコンをクリックします。
3. [脅威レポート] オブジェクトに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

脅威レポートの詳細ビュー

フィールド	説明
ID	脅威レポートを識別する名前を指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
名前	メモの内容の簡単な概要を指定します。
説明	レポートに関する追加のインサイトとコンテキストの説明。
レポートタイプ	作成者の名前 (アナリストなど) を指定します。
公開	このレポートがレポート作成者によって正式に公開された日付。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、黄、赤) を使用して、さまざまな感度を示します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	この脅威メモにメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	この攻撃パターンのコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。
作成日時	ソースでオブジェクトが作成された日時を指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
更新日時	ソースでオブジェクトが更新された日時を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	脅威グループ化に関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	この脅威グループ化に関連付けられている分類を選択します。
分類値を追加	この脅威グループ化に関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、脅威レポートに関連するオブジェクトの追加情報が表示されます。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコード (続く)

フィールド	説明
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。
観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
観測データ	このオブジェクトに関連付けられた観測データを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
脅威イベント	このオブジェクトに関連付けられている脅威イベントの一覧を示します。
脅威グループ化	このオブジェクトに関連付けられている脅威グループ化を一覧表示します。
脅威レポート	このオブジェクトに関連付けられた脅威レポートを一覧表示します。
ツール	このオブジェクトに関連付けられている、攻撃者が攻撃を実行するために使用する正当なソフトウェアを一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

ツール

ツールは、攻撃者が攻撃を行うために使用する正当なソフトウェアのことです。ツールは STIX 2.x に適用されます。

ツールを使用すると、攻撃者がツールをいつどのように使用してキャンペーンを実行するかを知ることができます。マルウェアとは異なり、これらのツールまたはソフトウェアパッケージはシステム上で見つかることが多く、パワーユーザー、アドミン、ネットワークアドミニストレーター、または通常のユーザーにとっても正当な目的を持っています。

たとえば、リモートアクセスツール (RDP) やネットワークスキャンツール (Nmap) は、攻撃者が攻撃中に使用するツールです。

ツールの定義

攻撃者が攻撃を実行するために使用する正当なソフトウェアとしてツールを定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [ツール] オブジェクトに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

ツールの詳細ビュー

フィールド	説明
ID	ツールを識別する一意の ID。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
名前	ツールを識別するわかりやすい名前を入力します。
説明	ツールに関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。
ツールタイプ	説明されているツールの種類。
エイリアス	このツールを識別するために使用する代替名。 注: アプリケーションに存在しない新しいエイリアスを追加するには、[エイリアス] フィールド自体で使用できる [新しいエイリアスを追加] アイコンをクリックします。
ツールバージョン	ツールに関連付けられているバージョン識別子。
攻撃フェーズ	LM、MITRE ATT&CK などのキルチェーンの攻撃フェーズを表します。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、黄、赤) を使用して、さまざまな感度を示します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	このツールに関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	このツールのコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。
作成日時	ソースでオブジェクトが作成された日時を指定します。
更新日時	ソースでオブジェクトが更新された日時を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	脅威グループ化に関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	この脅威グループ化に関連付けられている分類を選択します。
分類値を追加	この脅威グループ化に関連付けられている分類値を追加します。

次のタスク
次の関連リストのいずれかをクリックすると、ツールに関連するオブジェクトの追加情報が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
検出と軽減	このオブジェクトに関連付けられている検出と軽減を一覧表示します。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。
観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
観測データ	このオブジェクトに関連付けられた観測データを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

脆弱性

脆弱性とは、攻撃者が悪用するソフトウェアまたはハードウェアコンポーネントの弱点または欠陥のことです。脆弱性は STIX 2.x に適用されます。

脆弱性または欠陥は、ソフトウェアまたはハードウェアコンポーネントに含まれるコードの要件、設計、または実装にあります。この脆弱性は、そのシステムの機密性、完全性、または可用性に悪影響を及ぼすために直接悪用されます。

CVE は、公開されている既知の問題 [CVE] の共通名を提供する情報セキュリティの脆弱性とエクスポージャーのリストです。

たとえば、マルウェアが CVE-2015-12345 を悪用する場合、マルウェアオブジェクトは CVE-2015-12345 を参照する脆弱性オブジェクトにリンクされます。

脆弱性の定義

攻撃者が悪用するソフトウェアまたはハードウェアコンポーネントの弱点または欠陥として脆弱性を定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [脆弱性]オブジェクトに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脆弱性の詳細ビュー

フィールド	説明
ID	脆弱性を識別する一意の ID。
名前	脆弱性を識別するために使用される名前。
説明	脆弱性に関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。
重大度	この脆弱性の重大度を正規化したものを示します
CVSS3.0	この脆弱性の CVSS v3 を示します。
CVSS2.0	この脆弱性の CVSS v2 を示します。
エクスプロイトステータス	この脆弱性に関連付けられているエクスプロイトステータスを示します。
公開	脆弱性が公開される時期を示します。
最後に変更されたレコード	レコードが最後に変更された日時を示します。
影響を受けるソフトウェア	脆弱性に関連する影響を受けるソフトウェアを一覧表示します。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、黄、赤) を使用して、さまざまな感度を示します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	この脆弱性に関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	この脆弱性のコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。
作成日時	ソースでオブジェクトが作成された日時を指定します。
更新日時	ソースでオブジェクトが更新された日時を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	脆弱性に関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	この脆弱性に関連付けられている分類を選択します。
分類値を追加	この脆弱性に関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、脆弱性に関連するオブジェクトの追加情報が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
検出と軽減	このオブジェクトに関連付けられている検出と軽減を一覧表示します。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
マーケティング定義	このオブジェクトに関連付けられたマーケティング定義を一覧表示します。
サイティング	このオブジェクトに関連付けられたサイティングを一覧表示します。
観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
観測データ	このオブジェクトに関連付けられた観測データを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
脆弱性	このオブジェクトに関連付けられている、攻撃者が悪用するソフトウェアまたはハードウェアの脆弱性または欠陥を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

脆弱性データのフェッチ

構成アイテム、脆弱性エントリー、ビジネスコンテキストなどの脆弱性関連データをフェッチします。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [脆弱性]オブジェクトに移動します。
   このオブジェクトに関連付けられている関連する脆弱性が表示されます。
4. それぞれの脆弱性レコードを選択します。
   CVE が関連付けられている場合は、表示されたボタンを使用して脆弱性関連データを自動的にフェッチできます。これらの関連レコードは、[脆弱性] の [ビジネスコンテキスト] セクションに表示されます。
5. 検索項目 内部インテリジェンス > 脆弱なエントリー.
   関連する CVE レコードが表示されます。
6. 任意の CVE を選択し、[脆弱性関連データをフェッチ] ボタンをクリックします。

注:

- このリンクは、レコードを自動的に関連付け、レコードの特定のビジネスコンテキストをフェッチします。
- レコードが関連付けられていない場合は、[この特定の脆弱性オブジェクトには、関連付けられた脆弱性エントリーがありません。データをフェッチするには、オブジェクトを脆弱性エントリーに関連付ける必要があります。(This specific vulnerability object doesn't have any vulnerable entries associated with it.)] という情報メッセージが表示されます。
- このボタンをクリックすると、バックグラウンドのスケジュール済みジョブがトリガーされ、ジョブの開始と実行の詳細が [アクティビティストリーム] セクションに表示されます。たとえば、ジョブがトリガーされると、アクティビティストリームには、脆弱性エントリーに関連するデータのフェッチを開始したアクティビティが表示されます。スケジュール済みジョブを実行してデータをフェッチする方法の詳細については、「スケジュール済みジョブ」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. [リンク] をクリックして、オブジェクトを手動でリンクします。
8. リンクするレコードを選択し、[脆弱性関連データをフェッチ **(Fetch Vulnerability related data)**] ボタンを使用して脆弱性関連データをフェッチします。
このボタンをクリックすると、バックグラウンドジョブがトリガーされ、データがそれぞれのセクションに自動的にフェッチされます。[脆弱性エントリーに関連付けられたデータをフェッチするジョブが開始されました (Job to fetch data associated with the vulnerable entries has started.)]というメッセージが表示されます。アクティビティストリームでステータスを追跡し、ジョブが完了したらリストを更新して結果を確認できます。たとえば、データが構成アイテムに関連している場合は、[構成アイテム] セクションで結果を確認します。CVE の追加の詳細については、「CVE をサードパーティエントリーに追加」を参照してください。

> **注:**
> 同様に、観測事象レコードデータをフェッチできます。詳細については、「脆弱性データのフェッチ」を参照してください。

マーキング定義

マーキング定義オブジェクトは、特定のマーキングを示します。データマーキングは通常、データの処理または共有の要件を表します。

マーキング定義を定義する

データの要件を処理および共有するためのマーキング定義を定義します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)**] アイコンをクリックします。
3. [マーキング定義] オブジェクトに移動します。
4. [新規] をクリックします。

> **注:**
> 観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

マーキング定義ソースの詳細ビュー

フィールド	説明
ID	マーキング定義を識別する一意の ID。
名前	マーキング定義を識別するために使用される名前。
定義タイプ	type プロパティは、オブジェクトのタイプを識別します。definition_type プロパティは、マーキング定義のタイプを識別します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
定義	definition プロパティには、マーキングオブジェクト自体 (TLP など) が含まれます。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、オレンジ、赤) を使用して、さまざまな感度を示します。
信頼性	このオブジェクトの信頼度を入力します。 信頼度プロパティは、作成者がデータの正確性に対して持っている信頼性を識別します。信頼度値は 0～100 の範囲にする必要があります。

インサイト

フィールド	説明
メモ	このマーキング定義に関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	このマーキング定義のコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。
作成日時	ソースでオブジェクトが作成された日時を指定します。
更新日時	ソースでオブジェクトが更新された日時を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [保存] をクリックします。
   保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

> **重要:**
> 新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。
>
> 観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	脆弱性に関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	この脆弱性に関連付けられている分類を選択します。
分類値を追加	この脆弱性に関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、脆弱性に関連するオブジェクトの追加情報が表示されます。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。
攻撃パターン	このオブジェクトに関連付けられた攻撃パターンを一覧表示します。
キャンペーン	このオブジェクトに関連付けられたキャンペーンを一覧表示します。
検出と軽減	このオブジェクトに関連付けられている検出と軽減を一覧表示します。
ID	このオブジェクトに関連付けられた ID を一覧表示します。
インジケーター	このオブジェクトに関連付けられた脅威ソースによって特定された、関連するセキュリティ侵害のインジケーター (IoC) を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコード (続く)

フィールド	説明
インフラストラクチャ	このオブジェクトに関連付けられているシステム、ソフトウェア サービス、および関連する物理リソースまたは仮想リソースを一覧表示します。
侵入セット	このオブジェクトに関連付けられた共通プロパティを持つ、一連の攻撃者の行動とリソースを一覧表示します。
場所	このオブジェクトに地理的コンテキストを提供する場所を一覧表示します。
マルウェア	このオブジェクトに関連付けられた悪意のあるコードを一覧表示します。
マルウェア分析	このオブジェクトに関連付けられた悪意のある分析を一覧表示します。
観測事象	このオブジェクトに関連付けられた観測事象を一覧表示します。
観測データ	このオブジェクトに関連付けられた観測データを一覧表示します。
攻撃者	このオブジェクトに関連付けられている、悪意を持って行動する個人、グループ、または組織を一覧表示します。
脅威イベント	このオブジェクトに関連付けられている脅威イベントの一覧を示します。
脅威グループ化	このオブジェクトに関連付けられている脅威グループ化を一覧表示します。
脅威メモ	このオブジェクトに関連付けられている脅威メモを一覧表示します。
脅威に関する意見	このオブジェクトに関連付けられた脅威に関する意見を一覧表示します。
ツール	このオブジェクトに関連付けられているツールを一覧表示します。
脆弱性	このオブジェクトに関連する脆弱性を一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

データコンポーネント

データコンポーネントは、データソースの特定のプロパティまたは値を識別するために使用されます。

データコンポーネントを定義する

データソースのプロパティまたは値を識別するデータコンポーネントを定義します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [データコンポーネント] オブジェクトに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

データコンポーネントの詳細ビュー

フィールド	説明
ID	データコンポーネントを識別する一意の ID。
名前	データコンポーネントを識別するために使用される名前。
説明	脆弱性に関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
データソース	この脆弱性の重大度を正規化したものを示します
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、黄、赤) を使用して、さまざまな感度を示します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
信頼性	このオブジェクトの信頼度を示します。信頼度は 0～100 の間でなければなりません。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	このデータコンポーネントに関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	このデータコンポーネントのコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	データコンポーネントの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。
作成日時	ソースでオブジェクトが作成された日時を指定します。
更新日時	ソースでオブジェクトが更新された日時を指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

> **重要:**
> 新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。
>
> 観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	脆弱性に関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	この脆弱性に関連付けられている分類を選択します。
分類値を追加	この脆弱性に関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、データコンポーネントに関連するオブジェクトの追加情報が表示されます。

関連レコード

フィールド	説明
攻撃パターン	このオブジェクトに関連付けられた攻撃パターンを一覧表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

データソース

データソースは、センサー/ログによって収集できる情報のさまざまな主題/トピックを表します。データソースには、データソースの特定のプロパティ/値を識別するデータコンポーネントも含まれます。

データソースを定義する

情報のさまざまな主題またはトピックを表すデータソースを定義します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. [データソース] オブジェクトに移動します。
4. [新規] をクリックします。

   注:
   観測事象、インジケーター、エンティティ、オブジェクトのオブジェクトレコードを新たに作成するたびに、ソースレコードが作成され、新しいオブジェクトレコードが作成されたことを示すプロンプトメッセージが表示されます。その後、ユーザーは集計レコードにリダイレクトされます。

5. フォームのフィールドに入力します。

脆弱性の詳細ビュー

フィールド	説明
ID	データソースを識別する一意の ID。
名前	データソースを識別するために使用される名前。
説明	データソースに関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
コレクションレイヤー	ホスト、ネットワーク、クラウドコントロールプレーンなど、データソースを物理的に収集する場所の説明を示します。
プラットフォーム	攻撃者が操作しているシステムがオペレーティングシステムまたはアプリケーションである可能性があることを示します。
貢献者	このデータソースの貢献者を示します。
TLP	TLP は、機密情報が適切な対象者と共有されるようにするために使用されるものです。4 つの色 (白、緑、黄、赤) を使用して、さまざまな感度を示します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。

インサイト

フィールド	説明
メモ	このデータソースに関するメモを追加します。

追加情報

フィールド	説明
追加コンテキスト	このデータソースに関するコンテキストを追加します。
仕様バージョン	このオブジェクトを表すために使用される STIX 仕様のバージョン。 この仕様に従って定義された STIX オブジェクトの場合、このプロパティの値は 2.1 である必要があります。
言語	このプロパティは、このオブジェクトのテキストコンテンツの言語を識別します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
拡張	攻撃パターンの拡張を示します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
処理ステータス	このオブジェクト (対処措置) の処理ステータスを表します。
作成日時	ソースでオブジェクトが作成された日時を指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
更新日時	ソースでオブジェクトが更新された日時を指定します。
作成者参照	このプロパティは、エンティティを記述する ID オブジェクトがこのオブジェクトを作成したことを示します。

6. [保存] をクリックします。
保存すると、「新しい観測事象レコードが作成されました。レコードを編集して新たな関連を作成するには [続行] をクリックしてください」というプロンプトメッセージが表示されます。
7. [続行] をクリックします。

重要:
新しい観測事象レコードを作成すると、[システムの更新を防止] チェックボックスが表示されます。

観測事象、インジケーター、STIX オブジェクトのレコードが作成された後、システムにより更新されないようにするには、このチェックボックスをオンにします。

タグと分類

フィールド	説明
Tags	
タグを選択	データソースに関連付けられているタグを選択します。
タグを追加	新しいタグを追加します。
分類	
分類を選択	このデータソースに関連付けられている分類を選択します。
分類値を追加	このデータソースに関連付けられている分類値を追加します。

次のタスク

次の関連リストのいずれかをクリックすると、データソースに関連するオブジェクトの追加情報が表示されます。

関連レコード

フィールド	説明
外部参照	STIX 以外の情報を参照する外部参照を一覧表示します。このプロパティは、1 つ以上の外部オブジェクト識別子を指定するために使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

1. このオブジェクトに関連付けられた関連レコードをリンクおよびリンク解除できます。詳細については、「脅威インテリジェンス関連レコードへのリンク」を参照してください。
2. TI ライブラリ内のさまざまな SDO には、潜在的な関係も含まれています。任意の 2 つのオブジェクト間の関係を確立するには、脅威インテリジェンスライブラリの [潜在リレーションシップ] リンクを使用してオブジェクト間の関係を確定します。詳細については、「オブジェクトとオブジェクトの潜在リレーションシップを確認する」を参照してください。
3. また、オブジェクトフォームビューの [関連レコード] セクションを使用し、フォームビューで使用可能な [潜在リレーションシップ] セクションを使用して、2 つのオブジェクト間の関係を確認します。詳細については、「関連レコードから潜在リレーションシップを確認する」を参照してください。
4. ケースにオブジェクトを追加できます。詳細については、「ケースに追加する」を参照してください。

RSS フィードの定義

脅威インテリジェンスフィードは、サイバーリスクまたは脅威に関連する情報を収集するリアルタイムの継続的なデータストリームです。RSS フィードを使用すると、ブログや最新のサイバーセキュリティニュースなど、お気に入りの Web サイトの最新情報を簡単に入手できます。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. **[RSS** フィード] オブジェクトに移動します。

   注:
   取り込まれたフィードはこのセクションを使用して参照できますが、新しいレコードを作成することはできません。

4. フォームでは、次のフィールドが自動入力されます。

RSS フィードの詳細ビュー

フィールド	説明
タイトル	RSS フィードのタイトル。
説明	RSS フィードに関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。
リンク	RSS フィードに追加されたリンクを示します。
ソース	このオブジェクトレコードの作成元の RSS フィードソースを指定します。
公開日	RSS フィードがいつ公開されるかを示します。
作成者	RSS フィードの作成者を示します。

5. [保存] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インサイト

フィールド	説明
メモ	このフィードにメモを追加します。

追加情報

フィールド	説明
メディア URL	メディア URL を示します。
フィードバックコメント	フィードバックに関する追加のフィードバックコメント。

関係オブジェクト

関係オブジェクトを使用して、2 つの観測事象または観測事象と SDO をリンクし、それらが互いにどのように関連しているかを説明します。

STIX 関係オブジェクト (SRO) は、さまざまな STIX オブジェクト間の関係のタイプを表します。次の関係オブジェクトを使用できます。

- 観測事象と観測事象の関係：このオブジェクトは、観測事象間の関係を定義します。
- オブジェクトとオブジェクトの関係：このオブジェクトは、インジケーターオブジェクトを除く SDO 間の関係を定義します。オブジェクトとオブジェクトで定義された関係の例は、攻撃パターンがマルウェアを配信する関係です。
- オブジェクトと観測事象の関係：このオブジェクトは、SDO と観測事象オブジェクト (SCO) の間の関係を定義します。オブジェクトと観測事象で定義された関係の例は、潜在的な攻撃の情報を提供するサイバー観測事象オブジェクトでインフラストラクチャが構成されている関係です。
- オブジェクトとインジケーターの関係：このオブジェクトは、SDO とインジケーターオブジェクト間の関係を定義します。
- インジケーターとインジケーターの関係：このオブジェクトは、インジケーターオブジェクト間の関係を定義します。
- インジケーターと観測事象の関係：このオブジェクトは、インジケーターオブジェクトと他の SDO の間の関係を定義します。オブジェクトとインジケーターで定義された関係の例は、インジケーターがキャンペーンの証拠を検出する関係です。

オブジェクトリレーションシップ

関係オブジェクト	ソースの例	ターゲットの例	説明の例
観測事象と観測事象の関係	IP アドレス、ドメイン名		この関係は、観測事象間の関係を表します。
オブジェクトとオブジェクトのリレーションシップ	攻撃パターン	マルウェア	この関係は、このマルウェアインスタンス (またはファミリ) を配信するためにこの攻撃パターンが使用されることを示しています。
オブジェクトと観測事象のリレーションシップ			この関係は、オブジェクトと観測事象間の関係を表します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オブジェクトリレーションシップ (続く)

関係オブジェクト	ソースの例	ターゲットの例	説明の例
オブジェクトとインジケーターの関係	インジケーター	攻撃パターン、キャンペーン、インフラストラクチャ、侵入セット、マルウェア、攻撃者、ツール	この関係は、関連する攻撃パターン、キャンペーン、インフラストラクチャ、侵入セット、マルウェア、攻撃者、またはツールの証拠をインジケーターが検出できることを示しています。 証拠が直接的でない場合があります。たとえば、特定のキャンペーンでよく使用されるマルウェアなど、キャンペーンの二次的証拠をインジケーターで検出することもできます。
インジケーターとインジケーターの関係	インフラストラクチャ	観測データ	この関係は、観測されたデータオブジェクトからの情報に基づいてインジケーターが作成されていることを示しています。 オブジェクトと観測事象で定義された関係の例は、潜在的な攻撃の情報を提供するサイバー観測事象オブジェクトでインフラストラクチャが構成されている関係です。
インジケーターと観測事象			この関係は、インジケーターと観測事象間の関係を表します。

自動翻訳

観測事象と観測事象の関係を定義する

観測事象間の関係を定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. 検索項目 リレーションシップ > 観察事項 - 観察事項.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [**New**] をクリックします。
5. 必要に応じて、フォームのフィールドに入力します。
6. [送信] をクリックします。

オブジェクトとオブジェクトの関係の定義

SDO 間の関係を定義します (インジケーターオブジェクトを除く)。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. 検索項目 リレーションシップ > オブジェクト - オブジェクト.
4. [**New**] をクリックします。
5. 必要に応じて、フォームのフィールドに入力します。
6. [送信] をクリックします。

オブジェクトと観測事象の関係の定義

SDO と観測事象オブジェクト (SCO) 間の関係を定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. 検索項目 リレーションシップ > オブジェクト:観察事項.
4. [**New**] をクリックします。
5. 必要に応じて、フォームのフィールドに入力します。
6. [送信] をクリックします。

オブジェクトとインジケーターの関係の定義

インジケーターオブジェクトと他の SDO 間の関係を定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)**] アイコンをクリックします。
3. 検索項目 リレーションシップ > オブジェクトインジケーター.
4. [**New**] をクリックします。
5. 必要に応じて、フォームのフィールドに入力します。
6. [送信] をクリックします。

インジケーターとインジケーターの関係を定義する

インジケーターオブジェクトと他のオブジェクト間の関係を定義します。関係オブジェクトを使用して、2 つの観測事象または観測事象と SDO をリンクし、それらが互いにどのように関連しているかを説明します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)**] アイコンをクリックします。
3. 検索項目 リレーションシップ > インジケーター **-** インジケーター.
4. [**New**] をクリックします。
5. 必要に応じて、フォームのフィールドに入力します。
6. [送信] をクリックします。

インジケーターと観測事象の関係を定義する

インジケーターオブジェクトと他の SDO 間の関係を定義します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)**] アイコンをクリックします。
3. 検索項目 リレーションシップ > インジケーターと観測事象.
4. [**New**] をクリックします。
5. 必要に応じて、フォームのフィールドに入力します。
6. [送信] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

潜在リレーションシップ

アプリケーションは、自動相関を使用して、2 つの SDO、2 つの観測事象、または観測事象と SDO の間に起こりうる関係を確立します。

1. 関連する可能性があるレコードを 1 つ以上選択し、UI でこのアクションを適用すると、レコードがさらに確認済みの関係に変更され、[関連レコード] セクションに表示されます。
2. アナリストが取り込んだ、または手動で作成した確認済みの相関関係は、自動相関によって作成された潜在的な関係を上書きします。

観測事象と観測事象の潜在リレーションシップを確認する

このセクションを使用して、観測事象間の関係を確認します。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。
3. 検索項目 潜在リレーションシップ > 観察事項 **-** 観察事項.
4. 観測事象レコードを選択します。
5. [関係を確認 **(Confirm Relation)]** をクリックします。
   潜在リレーションシップレコードを作成するのが理想的で、相関ルールに基づいて識別されます。関係を確認すると、観測事象レコードは [関係] セクションに移動します。これは、観測事象と観測事象の関係が確認されたことを意味します。レコードには、相関ルールに一致した場合にのみ確認済みの関係が表示されます。たとえば、URL タイプの 2 つの観測事象のドメイン名が同じ場合に、潜在リレーションシップを作成できます。

   または、観測事象のリストから観測事象をリンクして新しい観測事象レコードを作成し、各観測事象の [関連レコード] タブで関係を確認することもできます。

   a. 任意の観測事象レコードを開きます。

   b. [関連レコード] タブに移動します。

   c. [リンク] ボタンをクリックします。

   d. 観測事象を 1 つ以上選択します。

   e. [リンク] をクリックします。
      これにより、選択した観測事象レコードと新しくリンクされた観測事象の間に新しい関係が作成されます。

6. [削除] をクリックして関係を削除します。

オブジェクトとオブジェクトの潜在リレーションシップを確認する

オブジェクト間の潜在リレーションシップを定義します。

始める前に

必要なロール：sn_sec_tisc.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)**] アイコンをクリックします。
3. 検索項目 潜在リレーションシップ > オブジェクト - オブジェクト.
4. 観測事象レコードを選択します。
5. [関係を確認 **(Confirm Relation)**] をクリックします。
   潜在リレーションシップレコードを作成するのが理想的で、相関ルールに基づいて識別されます。このセクションから関係を確認すると、観測事象レコードが [関係] セクションに移動します。これは、観測事象と観測事象の関係が確認されたことを意味します。レコードには、相関ルールに一致した場合にのみ確認済みの関係が表示されます。たとえば、URL タイプの 2 つの観測事象のドメイン名が同じ場合に、潜在リレーションシップを作成できます。

   または、観測事象のリストから観測事象をリンクして新しい観測事象レコードを作成し、各観測事象の [関連レコード] タブで関係を確認することもできます。

   a. 任意の観測事象レコードを開きます。

   b. [関連レコード] タブに移動します。

   c. [リンク] ボタンをクリックします。

   d. 観測事象を 1 つ以上選択します。

   e. [リンク] をクリックします。
      これにより、選択した観測事象レコードと新しくリンクされた観測事象の間に新しい関係が作成されます。
6. [削除] をクリックして関係を削除します。

インジケーターとインジケーターの潜在リレーションシップを確認する

オブジェクト間の潜在リレーションシップを定義します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)**] アイコンをクリックします。
3. 検索項目 潜在リレーションシップ > **indicator-indicator**.
4. 観測事象レコードを選択します。
5. [関係を確認 **(Confirm Relation)**] をクリックします。
   潜在リレーションシップレコードは、関連付けの自動化ルールに基づいて確認するのが理想的です。関係を確認すると、観測事象レコードは [関係] セクションに移動します。これは、観測事象と観測事象の関係が確認されたことを意味します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レコードには、相関ルールに一致した場合にのみ確認済みの関係が表示されます。たとえば、URL タイプの 2 つの観測事象のドメイン名が同じである場合、潜在リレーションシップが確認されます。

または、観測事象のリストから観測事象をリンクして新しい観測事象レコードを作成し、各観測事象の [関連レコード] タブで関係を確認することもできます。

a. 任意の観測事象レコードを開きます。

b. [関連レコード] タブに移動します。

c. [リンク] ボタンをクリックします。

d. 観測事象を 1 つ以上選択します。

e. [リンク] をクリックします。
これにより、選択した観測事象レコードと新しくリンクされた観測事象の間に新しい関係が作成されます。

6. [削除] をクリックして関係を削除します。

関連レコードから潜在リレーションシップを確認する

2 つの SDO 間の関係を確認します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.

2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library)]** アイコンをクリックします。

3. [関連レコード] セクション移動します。

4. [潜在リレーションシップ **(Potential Relationships)]** を展開します。

5. 観測事象、インジケーター、または 2 つの SDO 間の関係を確認するその他のオブジェクトなどのレコードを開きます。

6. たとえば、ここでは左側のナビゲーションから [観測事象] を選択します。

7. リストから [観測事象] レコードを選択します。

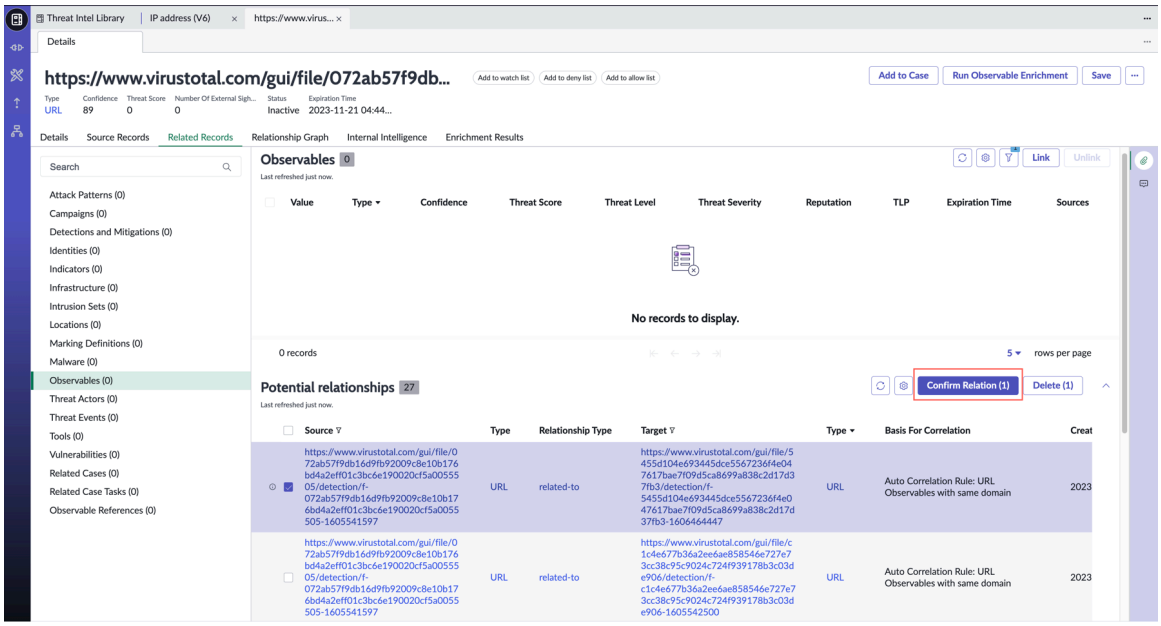
> **注:**
> リストセクションには、関連する観測事象のリンクされた観測事象レコードがすべて表示されます。

8. [関係を確認 **(Confirm Relationships)]** ボタンをクリックして、オブジェクト間の関係を確認します。

> **注:**
> 詳細については、「関係オブジェクト」と「潜在リレーションシップ」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



9. [削除] をクリックして、関連する観測事象を削除します。
SDO 間の潜在的な関係および関係の確立方法については、「潜在リレーションシップ」および「関係オブジェクト」を参照してください。

関連付けの自動化

関連付けの自動化は、観測事象、インジケーター、およびオブジェクト間の関係を識別するのに役立ちます。

相関プロセスにより、アプリケーションは事前定義されたルールに基づいて脅威インテリジェンスレコード間の相関を自動的に確立します。適用されたルールのタイプに基づいて、リレーションシップは確認済みのリレーションシップまたは潜在リレーションシップである可能性があります。オブジェクト間のリレーションシップが確認されると、それらのオブジェクトが [関連レコード] セクションのそのオブジェクトの詳細ビューに自動的に表示されます。

以下では、リレーションシップと潜在リレーションシップについて説明します。

- リレーションシップ：リレーションシップオブジェクトを使用して、2 つの観測事象または観測事象と SDO をリンクし、それらが互いにどのように関連しているかを説明します。
- 潜在リレーションシップ：潜在リレーションシップを使用して、自動相関を使用して、2 つの SDO、2 つの観測事象、または観測事象と SDO の間の潜在的な関係を確立します。

ベースシステム内でプロビジョニングされる事前定義された相関ルールは、次のとおりです。

相関ルール

ルール名	ルールの説明	ルール定義	ルールアクション
同じファイルハッシュを持つ観測事象	このルールは、(同じタイプの) 観測事象のハッシュ値を比較し、同じハッシュを共有しているかどうかを識別します。	このルールは、インジケーターの (同じタイプの) ハッシュ値を比較し、同じハッシュを共有しているかどうかを識別します。	リレーションシップを作成
同じドメインの URL 観測事象	このルールは、URL の構造の共通性を調べて、同じベースドメイ	このルールは、URL の構造の共通性を調べます。つまり、URL が	潜在リレーションシップを作成

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

相関ルール (続く)

ルール名	ルールの説明	ルール定義	ルールアクション
	ンを共有しているかどうかを識別します。	同じベースドメインを共有し、類似したサブディレクトリ構造を持っているかどうかを識別します。	
ネットワークオブジェクトのソースとして検出された観測事象	このルールは、ネットワークソース属性値をシステム内の IPV4、IPV6、またはドメイン名の観測事象と照合し、トラフィックのソースとしてリンクします。	このルールは、ソース属性値をシステム内の IPV4、IPV6、またはドメイン名の観測事象と照合し、トラフィックのソースとしてリンクします。	リレーションシップを作成
ネットワークオブジェクトの宛先として検出された観測事象	このルールは、ネットワーク宛先属性値をシステム内の IPV4、IPV6、またはドメイン名の観測事象と照合し、トラフィックの宛先としてリンクします。	このルールは、ソース属性値をシステム内の IPV4、IPV6、またはドメイン名の観測事象と照合し、トラフィックの宛先としてリンクします。	リレーションシップを作成
通信に基づいて観測事象を関連付ける	このルールは、ネットワークオブジェクトに基づいて、同じ宛先 (IPV4、IPV6、またはドメイン名) と通信するすべての観測事象 (IPV4、IPV6、およびドメイン名) を識別し、これらの観測事象間の関係を確立します。 また、関連する観測事象 (IPV4、IPV6、およびドメイン名) は、宛先と通信するソースと同じネットワークオブジェクトに関連しています。	このルールは、ネットワークオブジェクトに基づいて、同じ宛先 (IPV4、IPV6、mac-addr、または domain-name) と通信しているすべてのインジケーターを識別し、同じ C2 インフラストラクチャに接続されているこれらのインジケーター間の関係を確立します。	リレーションシップを作成
サブドメインに関連するルートドメイン観測事象	このルールは、観測事象のドメインタイプに対してルートドメインとサブドメインを結び付け、その逆も同様にします。	このルールは、ルートドメインとサブドメインを結び付けます。	リレーションシップを作成
DNS 解決に基づく IP への関連ドメイン	このルールでは、ドメイン観測事象の domain-ipv4 または domain-ipv6 の属性を	属性 domain-ipv4 または domain-ipv6 を使用します。このルールは、同じ IP アドレ	リレーションシップを作成

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

相関ルール (続く)

ルール名	ルールの説明	ルール定義	ルールアクション
	使用して、ドメインと IP の間の関係を確立します。	スに解決されるすべてのドメインまたはサブドメインを識別し、インジケーター間の関係を確立し、同じ C2 インフラストラクチャへの接続を示します。	
ドメインと SSL 証明書の照合	このルールは、ドメイン観測事象に関連付けられた SSL 証明書情報を分析し、それらの間の関係を確立します。	このルールは、インジケーターに関連付けられた SSL 証明書情報を分析し、両方の証明書が同じ認証局によって発行され、同じ有効期限を共有していることを特定し、インジケーター間の関係を確立して、同じ C2 インフラストラクチャまたは脅威キャンペーンへの接続を示します。	リレーションシップを作成
一般的な観測事象に基づいてエンティティを関連付ける	このルールは、同じ観測事象が 2 つの異なるエンティティに関連しているかどうかを比較し、それらを相互に関連付けます。	このルールは、同じ観測事象が 2 つの異なるエンティティに関連しているかどうかを比較し、それらが互いに関連しているものとして識別します。	潜在リレーションシップを作成
一般的な観測事象に基づいてインジケーターを関連付ける	このルールは、同じ観測事象が 2 つの異なるインジケーターに関連しているかどうかを比較し、それらを相互に関連付けます。	このルールは、同じ観測事象が 2 つの異なるインジケーターに関連しているかどうかを比較し、それらが互いに関連しているものとして識別します。	潜在リレーションシップを作成
一般的な観測事象に基づいてインジケーターをオブジェクトに関連付ける	このルールは、同じ観測事象がインジケーターやオブジェクトに関連しているかどうかを比較し、それらを相互に関連付けます。	このルールは、同じ観測事象が 2 つの異なるインジケーターとオブジェクトに関連しているかどうかを比較し、それらが互いに関連しているものとして識別します。	潜在リレーションシップを作成

MITRE-ATT&CK™ リポジトリ

MITRE-ATT&CK リポジトリは、MITRE ソースからのデータが取り込まれるインテリジェンスライブラリで利用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リポジトリに送られる MITRE データは、脅威インテリジェンスライブラリデータとは別の MITRE リポジトリに保存されます。MITRE データは、集約または重複排除フローに関与されず、独立しています。

アプリケーション内で利用可能なデータソースは次のとおりです。

1. MITRE - エンタープライズ ATT&CK
2. MITRE - モバイル ATT&CK
3. MITRE - ICS ATT&CK

これらのソースのデータは、ベースシステムの TI ライブラリにある個別の MITRE リポジトリに保存されます。新しい MITRE ソースを作成する場合は、カスタムソースを構成します。詳細については「カスタムフィードの表示」を参照し、フォームビューで [詳細] チェックボックスをオンにして、[プロセッサをレポート] で **[MITRECollectionDataProcessor]** を選択します。

マトリクスを管理する

MITRE TAXII コレクションからインポートされたマトリクスを管理します。マトリクスとは、戦術やテクニックのコレクションです。マトリクスを表示して、自分のコレクションが MITRE-ATT&CK リポジトリで使用可能かどうかを確認できます。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. ベースシステムで利用可能な MITRE ATT&CK 関連のフィードデータソースを有効化したら、[今すぐ実行] をクリックして統合を実行し、MITRE 関連情報をフェッチします。
   統合の有効化に関する詳細
2. MITRE ATT&CK リポジトリデータを表示するには、次の場所に移動します ワークスペース > 脅威インテリジェンスセキュリティセンター > 脅威インテリジェンスライブラリ > **MITRE** の **ATT**&**CK**.
   MITRE ATT&CK 関連のレコードが表示されます。デフォルトでは、すべてのレコードが有効ステータスになっています。

   > **注:**
   > 組織に関連するマトリクスのみを有効化することができます。

3. 特定のレコードを無効にする場合は、マトリクスレコードを選択して [無効化] をクリックします。
4. 一方で、[新規] をクリックし、手動で MITRE ATT&CK マトリクスを作成して、マトリクスレコードを新たに作成することもできます。
5. 必要に応じてフィールドを入力します。

新しい **MITRE** 緩和の作成 **-** 詳細

フィールド	説明
名前	マトリクスの名前を入力します。
ソース	このレコードの作成元である脅威のソースを指定します。
アクティブ	このチェックボックスをオンにして、マトリクスレコードをアクティブ化します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
説明	侵入セットに関する詳細とコンテキストの説明(目的や主要な特性を含む可能性があります)。
インサイト	
メモ	緩和に関連する追加情報。
追加情報	
追加コンテキスト	このオブジェクトタイプにコンテキストを追加します。
コメント	コメントがあれば追加します。

テクニックの管理

MITRE TAXII コレクションからインポートされたテクニックを管理します。テクニックには、攻撃者が特定の戦術を使用するために開発したさまざまな方法が含まれています。組織に関係のないテクニックは、確認して非アクティブ化できます。STIX では、テクニックは攻撃パターンと呼びます。

始める前に

必要なロール：sn_sec_tisc.analyst

テクニックは、攻撃者がアクションを実行して戦術的目標を達成する方法を表します。

手順

1. ベースシステムで利用可能な MITRE ATT&CK 関連のフィードデータソースを有効化したら、[今すぐ実行] をクリックして統合を実行し、MITRE 関連情報をフェッチします。
   統合の有効化に関する詳細
2. MITRE ATT&CK リポジトリデータを表示するには、次の場所に移動します ワークスペース > 脅威インテリジェンスセキュリティセンター > 脅威インテリジェンスライブラリ > **MITRE** の **ATT&CK** > テクニック.
   MITRE ATT&CK テクニックのレコードが表示されます。デフォルトでは、すべてのレコードが有効ステータスになっています。
3. 特定のレコードを無効にする場合は、テクニックレコードを選択して [無効化] をクリックします。
4. 一方で、[新規] をクリックし、手動で MITRE ATT&CK テクニックを作成して、テクニックレコードを新たに作成することもできます。
5. 必要に応じてフィールドを入力します。

新しい **MITRE** 緩和の作成 **-** 詳細

フィールド	説明
ID	テクニックの一意の ID。
名前	テクニックの名前を入力します。
ソース	このレコードの作成元である脅威のソースを指定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
プラットフォーム	必要なプラットフォームを追加します。
必要な権限	必要な権限を追加します。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
説明	侵入セットに関する詳細とコンテキストの説明(目的や主要な特性を含む可能性があります)。
検出	この検出テクニックは、攻撃者によるコンピューターネットワークへのアクセスや不正なアクティビティを識別するために使用されます。
インサイト	
メモ	緩和に関連する追加情報。
追加情報	
追加コンテキスト	このオブジェクトタイプにコンテキストを追加します。
コメント	コメントがあれば追加します。

緩和の管理

MITRE TAXII コレクションからインポートされた緩和を管理します。緩和により、攻撃者が組織に対してテクニックまたはサブテクニックを実行することを防ぐことができます。STIX では、緩和は対処措置として知られています。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. ベースシステムで利用可能な MITRE ATT&CK 関連のフィードデータソースを有効化したら、[今すぐ実行] をクリックして統合を実行し、MITRE 関連情報をフェッチします。
   統合の有効化の詳細については、以下を参照してください。
2. MITRE ATT&CK リポジトリデータを表示するには、次の場所に移動します ワークスペース > 脅威インテリジェンスセキュリティセンター > 脅威インテリジェンスライブラリ > **MITRE** の **ATT**&**CK** > 緩和.
   緩和をクリックして、すべての関連情報を表示します。
3. [新規] をクリックして、MITRE ATT&CK 緩和を手動で作成します。
4. 必要に応じてフィールドを入力します。

新しい **MITRE** ツールの作成 **-** 詳細

フィールド	説明
ID	攻撃を防ぐ対処措置の一意の ID。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。
名前	オブジェクトを識別できるわかりやすい名前を入力します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
エイリアス	このオブジェクトを識別する他の名前のリスト。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
説明	オブジェクトに関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。
貢献者	貢献者を指定します。
インサイト	
メモ	緩和に関連する追加情報。
追加情報	
追加コンテキスト	このオブジェクトにコンテキストを追加します。
コメント	このオブジェクトにコメントを追加します。

5. [保存] をクリックします。

グループを管理

MITRE TAXII コレクションからインポートされたグループを管理します。グループは、セキュリティコミュニティで共通の名前で追跡される、関連する侵入アクティビティのセットです。アナリストは、脅威グループ、アクティビティグループ、攻撃者、侵入セット、キャンペーンなどのさまざまな用語を使用して、アクティビティのクラスターを追跡します。STIX では、グループは侵入セットと呼ばれます。

始める前に

必要なロール：sn_sec_tisc.analyst

手順

1. MITRE ATT&CK リポジトリデータを表示するには、次の場所に移動します ワークスペース > 脅威インテリジェンスセキュリティセンター > 脅威インテリジェンスライブラリ > **MITRE** の **ATT**&**CK** > グループ.
   リストされたグループを表示できます。
2. [新規] をクリックして、MITRE ATT&CK グループを手動で作成します。
3. 必要に応じてフィールドを入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

新しい **MITRE** グループの作成 - 詳細

フィールド	説明
ID	攻撃を防ぐ対処措置の一意の ID。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。
名前	オブジェクトを識別できるわかりやすい名前を入力します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
エイリアス	このオブジェクトを識別する他の名前のリスト。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
説明	オブジェクトに関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。
インサイト	
メモ	緩和に関連する追加情報。
追加情報	
追加コンテキスト	このオブジェクトにコンテキストを追加します。
コメント	このオブジェクトにコメントを追加します。

自動翻訳

4. [保存] をクリックします。
5. これらのオブジェクトがどのように関連しているかを表示するには、[関係] をクリックします。

マルウェアの管理

MITRE TAXII コレクションからインポートしたマルウェア情報を管理します。悪意のあるコードを表す TTP の一種です。

始める前に

これは、システムに密かに挿入されるプログラムを指します。マルウェアの目的は、被害者のデータ、アプリケーション、またはオペレーティングシステム (OS) の機密性、完全性、または可用性を侵害することです。

必要なロール：sn_sec_tisc.analyst

手順

1. MITRE ATT&CK リポジトリデータを表示するには、次の場所に移動します ワークスペース > 脅威インテリジェンスセキュリティセンター > 脅威インテリジェンスライブラリ > **MITRE** の **ATT&CK** > グループ.
   リストされたマルウェアを表示できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. マルウェアをクリックして、すべての関連情報を表示します。
3. [新規 **(New)**] をクリックして、MITRE ATT&CK マルウェアを手動で作成します。
4. 必要に応じてフィールドを入力します。

新しい **MITRE** マルウェアの作成 **-** 詳細

フィールド	説明
ID	攻撃を防ぐ対処措置の一意の ID。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。
名前	オブジェクトを識別できるわかりやすい名前を入力します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
エイリアス	このオブジェクトを識別する他の名前のリスト。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
説明	オブジェクトに関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。
貢献者	貢献者を指定します。
インサイト	
メモ	緩和に関連する追加情報。
追加情報	
追加コンテキスト	このオブジェクトにコンテキストを追加します。
コメント	このオブジェクトにコメントを追加します。

5. [保存] をクリックします。
6. これらのオブジェクトがどのように関連しているかを表示するには、[関係] をクリックします。

ツールの管理

MITRE TAXII コレクションからインポートしたツール情報を管理します。ツールは、攻撃者が攻撃を行うために使用する正当なソフトウェアのことです。

始める前に

必要なロール：sn_sec_tisc.analyst

このタスクについて

ツールを使用すると、攻撃者がツールをいつどのように使用してキャンペーンを実行するかを知ることができます。マルウェアとは異なり、これらのツールまたはソフトウェアパッケージはシステム上

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

で見つかることが多く、パワーユーザー、アドミン、ネットワークアドミニストレーター、または通常のユーザーにとっても正当な目的を持っています。

手順

1. MITRE ATT&CK リポジトリデータを表示するには、次の場所に移動します ワークスペース > 脅威インテリジェンスセキュリティセンター > 脅威インテリジェンスライブラリ > **MITRE** の **ATT&CK** > ツール.
   ツールリストを表示できます。
2. ツールを選択して、すべての関連情報を表示します。
3. [新規] をクリックして、MITRE ATT&CK ツールを手動で作成します。
4. 必要に応じてフィールドを入力します。

新しい **MITRE** ツールの作成 **-** 詳細

フィールド	説明
ID	攻撃を防ぐ対処措置の一意の ID。
取り消し	取り消されたオブジェクトが、オブジェクト作成者によって有効と見なされなくなったことを示します。
名前	オブジェクトを識別できるわかりやすい名前を入力します。
ソース	このオブジェクトレコードの作成元である脅威のソースを指定します。
エイリアス	このオブジェクトを識別する他の名前のリスト。
ソースでの作成時間	ソースでオブジェクトが作成された時刻を指定します。
ソースでの変更時間	ソースでオブジェクトが変更された時刻を指定します。
説明	オブジェクトに関する詳細とコンテキストの説明 (目的や主要な特性を含む可能性があります)。
貢献者	貢献者を指定します。
インサイト	
メモ	緩和に関連する追加情報。
追加情報	
追加コンテキスト	このオブジェクトにコンテキストを追加します。
コメント	このオブジェクトにコメントを追加します。

5. [保存] をクリックします。
6. これらのオブジェクトがどのように関連しているかを表示するには、[関係] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MITRE 関係の管理

MITRE TAXII コレクションからインポートした MITRE 関係の情報を管理します。

始める前に
必要なロール：sn_sec_tisc.analyst

手順

1. MITRE ATT&CK リポジトリデータを表示するには、次の場所に移動します ワークスペース > 脅威インテリジェンスセキュリティセンター > 脅威インテリジェンスライブラリ > **MITRE** の **ATT&CK** > リレーションシップ.
   リスト化された関係を表示できます。
2. 任意のソースオブジェクトをクリックして、関連情報をすべて表示します。
3. [新規] をクリックして、MITRE ATT&CK 関係を手動で作成します。
4. 必要に応じてフィールドを入力します。

新しい **MITRE** ツールの作成 **-** 詳細

フィールド	説明
ソース MITRE オブジェクト	ソース MITRE オブジェクトを追加します。
ターゲット MITRE オブジェクト	ターゲット MITRE オブジェクトを追加します。
ソース MITRE タイプ	ソース MITRE タイプを入力します。
ターゲット MITRE タイプ	ターゲット MITRE タイプを入力します。
関係性タイプ	オブジェクト間の関係を定義します。関係性タイプの詳細とコンテキストの説明。使用可能なオプションは、次のとおりです。 直接か逆の関係の方向を定義します。 ○ 逆：「観測事象 - オブジェクト」の関係タイプです。 ○ 直接：「オブジェクト - 観測事象」の関係タイプです。
ソース	ソースオブジェクトを選択して定義します。
関係 ID	関係 ID を定義します。

5. [保存] をクリックします。
6. これらのオブジェクトがどのように関連しているかを表示するには、[関係] をクリックします。

データの管理と保持

データは、TIDC ライブラリオブジェクトの構造に従って TISC インスタンスに格納および管理され、管理者は組織のニーズに応じて表示および構成することができます。

データのアーカイブや復元は、今後の使用のためにレコードを保護する重要な機能の 1 つとなります。脅威インテリジェンスが有するデータやレコードは膨大な量となります。そこで以下のセクションでは、TISC のアーカイブプロセスやレコード保持を定義および説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データアーカイブプロセス

プラットフォームのアダプションが進むにつれて、テーブル内のデータが急速に増加します。一部のテーブルはさまざまなデータ管理ポリシーを持つベースシステム内にありますが、他のユーザーはそれらを自分で実装する必要があります。

ユーザーがテーブル内のデータを管理する方法は、いくつかの方法があります。

- データを削除する
- データをアーカイブする

> **注:**
> ユーザーがデータを管理する方法をどれも採用しない場合、時間の経過とともに使用量が増加し、データが大幅に大きくなる傾向があり、アプリケーションインスタンスのパフォーマンスとストレージに大きな影響を与えます。

TISC データアーカイブ

脅威インテリジェンスセキュリティセンターは、TISCテーブルのベースシステムでアーカイブルールを使用してプロビジョニングされます。関連レコードは、ベースシステムの TISC アーカイブルールにも追加されます。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > システムアーカイブ > アーカイブルール.
   TISCに適用可能なアーカイブルールのリストが表示されます。これらのアーカイブルールはオブジェクトタイプごとに異なり、個別に適用されます。
2. sn_sec_tiscで始まるテーブル名をフィルタリングします。
3. TISC関連レコードを表示します。

   > **注:**
   >
   > アーカイブルールの作成方法については、「 Create an archive rule 」を参照してください。

4. アーカイブルールを選択します。
   たとえば、[ディレクトリ観測事象レコード] を選択すると、ベースシステムのアーカイブルールが表示されます。
5. 必要に応じてルールを更新します。

TISC関連レコードのアーカイブ

TISCの [アーカイブ関連レコード] 関連リストを使用して、関連レコードをアーカイブルールに追加します。

始める前に
必要なロール：admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > システムアーカイブ > アーカイブルール.
2. 30 日間以上非アクティブなアーカイブルールを選択します。
3. [アーカイブ関連レコード] 関連リストに移動します。

インテリジェンスレコードを削除

脅威インテリジェンスライブラリからレコードを削除します。

始める前に
必要なロール：sn_sec_tisc.admin

手順

1. 次のように移動する。 ワークスペース > 脅威インテリジェンスセキュリティセンター.
2. ワークスペースの [脅威インテリジェンスライブラリ **(Threat Intel Library**)] アイコンをクリックします。
3. レコードを開きます。
4. [ソースレコード] セクションに移動します。
5. ソースレコードを削除するには、[削除] を選択します。
6. ライブラリレコードを削除します。

注:

a. ソースレコードが関連付けられているライブラリレコードが削除されると、ソースレコードが再処理され、ソースレコードのフィールド値を集計して新しいライブラリレコードが作成されます。

b. 脅威インテリジェンスライブラリからデータを完全に削除するには、ライブラリレコードを削除する代わりにアーカイブルールを使用します。詳細については、「観測事象のアーカイブルール」、「オブジェクトのアーカイブルール」、「インジケーターと関連レコードのアーカイブルール」を参照してください。

観測事象のアーカイブルール

ベースシステムでプロビジョニングされた観測事象のアーカイブルールを以下のセクションにリストします。

- メールメッセージ
- SHA256 ハッシュ
- その他の観測事象
- SHA512 ハッシュ
- ファイル
- SHA1 ハッシュ
- メールアドレス
- URL
- AS 番号
- メールの件名
- IPv4 CIDR

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ミューテックス名
- アーティファクト☒
- ユーザーアカウント☒
- Windows レジストリキー
- IPv6 アドレス
- MD5 ハッシュ
- IPv4 アドレス
- ディレクトリ☒
- X.509 証明書
- RSS フィードアーカイブルール☒
- アーカイブルールをインポート☒
- 場所プロセス

観測事象のアーカイブルールの変更

観測事象のアーカイブルールを変更し、ルールの影響を受けるレコードの推定数も表示します。

始める前に
必要なロール：sn_sec_tisc.admin

このタスクについて
デフォルトでは、サンプルアーカイブルールは非アクティブです。

観測事象、インジケーター、関連レコード、およびオブジェクトに対して、[履歴上有意 (Historically Significant)] オプションと条件は常に [False] に設定する必要があります。このオプションを False に設定すると、レコードをアーカイブできますが、このオプションが True に設定されている場合は、ルール定義に関係なくレコードをアーカイブできなくなります。

手順

1. 次のように移動する。 **All** (すべて) > システムアーカイブ > アーカイブルール.
   TISC に適用可能なアーカイブルールのリストが表示されます。これらのアーカイブルールはオブジェクトタイプごとに異なり、個別に適用されます。
2. 任意のアーカイブルールを選択します。
   たとえば、[ディレクトリ観測事象レコード] を選択すると、ベースシステムのアーカイブルールが表示されます。
3. [フィルター条件の追加] をクリックします。
4. [履歴上有意 **(Historically Significant)]** オプションを選択し、条件を **[False]** に設定します。
   このオプションを False に設定すると、レコードをアーカイブできますが、このオプションが True に設定されている場合は、ルール定義に関係なくレコードをアーカイブできなくなります。
5. この例では、観測事象の [ステータス] を [非アクティブ] に設定し、[有効期限] を 2 年に設定します。
   つまり、ステータスが非アクティブで、その観測事象の有効期限が 2 年に設定されている場合、観測事象レコードをアーカイブできるため、現在の日付からその期間より前の期間はすべてアーカイブされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> すべてのアーカイブルールは 1 時間ごとにトリガーされるため、ルールの変更はスケジュール済みジョブの時間から変更されます。ジョブを明示的に実行し、ジョブがスケジュールされるまで待機したくない場合は、それに応じて変更できます。以下の手順に従ってください。

6. 次のように移動する。 関連リンク > 見積りの再計算.

   レコード推定が再計算され、推定値で更新されました。

   > **注:**
   > レコード推定値が 0 の場合、レコードはアーカイブされませんが、レコード推定値が 1 の場合、アプリケーションがその値を識別し、その 1 つのレコードがアーカイブされます。

7. [アーカイブ化を今すぐ実行] を選択します。
8. 以下の [アーカイブ実行] セクションに移動して、アーカイブ実行プロセスを確認します。

   > **注:**
   > レコード推定値も 1 であるため、アーカイブされるレコードの合計数は 1 レコードのみであることがわかります。

9. 次のように移動する。 脅威インテリジェンスライブラリ > 観察事項.
10. アーカイブされたレコードを検索します。
    レコードはアーカイブされている必要があり、レコードを検索しても結果は表示されません。

    > **注:**
    > - TISC アーカイブルールの一環として、アーカイブされた関連レコードの一部としてリストされているすべてのソースとその関連レコードも、集計された観測事象レコードとともにアーカイブされます。[アーカイブログ] セクションにドリルダウンすると、バックグラウンドで自動的に実行され、このセクションに表示されたアーカイブ済みレコードリストを表示できます。
    > - アーカイブ済みレコードを表示する場合は、その関連テーブル内のレコードを検索します。同時に、次の場所に移動して、アーカイブされたレコードを確認することもできます システムアーカイブ > アーカイブログ. アーカイブされたレコードの数が表示されます。

オブジェクトのアーカイブルール

ベースシステムでプロビジョニングされた観測事象のアーカイブルールを以下のセクションにリストします。

デフォルトでは、サンプルアーカイブルールは非アクティブです。

観測事象、インジケーター、関連レコード、およびオブジェクトに対して、[履歴上有意 **(Historically Significant)]** オプションと条件は常に **[False]** に設定する必要があります。このオプションを False に設定すると、レコードをアーカイブできますが、このオプションが True に設定されている場合は、ルール定義に関係なくレコードをアーカイブできなくなります。

- ID のアーカイブ
- データコンポーネントのアーカイブ
- マルウェアのアーカイブ
- オブジェクトのサイティングのアーカイブ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ツールのアーカイブ
- 脅威イベントのアーカイブ
- 攻撃パターンのアーカイブ
- 脅威グループ化のアーカイブ
- 脆弱性のアーカイブ
- インフラストラクチャのアーカイブ
- 脅威メモのアーカイブ
- 対処措置のアーカイブ
- 攻撃者のアーカイブ
- 脅威レポートのアーカイブ
- 侵入セットのアーカイブ
- キャンペーンのアーカイブ
- 観測事象データのアーカイブ
- マーキング定義のアーカイブ
- 脅威に関する意見のアーカイブ
- マルウェア分析のアーカイブ

注:
さまざまなオブジェクトをアーカイブするには、「観測事象アーカイブルール 観測事象のアーカイブルールの変更」で説明されている手順に従います。

インジケーターと関連レコードのアーカイブルール

ベースシステムにプロビジョニングされたインジケーターと関連レコードのアーカイブルールを以下のセクションにリストします。

デフォルトでは、サンプルアーカイブルールは非アクティブです。

観測事象、インジケーター、関連レコード、およびオブジェクトに対して、[履歴上有意 **(Historically Significant)]** オプションと条件は常に **[False]** に設定する必要があります。このオプションを False に設定すると、レコードをアーカイブできますが、このオプションが True に設定されている場合は、ルール定義に関係なくレコードをアーカイブできなくなります。

- インジケーター：インジケーターアーカイブルール
- 関連レコードアーカイブ：
  - 関連する観測事象アーカイブルール
  - オブジェクトとオブジェクトのリレーションシップアーカイブルール
  - オブジェクトとオブジェクトのリレーションシップアーカイブルール
  - 関連するインジケーターオブジェクトアーカイブルール
  - 関連するインジケーターアーカイブルール
  - 関連するインジケーター観測事象アーカイブルール

注:
インジケーターと関連レコードをアーカイブするには、「観測事象アーカイブルール 観測事象のアーカイブルールの変更」で説明されている手順に従います。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連レコードのアーカイブルール

1. 関連レコードの場合、レコードはソースとターゲットのオブジェクトまたは観測事象に基づいてアーカイブされます。
2. [リレーションシップのアーカイブ列を更新 **(Updating Relationship Archived Column)**] スケジュール済みジョブがトリガーされ、1 日に 1 回実行されます。
3. スケジュール済みジョブがトリガーされて実行されると、それに応じて関連レコードの [ソースアーカイブ済み (source archived)] 列と [ターゲットアーカイブ済み (target archived)] 列が更新されます。
4. 関係アーカイブルールは、次回の実行時にトリガーされ、[ソースアーカイブ済み (source archived)] 列と [ターゲットアーカイブ済み (target archived)] 列を持つレコードを識別するときに True に設定され、それらのレコードがアーカイブされます。

アーカイブジョブスケジュール

アーカイブルールが設定され、アクティブなアーカイブルールが存在すると、アーカイブジョブによってこれらのルールが処理され、レコードがアーカイブされます。

アーカイブのスケジュール済みジョブは、1 時間の繰り返し間隔ジョブとして設定されます。スレッドを glide.db.archiver というバックグラウンドスレッドに渡すクラスを呼び出します。

アーカイブプロセスがシステムリソースを消費しすぎないようにするために、以下のアーカイブプロパティを使用して、アーカイブルールが 1 間隔で処理するレコードの数を制御できます。

アーカイブプロパティを変更すると、アーカイブジョブが 1 時間を超えることができ、複数のアーカイブジョブを実行できます。

アーカイブルールのプロパティ

以下はアーカイブルールのプロパティに関する説明となります。

名前	説明	タイプ	整数値
glide.db.archive.batch_size	バッチジョブごとに、アーカイブルールが処理するレコードの数を制御します。	整数	1000 以上
glide.db.archive.sleep_time	各アーカイブルールのバッチジョブが実行される間隔におけるスリープ時間を秒単位で制御します。	整数	1
glide.db.archive.max_iterations	1 時間に実行するバッチジョブの最大数を制御します。	整数	10

アーカイブルールの診断ページ⊠

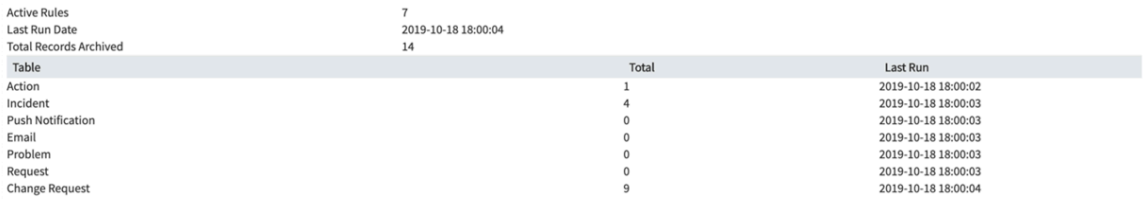
このページでは、アクティブなアーカイブルールの数、アーカイブされた合計レコード数、前回のアーカイブジョブ実行に関する詳細を確認できます。

診断ページへのアクセスリンク：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

https://<your-instance>.service-now.com/ui_page.do?sys_id=71681edc9f3120007aaa207c7f4bcc2b



Active Rules	7
Last Run Date	2019-10-18 18:00:04
Total Records Archived	14

Table	Total	Last Run
Action	1	2019-10-18 18:00:02
Incident	4	2019-10-18 18:00:03
Push Notification	0	2019-10-18 18:00:03
Email	0	2019-10-18 18:00:03
Problem	0	2019-10-18 18:00:03
Request	0	2019-10-18 18:00:03
Change Request	9	2019-10-18 18:00:04

アーカイブ手順

1. アーカイブルール基準を満たす N 個のレコードをロードします (N はバッチサイズのプロパティ)。
2. ar_* テーブルに挿入します。
3. 元のテーブルからレコードを削除します。
4. sys_archive_log エントリーを作成します。

レコードがアーカイブされると、アーカイブログ (sys_archive_log) テーブルにエントリーが作成され、xml のレコードがペイロードとして保存されます。

デバッグ

次の列はデバッグに役立ちます：アーカイブ実行、アーカイブ、復元済み、ID、From テーブル。

1. アーカイブ実行：このレコードをアーカイブした特定のアーカイブ実行に関する詳細情報が確認できます。
2. アーカイブ：条件を満たしたアーカイブルール。
3. 復元済み：レコードが復元されていない場合、このフィールドは空白になります。レコードが復元された場合、復元された日時がこのフィールドに表示されます。
4. **From** テーブル：レコードが削除されたテーブル。

> **重要:**
> アーカイブログエントリーを削除すると、アーカイブされたレコードのデータを復元できなくなります。

アーカイブログにエントリーが存在する場合、その時点でシステムではレコードが以前にアーカイブ済みであること (復元済みかどうか) を識別する必要があります。スキップされた場合、アーカイブエンジンは復元済みのものを再アーカイブしないということになります。

アーカイブルールではアーカイブする関連レコードを指定できるため、関連するレコードと添付ファイルもアーカイブすることができます。元のレコードを復元する場合は、関連レコードも復元する必要があります (アーカイブ後は関連レコードのテーブルが独立するため、自動的に行われません)。

スクリプトから破棄ルールを開始

指定された時間が経過するとアーカイブされたレコードと関連レコードを削除する破棄ルールを作成します。

始める前に
必要なロール：admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて

- new GlideArchiver().archiveDestroyByRule(xxxx); ここでは、xxxx は破棄ルールの sys_id となります。
- アーカイブされたデータに対して実行されている破棄ルールのプロパティを変更する必要がある場合は、「アーカイブルールと破棄ルールのプロパティ」を参照してください。

アーカイブされたレコードの破棄ルールを表示します。

手順

1. 次のように移動する。 **All** (すべて) > システムアーカイブ > アーカイブ破棄ルール.
2. 任意のレコードを選択して破棄ルールを表示します。
   アーカイブ保持期間に基づいて、レコードはアプリケーションから自動的に削除されます。破棄ルールを手動で実行してから [アーカイブ破棄を今すぐ実行] を実行する場合、またはデフォルトのアーカイブ保持を変更する場合は、フォームを適切に編集または変更します。

   注:
   すべてのテーブルに個別の破棄ルールが適用されます。

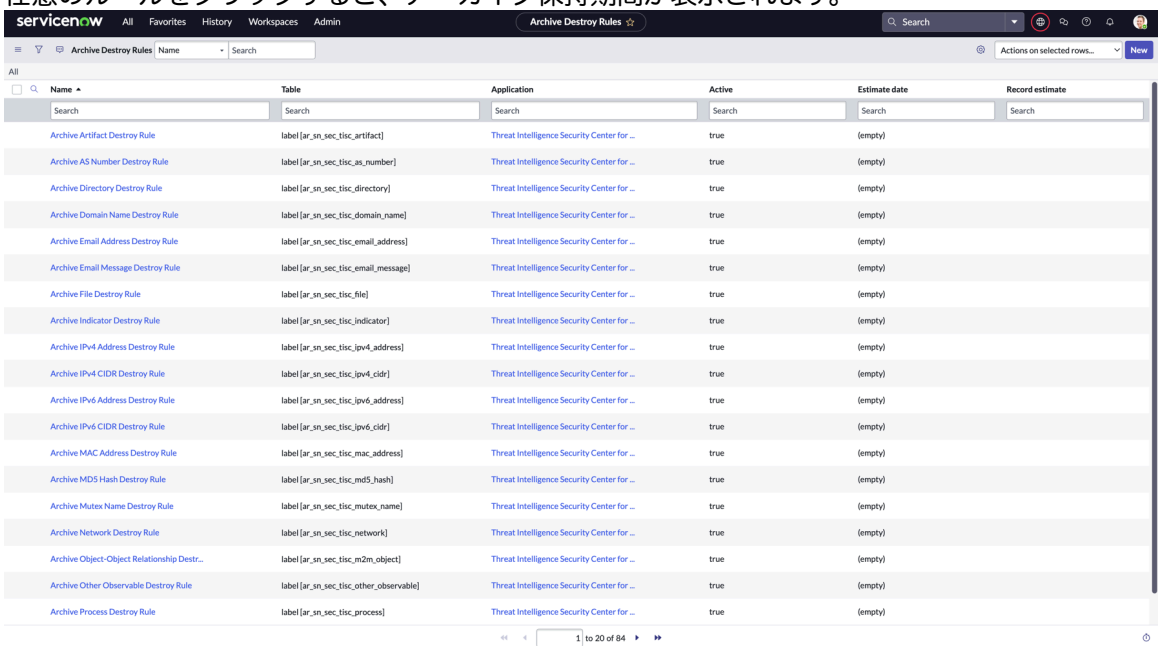
TISC での破棄ルールの表示

ベースシステムでプロビジョニングされた破棄ルールを表示します。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > システムアーカイブ > アーカイブ破棄ルール.
   TISC で適用可能な破棄ルールのリストが表示されます。これらの破棄ルールはオブジェクトタイプごとに異なり、個別に適用されます。
2. TISC で適用可能な破棄ルールを表示します。
3. 任意のルールをクリックすると、アーカイブ保持期間が表示されます。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データアーカイブの制限事項

データを格納するために作成できるアーカイブテーブルのサイズには制限があります。制限は、レコード数ではなく、データのサイズに基づいています。

アーカイブテーブルを作成できなかったというエラーが表示された場合は、このサイズ制限に関連している可能性があります。詳細については、「データアーカイブテーブルのサイズ制限」を参照してください。

アーカイブルールの監視

このセクションは、アーカイブルールを追跡および監視するのに役立ちます。

ルールの説明	移動先	予想される出力
アクティブなアーカイブスレッド	システムアーカイブ > アーカイブステータス	• 名前：glde.db.archiver.xxxx (xxxx は対応するアーカイブルールの sysid) • 値：アクティブまたはアイドルで開始
全体的なアーカイブの進行状況	システムアーカイブ > アーカイブルール	推定列には、まだアーカイブされるレコードの数が表示されます。次の反復の前に 1 時間ごとに更新されます。
個々のアーカイブの進行状況	システムアーカイブ > アーカイブルール	• 所要時間：約 45 分。 • プライマリ合計：実行ごとに 30,000。

学習リソース

以下のセクションでは、データアーカイブのプロセスとベストプラクティスについて詳しく説明します。

参照

参照タイトル	参照リンク
アーカイブされたレコードの複数の関連レコードをバッチモードで復元する方法。	KB0819650
データアーカイブ：概要と FAQ	KB0785300
アーカイブ | Splunk 検索	KB0782324
アーカイブにより孤立した添付ファイルドキュメントレコード	KB0647663
アーカイブジョブアーキテクチャ、アーカイブルールのセットアップ、アーカイブ破棄ルール	
マルチスレッドアーカイブ	KB0821186
アーカイブのベストプラクティス	KB0999731

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

参照 (続く)

参照タイトル	参照リンク
servicenow.com/docs でのデータのアーカイブ	Now Platform 管理
servicenow.com/docs のアーカイブルールと破棄ルールのプロパティ	Now Platform 管理
TOI 記録のアーカイブ	アーカイブ
パフォーマンストレーニングビデオ	KB0960168

TISC データ処理機能フロー

脅威インテリジェンスセキュリティセンター (TISC) では、データの収集や処理を自動化するソリューションを提供し、手動による手順を回避することで脅威インテリジェンスアナリストの負担を軽減します。

脅威インテリジェンスセキュリティセンター (TISC) では、次のいずれかの方法でインテリジェンスを収集します。

1. スケジュールに従って実行される事前構成済みのデータソースからの取り込み。
2. 脅威インテリジェンスアナリストが「インテリジェンスをインポート (Import Intelligence)」機能を使用してデータをインポート。
3. アプリケーション内で個々のレコードを手動で作成。

> **注:**
> アプリケーションで収集されたデータは、脅威インテリジェンスライブラリにロードされる前に、情報の正規化、重複排除、集計の処理が行われます。

データ処理で使用される基本用語

1. ソーステーブル：ソーステーブルには、複数のソースからフェッチされたエンティティに関連するデータが含まれ、各ソースでレコードが作成されます。
2. 集計レコード：集計レコードテーブルには、特定のエンティティに関連するデータが含まれ、特定のエンティティが有するあらゆるソースレコードからのデータが集計されています。

TISC データフロー

1. インテリジェンス / データソースのインポートが正常に実行されると、該当のソーステーブルにレコードが作成されます。
2. データがソーステーブルに取り込まれると、データはフィルターロジックを経て、構成済みの受信フィルタリングルールに基づいてレコードをフィルタリングする必要があるか検証されます。(SourceRecord1 をソースレコードとして説明します)。
3. 構成済みの受信フィルタリングルールによってレコードがフィルタリングされた場合、該当のソースレコード (SourceRecord1) は「フィルタリング済み」としてマークされ、レコードをフィルタリングしたルールは [適用されたフィルタールール] で確認することができます。
4. ソースレコード (SourceRecord1) が AggregateRecord1 に集計されると仮定します。
5. レコードがフィルタリングされていない場合、処理ステータスを [重複排除の準備が完了] に設定すると、レコードに重複排除のマークが付けられます。
6. 重複排除ロジックでは、以下が検証されます。

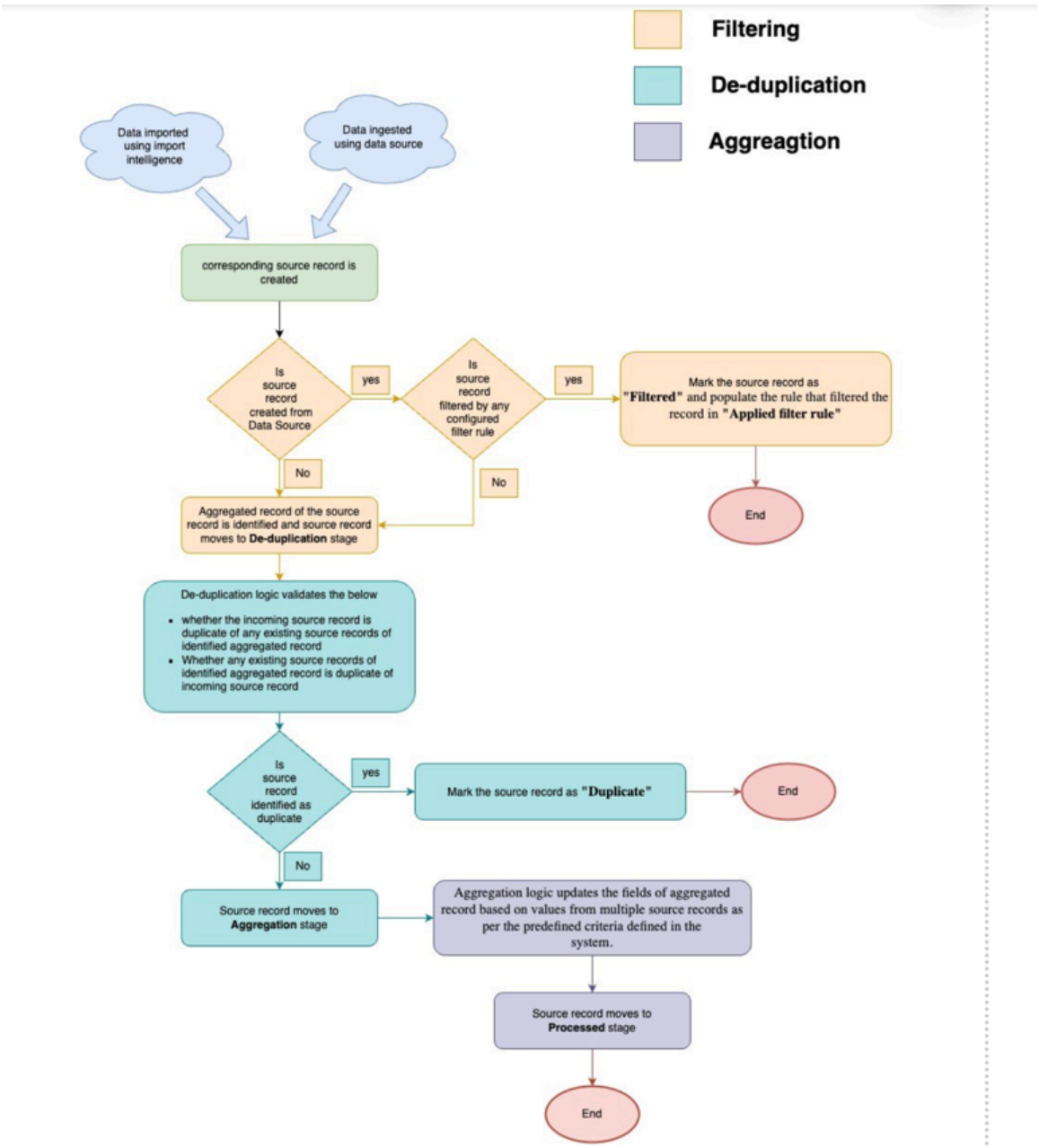
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. 受信ソースレコード (SourceRecord1) が AggregateRecord1 の既存ソースレコードと重複しているか。

b. AggregateRecord1 の既存ソースレコードのいずれかが、受信ソースレコード (SourceRecord1)と重複しています。

7. 各エンティティは、ソースレコードの重複検証に基づく固有のフィールドや関連性を有しています。
8. 受信ソースレコード (SourceRecord1) が AggregateRecord1 の既存ソースレコードと重複している場合、受信ソースレコード (SourceRecord1) は重複としてマークされます。
9. AggregateRecord1 の既存ソースレコード (既存ソース Record1) のいずれかが受信ソースレコード (SourceRecord1) と重複していると識別された場合、処理ステータスを [集計の準備が完了] に設定しておくと、既存ソースレコード (既存ソース Record1) は「重複」としてマークされ、受信ソースレコード (SourceRecord1) は「集計対象」としてマークされます。
10. 集計の一環として、集計レコード「AggregateRecord1」のフィールドは、複数のソースレコードの値に基づいて更新され、システムで定義されている事前定義の基準に従って集計されます。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

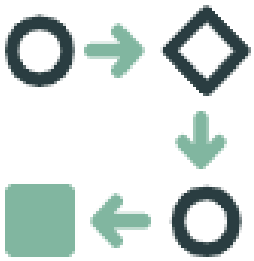
Data Loss Prevention Incident Response

Data Loss Prevention Incident Response (DLP IR) アプリケーションでは、エンドポイントやネットワーク、メール、クラウドといった複数のソースから発生した DLP インシデントの修復ワークフローを確認および管理できます。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

Data Loss Prevention Incident Response

探索	のインストールと構成	管理
		
アナリストとアドミニストレーターが DLP インシデント応答を使用する方法の説明	DLP Incident Response アプリケーションのインストールと構成	Now Platform での DLP インシデントの管理方法に関する管理タスク

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Data Loss Prevention Incident Response (続く)

使用	統合	
DLP エンドユーザーポータル、DLP 運用ポータル 、および DLP ダッシュボードを活用して、インシデントを更新および管理します。	サードパーティのアプリケーションと統合することで DLP の機能を拡張します。	

トラブルシューティングとサポート

- セキュリティオペレーションリソースライブラリ
- セキュリティオペレーションコミュニティ
- 既知のエラーポータルで既知のエラー記事を検索する
- 連絡先 カスタマーサービス & サポート

Data Loss Prevention Incident Response の詳細

Data Loss Prevention Incident Response アプリケーションの解説を読んで、顧客の機密情報 (財務データや独自データ、健康の記録、社会保障番号など) を管理する方法を学習します。

データ損失は、不正な通信の結果として機密情報が企業ネットワークから離れたときに発生します。DLP アプリケーションを使用して、データ損失の経路を特定、対応、および保護できます。

Data Loss Prevention Incident Response アプリケーションには、組織に対して主に次のようなメリットがあります。

- 複数のサードパーティ製 DLP ソリューションと統合して、Now Platform でインシデントを統一的に表示する。
- DLP インシデント管理を簡素化できるように、インシデントを監視してエンドユーザーにアサインする。
- インシデントごとに送信されるカスタマイズ済みのメールテンプレートと通知を通じて、またダイジェストの形式で従業員を指導する。
- 期限切れの DLP インシデントをエンドユーザーからマネージャーにエスカレーションする。
- オープンインシデントのサマリーレポートを、ポリシー、重大度、上位違反者などを基準に表示する。
- DLP インシデントの傾向、誤検出の傾向、および修復の傾向を追跡する。

自動翻訳

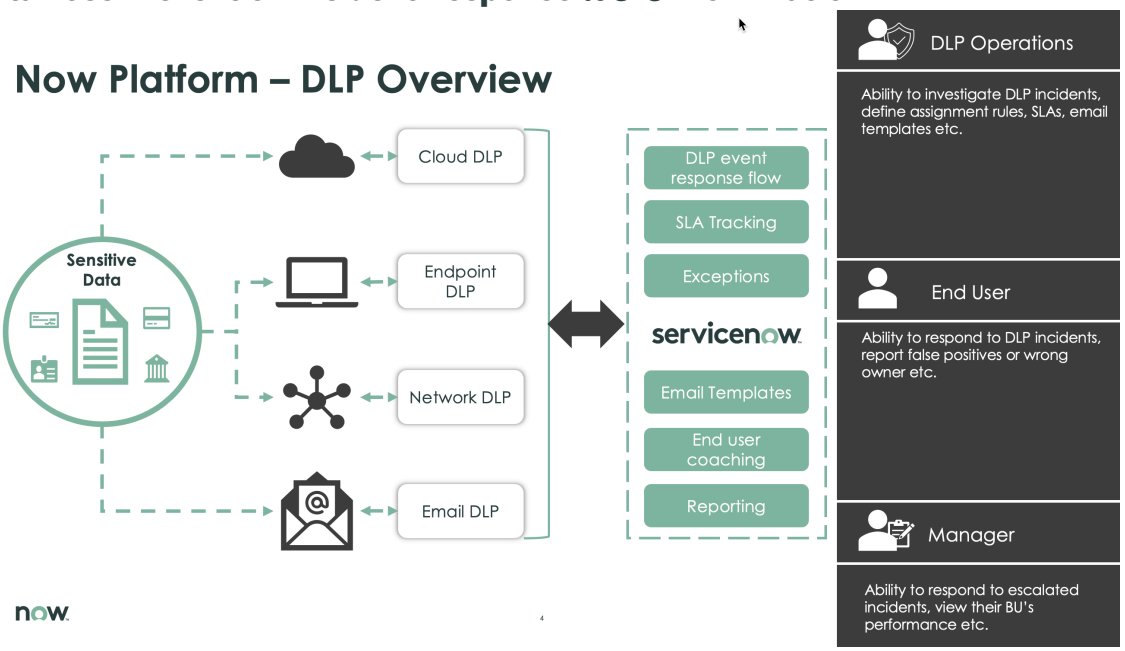
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このセクションを使用して、DLP インシデントの操作に関与する主な機能や各種ロールについて学習します。

DLP インシデント応答の概要

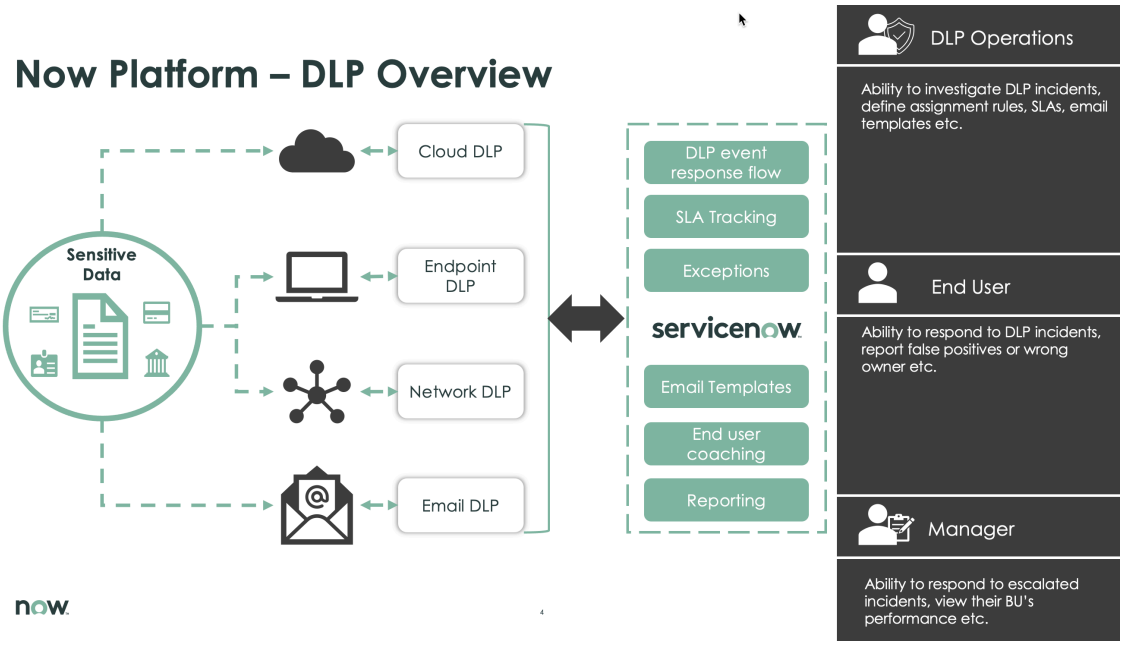
Now Platform および Data Loss Prevention Incident Response (DLP IR) アプリケーションの使用方法について説明します。顧客の機密情報 (財務データや独自データ、健康の記録、社会保障番号など) を管理します。DLP インシデント応答アプリケーションを使用して修復ワークフローを自動化します。

Data Loss Prevention Incident Response および Now Platform



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



1. これはクリック可能な画像です。さまざまなセクションをクリックすると DLP の詳細を確認できます
2. DLP 管理タスク - これはクリック可能な画像です。さまざまなセクションをクリックすると DLP の詳細を確認できます
3. DLP エンドユーザーポータルの使用 - これはクリック可能な画像です。さまざまなセクションをクリックすると DLP の詳細を確認できます
4. DLP 運用ポータルの使用 - これはクリック可能な画像です。さまざまなセクションをクリックすると DLP の詳細を確認できます
5. DLP ダッシュボードの使用 - これはクリック可能な画像です。さまざまなセクションをクリックすると DLP の詳細を確認できます

自動翻訳

Data Loss Prevention Incident Response アプリケーションには、次の機能があります。

- エンドユーザーや従業員が、アサインされた DLP インシデントを確認して応答できるエンドユーザーワークスペース。
- エスカレーションされた DLP インシデントをマネージャーが確認し、適切に処理できるマネージャーワークスペース。
- DLP 運用チームがオープンインシデント、上位違反者、インシデントの傾向をスキャンソース別に追跡し、複数のソース (エンドポイント、ネットワーク、メール) を対象に DLP インシデントを表示、編集、アサイン、クローズできる統合ワークスペース。
- エンドユーザーのコーチングとコミュニケーションのためのメールテンプレート、インシデントの自動アサインのためのアサインルール、自動エスカレーションルール、およびインシデント応答の委任を定義する管理コントロール。

DLP インシデント応答の開始

Data Loss Prevention Incident Response (DLP IR) アプリケーションの設定を開始する前に、次の情報を確認します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト

セットアップタスク	説明
必要な Now Platform ロールと DLP ロールがアサインされていることを確認する。	DLP インシデント応答は、次のロールをサポートしています。 • アドミン (admin) が ServiceNow Store からアプリケーションをインストールし、DLP アドミン (sn_si.admin) にアサインする。 • sn_dlir.admin • sn_dlir.analyst
Data Loss Prevention Incident Response アプリケーションをサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認する。	Data Loss Prevention Incident Response 製品をサポートするには、Data Loss Prevention Incident Response プラグイン (com.snc.data_loss_incident) が必要です。 次の セキュリティオペレーション アプリケーションが、ServiceNow Store からインストールされ、有効化されていることを確認します。インストールされていない場合は、スムーズにインストールできるように、次の順序で一度に 1 つずつアプリケーションをインストールして有効にします。 • Data Loss Prevention Incident Response (com.snc.data_loss_incident) • Security Support Common 統合のための Now Platform インスタンスの設定の詳細については、「Security Operations 製品またはアプリケーションのエンタイトルメントの取得」または「ServiceNow Store アプリケーションのアクティブ化」を参照してください。
ドメインセパレーション	データ、プロセス、および管理タスクを分離する場合は、「ドメインセパレーションと DLP インシデント応答」のトピックを確認してください。

DLP IR インシデント応答のインストールと構成

ServiceNow Store からインスタンスに Data Loss Prevention Incident Response (DLP IR) アプリケーションをダウンロードしてインストールします。

統合のワークフローを呼び出す前に、Now Platform インスタンスで ServiceNow Store から Data Loss Prevention Incident Response アプリケーションをインストールして構成します。

DLP Incident Response アプリケーションのインストールと構成

Now Platform インスタンスで Data Loss Prevention Incident Response (DLP IR) アプリケーションを使用して、機密情報を管理し、修復ワークフローを自動化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
構成手順を完了する前に、 アプリケーションを ServiceNow Store からインスタンスにダウンロードしてインストールする必要があります。

必要なロール：admin および sn_dlir.admin

手順

1. 「ServiceNow Store からのアプリケーションのダウンロード - 」の手順に従います。
2. **DLP** インシデントレスポンスアプリケーションとそのすべての依存関係アプリケーションをダウンロードしたら、 **All** (すべて) > **DLP** 管理 > デフォルト構成 をクリックして、 残りのアプリケーション構成を完了します。

ドメインセパレーションと **DLP** インシデント応答

DLP インシデント応答とドメインセパレーションを併用すると、データ、プロセス、管理タスクをドメインという論理グループに分けることができます。その後、どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル：標準

- ベーシックレベルのサポートのすべての側面が含まれています。
- アプリケーションプロパティは、必要に応じてドメイン対応です。
- ビジネスロジック：サービスプロバイダー (SP) によって顧客ごとにプロセスを作成または変更できます。ユースケースには、単一のインスタンスでの複数のサービスプロバイダー顧客によるアプリケーションの正しい使用が反映されています。
- インスタンスのオーナーは、特定のアプリケーションに期待される通りに、テナントごとに MVP ビジネスロジックとデータパラメーターを設定できる必要があります。

サンプルユースケース：アドミンは、レコードを他のテナントに対してはクローズしないが、1 つのテナントに対してクローズする場合、コメントを必須にすることができる必要があります。

サポートレベルの詳細については、「アプリケーションでのドメインセパレーションのサポート) 」を参照してください。

ドメインセパレーションが **DLP** インシデント応答と連動する仕組み

- 必要な sn_dlir.admin および sn_dlir.analyst ロールを持つユーザーをそれぞれのドメインに作成します。
- 適切なドメインで DLP インシデント応答構成を実行します。

DLP インシデント応答の管理

ルールの設定とアサイン、期日ルールの設定、メールテンプレートの使用、エンドユーザーの応答アクションの設定など、Now Platform で Data Loss Prevention Incident Response (DLP IR) インシデントを管理する作業を行うことができます。

Data Loss Prevention Incident Response アプリケーションでは、次の構成作業を実行できます。

DLP デフォルト構成の設定

Data Loss Prevention Incident Response (DLP IR) インシデントのデフォルト構成設定を定義して、エンドユーザーのインシデント通知とインシデントアサイン設定を識別して設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

このタスクについて
このモジュールを使用して、コアアサインルールと識別子ルールが使い果たされ、条件またはユーザーと一致しない場合のデフォルトの構成設定を定義できます。エンドユーザールックアップルールとアサインルールを定義して、既存のアクティブな DLP インシデントに再適用することもできます。

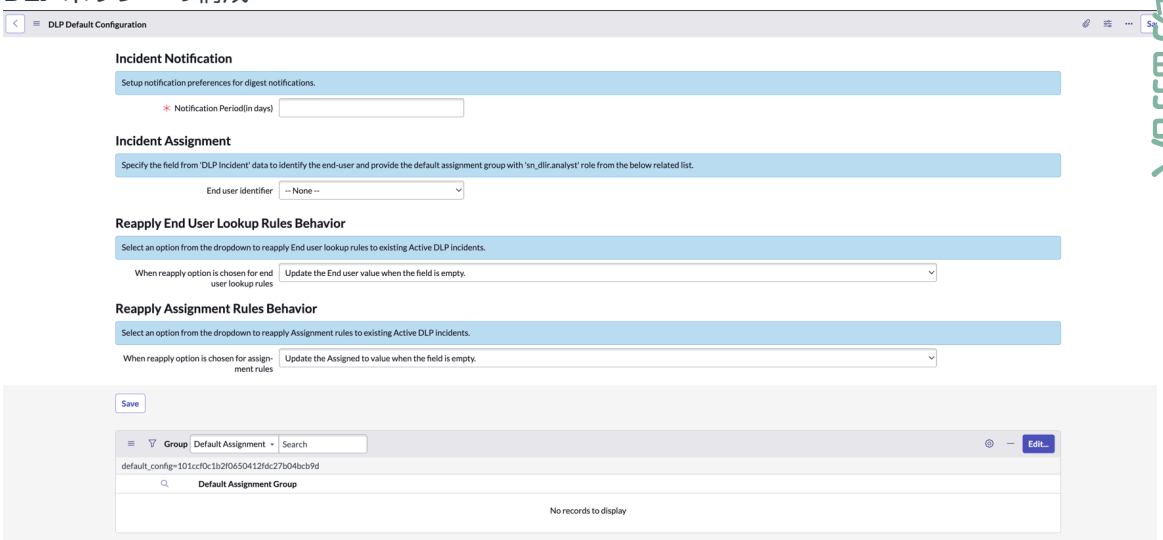
エンドユーザーインシデント通知では、エンドユーザーにメール通知を送信する頻度を指定できます。たとえば、インシデントを蓄積しておき、週に 1 回メールダイジェストを送信するように通知を設定できます。インシデントをアサインすることで、DLP インシデントを最初にアサインするグループを指定できます。DLP 運用チームがエンドユーザーをさらに詳しく識別する方法を指定することもできます。

たとえば、あるユーザーがネットワーク上のファイルにクレジットカード情報を保存しているとします。サードパーティの DLP 統合製品で機密データポリシー違反のインシデントが作成されると、Now Platform DLP が取り込むインシデントデータに、そのエンドユーザーに関する情報が含まれます。それによって、インシデントを適切なエンドユーザーにアサインできるようになります。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > デフォルト構成.

DLP ポリシーの構成



2. フォームのフィールドに入力します。

[DLP デフォルト構成] フォーム

構成名	フィールド	説明
エンドユーザーインシデント通知	通知期間 (日数)	メール通知をエンドユーザーに送信するまでの日数を定義します。日数は 1 ～ 60 日である必要があります。
	クローンされたインシデント/子インシデントに基づいて親ステータ	クローンされたインシデントまたは子インシデントに基づいて親インシデントのステータスを自動的に更新するオプション。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

構成名	フィールド	説明
	スを自動的に更新する (Automatically update parent state based on cloned/child incidents)	
インシデントアサイン	エンドユーザー識別子	エンドユーザーを識別するためにインシデントデータから使用するフィールドを指定します。指定可能な値は次のとおりです。 ○ データ所有者メール ○ 宛先 ○ ファイル作成者 ○ ファイル変更者 ○ ファイルの所有者 ○ **FTP** ユーザー名 ○ 送信者
エンドユーザールックアップルールの動作を再適用する (Reapply End User Lookup Rules Behavior)	エンドユーザールックアップルールで再適用オプションが選択されたとき (When reapply option is chosen for end user lookup rules)	既存のアクティブな DLP インシデントにエンドユーザールックアップルールを再適用するオプション。再適用するには次のいずれかのオプションを選択できます。 ○ [エンドユーザー] フィールドが空の場合にこのフィールドの値を更新 **(Update the End user value when the field is empty)**：[エンドユーザー] フィールドが空の場合に、既存のアクティブな DLP インシデントの [エンドユーザー] の値を更新します。 ○ [エンドユーザー] の値を更新 **(Update the End user value)**：既存のアクティブな DLP インシデントの [エンドユーザー] の値を更新します。 ○ [エンドユーザー] と [アサイン先] の両方が空の場合に、これらのフィールドを更新 **(Update the End user and Assigned to values when both fields are empty)**：既存のアクティブな DLP インシデントの [エンドユーザー] と [アサイン先] の両方が空の場合に、これらのフィールドの値を更新します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

構成名	フィールド	説明
		注: このオプションが選択されている場合、[アサインルール動作を再適用 (Reapply Assignment Rules Behavior)] セクションの [[アサイン先] フィールドが空の場合にこのフィールドの値を更新 **(Update the Assigned to value when the field is empty)]** オプションは自動的に無効になります。これは、この両方のオプションが適用可能になるためです。 ○ すべてのアクティブな **DLP** インシデントの [エンドユーザー] と [アサイン先] の値を更新**(Update the End user and Assigned to values for all the active DLP incidents)**：すべてのアクティブな DLP インシデントの [エンドユーザー] と [アサイン先] の値を更新します。 注: このオプションが選択されている場合、[アサインルール動作を再適用 (Reapply Assignment Rules Behavior)] セクションの [すべてのアクティブな **DLP** インシデントの [アサイン先] の値を更新 **(Update the Assigned to value for all the active DLP incidents)]** オプションは自動的に無効になります。これは、この両方のオプションが適用可能になるためです。
アサインルール動作を再適用 (Reapply Assignment Rules Behavior)	アサインルールで再適用オプションが選択されたとき (When reapply option is chosen for assignment rules)	既存のアクティブな DLP インシデントにアサインルールを再適用するオプション。再適用するには次のいずれかのオプションを選択できます。 ○ [アサイン先] フィールドが空の場合にこのフィールドの値を更新 **(Update the Assigned to value when the field is empty)** ○ すべてのアクティブな **DLP** インシデントの [アサイン先] の値を更新 **(Update the Assigned to value for all the active DLP incidents)**

3. 関連リストのセクションから、すべての DLP インシデントがアサインされている [デフォルトのアサイン先グループ] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ユーザーグループを追加するには、[編集] をクリックします。[関連リスト] セクションから [編集] をクリックし、[コレクション] 列からアイテムを選択してから、選択したアサイニーを [メンバーの編集] ページの [グループ] 列に追加して、リストを保存します。

> **注:**
> 関連リストから表示および選択できるのは、sn_dlir.analyst ロールがアサインされているグループのみです。選択できるグループは 1 つだけです。

4. [保存] をクリックします。

エンドユーザールックアップルールを作成する

エンドユーザールックアップルールを作成して構成し、これらのルールに基づいて DLP インシデントを各エンドユーザーにアサインできます。

始める前に

必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

このタスクについて

DLP アドミニストレーターは、エンドユーザーフィールドのみを使用してエンドユーザーを DLP インシデントに自動的にアサインするように、これらのエンドユーザールックアップルールを定義します。DLP エンドユーザールックアップルールを使用すると、エンドユーザー識別子、カスタム属性、またはスクリプトに基づいて DLP インシデントにエンドユーザーをアサインできます。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > **DLP** エンドユーザールックアップルール.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

[DLP エンドユーザールックアップルール **(DLP End User Lookup Rules)]** フォーム

フィールド	説明
名前	エンドユーザールックアップルールの名前。
アクティブ	エンドユーザールックアップルールがアクティブかどうかを示すオプション。
実行順序	エンドユーザールックアップルールの優先度。このフィールドは、2 つ以上のエンドユーザールックアップルールがトリガー条件を共有する場合にルールが実行される順序を示します。 番号が最も小さいエンドユーザールックアップルールの優先度が最も高くなります。操作の順序を設定するには、値を入力します。たとえば、100、200、300 などです。 デフォルト値は 100 です。
説明	エンドユーザールックアップルールの一意の説明。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
条件	条件ビルダーの条件。ここの条件は DLP インシデントテーブルに基づいて決まります。エンドユーザールックアップルールの条件を作成するには、いずれかのインシデントフィールドを選択します。 条件ビルダーのリストとフィールドを使用して、最初の行のフィルターを設定します。 条件を追加するには、**[AND]** または **[OR]** をクリックします。 ○ [**AND**] を選択した場合は、すべての条件に一致する必要があります。 ○ **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。 2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。 たとえば、このエンドユーザールックアップルールの条件を設定するには、条件として [統合ソース]、[次の値を含む]、**[Symantec]** を選択します。 **注:** 条件ビルダーの条件では大文字と小文字が区別されます。
エンドユーザーのルックアップに使用するアイテム (Lookup end user by using)	[インシデントフィールド] または [スクリプト] を使用してエンドユーザーをルックアップするオプション。
エンドユーザー識別子	DLP インシデントのエンドユーザー識別子。このフィールドは、[エンドユーザーのルックアップに使用するアイテム **(Lookup end user by using)]** フィールドで [インシデントフィールド] が選択されている場合にのみ表示されます。次からエンドユーザー識別子を選択できます。 ○ データ所有者メール ○ 宛先 ○ ファイル作成者 ○ ファイル変更者 ○ ファイルの所有者 ○ **FTP** ユーザー名 ○ 送信者

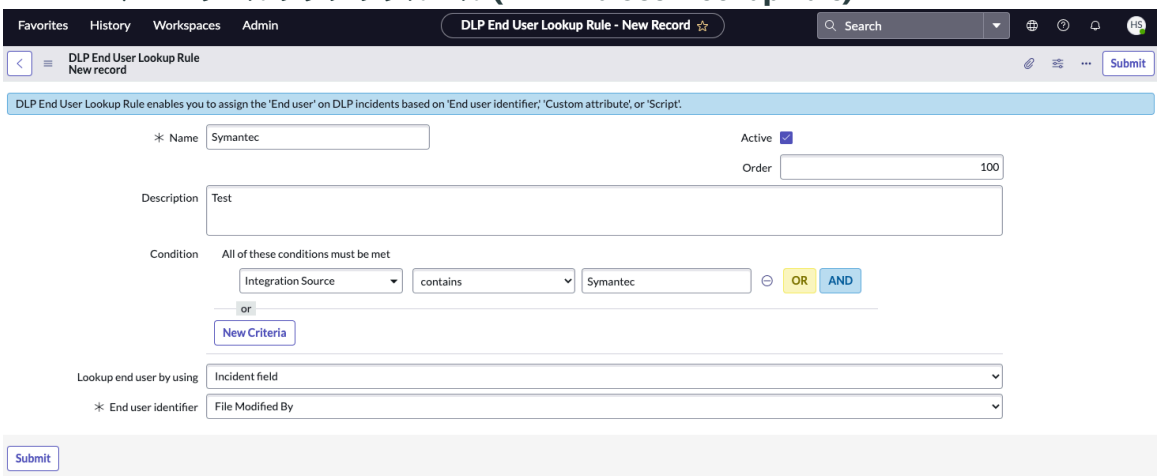
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: 上記のエンドユーザー識別子は、システムプロパティ sn_dlir.assignment.fields を使用して構成できます。詳細については、「詳細設定を構成します」を参照してください。 ○ インシデントからのカスタムユーザー
カスタム属性	ユーザーへの参照があるインシデントからカスタム属性を指定するオプション。このフィールドは、[エンドユーザー識別子] フィールドで **[a]** が選択されている場合にのみ表示されます。
スクリプト	スクリプトエディターを使用して、エンドユーザールックアップルールの作成時にフィールド値をカスタマイズおよび書式設定することができます。たとえば、メールアドレスフィールドを使用してエンドユーザーを識別することができます。

Example
次の例は、「Symantec」という名前のエンドユーザールックアップルールを示しています。条件ビルダーでは、[統合ソース] を [Symantec] にする必要があります。[エンドユーザーのルックアップに使用するアイテム **(Lookup end user by using)]** オプションが [インシデントフィールド] に設定され、[エンドユーザー識別子] オプションが [ファイル変更者] に設定されています。

DLP エンドユーザールックアップルール **(DLP End User Lookup Rule)**



4. [送信] をクリックします。
   1 つ以上のエンドユーザールックアップルールを選択し、既存のすべての DLP インシデントに再適用するオプションもあります。
5. 既存のすべての DLP インシデントにエンドユーザールックアップルールを再適用するには、[再適用 **(Reapply)]** をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アサインルールを作成する

このセクションを使用して、アサインルールを作成します。その後、Data Loss Prevention Incident Response (DLP IR) インシデントをユーザーグループ、エンドユーザー、マネージャー、またはインシデントからのユーザーにアサインします。

始める前に

必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

このタスクについて

アサインルールを使用して、DLP IR インシデントをユーザーグループ、エンドユーザー、またはマネージャーにアサインできます。DLP インシデントのアサインは、アサインルールの条件が満たされたときに発生します。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > アサインルール.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

[DLP アサインルール] フォーム

フィールド	説明
名前	アサインルールの名前。
アクティブ	アサインルールがアクティブかどうかを示すオプション。
実行順序	アサインルールの優先度。このフィールドは、2 つ以上のルールがトリガー条件を共有する場合にアサインルールが実行される順序を示します。 番号が最も小さいアサインルールの優先度が最も高くなります。操作の順序を設定するには、値を入力します。たとえば、100、200、300 などです。 デフォルト値は 100 です。
説明	このアサインルールの固有の説明。
条件	条件ビルダーの条件。ここの条件は DLP インシデントテーブルに基づいて決まります。アサインルールの条件を作成するには、いずれかのインシデントフィールドを選択します。 条件ビルダーのリストとフィールドを使用して、最初の行のフィルターを設定します。 条件を追加するには、**[AND]** または **[OR]** をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ [**AND**] を選択した場合は、すべての条件に一致する必要があります。 ○ **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。 2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。 たとえば、あるエンドポイントの DLP アサインルールを作成するとします。その際に、インシデントをアサインするために満たす必要があるエンドポイントファイルシステムがその条件スキャンソースであることを指定できます。 **注:** 条件ビルダーの条件では大文字と小文字が区別されます。
アサイン先	次のいずれかにアサインします。 ○ ユーザーグループ ○ エンドユーザー ○ マネージャー ○ インシデントからのユーザー 条件ビルダー内の条件が満たされると、アサインされます。
ユーザーグループ	DLP インシデントのアサイン先のユーザーグループを検索して選択するオプション。このフィールドは、[アサイン先] フィールドで [ユーザーグループ] が選択されている場合にのみ表示されます。 **注:** 表示および選択できるのは、sn_dlir.analyst ロールがアサインされているグループのみです。
エンドユーザー	DLP インシデントをエンドユーザーにアサインするオプション。条件ビルダー内の条件が満たされると、アサインされます。
マネージャーフィールドを使用してアサイン	エンドユーザーのマネージャー。このフィールドは、[アサイン先] フィールドで [マネージャー] が選択されている場合にのみ表示されます。 [マネージャー] のフィールド ([姓]、[メール]、[市区町村]、[従業員番号] などの) を 1 つ選択することで、DLP インシデントを特定のマネージャーにアサインできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

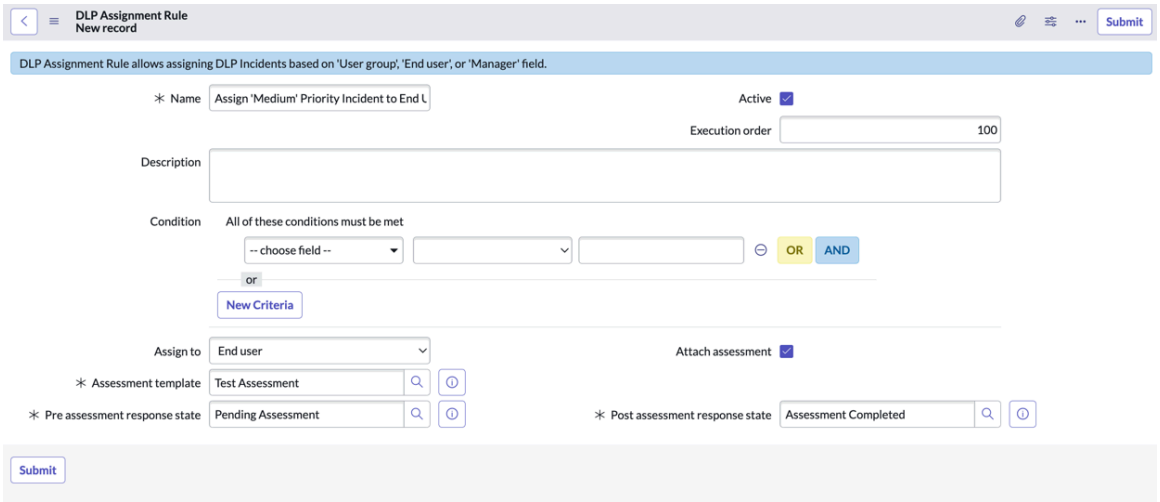
フィールド	説明
ユーザー識別子 (User Identifier)	インシデントのユーザー識別子。このフィールドは、[アサイン先] フィールドで [インシデントからのユーザー **(User from Incident)]** が選択されている場合にのみ表示されます。次のいずれかのユーザー識別子を選択できます。 ○ データ所有者メール ○ 宛先 ○ ファイル作成者 ○ ファイル変更者 ○ ファイルの所有者 ○ **FTP** ユーザー名 ○ 送信者 ○ インシデントからのカスタムユーザー
カスタム属性	ユーザーへの参照があるインシデントからカスタム属性を指定するオプション。このフィールドは、[ユーザー識別子 **(User Identifier)]** フィールドで [インシデントからのカスタムユーザー] が選択されている場合にのみ表示されます。
アセスメントの添付	インシデントにアセスメントを添付するかどうかを指定するオプション。
アセスメント前の応答ステータス (Pre assessment response state)	エンドユーザーが応答する前のインシデントのステータスを選択するオプション。カスタム状況に設定することもできます。 デフォルト値は [アセスメント待ち] です。
アセスメント後の応答ステータス (Post assessment response state)	ユーザーの応答後の DLP インシデントのステータスを選択するオプション。 デフォルト値は [アセスメントが完了しました] です。
詳細	エンドユーザーを識別するための詳細オプション。このフィールドは、[ユーザー識別子 **(User Identifier)]** フィールドで [インシデントからのカスタムユーザー] が選択されている場合にのみ表示されます。 スクリプトエディターを使用して、アサインルールの作成時にエンドユーザーを識別するためのフィールド値をカスタマイズおよび書式設定することができます。次に、DLP インシデントをアサインするユーザー (エンドユーザーまたはエンドユーザーのマネージャー) を選択します。 たとえば、メールアドレスフィールドを使用してエンドユーザーを識別することができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Example
次の例は、「Assign 'Medium' Priority Incident to End User」という名前のアサインルールを示しています。条件ビルダーでは、[スキャンソース] を「Assign 'Medium' Priority Incident to End User」に設定し、[アサイン先] フィールドを [エンドユーザー] に設定する必要があります。次に、エンドユーザーの「メール」を検索できます。

DLP アサインルール



4. すべての DLP インシデントがアサインされている関連リストセクションから [アサイン先] フィールドを選択します。
ユーザーグループを追加するには、[編集] をクリックします。[関連リスト] セクションから [編集 **]** をクリックし、[コレクション] 列からアイテムを選択してから、選択したアサイニーを [メンバーの編集] ページの [グループ] 列に追加して、リストを保存します。

   注:
   関連リストから表示および選択できるのは、sn_dlir.analyst ロールがアサインされているグループのみです。選択できるグループは 1 つだけです。

5. [送信] をクリックします。
1 つ以上のアサインルールを選択し、既存のすべての DLP インシデントに再適用するオプションもあります。
6. 既存のすべての DLP インシデントにアサインルールを再適用するには、[再適用] をクリックします。

インシデント統合ルールを作成する

インシデント統合ルールを作成して、類似した性質の複数のインシデントを 1 つの親インシデントの下に統合します。

始める前に
必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)

このタスクについて
DLP アドミニストレーターは、同じ性質の DLP インシデントを 1 つの親インシデントの下に自動的に統合するように、これらのインシデント統合ルールを定義します。DLP インシデント

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統合ルールを使用すると、[統合期間 (Consolidation duration)] と [統合識別 (Consolidation identification)] に指定された構成に基づいて DLP インシデントを統合できます。

注:

統合インシデントが作成されると、親 DLP インシデントの子になります。統合インシデントの重大度が親インシデントの重大度よりも高い場合、親インシデントの重大度は子インシデントと一致するように更新されます。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > **DLP** インシデント統合ルール.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

[DLP アサインルール] フォーム

フィールド	説明
名前	インシデント統合ルールの名前。
アクティブ	インシデント統合ルールがアクティブかどうかを示すオプション。
実行順序	インシデント統合ルールの優先度。このフィールドは、2 つ以上のルールがトリガー条件を共有する場合にインシデント統合が実行される順序を示します。 番号が最も小さいインシデント統合ルールの優先度が最も高くなります。操作の順序を設定するには、値を入力します。たとえば、100、200、300 などです。 デフォルト値は 100 です。
説明	インシデント統合ルールの一意の説明。
条件	条件ビルダーの条件。ここの条件は DLP インシデントテーブルに基づいて決まります。インシデント統合ルールの条件を作成するには、いずれかのインシデントフィールドを選択します。 条件ビルダーのリストとフィールドを使用して、最初の行のフィルターを設定します。 条件を追加するには、**[AND]** または **[OR]** をクリックします。 ○ [**AND**] を選択した場合は、すべての条件に一致する必要があります。 ○ **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。 2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	たとえば、このインシデント統合ルールの条件を設定するには、条件として [統合ソース]、[次の値を含む]、**[Symantec]** を選択します。 **注:** 条件ビルダーの条件では大文字と小文字が区別されます。
統合期間 (Consolidation duration)	インシデント統合の期間を設定するオプション。 この期間のインシデントのうち、選択したフィールドの値が同じであるインシデントが、最初のインシデントの下に統合されます。このルールに一致する最初のインシデントが親インシデントになり、残りのインシデントが子インシデントになります。
インシデントの統合基準フィールド (Consolidate incidents by)	DLP インシデントフィールドを選択します。選択したフィールドに同じ値が含まれているインシデントが統合されます。 少なくとも 1 つのフィールドを選択してください。少なくとも 1 つのフィールドを選択してください。

次の例は、「Consolidate incidents for Symantec Integration」という名前のインシデント統合ルールを示しています。条件ビルダーでは、[統合ソース] を [Symantec] にする必要があります。[統合期間 **(Consolidation duration)]** オプションが 1 時間に設定され、[インシデントの統合基準フィールド **(Consolidate incidents by)]** で [ポリシー名] オプションが選択されています。

Symantec DLP インシデントの取り込み時にこのルールが実行され、複数のインシデントのポリシー名が同一である場合に、最初にこのルールに一致したインシデントの下に、それ以降のインシデントが統合されます。

4. [送信] をクリックします。
   統合ルールに基づいて統合されたインシデントは、DLP アナリストワークスペースの [子インシデント] リストで使用可能になります。

応答期日ルールの作成

応答期日ルールを設定して、アサインされた Data Loss Prevention Incident Response (DLP IR) インシデントに対してエンドユーザーに応答してもらいたい時間を決定します。

始める前に

必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

このタスクについて

このモジュールを使用して、さまざまなタイプの DLP インシデントの応答期日ルールと、期日のカウントを開始するルールを定義できます。期日が経過すると、ユーザーは期限切れのインシデントに

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ついて通知されます。期限切れのインシデントを次のいずれかにエスカレートするオプションもあります。

- マネージャー
- インシデントからのカスタムユーザー
- ユーザーグループ

たとえば、期限切れのインシデントをマネージャーにエスカレートし、最大 3 つのレベルのエスカレーションを指定した場合です。第 1 レベルのマネージャーが最初に通知されます。インシデントが再び期限切れになった場合は、第 2 レベルのマネージャーに通知され、インシデントが引き続き期限切れの場合は第 3 レベルのマネージャーに通知されます。マネージャーに代理人がいる場合、マネージャーはエスカレーションまたは期限切れのインシデントを代理人にアサインすることができます。

複数の応答期日ルールを作成することもできます

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > 応答期日ルール.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

[応答期日ルール] フォーム

フィールド	説明
名前	応答期日ルールの名前。
アクティブ	応答期日ルールがアクティブかどうかを示すオプション。
期限 (日数)	期限の日数。
期日がカウントされた起点	期日の計算に使用する開始日。期日は、ユーザーがインシデントについて最初に通知を受けた日、またはインシデントのアサイン日から計算できます。
期日前に通知	期日前に DLP インシデントについてエンドユーザーに通知するオプション。
通知日 (期日までの日数)	ルールによってエンドユーザーへの通知がトリガーされる日から期日までの日数。
説明	この応答期日ルールの固有の説明。
条件	条件ビルダーの条件。ここの条件は DLP インシデントテーブルに基づいて決まります。応答期日ルールの条件を作成するには、いずれかのインシデントフィールドを選択します。 条件ビルダーのリストとフィールドを使用して、最初の行のフィルターを設定します。 条件を追加するには、**[AND]** または **[OR]** をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ [**AND**] を選択した場合は、すべての条件に一致する必要があります。 ○ **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。 2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。 **注:** 条件ビルダーの条件では大文字と小文字が区別されます。
エスカレート	応答期日を過ぎた場合に DLP インシデントを誰かにエスカレーションするオプション。詳細については、「DLP インシデントにアクセスする複数ユーザーの追加」を参照してください。
期限切れインシデントのエスカレーション先	インシデントをマネージャー、カスタムユーザー、ユーザーグループのうちの誰にエスカレーションするかを指定するオプション。 このフィールドは、[エスカレーション] オプションが有効になっている場合にのみ表示されます。
次を使用してアサイン	マネージャーの識別方法を指定します。 このフィールドは、[期限切れインシデントのエスカレーション先] フィールドで [マネージャー] が選択されている場合にのみ表示されます。
最大エスカレーションレベル	マネージャーおよびカスタムユーザーが設定できるエスカレーションレベルの最大数を定義するオプション。 マネージャーまたはカスタムユーザーは、任意の数のエスカレーションレベルを定義できます。デフォルトでは、3 つのレベルのエスカレーションが提供されています。 ○ マネージャーは、このフィールドの値を更新することで、任意の数のエスカレーションレベルを定義できます。 ○ カスタムユーザーは、[+] アイコンを使用して、任意の数のエスカレーションレベルを定義できます。
カスタム属性	ユーザーへの参照があるインシデントからカスタム属性を指定するオプション。 このフィールドは、[期限切れインシデントのエスカレーション先] フィールドで [インシデ

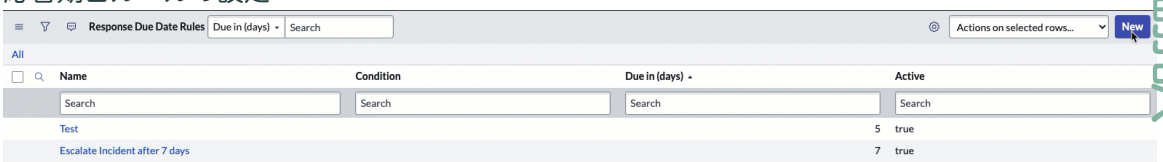
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	ントからのカスタムユーザー] が選択されている場合にのみ表示されます。
ユーザーグループ	DLP インシデントのエスカレーション先のユーザーグループを検索して選択するオプション。 このフィールドは、[期限切れインシデントのエスカレーション先] フィールドで [ユーザーグループ] が選択されている場合にのみ表示されます。 **注:** 表示および選択できるのは、sn_dlir.analyst ロールがアサインされているグループのみです。

Example
次の例では、アサインされた Data Loss Prevention Incident Response (DLP) インシデントに対してエンドユーザーに応答してもらいたい時間を決定する応答期日を示します。エンドユーザーへの最初の通知後の応答期日は 2 日後です。条件ビルダーでは、応答期日の作成を続行するには、スキャンソースがエンドポイントファイルシステムと一致する必要があることが示されています。エスカレーションのオプションが選択されています。応答期日を過ぎると、インシデントがマネージャーにエスカレーションされます。

応答期日ルールの設定



4. [送信] をクリックします。

DLP インシデントにアクセスする複数ユーザーの追加

エスカレーションチェーン機能を使用して、DLP インシデントが別のユーザーにアサインされている場合でも、その DLP インシデントに関与するすべてのユーザーがリストビューからその DLP インシデントにアクセスできるようにします。

始める前に
必要なロール：

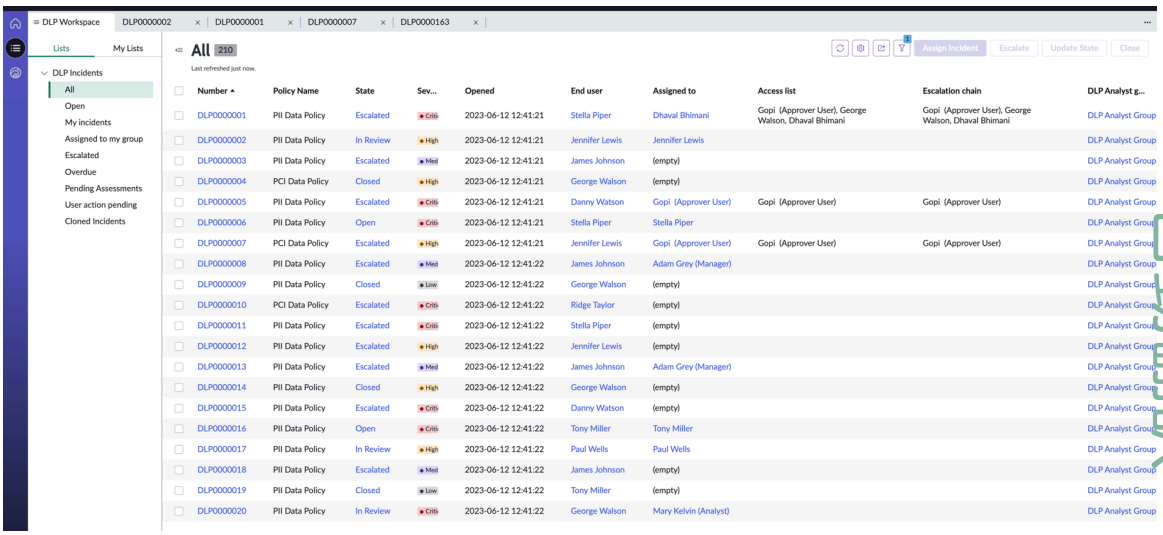
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.read、sn_dlir.analyst、および sn_dlir.analyst_read - 表示 (読み取り専用)。

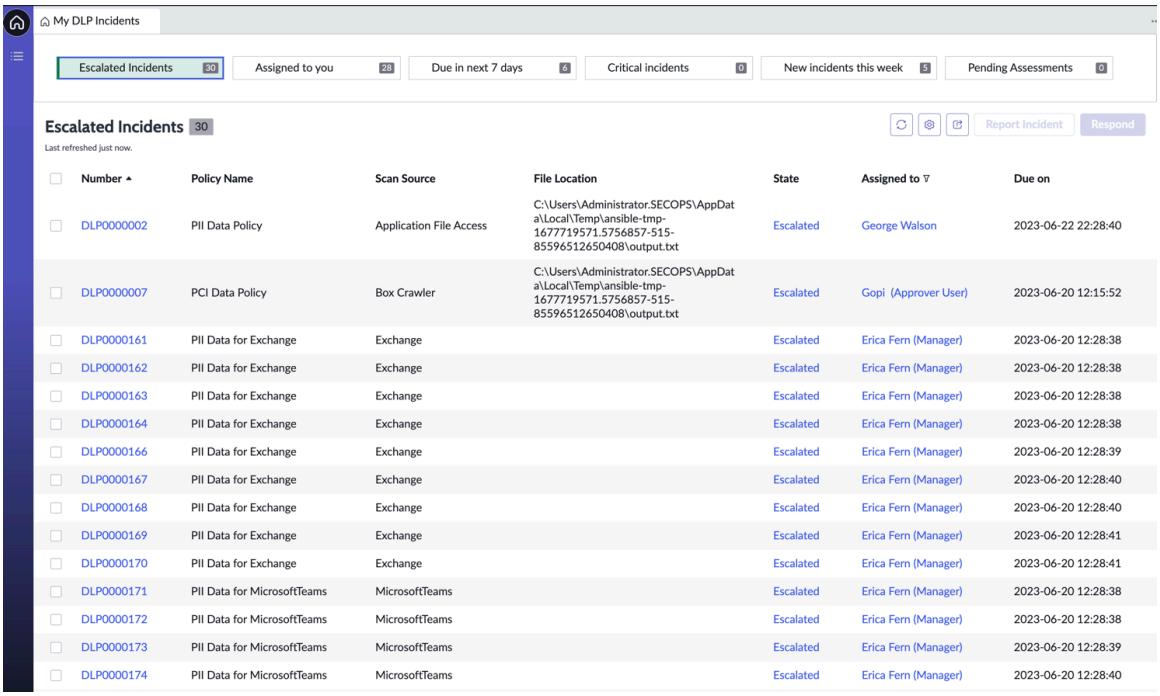
手順

1. 次のように移動する。 **DLP** > **DLP** アナリストワークスペース.
   リストビューでは、ユーザーとその代理人が、エンドユーザーポータルの [エスカレーション済み] インデントタブで DLP インシデントを表示できる必要があります。
2. 任意のインシデントを開きます。
3. [エスカレート] ボタンをクリックして、インシデントをエスカレートします。
4. ドロップダウンリストからユーザーまたはユーザーグループを選択します。
   複数のユーザーをエスカレーションチェーンに追加できます。アクセス権を持つすべてのユーザーは、フォームビューの [詳細] セクションと [すべて] インシデントタブに一覧表示されます。エスカレーションチェーンは、構成設定に基づいて表示されます。詳細については、「詳細設定を構成します」を参照してください。



5. [送信] をクリックします。
   送信後、インシデントはマネージャーにアサインされますが、エンドユーザーは引き続きインシデントを表示できます。
6. これを確認するには、エンドユーザーとして **[DLP** ユーザーワークスペース **(DLP User Workspace)]** に移動します。
   エンドユーザーにアサインされているすべてのインシデントが表示されます。
7. [エスカレートされたインシデント **(Escalated Incidents)]** セクションで、エスカレートされたインシデントのリストを確認します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



リストビューの [エスカレーションチェーン **(Escalation Chain)]** 列で、ユーザーアクセスリストを確認することもできます。

8. 任意のインシデントを開きます。
9. [応答] ボタンをクリックして、インシデント応答を送信します。
10. ドロップダウンリストから応答を選択します。
11. [送信] をクリックします。

承認ルールを作成する

詳細タイプの応答オプションが選択されるたびに、さまざまなレベルの承認者ユーザーから承認を得るための承認ルールを作成します。

始める前に

必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

このタスクについて

DLP アドミニストレーターは、詳細タイプの応答オプションの承認のためにエンドユーザーが提出した要求に同意するように、これらの承認ルールを定義します。DLP アドミニストレーターは、ここから複数レベルの承認を定義することもできます。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > **DLP** 承認ルール.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[DLP アサインルール] フォーム

フィールド	説明
名前	承認ルールの名前。
アクティブ	承認ルールがアクティブかどうかを示すオプション。
実行順序	承認ルールの優先度。このフィールドは、2 つ以上のルールがトリガー条件を共有する場合に承認ルールが実行される順序を示します。 番号が最も小さい承認ルールの優先度が最も高くなります。操作の順序を設定するには、値を入力します。たとえば、100、200、300 などです。 デフォルト値は 100 です。
説明	承認ルールの一意の説明。
条件	条件ビルダーの条件。ここの条件は DLP インシデントテーブルに基づいて決まります。承認ルールの条件を作成するには、いずれかのインシデントフィールドを選択します。 条件ビルダーのリストとフィールドを使用して、最初の行のフィルターを設定します。 条件を追加するには、**[AND]** または **[OR]** をクリックします。 ○ [**AND**] を選択した場合は、すべての条件に一致する必要があります。 ○ **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。 2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。 たとえば、このインシデント統合ルールの条件を設定するには、条件として [統合ソース]、[次の値を含む]、**[Microsoft]** を選択します。
応答オプションに適用可能 (Applicable for response options)	詳細タイプの応答オプションを選択するオプション。 複数の応答オプションを選択できます。
承認者	設定する承認者ユーザーのタイプを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ ユーザーテーブル：ユーザー (sys_user) テーブルから承認者ユーザーを選択する場合は、このオプションを選択します。 ○ カスタム承認リスト **(Custom Approval List)**：1 つの要求に対してカスタム承認者の複数レベルを構成する場合は、このオプションを選択します。
承認者識別 (Approver identifier)	このフィールドは、[承認者] オプションで [ユーザーテーブル] が選択されている場合に表示されます。 ユーザー (sys_user) テーブルからの承認者を識別するフィールドを選択します。
レベル数	このフィールドは、[承認者] オプションで [ユーザーテーブル] が選択されている場合に表示されます。 このフィールドには、承認レベルを定義する数値を入力します。 たとえば、[レベル数] フィールドに 3 が追加され、[承認者識別 (Approver identifier)] フィールドで [マネージャー] が選択されている場合、承認要求は 3 レベルの承認に移ります。

次の例は、1 つの詳細応答オプションに対して作成された承認ルールを示しています。条件では、この構成をトリガーする Microsoft キーワードが統合ソース名に含まれている必要があることが指定されています。

4. [承認者] オプションで **[** カスタム承認リスト **(Custom Approval List)]** を選択します。
5. [送信] をクリックします。
6. フォームビューで [承認レベル] 関連リストが入力されます。
7. [承認レベル] セクションで [新規] をクリックします。
8. フォームのフィールドに入力します。

承認レベルフォーム

フィールド	説明
名前	承認レベルの名前。
アクティブ	承認レベルがアクティブかどうかを示すオプション。
level	承認ルールのレベル。このフィールドは、2 つ以上の承認レベルが構成されている場合の承認レベルの実行順序を示します。 番号が最も小さい承認レベルの優先度が最も高くなります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	操作のレベルを設定するには、値を入力します。たとえば、100、200、300 などです。 デフォルト値は 100 です。
承認ルール	この構成を定義する対象の承認ルール。 これは読み込み専用フィールドです。
説明	承認ルールの一意の説明。
承認が必要 (Approvals required)	構成されているすべてのユーザー/グループからの承認が必要か、または任意の 1 人のユーザーからの承認のみが必要かを定義するオプションを選択します。
承認者	承認者を選択するオプション。 **a.** ユーザーとグループ： **i.** ユーザー： アイコンをクリックして、リストから特定のユーザーを追加します。メールアドレスまたは検索オプションを使用してユーザーを追加することもできます。 DLP 条件を適用できるユーザーとして自分自身を追加するには、 をクリックします。 **ii.** グループ：<add_icon> アイコンをクリックして、リストから特定のグループを追加します。検索オプションを使用してグループを追加することもできます。 **b.** スクリプトを使用して検索 **(Find by using script)**：スクリプトエディターを使用して、承認レベルの作成時にフィールド値をカスタマイズおよび書式設定することができます。たとえば、メールアドレスフィールドを使用して承認者ユーザーを識別できます。

9. [送信] をクリックします。

ユーザー指示テンプレートを作成する

DLP インシデントのユーザー指示テンプレートを作成および管理して、ユーザーがインシデント解決と解決プロセスの次のステップに関連する指示を理解できるようにします。

始める前に

ユーザー指示カードテンプレートに表示される 2 種類のヘッダーは、フォームビューの特定のインシデントに関する詳細情報を示します。

必要なロール：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

このタスクについて
インシデントがアサインされたエンドユーザーは、インシデント応答方法に関する追加の指示を把握し、ユーザーに用語を紹介し、インシデントに関する追加情報を提供することが必要となることがあります。これらのテンプレートは、DLP インシデントに正確に対応できるようにユーザーをガイドします。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > ユーザー指示テンプレート.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

DLP インシデントのアセスメント

フィールド	説明
名前	ユーザー指示テンプレートの名前。
簡単な説明	このユーザー指示テンプレートの一意の説明。
アクティブ	ユーザー指示テンプレートがアクティブかどうかを示すオプション。
実行順序	インシデントユーザー指示テンプレートの優先度。このフィールドは、インシデントの作成時のユーザー指示テンプレートの評価実施順序を示します。 番号が最も小さいオプションの優先度が最も高くなります。 操作の順序を設定するには、値を入力します。たとえば、100 や 200 などの数字です。 デフォルトは 100 です。
インシデント一致条件	条件ビルダーで定義された条件に一致するインシデントが表示されます。 ここの条件は DLP インシデントデータに基づいて決まります。ユーザー指示の条件を作成するには、いずれかのインシデントフィールドを選択します。 条件ビルダーのリストとフィールドを使用して、最初の行のフィルターを設定します。 さらに条件を追加するには、[AND] または [OR] をクリックします。 [AND] を選択した場合は、すべての条件に一致する必要があります。[OR] を選択した場合は、いずれかの条件に一致します。2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: 条件ビルダーの条件では大文字と小文字が区別されます。
適用先	テンプレートが適用されるユーザーまたはユーザーグループを選択します。その他の利用可能なオプションは次のとおりです。 ○ すべてのエンドユーザー：指示テンプレートがすべてのユーザーに適用される場合は、このチェックボックスをオンにします。 ○ エスカレートされたインシデントのすべてのレビュー担当者：エスカレートされたインシデントのすべてのレビュー担当者にこのテンプレートが適用される場合は、このチェックボックスをオンにします。 ○ 特定のユーザー：アイコンをクリックして、DLP インシデント条件が適用される特定のユーザーをリストから追加します。メールアドレスまたは検索オプションを使用してユーザーを追加することもできます。たとえば、「法務マネージャー」などです。 DLP 条件を適用できるユーザーとして自分自身を追加するには、[自分を追加] アイコンをクリックします。 ○ 特定のユーザーグループ：アイコンをクリックして、DLP インシデント条件が適用される特定のグループをリストから追加します。検索オプションを使用してグループを追加することもできます。たとえば、「サーベイ作成者」などです。
指示テンプレート：指示 (Instructions Template: Instructions)	インシデントレベルで利用可能な変数を使用して、リッチテキストエディターで指示を追加します。

4. [指示テンプレート **(Instructions Template)]** セクションにドリルダウンし、テンプレートの指示を入力し、必要に応じてインシデントレベル情報をこのセクションに追加します。
5. 特定のフィールドを動的に表示するには、必要な変数をドラッグアンドドロップします。
6. [送信] をクリックします。
これでユーザー指示テンプレートが作成されました。いずれかのユーザー指示ヘッダーをクリックすると、DLP インシデントの追加の詳細を確認できます。

   詳細については、「Data Loss Prevention Incident Response ユーザーワークスペース」を参照してください。

DLP UI ユーザー指示の構成

必要に応じて詳細なユーザー指示ヘッダーを追加するように、システム UI メッセージを構成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > システム **UI** > メッセージ.
2. **user_instruction_card_heading** を検索します。

   デフォルトでは、user_instruction_card_heading と user_instruction_modal_window_heading が、ユーザーにプロビジョニングされる 2 つの UI メッセージ構成です。

3. 更新または変更するユーザー指示をクリックします。

メールテンプレートを作成する

エンドユーザー、ユーザーグループ、またはマネージャーに通知を送信するための事前設定済みメールテンプレートを作成および管理します。このテンプレートを使用すると、Data Loss Prevention Incident Response (DLP IR) インシデントについてエンドユーザーに指示と連絡を行うことができます。

始める前に
必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

> **重要:**
> アナリストがアクティビティストリームで DLP インシデントのメール通信を確認できるようにするには、グローバルシステムプロパティ glide.ui.activity.email_roles に「sn_dlir.analyst」ロールを追加する必要があります。

このタスクについて
メール通知は、エンドユーザーに送信されるインシデント通知、マネージャーに送信されるエスカレーション通知、または期日の通知ごとに分類されます。DLP インシデントの期日に関するメール通知を送信したり、メール条件フィルターの特定の条件が満たされた場合の操作をエンドユーザーに指示したりすることもできます。
DLP メールテンプレートを使用すると、エンドユーザー、マネージャー、およびアナリストにメール通知を送信できます。テンプレートは、インシデントごとに送信するか、ダイジェストとして送信するように設定できます。既存のコンテンツを再利用できるように、メールの件名と本文に変数を含めることができます。

DLP には、カテゴリに基づいて次のメールテンプレートが事前設定されています。

- **DLP** メールテンプレート - インシデントごとの承認通知 **(Per incident approval** notification)：要求の承認についてユーザーに通知します。
- **DLP** メールテンプレート - エスカレーション通知：エスカレーション通知をダイジェスト形式でマネージャーに送信します。
- **DLP** メールテンプレート - 承認待ち通知 **(Pending approval** notification)： 保留中のアイテムについて承認者に通知します。
- **DLP** メールテンプレート - インシデントごとの承認要求キャンセル通知 **(Per incident approval request cancellation** notification)：DLP アナリストチームがキャンセルした承認要求についてユーザーに通知します。
- **DLP** メールテンプレート - ユーザー応答完了通知 **(User response completion** notification)：ユーザーにが送信した応答について DLP アナリストチームに通知します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- **DLP** メールテンプレート **-** ユーザーインシデント通知 **(User incident** notification)：これは、ユーザーダイジェスト通知のデフォルトテンプレートです。新しいインシデントが発生していない場合でも、数日ごとにインシデント通知をダイジェスト形式でエンドユーザーに送信して、特定のユーザー名のインシデント合計数をユーザーに通知します。ダイジェスト通知を送信して、重大度が重大、高、中、または低の DLP インシデントの直近の期日についてユーザーに通知することもできます。
- **DLP** メールテンプレート **-** インシデントごとの承認待ち通知 **(Per incident pending approval** notification)： 保留中の承認について承認者に通知します。
- **DLP** メールテンプレート **-** 却下通知 **(rejection** notification)： 要求者に却下通知を送信します。
- **DLP** メールテンプレート **-** 期日の通知： インシデント期日の通知を送信します。DLP インシデントがエンドユーザーにアサインされていて、そのエンドユーザーが期日までにアクションを実行しなかった場合、エンドユーザーにメール通知が送信されます。応答期日に違反した場合は、DLP インシデントをマネージャー、カスタムユーザー、またはユーザーグループにエスカレーションすることもできます。

  注:
  期日の通知はダイジェスト形式である必要があります。

- **DLP** メールテンプレート **-** インシデントごとのユーザー応答通知 **(Per incident user response** notification)： インシデントごとの応答送信ユーザーについてアナリストに通知します。
- **DLP** メールテンプレート **-** インシデントごとのエスカレーション通知 **(Per incident escalation** notification)：インシデントごとのエスカレーションについてマネージャーに通知します。
- **DLP** メールテンプレート **-** インシデントごとのユーザー通知 **(Per incident user** notification)：インシデントごとのアサインについてマネージャーに通知します。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > メールテンプレート.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

[DLP メールテンプレート] フォーム

フィールド	説明
名前	メールテンプレートの名前。
アクティブ	DLP メールテンプレートがアクティブかどうかを示すオプション。このオプションが有効でない場合、このメールテンプレートの通知は送信されません。
カテゴリ	メール通知カテゴリ。DLP は次のオプションをサポートしています。 ○ エンドユーザーへのインシデント通知：インシデントがエンドユーザーにアサインされると送信されます。 ○ マネージャーへのエスカレーション通知：応答期日に違反した場合、または DLP 運用ポータルを介してマネージャーに手動でアサインされた場合に送信されます。 ○ 期日の通知：応答期日への違反があった場合に送信されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ アナリストへのユーザー応答通知：エンドユーザーが DLP インシデントに対してアクションを実行すると送信されます。 ○ 承認待ち通知 **(Pending approvals** notification)：保留中のアイテムについて承認者に通知します。 ○ 要求者への承認通知 **(Approval notification to the** requester)：要求の承認についてユーザーに通知します。 ○ 要求者への却下通知 **(Reject notification to the** requester)：要求の却下についてユーザーに通知します。 ○ 要求者へのキャンセル通知 **(Cancel notification to the** requester)： 要求のキャンセルについてユーザーに通知します。
タイプ	メールをインシデントごとに送信するか、ダイジェストとして送信するかを指定するオプション。 **注:** [カテゴリ] フィールドから [期日の通知] を選択した場合は、ダイジェストのみが使用できます。このオプションを選択します。
説明	このメールテンプレートの固有の説明。
実行順序	メールテンプレートの優先度。このフィールドは、2 つ以上のメールテンプレートがトリガー条件を共有する場合にメールテンプレートが実行される順序を示します。 番号が最も小さいメールテンプレートの優先度が最も高くなります。操作の順序を設定するには、値を入力します。たとえば、100 や 200 などの数字です。デフォルト値は 100 です。
テンプレート条件	DLP インシデントテーブルに基づいたテンプレート条件のオプション。メールテンプレートのトリガー条件をビルドするための任意のインシデントフィールドを選択できます。 条件ビルダーのリストとフィールドを使用して、最初の行のフィルターを設定します。 条件を追加するには、**[AND]** または **[OR]** をクリックします。 ○ [**AND**] を選択した場合は、すべての条件に一致する必要があります。 ○ **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。 2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: 条件ビルダーの条件では大文字と小文字が区別されます。
ターゲットユーザー	条件が満たされた場合のテンプレートのターゲットユーザー。ターゲットユーザーは次のいずれかに設定できます。 ○ すべての受信者： ターゲットユーザーにメールを送信します。 ○ グループ内の受信者： フィルターオプションを使用して、特定のグループ内の受信者にのみメールを送信します。 ○ 基準に一致する受信者：基準に一致するターゲットユーザーにメールを送信します。このフィルターを使用すると、条件に基づいてターゲットユーザーをドリルダウンできます。たとえば、市区町村などです。

メールテンプレート	選択できるメールテンプレート。既存のコンテンツを再利用してメール通知に追加する変数を定義できます。
	[カテゴリ] フィールドと [タイプ] フィールドによって、選択可能な変数が決まります。たとえば、メールカテゴリがインシデント通知に設定されていて、メールタイプがダイジェストである場合、選択肢となる変数は、複数の DLP インシデントの蓄積に対応できるダイジェストフィールドになります。
	各メールテンプレートのメール本文 HTML の例を次に示します。
	○ インシデントごとの承認通知のデフォルトテンプレート：
	`Dear ${respondent.first_name},`
	
	`Your request "${end_user_response}" on the incident ${number} has been approved.`
	
	`- Date protection team`
	○ インシデントごとの承認要求キャンセル通知
	`Dear ${respondent.first_name},`
	
	`Your request "${end_user_response}" on the DLP incident ${number} has been cancelled.`
	
	`No action is required from you at this point. Data protection team will contact you for any further information required.`
	
	`- Data protection team`
	○ 期日の通知のデフォルトテンプレート：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	Dear ${target_user.name}, Following incidents require your response. ${due_days_table} - Data protection team ○ インシデントごとのユーザー通知のデフォルトテンプレート： Dear ${assigned_to.name}, DLP Incident ${number} is assigned to you. Please review and submit your response. - Data protection team ○ ユーザーインシデント通知のデフォルトテンプレート： Hello ${target_user.name}, You have ${total_number_of_incidents} incidents assigned to you currently that require your response. ${new_incidents_in_period} new incidents got assigned to you since the last email communication. Nearest upcoming due date for responding to a critical incident is ${nearest_due_date_for_critical_severity_incidents}. Please log in to the ${link_to_dlp_portal} and submit your response. - Data protection team ○ エスカレーションのデフォルトテンプレート - ダイジェスト： Hi ${target_user.name}, The following data security incidents have been escalated to you due to lack of response from the assignees. Please login to the incident response workspace to review the incidents and submit your response. ${overdue_table} - Data protection team ○ エスカレーションのデフォルトテンプレート - インシデントごと：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	Dear ${assigned_to.name}, Data security incident ${number} has been escalated to you. Please review and submit your response or assign the incident back to the user. - Data protection team ○ 承認待ち通知 **(Pending approval notification)** のデフォルトテンプレート： Dear ${approver.first_name}, Your approval is required for a few requests on data security incidents. Please login to the workspace here and review the requests. - Data protection team ○ インシデントごとの承認待ち通知のデフォルトテンプレート： Dear ${Approver}, Your approval is required for the incident ${number} requested by the user ${respondent.first_name} ${respondent.last_name}. Please visit this here to approve or reject the request. - Data Protection Team ○ インシデントごとの却下通知のデフォルトテンプレート： Dear ${respondent.first_name} ${respondent.last_name}, This is to inform you that your request "${end_user_response}" for the DLP incident ${number} has been rejected. Please review the incident here. - Data protection team ○ インシデントごとのユーザー応答通知のデフォルトテンプレート： Hi ${assigned_to.name},

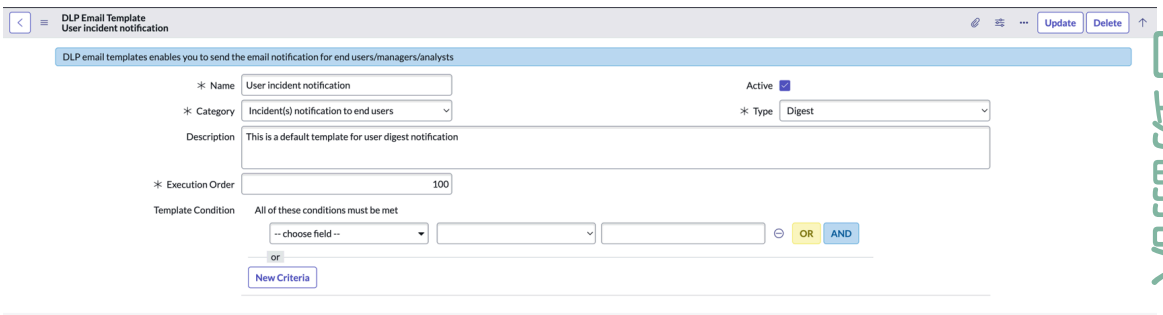
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	This is to inform you that a response has been submitted for the DLP Incident ${number}. ○ ユーザー応答完了通知のデフォルトテンプレート： Hello ${target_user.name}, This email is to inform you that users have submitted their response for ${new_incidents_in_period_user_response_completed} new incidents since the last email communication. Please review the response for these incidents ${link_to_incidents_in_period_user_response_completed}.

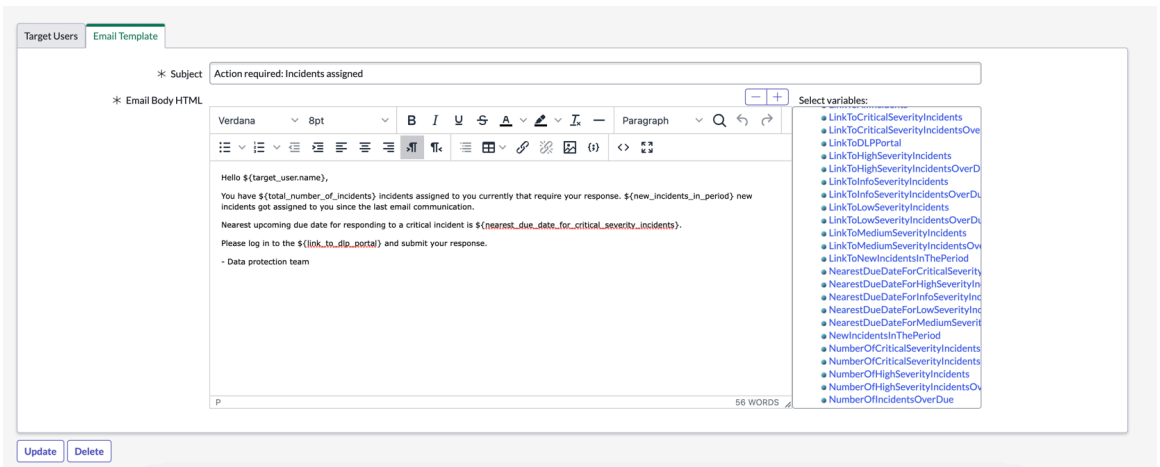
Example
次の例では、すべての受信者がターゲットユーザーに定義された DLP メールテンプレートを示します。

メールテンプレート



次の例は、件名が「User incident notification」で変数 *new_incidents_in_period* が使用されているメールテンプレートを示します。メールの本文に、[変数の選択] 列から追加された複数の変数が含まれています。

メールテンプレートの変数



4. [送信] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスクの結果
テンプレートで選択したすべての変数フィールドを含むダイジェスト通知メールがエンドユーザーに届きます。

アセスメントを作成

エンドユーザーが DLP インシデントに対応できるようにするためのアセスメントを作成および管理します。アセスメントを使用して、DLP インシデントから公開または漏洩した機密データに関する情報を収集できます。

DLP インシデントのアセスメントの作成と管理

始める前に
必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

このタスクについて
DLP インシデントのアセスメントは、エンドユーザーの応答に基づいて、データに対する潜在的な脅威と脆弱性を特定する際に役立ちます。この情報を使用して、エンドユーザーの既存のギャップ、懸念事項、および期待していることを判断できます。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > アセスメント.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

DLP インシデントのアセスメント

フィールド	説明
名前	DLP インシデントのアセスメントの名前。
アクティブ	DLP インシデントのアセスメントがアクティブかどうかを示すオプション。
説明	この DLP インシデントのアセスメントの固有の説明。
アセスメントの概要	アセスメントの概要またはコンテキストを入力します。[変数の選択] セクションの変数を使用して、特定のフィールドを動的に表示することもできます。

4. [送信] をクリックします。
5. アセスメントを作成したら、そのアセスメントを開き、[アセスメントデザイナー] をクリックします。
6. [新しいアセスメント] セクションの [コントロール] セクションで、アセスメントの質問のタイプを選択します。
7. [新しいアセスメント] セクションの下に、必要なアセスメントの質問のタイプをドラッグアンドドロップします。
たとえば、[新しいアセスメント] または [新しいカテゴリ] セクションの下に [選択肢] コントロールをドラッグアンドドロップできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

8. アセスメントのカテゴリをさらに追加するには、 アイコンをクリックします。
9. 既存のカテゴリを変更するには、 アイコンをクリックします。
10. 最初にさまざまなアセスメントの質問を作成した後、[保存] をクリックし、[公開] をクリックします。

インシデントレスポンスオプションルールを作成する

エンドユーザーまたはアナリストがインシデントに対応する際に使用できるインシデントレスポンスオプションルールを作成します。

始める前に

必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

このタスクについて

エンドユーザーが実行する必要のある応答のタイプは、DLP インシデントのタイプに基づいて設定できます。ベースシステムの DLP Incident Response アプリケーションには、ユーザーが使用できる次の応答オプションがあります。

- アセスメント完了
- 削除されたコンテンツ
- 削除されたファイル
- 暗号化されたファイル
- マスクされたコンテンツ (Masked Content)
- 誤検出を報告
- 不適切なオーナーを報告
- ビジネスプロセスに必要 (Required for Business Process)
- レビュー済みエンタイトルメント (Reviewed Entitlements)

たとえば、あるエンドユーザーが DLP インシデントを誤検出として報告したとします。設定したターゲットステータスがクローズされるため、このインシデントのステータスは自動的にクローズ済みとしてマークされます。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > インシデントレスポンスオプションルール.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

[インシデント応答オプションルール **(Incident Response Option Rules)**] フォーム

フィールド	説明
名前	インシデント応答オプションの名前。
アクティブ	インシデント応答オプションがアクティブかどうかを示すオプション。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
実行順序	インシデント応答オプションの優先度。このフィールドは、2 つ以上のインシデント応答オプションがトリガー条件を共有する場合にインシデント応答オプションが実行される順序を示します。 番号が最も小さいインシデント応答オプションの優先度が最も高くなります。 操作の順序を設定するには、値を入力します。たとえば、100 や 200 などの数字です。 デフォルトは 100 です。
説明	このインシデント応答オプションの固有の説明。
デフォルトのターゲットステータス	設定したデフォルトのターゲットステータス。
条件	条件ビルダーの条件。ここの条件は DLP インシデントテーブルに基づいて決まります。インシデント応答オプションの条件を作成するには、いずれかのインシデントフィールドを選択します。 条件ビルダーのリストとフィールドを使用して、最初の行のフィルターを設定します。 さらに条件を追加するには、**[AND]** または **[OR]** をクリックします。 ○ **[AND]** を選択した場合は、すべての条件に一致する必要があります。 ○ **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。 2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。 **注:** 条件ビルダーの条件では大文字と小文字が区別されます。

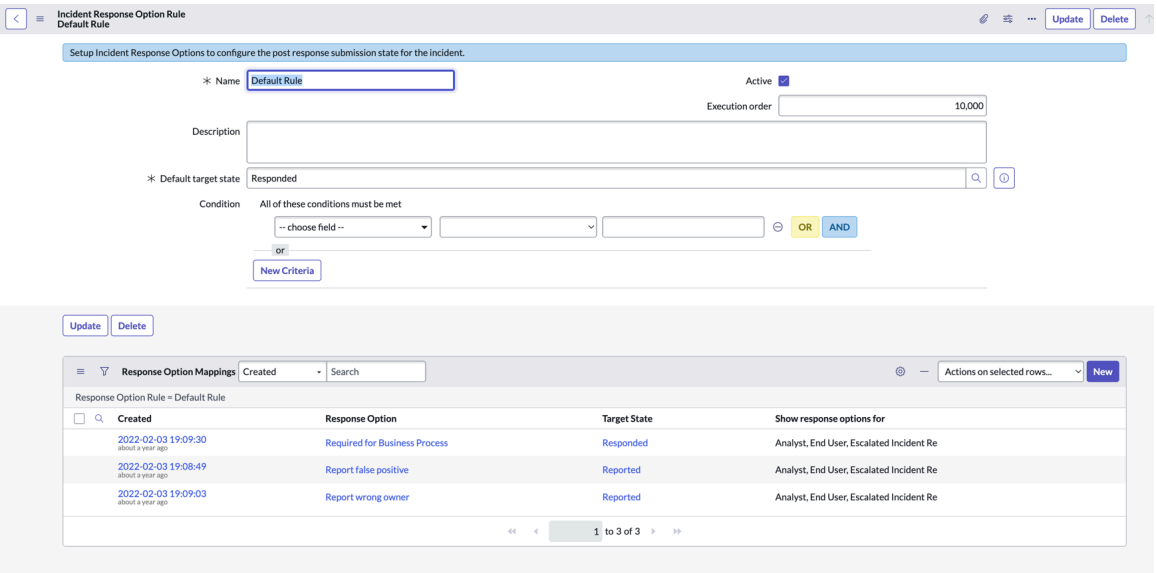
Example

次の例は、あるエンドポイントのエンドユーザーアクションの構成を示しています。この条件では、スキャンソースがこのエンドユーザーアクションの構成をトリガーするエンドポイントファイルシステムであることが要求されています。マッピングでは、エンドユーザーが使用できる応答オプションとして、不適切なオーナーの報告、誤検出の報告、および削除されたファイルがあることが示されています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インシデント応答オプションルール



4. [応答オプションマッピング **(Response Option Mappings)]** セクションで、[新規] をクリックします。
5. フォームのフィールドに入力します。

[応答オプションマッピング **(Response Option Mapping)]** フォーム

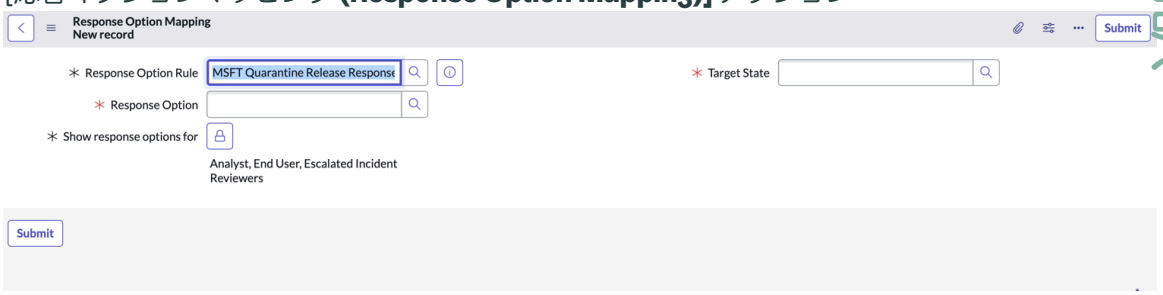
応答オプションルール (Response Option Rule)	インシデント応答オプションルールの名前。たとえば、SharePoint はスキャンソースが SharePoint であることを意味します。インシデント応答の名前を入力するか、検索機能を使用して検索できます。
応答オプション	応答オプションを選択するオプション。応答オプションを入力するか、検索機能を使用して検索できます。
ターゲットステータス	エンドユーザーが適切なアクションを選択した後の DLP インシデントのターゲットステータス。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

	注: **a.** [ターゲットステータス] フィールドは、[タイプ：基本] の応答オプションを選択した場合にのみ表示されます。ターゲットステータスタイプの構成方法の詳細については、「DLP インシデントの応答オプションの構成」を参照してください。 **b.** [タイプ：詳細 **(Type: Advanced)]** の応答オプションが選択されている場合、ターゲットステータスを設定できず、非表示になります。ターゲットステータスは、フローデザイナーサブフローから構成されたカスタム状況に基づいてアサインされます。
次の応答オプションを表示	応答オプションの表示対象となるユーザーロールを決定するオプション。 ロック解除オプションを使用して、[アナリスト]、[エンドユーザー]、および [エスカレートされたアナリストレビュー担当者 **(Escalated Analyst Reviewers)]** から選択できます。選択するロールは、1 つでも全部でもかまいません。

[応答オプションマッピング **(Response Option Mapping)]** アクション



6. [送信] をクリックします。

DLP インシデントの応答オプションの構成

この機能を使用して、エンドユーザーまたはアナリストが実行する必要がある応答のタイプを構成します。

始める前に

ベースシステムの DLP Incident Response アプリケーションには、次の応答オプションがあります。

1. アセスメント完了

2. 削除されたコンテンツ

3. 削除されたファイル

4. 暗号化されたファイル

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. マスクされたコンテンツ (Masked Content)
6. 誤検出を報告
7. 不適切なオーナーを報告
8. 隔離からのメールのリリースを要求する (Request email release from quarantine)

   注:
   このオプションは、DLP Microsoft Exchange レコードで使用できます。

9. ビジネスプロセスに必要 (Required for Business Process)
10. レビュー済みエンタイトルメント (Reviewed Entitlements)

必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > 応答オプション.

   デフォルトでは、ベースシステムには次の 2 つのタイプの応答オプションがあります。

   a. 基本：ユーザーによって送信される手動の応答オプション。
   b. 詳細：ユーザーが応答オプションを送信すると、自動応答オプションによりフローデザイナーサブフローがトリガーされます。

2. [新規] をクリックします。
3. フォームのフィールドに入力します。

[タイプ：基本 **(Type: Basic)]** の [応答オプション] フォーム

フィールド	説明
名前	インシデント応答オプションの名前を入力します。
タイプ	応答オプションタイプを選択するオプション。

[タイプ：詳細 **(Type: Advanced)]** の [応答オプション] フォーム

フィールド	説明
名前	インシデント応答オプションの名前を入力します。
タイプ	応答オプションを選択するオプション。デフォルトでは、このフィールドには次の 2 種類のオプションが表示されます。 ○ 基本：新しい応答オプションの作成時にこのオプションを選択すると、応答オプション名とタイプの追加が必要となる場合があります。 ○ 詳細：このオプションを選択すると、次のフィールドを選択できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	▪ フロー：フローデザイナーサブフローを選択します。 ▪ **MID** サーバーが必要 **(Requires MID Server)**：選択したフローが MID サーバーを使用する場合は、このチェックボックスをオンにします。
フロー	必要なフローデザイナーフローを選択して、MID アプリケーションと MID 機能をアクティブにします。 応答オプションのサブフローを作成する場合は、次のサブフロー入力を追加します。 **a. Name :** ▪ dlp_incident ▪ mid_server_capability ▪ mid_server_application **b.** タイプ： ▪ 参照 (DLP インシデントテーブルへの参照) ▪ MID サーバーアプリケーションと MID サーバー機能の両方の Sys ID
MID サーバーが必要 (Requires MID Server)	その MID サーバー構成を決定するオプション。**[MID** サーバーが必要 **(Requires MID Server)]** チェックボックスをオンにすると、**[MID** サーバーアプリケーション] および **[MID** サーバーの機能] フィールドで MID アプリケーションと MID 機能を構成できます。 **注:** MID サーバーアプリケーションと MID サーバー機能の構成に基づき、MID が稼働している場合には、[応答オプション] のみがワークスペースに表示されます。
MID サーバーアプリケーション	ドロップダウンリストから必要な MID サーバーアプリケーションを選択します。
MID サーバーの機能	ドロップダウンリストから必要な MID サーバー機能を選択します。

注:
選択した MID サーバー機能に対して利用可能な MID サーバーがない場合、応答オプションは表示されません。リストに特定の MID サーバーが必要な場合は、MID アプリを構成してリストに表示する必要があります。構成されている少なくとも 1 つの MID サーバーが、選択した MID アプリケーションから稼働中であり、選択されている MID サーバー機能が含まれている必要があります。

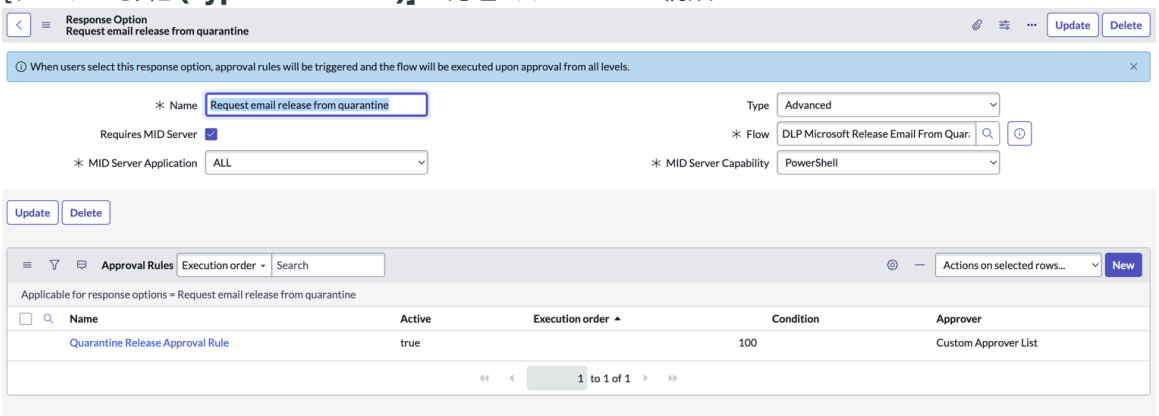
4. [送信] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:
[詳細] タイプの応答オプションを作成している場合は、その新しい応答オプションの承認ルールを構成できるように、[承認ルール] 関連リストが入力されます。詳細については、「承認ルールを作成する」を参照してください。

[タイプ：詳細 **(Type: Advanced)**] の応答オプションの構成



経過時間グラフ構成を作成する

Data Loss Prevention Incident Response (DLP IR) 運用ポータルに表示される年齢グラフを構成します。このグラフには、オープンインシデントの数が日数で表示されます。

始める前に
必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > 年齢グラフ構成.
2. 次の表の年齢グラフのエントリを確認し、環境に合わせてエントリをカスタマイズします。

[DLP 年齢グラフ構成] フォーム

名前	条件
0 ～ 30 日	0 日から 30 日までの、オープンインシデントの年齢。
31 ～ 60 日	31 日から 60 日までの、オープンインシデントの年齢。
61 ～ 90 日	61 日から 90 日までの、オープンインシデントの年齢。
90 日以上	90 日を超えるオープンインシデントの年齢。

3. [新規] をクリックして、新しい年齢グラフ構成を追加します。
4. [名前] フィールドに、DLP 年齢グラフ構成の名前を入力します。
5. DLP 年齢グラフ構成の条件を設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. 条件を追加するには、**[AND]** または **[OR]** をクリックします。

- **[AND]** を選択した場合は、すべての条件に一致する必要があります。
- **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。

> **注:**
> 条件ビルダーの条件では大文字と小文字が区別されます。

b. 2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。

6. [送信] をクリックします。

ユーザー委任構成を作成する

組織内の特定の重役が、アサインされたインシデントやエスカレーションされたインシデントに関する通知を受信しないように設定します。

始める前に

必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

このタスクについて

当該の重役がリーダーシップまたは重役グループに属するユーザーであるシナリオを考えてみましょう。この重役にはインシデントのアサインやエスカレーションに関するメールを送信しないようにする必要があります。そのため、委任を受けたユーザーが重役の代わりに必要なアクションを実行できます。

あるユーザーが特定のユーザー (Henry) を委任者としてアサインすると、別のユーザーが再度 Henry を委任者としてアサインすることはできません。同様に、委任者は他のユーザーを委任者としてアサインすることはできません。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > 委任者構成.

2. [**New**] をクリックします。

3. フォームのフィールドに入力します。

[委任者構成] フォーム

フィールド	説明
ユーザー	DLP インシデントに関する委任者を必要とするユーザーの名前。
委任	元のエンドユーザーの代わりに DLP インシデントに応答できるユーザーの名前。

4. [送信] をクリックします。

再犯者識別ルールの作成

同じ問題を複数回繰り返すユーザーを識別するための再犯者識別ルールを作成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

このタスクについて
特定のルールまたは基準を使用して再犯者を特定できます。Data Loss Prevention Incident Response に、再犯者を特定するためのフィールドがあります。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > 再犯者識別ルール.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

[再犯者識別ルール **(Repeat offender identification rules)**] フォーム

フィールド	説明
名前	再犯者識別ルールの名前。
実行順序	再犯者識別ルールの優先順位。このフィールドは、2 つ以上の再犯者識別ルールがトリガー条件を共有する場合にそのルールが実行される順序を示します。 番号が最も小さい再犯者識別ルールの優先度が最も高くなります。 操作の順序を設定するには、値を入力します。たとえば、100 や 200 などの数字です。デフォルト値は 100 です。
簡単な説明	この再犯者識別ルールの固有の説明。
条件	DLP インシデントテーブルに基づいた条件ビルダー内の条件。任意のインシデントフィールドを選択して、繰り返し違反者識別ルールのトリガー条件をビルドできます。 条件ビルダーのリストとフィールドを使用して、最初の行のフィルターを設定します。 さらに条件を追加するには、**[AND]** または **[OR]** をクリックします。 ○ **[AND]** を選択した場合は、すべての条件に一致する必要があります。 ○ **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。 2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。

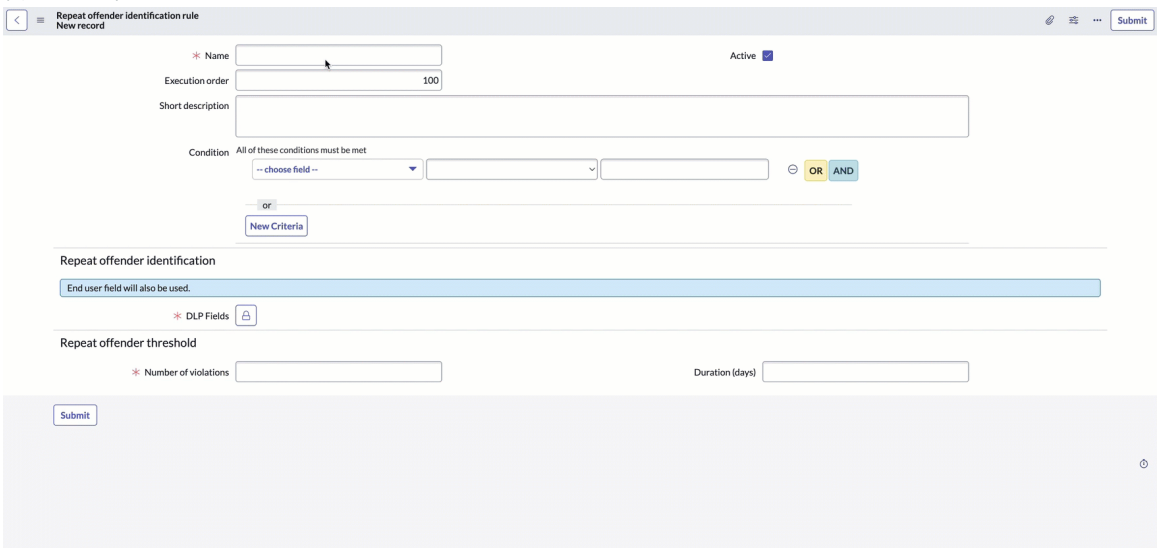
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: 条件ビルダーの条件では大文字と小文字が区別されます。
DLP フィールド	必須の DLP フィールドに基づいて、再犯者を特定します。[DLP フィールド] の横にあるアイコンをクリックすると、利用可能な DLP フィールドのリストが表示されます。使用する DLP フィールドを [利用可能] 列から選択して、[選択済み] 列に移動します。 たとえば、[利用可能] 列から [ファイル名] および [ファイルの所有者] フィールドを選択して [選択済み] 列に移動できます。その後、[ファイル名] フィールドと [ファイルの所有者] フィールドに基づいて再犯者を特定できます。 したがって、あるユーザーが再犯者しきい値 (違反の数と期間) に違反し、同じユーザーが DLP フィールドに一致した場合、そのユーザーは再犯者として識別されます。
違反の数	再犯者しきい値の制限値を定義します。ユーザーが同じアクションを繰り返し、指定された回数違反すると、そのユーザーは再犯者として識別されます。
期間 (日数)	再犯者しきい値の制限値を日数の形式で定義します。ユーザーが同じアクションを繰り返し、しきい値の期間を違反すると、そのユーザーは再犯者として識別されます。

自動翻訳

再犯者の特定



4. [送信] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

追加のインシデントデータフィールドを作成する

DLP インシデントの追加インシデントデータフィールドを作成します。文字列、数値、チェックボックス、選択肢、日時などのさまざまなタイプの追加インシデントデータフィールドを作成し、DLP インシデントフォームで使用できます。

始める前に

必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

重要:
DLP インシデントの追加インシデントデータフィールドは、San Diego バージョン以降でのみサポートされています。

このタスクについて

追加インシデントデータフィールドはフィールドレベル制限に関連付けられているため、フィールドレベル制限がある場合は、DLP 運用ポータルとエンドユーザーポータルの追加インシデントデータフィールドに適用されます。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > 追加のインシデントデータフィールド.
2. [新規] をクリックして、追加のインシデントデータフィールドを作成します。
3. フォームのフィールドに入力します。

DLP 追加インシデントデータフィールドフォーム

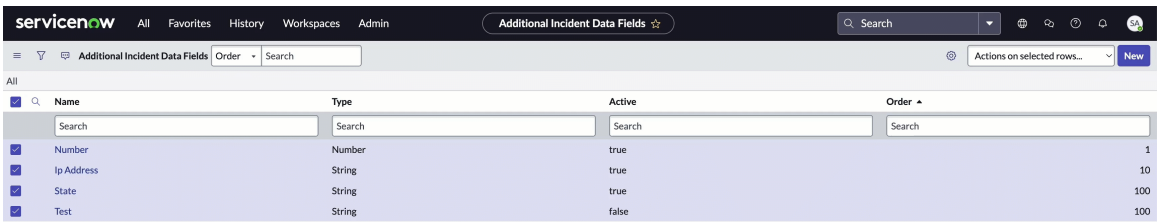
フィールド	説明
名前	追加のインシデントデータフィールドの名前。
タイプ	追加のインシデントデータフィールドのタイプを選択するオプション。次のいずれかのタイプを選択できます。 ○ 文字列 ○ 番号 ○ チェックボックス ○ **Choice** (選択肢) [追加インシデントデータフィールド] タイプに [選択肢] を選択した場合は、[追加インシデントデータフィールド] を作成した後に、[追加インシデントデータフィールド] の選択肢オプションを定義できます。 [追加のインシデントデータフィールド] 選択オプションを作成するには: **a.** 必要な追加のインシデントデータフィールドを開きます。 **b.** [カスタム選択肢フィールドオプション] セクションで、[新規] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	c. [オプション名] フィールドで、必要なオプション名を定義します。 **d.** [送信] をクリックします。 ○ 日付 ○ **Date/Time** (日付/時刻) **注:** 新しい [追加インシデントデータ] フィールドのタイプを選択した後は、変更することはできません。タイプを変更する場合は、必要なタイプで新しい追加インシデントデータフィールドを再度作成する必要があります。
順序	追加のインシデントデータフィールドを表示する順番を選択するオプション。追加のインシデントデータフィールドごとに順序値を定義できます。[追加インシデントデータ] フィールドは、定義した順序値に基づいてソートされます。 デフォルトでは、[追加インシデントデータ] フィールドは昇順でソートされます。[順序] 列をクリックすると、[Additional Incident Data] フィールドを降順でソートできます。
アクティブ	追加のインシデントデータフィールドがアクティブかどうかを示すオプション。
説明	作成した追加のインシデントデータフィールドの説明。

DLP 追加インシデントデータフィールド



4. [**Submit** (送信)] を選択します。

詳細設定を構成します

詳細設定を構成して、各種機能の中でも特にエンドユーザーの識別を行うためのインシデントのフィールドを決定できるようにします。

始める前に

必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
Data Loss Prevention Incident Response の詳細設定の指定は任意です。詳細設定には次のようなものがあります。

- ダイジェストメールで送信できるインシデントの最大数を定義する。
- クイックモードを有効にしてメールの送信速度を上げる。
- アプリケーションのログの詳細度を決定する。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > 詳細設定.
2. フォームのフィールドに入力します。

[詳細設定] フォーム

フィールド	説明
違反の原因となった機密データをインシデントに表示するかどうか	違反の原因となった機密データを DLP インシデントに表示するかどうかを選択するオプション。 デフォルトでは、このオプションは有効になっています。
違反の原因となった機密データを子インシデントにも表示するかどうか	違反の原因となった機密データを DLP の子インシデントにも表示するかどうかを選択するオプション。 デフォルトでは、このオプションはオフになっています。
エンドユーザーを識別するために使用されるインシデントのフィールドのリスト	エンドユーザーを識別するために使用される [アサインルール] モジュールのインシデントのフィールドのリスト。エンドユーザーを識別するための独自のカスタム属性を指定することもできます。
ダイジェストメールのインシデントの最大数	ダイジェストメールで送信できるインシデントの最大数。 デフォルト値は 100 です。
違反の最大繰り返し期間 (日数)	再犯者を識別するための最長期間。 デフォルト値は 90 日です。
メールを送信するクイックモード	メールを検証して問題を特定するオプション。[はい] オプションを有効にすると、検証を実行できます。 デフォルトでは、このオプションは有効になっています。
このプロパティを使用して、アプリケーションのログの詳細度を設定します。	アプリケーションのログの詳細度レベル、すなわち情報のタイプの名前。値を次のオプションに更新することもできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ エラー ○ 警告 ○ 情報 ○ **debug** デフォルト値は **INFO** です。
クローンされたインシデントと子インシデントをレポートから除外する (Exclude cloned and child incidents from reports)	クローンされたインシデントと子インシデントをレポートから除外するオプション。 デフォルトでは、このオプションは [はい] になっています。
インシデントのクローズ後に、クラウドストレージで一致するコンテンツが削除されるまでの待機日数 (Day(s) to wait for deleting match content on cloud storage after incident gets closed)	特定の期間にわたり非アクティブだったインシデントの一致コンテンツをクリーンアップするまでに待機する日数を選択するオプション。 デフォルト値は 90 です。90 日後に DLP インシデントが非アクティブな場合、一致コンテンツはクラウドストレージからクリーンアップされます。
最終エスカレーションレベルの後に DLP アナリストグループにインシデントをアサインする (Assign Incident to DLP Analyst group after last escalation level)	最終エスカレーションレベルの後にインシデントをアナリストにアサインするには、このチェックボックスをオンにします。
エスカレーション後のインシデントへのアクセスをユーザーに許可する (Allow users to access incidents post escalation)	アサインされたユーザーがエスカレーション後のインシデントにアクセスできるようにするには、このチェックボックスをオンにします。 このオプションを選択すると、エスカレーションチェーンリストに追加されたすべてのユーザーがインシデントにアクセスできるようになります。
完了したアセスメントの編集をアナリストに許可	アナリストが完了したアセスメントを編集できるようにするには、このチェックボックスをオンにします。 このオプションを選択すると、アナリストはアセスメントを編集でき、選択を解除すると、読み取り専用モードでアセスメントを表示できます。
証拠ファイルのプレビュープロパティ	
このシステムプロパティを有効にすると、DLP アナリストワークスペースで証拠ファイルのプレビュー機能が有効になります。 sn_dlir.enable_evidence_file_preview	証拠ファイルをワークスペースで直接プレビューするかどうかを選択するオプション。 デフォルトでは、このオプションは [はい] になっています。
これにより、DLP ユーザーはプレビューされた証拠ファイルをダウンロードできます。こ	ドキュメントビューアにダウンロードボタンを表示するかどうかを選択するオプション。これ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
のプロパティを有効にすると、ドキュメントビューアーに証拠ファイルをダウンロードするためのダウンロードボタンが表示されます。 sn_dlir.enable_download in_preview	により、プレビューされた証拠ファイルをダウンロードできます。 デフォルトでは、このオプションは [はい] になっています。
このプロパティは、証拠ファイルのプレビューのためにファイルが一時的に保持される期間を決定します。(分単位) sn_dlir.preview_temp_files_cleanup_interval	証拠ファイルのプレビューのためにファイルが一時的に保存される最大期間。 デフォルト値は 10 です。10 分後、DLP インシデントが非アクティブである場合、証拠ファイルはアナリストワークスペースからクリーンアップされます。
このプロパティを有効にすると、証拠ファイルが使用中の場合、クリーンアップ間隔が延長されます。これにより、システムプロパティ「sn_dlir.preview_temp_files_cleanup_interval」で設定された値に基づいて証拠ファイルの有効期限を延長できます。 sn_dlir.extend_cleanup_interval_on_usage	証拠ファイルが使用されている場合に削除されるまでの時間を延長するオプション。 デフォルトでは、このオプションは [はい] になっています。
証拠ファイルのクリーンアップ間隔を延長する最大期間 (分)。 sn_dlir.max_extension_duration_for_cleanup	証拠ファイルをクリーンアップする前にシステムが保持する期間を分単位で選択するオプション。 デフォルト値は 60 です。

3. **[Save** (保存)] をクリックします。

DLP 統合実行プロセスを監視する

進行中の取り込みまたは統合実行プロセスを追跡および監視します。統合実行プロセスには、処理されたデータの量と統合のステータスに関する統計情報が含まれています。

必要なロール：sn_dlir.admin

統合実行プロセスには、取り込まれたレコード数の詳細がリストされます。例：

1. Symantec 統合では、プロセスに子と親の両方の統合実行が含まれます。親レコードは取り込みデータを示し、子レコードは拡張呼び出しとカスタム属性レコードを示します。
2. Microsoft 統合では、実行されるプロセスは親レコード取り込みプロセスのみです。

DLP 統合実行プロセス **(DLP Integration Run Processes)**：キューエントリ、キューエントリのステータス、およびフェッチされたレコードが表示されます。

統合実行には、統合プロファイルと統合実行レコードの作成元のソース、プロファイルのポーリング間隔、取り込みのステータスとサブステート、取り込まれたレコードの数を示すインシデント数が含まれます。

1. 次のように移動する。 **DLP** 管理 > 統合実行.
2. リストから統合実行を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. **[DLP** 統合実行プロセス **(DLP Integration Run)]** に移動します。
4. レコードのキューエントリのステータスを表示します。

DLP インシデントアクセス制限

機密情報を含む特定の DLP インシデントの可視化を管理します。インシデントアクセス制限を使用すると、特定の DLP インシデントにアクセスできるユーザーを定義して、特定のユーザーやグループがそのインシデントにアクセスできないようにすることができます。

フィールドレベル制限の作成

DLP インシデントにフィールドレベル制限を設定して、機密情報が公開されないようにします。フィールドレベル制限を使用すると、DLP インシデントの特定のフィールドにアクセスできるユーザーやグループを制御できます。

始める前に

必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

このタスクについて

フィールドレベル制限を使用すると、特定のユーザーやグループに対して特定のフィールドのみを表示し、ユーザーがアクセスできるデータをよりきめ細かく制御できます。フィールドレベル制限を作成するには、DLP インシデント一致条件を定義し、その条件を適用するユーザーやグループを選択して、そのユーザーやグループに表示される DLP フィールドを選択します。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > インシデントアクセス制限 > フィールドレベル制限.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

[DLP フィールドレベル制限] フォーム

フィールド	説明
名前	DLP フィールドレベル制限の名前。
アクティブ	フィールドレベル制限がアクティブかどうかを示すオプション。
実行順序	DLP フィールドレベル制限の優先度。このフィールドは、2 つ以上のフィールドレベル制限がトリガー条件を共有する場合にそのフィールドレベル制限が実行される順序を示します。 番号が最も小さいフィールドレベル制限の優先度が最も高くなります。 操作の順序を設定するには、値を入力します。たとえば、100 や 200 などの数字です。デフォルト値は 100 です。
簡単な説明	このフィールドレベルの制限に固有の説明。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

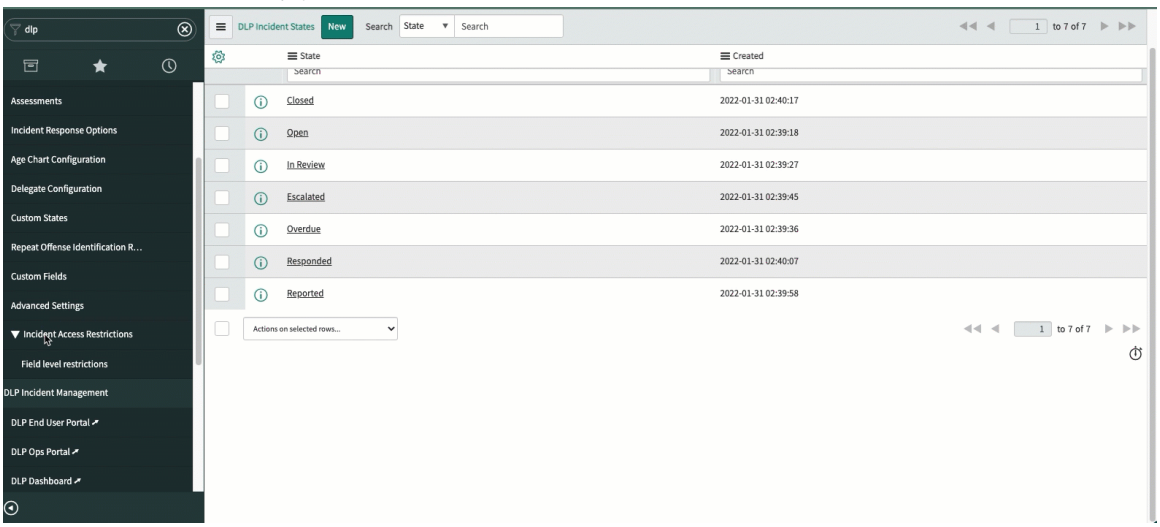
フィールド	説明
インシデント一致条件	定義された条件に一致するインシデントのオプション。フィールドレベルの制限のトリガー条件を定義するインシデントフィールドを任意に選択できます。 条件ビルダーのリストとフィールドを使用して、最初の行のフィルターを設定します。さらに条件を追加するには、**[AND]** または **[OR]** をクリックします。 ○ **[AND]** を選択した場合は、すべての条件に一致する必要があります。 ○ **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。 2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。 たとえば、フィールドを [ポリシー名] として選択し、条件を [次のうち] と [ポリシー名] に設定することができます。 **注:** 条件ビルダーの条件では大文字と小文字が区別されます。
適用先	インシデント一致条件を特定のユーザーやグループに適用するオプション。適用できる条件は次のとおりです。 ○ すべてのエンドユーザー：DLP インシデント条件が適用されるすべてのエンドユーザーを選択するオプション。 ○ エスカレートされたインシデントのすべてのレビュー担当者：エスカレーションされたインシデントのレビュー担当者のうち、DLP インシデント条件が適用されるすべての担当者を選択するオプション。このオプションでは、マネージャーにエスカレーションされたすべての DLP インシデントを参照します。 ○ ユーザー：アイコンをクリックして、DLP インシデント条件を適用できる特定のユーザーをリストから追加します。メールアドレスまたは検索オプションを使用してユーザーを追加することもできます。たとえば、「法務マネージャー」などです。 DLP 条件を適用できるユーザーとして自分を追加するには、をクリックします。 ○ グループ：アイコンをクリックして、DLP インシデント条件を適用できる特定のグループをリストから追加します。検索オプションを使用してグループを追加することもできます。たとえば、「サーベイ作成者」などです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
次のフィールドへのアクセスのみを許可	○ **DLP** フィールド：選択されたユーザーやグループにアクセスを許可する DLP フィールドを定義するオプション。アクセスを許可する DLP フィールドを [利用可能] 列から選択して、[選択済み] 列に移動します。 **注:** 選択されたユーザーやグループは、ここで選択した DLP フィールドにのみアクセス可能になります。 たとえば、[利用可能] 列から [アサイン先] および [オープン] フィールドを選択して [選択済み] 列に移動できます。その後、[アサイン先] および [オープン] フィールドにのみ、選択したユーザーまたはグループがアクセス可能になります。 ○ 添付ファイルをアップロード：選択されたユーザーやグループに添付ファイルのアップロードを許可するかどうかを指定するオプション。 ○ カスタムフィールド：選択されたユーザーやグループにアクセスを許可するカスタムフィールドを定義するオプション。作成したカスタムフィールドは [利用可能] 列に表示されます。 アクセスを許可するカスタムフィールドを [利用可能] 列から選択して、[選択済み] 列に移動します。 **重要:** ▪ DLP インシデントのカスタムフィールドは、San Diego バージョン以降でのみサポートされています。 ▪ 選択されたユーザーやグループは、ここで選択したカスタムフィールドにのみアクセス可能になります。

DLP フィールドレベル制限



4. [送信] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

レコードレベル制限の作成

DLP インシデントにレコードレベル制限を設定して、機密性の高いレコードが公開されないようにします。レコードレベル制限を使用すると、DLP インシデントの特定のレコードにアクセスできるユーザーやグループを制御できます。

始める前に

必要なロール：

- sn_dlir.admin - 作成、編集、および削除
- sn_dlir.analyst および sn_dlir.analyst_read - 表示 (読み取り専用)。

このタスクについて

レコードレベル制限を使用すると、特定のユーザーやグループのみにレコードへのアクセスを許可し、ユーザーがアクセスできるレコードをよりきめ細かく制御できます。レコードレベル制限を作成するには、DLP インシデント一致条件を定義し、その条件を適用するユーザーやグループを選択して、そのユーザーやグループに表示される DLP レコードを選択します。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** 管理 > インシデントアクセス制限 > レコードレベル制限.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

[DLP レコードレベル制限] フォーム

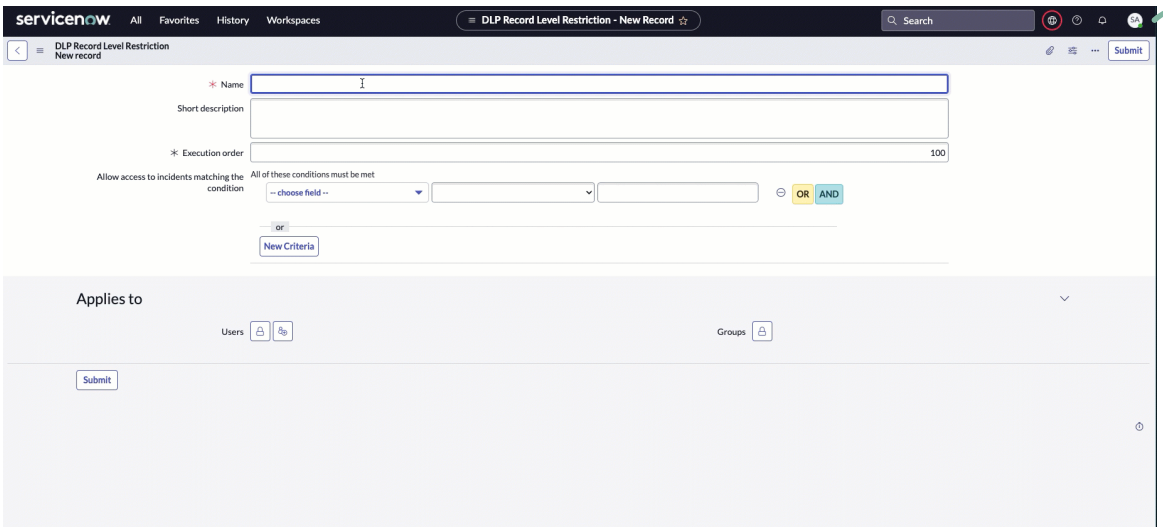
フィールド	説明
名前	DLP レコードレベル制限の名前。
簡単な説明	このレコードレベル制限に固有の説明。
実行順序	レコードレベル制限の優先度。このフィールドは、2 つ以上のレコードレベル制限がトリガー条件を共有する場合にそのレコードレベル制限が実行される順序を示します。 番号が最も小さいレコードレベル制限の優先度が最も高くなります。 操作の順序を設定するには、値を入力します。たとえば、100 や 200 などの数字です。デフォルト値は 100 です。
条件に一致するインシデントへのアクセスを許可 (Allow access to incidents matching the condition)	定義された条件に一致するインシデントへのアクセスを許可するオプション。レコードレベル制限のトリガー条件を定義するインシデントフィールドを任意に選択できます。 条件ビルダーのリストとフィールドを使用して、最初の行のフィルターを設定します。さらに条件を追加するには、**[AND]** または **[OR]** をクリックします。 ○ **[AND]** を選択した場合は、すべての条件に一致する必要があります。 ○ **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	2 つ目のフィルター条件を設定するには、[新しい基準] をクリックします。 **注:** 条件ビルダーの条件では大文字と小文字が区別されます。 たとえば、フィールドを [アクティブ] として選択し、条件を [次のうち] と [true] に設定することができます。
適用先	特定のユーザーやグループにレコードレベル制限を適用するオプション。適用できる条件は次のとおりです。 ○ ユーザー：アイコンをクリックして、選択したレコードを適用できる特定のユーザーをリストから追加します。メールアドレスまたは検索オプションを使用してユーザーを追加することもできます。たとえば、「法務マネージャー」などです。 レコードを適用できるユーザーとして自分を追加するには、をクリックします。たとえば、システムアドミニストレーターです。 ○ グループ：アイコンをクリックして、選択したレコードを適用できる特定のグループをリストから追加します。検索オプションを使用してグループを追加することもできます。たとえば、「サーベイ作成者」などです。

DLP レコードレベル制限



4. [送信] をクリックします。

DLP インシデントのアーカイブ

Data Loss Prevention Incident Response は、DLP インシデントテーブルのベースシステムで 1 つのアーカイブルールを使用してプロビジョニングされます。関連レコードは、ベースシステムの DLP インシデントアーカイブルールにも追加されます。

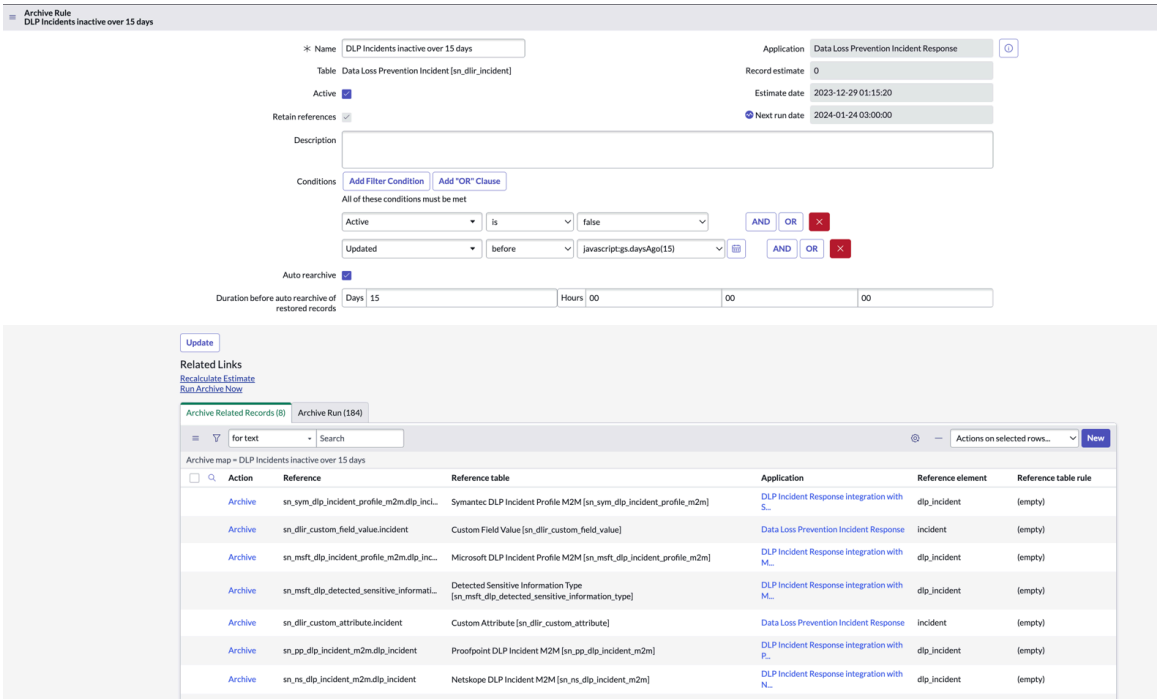
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > システムアーカイブ > アーカイブルール.
   ベースシステムにあるシステムアーカイブルールが表示されます。
2. DLP アーカイブルールを表示します。

   注:
   [15 日間にわたって非アクティブな **DLP** インシデント **(DLP Incidents inactive over 15 days)]** は DLP インシデントのデフォルトのベースシステムアーカイブルールで、必要に応じてアーカイブルールを変更できます。このルールは、15 日間を超えて非アクティブなインシデントが自動的にアーカイブされることを示します。



   注:
   アーカイブルールの作成方法については、「アーカイブルールの作成」を参照してください。

3. 必要に応じてルールを更新します。

DLP 関連レコードのアーカイブ

DLP インシデントの [アーカイブ関連レコード] 関連リストを使用して、関連レコードをアーカイブルールに追加します。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > システムアーカイブ > アーカイブルール.
2. **[15** 日間以上非アクティブの **DLP** インシデント **(DLP Incidents inactive over 15 days)]** アーカイブルールを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [アーカイブ関連レコード] 関連リストに移動します。
4. DLP 関連レコードを表示します。

アプリケーション	参照テーブル
DLP Incident Response integration with Symantec	Symantec DLP インシデントプロファイル M2M [sn_sym_dlp_incident_profile_m2m]
Data Loss Prevention Incident Response	カスタムフィールド値 [sn_dlir_custom_field_value]
Microsoft の DLP インシデントレスポンス統合	Microsoft DLP インシデントプロファイル M2M [sn_msft_dlp_incident_profile_m2m]
Microsoft の DLP インシデントレスポンス統合	検出された機密情報タイプ [sn_msft_dlp_detected_sensitive_information_type]
Data Loss Prevention Incident Response	カスタム属性 [sn_dlir_custom_attribute]
Proofpoint の DLP インシデントレスポンス統合	Proofpoint DLP インシデント M2M [sn_pp_dlp_incident_m2m]
Netskope と DLP インシデント応答の統合	Netskope DLP インシデント M2M [sn_ns_dlp_incident_m2m]
DLP Incident Response integration with Symantec	検出された機密情報タイプ [sn_sym_dlp_detected_sensitive_information_type]

注:
メール、アセスメント、添付ファイルなどのすべてのシステムテーブルは、アーカイブされた DLP レコードに自動的に転送されます。

5. アーカイブするアーカイブ関連レコードルールを選択します。

注:
関連レコードをさらに追加する方法の詳細については、Now Platform の「DLP 関連レコードのアーカイブ」を参照してください。

Data Loss Prevention Incident Response Incident Management

Data Loss Prevention Incident Response インシデント管理では、DLP ユーザーワークスペース、DLP アナリストワークスペース、および DLP ダッシュボードを活用してインシデントを更新および管理します。

Data Loss Prevention Incident Response ユーザーワークスペース

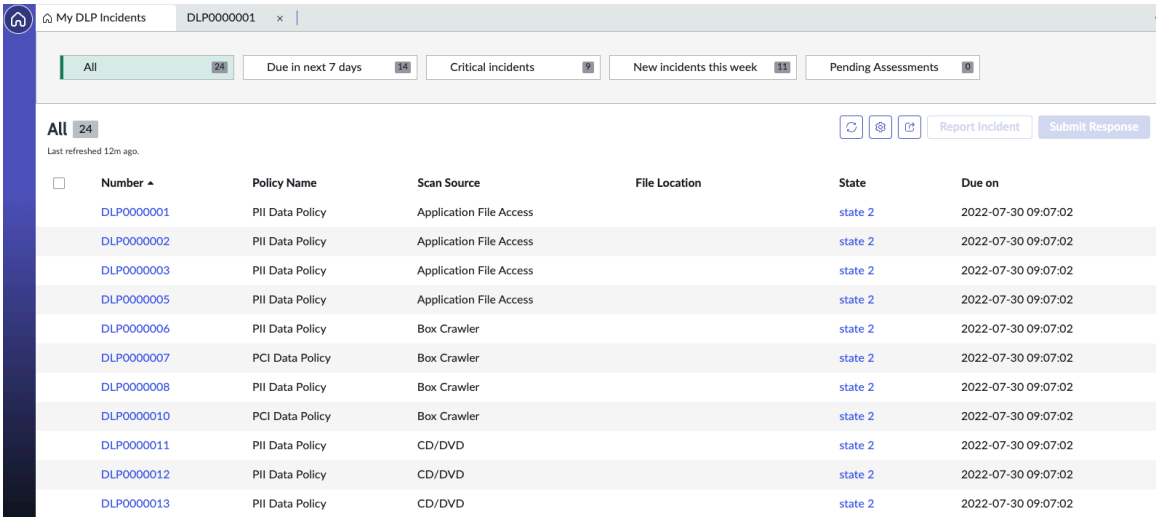
Data Loss Prevention Incident Response (DLP IR) ユーザーワークスペースは、エンドユーザー、マネージャー、および承認者がアサインされた DLP インシデントに対応するために使用できるワークスペースです。エンドユーザー、マネージャー、および承認者は、正しいアクションを指定することでインシデントに対応できます。

エンドユーザーが DLP インシデントに対応できるようにするためのアセスメントを作成および管理できます。ワークスペースはランディングページとリストビューで構成されており、ここでアサインされた DLP インシデントを確認できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

DLP ユーザーワークスペースのホームページ



DLP インシデントの報告または対応

Data Loss Prevention Incident Response (DLP) ユーザーワークスペースにアクセスし、アサインされた DLP インシデントを確認し、インシデントを報告またはインシデントに対応します。

始める前に

必要なロール：

- 任意の有効なユーザー/従業員

手順

1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** ユーザーワークスペース. [自分の DLP インシデント] ページが新しいタブで開きます。
2. リストビューをクリックして、自分にアサインされているインシデントを確認します。

リストビュー	説明
すべて	すべてのアサイン済みインシデントを表示します。
7 日以内に期限 (Due in the next 7 days)	7 日以内に期限が来るすべてのインシデントを表示します。
最重要のインシデント	重大度ラベルが「重大」のすべてのインシデントを表示します。
今週の新規インシデント (New incidents this week)	今週アサインされたすべてのインシデントを表示します。
処理待ちのアセスメント	まだ処理待ちのすべてのアセスメントを表示します。

3. DLP インシデントは、次の 2 つの方法で確認できます。

   a. 1 つ目は、確認する 1 つ以上の DLP インシデントを見つけて選択し、そのインシデントの横にあるチェックボックスをクリックする方法です。

   b. 自分に適したオプションを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

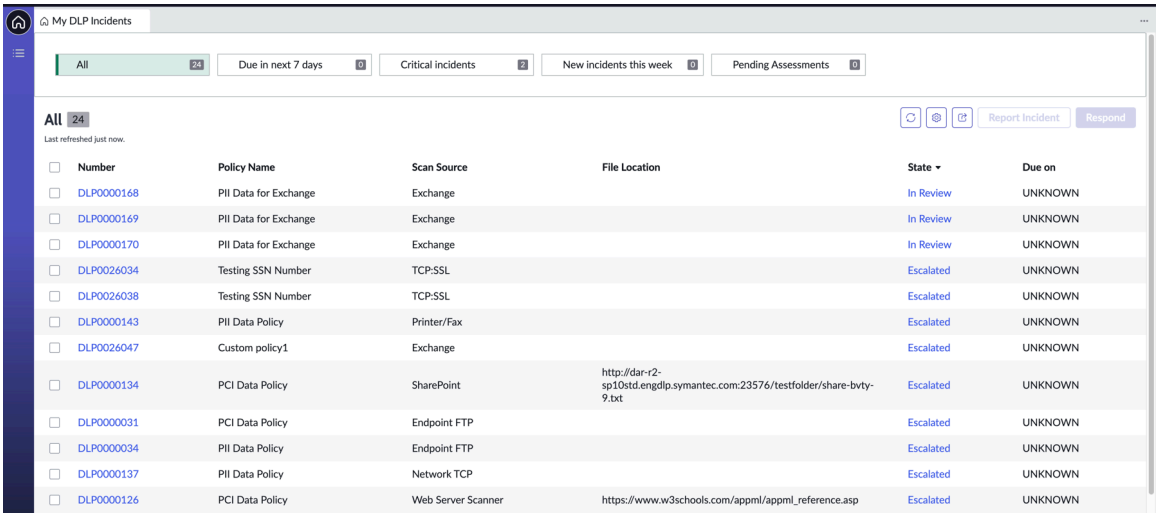
DLP エンドユーザーポータルのホームページ

オプション	説明
リストを更新	更新を行った場合に DLP インシデントのリストを更新するオプション。
リストアクション	実行できるアクションのリスト。選択肢は次のとおりです。 ▪ 名前を付けて保存 ▪ 列を編集 ▪ 幅をリセット **注:** [自分のリスト] セクションで作成された独自のカスタムリストを、各自のワークスペースに合わせて構成している場合は、以下の追加のリストアクションも実行できます。 ▪ 名前の変更 ▪ 保存 ▪ 削除
すべての URL をコピー (Copy URL for All)	すべての DLP インシデントの URL をコピーするオプション。
インシデントを報告	インシデントを誤検出または不適切なオーナーとして報告するアクション。たとえば、不適切なオーナーを報告して別のオーナーを提案したり、インシデントを誤検出として報告したりすることができます。
応答	インシデント応答オプションを選択して、インシデントに対応します。たとえば、ユーザーが DLP ポリシーに違反しているファイルを削除した場合、ユーザーは [削除されたファイル] オプションを選択して、ファイルが削除されたことを手動で確認し、コメントを入力できます。 ここから、詳細な応答オプションを選択することもできます。たとえば [隔離からのメールのリリースを要求する **(Request email release from quarantine)]** などです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

DLP ユーザーポータルのホームページ



c. 2 つ目の方法は、特定の DLP インシデントをクリックして開く方法です。
[詳細] タブに次のセクションが表示されます。

- 詳細：インシデント番号、重大度、ファイル名など、DLP インシデントの詳細を確認できます。
- 作成：全員に表示される DLP インシデントに関するコメントを追加するには、[コメント] タブにコメントを入力します。特定のユーザーに表示されるコメントを追加するには、 [作業メモ (プライベート)] タブにコメントを入力します。
- アクティビティ：DLP インシデントでのさまざまなアクティビティの詳細を確認できます。
- 添付ファイル：DLP インシデントに関連する添付ファイルがある場合は、[参照] をクリックしてローカルドライブから添付ファイルを選択します。

  [その他の詳細] タブに、DLP インシデントに関する、カスタムフィールドを含めたその他すべての情報が表示されます。

  重要:
  - DLP インシデントのカスタムフィールドは、San Diego バージョン以降でのみサポートされています。
  - 特定の DLP インシデントで利用可能なカスタムフィールドデータがある場合は、[その他の詳細] タブで確認できます。DLP インシデントのカスタムフィールドがない場合は、空白のページが表示されます。

- 検出された機密情報タイプ **(Detected Sensitive Information Type)**：インシデントで検出された機密情報を表示します。

  注:
  この関連リストは、Microsoft または Symantec の統合で作成された DLP インシデントの場合にのみ表示されます。Microsoft または Symantec のインシデントレコード内で、検出された機密情報タイプのレコードにユーザーがアクセスするたびに、その統合に関連して強調表示された一致コンテンツが表示されます。

d. 自分に適したオプションを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

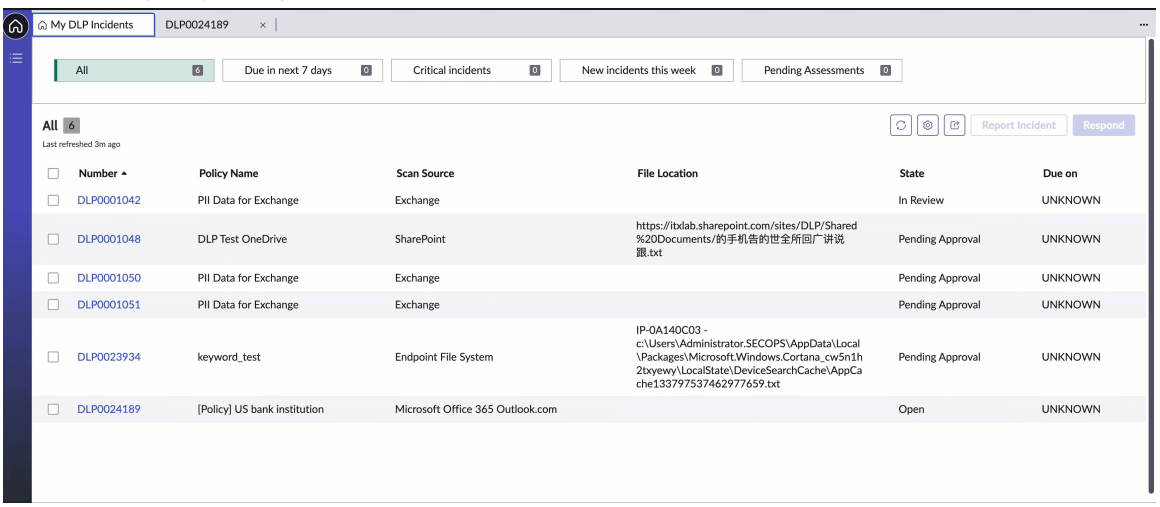
オプション	説明
誤検出を報告	DLP インシデントが誤ってトリガーまたは作成されたことを報告するアクション。インシデントを誤検出としてマークした理由の詳細を [コメント] フィールドに記入できます。
不適切なオーナーを報告	DLP インシデントが誤ったユーザーにアサインされたことを報告するアクション。インシデントの正しいオーナーが分かっている場合は、[オーナーの提案] フィールドでオーナーの名前を選択できます。詳細を追加するには、 [コメント] フィールドを使用します。
応答	インシデント応答オプションを選択して、インシデントに対応します。たとえば、ユーザーが DLP ポリシーに違反しているファイルを削除した場合、ユーザーは [削除されたファイル] オプションを選択して、ファイルが削除されたことを手動で確認し、コメントを入力できます。 ここから、詳細な応答オプションを選択することもできます。たとえば [隔離からのメールのリリースを要求する **(Request email release from quarantine)]** などです。

e. アナリストのクエリに回答した後、[応答] ボタンを選択します。
インシデント応答を送信するためのポップアップが表示されます。ドロップダウンメニューから応答を選択し、コメントを追加します。

f. [**Submit** (送信)] を選択します。
応答が正常に送信されたことを確認するバナーが表示されます。

注:
インシデントは対応する承認者またはアナリストにアサインされ、エンドユーザーはインシデントにアクセスできなくなります。

DLP インシデントのアクション



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

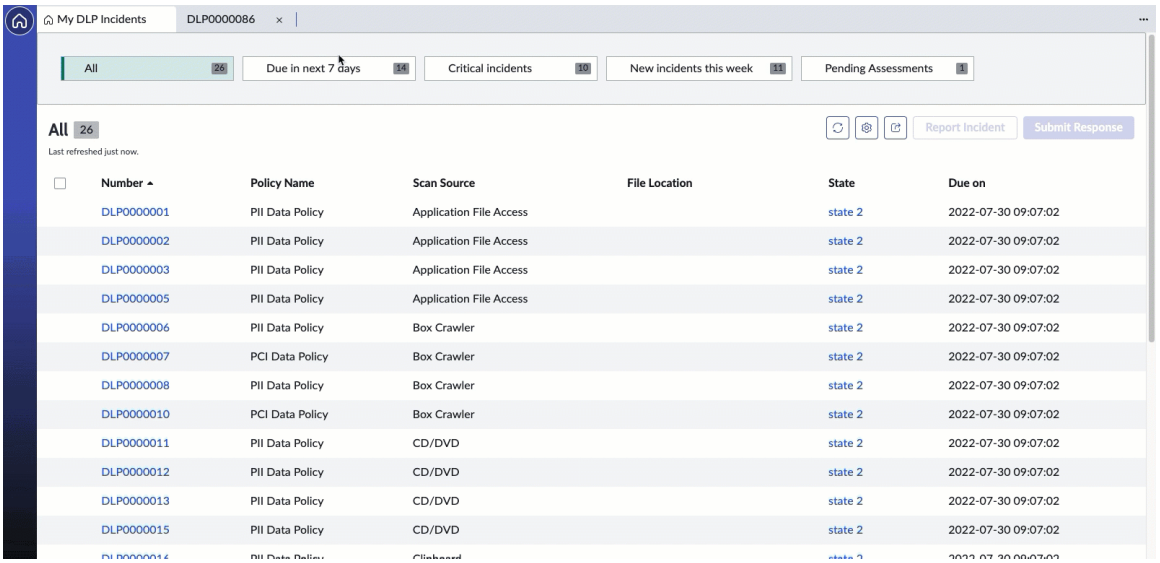
自動翻訳

4. アセスメントを受けるには、[処理待ちのアセスメント] リストビューを選択します。

   a. 特定のアセスメント番号をクリックして開きます。

   b. アセスメントの質問に回答し、要件に基づいて [保存] または [送信] をクリックします。

DLP アセスメント



5. DLP インシデントフォームビューのすべてのフィールドの上部に表示される [指示] カードセクションをクリックして、特定のインシデントに関する追加情報を表示します。

   注:
   ワークスペースのこのセクションでは、インシデント情報に関するガイドをユーザーに提供します。これは、インシデント解決の次のステップを理解する上で役立ちます。

   ユーザー指示カードに表示される 2 種類のヘッダーには、フォームビューの特定のインシデントに関する詳細情報が示されます。追加の詳細情報を確認するには、ユーザー指示ヘッダーをクリックします。

   詳細については、「ユーザー指示テンプレートを作成する」と「DLP UI ユーザー指示の構成」を参照してください。

[自分の承認 **(My Approvals)**] モジュールの操作

ログインユーザーは、DLP ユーザーワークスペースで [自分の承認 (My Approvals)] モジュールを利用できます。ユーザーはここからアサイン承認要求を承認または却下できます。

始める前に

必要なロール：

- エンドユーザー
- マネージャー
- 承認者

手順

1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** ユーザーワークスペース.
   [自分の **DLP** インシデント] ページが新しいタブに表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. [自分の **DLP** インシデント] モジュールの下にある [自分の承認 **(My Approvals)]** モジュールをクリックします。
[自分の承認 (My Approvals)] リストビューが表示されます。

   承認者は、[自分の承認] ページのリストビューから要求を承認または却下できます。リストビューから複数の要求を承認または却下できます。

   承認者は、アサインされた要求の詳細をフォームビューで表示できます。個別の要求を承認または却下するには、フォームビューから [承認] または [却下] アクションをクリックします。

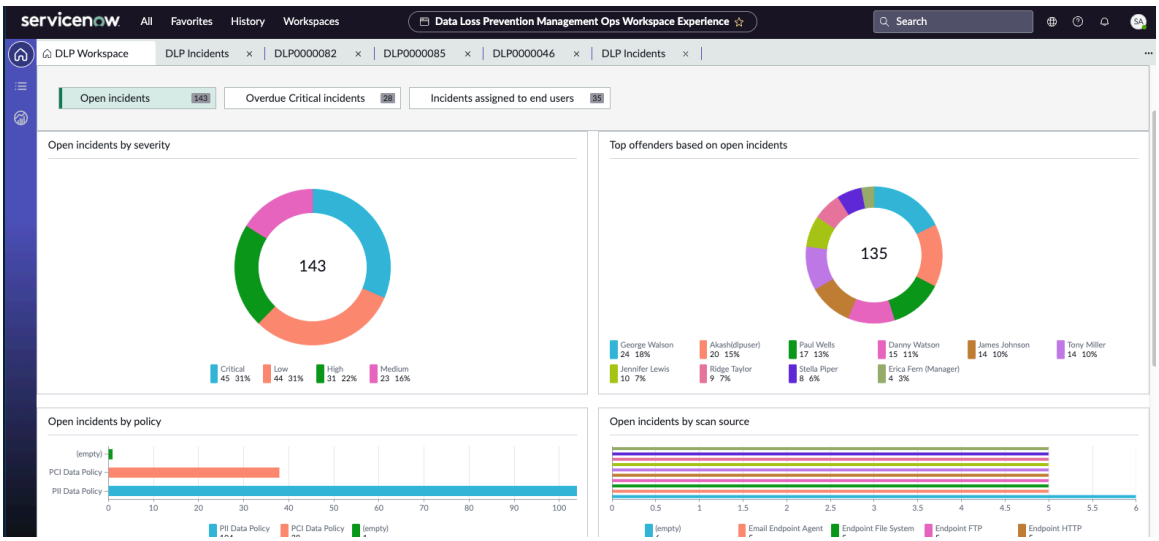
   注:
   DLP インシデントの詳細を表示するには、[承認] フィールドで利用可能な 情報アイコンをクリックします。

Data Loss Prevention Incident Response アナリストワークスペース

Data Loss Prevention Incident Response (DLP IR) アナリストワークスペースを使用して、DLP インシデントを確認します。インシデントを解決などの目的でエンドユーザーにアサインします。

DLP ワークスペースは、DLP インシデントを監視できるダッシュボード、リストビュー、およびフォームビューで構成されています。

DLP ワークスペースの概要ページ



DLP インシデントのレビューとアサイン

Data Loss Prevention Incident Response (DLP IR) アナリストワークスペースにアクセスすると、DLP インシデントを確認して、インシデントをアサインしたり解決したりすることができます。重大度別のインシデント、上位違反者、スキャンソース別のインシデント、ポリシー別のインシデントの傾向を追跡できます。

DLP ワークスペースホームページ

DLP ワークスペースの概要

始める前に
必要なロール：

- sn_dlir.analyst - DLP インシデントの編集および表示。
- sn_dlir.analyst_read および sn_dlir.read - DLP インシデントの表示。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース. DLP ワークスペースの [自分のインシデント] オプションリストページが新しいタブで開きます。
2. **DLP** ワークスペースのホームアイコンをクリックすると、ワークスペースホームページビューが表示されます。
3. ダッシュボードウィジェットを確認して、重大度別のインシデント、上位違反者、スキャンソース別のインシデント、ポリシー別のインシデントの傾向を識別します。
4. ホームページで適切なフィルターをクリックして、各種カテゴリごとにウィジェットを確認します。

フィルター	説明
オープンインシデント	すべてのオープンインシデントを表示します。
期限切れの最重要のインシデント (Overdue critical incidents)	重大度ラベルが「重大」で期限切れのインシデントを表示します。
エンドユーザーにアサインされたインシデント	エンドユーザーにアサインされたすべてのインシデントを表示します。

5. DLP インシデントは、次の 2 つの方法で確認およびアサインできます。

   a. 1 つ目は、確認する 1 つ以上の DLP インシデントを見つけて選択し、そのインシデントの横にあるチェックボックスをクリックする方法です。

   b. 自分に適したオプションを選択します。

オプション	説明
リストを更新	更新を行った場合に DLP インシデントのリストを更新するオプション。
リストアクション	実行できるアクションのリスト。選択肢は次のとおりです。 ▪ 名前を付けて保存 ▪ 列を編集 ▪ 幅をリセット **注:** [自分のリスト] セクションで作成された独自のカスタムリストを、各自のワークスペースに合わせて構成している場合は、以下の追加のリストアクションも実行できます。 ▪ 名前の変更 ▪ 保存 ▪ 削除
すべての URL をコピー (Copy URL for All)	すべての DLP インシデントの URL をコピーするオプション。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
フィルターパネルを表示	フィルターオプションを使用して必要なインシデントをドリルダウンするオプション。 **i.** ページの左上にあるフィルターをクリックし、[詳細ビュー] を選択します。 **ii.** 既存のフィルターを使用するか、フィールド、演算子、および値を含む条件を追加してフィルターを作成します。 **iii.** さらに条件を追加するには、**[AND]** または **[OR]** をクリックします。 ▪ **[AND]** を選択した場合は、すべての条件に一致する必要があります。 ▪ **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。 **iv.** [更新] をクリックします。
インシデントをアサイン	DLP インシデントのアサイン先を決定するアクション。選択肢は次のとおりです。 ▪ インシデントのアサイン先：インシデントをアナリスト、エンドユーザー、または他のユーザーにアサインするオプション。 ▪ ユーザー：インシデントのアサイン先のユーザーを決定するオプション。 ▪ ユーザー応答前のインシデント状況：ユーザーの応答前にインシデントがどのステータスであるべきかを決定するオプション。カスタム状況に設定することもできます。 ▪ アセスメントの添付：インシデントにアセスメントを添付するかどうかを指定するオプション。有効にすると、以下のオプションが利用可能になります。 ▪ アセスメントテンプレート：DLP インシデントのアセスメントテンプレートを選択するオプション。 ▪ ユーザー応答後のインシデント状況：ユーザーの応答後の DLP インシデントのステータスを選択するオプション。
応答	インシデント応答オプションを選択して、インシデントに対応します。たとえば、ユーザーが DLP ポリシーに違反しているファイルを削除した場合、ユーザーは [削除されたファイル] オプションを選択して、ファイルが削除されたことを手動で確認し、コメントを入力できます。 ここから、詳細な応答オプションを選択することもできます。たとえば [隔離からのメールのリリースを要求する **(Request email release from quarantine)]** などです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

オプション	説明
エスカレート	インシデントをエスカレーションするアクション。インシデントをエスカレーションするには、エスカレーション先のユーザーを選択します。[コメント] フィールドに追加情報を入力することもできます。
ステータスの更新	インシデントのステータスを更新するアクション。ドロップダウンオプションからいずれかの状況を選択することで、インシデントの状況を更新できます。カスタム状況に設定することもできます。
クローズ	インシデントをクローズするアクション。ドロップダウンリストから対応するクローズコードを選択し、クローズコメントを追加します。 Data Loss Prevention Incident Response のクローズ機能は、リストビューから非同期と同期の両方で実行されます。 i. 同期クローズ：インシデントを同期的にクローズする場合、クローズアクションがすぐに実行されることを意味します。クローズする複数のインシデントを選択し、インシデント数が 100 以下の場合、インシデントは DLP インシデントリストビューのフォアグラウンドでクローズされます。ここでは、100 がデフォルト値です。 ii. 非同期クローズ：選択したインシデント数が 100 を超える場合に、クローズ要求が送信され、アプリケーションがバックグラウンドで要求を実行することを意味します。 更新されたインシデントステータスを表示するには、DLP インシデントリストビューを更新する必要があります。 注: ▪ 非同期または同期の両方のクローズに対して選択されたインシデント数は、システムプロパティ *sn_dlir.closure_sync_count_limit* を使用して構成されます。 ▪ デフォルトでは、インシデント数は 100 に設定されています。

c. 2 つ目の方法は、特定の DLP インシデントをクリックして開く方法です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [詳細] タブ：次のセクションが表示されます。
  - 詳細：インシデント番号、重大度、ファイル名など、DLP インシデントの詳細を確認できます。また、[重大度]、[ステータス]、[エンドユーザー]、および [DLP アナリストグループ (DLP Analyst group)] の各フィールドを変更して保存することもできます。
  - 作成：全員に表示される DLP インシデントに関するコメントを追加するには、[コメント] タブにコメントを入力します。特定のユーザーに表示されるコメントを追加するには、 [作業メモ (プライベート)] タブにコメントを入力します。
  - アクティビティ：DLP インシデントでのさまざまなアクティビティの詳細を確認できます。
  - 添付ファイル：DLP インシデントに関連する添付ファイルがある場合は、[参照] をクリックしてローカルドライブから添付ファイルを選択します。
- [その他の詳細] タブ：DLP インシデントに関する、カスタムフィールドを含めたその他すべての情報が表示されます。

  重要:
  - DLP インシデントのカスタムフィールドは、San Diego バージョン以降でのみサポートされています。
  - [その他の詳細] タブを使用して、特定の DLP インシデントに対してカスタムフィールドが作成されているかどうかを確認できます。

- [カスタム属性] タブ：DLP インシデントに関連するカスタム属性のリストが表示されます。
- エンドユーザーからのその他のインシデント **(Other incidents from end user)**：同じエンドユーザーからのインシデントを表示します。この関連リストから [子インシデントとして追加 **(Add as child incident)]** アクションを実行することで、インシデントを統合できます。
- 検出された機密情報タイプ **(Detected Sensitive Information Type)**：インシデントで検出された機密情報を表示します。

  注:
  この関連リストは、Microsoft または Symantec の統合で作成された DLP インシデントの場合にのみ表示されます。Microsoft または Symantec のインシデントレコード内で、検出された機密情報タイプのレコードにユーザーがアクセスするたびに、その統合に関連して強調表示された一致コンテンツが表示されます。

- 子インシデント：([子インシデントとして追加 (Add as child incident)] アクションを実行して) 手動で作成された子インシデントまたは DLP 統合ルールから作成された子インシデントを表示します。この関連リストから [子インシデントのリンクを解除 (Unlink child incident)] を実行することで、子インシデントのリンクを解除できます。
- クローンされたインシデント **(Cloned incidents)**：親インシデントからクローンされたインシデントを表示します。フォームビューの [インシデントをクローン **(Clone incident)]** アクションをクリックすると、新しいクローンインシデントを作成できます。
- [アセスメント] タブ：DLP インシデントにアサインされているアセスメントのリストを表示します。

d. 自分に適したオプションを選択します。

オプション	説明
インシデントをアサイン	DLP インシデントのアサイン先を決定するアクション。選択肢は次のとおりです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

オプション	説明

	▪ インシデントのアサイン先：インシデントをアナリスト、エンドユーザー、または他のユーザーにアサインするオプション。
	▪ ユーザー：インシデントのアサイン先のユーザーを選択するオプション。
	▪ ユーザー応答前のインシデント状況：ユーザーの応答前にインシデントがどのステータスであるべきかを選択するオプション。カスタム状況に設定することもできます。
	▪ アセスメントの添付：インシデントにアセスメントを添付するかどうかを指定するオプション。有効にすると、以下のオプションが利用可能になります。
	  ▪ アセスメントテンプレート：DLP インシデントのアセスメントテンプレートを選択するオプション。
	  ▪ ユーザー応答後のインシデント状況：ユーザーの応答後に DLP インシデントがどのステータスであるべきかを選択するオプション。

承認をキャンセル	承認要求をキャンセルするアクション。 このアクションは、DLP インシデントのステータスが [承認待ち **(Pending Approval)**] である場合にのみ、フォームビューでアナリストに対して表示されます。使用可能なオプションは、次のとおりです。 ▪ インシデントのアサイン先：インシデントのアサイン先として、[該当者なし]、[アナリスト]、または [他の人] を設定するオプション。 ▪ ユーザー：インシデントのアサイン先のユーザーを選択するオプション。 ▪ キャンセル後のインシデントのステータス **(Post cancellation incident state)**：要求をキャンセルした後のインシデントのステータスを選択するオプション。 ▪ コメント：キャンセルに関する追加の詳細を入力します。
アセスメントをアサイン	インシデントのアサイン時にアセスメントを添付するアクション。選択肢は次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

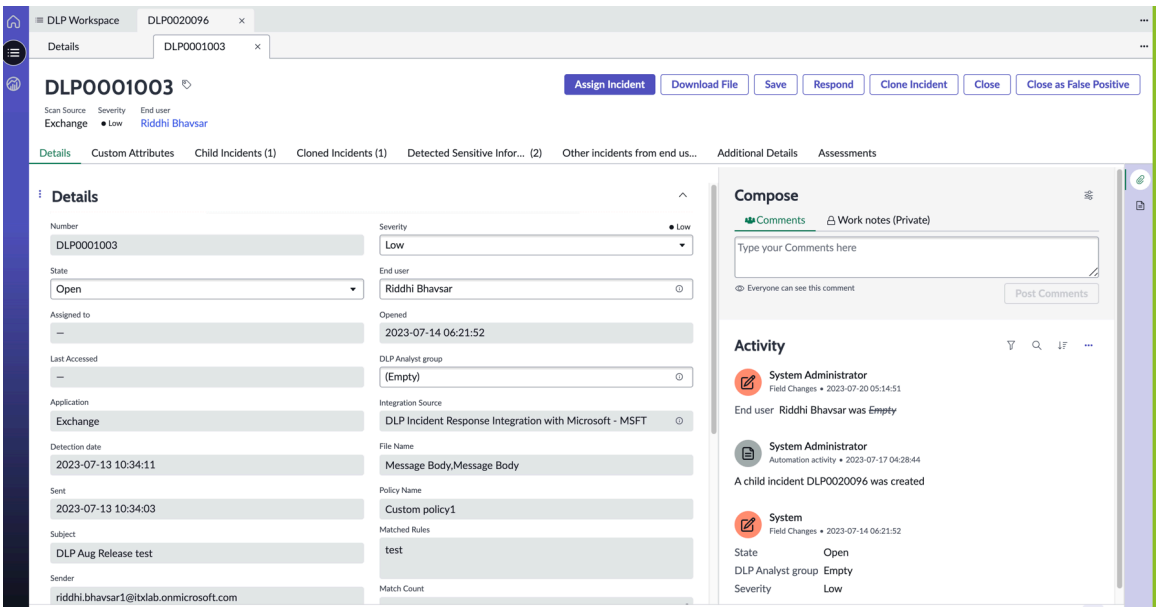
オプション	説明
	▪ アセスメントテンプレート：DLP インシデントのアセスメントテンプレートを選択するオプション。 ▪ ユーザー応答後のインシデント状況：ユーザーの応答後に DLP インシデントがどのステータスであるべきかを選択するオプション。
ファイルのダウンロード	違反コンテンツを含むファイルまたはメールをダウンロードするアクション。このアクションは、Microsoft OneDrive、SharePoint Online、または Exchange Online について作成されたインシデントに対して実行できます。
保存	行った変更を保存するアクション。DLP インシデントの [重大度]、[ステータス]、および [エンドユーザー] フィールドを変更して保存することができます。
応答	インシデント応答オプションを選択して、インシデントに対応します。たとえば、ユーザーが DLP ポリシーに違反しているファイルを削除した場合、ユーザーは [削除されたファイル] オプションを選択して、ファイルが削除されたことを手動で確認し、コメントを入力できます。 ここから、詳細な応答オプションを選択することもできます。例：[隔離からのメールのリリースを要求する **(Request email release from quarantine)]**
エスカレート	インシデントをエスカレーションするアクション。インシデントをエスカレーションするには、エスカレーション先のユーザーを選択します。[コメント] フィールドに追加情報を入力することもできます。
インシデントをクローン (Clone Incident)	インシデントレコードが複数のユーザーに影響する場合にクローンインシデントを作成するアクション。クローンされたインシデントは、法務/IT などの複数のステークホルダーにアサインできます。 クローンインシデントレコードを作成すると、親 DLP インシデントの下に新しい [クローンされたインシデント **(Cloned incidents)]** タブが作成され、すべてのクローンインシデントがこのビューに一覧表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
	注: ▪ 親 DLP インシデントレコードがクローズされると、すべてのクローンインシデントレコードが自動的にクローズされます。 ▪ DLP インシデントレコードにクローンインシデントが含まれている場合、そのレコードをエンドユーザーにアサインすることはできません。親 DLP インシデントレコードは、アナリストのロールを持つユーザーのみが管理できます。 ▪ [デフォルト構成] モジュールでのクローンインシデントのステータスに基づいて親ステータスを自動的に更新するオプションもあります。たとえば、すべてのクローンインシデントが [エスカレート済み] ステータスに移行すると、親インシデントも [エスカレート済み] ステータスに移行します。
クローズ	インシデントをクローズするアクション。ドロップダウンリストから対応するクローズコードを選択し、必要に応じてクローズコメントを追加する必要があります。
誤検出としてクローズ	インシデントを誤検出としてクローズするアクション。インシデントをクローズする前に、コメントを追加することもできます。

DLP アナリストワークスペース



6. ホームページからリストビューを表示するには、ページの左上にある [リスト] タブをクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

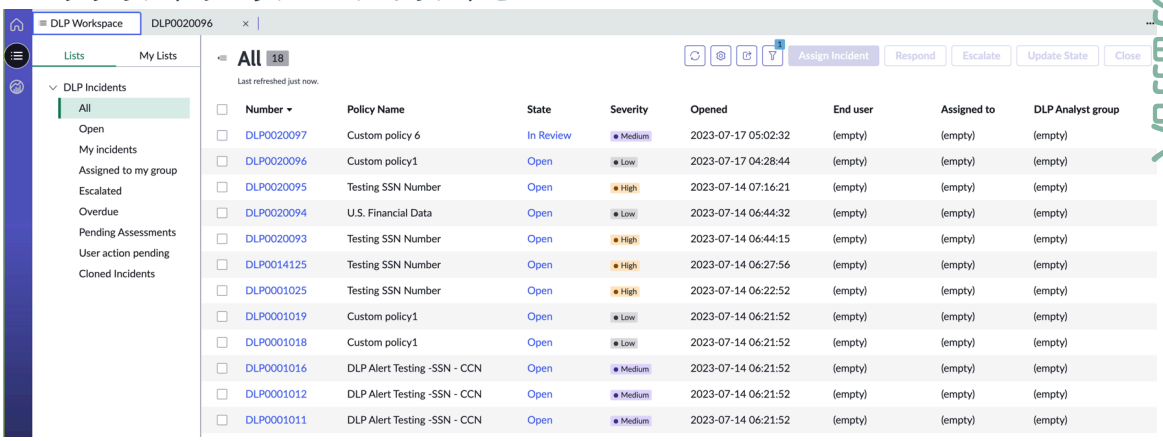
[リスト] カテゴリは、DLP インシデントのデフォルトのリストページとカスタマイズされたリストページで構成されています。

- [リスト] タブ：DLP インシデントのデフォルトのリスト。デフォルトのリストは次のとおりです。
  - すべて
  - オープン
  - 自分のインシデント
  - 自分のグループにアサイン済み
  - エスカレート済み
  - 期限切れ
  - 処理待ちのアセスメント
  - 処理待ちのユーザーアクション
  - クローンされたインシデント
  - アーカイブ化済みインシデント
- [自分のリスト] タブ：自分が名前を変更したリストと作成したリストが表示されます。

Example

次の例は、リストビューカテゴリを含む DLP ワークスペースを示しています。[すべて] リストビューオプションが選択されています。

DLP アナリストワークスペースのリストビュー



証拠ファイルのプレビュー

DLP IR アナリストワークスペースで Data Loss Prevention Incident Response 証拠ファイルをプレビューします。

始める前に

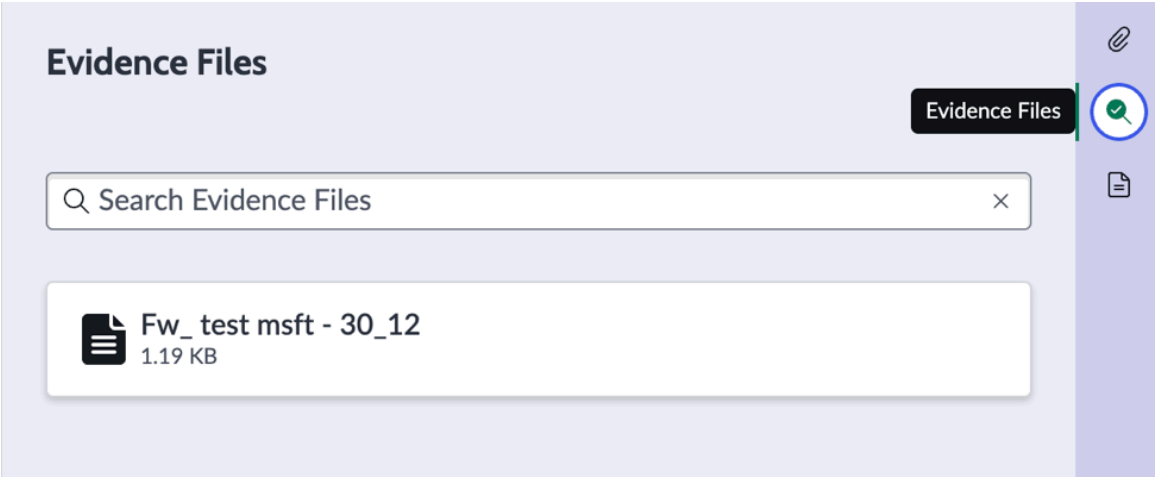
重要:
DLP アナリストワークスペースで証拠ファイルアクションを使用している間、証拠ファイルは暗号化されていない形式で ServiceNow データベースに一時的に保存されます。証拠ファイルを保存しない場合は、証拠ファイルのプレビュー機能を無効にします。詳細については、「詳細設定を構成します」を参照してください。

必要なロール：sn_dlir.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.
2. DLP インシデントレコードを開きます。
3. コンテキストサイドバーにある証拠ファイル) を選択します。
4. [証拠ファイル] タブで、 証拠ファイル カードを選択して、ドキュメントビューアーで証拠ファイルをプレビューします。



プレビュー機能は、次の表に示すように、ファイルタイプごとに異なります。

ファイル形式	ファイル拡張子
イメージ	.bmp、.gif、.ico、.jpeg、.jpg、.png、.svg、および .webp。 画像ファイルはドキュメントビューアーモードで開きます。
Microsoft Office ファイル	.doc、.docx、.ppt、.pptx、.xls、.xlsx Office ファイルはドキュメント ビューアーモードで開きます。
テキストファイル	.txt テキストファイルはテキストエディターモードで開きます。
メールファイル	.eml **注:** ファイルサイズは 5MB 未満である必要があります。コンテンツをプレビューするには、まずファイルをダウンロードする必要があります。
PDF ファイル	.pdf

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ファイル形式	ファイル拡張子
	○ キーワードを入力してドキュメントを検索します。 ○ ビューを調整して読みやすくするためのズームインおよびズームアウト機能。 ○ コンテンツをより鮮明に表示するには、ページを時計回りまたは反時計回りに回転させます。

注:

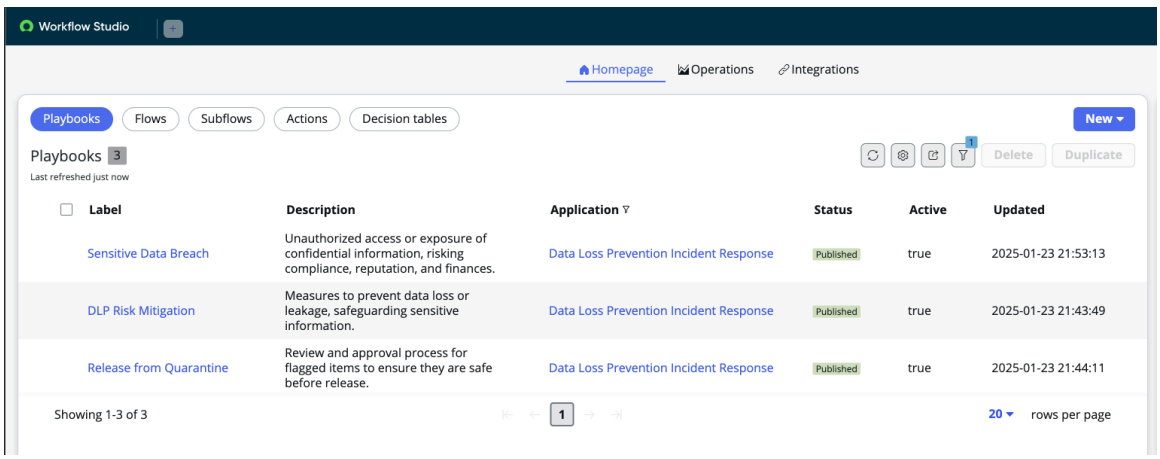
バイナリファイルはレンダリングされないため、コンテンツをプレビューするにはダウンロードする必要があります。証拠ファイルのプレビュー機能は、アーカイブされたインシデントでも機能します。

のプレイブック **Data Loss Prevention Incident Response**

Data Loss Prevention Incident Responseプレイブックは、組織のセキュリティを侵害する可能性のある機密情報の不正な公開、漏洩、または侵害を含むデータ損失インシデントに対処し、軽減するためのステップバイステップガイドです。

次の図は、DLP IR で利用可能なプレイブックのサンプルを示しています。

DLP インシデント応答のサンプルプレイブック



次の表に、プレイブックの作成に関連するアクティビティとステージを示します。詳細については、DLP プレイブックを追加を参照してください。

アクティビティ	説明
検出	機密データへの不正アクセスや公開を特定して確認します。
格納	影響を受けるシステムまたはユーザーを隔離して、さらなるデータ漏洩や不正アクセスを防止します。
調査	侵害を調査して、侵害がどのように発生したか、どのデータが影響を受けたか、および潜在的な影響について理解します。

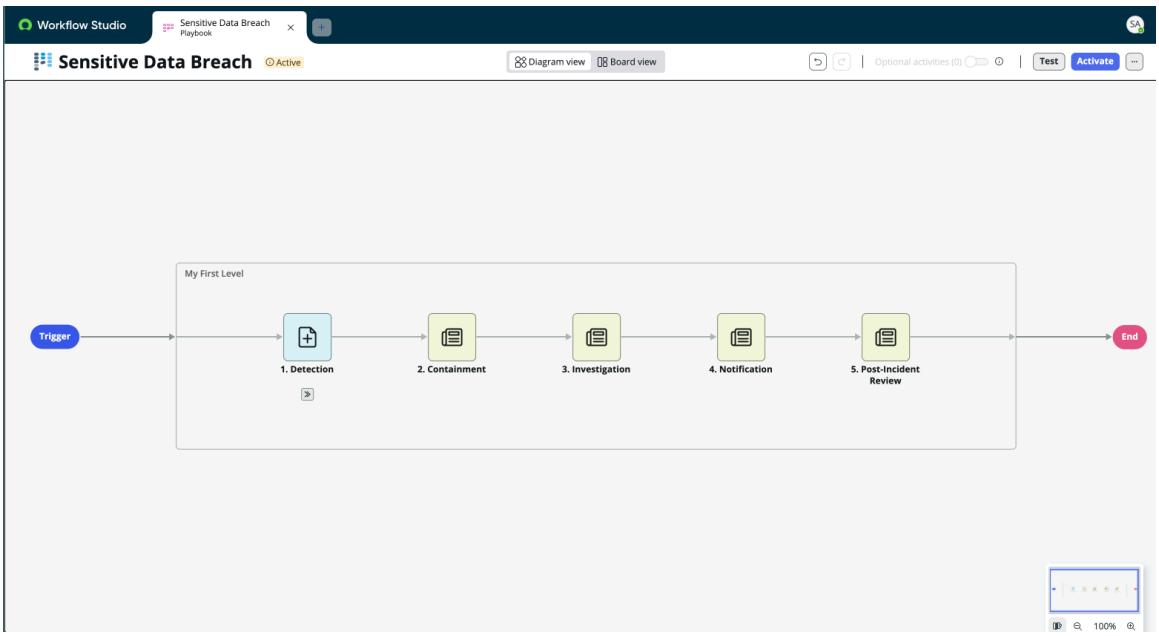
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクティビティ	説明
通知	法律またはポリシーの要求に応じて、社内チーム、外部のステークホルダー、および規制機関に通知します。
修復	是正措置を適用して、脆弱性に対処し、ポリシーを更新し、将来の侵害を防止します。
復旧	安全なバックアップからシステムを復元し、インシデント後のデータの整合性を検証します。
インシデント後レビュー	インシデントを分析して根本原因を特定し、セキュリティコントロールを改善し、ポリシーを強化します。

次の図は、プレイブックの作成に関連するアクティビティとステージのワークフローを示しています。

プレイブック設計ワークフロー



注:
これは、機密データ侵害のサンプルプレイブックです。プレイブックのタイプによっては、ワークフローが変更される場合があります。

関連情報

DLP プレイブックを追加

DLP プレイブックをキャンセル

DLP プレイブックを追加

組織のセキュリティを侵害する可能性のあるデータ損失インシデントに対処して軽減するためのガイドとして機能するプレイブックを Data Loss Prevention Incident Response アナリストワークスペースに追加します。

始める前に

必要なロール:sn_dlir.analyst - DLP ワークスペースでプレイブックを追加または表示します。

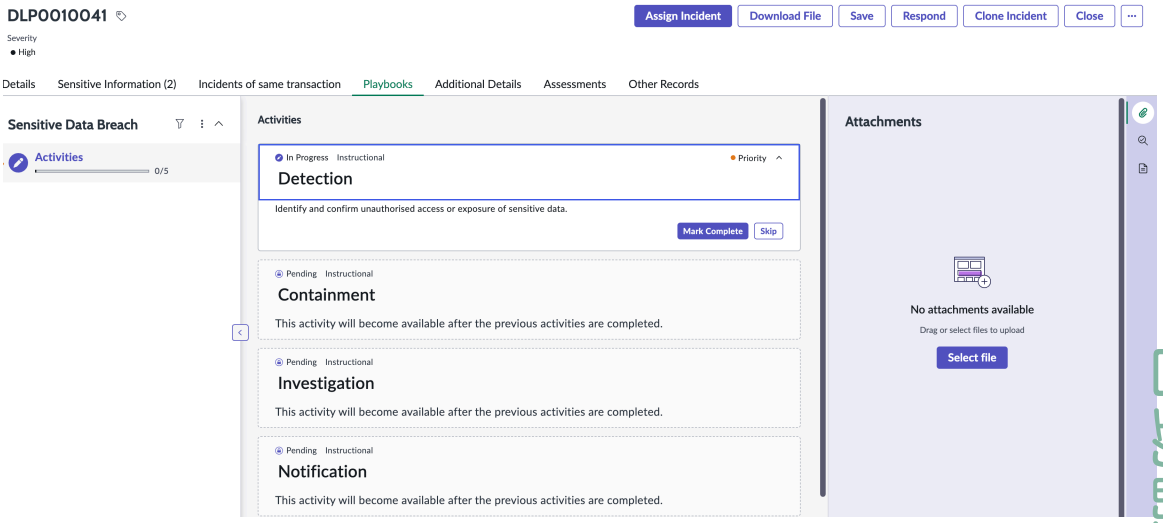
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.
2. [DLP アナリストワークスペース - 自分のインシデント] ページで、DLP インシデントを開きます。
3. [プレイブック] タブに移動します。
4. メニューから [プレイブックを追加] を選択し、ドロップダウンメニューからプレイブックを選択します。
5. [プレイブックを追加] を選択します。
6. 各レーンを選択して、このプレイブックが実行するタスクを確認します。

DLP プレイブックのサンプル



DLP プレイブックをキャンセル

Data Loss Prevention Incident Responseプレイブックが無効になったときにビジネスフローをキャンセルして停止します。

始める前に

> **注:**
> プレイブックは、関連する DLP インシデントがクローズされると自動的にキャンセルされます。

必要なロール：sn_dlir.admin

手順

1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.
2. 任意の DLP インシデントを開きます。
3. [プレイブック] タブに移動します。
4. キャンセルするプレイブックのヘッダーで、 アイコンを選択し、[プレイブックをキャンセル] を選択します。
5. このプレイブックをキャンセルする理由を入力します。
6. [プレイブックをキャンセル] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスクの結果
プレイブックのヘッダーの下に、プレイブックがキャンセルされたことを確認するバナーが表示されます。

アーカイブされた **DLP** インシデントの表示

DLP アナリストワークスペースを使用して、アーカイブされた DLP インシデントを表示します。

始める前に
必要なロール：

- sn_dlir.analyst - DLP インシデントの編集および表示。
- sn_dlir.analyst_read および sn_dlir.read - DLP インシデントの表示。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.
   デフォルトでは、[自分のインシデント] セクションが表示されます。
2. [アーカイブ化済みインシデント] をクリックします。
   アーカイブ化済み DLP インシデントのリストが表示されます。
3. [インシデント数を表示 **(Show Incidents Count)**] ボタンをクリックして、アーカイブされたインシデント数を表示します。

   注:
   - デフォルトでは、リストのロード時間を短縮するためにアーカイブされたインシデント数は非表示になっており、インシデント数を表示するには、[インシデント数を表示 **(Show Incidents Count)**] ボタンをクリックする必要があります。また、インシデント数を示す情報メッセージが表示されます。
   - アーカイブされたインシデントのベースシステムでシステムプロパティ glide.ui.list.seismic.omit.count が有効になり、インシデントリスト数が非表示になります。

4. 表示する 1 つ以上の DLP インシデントを選択します。
   DLP インシデントに [インシデントの詳細] セクションが表示されます。

   注:
   - [エンドユーザーからのその他のインシデント **(Other incidents from end users)**] タブには、アーカイブされたインシデントも含まれます。
   - [一致コンテンツ] はアーカイブされたすべてのインシデントでサポートされますが (すべての統合でもサポートされます)、[ファイルのダウンロード] は Microsoft 統合でのみサポートされます。

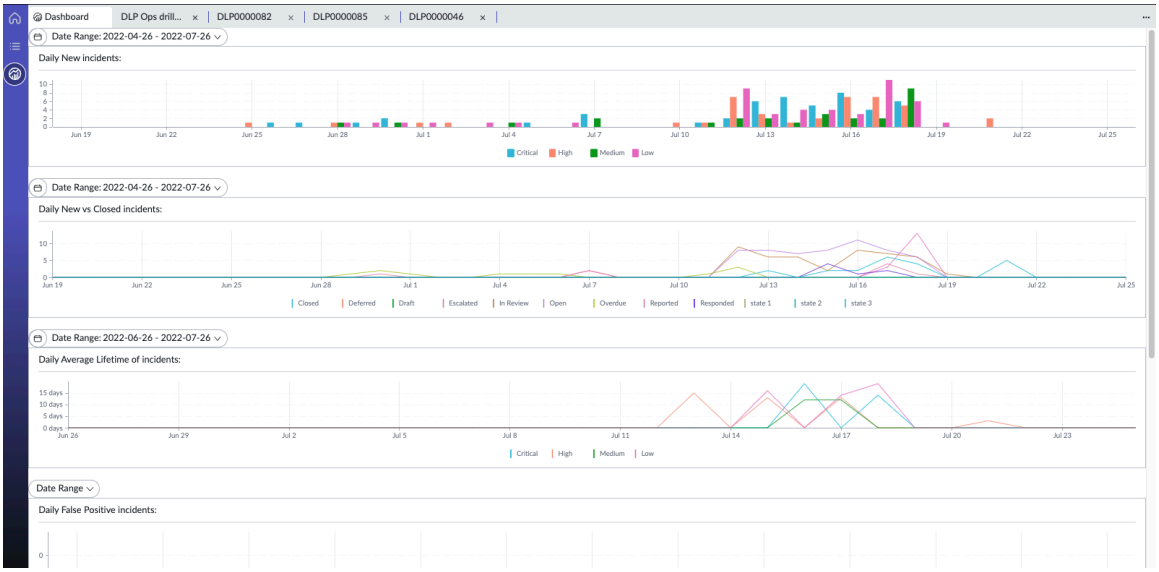
Data Loss Prevention Incident Response ダッシュボード

Data Loss Prevention Incident Response (DLP IR) ダッシュボードでは、インスタンス内の DLP インシデントと日次インシデントの傾向の概要がグラフの形式で示されます。これらのグラフは、DLP インシデントを効果的に確認、管理、および修復するために役立ちます。

Data Loss Prevention Incident Response ダッシュボードには、毎日の DLP インシデントに関する重要なインサイトが表示されます。インジケーターを設定して、インジケータープロパティの条件に一致するインシデントのデータスナップショットを定期的に収集できます。収集されたデータは、ダッシュボードのウィジェットを使用してビジュアル化されます。さまざまな時間間隔で DLP インシデントを分析するために、さまざまな日付範囲を適用できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

DLP ダッシュボード



DLP インシデントの日次インシデント傾向の分析

Data Loss Prevention Incident Response (DLP IR) ダッシュボードにアクセスして、DLP インシデントの日次傾向を分析し、効果的にインシデントを修正します。

始める前に

必要なロール：

- sn_dlir.analyst - DLP インシデントの編集および表示。
- sn_dlir.analyst_read および sn_dlir.read - DLP インシデントの表示。

このタスクについて

DLP ダッシュボードのウィジェットを使用して、日次の傾向をビジュアル化できます。DLP インシデントの日次傾向のデータや統計情報は、組織で定義されている日次インシデントのインジケータープロパティから収集されます。さまざまなデータ範囲を適用して、次のグラフに対してさまざまな時間間隔で DLP インシデントを分析することで、重要なインサイトを得ることができます。

- 日次新規インシデント：インシデントのステータスに関係なく、毎日作成される DLP インシデント全体のデータ。DLP インシデントは、中、重大、高、低などの重大度に基づいて分類されます。DLP インシデントの重大度は、それぞれ特定の色でグラフ上に表されます。
- 日次新規インシデント対クローズ済みインシデント：DLP インシデントのさまざまな状況および、日次新規インシデントとクローズ済みインシデントの比較。日次新規のカテゴリには、オープン、ドラフト、エスカレート済み、レビュー中、期限切れ、レポート済み、またはカスタム (あれば) のステータスの DLP インシデントがすべて含まれます。クローズ済みインシデントのカテゴリには、クローズ済みの DLP インシデントが含まれます。DLP インシデントのステータスは、それぞれ特定の色でグラフ上に表されます。
- インシデントの日次平均存続時間：インシデントの存続時間は、特定の DLP インシデントのオープンからクローズまでの時間です。日次平均存続期間は、クローズ済みの DLP インシデントに対してのみ計算されます。
- 日次誤検出インシデント：日次の誤検出として報告されたすべての DLP インシデントのデータ。日次語検出インシデントは、中、重大、高、低などの重大度に基づいて分類されます。日次誤検出インシデントの重大度は、それぞれ特定の色でグラフ上に表されます。
- インシデントの経過時間と重大度：すべての DLP インシデントのデータを、経過時間で分類し、DLP インシデントの重大度で構成した比較。経過時間のカテゴリには、組織が定義した経過時間に到達していないすべての DLP インシデントが含まれます。年齢グラフの詳細については、「経過時間グラフ構成を作成する」を参照してください。インシデントの重大度には、[高] または

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

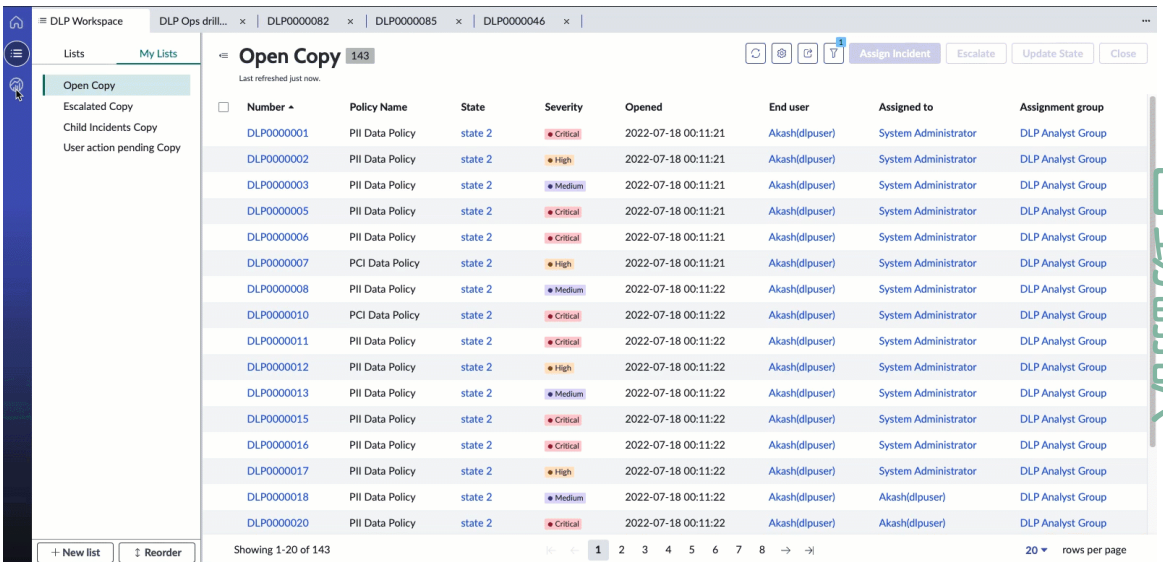
[低] カテゴリのすべての DLP インシデントが含まれます。重大度は、それぞれ特定の色でグラフ上に表されます。

- 日次エスカレーション済みインシデント：日次エスカレーションされたすべての DLP インシデントのデータ。日次エスカレーション済みインシデントは、中、重大、高、低などの重大度に基づいて分類されます。日次エスカレーション済みインシデントの重大度は、それぞれ特定の色でグラフ上に表されます。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** ダッシュボード.
   [自分の DLP ダッシュボード (My DLP Dashboard)] ページが新しいブラウザータブに表示されます。
2. 日次傾向分析を実行するダッシュボードウィジェットを選択します。
   たとえば、[日次新規インシデント] グラフなどです。
3. ダッシュボードウィジェットを確認して傾向を特定します。
4. [日付範囲]をクリックします。

DLP ダッシュボードの概要



5. カレンダーから日付範囲を選択し、[適用] をクリックします。

   Example
   たとえば、選択したデータ範囲に対して日次新規インシデントグラフが更新されます。
6. グラフの下にあるフィルターを使用してドリルダウンし、より詳細な分析を実行します。

Data Loss Prevention Incident Response のインバウンド統合

受信 REST API を使用して、単一または複数の DLP インシデントを作成します。

単一の DLP インシデントの作成

必要なロール：sn_dlir.api_integration_user

単一の DLP インシデントを作成するには、必要に応じて次のパラメーターを定義します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
HTTP メソッド	`POST`
URL	https://{instance}/api/now/import/sn_dlir_incident_import
要求ヘッダー	Accept： `application/json` Content-Type： `application/json`

サンプルペイロード	{
	"application_window_title": "<value>",
	"assigned_to": "<value>",
	"attachments": "<value>",
	"data_owner_email": "<value>",
	"destination": "<value>",
	"dest_ip": "<value>",
	"dest_ip_port": "<value>",
	"detection_date": "<value>",
	"endpoint_on_corporate_net": "<value>",
	"files": "",
	"file_created": "",
	"file_created_by": "",
	"file_location": "",
	"file_modified_by": "",
	"file_name": "",
	"file_owner": "",
	"file_permissions": "",
	"ftp_user_name": "",
	"last_modified": "",
	"machine_ip": "",
	"machine_name": "",
	"match_count": "",
	"policy_id": "",
	"policy_name": "",
	"printer_name": "",
	"printer_type": "",
	"print_job_name": "",
	"recipients": "",
	"scanned_machine": "",
	"scan_source": "",
	"seen_before": "",
	"sender":"",
	"source":"",
	"source_file":"",
	"source_ip":"",
	"source_ip_port":"",
	"subject":"",
	"url":"",
	"user_justification":""
	}

サンプル応答	{ "import_set": "ISET0010003",

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明

	"staging_table": "sn_dlir_incident_import",
	"result": [
	{
	"transform_map": "",
	"table": "sn_dlir_incident",
	"display_name": "number",
	"display_value": "DLP0001012",
	"record_link":
	"https://{instance}/api/now/table/sn_dlir_incident/7cda322297c2411056a43d1e6253af1f",
	"status": "inserted",
	"sys_id": "7cda322297c2411056a43d1e6253af1f"
	}
	]
	}

複数の **DLP** インシデントの作成

必要なロール：sn_dlir.api_integration_user

同じ要求から複数の DLP インシデントを作成するには、必要に応じて次のパラメーターを定義します。

フィールド	説明
HTTP メソッド	*POST*
URL	https://{instance}/api/now/import/sn_dlir_incident_import/insertMultiple
要求ヘッダー	Accept： *application/json* Content-Type： *application/json*
サンプルペイロード	{ "records": [{ "file_name": "<value>", "file_modified_by": "<value>", "work_notes": "<value>", "url": "<value>", "scan_source": "<value>", "data_owner_email": "<value>", "file_created_by": "<value>", "file_owner": "<value>", "policy_name": "<value>" }, { "dest_ip": "<value>", "dest_ip_port": "<value>", "detection_date": "<value>", "endpoint_on_corporate_net": "<value>",

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	"files": "<value>", "file_created": "<value>", "file_created_by": "<value>", "file_location": "<value>", "file_modified_by": "<value>", "file_name": "<value>", "file_owner": "<value>", }] }

サンプル応答	{
	"import_set_id": "a38f69229734dd1056a43d1e6253af75",
	"multi_import_set_id":
	"e78f69229734dd1056a43d1e6253af75"
	}

注:
デフォルトでは、変換は非同期です。同期変換を設定するには、REST での複数挿入 [sys_rest_insert_multiple] テーブルに新しいレコードを作成し、ソーステーブルに **sn_dlir_incident_import** を選択して、変換を[同期]に設定します。

DLP 統合

Data Loss Prevention Incident Response ベースシステムには、サードパーティのデータ損失防止ソフトウェアパッケージへの統合機能が含まれています。

このセクションでは、プラグインを有効にし、ServiceNow とサードパーティの両方の統合機能を設定する手順について説明します。また、独自の統合を開発するための基本的なガイドラインと、ベースシステムに含まれる特定の統合についても詳しく説明します。

統合設定

ベースシステムには、有効化して使用できるそれぞれの統合実装に対する一連のカードがあります。また、セキュリティオペレーション プラグインに依存する ServiceNow Store に投稿された統合についてもカードが表示されます。統合カードを表示するには、次を選択します。 セキュリティオペレーション > 統合設定.

Data Loss Prevention Incident Response は、次に挙げるサードパーティのデータ損失防止ソフトウェアパッケージをサポートしています。

Data Loss Prevention Incident Response に対する Symantec の統合

Symantec DLP 統合では、Symantec Data Loss Prevention Incident Response の展開時に作成された Data Loss Prevention Incident Response インシデントの取り込みをサポートしています。取り込み後に、DLP インシデントを修復するインシデント管理機能を使用できます。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースメモ情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

概要と主な機能

Symantec DLP 統合を使用することで、さまざまなプラットフォームでの機密データの取り扱いや移動を追跡できます。

この統合の主な機能は次のとおりです。

- Symantec のさまざまな API エンドポイントに対して複数の統合プロファイルを作成する機能。
- Symantec から ServiceNow インスタンスへの DLP インシデントのスケジュールされた取り込み。
- API フィルターを適用してフィルター基準に一致するインシデントを取得し、インポートする必要がある Symantec DLP インシデントのフィルターを指定する機能。
- ServiceNow インスタンスの DLP インシデント状況の Symantecの DLP インシデント状況へのマッピング。
- ServiceNow インスタンスでのステータス変更時の、Symantec のインシデント状況の自動更新。
- Symantec DLP インシデントと ServiceNow インシデント間の重大度マッピングをカスタマイズおよび定義する機能。

統合の詳細については、シマンテック製品のドキュメント を参照してください。

Symantec DLP integration for Data Loss Prevention の概要

統合を使用する前に、ServiceNow® Store からダウンロードする必要があります。

チェックリスト

Symantec DLP integration for Data Loss Prevention の設定を開始する前に、次の情報を確認します。

チェックリスト

フィールド	説明
必要な Now Platform、Data Loss Prevention アプリケーション、および MID アプリケーションのロールをアサインしていることを確認します。	Now Platform 上の Symantec DLP 統合全体で、次のロールを使用します。 • アドミン (admin) が ServiceNow® Store からアプリケーションをインストールし、データ損失防止アドミン (sn_dlir.admin) をアサインする。 • sn_dlir.admin ロールを持つユーザーが、統合を構成し、インシデントプロファイルを設定できる。 • sn_dlir.analyst ロールを持つユーザーが、統合全体での読み取りロールを持つことになる。
必要な Symantec DLP ユーザーロールをアサインする。	Symantec DLP 統合ロールと権限をレビューします。
Symantec DLP 15.8 を使用していることを確認します。	Symantec DLP integration for Data Loss Prevention は、Symantec Data Loss Prevention のバージョン 15.8 でテストされています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト (続く)

フィールド	説明
	注: Symantec DLP 15.8 を使用していることを確認します。
Symantec DLP 統合のサポートに必要な ServiceNow コアアプリケーションがインストールされてアクティブ化されていることを確認します。	以下の DLP アプリケーションと Security Support Common アプリケーションが ServiceNow Store からインストールされてアクティブ化されていることを確認します。インストールされていない場合は、 アプリケーションをインストールしてアクティブ化します。 • Security Support Common • Data Loss Prevention Incident Response

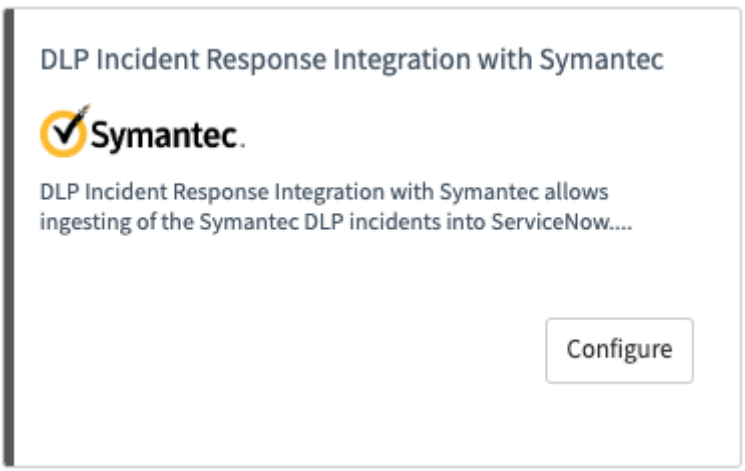
Symantec DLP integration for Data Loss Prevention のインストールおよび構成

ServiceNow Store から Now Platform インスタンスに Symantec DLP 統合をインストールして構成します。Symantec DLP インシデントデータを使用して DLP インシデントの調査調査を開始します。

始める前に
必要なロール：sn_dlir.admin

手順

1. Symantec DLP 統合から ServiceNow Store をダウンロードしてインストールします。
2. 次のように移動する。 セキュリティオペレーション > 統合 > 統合設定.
3. [DLP Incident Response Integration with Symantec] タイルを検索して、[構成] をクリックします。

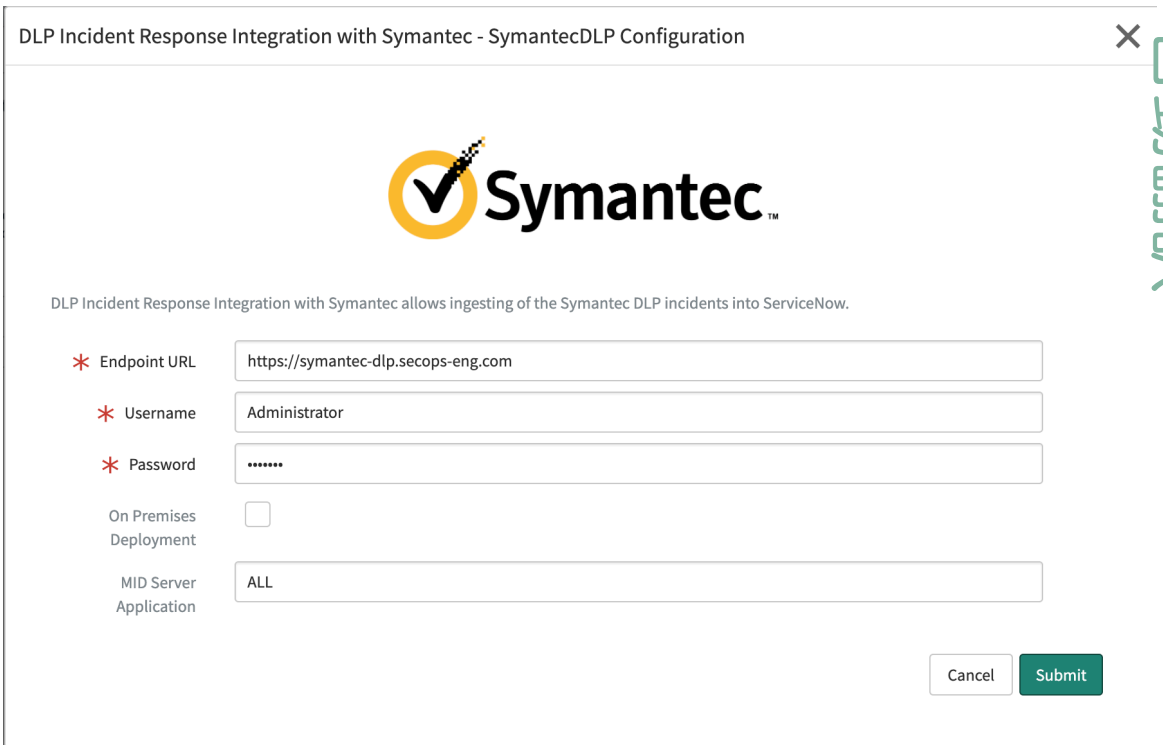


4. フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[Symantec DLP 統合構成 (Symantec DLP Integration Configuration)] フォーム

フィールド	説明
名前	Symantec DLP 統合構成の名前。
エンドポイント URL	Symantec REST API エンドポイント。
ユーザー名	Symantec アカウント名。必要なロールと権限の詳細については、「ロールと権限」を参照してください。
パスワード	Symantec アカウントのパスワード。
オンプレミス展開	Symantec がオンプレミスのインスタンスに展開されている場合に選択できるオプション。このオプションを選択する場合は、MID サーバーを使用して Symantec に接続する必要があります。
MID サーバーアプリケーション	Symantec との通信に使用される MID アプリケーションの名前。 [オンプレミス展開] オプションを選択する場合にこのフィールドが必要です。



自動翻訳

5. [**Submit** (送信)] を選択します。

タスクの結果

注:
symantec sub prod を ServiceNow sub prod に接続してください。アカウントがログアウトされないように、インスタンス間ですべてのユーザー名とパスワードの同期を維持します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

構成の検証と送信が正常に完了すると、Symantec DLP 統合が [セキュリティ統合] ページにタイルとして保存されます。

Symantec DLP 統合のプロファイルの作成

Now Platform インスタンスにインシデントプロファイルを作成します。DLP インシデントの作成に適した Symantec DLP インシデントを判断します。

始める前に
必要なロール：sn_dlir.admin

このタスクについて
Symantec エンドポイントから DLP インシデントを取得するように Now Platform® を構成します。取得したインシデントは DLP インシデントとして ServiceNow インスタンスに格納します。

手順

1. 次のように移動する。 **Symantec DLP** 統合 > インシデントプロファイル.
2. [**New**] をクリックします。
3. フォームで [名前] セクションのフィールドを入力します。

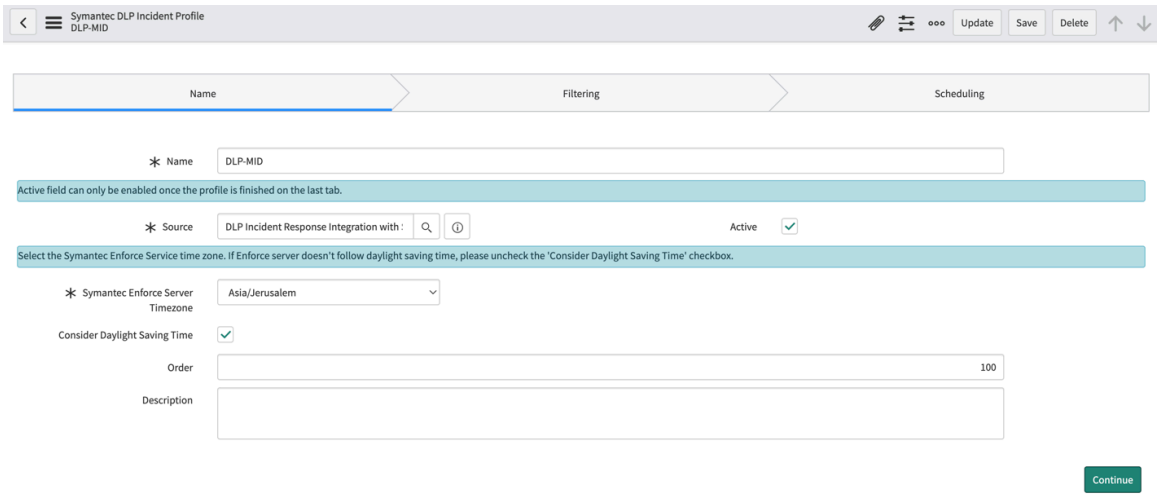
プロファイルの作成

フィールド	説明
名前	プロファイルの名前。このフィールドでプロファイルを識別できます。 **注:** プロファイルごとに名前は一意である必要があります。
ソース	インシデントを取り込むように構成した Symantec DLP インスタンス。複数のインスタンスが構成されている場合は、プロファイルに取り込む予定のインシデントタイプに適したインスタンスを選択します。
アクティブ	プロファイルがアクティブかどうかを示すオプション。このフィールドは、[スケジューリング] セクションで [完了] をクリックした後にのみアクティブになります。 プロファイルがアクティブな場合は、Now Platform が Symantec DLP インシデントをアクティブにポーリングしていることを暗示しています。入力したフィルター条件が [スケジューリング] パラメーターに基づいて一致すると、対応する DLP インシデントが DLP 内に作成されます。
Symantec サーバータイムゾーンを適用	タイムゾーンの問題が原因でインシデントが見逃されることがないようにするため、プロファイルで symantec Enforce Server のタイムゾーンを選択します。
夏時間を考慮	サーバーが夏時間に準拠している場合は、このチェックボックスをオンにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
順序	プロファイルの実行順序。順序の値が最も小さいプロファイルの優先度が最も高いと見なされます。 デフォルト値は 100 です。
説明	このプロファイルの固有の説明。



次のタスク
[フィルタリング] セクションに移動するには、[続行] をクリックします。

インシデント作成の際に適用するフィルターの定義

フィルター条件を定義および設定して、受信される Symantec DLP インシデントをドリルダウンします。ServiceNow で DLP インシデントとして作成する必要のあるインシデントを決定します。

始める前に
必要なロール：sn_dlir.admin

このタスクについて
フィルタリングを行うことで、DLP インシデントを切り分け、作成する DLP インシデントの数を制限することができます。それ以外のフィルタリング基準が設定されている場合は、その条件に一致するインシデントのみが作成されます。

手順

1. API フィルターを適用し、フィルター基準に一致するインシデントを取得するには、[インシデント取り込み用の **API** ベースのフィルター **(API based filter for incident ingestion)]** チェックボックスをオンにします。
2. API フィルターを追加します。
   API フィルターを示す例を次に示します。

```
{
            "operandOne": {
               "name": "incidentStatusName"
            },
            "filterType": "string",
            "operator": "EQ",
            "operandTwoValues": [
```

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

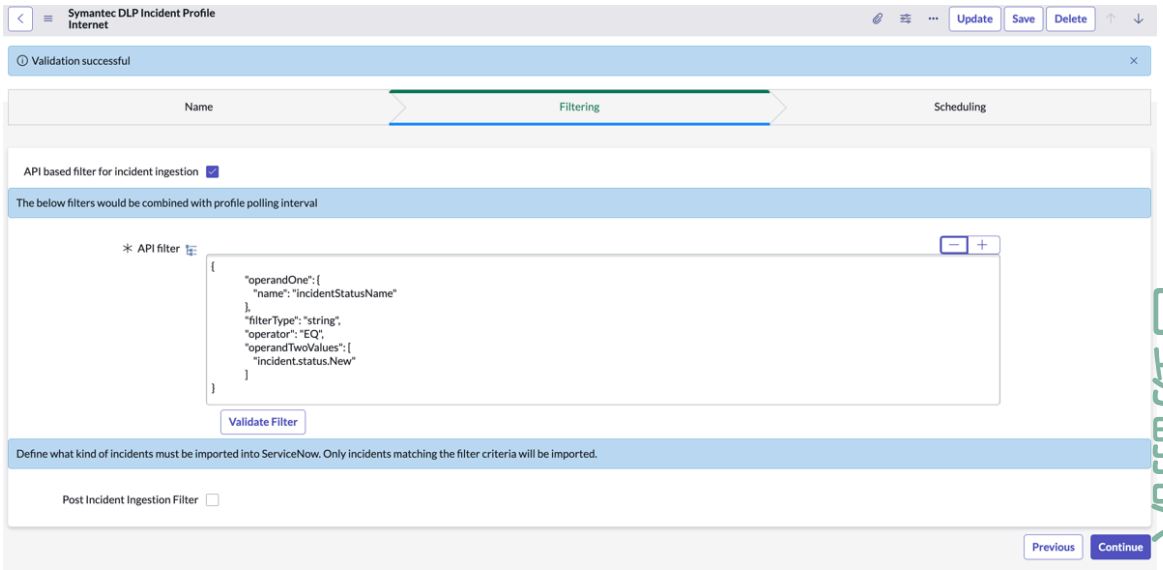
```
            "incident.status.New"
          ]
        }
```

注:
Symantec 統合の API フィルターの詳細については、「Incident Lists: Parameters - Request object details (インシデントリスト：パラメーター - 要求オブジェクトの詳細)」を参照してください。

3. API フィルターを適用した後で、[フィルターを検証 **(Validate Filter)**] クリックします。

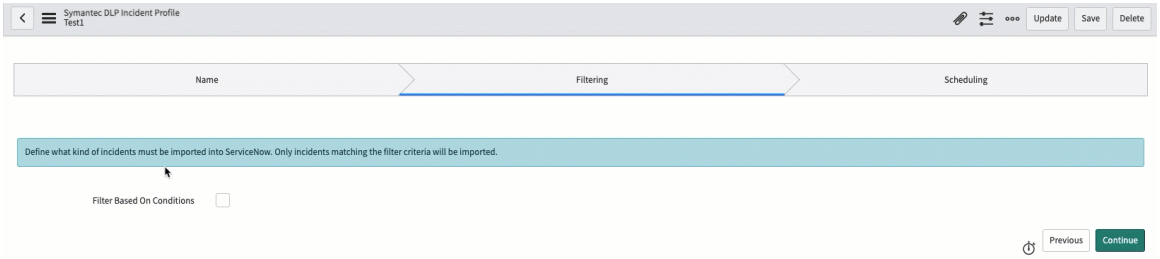
注:
検証が失敗した場合、検証が失敗したことを示すエラーメッセージが表示されます。これは、Symantec API に従ってフィルターが適切に入力されていない場合に発生します。

API フィルターの追加



4. [インシデント取り込み後のフィルター **(Post Incident Ingestion Filter)**] チェックボックスをオンにして、DLP インシデントを作成するために、受信される Symantec DLP インシデントが満たすべき条件を定義します。
[フィルター条件] の最初のフィールドのオプションは、DLP インシデントで使用可能なフィールドと一致します。入力する基準は大文字と小文字を区別します。定義した基準がインシデントの値と一致していることを確認します。
5. 条件ビルダーの [フィルター条件] フィールドで、フィルターを設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



6. さらに条件を追加するには、**[AND]** または **[OR]** をクリックします。
   - **[AND]** を選択した場合は、すべての条件に一致する必要があります。
   - **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。

次のタスク
スケジュールを設定するには、[続行] をクリックします。

証拠ファイルストレージの設定

DLP インシデントの証拠ファイルを安全に保存するように証拠ファイルストレージを設定します。

始める前に
必要なロール：sn_dlir.admin

ServiceNow Symantec DLP 統合用に構成しているSymantecユーザーの DLP ポータルのロール構成ページで、[本文]、[添付ファイル]、および [元のメッセージ] オプションが有効になっている必要があるSymantecを確認します。詳細については、「ロールの設定」ドキュメントの「表示属性」セクションを参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
証拠ファイルストレージを設定して、ファイルを安全に保存できます。これにより、ServiceNow インスタンスの内部ストレージのオプションが提供され、ServiceNow の フィールド暗号化を使用してファイルが保存および暗号化されます。詳細については、NowPlatform ドキュメントの 「フィールド暗号化」 を参照してください。

DLP アナリストがアナリストワークスペースから [DLP インシデントの証拠ファイルをダウンロード (Download evidence files for DLP Incidents)] アクションを実行すると、証拠ファイルのストレージオプションが有効になっている場合、選択したストレージからファイルがダウンロードされます。それ以外の場合、ファイルは Symantec ソースから直接ダウンロードされ、ServiceNow インスタンスには保持されません。

注:
DLP アナリストがアナリストワークスペースから [DLP インシデントの証拠ファイルをダウンロード] アクションを実行すると、証拠ファイルストレージオプションが有効になっている場合、選択したストレージからファイルがダウンロードされます。それ以外の場合、ファイルは Symantec ソースから直接ダウンロードされ、ServiceNow インスタンスには保持されません。

手順

1. 次のように移動する。 **All** (すべて) > **Symantec DLP** 統合 > インシデントプロファイル.
2. インシデントプロファイルフォームの [証拠ストレージ **(Evidence Storage)]** セクションをクリックします。
3. [証拠ファイルストレージ **(Evidence File Storage)]** チェックボックスをオンにして、ファイルストレージを有効にします。
4. 優先するストレージタイプを選択します。
5. [続行] をクリックし、[スケジューリング] セクションに移動します。

タスクの結果
インシデントの取り込みが完了した後、証拠ファイルは設定に従って保存されます。

証拠ファイルのダウンロード

Symantec の DLP ポリシーに違反する DLP インシデント証拠ファイルをダウンロードします。

始める前に
DLP IR アナリストワークスペースと DLP IR エンドユーザーワークスペースから、このファイルをローカルマシンにダウンロードします。ファイルのダウンロードアクションは、DLP IR エンドユーザーワークスペースで承認者のみが利用できます。

必要なロール：

- sn_dlir.analyst
- sn_dlir.secure_file_download (このロールを持つ任意の承認者)

手順

1. 次のように移動する。 **All** (すべて) > **Symantec DLP** 統合 > 設定.
2. [報告されたインシデントの違反ファイルのダウンロードを許可すべきですか] プロパティを有効にします。
   このプロパティを有効にすると、DLP アナリストワークスペースで Symantec DLP インシデントの [ファイルのダウンロード] アクションを表示できるようになります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.
4. Symantec ソースから取り込まれた DLP インシデントレコードを開きます。
5. [ファイルのダウンロード] をクリックします。

   注:
   Symantec で DLP ポリシーに違反したファイルは、ユーザーのローカルマシンにダウンロードされます。

   承認者が [ファイルのダウンロード] アクションを表示するには、以下の手順に従います。

6. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** ユーザーワークスペース.
   [自分の DLP インシデント] ページが新しいタブに表示されます。
7. [自分の DLP インシデント] モジュールで利用可能な [自分の承認] モジュールを選択します。
   [自分の承認] リストビューが表示されます。
8. Symantec DLP インシデントに対して発生した承認要求レコードを開きます。
9. フォームビューの [DLP インシデント] フィールドにある情報アイコン (i) をクリックします。
10. [ファイルのダウンロード] をクリックします。

タスクの結果

このアクションを実行すると、ZIP 形式 (インシデントに複数のコンポーネントで違反がある場合や、元のメッセージデータも利用可能な場合) または単一のファイル (インシデントに単一のコンポーネントで違反がある場合、または元のメッセージデータのみが利用可能な場合) のいずれかの証拠ファイルがユーザーのローカルマシンにダウンロードされます。

注:
DLP アドミンは、[詳細設定] ページから [報告されたインシデントの違反ファイルのダウンロードを許可するかどうか **(Should the viroling file of the reported incident)**] オプションを無効にすることで、[ファイルのダウンロード] アクションのアクセスを制御できます。詳細については、「Data Loss Prevention インシデントレスポンスの詳細設定を構成する」を参照してください。

証拠ファイルのプレビュー

DLP IR アナリストワークスペースで DLP インシデント証拠ファイルをプレビューします。

始める前に

- 次のように移動する。 **All** (すべて) > **DLP** 管理 > 詳細設定.
- **sn_sym_dlp.enable_evidence_file_preview** プロパティが既に有効になっていることを確認してください。

重要:
DLP アナリストワークスペースで証拠ファイルアクションを使用している間、証拠ファイルは、[詳細設定] ページの **sn_dlir.preview_temp_files_cleanup_interval** プロパティを使用して選択した期間、暗号化されていない形式で ServiceNow データベースに一時的に保存されます。ServiceNow データベースにデータを保存しない場合は、 証拠ファイルの プレビュー機能を無効にすることができます。詳細については、「詳細設定を構成します」を参照してください。

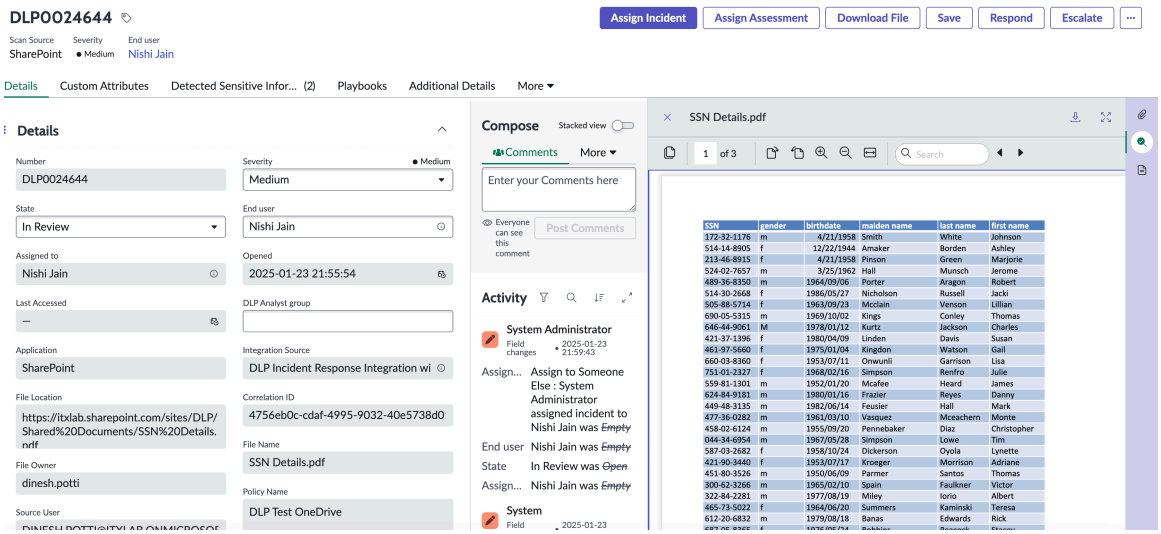
必要なロール：sn_dlir.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

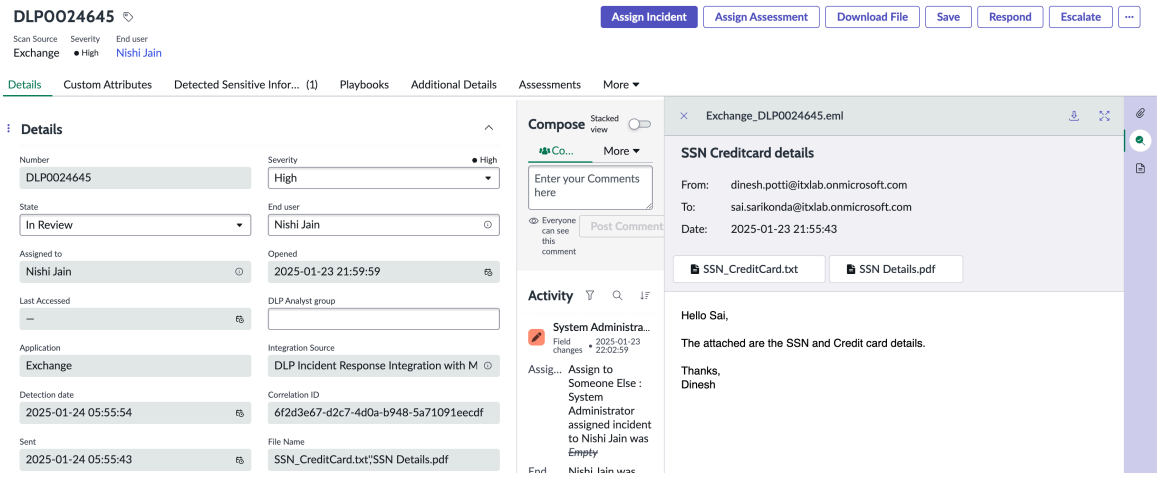
1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.
2. DLP インシデントレコードを開きます。
3. コンテキストメニューにある 証拠ファイル アイコンを選択します。
   すべての証拠ファイルを取得するタブが開きます。ダウンロードが完了すると、[証拠ファイル] タブですべての証拠ファイルを表示できます。
4. プレビューする 証拠ファイル カードを選択します。
   プレビュー機能は、ファイルタイプごとに異なります。
5. ドキュメントビューアーで PDF と Office ドキュメントをプレビューするには、証拠ファイルの右上にある [展開] アイコンを選択して PDF を全画面で開きます。
   ドキュメントビューアーが証拠ファイルを開く Office 拡張機能には、doc、docx、ppt、pptx、xls、xlsx などがあります。
   a. 検索バーを見つけて、探しているキーワードを入力します。
   b. ズームインおよびズームアウト機能を使用して、ビューが読みやすくなるように調整します。
   c. コンテンツをより鮮明に表示するには、ページを時計回りまたは反時計回りに回転させます。
   これらのコントロールオプションにより、証拠ファイルを包括的に理解する能力が向上します。
   ヘッダーにコントロールオプションがあるのは PDF だけです。



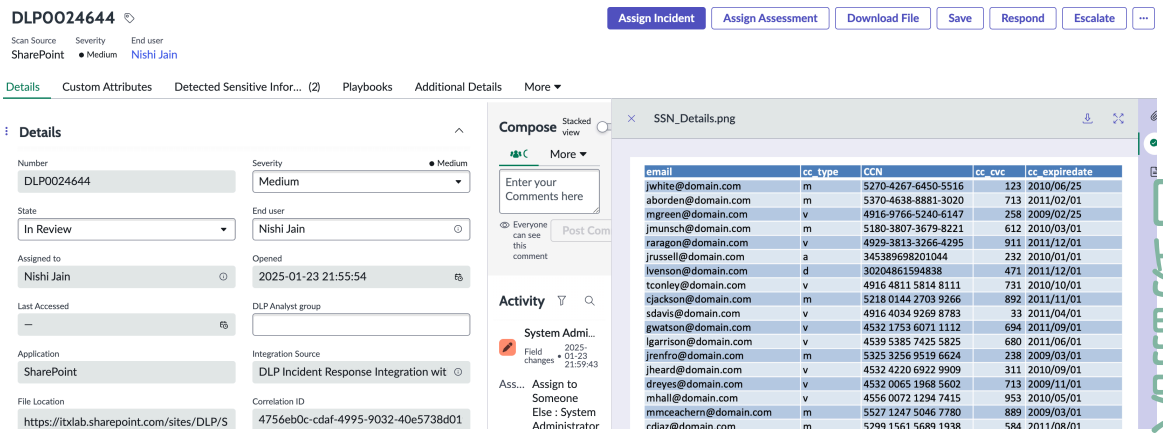
6. eml ファイルをプレビューします。
   メールの添付ファイルを選択してプレビューします。

> **注:**
> 選択した証拠ファイルが 5 MB の制限を超えた場合、アナリストワークスペースでプレビューすることはできません。コンテンツをプレビューするには、ファイルをダウンロードする必要があります。この制限は、.emlファイルに対してのみ適用されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

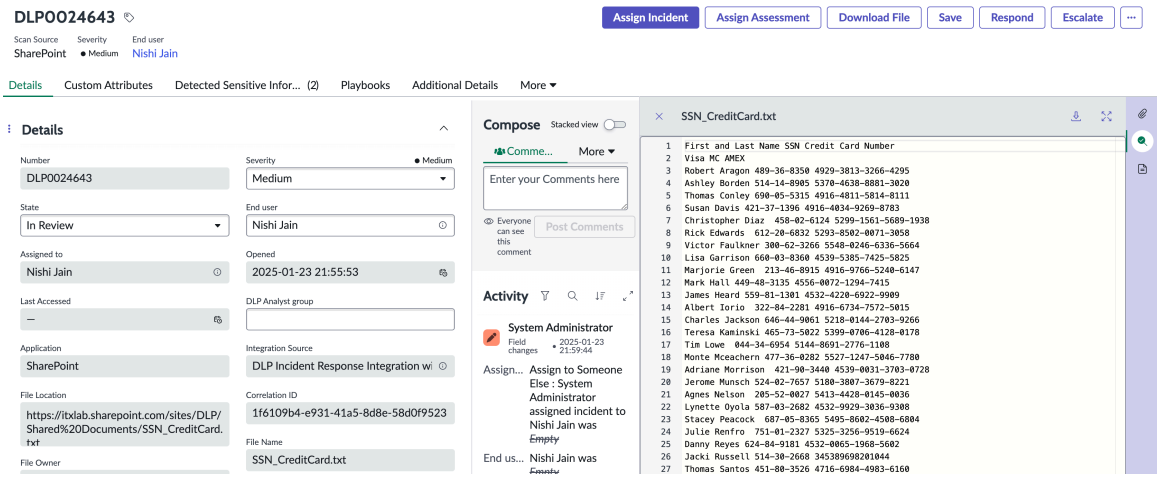


7. DLP アナリストワークスペースで画像をプレビューします。
.bmp、.gif、.ico、.jpeg、.jpg、.png、.svg、および .webp 拡張子のイメージのみがサポートされています。



8. 証拠ファイルの右上にある [展開] アイコンを選択して、テキストエディターでテキストファイルをプレビューします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
Office ドキュメント以外の証拠ファイル、eml ファイル、テキスト、画像拡張子は、プレビューではサポートされません。バイナリファイルはレンダリングされないため、コンテンツをプレビューするにはダウンロードする必要があります。証拠ファイルのプレビュー機能は、アーカイブされたインシデントでも機能します。

Symantec DLP インシデントの取得のスケジュール設定

インシデントデータを取得してプロファイルの条件に一致する Symantec DLP インシデントを取り込むスケジュールを設定します。Symantec からインシデントをプルする方法とタイミングを定義するスケジュールを設定します。

始める前に
必要なロール：sn_dlir.admin

このタスクについて
インシデントプロファイル構成に一致する将来のインシデントをポーリングする頻度を設定できます。インシデントの自動取り込みを有効にするには、プロファイルを有効にする前に、スケジュールとインシデントの取得を設定する必要があります。**[1** 回限りの 取得] チェックボックスを使用すると、1 回限りの取得を実行するようにプロファイルを構成できます。過去の日付は 最大 3 か月前以降に設定できます。

ポーリング間隔は、各プロファイルで個別に設定されます。ポーリング間隔が異なると、Symantec DLP インシデント統合のパフォーマンスに影響する可能性があります。スケジュールを設定するときは、インシデントの緊急度とシステム負荷のバランスを取るように計画してください。

手順

1. データを取得し、プロファイルの基準に一致するインシデントを取り込むスケジュールを設定します。
2. フォームの各フィールドに入力します。

DLP インシデントのスケジュール

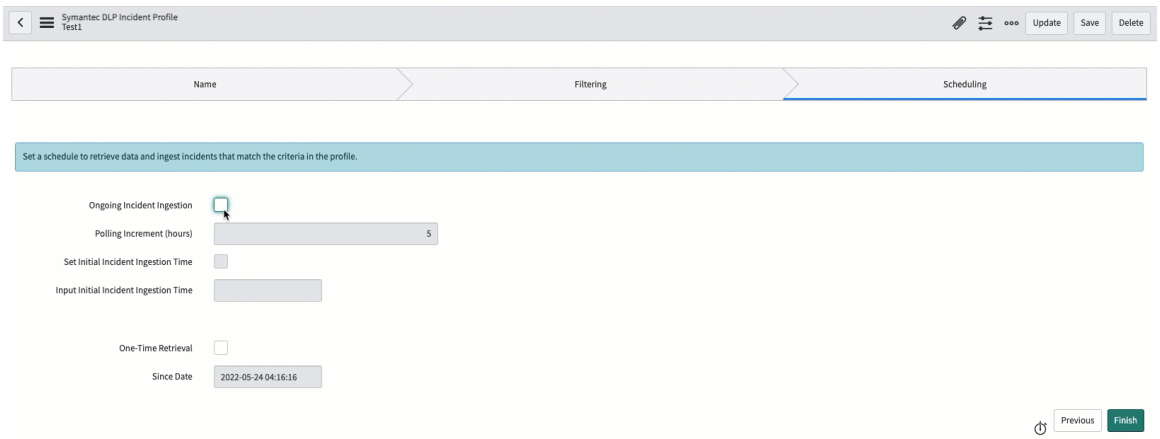
フィールド	説明
進行中のインシデントの取り込み	Now Platform インスタンスが☒ Symantec から新しいインシデントを取得する、進行中のインシデントの取り込み。トリガーされたインシデントが検出され、インシデント生成のフィル

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	ター基準が一致すると、DLP インシデントが作成されます。
ポーリングインクリメント (分)	定義されたポーリング頻度 (分単位)。このフィールドは自動的に 300 分に設定されます。
最初のインシデントの取り込み時刻を設定	最初の取り込みの日時を定義するオプション。それ以降の取り込みはポーリング間隔の時間に基づいて決まります。
入力の最初のインシデントの取り込み時刻	インシデントの取り込みに指定した日時。
最初のインシデントの取り込み時刻	データが最初に取り込まれる時刻。 最初のインシデントの取り込み時刻を設定すると、値の表示が始まります。
次のインシデント取り込み時刻 (推定)	次にインシデントが取り込まれるまでの推定時間。
1 回限りの取得	履歴データの 1 回限りのプルを有効にするオプション。 このフィールドが選択されている場合は、[開始日] フィールドに追加された日付に従って、Symantec DLP から履歴データが取得されます。
開始日	Symantec からデータを取得すると考えられる日付。 このフィールドは最大 3 か月に設定できます。

自動翻訳



3. 作成したプロファイル構成を保存するには、ポップアップで [終了] をクリックします。
4. プロファイルをアクティブ化するには、作成したプロファイルを開きます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. [アクティブ] オプションを有効にします。
6. [更新] をクリックします。

タスクの結果
プロファイルが正常に作成およびアクティブ化されると、プロファイルで設定されて DLP インシデントテーブルに追加された構成に従って、インシデントが定期的に取得されます。

Symantec DLP インシデントのステータスと **ServiceNow** インシデントのステータスのマッピング

ServiceNow で取り込んだ DLP インシデントのステータスを、Symantec の DLP インシデントと同期します。**[ServiceNow** インシデント状況] フィールドを **[Symantec** インシデント状況 **(Symantec Incident Status)]** フィールドとマッピングします。

始める前に
必要なロール：sn_dlir.admin

このタスクについて
インシデント状況は、マッピングに追加された Symantec エンドポイントソースから動的に取得されます。1 対 1 のインシデント状況マッピングを実行する必要があります。

手順
1. 次のように移動する。 **Symantec DLP** 統合 > インシデントステータスマッピング.
2. [名前] にマッピングを識別するための名前を入力します。
3. ソース でステータスのフェッチ元のソース統合を選択します。
4. **DLP** インシデント状況を **Symantec** インシデント状況にマッピングします。

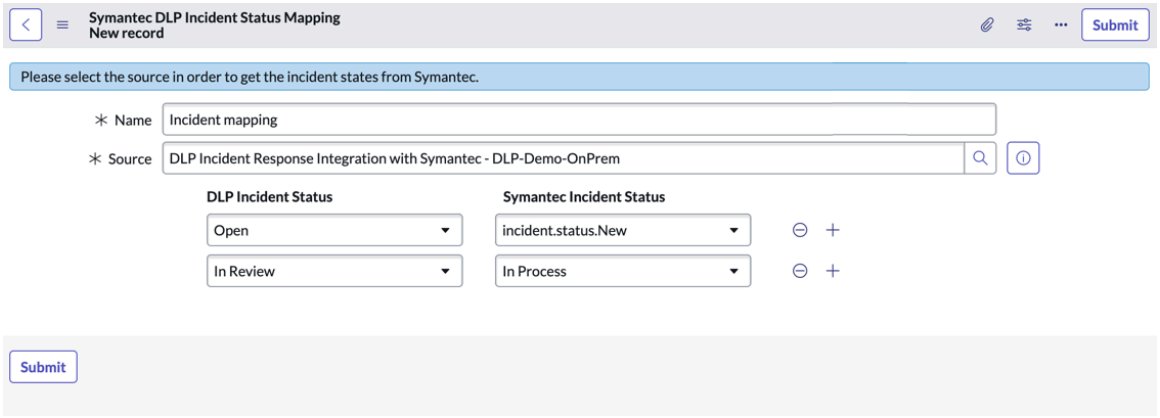
> **注:**
> すべてのステータスをマッピングする必要はありません。必要なステータスのみをマッピングできます。

Symantec DLP インシデント状況マッピング

フィールド	説明
名前	マッピングレコードの名前。
ソース	インシデント状況の取得元となる設定済みの Symantec エンドポイントソース。
DLP インシデント状況	DLP インシデントのステータスのリスト。
Symantec インシデント状況 (Symantec Incident Status)	ソース (Symantec エンドポイント) からフェッチされたステータスのリスト。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. [送信] をクリックします。

タスクの結果
ServiceNow のインシデントのマッピングステータスのレコードが正常に作成されると、ServiceNow のインシデント状況が Symantec DLP インシデント状況と同期されます。

ServiceNow インスタンスで DLP インシデントのステータスを変更すると、関連する Symantec DLP インシデントのステータスが、レコードに設定されたマッピングに基づいてソースの Symantec プラットフォームで変更されます。

Symantec DLP インシデントと **ServiceNow** インシデント間の重大度マッピング

重大度マッピング機能を使用して、Symantec インシデントと Now Platform® インシデント間のマッピングを構成して同期します。

始める前に
必要なロール：sn_dlir.admin

このタスクについて
DLP 重大度マッピングを使用すると、ソース重大度を DLP インシデント重大度にマッピングできます。ソースの重大度の値をカスタマイズして定義し、目的の DLP インシデントの重大度の値にマッピングできます。

手順

1. 次のように移動する。 **Symantec DLP** 統合 > インシデント重大度マッピング.

2. [**New**] をクリックします。

3. フォームのフィールドに入力します。

DLP 重大度マッピング

フィールド	説明
ソース	インシデントの取得元となる設定済みの Symantec エンドポイントソース。
ターゲット値	ターゲット値は DLP インシデント重大度 ID です。利用可能な値は、[重大]、[高]、[中]、[低]、および [情報] (Symantec では情報の重大度として使用) です。
ソース値	ソースの値は Symantec インシデントの重大度です。

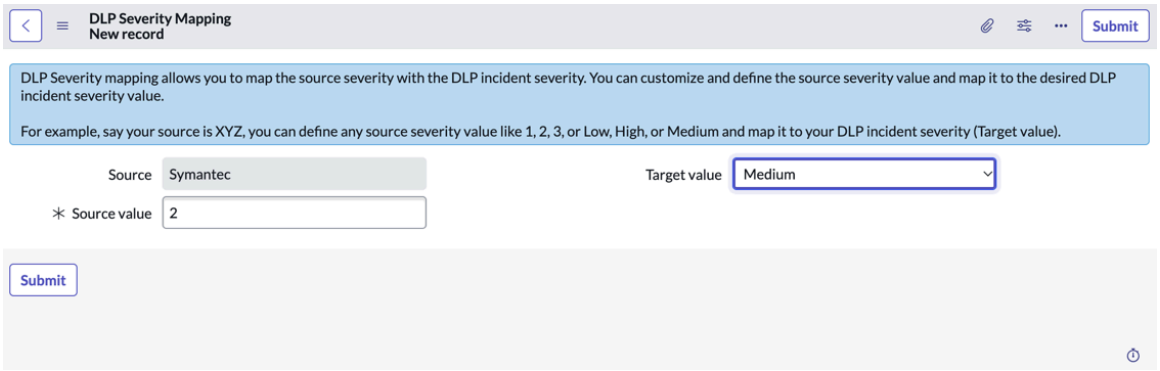
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
ベースシステム内には、DLP ユーザーに提供される 4 つの重大度マッピングがあります。

4. [送信] をクリックします。

重大度マッピング



スマート応答ルールの設定

取り込まれた Symantec DLP インシデントに対して応答アクションを実行するように Symantec スマート応答ルールを設定します。

始める前に

必要なロール：sn_dlir.admin

このタスクについて

ServiceNow Symantec DLP 統合用に設定している Symantec ユーザーの [ロール設定 **(Roles configuration)]** ページで、これらのスマート応答ルールが選択されている必要があることを確認します。詳細については、「ロールの設定」ドキュメントの「アクション」の項を参照してください。

フェッチされたスマート応答ルールに対して、DLP 管理者はインシデントレスポンスオプションルールと応答オプションマッピングを作成して、取り込まれた Symantec DLP インシデントに対して実行する応答アクションを設定できます。

手順

1. 次のように移動する。 **All** (すべて) > **Symantec DLP** 統合 > スマート応答ルール.
   構成された各統合設定で利用可能なすべてのスマート応答オプションを表示できます。詳細については、「設定されていない場合は、Symantec 統合設定ソースを設定する」 Symantec DLP integration for Data Loss Prevention のインストールおよび構成 、説明されている手順に従ってください)
2. いずれかのスマート応答ルールをクリックして、そのフォームビューを開きます。

   「インシデントレスポンスオプションルールを作成する」の手順に従ってインシデントレスポンスオプションルールと応答オプションマッピングを作成し、DLP ワークスペースの応答モーダルにこのスマート応答ルールを表示します。

3. スマート応答ルールの承認ルールを作成するには、関連リストの [承認ルール**(Approval Rules**)] タブを使用するか、「承認ルールの設定」セクションで説明されている手順に従います。
   各スマート応答ルールの承認ルールは、[承認ルール] 関連リストに表示されます。
4. インシデントレスポンスオプションルールを作成すると、スマート応答ルールレコードの関連リストにレコードが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. リストビューの [スマート応答ルールを更新 **(Refresh Smart Response Rule)]** ボタンを使用して、ソースを手動で更新します。
   スマート応答ルールは、すべてのソースに対して毎日自動的に追加、更新、または削除されます。

スマート応答ルールの実行

この機能を使用して、Symantec DLP インシデントのスマート応答ルールを実行します。

始める前に

スマート応答ルールは、このセクションの「スマート応答ルールの設定」で説明している手順に従って設定する必要があります。

必要なロール：sn_dlir.admin

> **注:**
>
> ワークスペースの応答オプションは、セクション「DLP インシデントの応答オプションの構成」で説明した設定に基づいてエンドユーザー、アナリスト、またはマネージャーが利用できます。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** > **DLP** ユーザーワークスペース.
2. 任意の Symantec DLP インシデントを開きます。
3. [応答] をクリックします。
4. [応答] ドロップダウンリストから応答オプションを選択します。
   応答オプションは、[インシデント応答オプションルール] と [応答オプションマッピング] の設定に基づいて表示されます。
5. [送信] をクリックします。

> **注:**
> 「承認ルールを作成する」セクションで説明している手順に従って、応答オプションの承認ルールを設定することもできます。スマート応答ルールに承認ルールが設定されている場合、最初に承認フローがトリガーされ、すべての承認を受信した後にスマート応答オプションフローがトリガーされます。応答オプションが正常に実行されると、DLP インシデントのステータスは、応答オプションマッピングのターゲットステータスに従って更新されます。

Symantec DLP#統合設定の構成

Symantec DLP 統合のデフォルトのシステムプロパティを変更します。

始める前に

必要なロール：sn_dlir.admin

手順

1. 次のように移動する。 **Symantec DLP** 統合 > 設定.
2. 必要に応じて次の設定を変更します。

設定

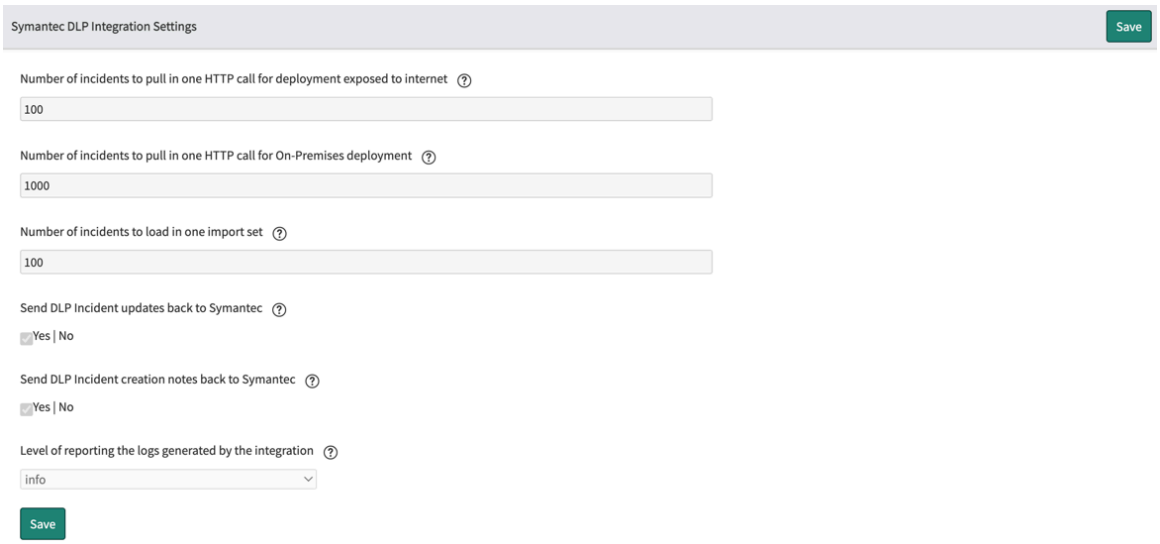
フィールド	説明
オンプレミスの展開への 1 回の HTTP 呼び出しでプルするインシデントの数に制限を強制する (Enforce a limit on	Symantec のオンプレミスの展開への 1 回の HTTP 呼び出しで取得するインシデントの最大数。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
Number of incidents to pull in one HTTP call for On-Premises deployment) sn_sym_dlp.page_size_on_prem	○ タイプ：整数 ○ デフォルト値：1000
インターネットに公開された展開への 1 回の HTTP 呼び出しで取得するインシデントの数に制限を強制する (Enforce a limit on Number of incidents to pull in one HTTP call for deployment exposed to internet) sn_sym_dlp.page_size_on_internet	インターネットに公開された Symantec 展開への 1 回の HTTP 呼び出しで取得するインシデントの最大数。 ○ タイプ：整数 ○ デフォルト値： 100
1 つのインポートセットにロードするインシデントの数	1 つの添付ファイルに保存する処理対象のレコードの数。 ○ タイプ：整数 ○ デフォルト値： 100
DLP インシデントの更新を Symantec に送信 sn_sym_dlp.incident_update	このプロパティを使用すると、ServiceNow と Symantec の DLP インシデント間のステータスの同期を制限できます。 ○ タイプ：ブーリアン ○ デフォルト値：**True**
DLP インシデントの作成メモを Symantec に送信 sn_sym_dlp.incident_creation_notes	このプロパティにより、ServiceNow でインシデントが作成されるとすぐに Symantec にメモを送信できます。 ○ タイプ：ブーリアン ○ デフォルト値：**True**
統合によって生成されたログのレポートレベル sn_sym_dlp.logging.verbosity	統合によって生成されたログのレポートを定義するプロパティ。

自動翻訳



3. [保存] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Symantec DLP 統合でのドメインセパレーション

ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。その後、どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル

サポート：ベーシック。

ドメインセパレーションが Symantec DLP 統合と連動する仕組み

ドメインセパレーションを実現するには、次の手順に従います。

- それぞれのドメインで、必要なロールを持つユーザーを作成します。
- 適切なドメインで Symantec DLP 統合の手順を実行します。

Data Loss Prevention Incident Response の Proofpoint との統合

Proofpoint DLP 統合では、Proofpoint Data Loss Prevention の実装時に作成された Data Loss Prevention インシデントの取り込みをサポートしています。取り込み後に、DLP インシデントを修復するインシデント管理機能を使用できます。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースメモ情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

概要と主な機能

Proofpoint DLP 統合を使用することで、さまざまなプラットフォームでの機密データの取り扱いや移動を追跡できます。

この統合の主な機能は次のとおりです。

- 異なる Proofpoint エンドポイントに対する複数のプロファイルの作成
- DLP インシデントの作成の自動化。
- Proofpoint DLP インシデント状況フィールドから DLP インシデント状況フィールドへのマッピング。
- Proofpoint DLP インシデントのフィルタリング。
- Proofpoint DLP テナントでのインシデントの作成直後の、ServiceNow インスタンスへのインシデントの取り込み。
- Proofpoint DLP 統合は、エンドポイントとメールタイプの両方のインシデントをサポートしています。
- Proofpoint DLP インシデントのステータスと、DLP インシデントの作成に関するコメント、および ServiceNow 側のステータス変更とクローズの自動更新。

この統合の詳細

ドキュメント識別子	ドキュメントタイトル
Proofpoint 製品ドキュメント Web サイト	Proofpoint 製品ドキュメント
ServiceNow 製品ドキュメント Web サイト	ServiceNow 製品ドキュメント Web サイト

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Proofpoint integration for Data Loss Prevention の概要

Proofpoint DLP 統合は、Proofpoint Data Loss Prevention テナントで作成されたデータ損失防止インシデントの取り込みをサポートしています。取り込み後、DLP インシデントを修復するインシデント管理機能が使用されます。

チェックリスト

Proofpoint DLP integration for Data Loss Prevention の設定を開始する前に、次の情報を確認します。

チェックリスト

フィールド	説明
必要な Now Platform および Data Loss Prevention Incident Response のアプリケーションロールがアサインされていることを確認します。	次のロールは、Now Platform 上の Proofpoint DLP 統合全体で使用されます。 • アドミン (admin) が ServiceNow® Store からアプリケーションをインストールし、データ損失防止アドミン (sn_dlir.admin) をアサインする。 • sn_dlir.admin ロールを持つユーザーが、統合を構成し、インシデントプロファイルを設定できる。 • sn_dlir.analyst ロールを持つユーザーが、統合全体での読み取りロールを持つ。
必要な Proofpoint DLP ユーザーロールをアサインします。	Proofpoint DLP 統合ロールと権限をレビューします。
Proofpoint DLP 1.0.1 以上を使用していることを確認します。	Proofpoint DLP integration for Data Loss Prevention は、Proofpoint Data Loss Prevention バージョン 1.0.1 以上でテストされています。
Proofpoint DLP 統合のサポートに必要なエンドユーザー用コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	次の DLP アプリケーションと Security Support Common アプリケーションが ServiceNow Store からインストールされ、有効化されていることを確認します。インストールされていない場合は、 アプリケーションをインストールしてアクティブ化します。 • Security Support Common • Data Loss Prevention Incident Response

Proofpoint integration for Data Loss Prevention のインストールおよび構成

ServiceNow® Store から Now Platform インスタンスに Proofpoint DLP 統合をインストールして構成します。Proofpoint DLP インシデントデータを使用して DLP インシデントの調査調査を開始します。

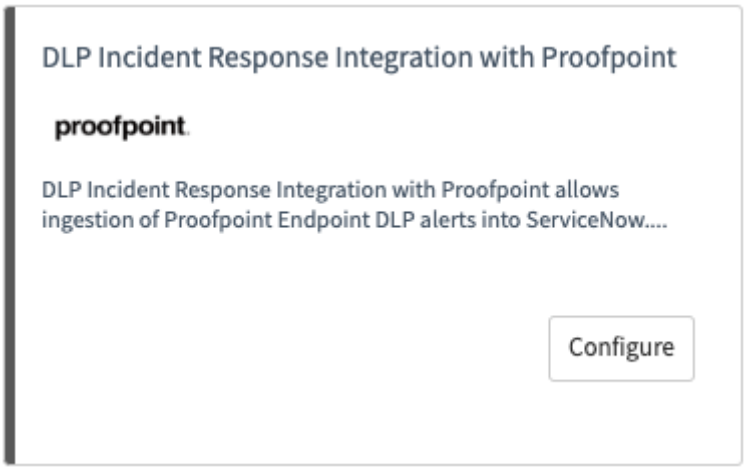
始める前に
必要なロール：sn_dlir.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. Proofpoint DLP 統合から ServiceNow® Store をダウンロードしてインストールします。
2. 次のように移動する。 セキュリティオペレーション > 統合 > 統合設定.
3. [Proofpoint の DLP インシデントレスポンス統合] タイルを検索して、[構成] をクリックします。



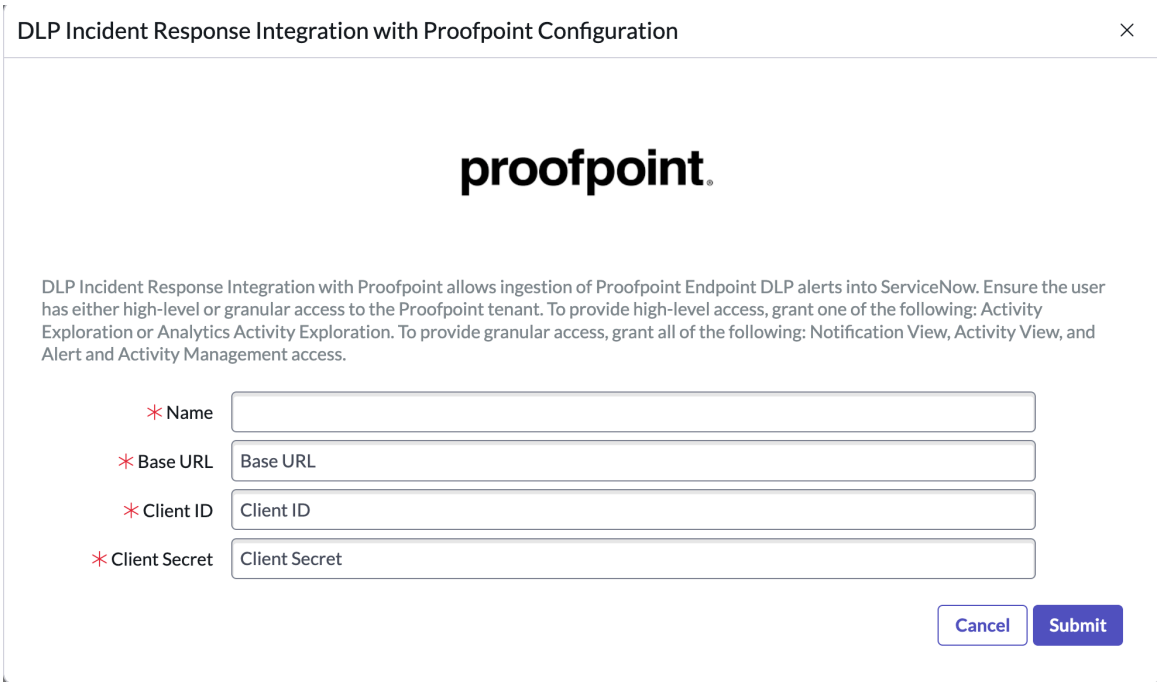
4. フォームのフィールドに入力します。

Proofpoint DLP 統合構成フォーム

フィールド	説明
名前	Proofpoint DLP 統合構成の名前。
ベース URL	REST エンドポイントとして機能する Proofpoint の URL。
クライアント ID	使用する Proofpoint クライアントの ID。
クライアントシークレット	Proofpoint でユーザーアカウント用に構成されたシークレット。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
ユーザー名とパスワードは、この構成でサポートされなくなります。ただし、ユーザー名とパスワードを使用して作成された既存の [Proofpoint の DLP インシデントレスポンス統合] タイルは、引き続き正常に機能します。

5. [**Submit** (送信)] を選択します。

タスクの結果
構成の検証と送信が正常に完了すると、Proofpoint DLP 統合が [セキュリティ統合] ページにタイルとして保存されます。

Proofpoint DLP テナントで **ServiceNow** へのアラート通知のための **Webhook** を構成する

REST API エンドポイントを使用して、Proofpoint DLP テナントからアラートの取得を開始するための Webhook を Proofpoint 上に構成します。ここで取得されたアラートから、ServiceNow インスタンスが DLP インシデントを作成します。Proofpoint DLP 統合によって、エンドユーザーが Webhook を構成するための REST API エンドポイントが提供されます。

始める前に
必要なロール：sn_pp_dlp.api_integration_user

手順

1. **[Proofpoint]** にログインします。
2. 次のように移動する。 **Proofpoint** テナント > 管理アプリケーション > **Integration** (統合) > 通知ポリシー.
3. 適切な名前で通知ポリシーを作成します。
4. 作成した [通知ポリシー] をクリックし、通知ポリシーで構成された Webhook を管理します。
5. **[Webhook** を追加 **(Add Webhooks)]** をクリックして、新しい Webhook 構成を作成します。
6. Webhook タイプに [汎用 **(Generic)]** を選択します。
7. [URL 入力 (URL Input)] で、次の形式を使用して URL を入力します。https://<インスタンス名>.service-now.com/api/sn_pp_dlp/proofpointalertapi/getalerts

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

8. メソッドは **[POST]** のままにします。
9. Webhook に次のヘッダーを追加します。
   - Name: Authorization
     Value: Basic <Base64Encoded Username and Password of the ServiceNow instance user>
   - Name: Content-Type
     Value: application/json
10. 他の値は変更しないでください。
11. **[Save** (保存)] をクリックします。
12. 次のように移動する。 **Proofpoint** テナント > 管理アプリケーション > ポリシー > **Rules** (ルール).
13. [アクション] セクションで、Webhook 通知を生成する際のルールを選択します。
14. 新しく作成され、Webhook が構成されている通知ポリシーを追加します。
15. [保存] をクリックします。

Proofpoint DLP 統合のプロファイルの作成

Now Platform インスタンスにインシデントプロファイルを作成します。DLP インシデントの作成に適した Proofpoint DLP インシデントを判断します。

始める前に
必要なロール：sn_dlir.admin

このタスクについて
Proofpoint の DLP アラートを入力するように Now Platform を設定します。入力したアラートは DLP インシデントとして ServiceNow インスタンスに格納します。

手順

1. 次のように移動する。 **Proofpoint DLP** 統合 > インシデントプロファイル.
2. [**New**] をクリックします。
3. フォームで [名前] セクションのフィールドを入力します。

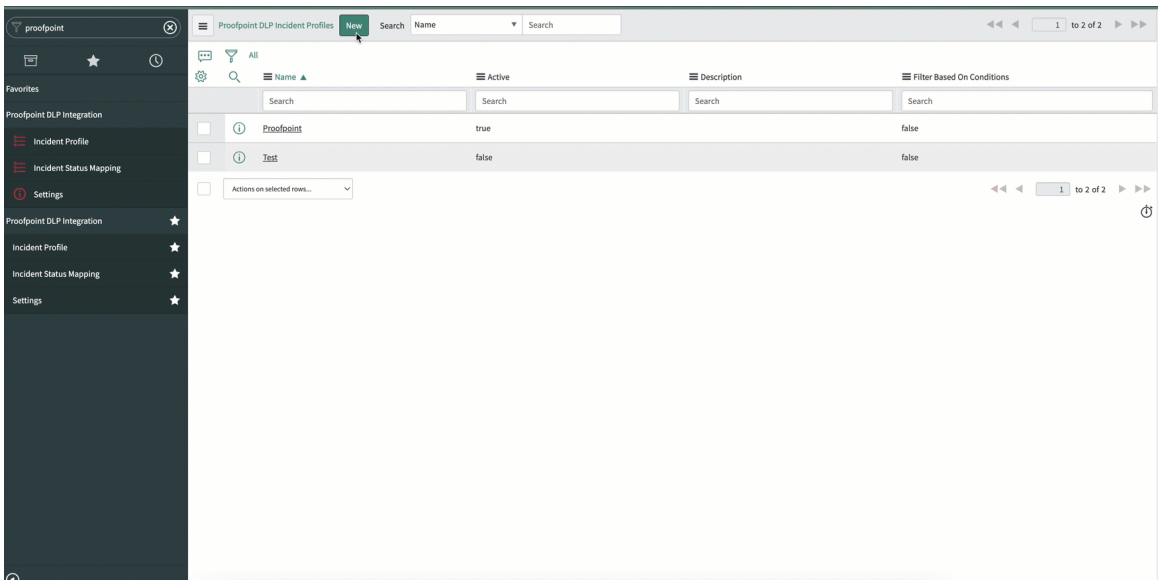
Proofpoint DLP 統合フォームのプロファイルの作成

フィールド	説明
名前	プロファイルの名前。この名前でプロファイルを識別できます。 **注:** プロファイルごとに名前は一意である必要があります。
ソース	インシデントを取り込むように構成した Proofpoint DLP インスタンス。複数のインスタンスが構成されている場合は、プロファイルに取り込む予定のインシデントタイプに適したインスタンスを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
アクティブ	プロファイルをアクティブにするオプション。 プロファイルがアクティブになると、Now Platform インスタンスは Proofpoint からインシデントを受信する準備ができます。
説明	このプロファイルを他のプロファイルと区別するための説明。



4. [続行] をクリックし、[フィルタリング] セクションに移動します。

インシデント作成の際に適用するフィルターの定義

受信した Proofpoint DLP インシデントをフィルタリングするためのフィルター条件を定義して設定します。ServiceNow　で作成する必要のある DLP インシデントを制御します。

始める前に

必要なロール：sn_dlir.admin

このタスクについて

このタイプのフィルタリングは、DLP インシデントを切り分けて、作成する DLP インシデントの数を制限する際に役立ちます。それ以外のフィルタリング基準が設定されている場合は、その条件に一致するインシデントのみが作成されます。

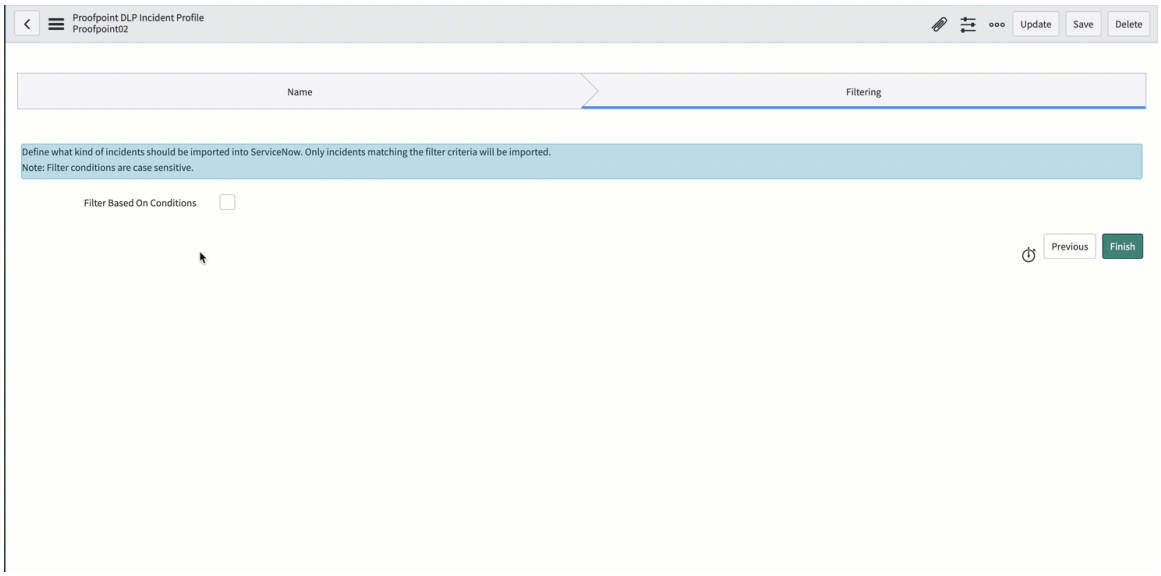
手順

1. [条件に基づいてフィルター] オプションを選択し、セキュリティインシデントを作成するために、受信した Proofpoint DLP インシデントが満たす必要のある基準を定義します。
2. 条件ビルダーのリストとフィールドを使用して、[フィルター条件] フィールドにフィルターを設定します。

   [フィルター条件] の最初のフィールドのオプションは、DLP インシデントで使用可能なフィールドに一致します。入力する基準は大文字と小文字を区別します。定義した基準がインシデントの値と一致していることを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. **[AND]** または **[OR]** をクリックして条件を追加します。
   - **[AND]** を選択した場合は、すべての条件に一致する必要があります。
   - **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。
4. [完了] をクリックします。

証拠ファイルストレージの設定

証拠ファイルストレージを構成して、Proofpoint メール DLP インシデントの ServiceNow インスタンスまたは外部に証拠ファイルを安全に保存します。

始める前に

必要なロール：sn_dlir.admin

このタスクについて

証拠ファイルストレージを設定して、ファイルを安全に保存できます。これにより、ServiceNow インスタンスに内部ストレージを保存するか、外部に保存するかのオプションが提供され、 列レベル暗号化 を使用してファイルが保存および暗号化されます。詳細については、NowPlatform ドキュメントの 「フィールド暗号化」 を参照してください。

DLP アナリストがアナリストワークスペースから [DLP インシデントの証拠ファイルをダウンロード] アクションを実行すると、証拠ファイルストレージオプションが有効になっている場合、選択したストレージからファイルがダウンロードされます。それ以外の場合、ファイルは Proofpoint ソースから直接ダウンロードされ、ServiceNow インスタンスに保存されません。詳細については、「DLP インシデントの証拠ファイルを Proofpoint でダウンロード」を参照してください。

手順

1. [インシデントプロファイル] フォームの [証拠ストレージ] セクションを選択します。
2. [証拠ファイルストレージ **(Evidence File Storage)]** チェックボックスをオンにして、ファイルストレージを有効にします。
3. 優先するストレージタイプを選択します。

内部ストレージ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [完了] をクリックします。

タスクの結果
証拠ファイルストレージオプションが有効になっていて、ServiceNow ストレージが選択されている場合、証拠ファイルは暗号化された形式で内部的に保存され、Proofpoint からのインシデントがフェッチされ、これらの Proofpoint インシデントのいずれかに対してファイルのダウンロードアクションを実行すると、システムはこのテーブルから証拠ファイルを取得します。

DLP インシデントの証拠ファイルを **Proofpoint** でダウンロード

Proofpoint の DLP ポリシーに違反する DLP インシデント証拠ファイルをダウンロードします。

始める前に
DLP IR アナリストワークスペースと DLP IR エンドユーザーワークスペースから、このファイルをローカルマシンにダウンロードします。

> **注:**
> [ファイルのダウンロード] アクションは、DLP IR エンドユーザーワークスペースでセキュアファイルアクセスロール (ServiceNow ストレージタイプにのみ適用され、外部ストレージに必要なロールはありません) を持つ承認者のみが使用できます。

[設定] で利用可能な [報告されたインシデントの違反ファイルのダウンロードを許可すべきですか] プロパティが有効になっている (またはアクティブが true に設定されている) ことを確認します。

必要なロール：

- sn_dlir.analyst
- sn_dlir.secure_file_download

> **注:**
> 内部ストレージに対してのみこのロールを持つ承認者は、ファイルをダウンロードできます。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.
2. スキャンソースを [メール **SMTP]** として Proofpoint DLP インシデントを開きます。
3. [ファイルのダウンロード] をクリックします。

承認者が [ファイルのダウンロード] アクションを表示するには、次の手順に従います。

4. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** ユーザーワークスペース.
   [自分の DLP インシデント] ページが新しいタブに表示されます。
5. [自分の DLP インシデント] モジュールで利用可能な [自分の承認] モジュールを選択します。
   [自分の承認] リストビューが表示されます。
6. スキャンソースメール SMTP を使用した Proofpoint DLP インシデントに対して発生した承認要求レコードを開きます。
7. フォームビューの [DLP インシデント] フィールドにある情報アイコン (i) をクリックします。
8. [ファイルのダウンロード] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスクの結果
このアクションを実行すると、Proofpoint の DLP ポリシーに違反したファイルがユーザーのローカルマシンにダウンロードされます。

注:

DLP アドミニストレーターは、[詳細設定] ページから [報告されたインシデントの違反ファイルのダウンロードを許可するかどうか **(Should the viroling file of the reported incident)**] 設定を無効にして、[ファイルのダウンロード] アクションへのアクセスを制御することもできます。詳細については、「Data Loss Prevention インシデントレスポンスの詳細設定を構成する」を参照してください。

証拠ファイルのプレビュー

DLP IR アナリストワークスペースで DLP インシデント証拠ファイルをプレビューします。

始める前に

- 次のように移動する。 **All** (すべて) > **DLP** 管理 > 詳細設定.
- **sn_pp_dlp.enable_evidence_file_preview** プロパティが既に有効になっていることを確認してください。

重要:
DLP アナリストワークスペースで証拠ファイルアクションを使用している間、証拠ファイルは、[詳細設定] ページの **sn_dlir.preview_temp_files_cleanup_interval** プロパティを使用して選択した期間、暗号化されていない形式で ServiceNow データベースに一時的に保存されます。ServiceNow データベースにデータを保存しない場合は、 証拠ファイルの プレビュー機能を無効にすることができます。詳細については、「詳細設定を構成します」を参照してください。

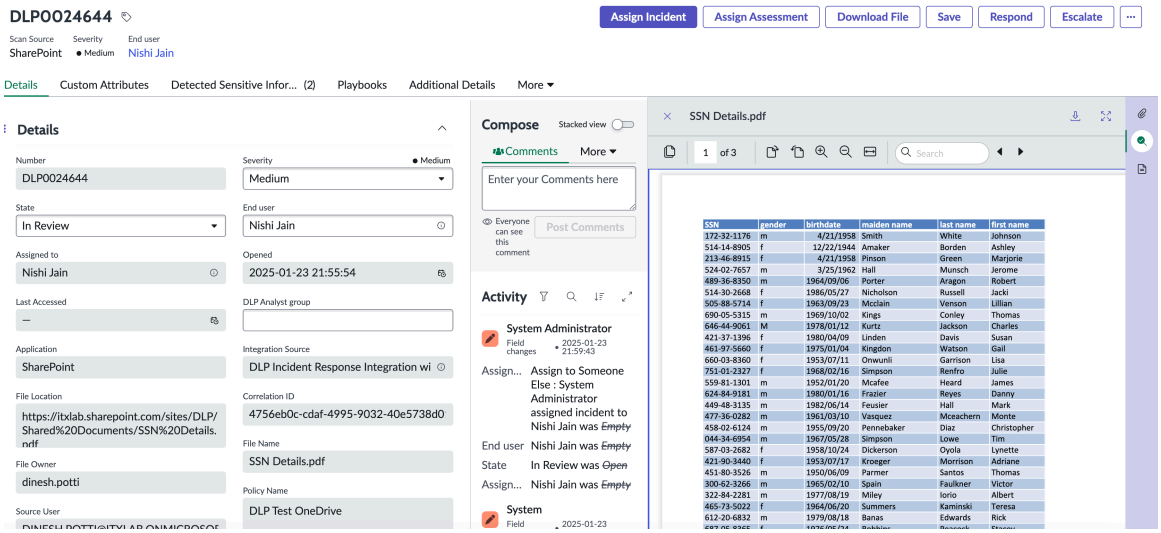
必要なロール：sn_dlir.analyst

手順

1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.
2. DLP インシデントレコードを開きます。
3. コンテキストメニューにある 証拠ファイル アイコンを選択します。
   すべての証拠ファイルを取得するタブが開きます。ダウンロードが完了すると、[証拠ファイル] タブですべての証拠ファイルを表示できます。
4. プレビューする 証拠ファイル カードを選択します。
   プレビュー機能は、ファイルタイプごとに異なります。
5. ドキュメントビューアーで PDF と Office ドキュメントをプレビューするには、証拠ファイルの右上にある [展開] アイコンを選択して PDF を全画面で開きます。
   ドキュメントビューアーが証拠ファイルを開く Office 拡張機能には、doc、docx、ppt、pptx、xls、xlsx などがあります。
   a. 検索バーを見つけて、探しているキーワードを入力します。
   b. ズームインおよびズームアウト機能を使用して、ビューが読みやすくなるように調整します。
   c. コンテンツをより鮮明に表示するには、ページを時計回りまたは反時計回りに回転させます。
   これらのコントロールオプションにより、証拠ファイルを包括的に理解する能力が向上します。
   ヘッダーにコントロールオプションがあるのは PDF だけです。

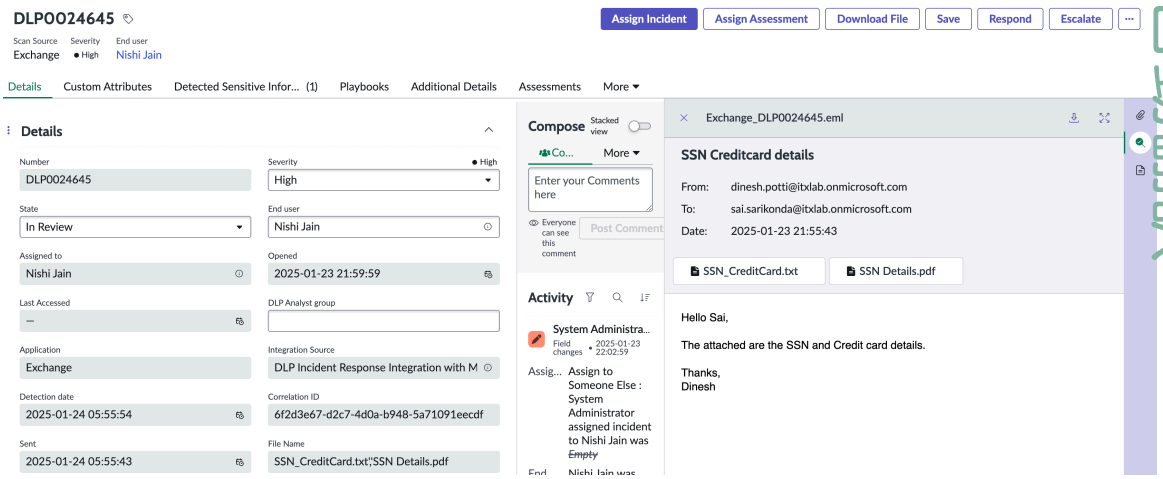
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



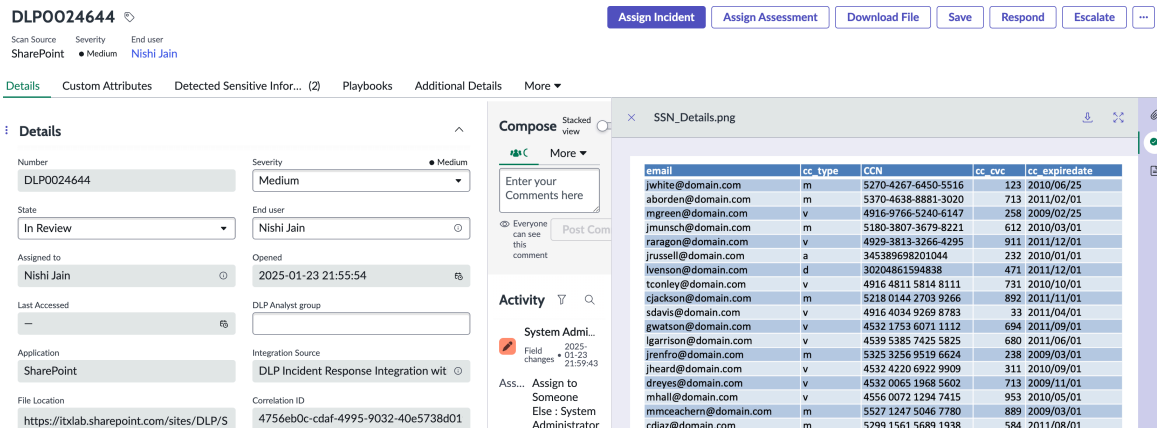
6. eml ファイルをプレビューします。
メールの添付ファイルを選択してプレビューします。

> **注:**
> 選択した証拠ファイルが 5 MB の制限を超えた場合、アナリストワークスペースでプレビューすることはできません。コンテンツをプレビューするには、ファイルをダウンロードする必要があります。この制限は、.emlファイルに対してのみ適用されます。

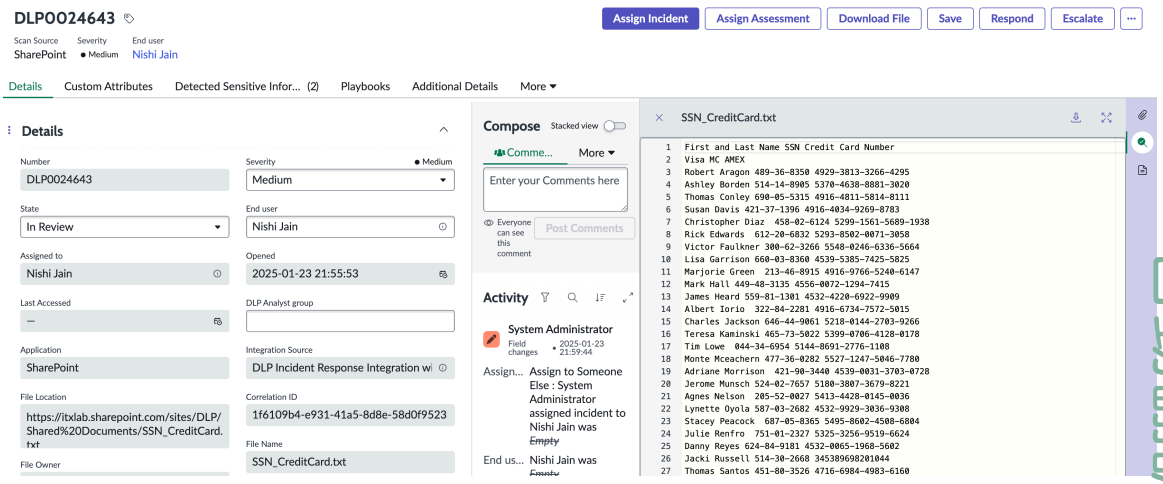


7. DLP アナリストワークスペースで画像をプレビューします。
.bmp、.gif、.ico、.jpeg、.jpg、.png、.svg、および .webp 拡張子のイメージのみがサポートされています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



8. 証拠ファイルの右上にある [展開] アイコンを選択して、テキストエディターでテキストファイルをプレビューします。



自動翻訳

> **注:**
> Office ドキュメント以外の証拠ファイル、eml ファイル、テキスト、画像拡張子は、プレビューではサポートされません。バイナリファイルはレンダリングされないため、コンテンツをプレビューするにはダウンロードする必要があります。証拠ファイルのプレビュー機能は、アーカイブされたインシデントでも機能します。

メール修復アクション

Proofpoint 用に隔離されたメールで修復アクションを実行します。

始める前に

Proofpoint には、次の 4 つの修復アクションが用意されています。

1. スキャンを含むメールをリリース
2. スキャンなしでメールをリリース
3. スキャン付きの暗号化されたメールをリリース
4. メールを削除

デフォルトでは、[スキャン付きのメールのリリース **(Release Email with Scan)**]、[スキャンなしでメールをリリース **(Release Email without** Scan)]、[スキャン付きの暗号化されたメールのリリース **(Release encrypted Email with Scan)**]、[メールを削除 **(Delete Email)]** 応答オプション と、メールに対して修復アクションを実行するための **Proofpoint** 修復アクションルール があります。こ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

れらの応答オプションには、これらのアクションの承認機能を利用するように、 **Proofpoint** メールリリース承認ルール も構成されています。これらの修復アクションは、エンドユーザー、アナリスト、エスカレートされたインシデントレビュー担当者が実行できます。

詳細については、「 DLP インシデントのインシデント応答オプションルールの設定 」、「 DLP インシデントの応答オプションの構成 」、および 「承認ルールの構成 」を参照してください。

必要なロール：

- sn_dlir.admin
- sn_dlir.analyst

Proofpoint Quarantine Release 応答オプションルール

Proofpoint 隔離リリース応答オプションマッピング

手順

次の手順では、DLP アナリストワークスペースから修復アクションを送信する方法について説明します。DLP アドミンおよび DLP アナリストは、次のことができます。

1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.
2. [スキャンソース] を [メール SMTP] として任意の Proofpoint DLP インシデントを開きます。
3. [応答] をクリックします。
4. [応答] ドロップダウンリストから応答オプションを選択します。
5. [**Submit** (送信)] を選択します。

次の手順では、DLP ユーザーワークスペースから修復アクションを送信する方法について説明します。エンドユーザーは、次のことができます。

6. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.
7. [スキャンソース] を [メール SMTP] として任意の Proofpoint DLP インシデントを開きます。
8. [応答] をクリックします。
9. [応答] ドロップダウンリストから応答オプションを選択します。
10. [**Submit** (送信)] を選択します。

注:

- このアクションに対して承認ルールが設定されている場合、最初に承認フローがトリガーされ、すべての承認を受信した後にメール修復フローがトリガーされ、アクションが実行されます。
- [メールを削除] が実行されると、DLP インシデントのステータスが [ファイルを削除] に更新されます。その他の応答オプションの場合、メールが正常にリリースされると、DLP インシデントのステータスが [隔離からリリースされたメール] に更新されます。

Proofpoint DLP インシデントのステータスと **ServiceNow** インシデントのステータスのマッピング

ServiceNow インスタンスで取り込んだ DLP インシデントのステータスを、Proofpoint の DLP インシデントと同期します。ServiceNow インシデント状況を Proofpoint インシデント状況にマッピングします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

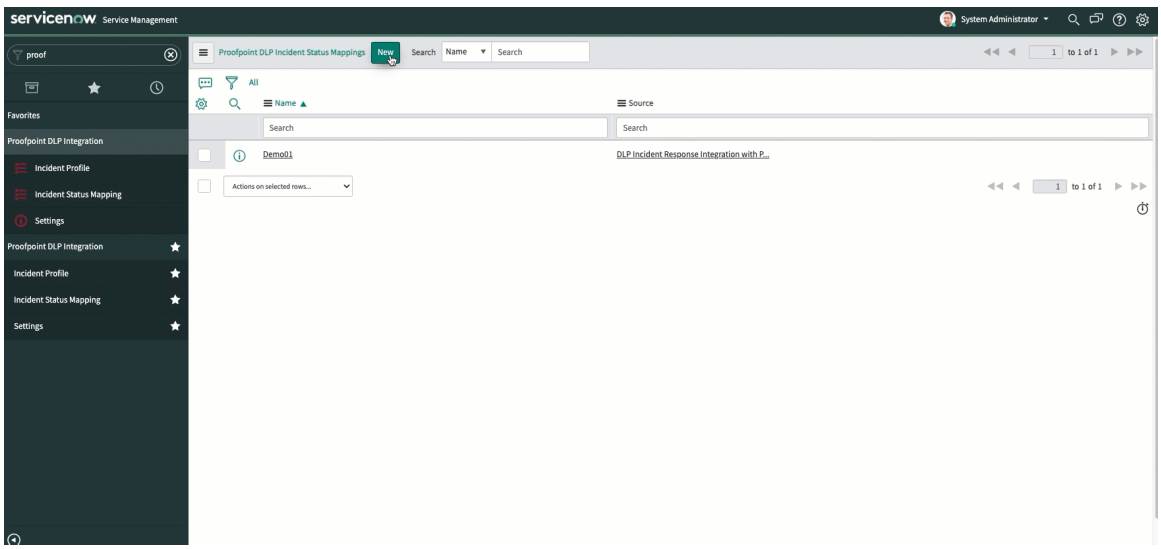
始める前に
必要なロール：sn_dlir.admin

手順

1. 次のように移動する。 **Proofpoint DLP** 統合 > インシデント > インシデントステータスマッピング.
2. [名前] にマッピングを識別するための名前を入力します。
3. ステータスマッピングを適用する必要のある [ソース] (統合構成) タイルを選択します。
4. **[ServiceNow DLP** インシデント状況 **(ServiceNow DLP incident Status)]** を **[Proofpoint** インシデント状況 **(Proofpoint Incident Status)]** とマッピングします。

Proofpoint DLP インシデント状況と **ServiceNow** インシデント状況とのマッピングのフォーム

フィールド	説明
名前	マッピングレコードのプレースホルダー。
ソース	インシデント状況の取得元となる設定済みの Proofpoint エンドポイントソース。
ServiceNow インシデント状況	DLP インシデントのステータスのリスト。
Proofpoint インシデント状況	DLP インシデントで使用可能なデフォルト状況に対するデフォルトのマッピング値。カスタム状況の場合、Proofpoint のデフォルトの状況は [新規] です。入力フィールドで、Proofpoint の必要なステータスを変更および追加できます。



5. [送信] をクリックします。

タスクの結果
マッピングのレコードが正常に作成されます。ServiceNow インシデントのステータスが Proofpoint DLP インシデントと同期されます。

ServiceNow インスタンスで DLP インシデントのステータスを変更すると、関連する Proofpoint DLP インシデントのステータスが、レコードに設定されたマッピングに従ってソースの Proofpoint プラットフォームで変更されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Proofpoint DLP 統合設定の構成

Proofpoint DLP 統合のデフォルトのシステムプロパティを変更します。

始める前に
必要なロール：sn_dlir.admin

手順

1. 次のように移動する。 **Proofpoint DLP** 統合 > 設定.
2. 必要に応じて次の設定を変更します。
3. [保存] をクリックします。

タスクの結果
変更した統合設定は、プロファイルで定義されている次のポーリング間隔で適用されます。

Proofpoint DLP 統合でのドメインセパレーション

ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。その後、どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル

サポート：ベーシック。

ドメインセパレーションが Proofpoint DLP 統合と連動する仕組み

ドメインセパレーションを実現するには、次の手順に従います。

- それぞれのドメインで、必要なロールを持つユーザーを作成します。
- 適切なドメインで Proofpoint DLP 統合の手順を実行します。

Data Loss Prevention Incident Response の Netskope との統合

Netskope DLP 統合では、Netskope Data Loss Prevention の実装時に作成された Data Loss Prevention インシデントの取り込みをサポートしています。Netskope DLP により、さまざまなプラットフォームでの機密データの取り扱いや移動を追跡できます。

取り込み後に、DLP インシデントを修復するインシデント管理機能を使用できます。

主な機能

この統合の主な機能は次のとおりです。

- 異なる Netskope テナントに対する複数のプロファイルの作成。
- Netskope DLP インシデントからの ServiceNow DLP インシデントの作成の自動化。
- Netskope DLP インシデントのフィルタリング。
- スケジュール設定された、ServiceNow で DLP インシデントを作成する Netskope DLP インシデントの取り込み。
- ServiceNow インスタンスでの DLP ステータス変更時の、Netskope のオブジェクトステータスの自動更新。
- DLP IR アナリストワークスペースと DLP エンドユーザーワークスペースで DLP インシデントのフォレンジックの詳細 (違反コンテンツ) の表示。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

> **注:**
> 違反コンテンツは ServiceNow に保持されません。コンテンツは、インシデントをワークスペースで開く際に取得されます。

- Netskope オンデマンドから証拠ファイルを直接ダウンロード。

> **注:**
> 証拠ファイルは ServiceNow に保持されません。証拠ファイルは、アナリストがワークスペースで [ファイルのダウンロード] をクリックする際に取得されます。

- Netskope トークンの有効期限に関する DLP 管理者ユーザーへのメールによる通知。
- インシデント API 呼び出しの失敗に対して定義された再試行制限を超えると、DLP 管理者ユーザーにメールによる通知。
- Netskope 統合実行プロセスもサポート。詳細については、「DLP 統合実行プロセスを監視する」を参照してください。

Netskope DLP integration for Data Loss Prevention の概要

Netskope DLP integration for Data Loss Prevention の設定を開始する前に、次の情報を確認します。

セットアップタスク	説明
必要な Now Platform Data Loss Prevention アプリケーションのロールが自分にアサインされていることを確認する。	次のロールは、Now Platform 上の Netskope DLP 統合全体で使用されます。 • アドミン (admin) が ServiceNow Store からアプリケーションをインストールし、データ損失防止アドミン (sn_dlir.admin) をアサインする。 • sn_dlir.admin ロールを持つユーザーが、統合を構成し、インシデントプロファイルを設定できる。 • sn_dlir.analyst ロールを持つユーザーが、統合全体での読み取りロールを持つことになる。
Netskope API v2 トークンに必要な権限をアサインします。	次のエンドポイント権限は、Netskope API v2 トークン化全体で使用されます。 • 読み取り：/api/v2/incidents/dlpincidents • 読み取り：/api/v2/events/dataexport/events/incident • 読み取り + 書き込み：/api/v2/incidents/update
Netskope DLP 統合のサポートに必要なエンドユーザー用コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	次の DLP アプリケーションと Security Support Common アプリケーションが ServiceNow Store からインストールされ、有効化されていることを確認します。インストールされていない場合は、 アプリケーションをインストールしてアクティブ化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セットアップタスク	説明
	• Security Support Common • Data Loss Prevention Incident Response

Netskope DLP integration for Data Loss Prevention のインストールおよび構成

ServiceNow Store Now Platform インスタンスから Netskope DLP 統合をインストールして構成します。DLP インシデントの調査を開始するには、Netskope DLP インシデントデータを使用します。

始める前に
必要なロール：sn_dlir.admin

手順

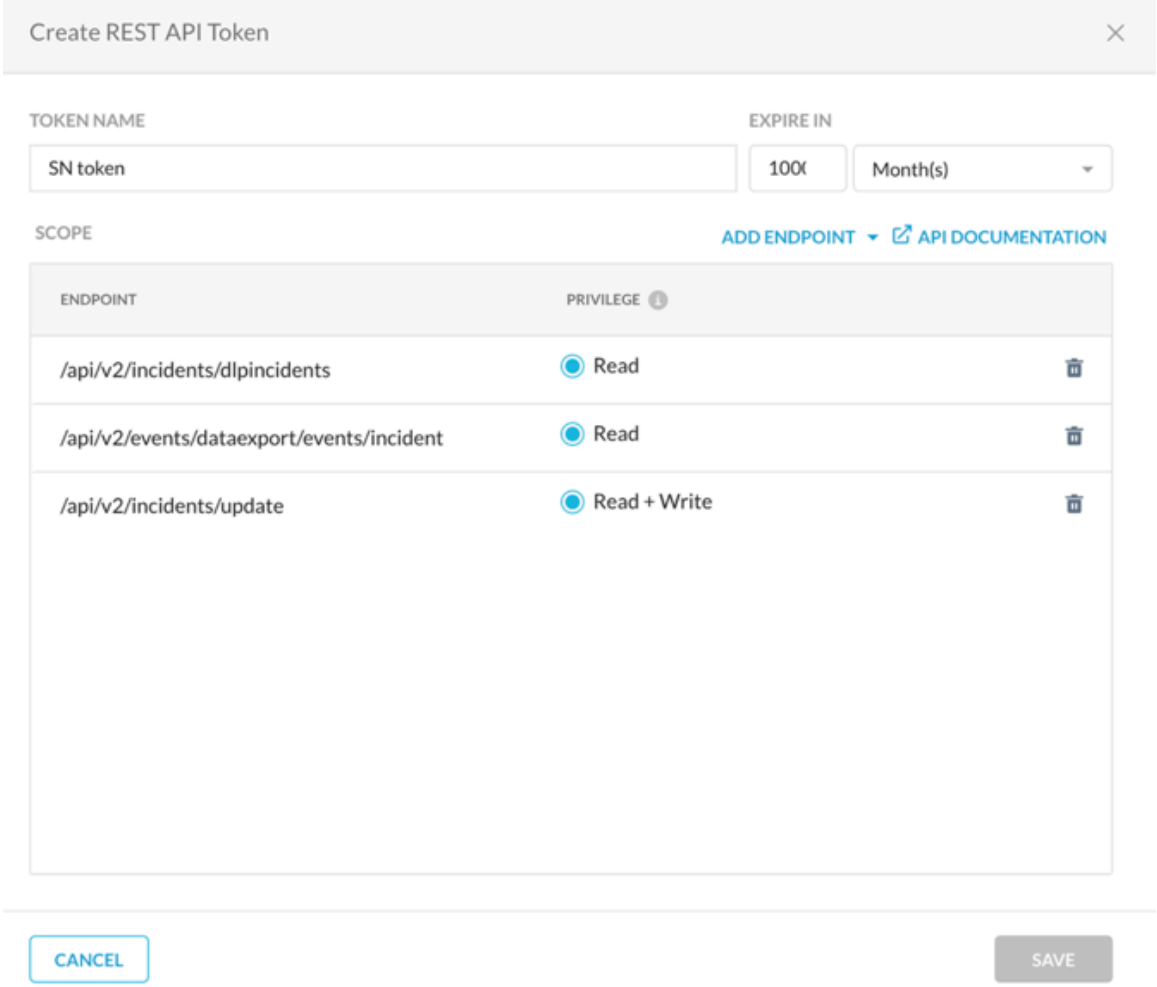
1. Netskope DLP 統合から ServiceNow Store をダウンロードしてインストールします。
2. 移動先 セキュリティオペレーション > 統合 > 統合設定
3. [DLP Incident Response Integration with Netskope] タイルを検索して、[構成] をクリックします。
4. フォームのフィールドに入力します。

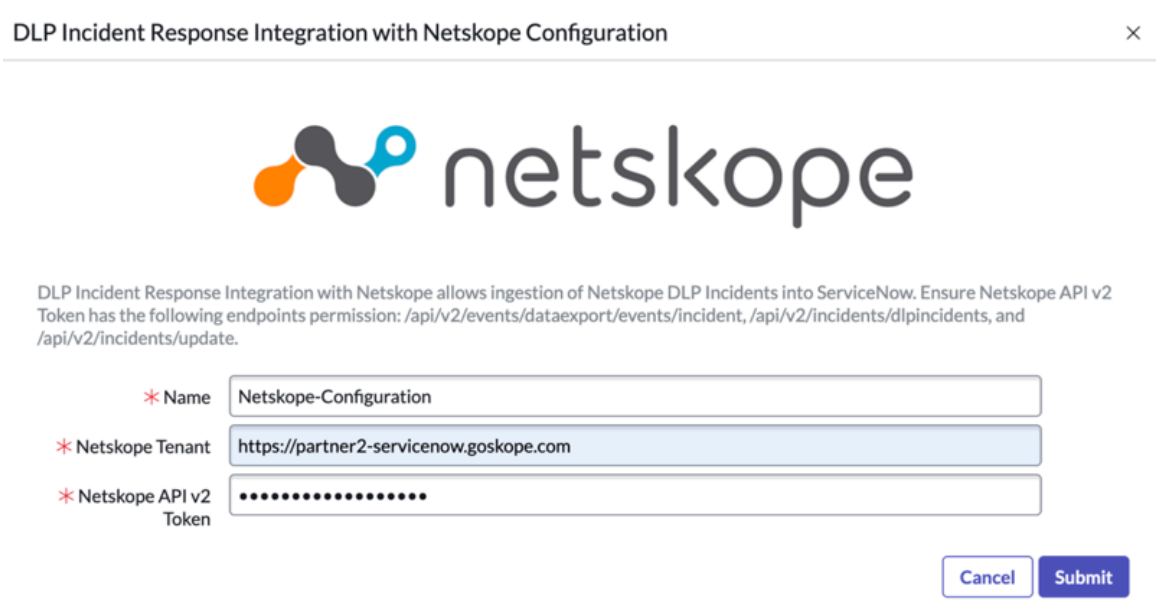
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
Netskope API v2 トークンに以下のエンドポイント権限があることを確認してください。

- 読み取り：/api/v2/incidents/dlpincidents
- 読み取り：/api/v2/events/dataexport/events/incident
- 読み取り + 書き込み：/api/v2/incidents/update





自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
名前	Netskope DLP 統合構成の名前。
Netskope テナント	Netskope テナントの Netskope ベース URL。
Netskope API v2 トークン	Netskope のユーザーアカウントで REST API v2 用に構成されたトークン。

5. [**Submit** (送信)] を選択します。

タスクの結果

注:
Netskope サブ本番環境を ServiceNow サブ本番環境に接続してください。アカウントがログアウトされないように、インスタンス間ですべてのユーザー名とパスワードの同期を維持します。

構成の検証と送信が正常に完了すると、Netskope DLP 統合が [セキュリティ統合] ページにタイルとして保存されます。

Netskope DLP 統合のプロファイルの作成

Now Platform インスタンスにインシデントプロファイルを作成します。

始める前に
必要なロール：sn_dlir.admin

このタスクについて
Netskope エンドポイントから DLP インシデントを取得するように Now Platform を構成します。取得したインシデントは DLP インシデントとして ServiceNow インスタンスに格納します。

手順

1. 次のように移動する。 **Netskope DLP** 統合 > インシデントプロファイル.
2. [**New**] をクリックします。
3. フォームのフィールドに入力します。

プロファイルの作成

フィールド	説明
名前	プロファイルの名前。プロファイルごとに名前は一意である必要があります。この名前でプロファイルを識別できます。
ソース	インシデントを取り込むように構成した Netskope DLP インスタンス。複数のインスタンスが構成されている場合は、プロファイルに取り込む予定のインシデントタイプに適したインスタンスを選択します。 注: ソースごとに許可されるアクティブなプロファイルは 1 つだけです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
アクティブ	プロファイルがアクティブであることを示すインジケーター。 **注:** このフィールドは、最後の [スケジューリング] セクションで [完了] をクリックした後にのみ使用できます。 プロファイルがアクティブな場合は、Now Platform インスタンスが Netskope DLP インシデントをアクティブにポーリングしています。 入力したフィルター条件が [スケジューリング] のパラメーターに基づいて一致すると、対応する DLP インシデントが #ServiceNow DLP インデントとして作成されます。
順序	プロファイルの実行順序。順序の値が最も小さいプロファイルの優先度が最も高いと見なされます。 デフォルト値は 100 です。
説明	このプロファイルを他のプロファイルと区別する際に役立つ説明。

4. [続行] をクリックし、[フィルタリング] セクションに移動します。

インシデント作成の際に適用するフィルターの定義

受信した Netskope DLP インシデントをフィルタリングするためのフィルター条件を定義して設定します。受信したインシデントのうちのどれを ServiceNow インスタンスで DLP インシデントとして作成すべきかを制御します。

始める前に
必要なロール：sn_dlir.admin

このタスクについて
このタイプのフィルタリングは、DLP インシデントを切り分けて、作成する DLP インシデントの数を制限する際に役立ちます。それ以外のフィルタリング基準が設定されている場合は、その条件に一致するインシデントのみが作成されます。

手順

1. [条件に基づいてフィルター] オプションを選択し、DLP インシデントを作成するために、受信した Netskope DLP インシデントが満たす必要のある基準を定義します。
2. 条件ビルダーのリストとフィールドを使用して、[フィルター条件] フィールドにフィルターを設定します。

   [フィルター条件] の最初のフィールドのオプションは、**[Netskope DLP** インシデントインポート] テーブルで使用可能なフィールドと一致します。入力する基準は大文字と小文字を区別します。定義した基準がインシデントの値と一致していることを確認します。

3. **[AND]** または **[OR]** をクリックして条件を追加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- **[AND]** を選択した場合は、すべての条件に一致する必要があります。
- **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。

4. [続行] をクリックし、[スケジューリング] セクションに移動します。

Netskope DLP インシデントの取得のスケジュール設定

プロファイルの基準に一致する Netskope DLP インシデントを取り込むスケジュールを設定します。

始める前に

必要なロール：sn_dlir.admin

このタスクについて

インシデントプロファイル構成に一致する正味の新しい Netskope インシデントをポーリングする頻度を設定できます。インシデントの自動取り込みを有効にするには、プロファイルをアクティブ化する前に、スケジュールとインシデントの取得を設定する必要があります。**[1** 回限りの 取得] チェックボックスを使用すると、1 回限りの取得を実行するようにプロファイルを構成できます。過去の日付は最大 1 か月前以降に設定できます。

手順

1. Netskope からインシデントをプルする方法とタイミングを定義するスケジュールを設定します。
2. フォームのフィールドに入力します。

Netskope DLP インシデントのスケジュール

フィールド	説明
進行中のインシデントの取り込み	Now Platform インスタンスが Netskope から新しいインシデントを取得する、進行中のインシデントの取り込み。インシデントのフィルタリング基準に一致するトリガーされたインシデントが見つかった場合は、DLP インシデントが作成されます。
ポーリングインクリメント (分)	定義されたポーリング頻度 (分単位)。このデフォルト値は **5** に設定されています。
最初のインシデントの取り込み時刻を設定	構成された日時に基づいて最初のインシデントの取り込みを設定するオプション。 このオプションを使用して、最初の取り込みに対する特定の日時を定義できます。それ以降の取り込みはポーリング間隔の時間に基づいて決まります。
入力の最初のインシデントの取り込み時刻	インシデントの取り込みに指定した日時。
最初のインシデントの取り込み時刻	データが初めて取り込まれる時刻。 **注:** この値は、[最初のインシデントの取り込み時刻を設定] オプションが選択されている場合にのみ表示されます。
次のインシデント取り込み時刻 (推定)	次のインシデント取り込みの推定時刻。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
1 回限りの取得	履歴データの 1 回限りのプルを有効にするオプション。 **注:** このオプションを選択すると、[開始日] フィールドに追加された日付に従って、Netskope DLP から履歴データが取得されます。
開始日	Netskope からのデータの取得が開始される日付。 **注:** 最大で過去 30 日間のデータを Netskope から取得できます。

3. [完了] をクリックします。
4. ポップアップで、[終了] をクリックして、作成したプロファイル構成を保存します。
5. プロファイルを有効化します。
   a. 作成したプロファイルを開きます。
   b. [アクティブ] を **true** に設定します。
   c. [更新] をクリックします。

タスクの結果
プロファイルが正常に作成およびアクティブ化されると、プロファイルで設定された構成に従って、インシデントが定期的に取得されます。取得されたインシデントは DLP インシデントテーブルに追加されます。

DLP インシデントステータスと **Netskope** のマッピング

[インシデントステータスマッピング] セクションでは、ServiceNow の DLP インシデントステータスと Netskope オブジェクトステータスの間のマッピングを指定できます。

始める前に
マッピングは、Netskope から ServiceNow に DLP インシデントを取り込むとき、および ServiceNow の DLP インシデントのステータス変更を Netskope に同期するときに使用されます。

ServiceNow で取り込んだ DLP インシデントのステータスを Netskope の DLP インシデントと同期します。[ServiceNow インシデントステータス (ServiceNow Incident Status)] フィールドを [Netskope オブジェクトステータス] フィールドとマッピングします。

必要なロール：sn_dlir.admin

このタスクについて
Netskope と ServiceNow ステータスの 1 対 1 のインシデントステータスマッピングを作成する必要があります。

手順
1. 次のように移動する。 **Netskope DLP** 統合 > インシデントステータスマッピング.
2. [名前] にマッピングを識別するための名前を入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. ソース統合を選択します。
4. DLP インシデントステータスを Netskope オブジェクトステータスにマッピングします (重複する Netskope ステータスもマッピング可能)。
マッピングレコードを作成しない場合、ServiceNow から Netskope へのステータス同期は無効になります。

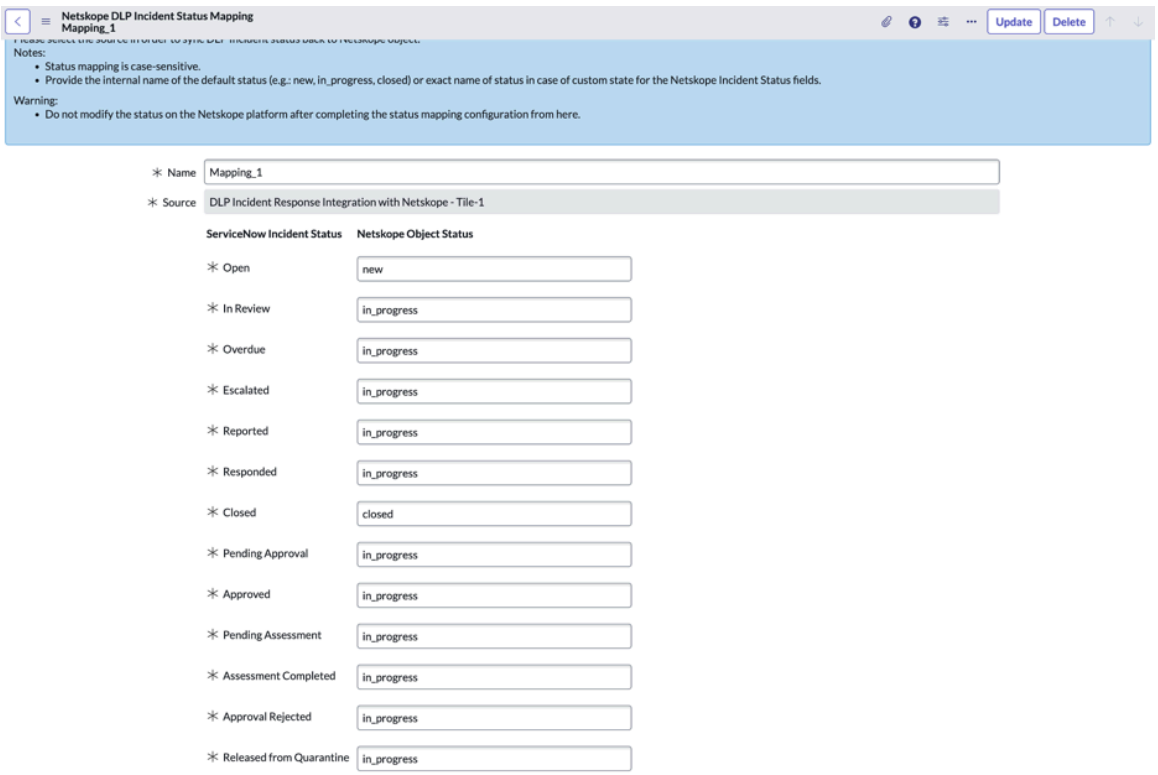
> **重要:**
> すべての Netskope オブジェクトステータスをすべての ServiceNow ステータスにマッピングする必要があります。ソースを選択して、DLP インシデントステータスを Netskope オブジェクトに同期します。

インシデントステータスをマッピングし、メッセージを確認して続行すると、次の情報とアラートメッセージが表示されます。

注:

- ステータスマッピングでは大文字と小文字が区別されます。
- [Netskope オブジェクトステータス] フィールドのデフォルトステータスの内部名 (新規、進行中、クローズ済みなど)、またはカスタムステータスの場合は正確なステータス名を指定します。

> **警告:**
> ここからステータスマッピング構成を完了した後は、Netskope プラットフォームでステータスを変更しないでください。



Netskope DLP インシデントステータスマッピング

フィールド	説明
名前	マッピングレコードの名前。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
ソース	インシデントステータスを同期する構成済みの Netskope エンドポイントソース。
DLP インシデントステータス	DLP インシデントステータスのリストを示します。
Netskope オブジェクトステータス	Netskope オブジェクトステータスのリストを示します。

5. [送信] をクリックします。

タスクの結果
ステータスマッピングのレコードを正常に作成すると、ServiceNow DLP インシデントのステータスが更新されるたびに、マッピングに従って Netskope 側に自動的に反映されます。

注:
Netskope テナントの DLP インシデントのステータスを直接変更した場合、SN から Netskope へのステータス同期は、API の制限を考慮して機能しません。すべての DLP インシデントステータスを Netskope オブジェクトステータスに慎重にマッピングしてください。

Netskope DLP 統合設定の構成

Netskope DLP 統合のデフォルトのシステムプロパティを変更します。

始める前に
必要なロール：sn_dlir.admin

手順

1. 次のように移動する。 **Netskope DLP** 統合 > 設定.
2. 必要に応じて次の設定を変更します。

Netskope DLP 統合設定の構成

フィールド	説明
報告されたインシデントの違反ファイルのダウンロードを n_ns_dlp.enable_file_download で許可するかどうか。	ファイルのダウンロードを有効にするかどうかを選択するオプション。デフォルトでは、このオプションは有効になっています。
HTTP 呼び出しの最大タイムアウト (秒単位)：sn_pp_dlp.maximum_http_time_out。	HTTP 呼び出しの最大タイムアウト (秒単位)。このフィールドは自動的に 30 に設定されます。
API の失敗に対して実行される再試行の最大回数：sn_ns_dlp.maximum_retry。	API の失敗に対して実行される再試行の最大回数。デフォルト値は 3 に設定されています。
統合によって生成されたログのレポートレベル：sn_ns_dlp.logging.verbosity。	統合によって生成されたログのレポートのレベルを定義します。このフィールドは自動的に [情報] に設定されます。

3. [保存] をクリックします。

タスクの結果
変更した統合設定は、プロファイルで定義されている次のポーリング間隔で適用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

証拠ファイルのプレビュー

DLP IR アナリストワークスペースで DLP インシデント証拠ファイルをプレビューします。

始める前に

- 次のように移動する。 **All** (すべて) > **DLP** 管理 > 詳細設定.
- **sn_ns_dlp.enable_evidence_file_preview** プロパティが既に有効になっていることを確認してください。

> **重要:**
> DLP アナリストワークスペースで証拠ファイルアクションを使用している間、証拠ファイルは、[詳細設定] ページの **sn_dlir.preview_temp_files_cleanup_interval** プロパティを使用して選択した期間、暗号化されていない形式で ServiceNow データベースに一時的に保存されます。ServiceNow データベースにデータを保存しない場合は、 証拠ファイルの プレビュー機能を無効にすることができます。詳細については、「詳細設定を構成します」を参照してください。

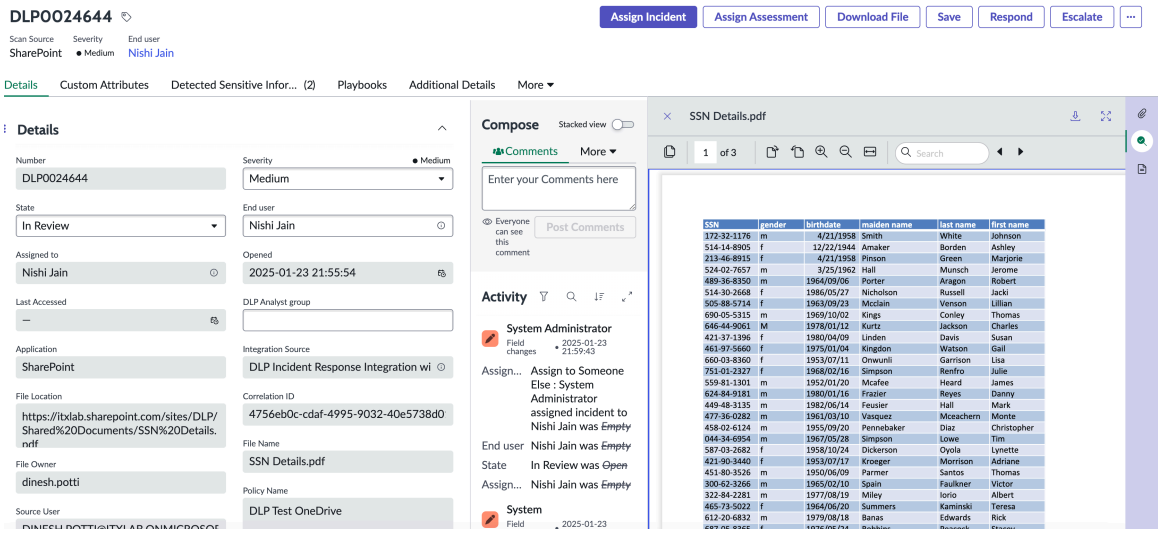
必要なロール：sn_dlir.analyst

手順

1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.
2. DLP インシデントレコードを開きます。
3. コンテキストメニューにある 証拠ファイル アイコンを選択します。
   すべての証拠ファイルを取得するタブが開きます。ダウンロードが完了すると、[証拠ファイル] タブですべての証拠ファイルを表示できます。
4. プレビューする 証拠ファイル カードを選択します。
   プレビュー機能は、ファイルタイプごとに異なります。
5. ドキュメントビューアーで PDF と Office ドキュメントをプレビューするには、証拠ファイルの右上にある [展開] アイコンを選択して PDF を全画面で開きます。
   ドキュメントビューアーが証拠ファイルを開く Office 拡張機能には、doc、docx、ppt、pptx、xls、xlsx などがあります。
   a. 検索バーを見つけて、探しているキーワードを入力します。
   b. ズームインおよびズームアウト機能を使用して、ビューが読みやすくなるように調整します。
   c. コンテンツをより鮮明に表示するには、ページを時計回りまたは反時計回りに回転させます。
   これらのコントロールオプションにより、証拠ファイルを包括的に理解する能力が向上します。
   ヘッダーにコントロールオプションがあるのは PDF だけです。

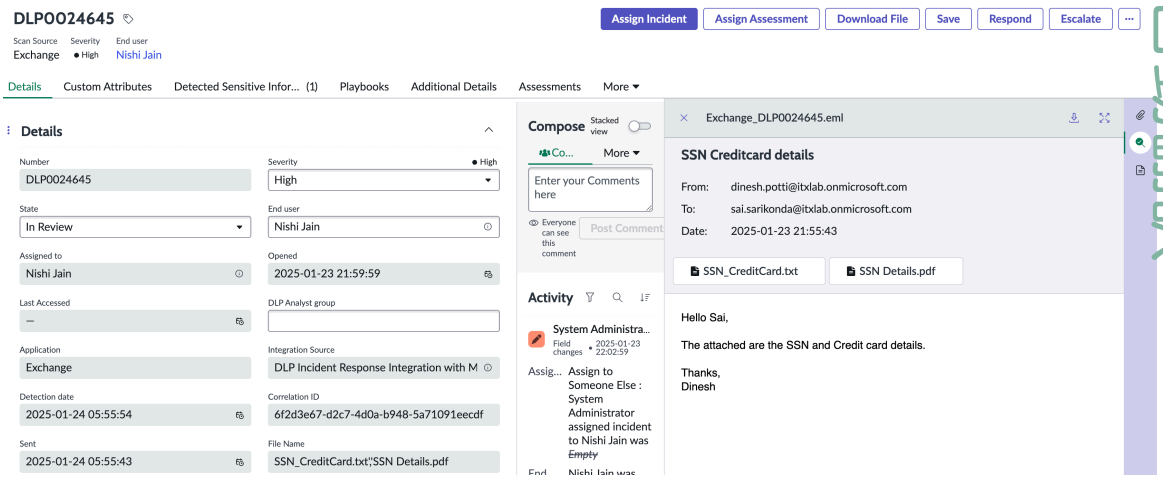
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



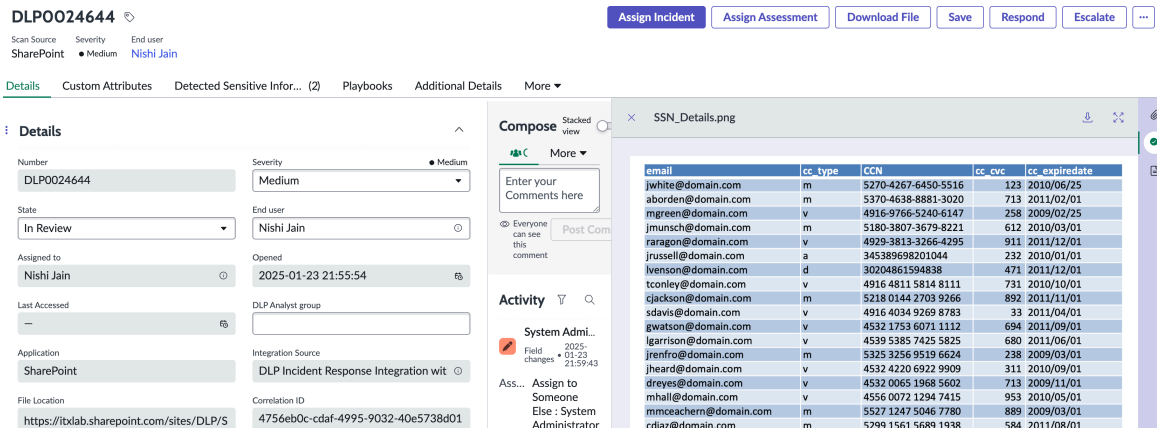
6. eml ファイルをプレビューします。
メールの添付ファイルを選択してプレビューします。

> **注:**
> 選択した証拠ファイルが 5 MB の制限を超えた場合、アナリストワークスペースでプレビューすることはできません。コンテンツをプレビューするには、ファイルをダウンロードする必要があります。この制限は、.emlファイルに対してのみ適用されます。

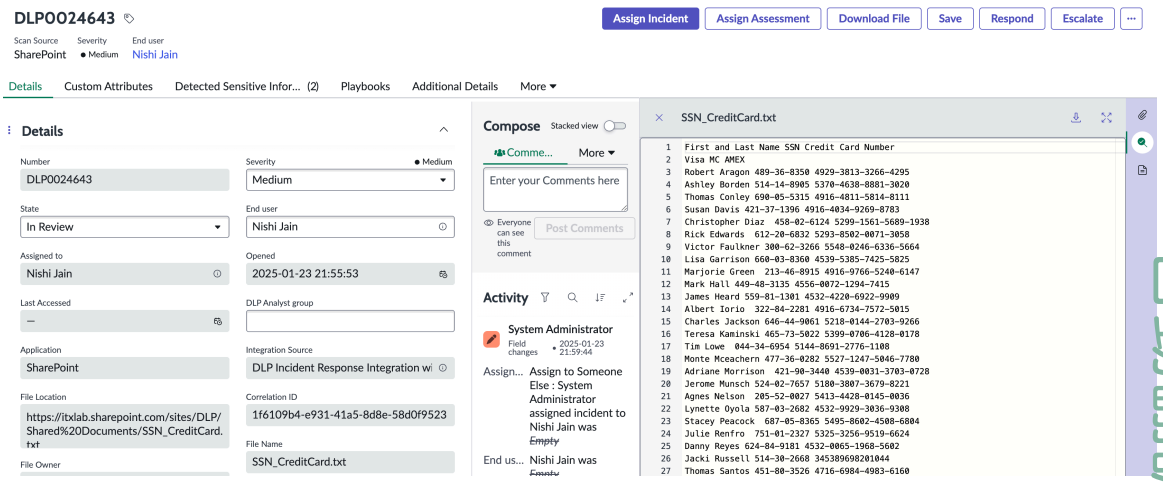


7. DLP アナリストワークスペースで画像をプレビューします。
.bmp、.gif、.ico、.jpeg、.jpg、.png、.svg、および .webp 拡張子のイメージのみがサポートされています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



8. 証拠ファイルの右上にある [展開] アイコンを選択して、テキストエディターでテキストファイルをプレビューします。



自動翻訳

> **注:**
> Office ドキュメント以外の証拠ファイル、eml ファイル、テキスト、画像拡張子は、プレビューではサポートされません。バイナリファイルはレンダリングされないため、コンテンツをプレビューするにはダウンロードする必要があります。証拠ファイルのプレビュー機能は、アーカイブされたインシデントでも機能します。

証拠ファイルのダウンロード

Netskope の DLP ポリシーに違反するファイルをダウンロードします。承認者用の DLP IR アナリストワークスペースと DLP IR エンドユーザーワークスペースから、このファイルをローカルマシンにダウンロードします。

始める前に

必要なロール：

- sn_dlir.analyst
- sn_dlir.secure_file_download (このロールを持つ任意の承認者)

このタスクについて

先に進む前に、Netskope のファイルのダウンロードを有効にする必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > **Netskope DLP** 統合 > 設定.
2. [報告されたインシデントの違反ファイルのダウンロードを許可すべきですか] のプロパティを有効にします。
   [ファイルのダウンロード] ボタンは、DLP IR アナリストワークスペースと DLP IR エンドユーザーワークスペースに表示されます。
3. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.
4. Netskope ソースから取り込まれた DLP インシデントレコードを開きます。
5. [ファイルのダウンロード] をクリックします。
   Netskope で DLP ポリシーに違反していたファイルは、ユーザーのローカルマシンにダウンロードされます。

   注:
   DLP 管理者は、DLP 管理の [詳細設定] ページから [報告されたインシデントの違反ファイルのダウンロードを許可すべきですか] オプションを無効にすることで、すべての統合の [ファイルのダウンロード] アクションのアクセスを制御できます。詳細については、「詳細設定を構成します」を参照してください。

再試行メカニズムに関するユーザーへの通知

Netskope 統合では、DLP インシデントの取り込み中に API エラーが発生した場合に、設定された回数だけ再試行します。

最大再試行回数の制限を超えると、Netskope 統合によって DLP 管理者 (sn_dlir.admin) ロールを持つユーザーにメール通知が送信されます。

統合のセットアップと構成が完了したら、DLP 管理者 (sn_dlir.admin) ロールを、最大再試行回数の制限を超えたときに通知する必要があるユーザーに付与します。

最大再試行回数の制限を超えると、プロファイルは最大 1 時間取り込みをスキップします。最大再試行回数は、「API エラーに対して実行される最大再試行回数 (Maximum number of retries to be performed for API failures)」プロパティを使用して設定されます。詳しくは、「Netskope DLP 統合設定の構成」を参照してください。

認証情報の期限切れに関するメール通知

ServiceNow インスタンスで使用されているトークンの有効期限が切れると、Netskope 統合から DLP アドミン (sn_dlir.admin) ロールを持つユーザーにメール通知が送信されます。

統合構成のセットアップが完了したら、DLP アドミン (sn_dlir.admin) ロールを、トークンの有効期限が切れた場合に通知する必要があるユーザーに付与します。

トークンの有効期限が切れると、関連するプロファイルのデータの取り込みは、Netskope 統合構成が有効なトークンで更新されるまで保留されます。

Netskope でトークンを作成するか古いトークンを更新してから、ServiceNow インスタンスでトークンを更新する必要があります。有効期限を延長してトークンを更新すると、Netskope アプリケーションが自動的に更新を検出し、データ収集を続行します。トークンを作成する場合は、構成内のトークンを更新する必要があります。

Netskope DLP 統合でのドメインセパレーション

ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。その後、どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

サポートレベル

サポート：ベーシック。

ドメインセパレーションが **Netskope DLP** 統合と連動する仕組み

ドメインセパレーションを実現するには、次の手順に従います。

- それぞれのドメインで、必要なロールを持つユーザーを作成します。
- 適切なドメインで Netskope DLP 統合の手順を実行します。

DLP IR の **Internet Content Adaption Protocol (ICAP)** 統合

Internet Content Adaption Protocol (ICAP) DLP 統合は、 Data Loss Prevention Incident Response アラートの取り込みをサポートし、ICAP でサポートされている展開で作成された Amazon S3 からの一致コンテンツと証拠ファイルをフェッチ Data Loss Prevention Incident Response できます。

アラートが取り込まれた後、DLP ワークスペースを使用して、一致コンテンツ、アラートの重大度、各種のインシデント管理機能などの重要な情報を表示し、DLP インシデントを修正できます。

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースメモ情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

概要と主な機能

Internet Content Adaption Protocol (ICAP) 統合は、さまざまなプラットフォームでの機密データの使用状況と移動を追跡するのに役立ちます。

この統合の主な機能は次のとおりです。

- DLP アラートの取り込み: ユーザーは、指定された Amazon S3 バケットからの DLP アラートの取り込みを設定およびスケジュールできます。これには、デルタインポートを実行して新しいデータのみが取り込まれるようにする機能が含まれます。
- 取り込まれたアラートを DLP ワークスペースに表示する:取り込まれたアラートは DLP ワークスペースに表示され、一致コンテンツ、アラートの重大度、関連するメタデータなど、各アラートに関する重要な詳細が提供されます。
- 一致コンテンツ:機密情報レコードは取り込み中に作成され、レコードを開くと一致コンテンツがフェッチされます。
- 証拠ファイルのダウンロード: システムを使用すると、ユーザーは関連する証拠ファイルを DLP ワークスペースから直接ダウンロードして、さらに調査またはレビューできます。
- ICAP DLP インシデントと ServiceNow インシデント間の重大度マッピングをカスタマイズおよび定義する機能。

データ損失防止のための **ICAP DLP** 統合の概要

統合を使用する前に、統合を ServiceNow® Store

チェックリスト

データ損失防止のためのプロバイダーの ICAP DLP 統合の設定を開始する前に、次の情報を確認してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

チェックリスト

フィールド	説明
必要な Now Platform Data Loss Prevention アプリケーションのアプリケーションロールがアサインされていることを確認します。	次のロールは、 Now Platform上の ICAP DLP 統合全体で使用されます。 • アドミン (admin) は、 ServiceNow® Store からアプリケーションをインストールし、データ損失防止アドミン (sn_dlir.admin) をアサインします。 • sn_dlir.admin ロールを持つユーザーが、統合を構成し、インシデントプロファイルを設定できる。 • sn_dlir.analyst ロールを持つユーザーは、統合構成全体の読み取りロールを持ちます。
必要な Amazon S3 バケットポリシーがアサインされていることを確認します。	IAM ユーザー、ポリシー、権限の作成と管理については、次のリンクから AWS の公式ドキュメントを参照できます。 • IAM ユーザーの作成 • IAM ポリシーの作成 • Amazon S3 権限 **注:** 上記のリンクを使用すると、AWS で IAM ユーザーと S3 権限を管理するための詳細な手順と詳細なオプション、AWS アカウントで IAM ユーザーを作成する方法 (AWS Identity and Access Management)、および AWS Identity and Access Management で IAM ユーザーと認証情報を作成するために使用されるプロセスの基本的な概要について詳しく知ることができます。
ICAP DLP 統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	以下の DLP アプリケーションと Security Support Common アプリケーションが ServiceNow Store からインストールされてアクティブ化されていることを確認します。インストールされていない場合は、 アプリケーションをインストールしてアクティブ化します。 • Security Support Common • Security Case Management 共通ワークスペースコンポーネント。 • Data Loss Prevention Incident Response

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ICAP DLP 統合のインストールと構成

Now Platformインスタンスの ServiceNow® Storeからプロバイダーの ICAP DLP 統合をインストールして構成します。プロバイダー ICAP DLP インシデントデータを使用して DLP インシデントの調査を開始します。

始める前に

必要なロール：sn_dlir.admin

手順

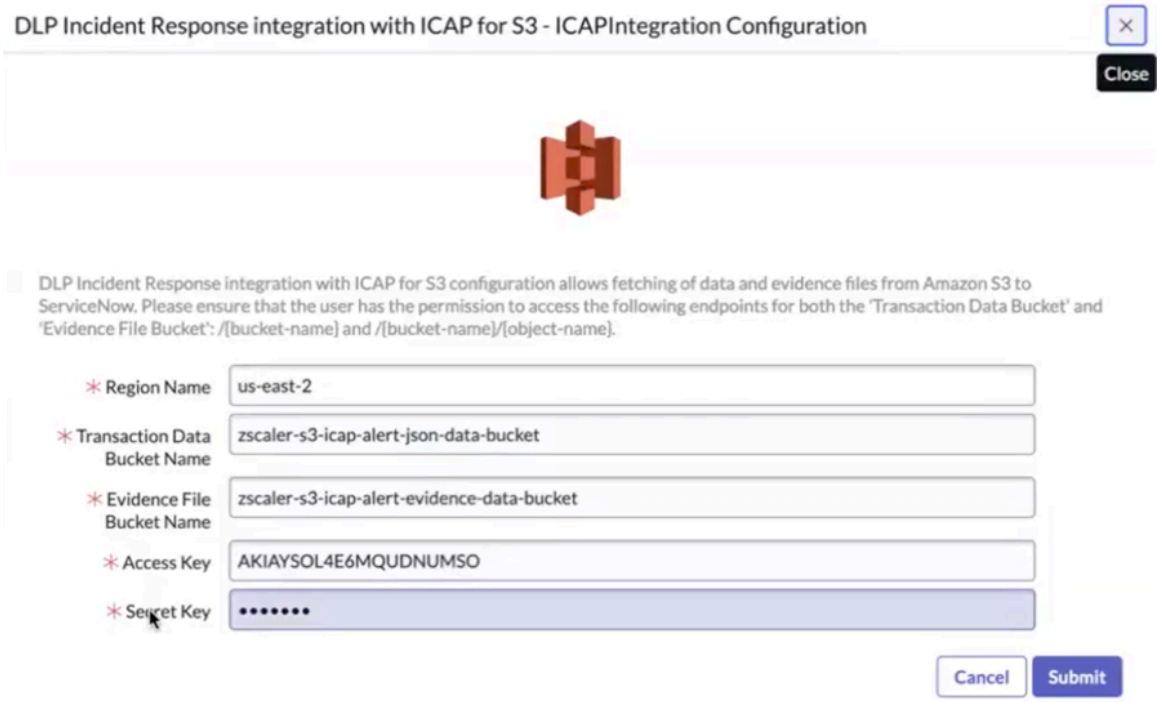
1. プロバイダーの ICAP DLP 統合を ServiceNow® Store からダウンロードしてインストールします。
2. 次のように移動する。 セキュリティオペレーション > 統合 > 統合設定.
3. [ICAP の DLP インシデントレスポンス統合] タイルを検索し、[構成] をクリックします。
4. フォームのフィールドに入力します。

ICAP DLP 統合構成フォーム

フィールド	説明
リージョン名	Amazon S3 バケット名のリージョン名。
トランザクションデータバケット名	トランザクションデータバケット名は、DLP 違反トランザクションが発生したバケットです。
証拠ファイルのバケット名	証拠ファイルのバケット名は、違反の原因となった DLP ファイルを見つけることができるバケットです。
アクセス キー	ICAP 構成の AWS IAM アクセスキー。
秘密キー	ICAP 構成の AWS IAM 秘密キー。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. [**Submit** (送信)] を選択します。

タスクの結果

注:
ICAP サブ本番環境を ServiceNow サブ本番環境に接続してください。アカウントがログアウトされないように、インスタンス間ですべてのユーザー名とパスワードの同期を維持します。

構成の検証と送信が正常に完了すると、ICAP DLP 統合構成が保存されます。

ICAP DLP 統合のプロファイルの作成

Now Platform インスタンスでインシデントプロファイルを作成します。DLP インシデントの作成に適した ICAP DLP アラートを判断します。

始める前に

必要なロール：sn_dlir.admin

このタスクについて

Amazon S3 設定から DLP アラートをフェッチするように NowPlatform を設定します。これらのアラートを DLP インシデントとして ServiceNow インスタンスに保存します。

手順

1. 次のように移動する。 **All** (すべて) > **ICAP DLP** 統合 > インシデントプロファイル.

2. [**New**] をクリックします。

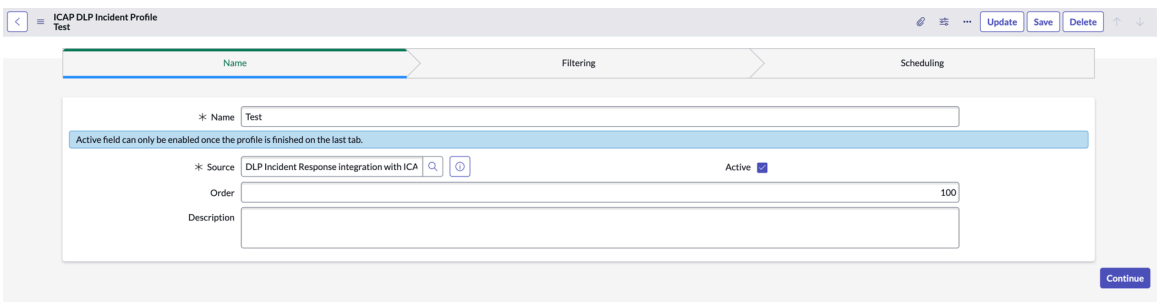
3. フォームで [名前] セクションのフィールドを入力します。

プロファイルの作成

フィールド	説明
名前	プロファイルの名前。このフィールドでプロファイルを識別できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: プロファイルごとに名前は一意である必要があります。
ソース	インシデントを取り込むように構成した Amazon S3 構成。複数のソースが構成されている場合は、プロファイルに取り込む予定のインシデントタイプに適したソースを選択します。 **注:** アクティブなプロファイルに対して許可されるソースは 1 つだけです。
アクティブ	プロファイルがアクティブかどうかを示すオプション。このフィールドは、[スケジューリング] セクションで [完了] をクリックした後にのみアクティブになります。 プロファイルがアクティブな場合は、 Now Platform が ICAP DLP アラートをアクティブにポーリングしていることを意味します。入力したフィルター条件が [スケジューリング] パラメーターに基づいて一致すると、対応する DLP アラートが DLP 内に作成されます。
順序	プロファイルの実行順序。順序の値が最も小さいプロファイルの優先度が最も高いと見なされます。 デフォルト値は 100 です。
説明	このプロファイルの説明。



次のタスク
[フィルタリング] セクションに移動するには、[続行] をクリックします。

インシデント作成の際に適用するフィルターの定義

受信 DLP アラートをフィルタリングするためのフィルター条件を定義して設定します。ServiceNow で DLP インシデントとして作成する必要があるアラートを決定します。

始める前に
必要なロール：sn_dlir.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

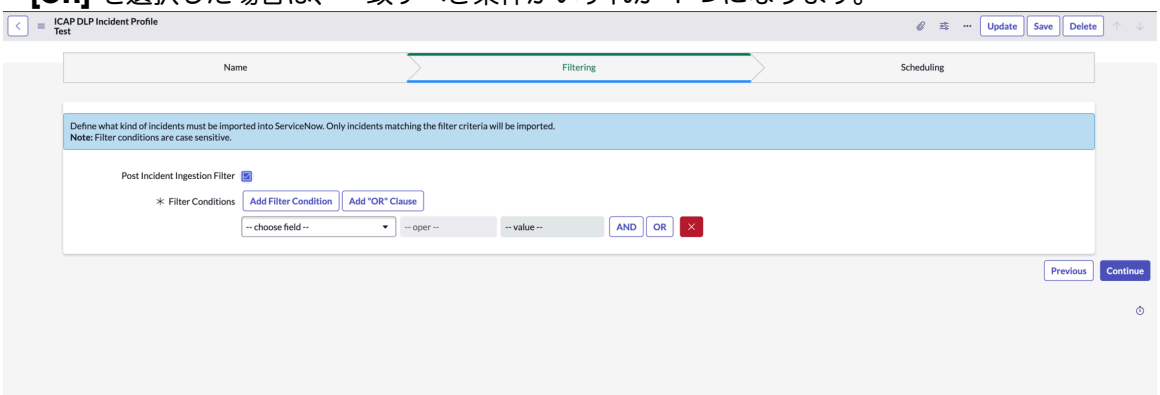
このタスクについて
フィルタリングは、DLP アラートを分離し、作成する DLP アラートの数を制限するのに役立ちます。追加のフィルタリング基準を設定すると、条件に一致するアラートのみが作成されます。

手順

1. [インシデント取り込み後のフィルター] チェックボックスをオンにして、インシデント取り込み後のフィルターを適用し、フィルター基準に一致するインシデントを取得します。
2. [条件に基づいてフィルター] オプションを選択し、DLP インシデントを作成するために受信 ICAP DLP インシデントが満たす必要がある条件を定義します。
3. [フィルター条件] フィールドでフィルターを設定します。

   ドロップダウン フィルター条件 のオプションは、 **ICAP DLP** インシデントインポート テーブルで利用可能なフィールドと一致します。入力する基準は大文字と小文字を区別します。定義した基準がインシデントの値と一致していることを確認します。

4. **[AND]** または **[OR]** をクリックして条件を追加します。
   - **[AND]** を選択した場合は、すべての条件に一致する必要があります。
   - **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。



次のタスク
スケジュールを設定するには、[続行] をクリックします。

ICAP DLP インシデントの取得をスケジュールする

プロファイルの基準に一致する ICAP DLP アラートを取得するスケジュールを設定します。

始める前に
必要なロール：sn_dlir.admin

このタスクについて
インシデントプロファイル構成に一致する正味の新しい ICAP インシデントをポーリングする頻度を計画できます。インシデントの自動取り込みを有効にするには、プロファイルをアクティブ化する前に、スケジュールとインシデントの取得を設定する必要があります。**[1** 回限りの 取得] チェックボックスを使用すると、1 回限りの取得を実行するようにプロファイルを構成できます。

手順

1. スケジュールを構成して、ICAP からインシデントをプルする方法とタイミングを定義します。
2. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ICAP DLP インシデントのスケジュール

フィールド	説明
進行中のインシデントの取り込み	Now Platformインスタンスが新しいインシデントのために ICAP からプルする進行中のインシデントの取り込み。インシデントのフィルタリング基準に一致するトリガーされたインシデントが見つかった場合は、DLP インシデントが作成されます。
ポーリングインクリメント (分)	定義されたポーリング頻度 (分単位)。このデフォルト値は **5** に設定されています。
最初のインシデントの取り込み時刻を設定	構成された日時に基づいて最初のインシデントの取り込みを設定するオプション。 このオプションを使用して、最初の取り込みに対する特定の日時を定義できます。それ以降の取り込みはポーリング間隔の時間に基づいて決まります。
入力の最初のインシデントの取り込み時刻	インシデントの取り込みに指定した日時。
最初のインシデントの取り込み時刻	データが初めて取り込まれる時刻。 **注:** この値は、[最初のインシデントの取り込み時刻を設定] オプションが選択されている場合にのみ表示されます。
次のインシデント取り込み時刻 (推定)	次のインシデント取り込みの推定時刻。
1 回限りの取得	履歴データの 1 回限りのプルを有効にするオプション。 **注:** 選択すると、[開始日] に追加された日付に従って、ICAP DLP から履歴データが取得されます。
フォルダ名	データの取得元のフォルダーの名前。指定されたフォルダー名よりも名前が辞書順に大きいすべてのフォルダーが、1 回限りの取得で取り込まれます。

3. [完了] をクリックします。
4. ポップアップで、[終了] をクリックして、作成したプロファイル構成を保存します。
5. プロファイルを有効化します。
   a. 作成したプロファイルを開きます。
   b. [アクティブ] を **true** に設定します。
   c. [更新] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスクの結果
プロファイルが正常に作成およびアクティブ化されると、プロファイルで設定された構成に従って、インシデントが定期的に取得されます。アラートは DLP インシデントテーブルに追加されます。

DLP アラートの機密情報の表示

DLP アラートの検出された機密情報を表示します。

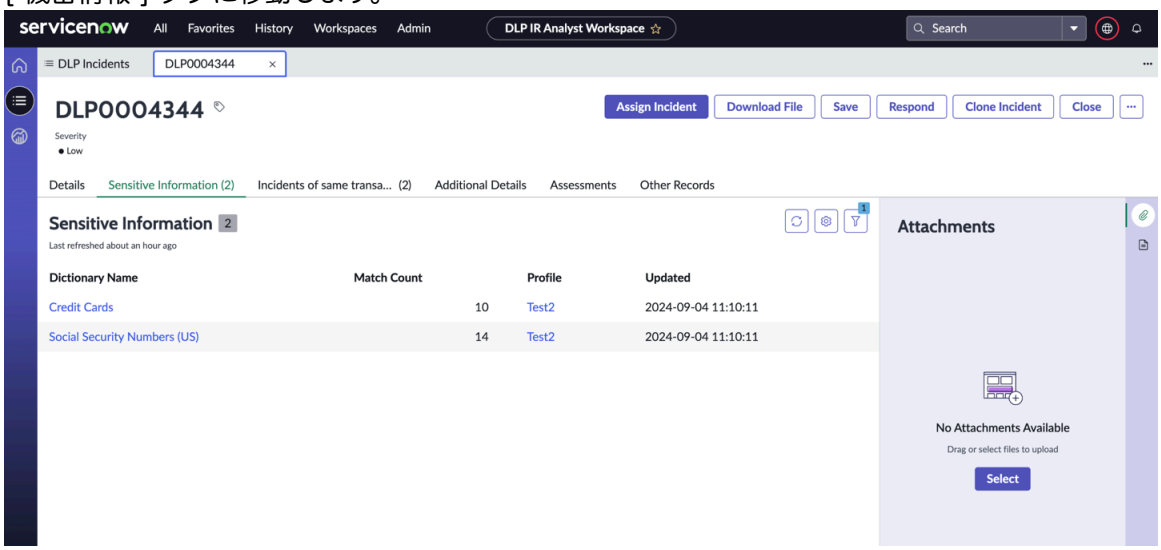
始める前に
それぞれの統合には特定のルールとポリシーが構成されており、定義されたポリシーに違反している場合は、DLP インシデントが作成され、一致コンテンツのその DLP インシデントレコードの [機密情報] セクションにその違反情報が表示されます。

必要なロール：sn_dlir.analyst

> **注:**
> エンドユーザーは、DLP ユーザーワークスペースにログインして機密情報を表示することもできます。

手順

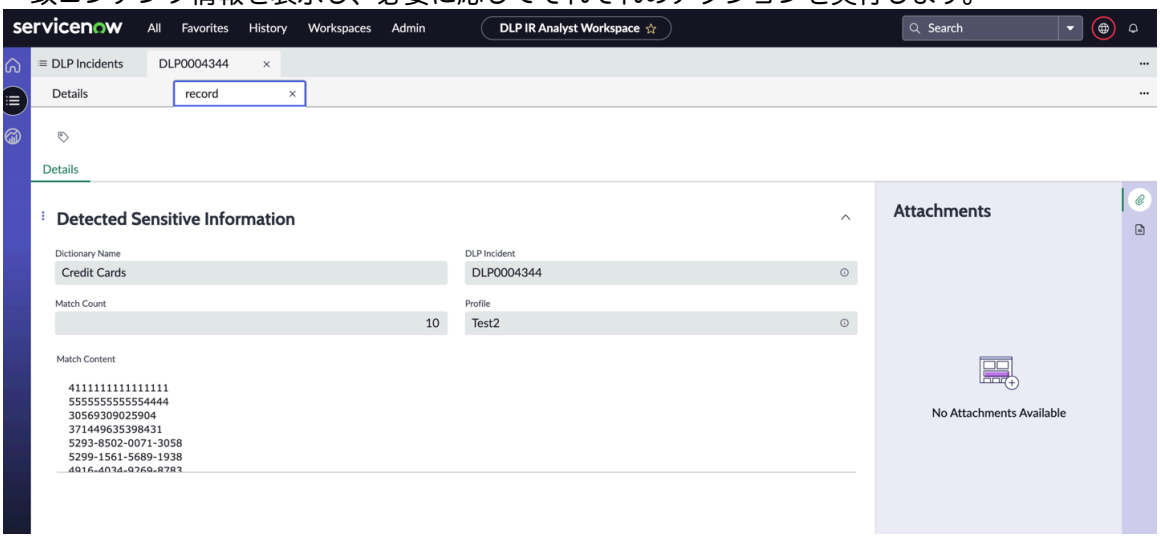
1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース. [DLP ワークスペース - 自分のインシデント (DLP Workspace - My Incidents)] ページが、アナリストの DLP アナリストワークスペースに表示されます。
2. 任意の DLP インシデントを開きます。
3. [機密情報] タブに移動します。



4. 違反レコードをクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. 一致コンテンツ情報を表示し、必要に応じてそれぞれのアクションを実行します。



DLP アラートの証拠ファイルのダウンロード

ICAP をサポートするプロバイダーの DLP ポリシーに違反するファイルをダウンロードします。承認者用の DLP IR アナリストワークスペースと DLP IR エンドユーザーワークスペースから、このファイルをローカルマシンにダウンロードします。

始める前に

必要なロール：

- sn_dlir.analyst と承認者はダウンロードできます

このタスクについて

先に進む前に、ICAP のファイルのダウンロードを有効にする必要があります。

手順

1. 次のように移動する。 **All** (すべて) > **ICAP DLP** 統合 > 設定.
2. プロパティ sn_icap_dlp.enable_file_download を有効にする このプロパティを有効にすると、報告された **ICAP** インシデントの証拠ファイルをダウンロードできます。
   DLP IR アナリストワークスペースと DLP IR エンドユーザーワークスペースに [ファイルのダウンロード] ボタンが表示されます。
3. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.
4. ICAP プロバイダーソースから取り込まれた DLP インシデントレコードを開きます。
5. [ファイルのダウンロード] をクリックします。

> **注:**
> DLP 管理者は、DLP 管理の [詳細設定] ページから [報告されたインシデントの違反ファイルのダウンロードを許可すべきですか] オプションを無効にすることで、すべての統合の [ファイルのダウンロード] アクションのアクセスを制御できます。詳細については、「詳細設定を構成します」を参照してください。

ICAP の証拠ファイルのプレビュー

DLP IR アナリストワークスペースで DLP インシデント証拠ファイルをプレビューします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に

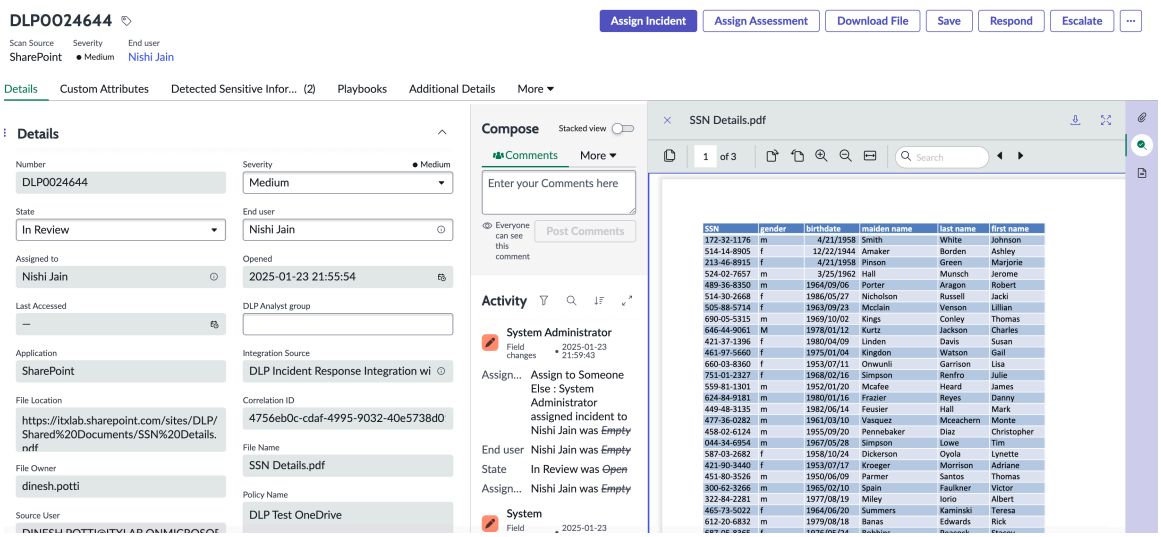
- 次のように移動する。 **All** (すべて) > **DLP** 管理 > 詳細設定.
- **sn_icap_dlp.enable_evidence_file_preview** プロパティが既に有効になっていることを確認してください。

> **重要:**
> DLP アナリストワークスペースで証拠ファイルアクションを使用している間、証拠ファイルは、[詳細設定] ページの **sn_dlir.preview_temp_files_cleanup_interval** プロパティを使用して選択した期間、暗号化されていない形式で ServiceNow データベースに一時的に保存されます。ServiceNow データベースにデータを保存しない場合は、 証拠ファイルの プレビュー機能を無効にすることができます。詳細については、「詳細設定を構成します」を参照してください。

必要なロール：sn_dlir.analyst

手順

1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.
2. DLP インシデントレコードを開きます。
3. コンテキストメニューにある 証拠ファイル アイコンを選択します。
   すべての証拠ファイルを取得するタブが開きます。ダウンロードが完了すると、[証拠ファイル] タブですべての証拠ファイルを表示できます。
4. プレビューする 証拠ファイル カードを選択します。
   プレビュー機能は、ファイルタイプごとに異なります。
5. ドキュメントビューアーで PDF と Office ドキュメントをプレビューするには、証拠ファイルの右上にある [展開] アイコンを選択して PDF を全画面で開きます。
   ドキュメントビューアーが証拠ファイルを開く Office 拡張機能には、doc、docx、ppt、pptx、xls、xlsx などがあります。
   a. 検索バーを見つけて、探しているキーワードを入力します。
   b. ズームインおよびズームアウト機能を使用して、ビューが読みやすくなるように調整します。
   c. コンテンツをより鮮明に表示するには、ページを時計回りまたは反時計回りに回転させます。
   これらのコントロールオプションにより、証拠ファイルを包括的に理解する能力が向上します。
   ヘッダーにコントロールオプションがあるのは PDF だけです。



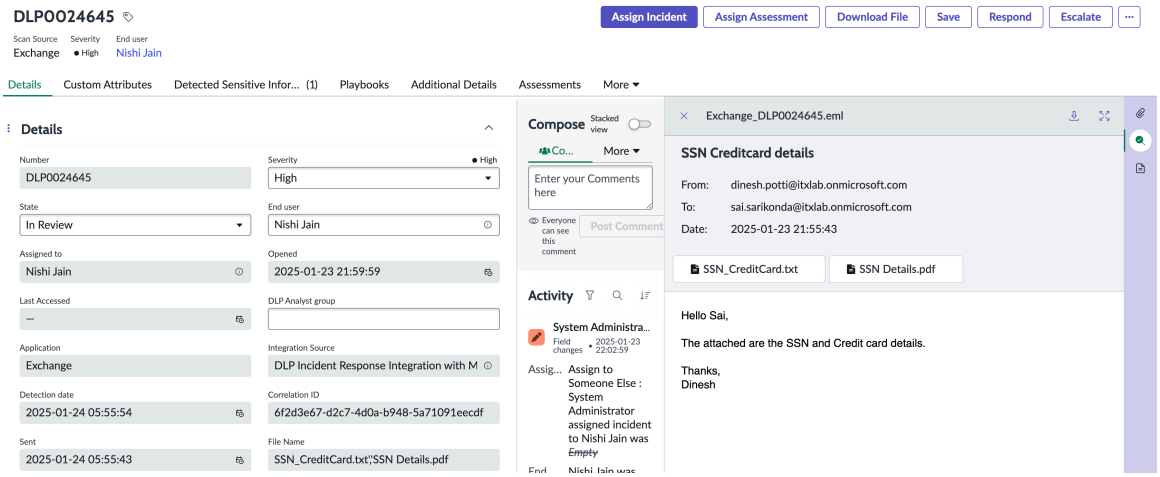
6. eml ファイルをプレビューします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

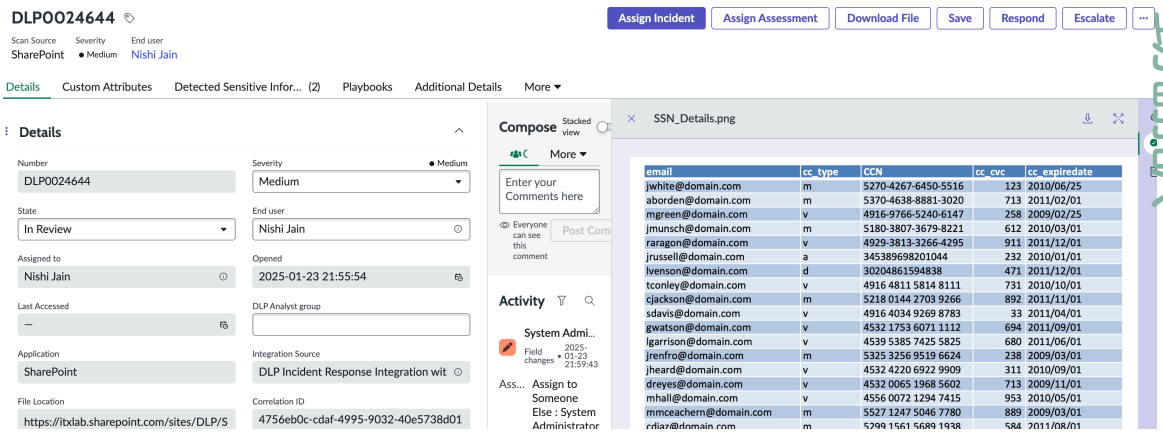
自動翻訳

メールの添付ファイルを選択してプレビューします。

注:
選択した証拠ファイルが 5 MB の制限を超えた場合、アナリストワークスペースでプレビューすることはできません。コンテンツをプレビューするには、ファイルをダウンロードする必要があります。この制限は、.emlファイルに対してのみ適用されます。

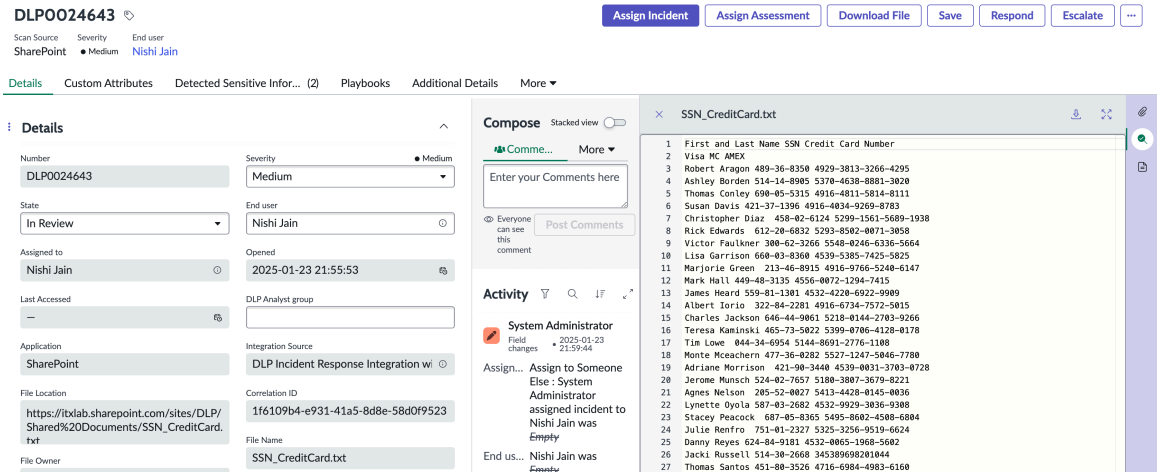


7. DLP アナリストワークスペースで画像をプレビューします。
.bmp、.gif、.ico、.jpeg、.jpg、.png、.svg、および .webp 拡張子のイメージのみがサポートされています。



8. 証拠ファイルの右上にある [展開] アイコンを選択して、テキストエディターでテキストファイルをプレビューします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
Office ドキュメント以外の証拠ファイル、eml ファイル、テキスト、画像拡張子は、プレビューではサポートされません。バイナリファイルはレンダリングされないため、コンテンツをプレビューするにはダウンロードする必要があります。証拠ファイルのプレビュー機能は、アーカイブされたインシデントでも機能します。

ICAP DLP 統合設定の確認

プロバイダーの ICAP DLP 統合設定を確認し、環境に合わせてデフォルトのシステムプロパティを変更します。

始める前に
必要なロール：sn_dlir.admin

手順

1. 次のように移動する。 **All** (すべて) > **ICAP DLP** 統合 > 設定.
2. 設定の確認と変更が必要です。

Microsoft 付きの Data Loss Prevention Incident Response

Data Loss Prevention Incident Response with Microsoft は、Microsoftプレビューアプリ (Microsoft Teams、Exchange Online、SharePoint Online、OneDrive for Business) やその他のイベントタイプなどの複数のソースからデータ損失防止 (DLP) インシデントをインポートするためのコアフレームワークを提供します。エンドポイントデバイスは、インシデントのアサインとエスカレーションを自動化し、エンドユーザー、マネージャー、DLP 運用チームが含まれる修復ワークフローを実現します。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

主な機能

この統合の主な機能を使用して、次のアクションを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 異なるアカウントに対する複数のプロファイルの作成。
- DLP IR インシデントの作成の自動化。
- Microsoft DLP IR イベントフィールドの DLP IR インシデントフィールドへのマッピング。
- Microsoft DLP IR イベントのフィルタリング。
- DLP IR インシデントを定期的に作成する DLP IR イベントの取り込みのスケジュール設定。
- 各 Microsoft DLP イベントの一致するコンテンツの、外部クラウドストレージへの保存。
- ServiceNow での DLP IR インシデントの削除時の、外部クラウドストレージにある一致するコンテンツの削除。
- Exchange、OneDrive、および SharePoint タイプの DLP IR インシデントのファイルのダウンロード。

この統合の詳細

ドキュメント識別子	ドキュメントタイトル
Microsoft 製品ドキュメント Web サイト	Microsoft 製品ドキュメント Web サイト
ServiceNow 製品ドキュメント Web サイト	ServiceNow 製品ドキュメント Web サイト

Microsoft DLP IR integration for Data Loss Prevention の概要

データ損失防止のための Microsoft DLP IR 統合の設定を開始する前に、次の情報を確認します。

チェックリスト

セットアップタスク	説明
イベントデータを取得するための Microsoft Purview 認証情報と、一致するコンテンツを保存するための AWS/Azure ストレージアカウント認証情報を取得する アプリケーションを Microsoft ID プラットフォームに登録する	ここ から Microsoft Azure プラットフォームにアプリケーションを登録して、クライアント ID、クライアントシークレット、およびテナント ID を取得します。アプリケーションの作成に必要なロールについては、「前提条件 」を参照してください。 ServiceNow Microsoft DLP 統合で Microsoft Azure アプリケーションを構成するために必要な API 権限/ロールについては、次の表を参照してください。
Azure ユーザーが Azure Storage で読み取り/書き込み/削除 BLOB のアクセス権を取得するために必要な権限	Azure ユーザーは、Azure Storage で BLOB を読み取り、書き込み、および削除するための [ストレージ **BLOB** データ共同作成者] ロールを持っている必要があります。
AWS ユーザーが AWS Storage で読み取り/書き込み/削除オブジェクトのアクセス権を取得するために必要な権限	AWS S3 ストレージ内のオブジェクトの一覧表示、読み取り、書き込み、および削除のアクセス権を付与するポリシーを作成する必要があります。
Now Platform に必要なロールとデータ損失管理ロールを持っていれば、それをアサインして確認する	期待される結果を構成および検証するには、次のロールが必要です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チェックリスト (続く)

セットアップタスク	説明
	• admin ロールは、ServiceNow Store から統合をインストールし、sn_dlir.admin ロールを割り当てます。 • 次のタスクを実行するには、sn_dlir.admin ロールが必要です。 ○ 統合を構成します。 ○ インシデントプロファイルを設定します。
この統合を構成する前に、Microsoft DLP IR 統合をサポートするために必要な ServiceNow コアアプリケーションがインストールされ、アクティブ化されていることを確認します。	次の DLP IR アプリケーションと Security Support Common アプリケーションが ServiceNow Store からインストールされ、アクティブ化されていることを確認します。インストールされていない場合は、 アプリケーションをインストールしてアクティブ化します。 • Security Support Common • Data Loss Prevention Incident Response

Microsoft Azure アプリケーションで必要な **API** 権限/ロール

ServiceNow ***Microsoft DLP*** 統合で ***Microsoft Azure*** アプリケーションを構成するには次の ***API*** 権限/ロールが必要です。

API	権限名	タイプ	説明	どの **ServiceNow** の機能に必要か	アドミンの同意が必要かどうか
Office 365 管理 API	ActivityFeed.ReadDlp	アプリケーション	検出された機密データを含む DLP ポリシーイベントを読み込みます。	DLP イベントを MSFT Purview から ServiceNow に取り込みます。 **注:** この権限は、MSFT データを ServiceNow に取り込むために必須です。	はい
Microsoft Graph API	Files.Read.All	アプリケーション	アクセス可能なすべてのサイトコレクションのファイルを読み取ります。	ファイルのダウンロード：DLP イベントの原因となった ServiceNow インスタンスの添付ファイルを OneDrive または SharePoint からダウンロードします。	はい

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Microsoft Azure アプリケーションで必要な **API** 権限/ロール

ServiceNow *Microsoft DLP* 統合で *Microsoft Azure* アプリケーションを構成するには次の *API* 権限/ロールが必要です。

(続く)

API	権限名	タイプ	説明	どの **ServiceNow** の機能に必要か	アドミンの同意が必要かどうか
				注: これはオプションです。DLP イベントの原因となった添付ファイルのダウンロードをアナリストに許可しない場合は、この API 権限をスキップできます。	
	Mail.Read	アプリケーション	すべてのメールボックスのメールを読み取ります。	ファイルのダウンロード：DLP イベントの原因となった ServiceNow インスタンスのメールコンテンツ (本文と添付ファイル) を Exchange からダウンロードします。 **注:** これはオプションです。DLP イベントの原因となったメールコンテンツ (本文、添付ファイル) のダウンロードをアナリストに許可しない場合は、この API 権限をスキップできます。	はい
	User.Read	委任	サインインしてユーザープロファイルを読み込みます。	これは、すべての新しいアプリケーションで使用できるデフォルトの権限です。	いいえ

検出された機密情報タイプ (オプション)

一致コンテンツは、外部の Azure BLOB ストレージまたは Amazon S3 バケットに保存され、ユーザーがインシデントを表示するときに外部ストレージからプルされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザーが DLP Core アプリケーションで一致コンテンツ/検出された機密情報を表示する場合は、次のいずれかの権限が必要です。

1. Microsoft Azure ユーザーである場合は、Azure Storage で BLOB を読み取り、書き込み、および削除するための [ストレージ BLOB データ共同作成者] ロールを持っている必要があります。
2. Amazon S3 ユーザーである場合は、AWS S3 ストレージ内のオブジェクトの一覧表示、読み取り、書き込み、および削除のアクセス権を付与するポリシーを作成する必要があります。

Microsoft DLP 統合のインストールと構成

Now Platform インスタンスの ServiceNow® Storeから DLP Incident Response integration with Microsoft DLP をインストールして構成します。Microsoft DLP イベントデータを使用して DLP インシデントの調査を開始します。

始める前に
必要なロール：sn_dlir.admin

手順

1. Microsoft DLP 統合から ServiceNow® Store をダウンロードしてインストールします。
2. 次のように移動する。 セキュリティオペレーション > 統合 > 統合設定.
3. Microsoft DLP☒ 統合の構成

   a. **[Microsoft** の **DLP** インシデントレスポンス統合] タイルを検索して、[構成] をクリックします。

   b. フォームのフィールドに入力します。

Microsoft DLP Integration Configuration フォーム

フィールド	説明
名前	Microsoft DLP 統合構成の名前。
クライアント ID	Microsoft Azure ポータルで作成されたアプリのクライアント ID。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
クライアントシークレット	Microsoft Azure ポータルで作成されたアプリのクライアントシークレット。
テナント ID	ユーザーのテナント ID。

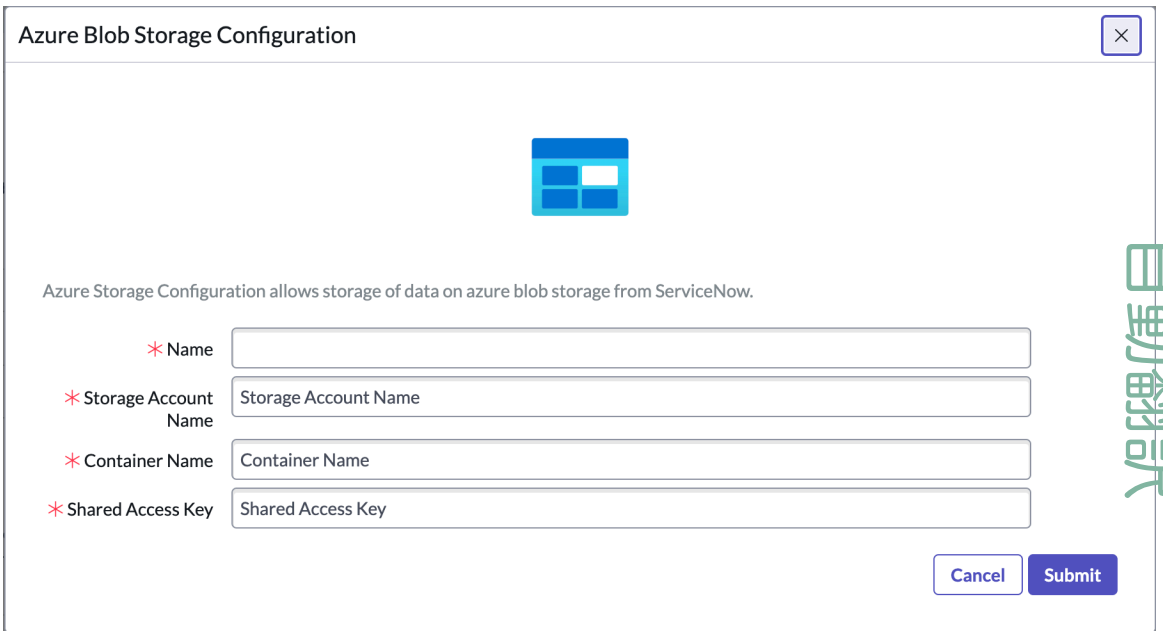
c. [送信] をクリックします。

構成の検証と送信が正常に完了すると、Microsoft DLP 統合が [セキュリティ統合] ページにタイルとして保存されます。

4. Azure Storage 構成を更新します。

a. [セキュリティ統合] ページで、**[Azure Storage** 構成] タイルを検索します。

b. [Azure Storage 構成] タイルで、[更新] をクリックします。



自動翻訳

c. フォームのフィールドに入力します。

Azure Storage 構成フォーム

フィールド	説明
名前	Azure Storage 構成の名前。
ストレージアカウント名	Azure ポータルで作成されたストレージアカウント名。
コンテナ名	Azure ポータルでストレージアカウント内に作成されたコンテナ名。
共有アクセスキー	ストレージアカウントの共有アクセスキー。

d. [送信] をクリックします。

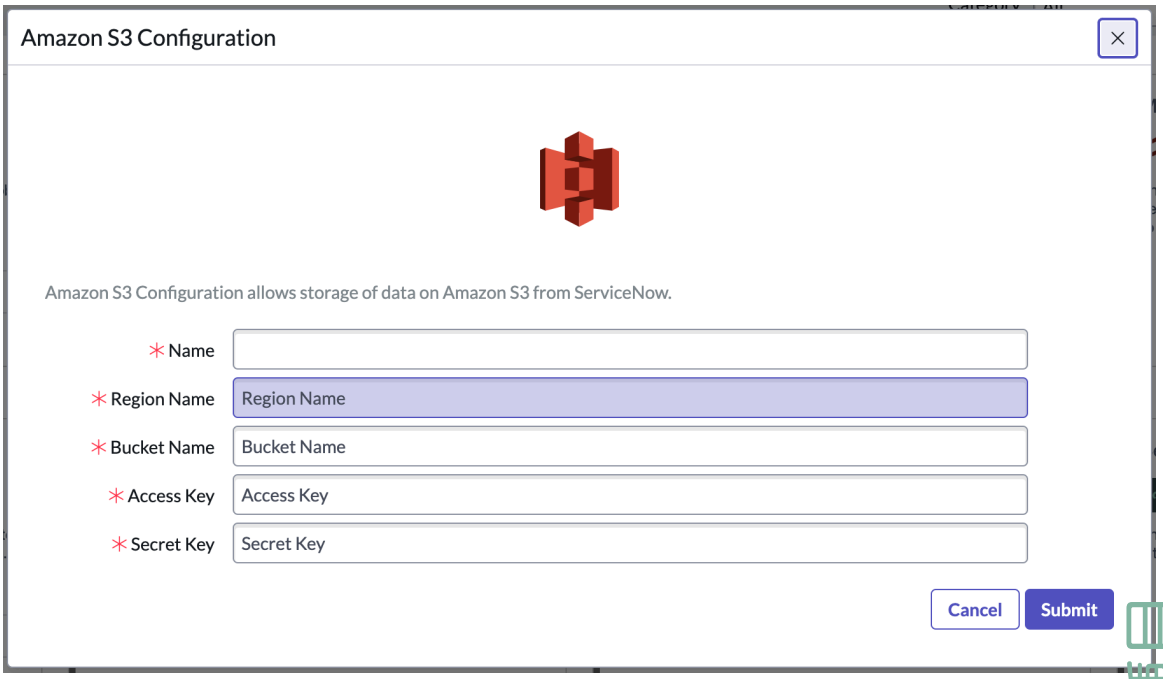
構成の検証と送信が正常に完了すると、Azure Storage 構成が [セキュリティ統合] ページにタイルとして保存されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. AWS Storage 構成を更新します。

a. [セキュリティ統合] ページで、**[AWS Storage** 構成] タイルを検索します。

b. [AWS Storage 構成] タイルで、[更新] をクリックします。



c. フォームのフィールドに入力します。

AWS Storage 構成フォーム

フィールド	説明
名前	AWS Storage 構成の名前。
リージョン名	AWS Storage アカウントのリージョン名。
バケット名	AWS ポータルで作成されたバケット名。
アクセス キー	読み取り、書き込み、および削除アクセス権を持つアクセスキー。
秘密キー	読み取り、書き込み、および削除アクセス権を持つ共有キー。

d. [送信] をクリックします。

タスクの結果
構成の検証と送信が正常に完了すると、AWS S3 構成が [セキュリティ統合] ページにタイルとして保存されます。

Microsoft DLP 統合の新しいインシデントプロファイルの作成

Now Platform インスタンスで Microsoft Purview からデータを取得してそのデータを ServiceNow DLP IR インシデントテーブルに追加するためのインシデントプロファイルを作成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：sn_dlir.admin (作成、編集、削除)

sn_dlir.analyst - 表示 (読み取り専用)

このタスクについて
Microsoft Purview からイベントを取得するように Now Platform を構成します。取得したイベントは ServiceNow インスタンスの DLP IR インシデントテーブルに保存します。

手順

1. 次のように移動する。 **Microsoft DLP** 統合 > インシデントプロファイル.
2. [**New**] をクリックします。
3. フォームで [名前] セクションのフィールドを入力します。

プロファイルフォームの作成

フィールド	説明
名前	プロファイルの名前。このフィールドでプロファイルを識別できます。 **注:** プロファイルごとに名前は一意である必要があります。
ソース	インシデントを取り込むように構成した Microsoft DLP IR インスタンス。複数の統合が構成されている場合は、プロファイルに取り込む予定のインシデントタイプに適した統合設定レコードを選択します。
アクティブ	プロファイルがアクティブかどうかを示すオプション。このフィールドは、[スケジューリング] セクションで [完了] フィールドをクリックした後にのみアクティブになります。 プロファイルがアクティブな場合は、Now Platform がプロファイルで定義された構成に基づいて Microsoft DLP IR イベントをアクティブにポーリングしていることを暗示します。
順序	プロファイルの実行順序。順序の値が最も小さいプロファイルの優先度が最も高いと見なされます。 デフォルト値は 100 です。
説明	プロファイルの固有の説明。

次のタスク
[フィルタリング] セクションに移動するには、[続行] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インシデント作成の際に適用するフィルターの定義

受信した Microsoft DLP イベントをフィルタリングするためのフィルター条件を定義して設定します。受信したイベントのうちのどれを ServiceNow インスタンスで DLP IR インシデントとして作成すべきかを制御します。

始める前に

必要なロール：sn_dlir.admin (作成、編集、削除)

sn_dlir.analyst - 表示 (読み取り専用)

このタスクについて

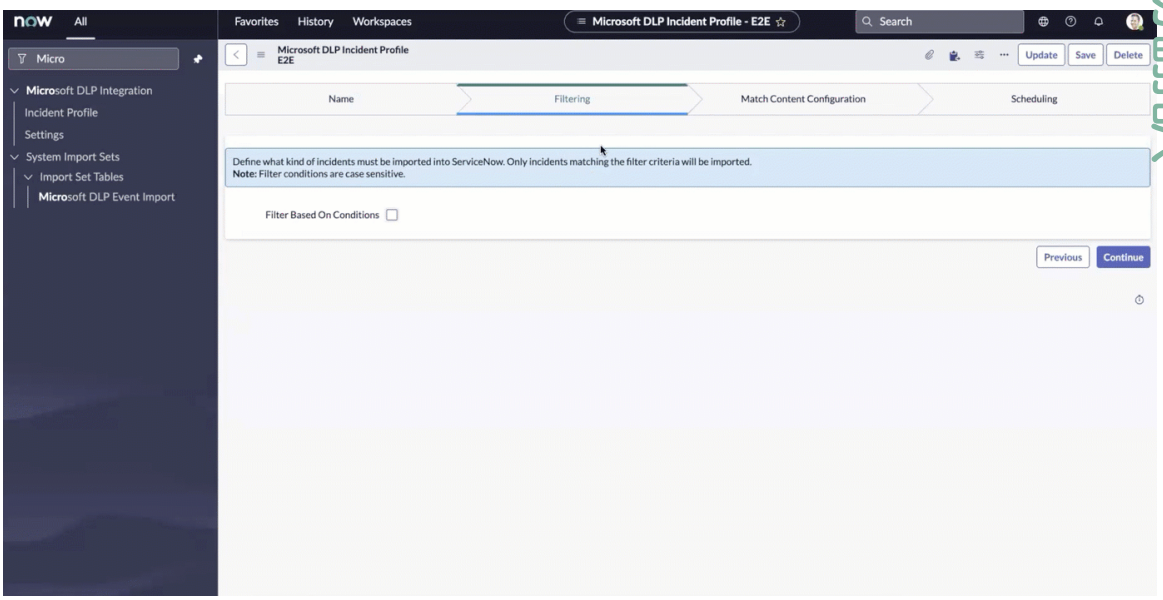
このタイプのフィルタリングは、Microsoft DLP イベントを切り分けて、作成する DLP IR インシデントの数を制限する際に役立ちます。フィルタリング基準が設定されている場合は、その条件に一致するイベントのみが DLP インシデントとして作成されます。

手順

1. [条件に基づいてフィルター] オプションを選択します。
2. 条件ビルダーのリストとフィールドを使用して、[フィルター条件] フィールドにフィルターを設定します。

   DLP インシデントを作成するために、受信される Microsoft DLP イベントが満たすべき条件を定義します。

   [フィルター条件] の最初のフィールドのオプションは、Microsoft DLP イベントで使用可能なフィールドと一致します。入力する基準は大文字と小文字を区別します。定義した基準がイベントの値と一致していることを確認します。



3. **[AND]** または **[OR]** をクリックして条件を追加します。
   - **[AND]** を選択した場合は、すべての条件に一致する必要があります。
   - **[OR]** を選択した場合は、一致すべき条件がいずれか 1 つになります。
4. [続行] をクリックし、[一致コンテンツの構成 (Match Content Configuration)] セクションに移動します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インシデントの一致コンテンツの構成

DLP IR インシデントにアクセスするときに、ロードの時点でそのコンテンツを取得できるようにするため、Azure ストレージや AWS S3 バケットなどの外部クラウドストレージに機密情報を保存する構成を指定します。

始める前に
必要なロール：sn_dlir.admin (作成、編集、削除)

sn_dlir.analyst - 表示 (読み取り専用)

手順

1. 進捗状況バーの [コンテンツ構成の一致 **(Match Content Configurationn)]** ステップをクリックします。
2. フォームのフィールドに入力します。

一致コンテンツ構成 **(Match Content Configuration)**

フィールド	説明
一致コンテンツを保存 (Store Match Content)	一致するコンテンツをクラウドストレージに保存するオプション。 **重要:** このオプションをオンにしないと、DLP インシデントのポリシー一致コンテンツは DLP ワークスペースに表示されません。このオプションを有効にすることで、DLP インシデントで返された一致コンテンツが外部クラウドストレージ (Azure、AWS など) に保存されます。DLP インシデントがワークスペースで開かれるたびに、一致コンテンツを取得して表示することもできます。 外部クラウドストレージの構成の詳細については、「Microsoft DLP 統合のインストールと構成」を参照してください。
インシデント削除時に一致コンテンツを削除 (Delete Match Content on Incident Deletion)	インシデントの一致コンテンツを外部クラウドストレージから削除するオプション。このオプションは、[一致コンテンツを保存 **(Store Match Content)]** フィールドが選択されている場合にのみ表示されます。
外部クラウド認証情報 (External Cloud Credentials)	一致コンテンツが保存される外部クラウドストレージ。ストレージ構成用に追加された外部クラウド認証情報を参照できます。このオプションは、[一致コンテンツを保存 **(Store Match Content)]** フィールドが選択されている場合にのみ表示されます。

3. [続行] をクリックし、[スケジューリング] セクションに移動します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

DLP IR Microsoft インシデントの取得のスケジュール設定

インシデントデータを取得し、プロファイルの基準に一致する Microsoft DLP IR インシデントを取り込むスケジュールを設定します。Microsoft からインシデントをプルする方法とタイミングを定義するスケジュールを設定します。

始める前に
必要なロール：sn_dlir.admin (作成、編集、削除)

sn_dlir.analyst - 表示 (読み取り専用)

このタスクについて
インシデントプロファイル構成に一致する将来のインシデントをポーリングする頻度を設定できます。インシデントの自動取り込みを有効にするには、プロファイルをアクティブ化する前に、スケジュールとインシデントの取得を設定する必要があります。**[1** 回限りの 取得] チェックボックスを使用すると、1 回限りの取得を実行するようにプロファイルを構成できます。過去の日付は 最大 3 か月前以降に設定できます。

ポーリング間隔は、各プロファイルで個別に設定されます。ポーリング間隔が異なると、Microsoft DLP IR インシデント統合のパフォーマンスに影響する可能性があります。スケジュールを設定するときは、インシデントの緊急度とシステム負荷のバランスを取るように計画してください。

手順

1. データを取得し、プロファイルの基準に一致するインシデントを取り込むスケジュールを設定します。
2. フォームのフィールドに入力します。

DLP インシデントフォームのスケジュール

フィールド	説明
進行中のインシデントの取り込み	Now Platform インスタンスが Microsoft から新しいインシデントを取得する、進行中のインシデントの取り込み。トリガーされたインシデントが検出され、インシデント生成のフィルター基準が一致すると、DLP IR インシデントが作成されます。
ポーリングインクリメント (分)	Microsoft からのポーリング頻度。このフィールドは自動的に 300 分に設定されます。
最初のインシデントの取り込み時刻を設定	最初の取り込みの日時を定義するオプション。それ以降の取り込みはポーリング間隔の時間に基づいて決まります。 このオプションは、[進行中のインシデントの取り込み] フィールドが選択されている場合にのみ表示されます。
入力の最初のインシデントの取り込み時刻	インシデントの取り込みに指定した日時。 ○ この値が設定されている場合、Microsoft からのデータ取得は追加された未来の日付から開始されます。 ○ このフィールドは、[最初のインシデントの取り込み時刻を設定] が選択されている場合にのみ表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
最初のインシデントの取り込み時刻	データが最初に取り込まれる時刻。 最初のインシデントの取り込み時刻を設定すると、値の表示が始まります。
次のインシデント取り込み時刻 (推定)	次にインシデントが取り込まれるまでの推定時間。
1 回限りの取得	履歴データの 1 回限りのプルを有効にするオプション。 このフィールドが選択されている場合は、[開始日] フィールドに追加された日付に従って、Microsoft DLP IR から履歴データが取得されます。
開始日	Microsoft からデータを取得すると考えられる日付。 このフィールドは最大 7 日に設定できます。

3. ポップアップで、[終了] をクリックして、作成したプロファイル構成を保存します。
4. プロファイルをアクティブ化します。
   a. 作成したプロファイルを開きます。
   b. [アクティブ] オプションを有効にします。
   c. [更新] をクリックします。

タスクの結果
プロファイルが正常に作成およびアクティブ化されると、プロファイルで設定されて DLP インシデントテーブルに追加された構成に従って、インシデントが定期的に取得されます。

Microsoft DLP IR 統合設定の構成

Microsoft DLP IR 統合のデフォルトのシステムプロパティを変更します。

始める前に
必要なロール：sn_dlir.admin

手順
1. 次のように移動する。 **Microsoft DLP** 統合 > 設定.
2. 必要に応じて、次のプロパティを変更します。

Microsoft DLP 統合の設定

フィールド	説明
HTTP 呼び出しの最大タイムアウト (sn_pp_dlp.maximum_http_time_out)	HTTP 呼び出しの最大タイムアウト (秒単位)。 ○ タイプ：整数 ○ デフォルト値：30

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
統合によって生成されたログのレポートレベル (sn_pp_dlp.logging.verbosity)	統合で生成されたレポートログのレベル (情報のタイプの名前)。値を次のオプションに更新することもできます。 ○ エラー ○ 警告 ○ 情報 ○ **debug** ○ **off** デフォルト値は **INFO** です。
統合によって生成されたログのレポート先 (Destination of reporting the logs generated by the integration) (sn_pp_dlp.logging.destination)	統合によって生成されるログの宛先。値を次のオプションに更新することもできます。 ○ **db** ○ ファイル ○ なし デフォルト値は **db** です。

3. [保存] をクリックします。

タスクの結果
変更した統合設定は、プロファイルで定義されている次のポーリング間隔で適用されます。

隔離からのメールのリリースを要求する **(Request release email from quarantine)**

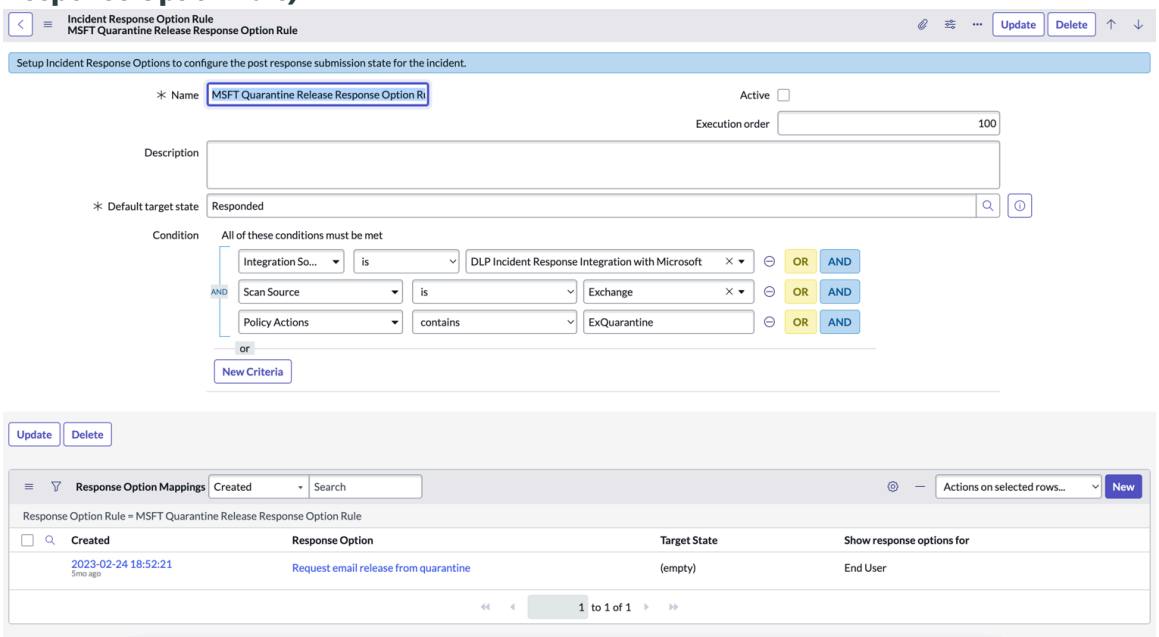
Microsoft Purview コンプライアンスポータルから隔離されたメールをリリースするには、この機能を使用します。

始める前に
デフォルトでは、ベースシステムには、[隔離からのメールのリリースを要求する **(Request mail release from quarantine)]** 応答オプションと、メールを隔離からリリースするための **[MSFT Quarantine Release** 応答オプションルール **(MSFT Quarantine Release Response Option Rule)]** が用意されています。このデフォルトレコードには、このアクションの承認機能を利用できるように **Quarantine Release** 承認ルールも設定されています。詳細については、「インシデントレスポンスオプションルールを作成する」、「DLP インシデントの応答オプションの構成」、「承認ルールを作成する」を参照してください。

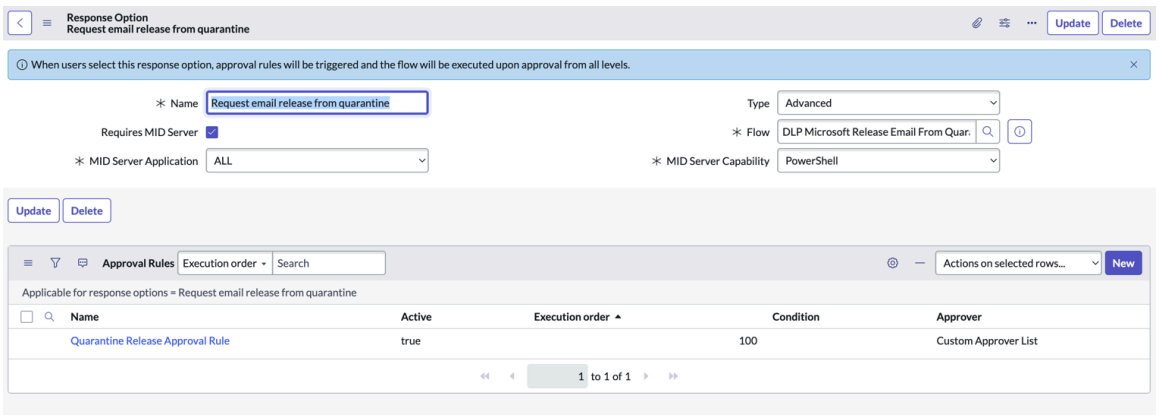
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MSFT Quarantine Release 応答オプションルール (MSFT Quarantine Release Response Option Rule)



デフォルトの MSFT 応答オプション



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
この応答オプションを使用している場合は、PowerShell 機能を使用して MID サーバーが稼働していることを確認してください。MID サーバーが稼働しておらず、PowerShell 機能がない場合、エンドユーザーは DLP ユーザーワークスペースから [隔離からのメールのリリースを要求する **(Request email release from quarantine)]** アクションを選択できません。詳細については、「インシデントレスポンスオプションルールを作成する」と「DLP インシデントの応答オプションの構成」を参照してください。

- リストに特定の MID サーバーが必要な場合は、MID アプリを構成してリストに表示する必要があります。構成されている少なくとも 1 つの MID サーバーが、選択した MID アプリケーションから稼働中であり、Power Shell 機能が含まれている必要があります。
- [検疫からのリリース (Release from quarantine)] オプションを使用するには、API アクセス許可が必要です。[Microsoft API のアクセス許可] ページで、次のことを確認します **Office 365 Exchange Online** > **Exchange.ManageAsApp** がリストされ、次の値が含まれています。
  - タイプ：アプリケーション。
  - アドミンの同意が必要：はい。
  - ステータス：現在の誤った値は、**Office 365 Exchange Online** > **Exchange.ManageAsApp** エントリの **<組織>** に付与されず、ステータス値を変更します。API アクセス許可の詳細な手順については、Microsoft ドキュメントサイトの「アプリケーションに API アクセス許可を割り当てる」を参照してください。

    注:
    この手順は、サービスプリンシパルを使用して Exchange Online に接続するために必要です。

- また、サービスプリンシパルのセキュリティアドミニストレーターロールも必要です。
  - Microsoft Azure ポータルで **Microsoft Entra ID** ロールとアドミニストレーターを検索し、登録済みアプリ (サービスプリンシパル) に割り当てを追加してから、ロールの割り当て方法について Microsoft のドキュメントで説明されている手順に従います。
- このオプションは、インシデントフォームビューで [ポリシーアクション] オプションが **[ExQuarantine]** に設定されている Microsoft Exchange インシデントにのみ適用されます。

必要なロール：エンドユーザー

次の手順では、DLP ユーザーワークスペースからこのアクションを送信する方法について説明します。

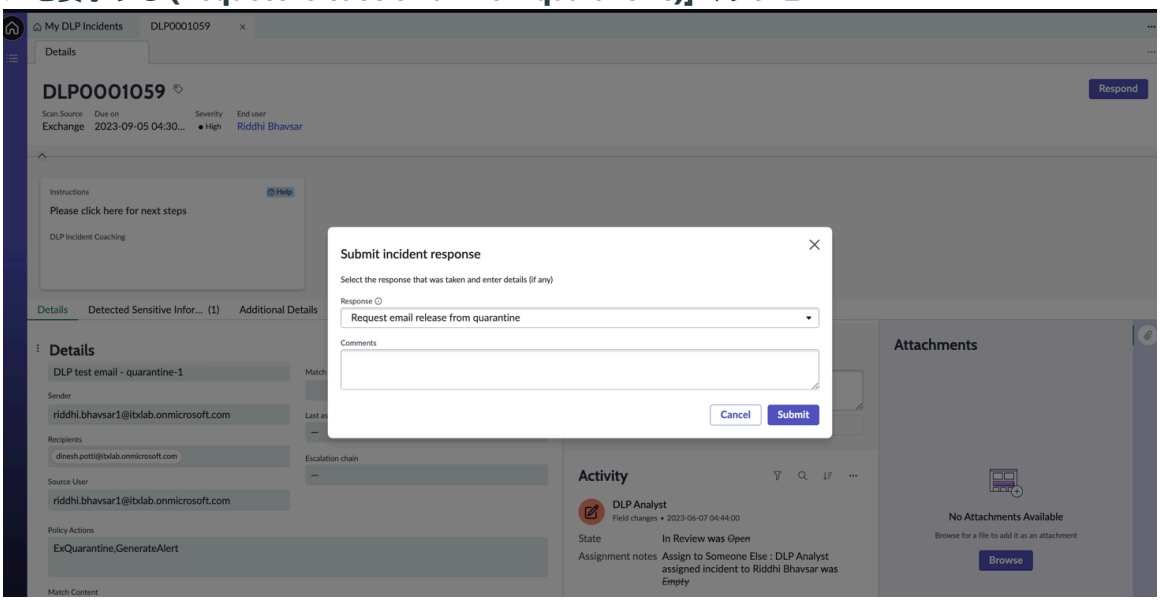
手順

1. 次のように移動する。 **DLP** > **DLP** ユーザーワークスペース.
2. 任意の Microsoft Exchange DLP インシデントを開きます。
   インシデントの [ポリシーアクション] が [ExQuarantine] に設定されていることを確認します。
3. [応答] をクリックします。
4. [応答] ドロップダウンリストから [隔離からのメールのリリースを要求する **(Request email release from quarantine)]** オプションを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[インシデント応答の送信 **(Submit incident response)]** - [隔離からのメールのリリースを要求する **(Request release email from quarantine)]** オプション



5. [送信] をクリックします。

> **注:**
> このアクションに対して承認ルールが設定されている場合、最初に承認フローがトリガーされ、すべての承認を受信した後に [隔離からのメールのリリースを要求する (Request release email from quarantine)] フローがトリガーされ、メールが隔離からリリースされます。リリースが完了すると、DLP インシデントのステータスは [隔離からリリース済み **(Released from Quarantine)]** に更新されます。

自動翻訳

Exchange Online、OneDrive、および **SharePoint** タイプの **DLP** インシデントの証拠ファイルをプレビュー

DLP IR アナリストワークスペースで DLP インシデント証拠ファイルをプレビューします。

始める前に

- 次のように移動する。 **All** (すべて) > **DLP** 管理 > 詳細設定.
- **sn_msft_dlp.enable_evidence_file_preview** プロパティが既に有効になっていることを確認してください。

> **重要:**
> DLP アナリストワークスペースで証拠ファイルアクションを使用している間、証拠ファイルは、[詳細設定] ページの **sn_dlir.preview_temp_files_cleanup_interval** プロパティを使用して選択した期間、暗号化されていない形式で ServiceNow データベースに一時的に保存されます。ServiceNow データベースにデータを保存しない場合は、 証拠ファイルの プレビュー機能を無効にすることができます。詳細については、「詳細設定を構成します」を参照してください。

必要なロール：sn_dlir.analyst

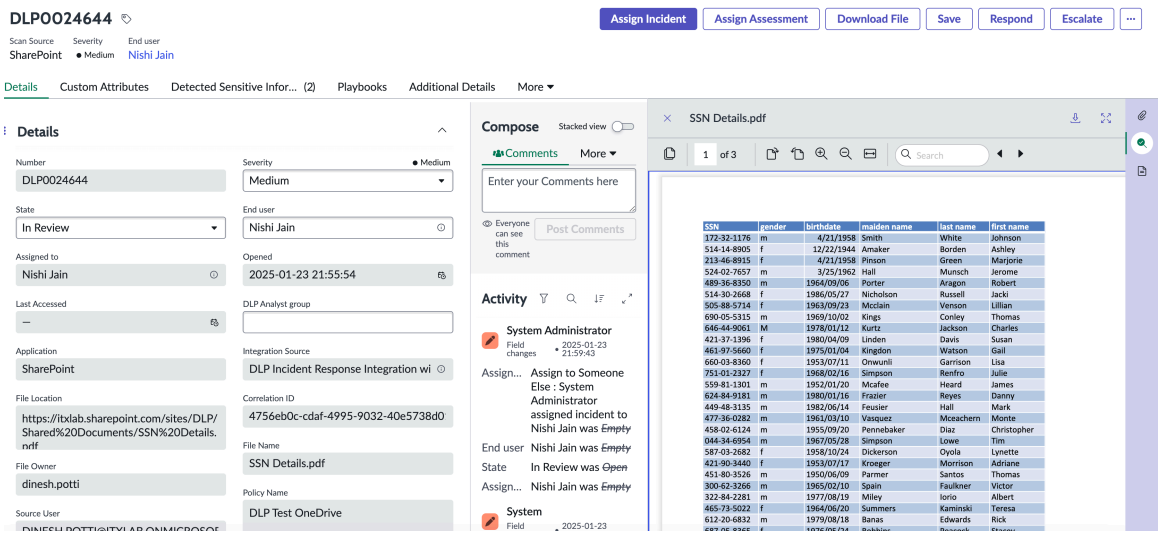
手順

1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.

2. DLP インシデントレコードを開きます。

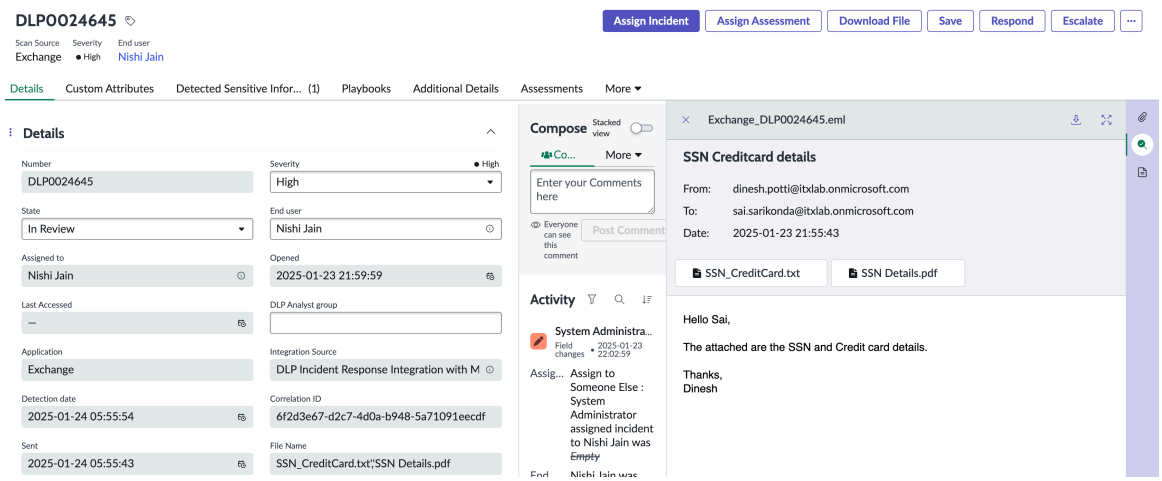
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. コンテキストメニューにある 証拠ファイル アイコンを選択します。
すべての証拠ファイルを取得するタブが開きます。ダウンロードが完了すると、[証拠ファイル] タブですべての証拠ファイルを表示できます。
4. プレビューする 証拠ファイル カードを選択します。
プレビュー機能は、ファイルタイプごとに異なります。
5. ドキュメントビューアーで PDF と Office ドキュメントをプレビューするには、証拠ファイルの右上にある [展開] アイコンを選択して PDF を全画面で開きます。
ドキュメントビューアーが証拠ファイルを開く Office 拡張機能には、doc、docx、ppt、pptx、xls、xlsx などがあります。
   a. 検索バーを見つけて、探しているキーワードを入力します。
   b. ズームインおよびズームアウト機能を使用して、ビューが読みやすくなるように調整します。
   c. コンテンツをより鮮明に表示するには、ページを時計回りまたは反時計回りに回転させます。
これらのコントロールオプションにより、証拠ファイルを包括的に理解する能力が向上します。
ヘッダーにコントロールオプションがあるのは PDF だけです。



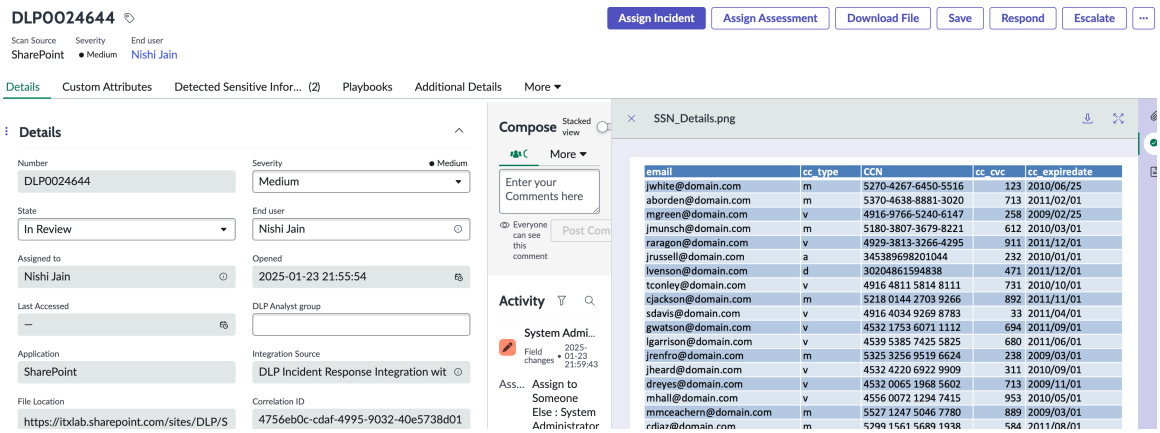
6. eml ファイルをプレビューします。
メールの添付ファイルを選択してプレビューします。

> **注:**
> 選択した証拠ファイルが 5 MB の制限を超えた場合、アナリストワークスペースでプレビューすることはできません。コンテンツをプレビューするには、ファイルをダウンロードする必要があります。この制限は、.emlファイルに対してのみ適用されます。

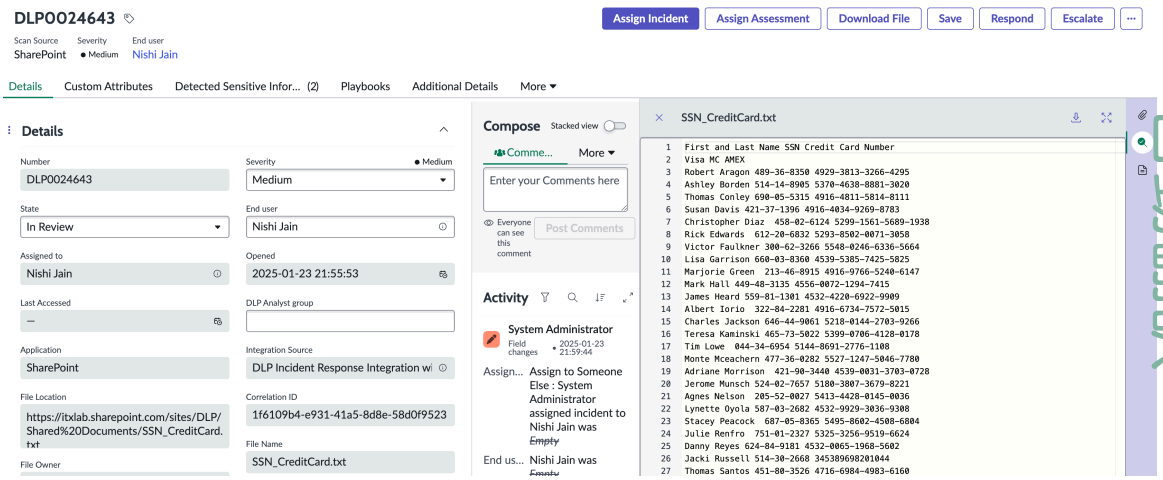


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. DLP アナリストワークスペースで画像をプレビューします。
.bmp、.gif、.ico、.jpeg、.jpg、.png、.svg、および .webp 拡張子のイメージのみがサポートされています。



8. 証拠ファイルの右上にある [展開] アイコンを選択して、テキストエディターでテキストファイルをプレビューします。



自動翻訳

> **注:**
> Office ドキュメント以外の証拠ファイル、eml ファイル、テキスト、画像拡張子は、プレビューではサポートされません。バイナリファイルはレンダリングされないため、コンテンツをプレビューするにはダウンロードする必要があります。証拠ファイルのプレビュー機能は、アーカイブされたインシデントでも機能します。

Exchange Online、OneDrive、および **SharePoint** タイプの **DLP** インシデントのファイルのダウンロード

Microsoft Purview の DLP ポリシーに違反するファイルまたはメールをダウンロードします。DLP IR インシデントビューからローカルマシンにこのファイルまたはメールをダウンロードします。タイプがスキャンでソースが Exchange Online、OneDrive、および SharePoint の DLP IR インシデントのファイルをダウンロードできます。

始める前に
必要なロール：

- sn_dlir.admin、sn_dlir.analyst
- 任意の有効な承認者

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > **DLP** インシデント管理 > **DLP** アナリストワークスペース.
2. Microsoft ソースから取り込まれた、タイプがスキャンでソースが Exchange Online、OneDrive、または SharePoint の DLP インシデントレコードを開きます。
3. [ファイルのダウンロード] をクリックします。
   Microsoft Purview 側で DLP ポリシーに違反していたファイルまたはメールは、ユーザーのローカルマシンにダウンロードされます。

   注:
   DLP アドミニストレーターは、[詳細設定] ページから [報告されたインシデントの違反ファイルのダウンロードを許可すべきですか] 設定を無効にすることで、[ファイルのダウンロード] アクションのアクセスを制御できます。詳細については、「詳細設定を構成します」を参照してください。

Microsoft DLP 統合でのドメインセパレーション

ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。その後、どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル

サポート：ベーシック。

ドメインセパレーションが Microsoft DLP 統合と連動する仕組み

ドメインセパレーションを実現するには、次の手順に従います。

- それぞれのドメインで、必要なロールを持つユーザーを作成します。
- 適切なドメインで Microsoft DLP 統合の手順を実行します。

セキュリティオペレーション の共通機能

メインの セキュリティオペレーション アプリケーション (セキュリティインシデントレスポンス、脆弱性対応、脅威インテリジェンス、またはコンフィギュレーションコンプライアンス) のいずれかのプラグインが有効になると、Security Support Common プラグインが有効になります。このプラグインは、すべての セキュリティオペレーション アプリケーションに共通の機能を提供するさまざまなモジュールをロードします。

注:
[sn_sec_cmn.admin] を持つユーザーのみが、セキュリティオペレーション モジュールを表示および使用できます。このロールは、セキュリティオペレーション アプリケーションのいずれかで管理ロールがアサインされると継承されます。

Security Operations のモジュール

機能	説明
Security Operations Integration の参考文献、脅威インテリジェンス の統合、脆弱性対応 の統合	セキュリティオペレーション アプリケーションにはいくつかの統合 (セキュリティインシデントレスポンス、脅威インテリジェンス、脆弱性対応) が含まれています。このセクションでは、プラグインをアクティブ化し、ServiceNow とサードパーティの両方の統合機能を設定する手順について説明します。また、独

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

機能	説明
	自の統合を開発するための基本的なガイドラインと、ベースシステムに含まれる特定の統合の詳細も含まれています。
セキュリティオペレーション メール処理	メール処理 を使用して、外部検出システムからの情報の統合を設定することで、セキュリティ運用レコードの処理に粒度をもたらし、一致しないメールを処理し、レコードの重複を防ぐことができます。
グループ	• フィルターグループ フィルターグループを作成して使用し、インスタンスの任意のテーブルからレコードを検索します。たとえば、同じメーカーのすべてのコンピューターのグループを作成できます。類似の脆弱性がある構成アイテム (CI) や、特定のサブネット IP アドレス範囲内にある構成アイテム (CI) をフィルタリングすることもできます。 • エスカレーション 注意や専門知識がさらに必要な問題のセキュリティインシデント用にエスカレーションパスを作成できます。エスカレーショングループが存在する場合、そのグループのセキュリティインシデントにボタンが表示されます。
セキュリティタグ	タグ：セキュリティタグルールは、セキュリティタグアクセスをフィルタリングできるようにします。
ワークフロー	• セキュリティワークフローを表示 Security Operations アプリケーションに含まれる多くのワークフローを表示できます。ワークフローエディターでは、テンプレートからワークフローを作成できます。 • ワークフロートリガー セキュリティオペレーション ワークフロートリガーには、テーブルの条件が含まれています。条件が満たされると、ワークフロートリガーレコードに添付されたすべてのワークフローが実行されます。
ユーティリティ	• 拡張データマッピング 拡張データマッピングは、XML、JSON、またはプロパティ ファイルから ServiceNow レコードにデータを変換します。セキュリティオペレーションワークフローは拡張データマップを使用し、セキュリティインシデントに出力データを提供します。 • フィールド値変換

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

機能	説明
	フィールドマップを使用して、一意の顧客フィールド値を、セキュリティオペレーション のメール解析、データ拡張、またはテーブルで認識されるフィールド値に変換します。選択フィールドをサポートし、外部データを参照して、新しいレコードの標準的な用語と形式に揃えることができます。 • フィールドマッピング セキュリティオペレーション テーブルは他のテーブルとの間でマッピングでき、セキュリティインシデントをカスタマーサービスケースに、または問題をセキュリティオペレーション システムの他の部分にリンクすることができます。たとえば、プラグインを セキュリティインシデントレスポンス タスクに統合できます。 • オンデマンドオーケストレーション セキュリティインシデントレスポンス 分析中、セキュリティインシデントワークフローによって駆動されるタスクをセキュリティアナリストが実行する必要がある場合があります。たとえば、特定の CI でプロセスダンプを実行します。これは、オンデマンドオーケストレーションで実現できます。 • オペレーティングシステムグループ 該当なし • **SecOps** 登録アプリケーション 該当なし
CMDB	**CI ID** ルール：CI ID は、CMDB でサードパーティ統合からの一致情報を含む構成アイテム (CI) をルックアップするときに使用するルールです。これらのルールは、一致するデータを含むフィールドと、それらが評価される優先順位を定義します。[順番] の値の最も小さいものが最初に評価されます。

Security Operations でのフィルターグループの作成と定義

フィルターグループを作成して使用し、インスタンスの任意のテーブルからレコードを検索します。たとえば、同じメーカーのすべてのコンピューターのグループを作成できます。類似の脆弱性がある構成アイテム (CI) や、特定のサブネット IP アドレス範囲内にある構成アイテム (CI) をフィルタリングすることもできます。

始める前に
必要なロール：sn_sec_cmn.write

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
フィルターグループには、動的に更新されるレコード、条件を使用してフィルタリングされていない一連の静的レコード、または動的に更新されるレコードと静的レコードの組み合わせを含めることができます。一部のフィルターグループ (CI 除外など) はベースシステムに含まれています。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > グループ > フィルターグループ.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
名前	フィルターグループの名前。
有効	グループをアクティブ化するためのボックス。
説明	フィルターグループの説明。
ネットワーク IP アドレス	グループに追加する CI の IP アドレスを含むネットワーク IP アドレス。 このフィールドは、[テーブル] フィールドで構成アイテム [cmdb_ci]、または構成アイテムを拡張するテーブルを選択した場合にのみ表示されます。
サブネットマスク	グループに追加する CI の IP アドレスを含むサブネット (例：255.255.255.0)。 このフィールドは、[テーブル] フィールドで構成アイテム [cmdb_ci]、または構成アイテムを拡張するテーブルを選択した場合にのみ表示されます。
テーブル	フィルターを適用するテーブル。
条件	条件ビルダー を使用して、フィルタリングする基準を定義します。

4. フォームヘッダーを右クリックし、[保存] を選択します。
[詳細条件] タブが表示されます。

[テーブル] フィールドで指定したテーブルのタイプに応じて、次のような他のタブが表示されます。

テーブル	表示されるタブ
構成アイテム [cmdb_ci]、または構成アイテムテーブルを拡張するテーブル	[手動で追加された **CI]** および [一致する **CI]**
タスク [task]、またはタスクテーブルを拡張するテーブル	[手動で追加されたタスク] および [一致タスク]
CI またはタスクに関連しないテーブル	手動で追加されたレコード

5. フィルターグループの条件をさらに定義するには：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. [詳細条件] をクリックします。

b. [追加のフィルターグループ条件] 埋め込みリストに新しい行を挿入し、更新するフィルターグループと組み合わせる他のビルド済みフィルターグループを選択します。
選択したフィルターグループで参照フィールドに基づいてレコードをフィルタリングする場合は、現在のレコードが保存されるとマップされたフィールドが自動的に選択されます。

> **注:**
> [マップされたフィールド] 値は、[追加のフィルターグループ条件] 埋め込みリストから編集できません。フィールドを変更するには、情報アイコン をクリックしてレコードを開きます。

c. [更新] をクリックします。

6. フィルターグループに CI またはタスクを手動でさらに追加するには：

a. [手動で追加された **CI]** または [手動で追加されたタスク] タブをクリックします。

b. [編集] をクリックします。

c. 追加する CI またはタスクを選択します。

d. [保存] をクリックします。

7. 選択基準に一致する CI またはタスクを表示するには：

a. [一致する **CI]** または [一致タスク] タブをクリックします。

b. 基準を変更した場合は、フォームヘッダーを右クリックし、[リストを更新] を選択してリストを更新します。

共有データ変換

セキュリティインシデントレスポンス、脆弱性対応、および 脅威インテリジェンス プラグインは、外部および内部情報を セキュリティオペレーション にインポートするために使用される関係性データと重複ルールに関する共通機能を共有しています。

メール解析、重複ルール、および フィールドマッピング は入力データ (メール、JSON または XML ファイル、レコード) を取得し、正しい形式に変換して新しいレコードを作成します。これらの機能はそれぞれ独自の方法でデータをプルしますが、おおむね同じプロセスを使用してデータを新しいレコードに変換します。

関係性データ

関連リスト (セキュリティインシデント内の関連する観測事象など) に情報を追加すると、m2m テーブルで構成される関係性レコードを作成できます。その関係性レコードに設定すべき追加のデータが存在することがあります。たとえば、観測事象が (宛先 IP ではなく) ソース IP である場合です。この情報は、[フィールドマッピング] フォームの [メールの解析] または [フィールドマッピングフィールド] 関連リストで使用される [フィールド変換] フォームの [関係性データ] フィールドに入力されます。

[関係性データ] フィールドは通常空です。このフィールドは、[メールの解析] の観測事象の IP アドレスで最もよく使用されます。

[フィールドマッピング] 機能の [フィールドマッピングフィールド] を使用して、任意の ServiceNow レコードのデータを任意の他の ServiceNow レコードに変換できます。たとえば、あるインシデントからセキュリティインシデントに、またはセキュリティインシデントから PRB にデータを変換します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Security Operations 重複ルール

重複ルール を使用して、セキュリティ、脆弱性、IoC などの重複レコードを処理します。

重複ルールには 2 つの目的があります。あまり多くの重複レコードが作成されないようにし、重複が検出された場合は、レコードのどのフィールドを更新するかを指定します。アクティブな重複のみが検索されます。レコードがアクティブでない場合、たとえば、インシデントがクローズされている場合、新しく同一の問題が発生すると、新しいインシデントになります。

重複ルールは、[メールの解析]、[フィールドマッピング]、および [拡張データマッピング] で使用されます。

関連情報

Security Operations でのメールパーサーの作成

Security Operations フィールドマッピングを使用したテーブル間のマッピング

セキュリティオペレーション での重複ルールの作成

重複ルール を使用して、アクティブな重複レコードを含む新しいメール、拡張データ、またはフィールドマップを識別し、それらを適切に処理できます。

始める前に
必要なロール：sn_sec_cmn.write

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > 重複ルール.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

重複ルール

フィールド	説明
名前	重複ルールの名前。
テーブル	レコードが作成され、重複を判断するために使用されるテーブル。
識別するフィールド	これらのフィールドの値が同じである場合に、重複するセキュリティインシデント、観測事象、脆弱性などを示すフィールドのセットを選択します。
重複アクション	重複するメールの処理方法を制御します。選択肢は次のとおりです。 子として作成 元の子としてレコードを作成します。子を親にリンクするフィールドは [親] フィールドです。 レコードを作成したり更新したりしない (デフォルト) 何もしません。重複を無視します。 重複レコードを更新 [重複アクション] で指定された既存のレコードのフィールドを更新します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: [重複レコードを更新] を選択すると、[重複アクション] 関連リストが表示されます。
有効	このルールをアクティブ化するには、このチェックボックスをオンにします。
説明	この重複ルールの目的と適用について記述します。たとえば、「IP ベースの観測事象やファイアウォールからのセキュリティインシデント用に設計されたルール」です。

4. レコードヘッダーを右クリックして、[保存] を選択するか、[更新] をクリックします。
5. 重複アクションを設定するには、[重複レコードを更新] を選択した場合は [新規] をクリックして、インシデント内の更新する各フィールドに対して重複アクションを作成します。
6. フォームのフィールドを入力または編集して、フィールドの更新方法を説明します。

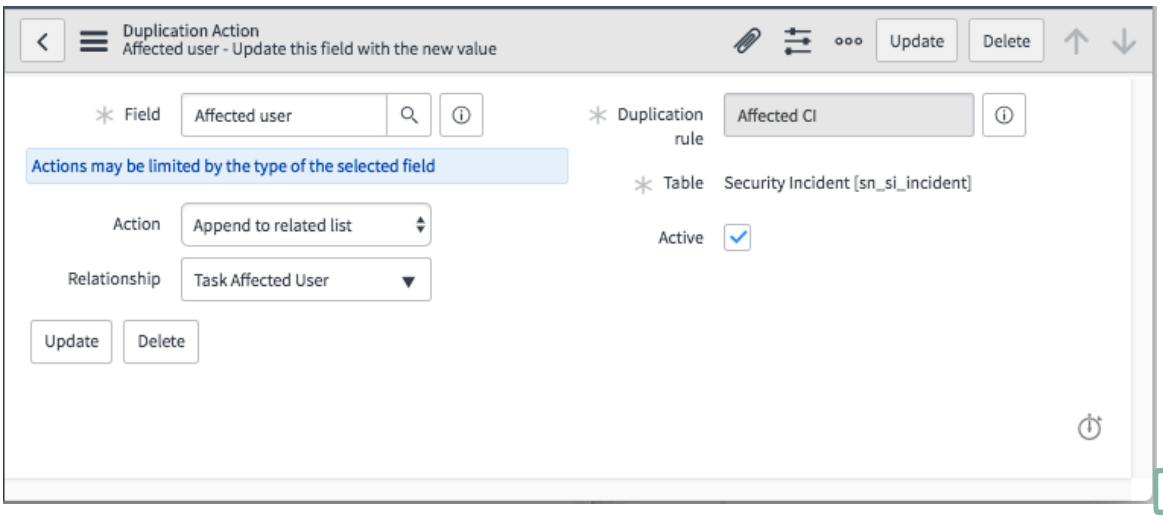
重複アクション

フィールド	説明
フィールド	複製アクションに使用するフィールドの名前。
アクション	サポートされているアクションはフィールドタイプによって異なります。 選択肢は次のとおりです。 このフィールドを新しい値で更新 既存のレコードの前の値をこの値に置き換えます。 一意の場合、新しい値をカンマで区切って列挙したリストに追加 値をカンマ区切りリストのエントリーとして扱い、新しいデータ (存在する場合) をそのリストの新しいエントリーとして追加します。データが既にリストにある場合、2 回追加されることはありません。 このフィールドに新しい値を追加 フィールド内の既存のテキストの末尾に新しい値を追加します。 カウンタフィールドに 1 を追加 数値フィールドに 1 を加算します。 フィールドを今日に設定 フィールドを現在の日時に設定します。 関連リストに追加 この値を持つ関連レコードを現在のレコードの関連リストに追加します。更新されるテーブルにリンクされた、同じタイプの列を持つ多対多テーブルがある場合に表示されます。 たとえば、[影響を受ける **CI]** または [影響を受けるユーザー] です。
関係	[オプション] このフィールドは、[関連リストに追加] アクションが選択されている場合にのみ表示されます。このルールに関連付ける関連リストの名前です。

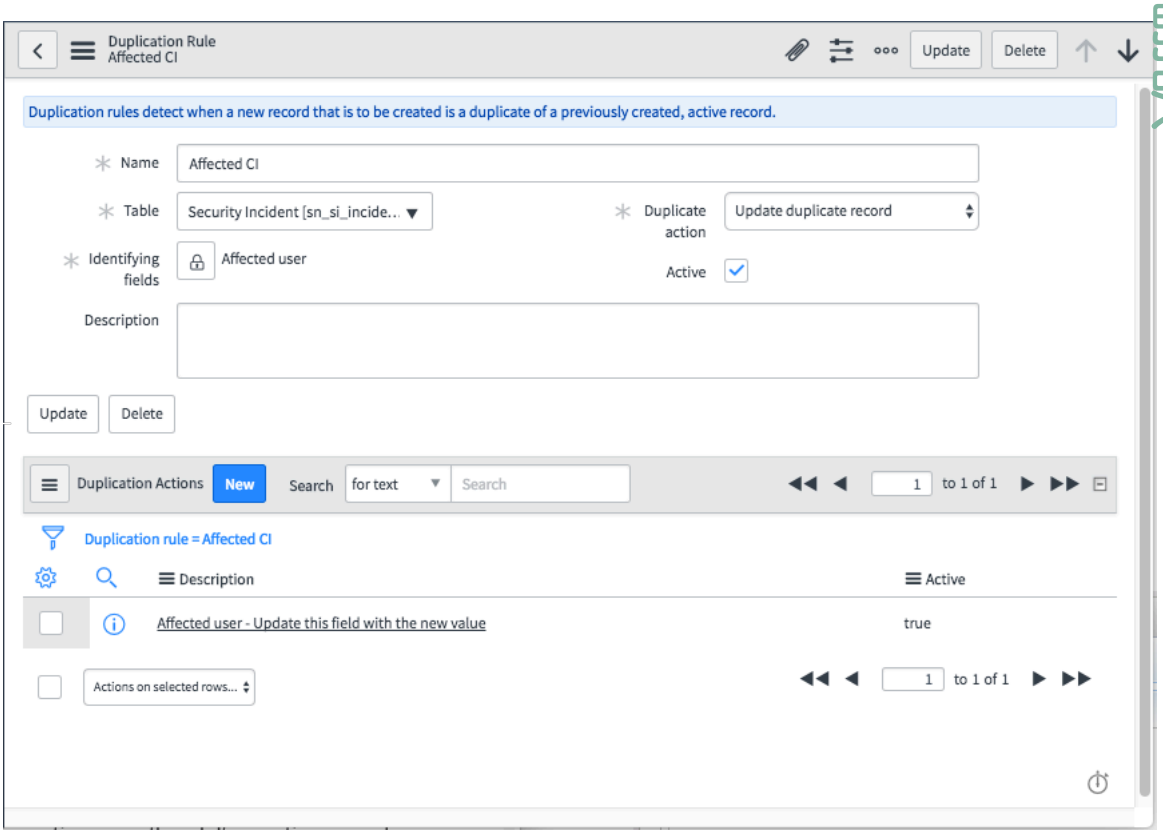
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
重複ルール	このアクションが含まれているルール。
テーブル	レコードが作成されるテーブル。情報としてのみ表示されます。
有効	このアクションをアクティブ化するには、このチェックボックスをオンにします。



7. **[Submit]** をクリックします。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティオペレーション メール処理

メール処理 を使用して、外部検出システムからの情報の統合を設定することで、セキュリティ運用レコードの処理に粒度をもたらし、一致しないメールを処理し、レコードの重複を防ぐことができます。

メール処理は次の機能で構成されています。

機能	説明
メール解析	外部システムメールから新しい セキュリティオペレーション レコードを生成します。
重複ルール	既知のインシデントを含む新しいメールを識別し、適切に処理します。
プロパティ	メール解析でセキュリティ、脆弱性、IoC の入力として使用するアカウントを指定します。セキュリティオペレーション のレコード処理の精度が向上します。
一致しないメール	どの セキュリティオペレーション レコードにも一致しないメールを一覧表示します。

セキュリティオペレーション メールプロパティ

メールプロパティは、外部検出システムから情報をインポートし、セキュリティ、脆弱性、IoC のレコードを作成するときに、メール解析で入力として使用する受信ボックスを指定します。外部検出システムすべてに使用する一般アカウントをセットアップすることも、セキュリティインシデントレスポンス、脅威インテリジェンス、脆弱性対応 のメールアカウントを個別にセットアップすることもできます。

セキュリティオペレーション メールプロパティの作成

メールの プロパティ を使用してレポートのメールアドレスを指定し、自動的なメール動作を制御することができます。

始める前に

必要なロール：sn_sec_cmn.admin
メール解析機能付き受信箱にメールを送信するように外部検出ツールを設定します。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > メール処理 > プロパティ.
2. 必要に応じて受信者のメールボックスを入力します。
   これらは、[受信アクション] ではなく [メール解析] によって処理される受信メールアドレスです。

メール解析プロパティ

フィールド	説明
セキュリティオペレーション ツールの受信ボックス	セキュリティオペレーション の完全なメールアドレス。例：secops_support@yourcompany.com。
セキュリティインシデント ツールの受信箱	セキュリティインシデントレスポンス の完全なメールアドレス。例：sir_support@your.company.com。
脆弱性対応 ツールの受信ボックス	脆弱性対応 の完全なメールアドレス。例：vuln_resp@yourcompany.com。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
脅威インテリジェンス ツールの受信ボックス	脅威インテリジェンス の完全なメールアドレス。例：threat_intel@yourcompany.com。

3. [保存] をクリックします。

セキュリティオペレーション メール解析

メール解析を使用して外部検出システムから新しい セキュリティオペレーション レコードを生成します。この機能は、マルウェア検出、脆弱性検出、ファイアウォール、脅威インテリジェンスなどの外部ツールからの情報を統合する手段となります。

メールの解析方法

メールを送信できる任意のシステムで、セキュリティオペレーション レコードを作成できます。たとえば、セキュリティインシデント、要求、脆弱性一致アイテム、脆弱性、セキュリティインシデント観測事象、攻撃方法などです。

すべての セキュリティオペレーション プラグイン (セキュリティインシデントレスポンス、脅威インテリジェンス、脆弱性対応) には、**email_to** プロパティがあります。このプロパティは、外部統合がメールパーサーにメールを解析させるときにメールを送信するメールアドレスを定義します。「」を参照してください。 メール処理 > プロパティ 詳細については、を参照してください。

セキュリティオペレーション メールアドレスのいずれかに送信されたメールは、メールイベントテーブルに保存されます。これらのメールが処理され、メールパーサーと一致するかどうかが判断されます。

一致したメールにはフラグが付けられ、変換ルールと重複ルールによって セキュリティオペレーション レコードが作成または更新されます。メールはそのレコードにリンクされ、一致しているとしてフラグが付けられます。

一致しないメールは、[一致しないメール] に セキュリティオペレーション レコードとしてリストされます。これらをレビューすることで、これらのメールを処理するメールパーサーのビルドに役立ちます。再処理アクションによって、パーサーを介して不一致メールを再実行できます。元のメールログはそのレコードにリンクされます。

メール変換の重複ルールは、同一の問題に関連する複数のメールを管理します。これらのルールは、重複レコードの構成要素を定義し、重複レコードの作成を防ぐことができます。ルールは重複が検出されたときに実行すべきアクションを指定します。アクションなし (新しいレコードを作成しない) か、新しいレコードを既存のレコードの子レコードとして作成するか、または既存のレコードを更新します。重複ルールを更新するときに、既存のレコードのどのフィールドを更新するかを指定します。

> **注:**
> セキュリティオペレーション メールパーサーは、プラットフォームの受信アクションと連携して機能し、それらを置き換えるものではありません。**sys_journal_field** エントリーなどの間接フィールドの値の設定はサポートされていません。

デフォルトでは、メールイベントは 30 日後に削除されます。

複数のレコード

外部検出システム (マルウェア検出、脆弱性など) は、一度に複数のアイテムを報告するメールを送信できます。メールパーサーは、メール内のセパレーターをサポートしています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

たとえば、マルウェア検出では、1 件の特定のマルウェアに感染したネットワーク内のすべてのシステムに関するメールレポートを、最初にマルウェアに関する情報、その後に影響を受けたシステムのリストを記載した 1 通のメールとして送信できます。

悪意のあるメールのサンプル

```
Subject: EvilChocolateBunny detected on multiple systems
Malware Hash: 20380285098260923490723
Malware Name: Evil Chocolate Bunny
Type: Keylogger
==========
System: WIN-GHARRISON
IP: 123.45.67.888
Status: File present, not infected
==========
System: WIN-ATUTER
IP: 123.45.67.889
Status: Infected
==========
System: WIN-BANGLIN
IP: 123.45.67.899
Status: File present, not infected
```

この例では、[メール変換] の [レコードセパレータ] が **[==========]** に設定されており、メールは 4 つのセクションに分割されて、個別に評価されます。これにより、影響を受ける 3 つのシステムについてセキュリティインシデントが 1 件ずつ作成されます。

注:
ヘッダーセクションは検出されますが、影響を受けるシステムがないため、3 件のレコードすべてで使用され、4 件目のレコードは作成されません。

[フィールド変換] は、各セクションからデータをプルします。この例の [マルウェアのハッシュ]、[マルウェア名]、[タイプ] など、メールのヘッダーまたはフッターの何かがすべてのレコードに適用される場合、それらのフィールド変換は、[値の検索] をメール本文内で検索する場所を表す値 ([メール本文の行の先頭] または [メール本文の任意の場所]) に設定する必要があります。

[フィールド変換] は、[システム]、[IP アドレス]、[ステータス] などの各セクション内に定義されたデータの、[レコードセクションの行の先頭] または [セクション **(Sec)]** を検索するように設定する必要があります。レコードセクションオプションは、メール変換にレコードセパレータが定義されている場合のみ使用できます。

セパレータを定義してメールを解析すると、セクション固有のデータを少なくとも 1 つ含むセクションに対してのみレコードが作成されます。

この例では、4 つのセクションが定義されていますが、作成されるレコードは 3 つです。最初のセクションはヘッダーであり、特定のシステム 1 台に固有の情報はありません。最初のセクションにシステム、IP、またはステータスのいずれかのフィールドがあった場合は、そのセクションのレコードも作成されます。

関連情報

- Security Operations でのメールパーサーの作成
- セキュリティオペレーション 拡張データマッピング
- セキュリティオペレーション フィールドマッピング

Security Operations でのメールパーサーの作成

メール解析 は、セキュリティ、脆弱性、および観測事象についてメールから セキュリティオペレーション レコードを作成し、脅威への対応と修復を迅速化します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に

- 中央のメールアドレスにメールを送信するように外部検出ツールを設定します。
- Security Operations プロパティでメールアドレスを設定します。詳細については、「セキュリティオペレーション メールプロパティの作成」を参照してください。
- このメールアドレスにユーザーアカウントを割り当て、そのユーザーにメールイベントレコードを作成および更新するためのセキュリティアクセスコントロールを付与します。
- 外部検出ツールからの関連メールのコピーを用意します。
- 作成するレコードのタイプ、セキュリティインシデント、脆弱性レコード、タスクなどを決定します。この選択により、選択するテーブルが決まります。

必要なロール：sn_sec_cmn.admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > メールの解析.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

> **注:**
> 複数のフィールドが指定されている場合は、すべてのフィールドがレコードを作成するメールと一致する必要があります。

メールパーサー

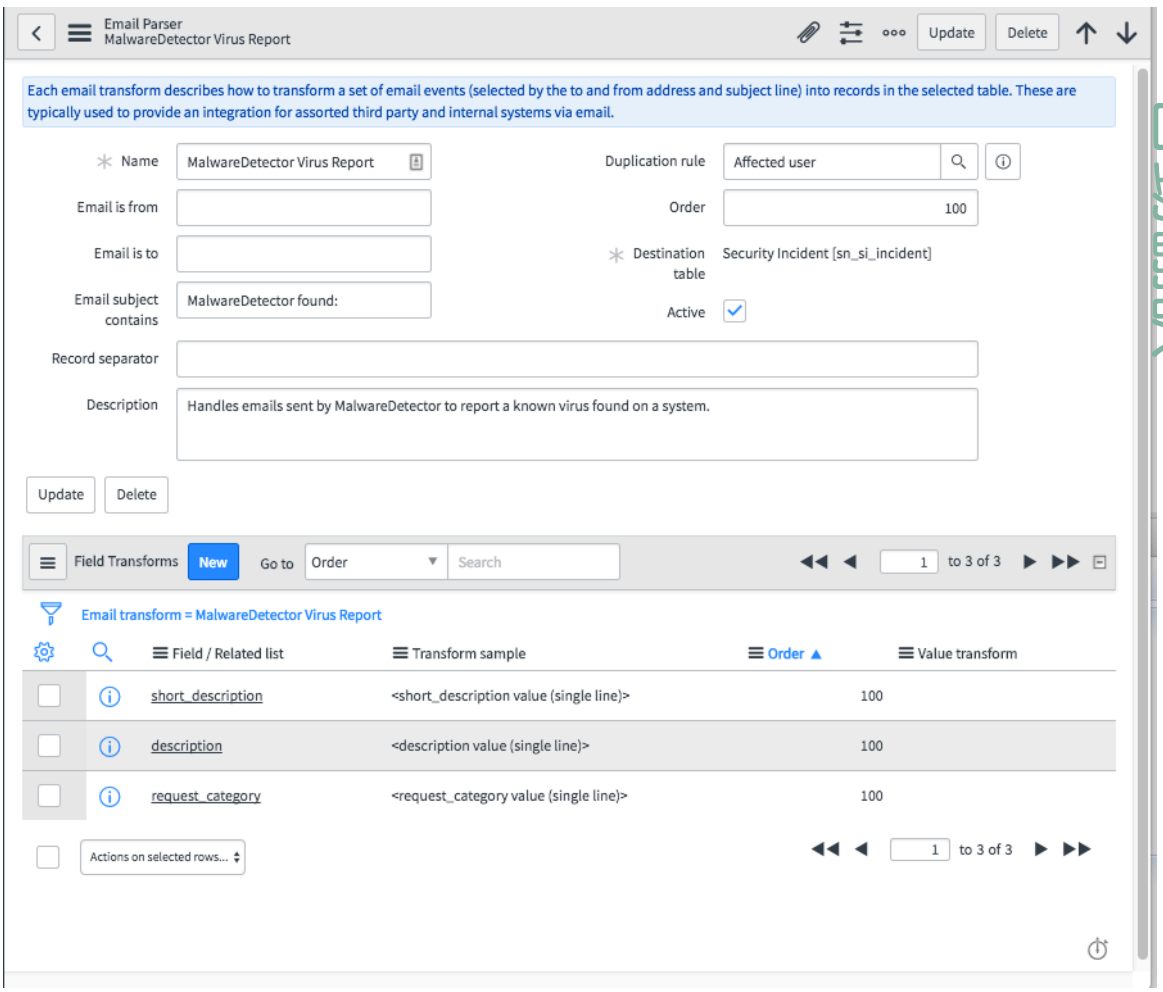
フィールド	説明
名前	メールパーサーの名前。
メールの送信元	入力すると、このアドレスからのメールのみがこのメールパーサーによって変換されます。
メールの送信先	入力すると、このアドレスからのメールのみがこのメールパーサーによって変換されます。
メールの件名に含まれる	入力すると、件名にこのフレーズが含まれるメールのみがこのメールパーサーによって変換されます。
重複ルール	この変換が処理するメールの重複メールを処理する方法を制御します。詳細については、「共有データ変換」を参照してください。
順序	変換を考慮する順序。最初に一致したメール変換が使用されます。通常は、最も限定的なメールパーサーを下位の番号で設定し、代替をいくつか用意します。一致するものが他にない場合に実行されるように、予備メールパーサーの [順序] 番号を大きくします。デフォルトは 100 です。すべてが一致する場合、最も限定的なメールパーサー ([送信元]、[宛先]、および [件名] に一致) が使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
宛先テーブル	レコードを作成するテーブル。
有効	この変換がアクティブか、使用中か、非アクティブか。オフにすると、このコードではメールは変換されません。
レコードセパレータ	このメールパーサーによって処理されるメールが複数のレコードを作成する場合、このフィールドにはそれらのレコードの情報間にセパレータが含まれます。詳細については、「セキュリティオペレーション メール解析」を参照してください。
説明	このメールパーサーの説明、連携するツール、目的など。

4. 入力が完了したら、フォームヘッダーを右クリックし、[保存] を選択します。
[フィールド変換] タブが表示されます。このタブには、宛先テーブル内の個々のフィールドがメールコンテンツに基づいてどのように設定されるかが表示されます。



5. フィールド変換を追加するには、次の手順を実行します。
   a. [フィールド変換] タブで、[新規] をクリックします。
   b. 必要に応じて、フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
フィールド	説明
フィールドまたは関連リストに値を保存する	値を検索する場所を選択します。次の選択肢があります。 ○ 新しいレコード内のフィールドに値を保存する (Store the value into a field in the new record) ○ 関連リスト内で、この値にリンクする ○ この値にリンクし、一致するレコードが存在しない場合、新しいレコードを作成する **注:** 宛先テーブルに関連リストがない場合、このフィールドは表示されません。
フィールド	この値を入力するフィールドを選択します。 **注:** 選択肢フィールドの場合、基礎となる選択肢のラベルまたは値を使用して、既存の選択肢が照合されます。一致するものが見つからない場合、フィールドは設定されますが、新しいエントリーは選択リストに追加されません。詳細については、次を参照してください： 選択リスト。 参照フィールドの場合、レコードの表示名に一致する値または有効な sys_id が見つかった場合にのみ、エントリーが設定されます。詳細については、次を参照してください： 参照フィールド。
関連リスト	[フィールドまたは関連リストに値を保存する] が [関連リスト内で、この値にリンクする] または [この値にリンクし、一致するレコードが存在しない場合、新しいレコードを作成する] に設定されている場合、このフィールドは情報を追加する関連リストを指定します。
値フィールド	[フィールドまたは関連リストに値を保存する] が [関連リスト内で、この値にリンクする] または [この値にリンクし、一致するレコードが存在しない場合、新しいレコードを作成する] に設定されている場合、このフィールドは関連リストに表示されるテーブル内のフィールドを指定します。既存のレコードをルックアップして見つけるために使用されます。たとえば、関連リストが [影響を受ける **CI**] である場合、このフィールドには [名前] または [完全修飾ドメイ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
	ン名] が含まれている可能性があります。そうでない場合、CI のルックアップに使用する CI レコードの他のフィールドが [影響を受ける **CI]** リストに追加されます。
関係性データ	[フィールドまたは関連リストに値を保存する] が [関連リスト内で、この値にリンクする] に設定されている場合、そのレコード (セキュリティインシデントなど) を値 (CI、観測事象など) にリンクするためにレコードが作成されます。このフィールドは、そのリンクレコードに追加する必要がある追加情報 (フィールドと値のペア) を指定します。たとえば、ソース IP の観測事象を追加する場合、この IP が宛先 IP ではなくソースであることを指定します。複数の値の場合は、^ 区切り文字を使用します (例：type= Source IP^Active=true)。
新規レコードデータ	[フィールドまたは関連リストに値を保存する] が [この値にリンクし、一致するレコードが存在しない場合、新しいレコードを作成する] に設定されている場合、解析された値に一致する関連レコードが見つからないときは、レコードが作成されます。このフィールドは、そのレコードに追加する静的データを指定します。[影響を受ける **CI]** の場合、一致する CI が見つからないと CI レコードが作成されます。その場合、メールで検出された値が CI レコードの [値] フィールドに設定されます。追加のデータ (CI が作成された理由を示すメモ、使用する CI のタイプに関する情報など) を設定できます。サンプル：description=Created by Malware Scanner email parser^type=autodetect。
値の検索	検索するメール内の場所を選択します。次の選択肢があります。 ○ メール本文の行の先頭 ○ メール本文の任意の場所 ○ メールの件名 ○ 常に静的値 レコードセパレータ を定義した場合、より多くのオプション ([レコードセクションの任意の場所] および [レコードセクションの行の先頭]) を使用すると、メール本文全体ではなく現在のセクション内のみを検索できます (詳細については、「セキュリティオペレーション メール解析」を参照してください)。 すべてのレコードに適用されるヘッダーまたはフッターの情報は、メール本文全体で検索され

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
	ます。レコード間で異なる情報はセクション内でのみ検索されます。
値のセパレータ	[フィールドまたは関連リストに値を保存する] が [関連リスト内で、この値にリンクする] または [この値にリンクし、一致するレコードが存在しない場合、新しいレコードを作成する] に設定されている場合、このフィールドはアイテムのリストに使用するセパレータ (例：メールのデータが IP アドレスのリストの場合はカンマまたはセミコロン) を指定します。
値プリフィックス	抽出するこのフィールド内の値の前に常に表示されるテキスト。
値の終了	値の終了を示すものを選択します。選択肢には、[行の最後]、[メールの最後] (メールの残りのすべてのテキストを取り込む)、または [期限] (指定されたテキストが見つかると停止する)、または [期限] (指定されたテキストが見つかると停止する) があります。
値サフィックス	[値の終了] が [期限] に設定されている場合、このフィールドは、このフィールド内に配置される値の後に常に表示されるテキストを指定します。 たとえば、「The affected computer is」の後、「.」の前に来る値を探す場合、次のメールを解析すると「AB123」が得られます：「The demented bunny virus has been found. The affected computer is AB123. Estimated time of infection was 3:45PM」
値の変換	適用するフィールド変換エントリーを選択します。メールで見つかった値を別の値に変換します。これは、選択肢フィールド、場合によっては参照フィールドやその他のフィールドの入力に使用されます。
順序	フィールド変換が実行される順序 (最低から最高)。最初に順序エントリーが 100 のフィールド変換が試行されます。そのフィールド変換が値を見つけることができない場合にのみ、同じフィールドでより高い順序 (200) のフィールド変換が実行されます。
メール変換	このフィールド変換が属する変換。
宛先テーブル	メール変換の宛先テーブル。メール変換からの情報データが含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
有効	デフォルトはオンです。オンにすると、フィールド変換が有効になります。このボックスをオフにすると、フィールド変換が無効になります。

a. **[Submit]** をクリックします。
新しいレコードは、メール内の情報を解析して新しいレコードを作成するために使用されます。

関連情報

セキュリティオペレーション での重複ルールの作成

セキュリティオペレーション フィールド値変換の作成

脆弱性対応 メール通知を定義する

セキュリティオペレーション でのメールレコードの編集

既存のメールイベントレコードに変換を追加または作成します。

始める前に

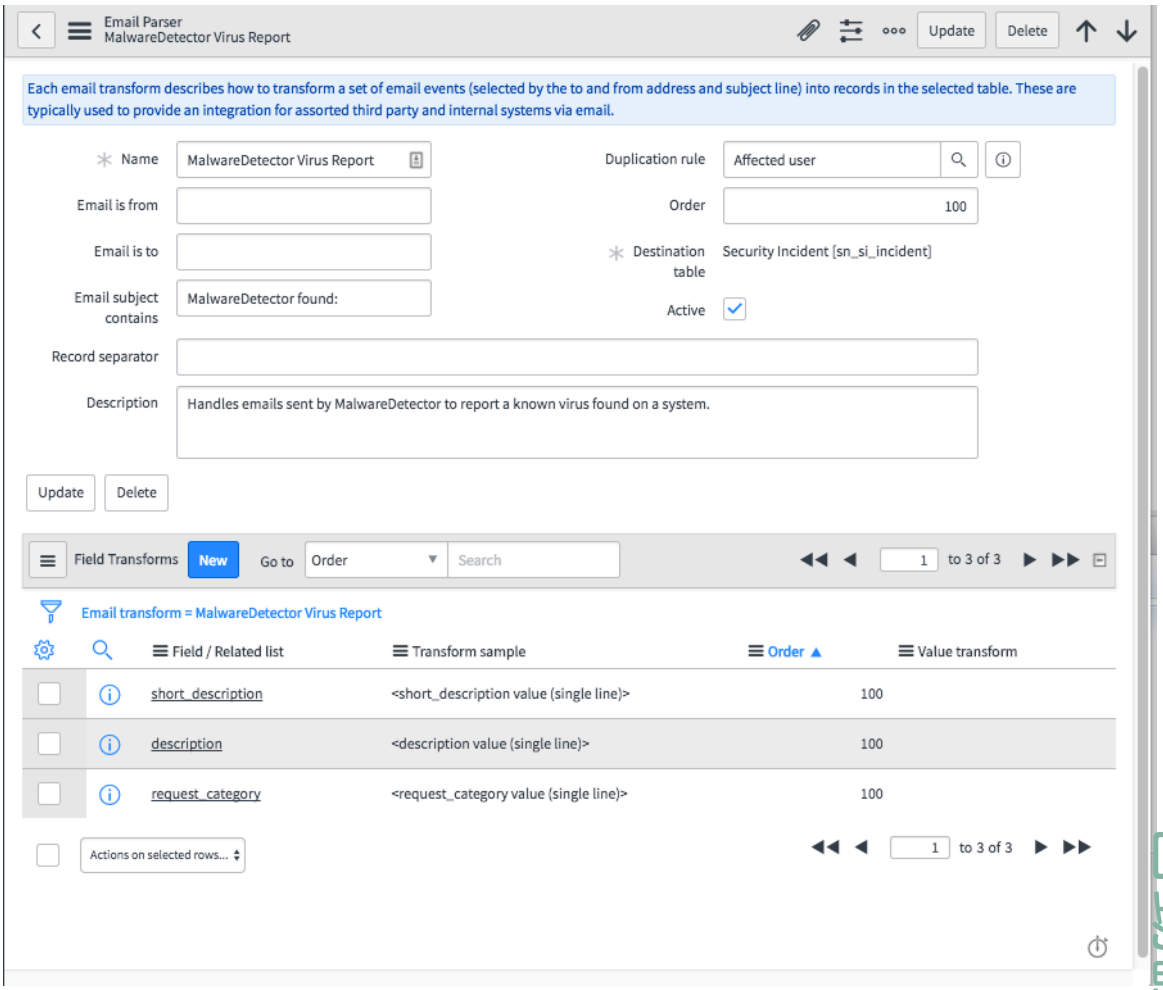
必要なロール：sn_sec_cmn.admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > メールの解析.
2. 編集するメールパーサーをクリックします。
レコードが読み取り専用の場合は、ヘッダーメッセージの [ここ (here)] リンクをクリックします。
変換の編集可能なフォームに移動します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. 必要に応じてフィールドを編集します。

4. フィールド変換を編集するには、フィールドをクリックし、必要に応じて変更します。

5. [更新] をクリックします。

一致しない セキュリティオペレーション メールイベント

メールパーサーと一致しないメールイベントには「一致」フラグが設定されません。これらのメールイベントレコードを 一致しないメール リストから表示して、メールがまだ解析されていない外部検出システムを明らかにすることができます。

メールパーサーを作成するときに、(フォームまたはリストから) メールイベントの再処理を試みることで、新しいメールパーサーを検証することができます。

一致しない **Security Operations** メールの表示と再処理

中止したフィルターまたは新しいフィルターの候補がないか 一致しないメール を確認し、メール脅威の検出率を維持または改善できます。

始める前に

必要なロール：sn_sec_cmn.read

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > 一致しないメール.
一致しないメールが見つかった場合は、リストに表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

2. フォームのフィールドは次のとおりです。

セキュリティメールイベント

フィールド	説明
送信元	送信者のメールアドレス。
終了	受信者のメールアドレス。
件名	メールの件名。
本文	メール本文のコンテンツ。
一致	このメールイベントが一致したかどうかを示します。

3. このメールを再処理するには、メールレコードを作成するか、このメールの情報と一致するように既存のメールレコードを編集します。
「Security Operations でのメールパーサーの作成」を参照してください。
4. に戻る セキュリティオペレーション > 一致しないメール.
5. [メールイベントを再処理] をクリックして、このメールを処理します。
一致しないメール のメインリストに戻ります。新しいメールレコードが一致すると、そのメールイベントはリストに表示されなくなります。一致したかどうかを示すメッセージが表示されます。

セキュリティオペレーション フィールドマッピング

セキュリティオペレーション テーブルは他のテーブルとの間でマッピングでき、セキュリティインシデントをカスタマーサービスケースに、または問題を セキュリティオペレーション システムの他の部分にリンクすることができます。

[フィールドマッピング] は、ソーステーブルのレコードを使用して宛先テーブルに新しいレコードを作成するときに使用されるマッピングを定義します。通常は、別のレコードからセキュリティインシデントを作成するために使用されるこれらのマップは、セキュリティインシデントのどのフィールドを新しい問題へ挿入するのか、または既存のカスタマーインシデントからどのフィールドを新しいセキュリティインシデントへ挿入するのかを定義します。

Security Operations フィールドマッピングを使用したテーブル間のマッピング

セキュリティオペレーション はより細やかなフィールドマッピングを提供するため、セキュリティオペレーション テーブルを他のテーブルにマップできます。

始める前に
必要なロール：sec_cmn.write

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > ユーティリティ > フィールドマッピング.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

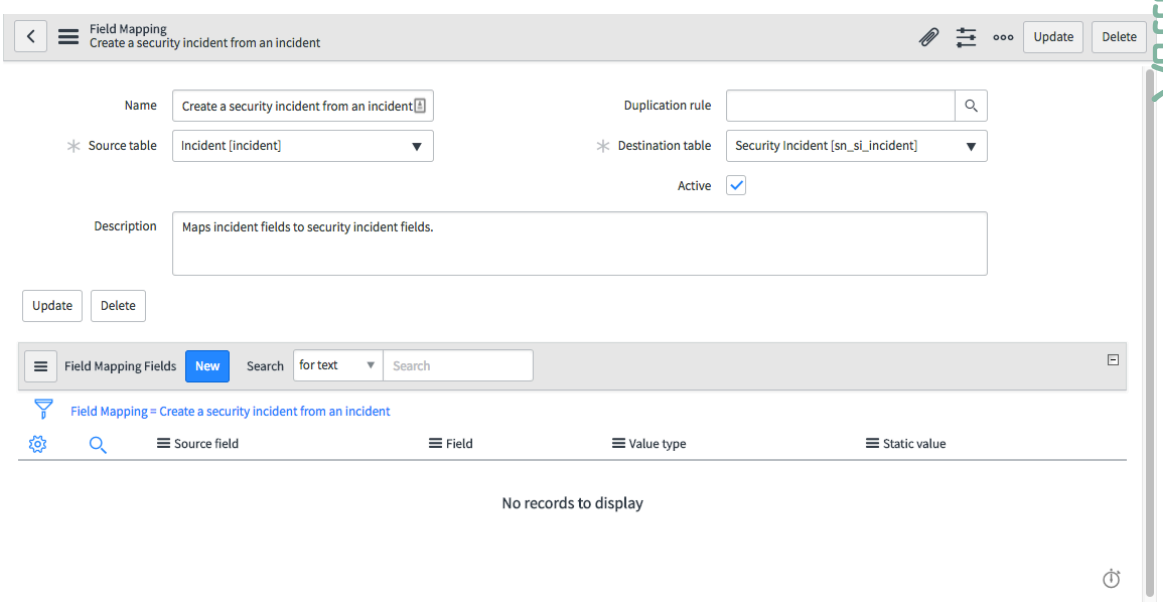
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールドマッピング

フィールド	説明
名前	フィールドマップの名前。
ソーステーブル	宛先テーブルにレコードを作成するために使用するデータを提供するテーブル。
重複ルール	重複レコードを生成するソースレコードの処理方法を制御します。詳細については、「共有データ変換」を参照してください。
宛先テーブル	新しいレコードが作成されるテーブル。
有効	このマッピングをアクティブ化するには、このチェックボックスをオンにします。 **注:** 一度にアクティブにできるテーブル間のマッピングは 1 つだけです。2 つのマップに同じテーブルが含まれている場合、古いバージョンは自動的に非アクティブ化されます。
説明	フィールドマップの説明。

4. 入力が完了したら、フォームヘッダーを右クリックし、[保存] を選択します。
[フィールドマッピングフィールド] タブが表示されます。このレコードは、このフィールド変換によって作成されたレコードのターゲットフィールドに格納されるデータを定義します。



5. [新規] をクリックします。
6. 必要に応じて、フォームのフィールドに入力します。

オプション	説明
フィールド	説明

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
フィールドまたは関連リストに値を保存する	値を検索する場所を選択します。次の選択肢があります。 ○ レコード内のフィールドに新しい値を追加する ○ 関連リスト内で、この値にリンクする ○ この値にリンクし、一致するレコードが存在しない場合、レコードを作成する **注:** 宛先テーブルに関連リストがない場合、このフィールドは表示されません。
フィールド	[フィールドまたは関連リストに値を保存する] が [レコード内のフィールドに新しい値を追加する] に設定されている場合、このフィールドは入力するフィールドを指定します。 **注:** 選択肢フィールドの場合、基礎となる選択肢のラベルまたは値を使用して、既存の選択肢が照合されます。一致するものが見つからない場合、フィールドは設定されますが、新しいエントリーは選択リストに追加されません。詳細については、次を参照してください： 選択リスト。 参照フィールドの場合、レコードの表示名に一致する値または有効な sys_id が見つかった場合にのみ、エントリーが設定されます。詳細については、次を参照してください： 参照フィールド。
関連リスト	[フィールドまたは関連リストに値を保存する] が [関連リスト内で、この値にリンクする] または [この値にリンクし、一致するレコードが存在しない場合、新しいレコードを作成する] に設定されている場合、このフィールドは情報を追加する関連リストを指定します。
値フィールド	[フィールドまたは関連リストに値を保存する] が [関連リスト内で、この値にリンクする] または [この値にリンクし、一致するレコードが存在しない場合、新しいレコードを作成する] に設定されている場合、このフィールドは関連リストに表示されるテーブル内のフィールド (既存レコードのルックアップと検索に使用される) を指定します。たとえば、関連リストが [影響を受ける **CI]** である場合、このフィールドには [名前] または [完全修飾ドメイン名] が

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
	含まれている可能性があります。そうでない場合、CI のルックアップに使用する必要がある CI レコードの他のフィールドが [影響を受ける **CI]** リストに追加されます。
関係性データ	[フィールドまたは関連リストに値を保存する] が [関連リスト内で、この値にリンクする] に設定されている場合、そのレコード (セキュリティインシデントなど) を値 (CI、観測事象など) にリンクするために新しいレコードが作成されます。このフィールドは、そのリンクレコードに追加する必要がある追加情報 (フィールドと値のペア) を指定します。たとえば、ソース IP の観測事象を追加する場合、この IP が宛先 IP ではなくソースであることを指定できます。複数の値の場合は、^ 区切り文字を使用します (例：type= Source IP^active=true)。
新規レコードデータ	[フィールドまたは関連リストに値を保存する] が [この値にリンクし、一致するレコードが存在しない場合、新しいレコードを作成する] に設定されている場合、解析された値に一致する関連レコードが見つからないときは、新しいレコードが作成されます。このフィールドは、そのレコードに追加する静的データを指定します。たとえば、[影響を受ける **CI]** では、CI が見つからない場合、この設定は新しい CI が作成されることを示します。ソースレコードで検出された値が CI レコードの [値] フィールドに設定されます。追加のデータ (この CI が作成された理由を示すメモ、使用する CI のタイプに関する情報) を設定できます。サンプル：description=Created by malware Incident report^type=autodetect
値のセパレータ	[フィールドまたは関連リストに値を保存する] が [関連リスト内で、この値にリンクする] または [この値にリンクし、一致するレコードが存在しない場合、新しいレコードを作成する] に設定されている場合、このフィールドはアイテムのリストに使用するセパレータ (一般的にカンマまたはセミコロン) を指定します。
値のタイプ	[フィールドまたは関連リストに値を保存する] が [レコード内のフィールドに新しい値を追加する] に設定されている場合、このフィールドは値のタイプを指定します。次の選択肢があります。 ○ ソースフィールドレコード **(Source field record)** ○ このフィールドに新しい行として追加

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
	○ 静的値 ○ 静的値とソースレコードフィールド値
ソースフィールド	宛先フィールドまたは選択した関連リスト内に配置される値を含むソースフィールドを選択します。
静的フィールド (Static field)	フィールドの静的値。
値の変換	適用するフィールド値変換エントリーを選択します。これは、レコード間で選択肢フィールドをマッピングするために使用されます。たとえば、セキュリティインシデントの [カテゴリ] 選択肢のセットを変更要求の適切な [タイプ] フィールドに変換します。
宛先テーブル	宛先テーブルが自動入力されます。
フィールドマッピング	親フィールドマップが自動入力されます。
ソーステーブル	ソーステーブルが自動入力されます。

7. [送信] をクリックします。

セキュリティオペレーション フィールド値変換

フィールドマップを使用して、一意の顧客フィールド値を、セキュリティオペレーション のメール解析、データ拡張、またはテーブルで認識されるフィールド値に変換します。選択フィールドをサポートし、外部データを参照して、新しいレコードの標準的な用語と形式に揃えることができます。

[カテゴリ]、[ステータス (State)]、[アサイン先グループ] などのフィールドのデータを、Security Operations テーブル内で使用される値にマッピングできます。たとえば、[分析中 (In Analysis)] を [対応中] にマッピングします。

セキュリティオペレーション フィールド値変換の作成

[フィールド値変換] は、指定されたソースデータと使用する置換値の間の 1 つの変換を定義します。

始める前に

必要なロール：sn_sec_cmn.basic または sn_si.basic

このタスクについて

検索値に一致するものがある場合、指定されたソースデータ内に検索値が含まれている場合、または一致するものが見つからない場合に適用する各変換エントリーを定義します。一致が見つからない場合のデフォルト値を設定します。デフォルト値が設定されておらず、一致するものが見つからない場合は、元のソースデータが使用されます。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > ユーティリティ > フィールド値変換.

2. [**New**] をクリックします。

3. 必要に応じて、フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド値変換

フィールド	説明
名前	フィールド値変換の名前。
説明	フィールドマップの説明。
フィールド値変換エントリー	エントリーのテーブルリスト。 **a.** [データを置換する] で、[新しい行を挿入] をダブルクリックします。 **b.** 次のいずれかを選択します。 このフィールドの日付が一致するとき (When the date for this field matches) このフィールドのデータが次を含むとき 他の変換エントリーがデータと一致しないとき (デフォルト) **c.** 緑色のチェック マークをクリックします。 **d.** [検索値] の下でダブルクリックし、検索値を追加します。 **e.** 緑色のチェック マークをクリックします。 **f.** [置換値] の下で、ServiceNow の対応する値をダブルクリックします。 **g.** 必要に応じて繰り返します。
有効	この変換をアクティブ化するには、このチェックボックスをオンにします。
アプリケーション	アプリケーションのスコープ。

4. [送信] をクリックします。

セキュリティオペレーション 拡張データマッピング

拡張データマッピングは、XML、JSON、または プロパティ ファイルから ServiceNow レコードにデータを変換します。セキュリティオペレーション ワークフローは拡張データマップを使用し、セキュリティインシデントに出力データを提供します。

セキュリティオペレーション には複数の拡張データマップが含まれ、[Security Operations Integrations - ネットワーク統計情報を取得] フローや Security Operations System Command Integration - 実行中のプロセスを取得フローなど、さまざまなワークフローによってトリガーされます。セキュリティオペレーション ワークフローからの拡張データマップ出力は、セキュリティインシデントフォームの [拡張データ] タブに表示されます。

セキュリティオペレーション 拡張データマップの作成

拡張データマップを使用して、JSON、XML、または プロパティ ファイル形式から ServiceNow レコードにデータを変換します。

始める前に
必要なロール：sn_sec_cmn.write

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
既存の拡張データマップは、セキュリティオペレーション 内で提供されるワークフローで使用されます。[拡張データマッピング] でリストを表示できます。マップを使用するには、ビジネスルールまたはワークフローのいずれかのトリガーが必要です。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > ユーティリティ > 拡張データマッピング.
2. [**New**] をクリックします。
3. 必要に応じてフィールドに入力します。

拡張データマップの作成

フィールド	説明
名前	この拡張データマップの名前。
入力形式	リストから形式を選択します。 JSON (デフォルト) XML プロパティファイル形式
プリフィックスキー	入力データセットを指定されたキーに制限するために使用します。入力データセットのルートはこのキーに設定されます。この例では、「file_info」と入力すると、入力値は file_info 内の値に制限されます。 <?xml version="1.0" encoding="UTF-8"?> <malware> <version>2.0</version> <file_info> <malware>yes</malware> <sha1>24c051142583e10451a53893fed3aa5d80bfb1f6</sha1> <filetype>PE</filetype> <sha256>be9bd96808173e2d967feef8c8c5b8c4d73b621584fb11eb68434da1e6a0a9307</sha256> <md5>ee8c91751b3010e38c479cf9ab09827a</md5> <size>546304</size> </file_info> </malware>
アプリケーション	アプリケーションのスコープ。
重複ルール	レコードが重複と見なされた場合に、重複レコードに対して実行するアクションを定義するルール。
宛先テーブル	リストからテーブルを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
有効	このマップをアクティブ化するには、このチェックボックスをオンにします。
説明	拡張データマップの説明を入力します。

4. [送信] をクリックします。
   [拡張データマッピングフィールド] タブが表示されます。
5. [新規] をクリックします。
6. 必要に応じて、フォームのフィールドに入力します。

拡張データマッピングフィールド

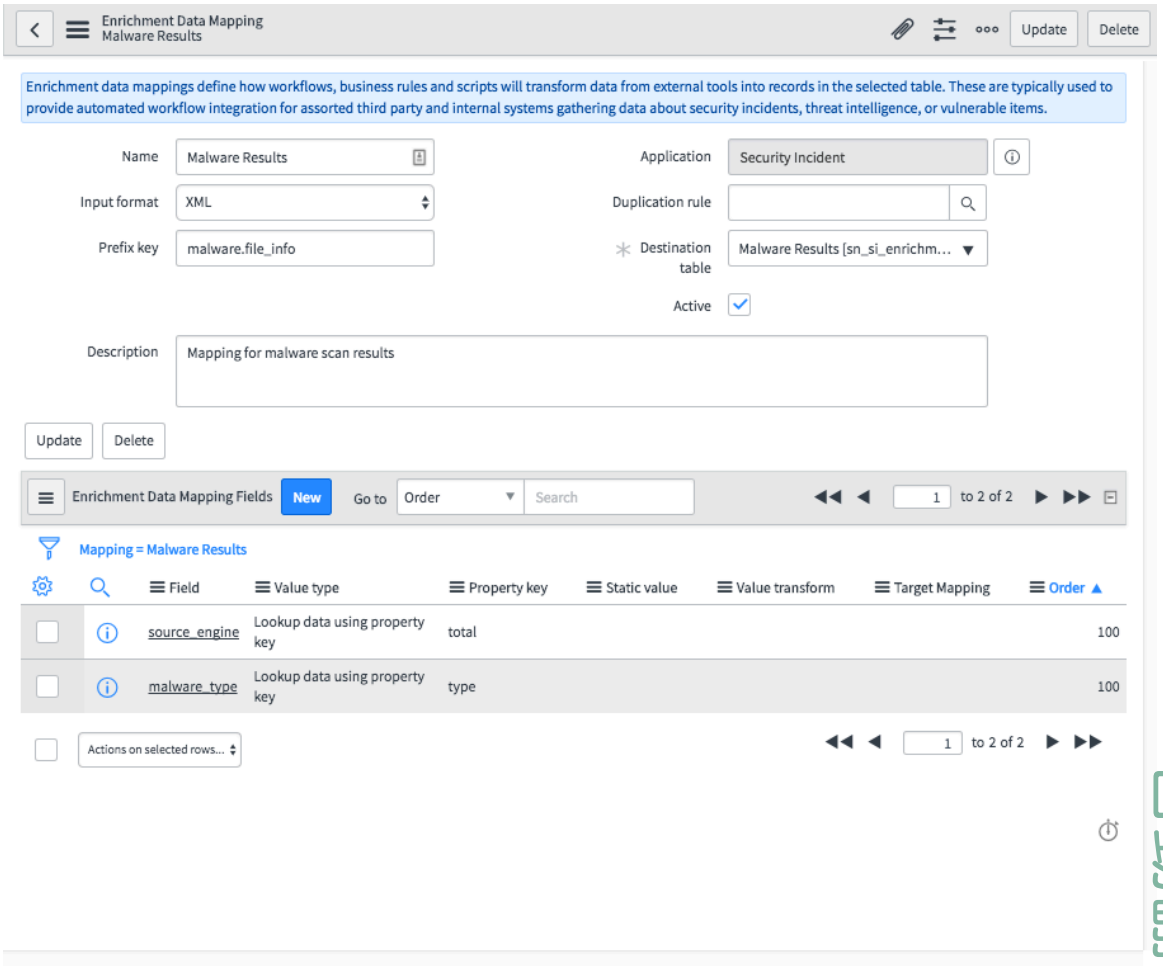
フィールド	説明
フィールド	拡張データマップの名前。
値のタイプ	リストから選択します。 プロパティキーを使用したルックアップデータ 静的値 静的な値にプロパティキーのデータを加えたもの フィールドは配列またはオブジェクト (生データのネスト) 選択肢ごとに異なるエントリーがあります。フィールド値とアレイまたはオブジェクトにはプロパティキーが必要です。
プロパティキー	入力データ検索のキー、およびターゲットフィールドに書き込まれる値を決定します。
値の変換	ある値を別の値にマップするフィールド値変換。
アプリケーション	アプリケーションのスコープ。
順序	マッピングを考慮する順序。最初の一致が使用されます。デフォルトは 100 です。
マッピング	拡張データマップの名前。
宛先テーブル	フィールドのマップ先テーブル。

7. **[Submit]** をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

拡張データマップの例を次に示します。



セキュリティオペレーション のユーザー定義のエスカレーション

注意や専門知識がさらに必要な問題のセキュリティインシデント用にエスカレーションパスを作成できます。エスカレーショングループが存在する場合、そのグループのセキュリティインシデントにボタンが表示されます。

セキュリティオペレーション ユーザー定義のエスカレーショングループの作成

エスカレーションを使用して、インシデントに関連付けられたグループにセキュリティインシデントをエスカレートします。

始める前に
必要なロール：sn_si.admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > グループ > エスカレーション.
2. [新規] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

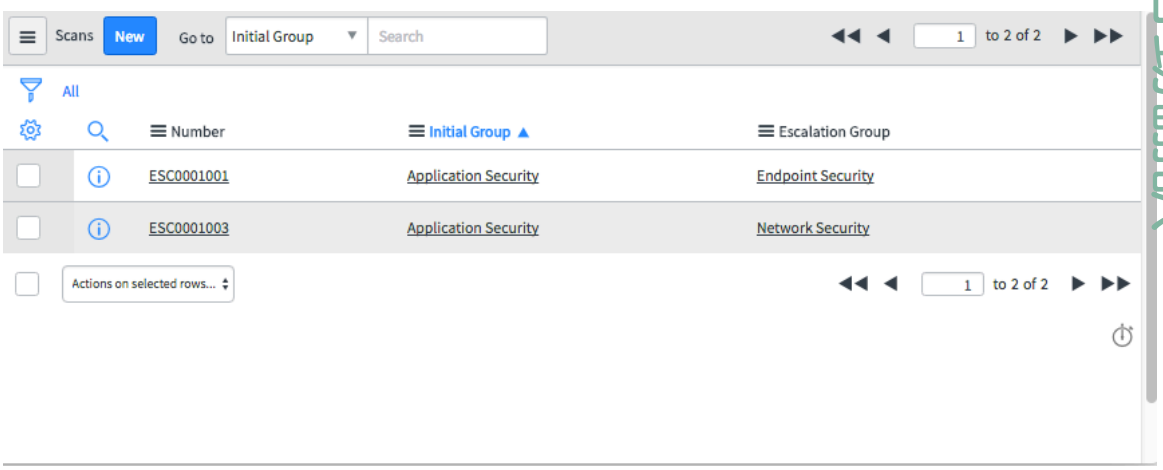
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エスカレーション

フィールド	説明
数値	エスカレーションインシデント番号 (フィールドは自動生成)。
初期グループ	このセキュリティインシデントが属するグループを選択します。
エスカレーション グループ	セキュリティインシデントをエスカレートするグループを選択します。

4. **[Submit]** をクリックします。
   エスカレーショングループは、初期グループ内のすべてのセキュリティインシデントで使用できます。複数のグループを作成できます。



ドメインセパレーションプロパティの上書きの作成

ドメインセパレーションを使用すると、既存の Security Operations プロパティを上書きして、各ドメイン内のアプリケーションの機能をカスタマイズできます。

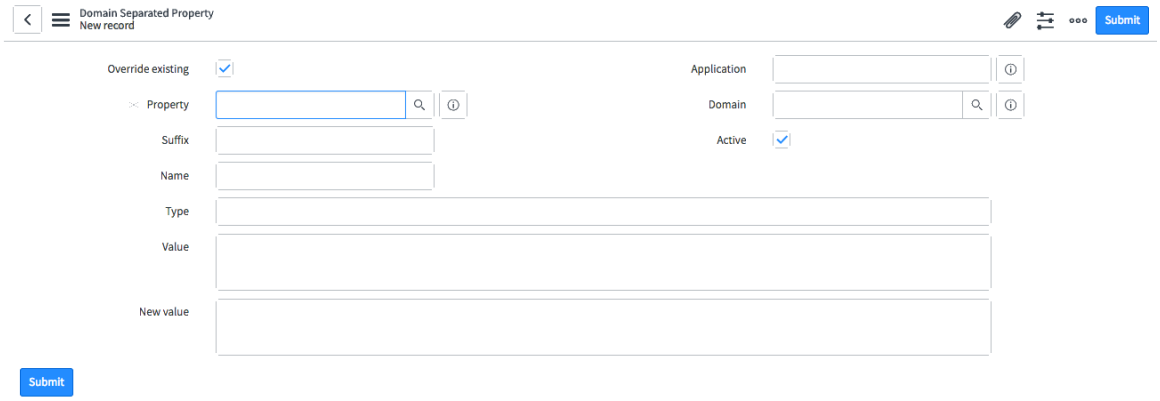
始める前に
ドメインサポート - ドメイン拡張 を有効にする必要があります。ドメイン上書きビューアー についても確認します。

必要なロール：admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > ユーティリティ > ドメイン区切りプロパティ.
2. [**New**] をクリックします。



3. フォームのフィールドに入力します。

ドメインセパレーションプロパティフォーム

フィールド	説明
既存の内容を上書き	既存のプロパティにドメイン固有の値を作成するには、このチェックボックスをオンにします。
アプリケーション	上書きするプロパティを含むアプリケーションを選択します。
プロパティ	ドメイン固有の上書きを作成する、選択したアプリケーションのプロパティを選択します。
ドメイン	このプロパティの上書きを作成するドメインを選択します。
有効	上書きをオンまたはオフにします。
サフィックス	プロパティのサフィックスを表示します。
名前	プロパティ名を表示します。
タイプ	プロパティタイプを表示します。
値	プロパティに設定されている現在の値を表示します。
新しい値	このドメインに適用するプロパティの新しい値を入力します。

4. **[Submit]** をクリックします。
プロパティの上書きは、指定されたドメイン内の選択したプロパティに適用されます。このプロパティのロジックがトリガーされると、ドメインセパレーションプロパティの上書きがチェックされます。ドメインの上書きが見つかった場合は、新しい値が使用されます。それ以外の場合は、デフォルトのドメインの値が使用されます。

関連情報

ドメインセパレーションの概要

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オペレーティングシステムグループの作成

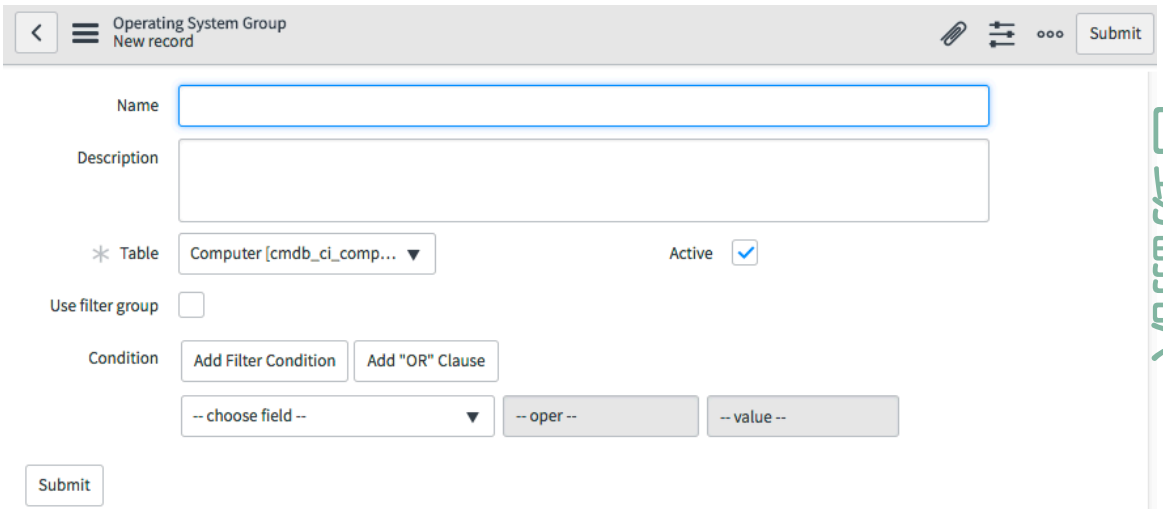
オペレーティングシステムグループは、セキュリティインシデントレスポンス ワークフロー内の特定のプロセスタイプとスクリプトにオペレーティングシステムをマッピングするために使用されます。スクリプトは、定義されたオペレーティングシステムグループの実行中のプロセスを取得する方法を定義します。必要に応じて新しいオペレーティングシステムを追加できます。

始める前に

必要なロール：sn_sec_cmn.admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > ユーティリティ > オペレーティングシステムグループ.
   ベースシステムには、次の 3 つのオペレーティングシステム用のスクリプトが含まれています。
   - BSD ベースの OS
   - POSIX ベースの OS
   - Windows OS
2. [新規] をクリックします。



3. 必要に応じて、フィールドに入力します。

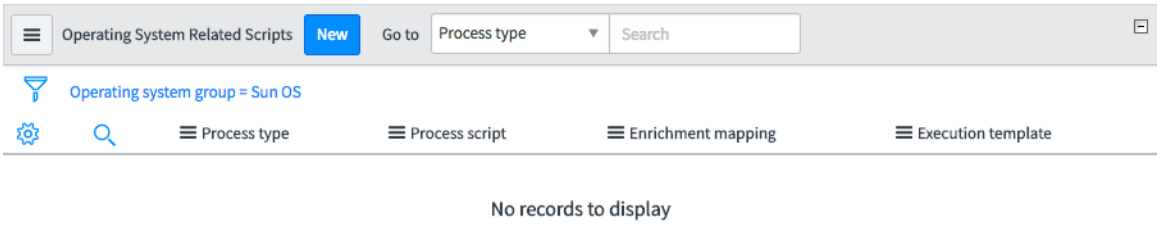
フィールド	説明
名前	オペレーティングシステムグループの名前。
説明	オペレーティングシステムグループの説明。
テーブル	影響を受けるテーブル。
有効	このオペレーティングシステムグループをアクティブ化するには、このチェックボックスをオンにします。
フィルタグループを使用	選択したテーブル内の一致するレコードを見つけるためにフィルターグループを使用するには、このチェックボックスをオンにします。
フィルターグループ	選択したテーブル内の一致するレコードを見つけるためのフィルターグループを選択します。このフィールドは、[フィルターグループを使用] チェックボックスをオンにした場合のみ表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
条件	- [条件ビルダー] フィールドは、[フィルターグループを使用] チェックボックスをオンにしなかった場合にのみ表示されます。

4. フォームヘッダーを右クリックし、[保存] を選択します。
[オペレーティングシステム関連スクリプト] 関連リストが開きます。



5. [新規] をクリックします。
6. 実行中のプロセス、サービス、ネットワーク統計情報を取得するために使用しているワークフローに対応するスクリプトを選択します。
7. **[Submit]** をクリックします。

関連情報

ファイル同期された MID サーバーへのスクリプトファイルの添付

セキュリティタググループとタグのセットアップ

セキュリティインシデント、応答タスク、脆弱性一致アイテム、観測事象、IoC、およびセキュリティケースにタグを割り当てて、応答レコードのメタデータを作成し、特定のタイプのセキュリティコンテンツにアクセスする必要があるユーザーを定義できます。タグをセキュリティグループに追加して整理することができます。

始める前に
必要なロール：sn_si.admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > セキュリティタグ > グループ.
デフォルトの分類グループ 3 つがベースシステムに含まれています。
   - 拡張許可リスト/拒否リスト **(Enrichment allow list/deny list)**：このグループは、レコードを許可リストまたは拒否リストのレコードとして扱うかどうかを定義します。許可リストレコードは一般的に重要性が低いため、無視できます。一般的に、拒否リストレコードの方が重要です。
   - メタタグ：このグループはデモデータとして提供されます。これを使用して、SecOps アプリケーションで使用されるカスタム分類タグを作成できます。
   - **Traffic Light Protocol**：このグループは、機密情報が正しい対象者と共有されるようにするために使用されます。4 つの色 (白、緑、オレンジ、赤) を使用して、さまざまな感度を示します。色ごとに適切な読み取り/書き込みアクセスロールを割り当てることができます。信頼できるセキュリティサークルと観測事象を共有する場合、信頼できるセキュリティサークルのプロファイルに割り当てられたタグによって、サークルで共有できる TLP タグ付き観測事象が次のように決まります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- TLP：白：TLP：白タグの付いた観測事象のみを TLP：白のプロファイルに共有できます。
- TLP：緑：TLP：白タグとTLP：緑タグの付いた観測事象を TLP：緑のプロファイルに共有できます。
- TLP：オレンジ：TLP：白タグ、TLP：緑タグ、TLP：オレンジタグの付いた観測事象を TLP：オレンジのプロファイルに共有できます。
- TLP：赤：TLP タグに関係なく、すべての観測事象を TLP：赤のプロファイルに共有できます。これは、TLP：赤が最高ランクの TLP タグであるためです。

注:
他の TLP 色を追加することもできますが、含まれている 4 つの色以外の色は、Forum for Incident Response and Security Teams (FIRST) では有効なものとみなしません。

2. [新規] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
名前	セキュリティグループの名前を入力します。
複数選択を許可する	グループを共有するレコードに複数のセキュリティタグをアサインできるようにする場合は、このボックスをオンにします。
有効	グループをオンまたはオフにします。
説明	このグループの説明を入力します。

4. フォームヘッダーを右クリックし、[保存] を選択します。
[セキュリティタグ] 関連リストが表示されます。
5. [セキュリティタグ] 関連リストで、[新規] をクリックします。
6. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
名前	分類タグの名前。
セキュリティタググループ	グループ関連リストの [新規] ボタンを使用してタグを作成した場合、このフィールドはデフォルトで現在のグループになります。必要に応じて別のグループにタグを追加できますが、これはオプションです。
順序	フォームまたはリスト内でのタグの表示順序を指定します。
色	このタグの色を選択します。
制限されたアクセスを強制する	このチェックボックスをオンにすると、ユーザーがこのセキュリティタグを持つレコードを読み書きするために必要な読み取りロールや書き込みロールをアサインできます。
有効	タグをオンまたはオフにします。
説明	このタグの説明。
ロール (読み込みアクセス)	セキュリティタグへの読み取りアクセス権をアサインするには、ロックアイコンをクリックし、適切なアクセスロールを選択して、ロックアイコン

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	を再度クリックします。このフィールドは、[制限されたアクセスを強制する] チェックボックスをオンにした場合のみ表示されます。
ロール (書き込みアクセス)	セキュリティタグへの書き込みアクセス権をアサインするには、ロックアイコンをクリックし、適切なアクセスロールを選択して、ロックアイコンを再度クリックします。このフィールドは、[制限されたアクセスを強制する] チェックボックスをオンにした場合のみ表示されます。

7. さらにセキュリティタグを作成するには、必要に応じて繰り返します。
8. **[Update** (更新)] をクリックします。

> **注:**
> に移動して、新しいタグを作成することもできます セキュリティオペレーション > セキュリティタグ > タグ. 手順は同じです。

セキュリティタグルールの作成

セキュリティタグルールは、セキュリティタグアクセスのフィルタリングを提供します。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > セキュリティタグ > タグ.
2. セキュリティタグを選択または作成します。
3. [セキュリティタグルール] 関連タブで、[新規] をクリックします。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
名前	セキュリティタグルールの名前。
セキュリティタグ	ルールに添付するセキュリティタグ。
有効	セキュリティタグをオンまたはオフにします。
説明	このルールの説明。

5. [レコードフィルタリング] を指定します。
6. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
フィルタグループを使用	フィルターグループをルールに関連付けます。
テーブル	ルールを格納するテーブル。
条件	1 つ以上のフィルター条件を追加します。

7. [送信] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

セキュリティタグルールをインポート

展開内の他のテーブルからセキュリティタグルールをインポートできます。

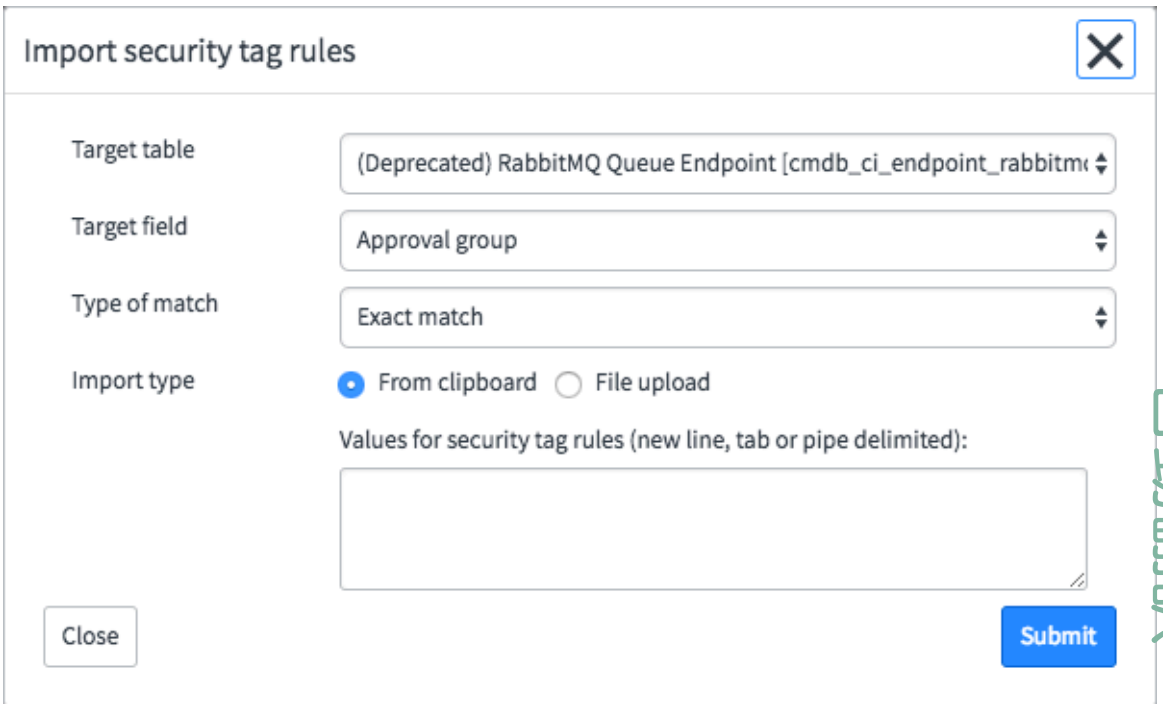
始める前に
必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > セキュリティタグ > タグ.

2. セキュリティタグを選択または作成します。

3. [セキュリティタグルールをインポート] 関連リンクをクリックします。



4. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
ターゲットテーブル	ルールのインポートに使用するテーブルを選択します。
ターゲットフィールド	ルールのインポートに使用するフィールドを選択します。
一致タイプ	インポートしたルールをセキュリティタグと照合する方法を次から選択します。 完全一致 (デフォルト) 包含 次で始まる 次で終了 正規表現
インポートタイプ	次から選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	ソースクリップボード 区切り付き値のリストをテキスト領域にコピーします。値はセキュリティタグに解析されます。 ファイルのアップロードから (From file upload) 区切り付き値を含むファイルをアップロードします。値はセキュリティタグに解析されます。 改行やパイプの区切り文字を使用して、セキュリティタグルールの値を追加します。

5. [送信] をクリックします。

セキュリティ注釈

セキュリティ注釈は、構成アイテム、観測事象、またはセキュリティインシデントの使用時に追加される説明のメモまたはコメントです。

ユーザーと観測事象に対して複数のセキュリティ注釈を使用できます (脅威インテリジェンス プラグインが必要)。セキュリティ注釈に関するレポートも利用できます。

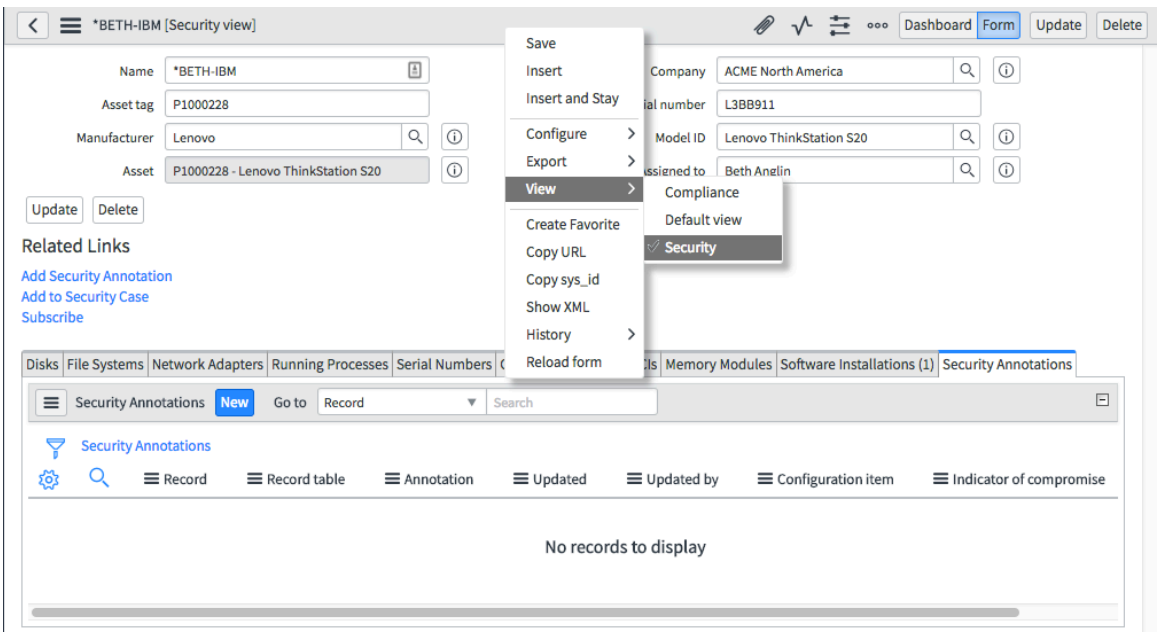
CI のセキュリティ注釈の作成

CI の注釈を使用すると、インシデント全体のアクティビティを追跡できます。単一または複数の CI に注釈を追加できます。

始める前に
必要なロール：admin

手順

1. セキュリティインシデントまたは構成アイテムテーブルから、CI を開きます。
2. ヘッダーを右クリックして、 ビュー > **Security** (セキュリティ).



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [セキュリティ注釈] 関連リストで、[新規] をクリックします。
4. 注釈を入力します。
   注釈は任意のテキスト形式にすることができます。
5. [送信] をクリックします。

> **注:**
> 複数の CI に同じ注釈を追加するには、リストで CI を選択し、[セキュリティ注釈を追加] を選択し、任意のテキスト形式で注釈を入力して、[送信] をクリックします。

観測事象のセキュリティ注釈の作成

1 つまたは複数の観測事象を選択し、[選択した行のアクション] 選択肢メニューを使用してそれらにセキュリティ注釈を適用できます。

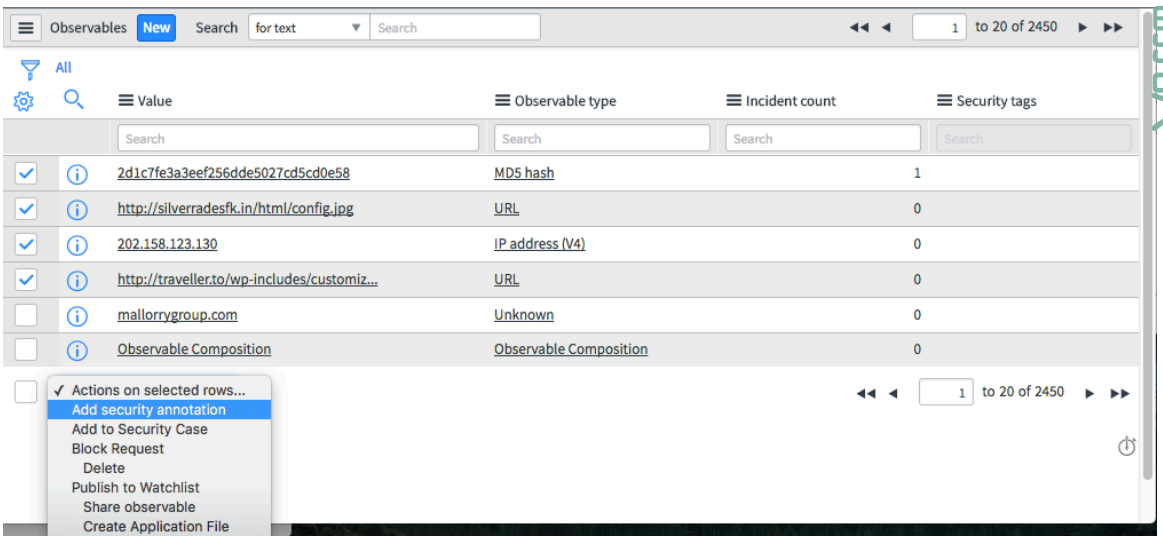
始める前に

- 脅威インテリジェンス プラグインとアクティベーションが必要です。脅威インテリジェンス プラグインは、個別のサブスクリプションとして使用できます。

必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > 脅威インテリジェンス > 観察事項
2. リストから 1 つ以上の観測事象を選択します。
3. [選択した行のアクション] ドロップダウンメニューで、[セキュリティ注釈を追加] を選択します。



4. 注釈を入力します。
   注釈は任意のテキスト形式にすることができます。
5. **[Submit]** をクリックします。

ユーザー向けセキュリティ注釈の作成

1 人または複数のユーザーを選択し、[選択した行のアクション] 選択肢メニューを使用してそれらにセキュリティ注釈を適用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
脅威インテリジェンス プラグインとアクティベーションが必要です。脅威インテリジェンス プラグインは、個別のサブスクリプションとして使用できます。

必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > ユーザー管理 **(User Administration)** > ユーザー
2. リストから 1 人以上のユーザーを選択します。
3. [選択した行のアクション] ドロップダウンメニューで、[セキュリティ注釈を追加] を選択します。
4. 注釈を入力します。
   注釈は任意のテキスト形式にすることができます。
5. **[Submit]** をクリックします。

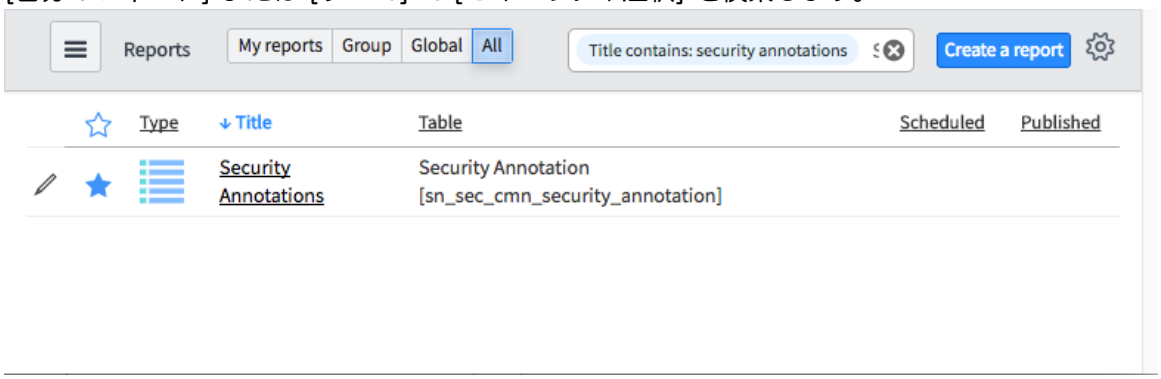
セキュリティ注釈レポートの表示

セキュリティ注釈レポートには、セキュリティ注釈 [sn_sec_cmn_security_annotations] テーブルに格納されている詳細が表示されます。レポートの列をカスタマイズし、必要に応じてデータをグループ化できます。

始める前に
必要なロール：admin

手順

1. 次のように移動する。 **All** (すべて) > レポート > 表示/実行.
2. [自分のレポート] または [すべて] で [セキュリティ注釈] を検索します。



関連情報

[レポート] リストの表示

一緒にインストールされるコンポーネント **Security Support Common**

Security Support Common と併せて、複数のタイプのコンポーネントがインストールされます。セキュリティインシデントレスポンス など、さまざまなセキュリティアプリケーションで使用する共通の機能を提供します。

インストールされているコンポーネントの検索と表示

インストールされているコンポーネントの検索と表示の詳細については、「Security Support Common とともにインストールされるコンポーネントの表示」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Security Support Common とともにインストールされるコンポーネントの表示

Security Support Common プラグインをアクティブ化すると、テーブル、ユーザーロール、モジュールなど、いくつかのタイプのコンポーネントがインストールされます。

コンポーネントの検索

> **注:**
> アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「アプリケーションとともにインストールされているコンポーネントの検索」を参照してください。

インストールされるコンポーネントのリストを、Security Support Common アプリケーションのロール、スケジュール済みジョブ、テーブルに制限するには、次の手順を実行します。

アプリケーションとともにインストールされるコンポーネントのフィルター済みリストの表示

アプリケーションファイルテーブルをフィルタリングして、アプリケーションとともにインストールされたロール、スケジュール済みジョブ、およびテーブルのみを表示します。これらのコンポーネントを表示するアプリケーションは、そのファイルがインスタンスとメタデータテーブルにロードされるようにインストールする必要があります。アプリケーションファイルテーブルからフィルター済みリストを表示するには、次の手順に従います。

1. フィルターナビゲーターで、「**sys_metadata.list**」と入力してメタデータテーブルに移動します。
2. 条件ビルダー (フィルターアイコン) を選択し、次を選択します。 アプリケーション > 次の値に等しい その後にアプリケーションの名前が続きます。
3. 条件ビルダーで 2 番目のフィルターを追加するには、[**AND**] をクリックして次を選択します。 クラス > は をクリックし、リストから [ロール]、[スケジュール済みジョブ]、または [テーブル] のいずれかのクラスを選択します。
4. **[Run** (実行)] を選択します。

選択したクラスの結果がフィルター済みリストに表示されます。

[store-future: BEGIN review]

Security Operations アプリケーションのロール別モジュールアクセス

アプリケーションごとに、特定のロールがアクセスできるメニューアイテムが表示されます。

[End]
[store-future: BEGIN review]

コンフィギュレーションコンプライアンスのロール別のモジュールアクセス

コンフィギュレーションコンプライアンスでは、特定のロールがアクセスできるメニューアイテムが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

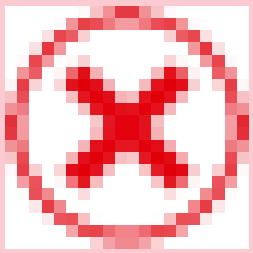
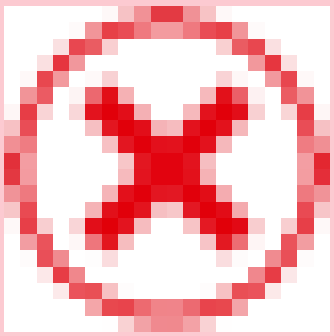
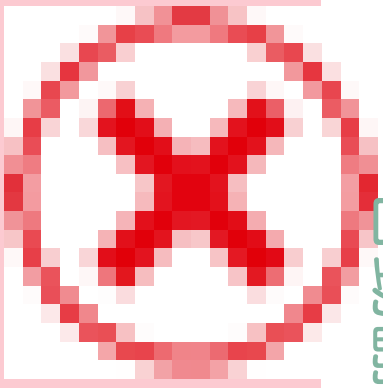
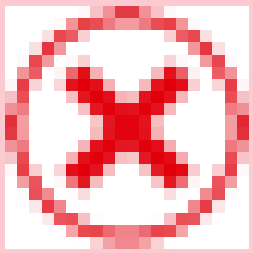
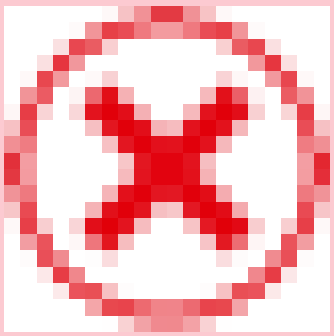
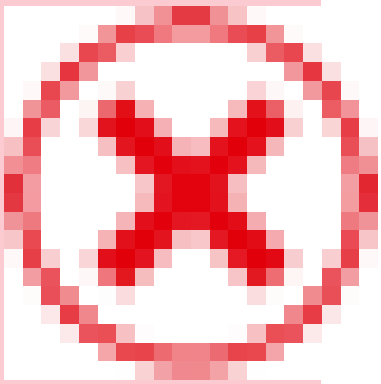
モジュールアクセス：
sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_approv

モジュールアクセス：
sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_approval_rules、sn_vu

その他のロールの情報：

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

sn_vulc.remediation_owner

モジュール	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vulc.m
(メインアプリグループ)					
概要					
ポリシー					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

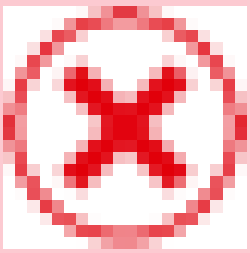
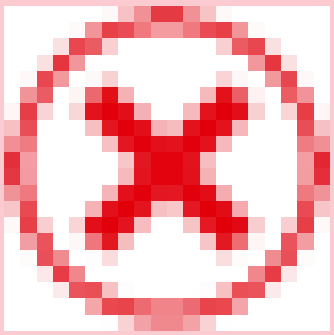
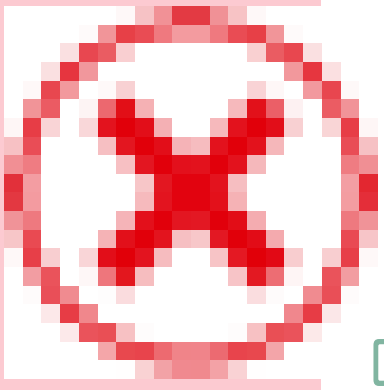
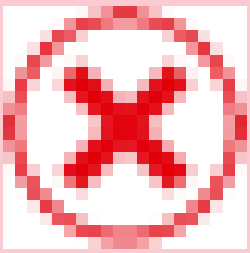
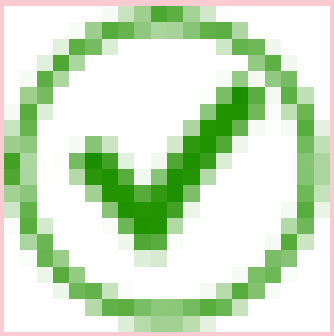
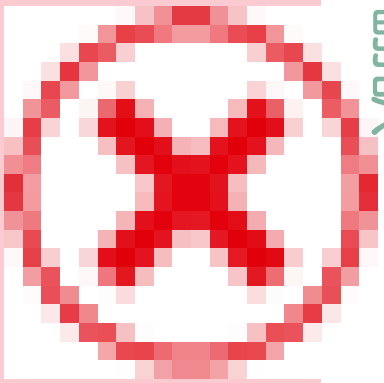
モジュールアクセス：
sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_approval_rules、sn_vu

その他のロールの情報：

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

sn_vulc.remediation_owner

(続く)

モジュール	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vulc.m
テスト					
自分の承認					

テスト結果

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

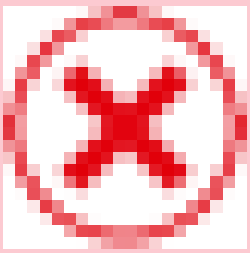
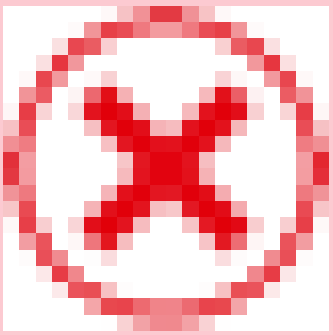
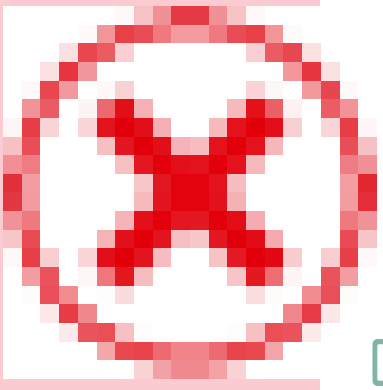
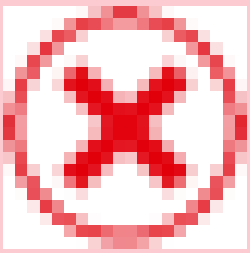
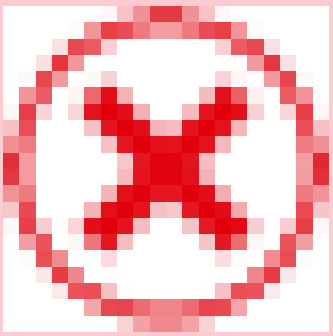
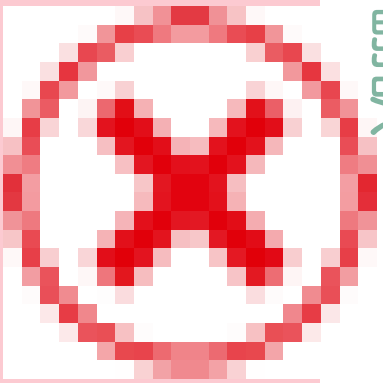
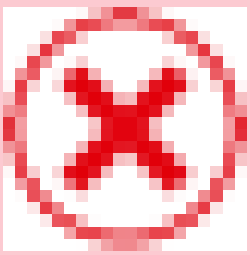
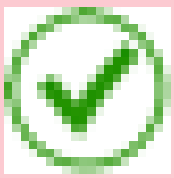
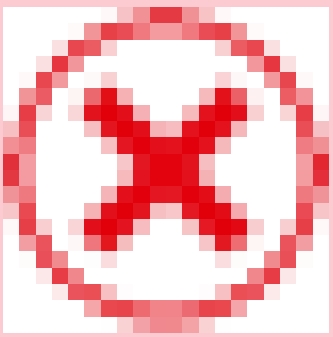
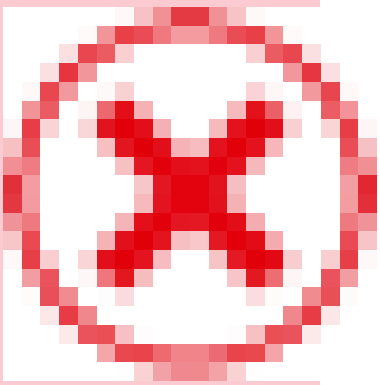
モジュールアクセス：
sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_approval_rules、sn_vu

その他のロールの情報：

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

sn_vulc.remediation_owner

(続く)

モジュール	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vulc.m
未トリアージのテスト結果					
自分のオープンなテスト結果					
テスト結果を開く					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

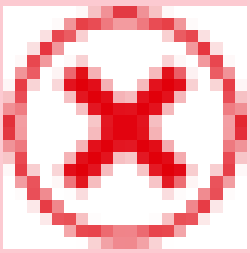
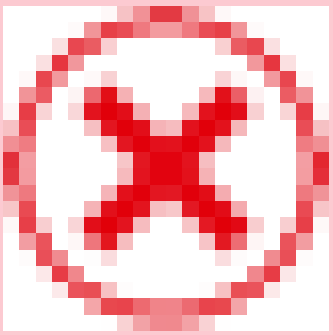
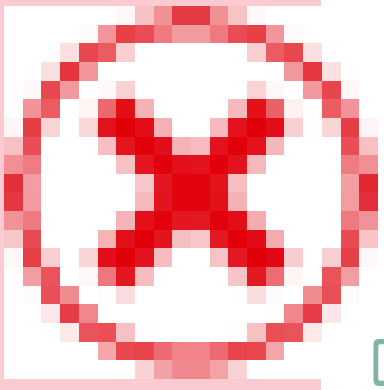
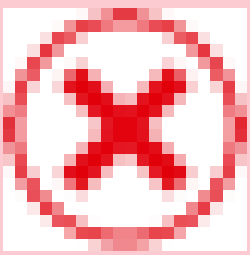
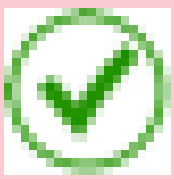
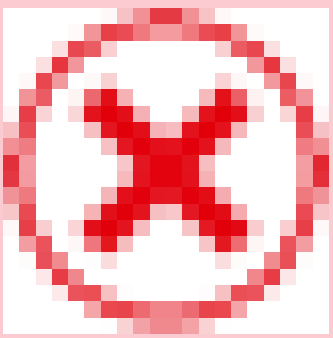
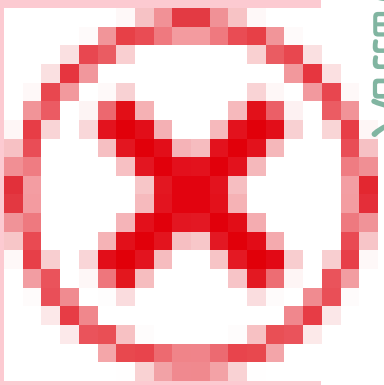
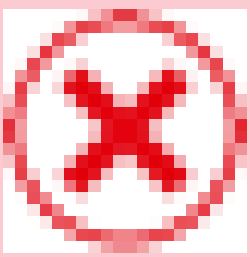
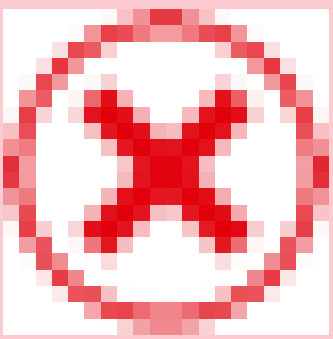
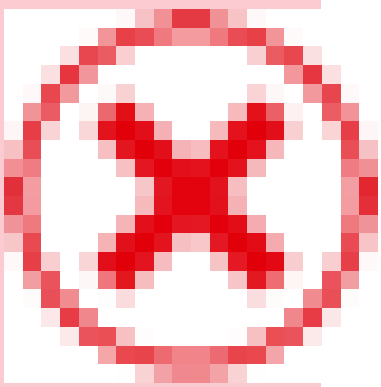
モジュールアクセス：
sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_approval_rules、sn_vu

その他のロールの情報：

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

sn_vulc.remediation_owner

(続く)

モジュール	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vulc.m
該当 CI 確認中					
CI 不明					
未アサイン					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

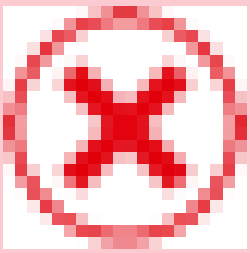
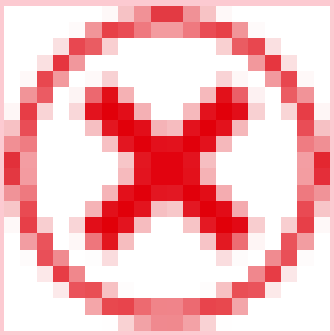
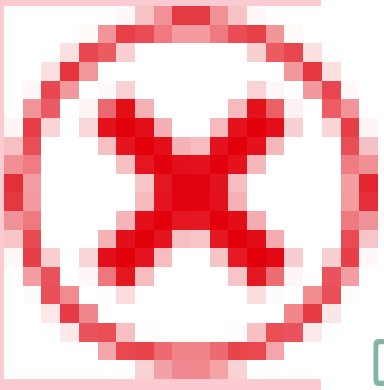
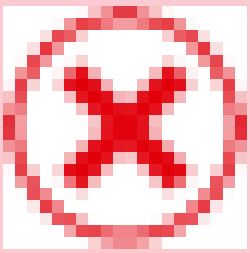
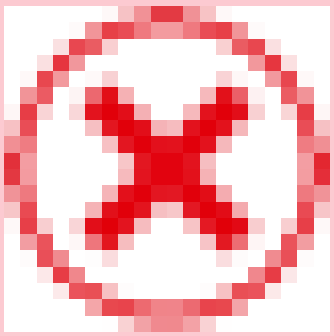
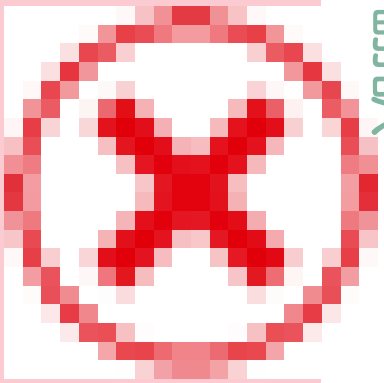
モジュールアクセス：
sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_approval_rules、sn_vu

その他のロールの情報：

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

sn_vulc.remediation_owner

(続く)

モジュール	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vulc.m
複数の保留					
すべて					

テスト結果グループ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

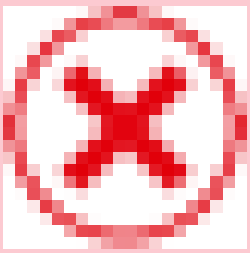
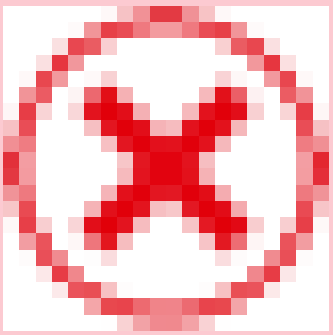
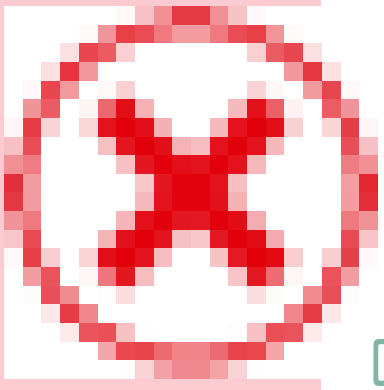
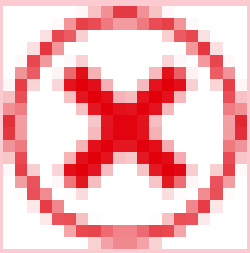
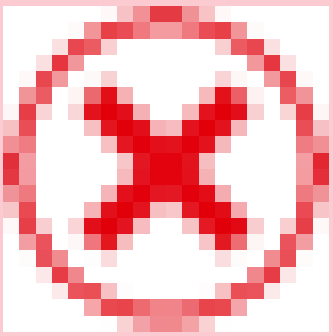
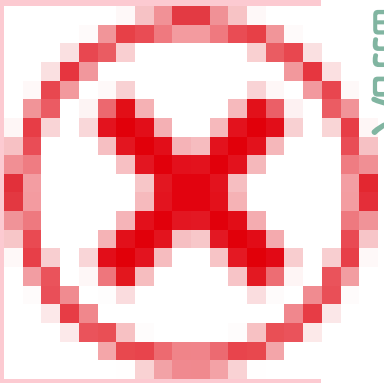
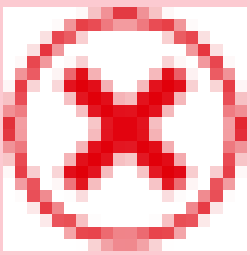
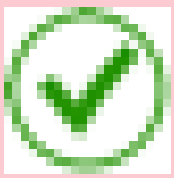
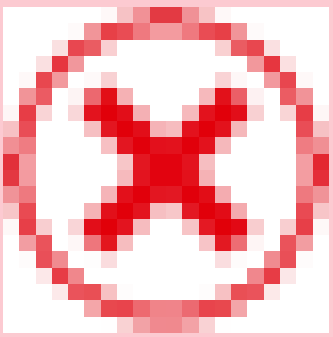
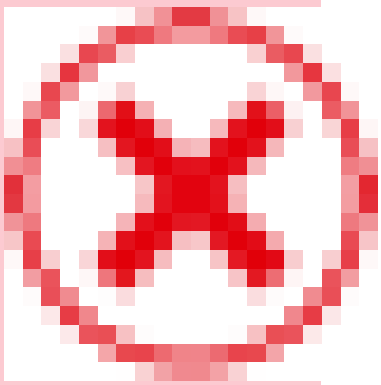
モジュールアクセス：
sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_approval_rules、sn_vu

その他のロールの情報：

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

sn_vulc.remediation_owner

(続く)

モジュール	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vulc.m
自分のオープングループ					
すべてのオープングループ					
複数の保留					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

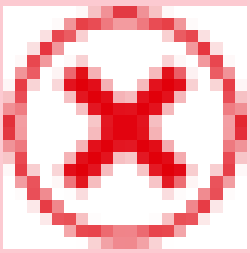
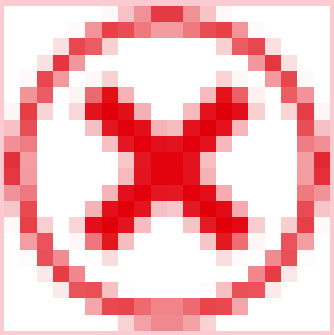
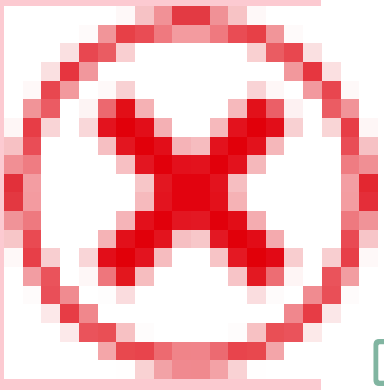
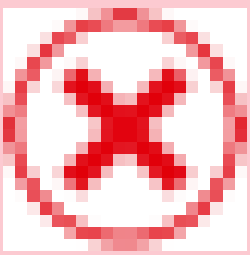
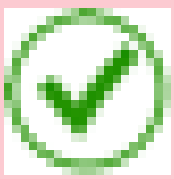
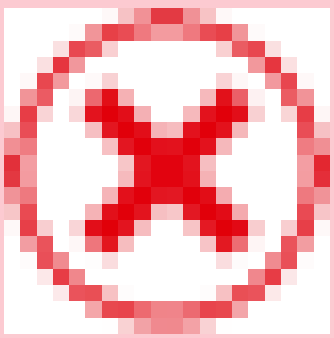
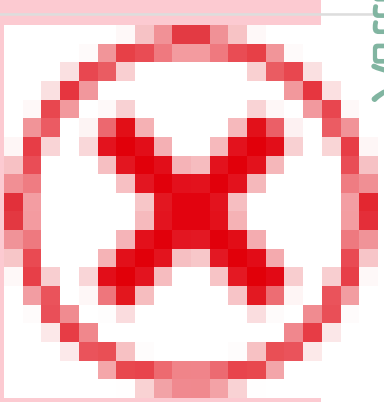
モジュールアクセス：
sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_approval_rules、sn_vu

その他のロールの情報：

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

sn_vulc.remediation_owner

(続く)

モジュール	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vulc.m
すべてのグループ					
提出データ					
信頼できるソース					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

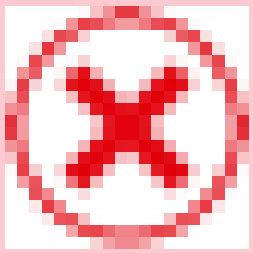
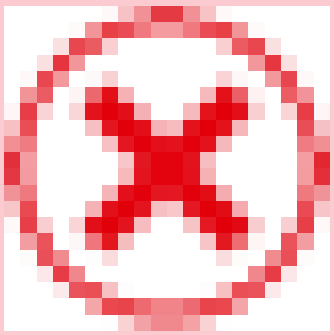
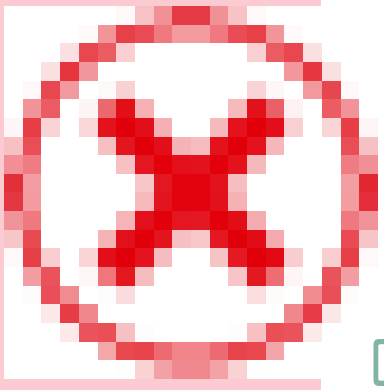
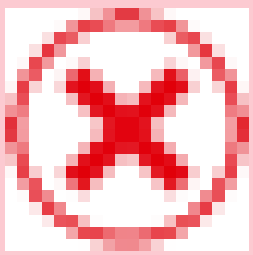
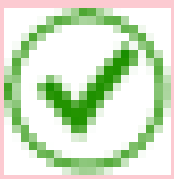
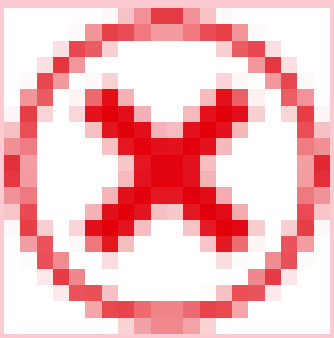
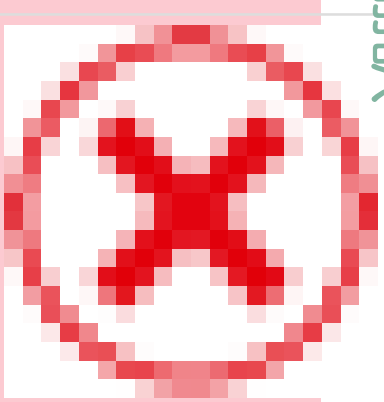
モジュールアクセス：
sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_approval_rules、sn_vu

その他のロールの情報：

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

sn_vulc.remediation_owner

(続く)

モジュール	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vulc.m
テクノロジー管理					
アサインルール					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

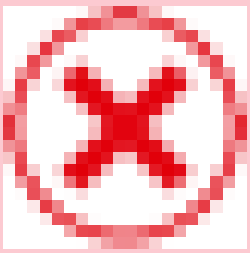
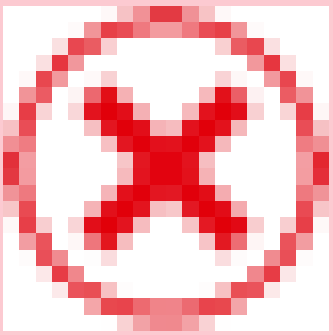
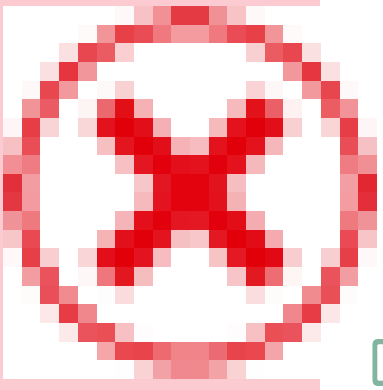
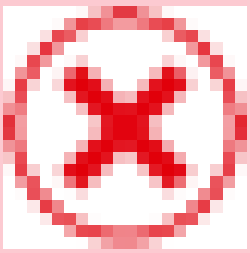
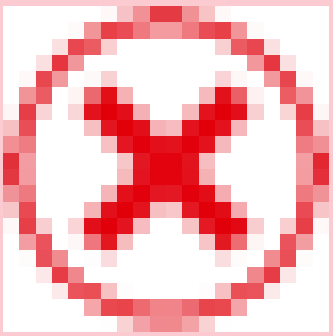
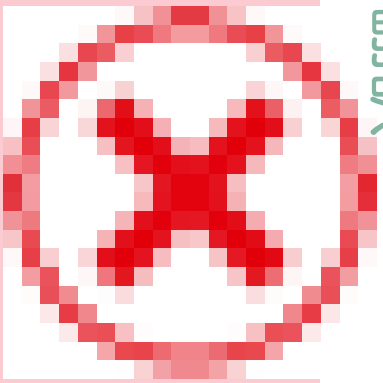
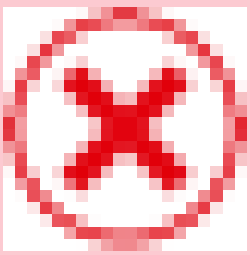
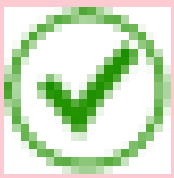
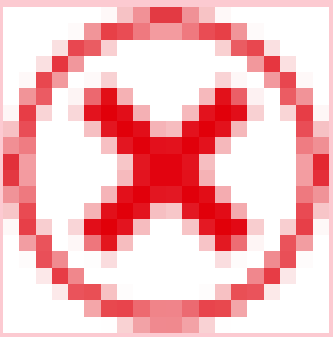
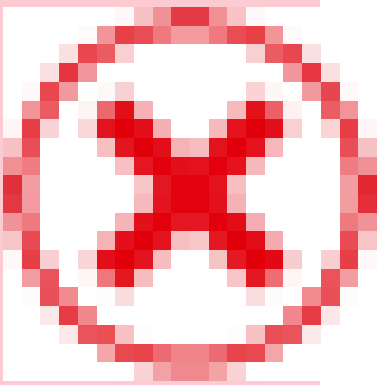
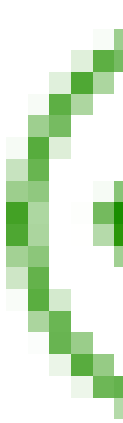
モジュールアクセス：
sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_approval_rules、sn_vu

その他のロールの情報：

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

sn_vulc.remediation_owner

(続く)

モジュール	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vulc.m
古いテスト結果の自動クローズ					
グループルール					
自動例外ルール					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

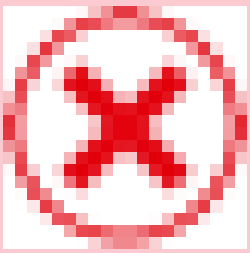
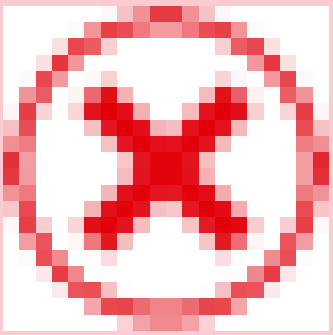
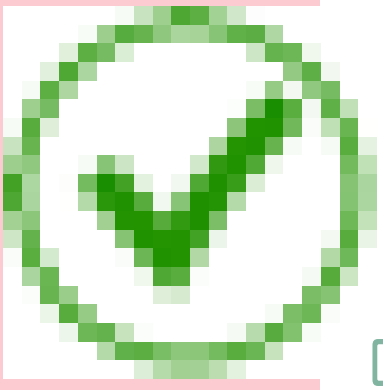
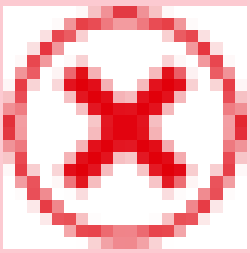
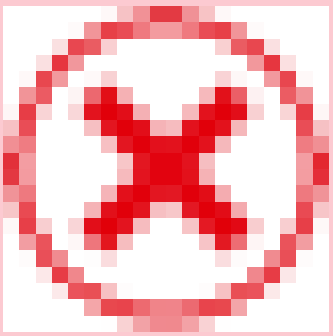
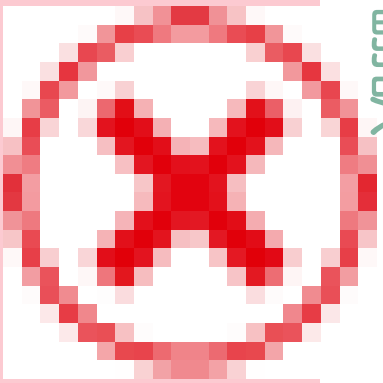
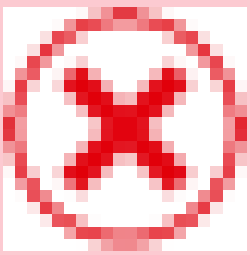
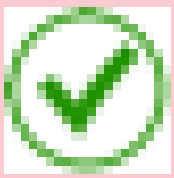
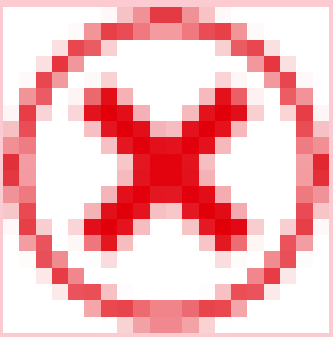
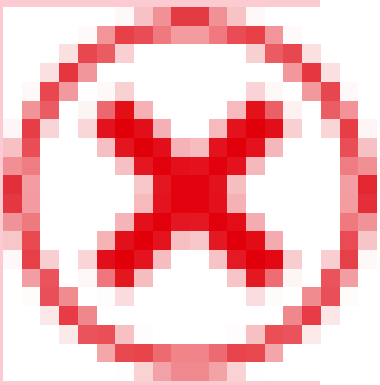
モジュールアクセス：
sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_approval_rules、sn_vu

その他のロールの情報：

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

sn_vulc.remediation_owner

(続く)

モジュール	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vulc.m
承認ルール					
リスク算出					
リスクスコアロールアップ算出					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

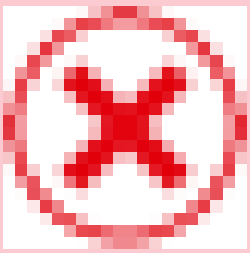
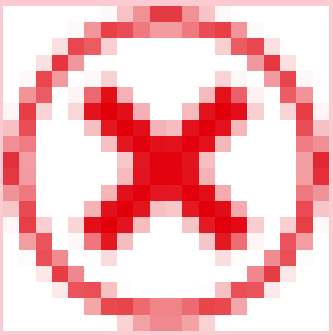
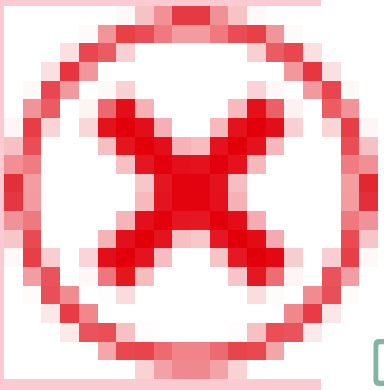
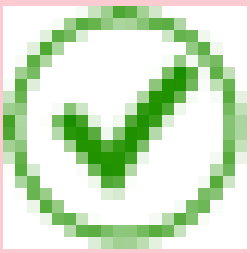
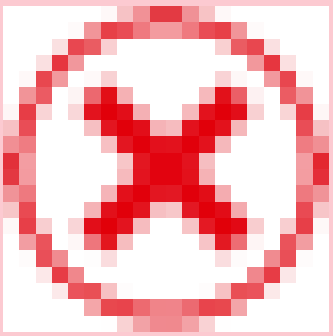
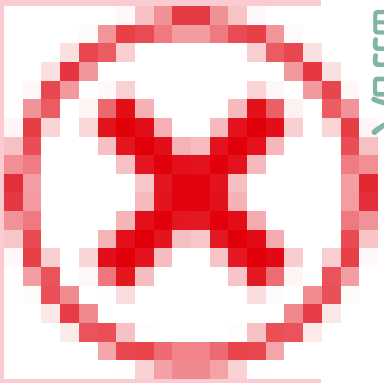
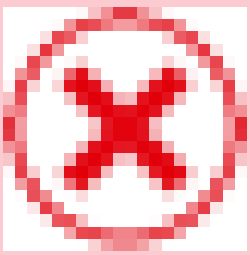
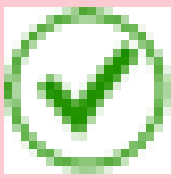
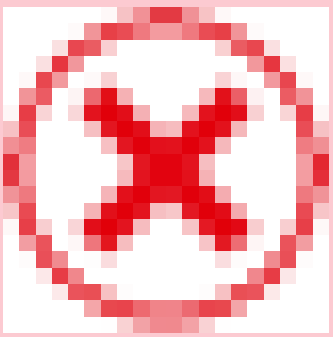
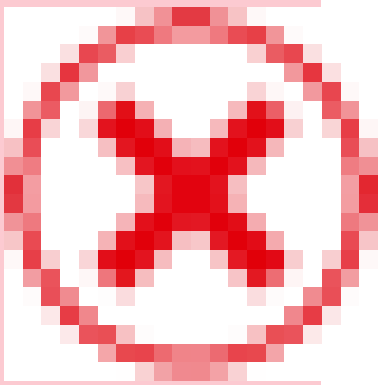
モジュールアクセス：
sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_approval_rules、sn_vu

その他のロールの情報：

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

sn_vulc.remediation_owner

(続く)

モジュール	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vulc.m
修復ターゲットルール					
重要度マッピング					
通知					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

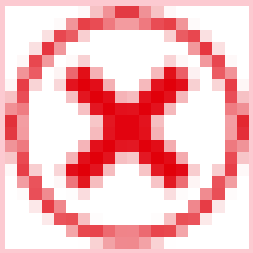
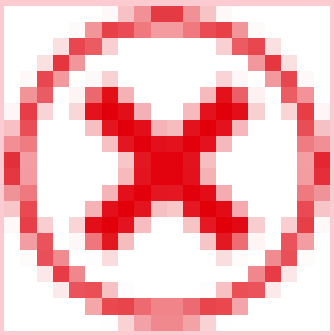
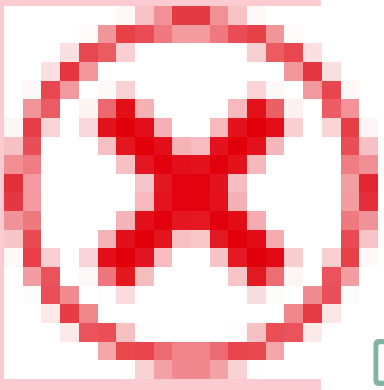
モジュールアクセス：
sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_approval_rules、sn_vu

その他のロールの情報：

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

sn_vulc.remediation_owner

(続く)

モジュール	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vulc.m
例外管理					

自動翻訳

モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn

モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
(メインアプリグループ)				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

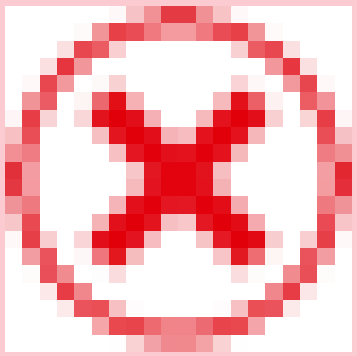
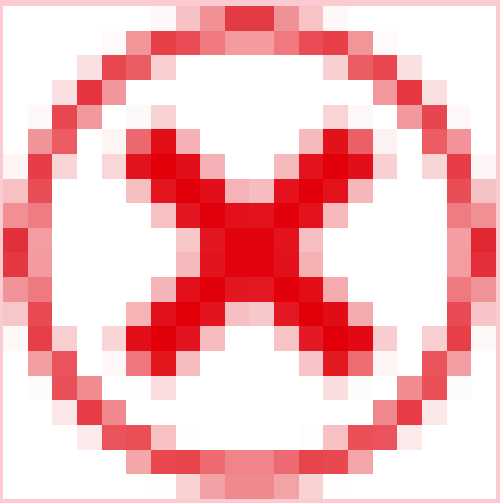
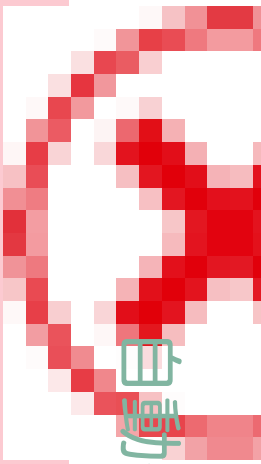
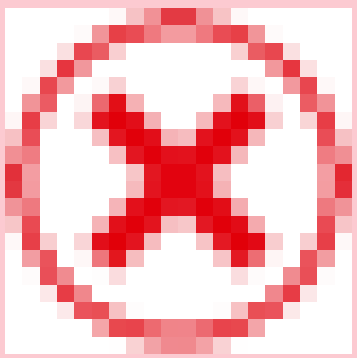
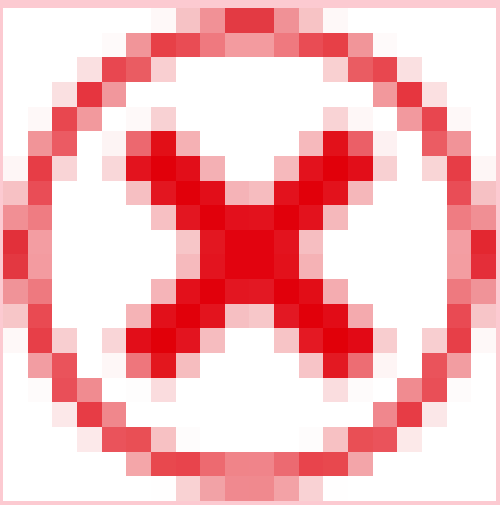
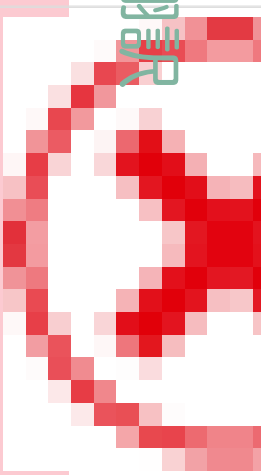
モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

(続く)

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
概要				
ポリシー				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

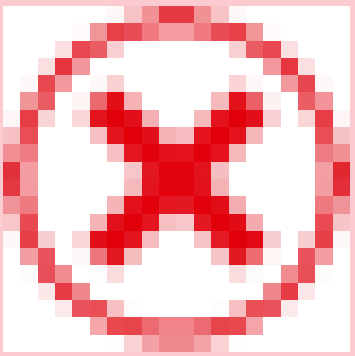
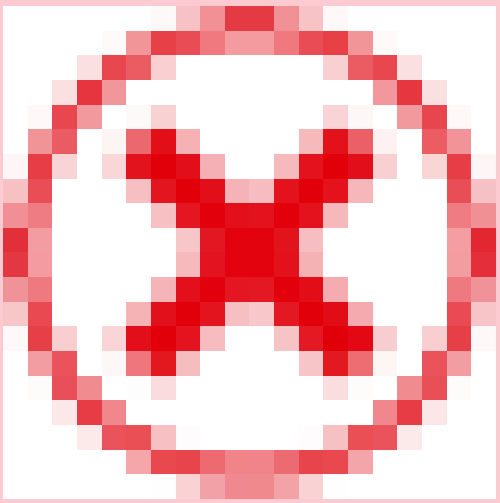
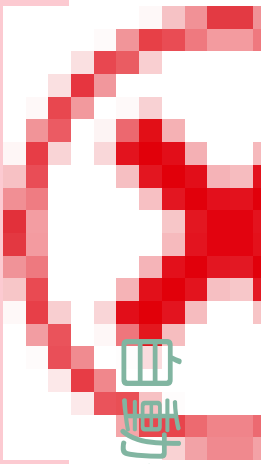
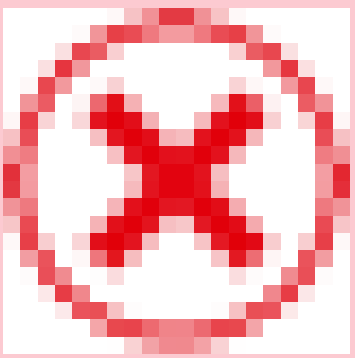
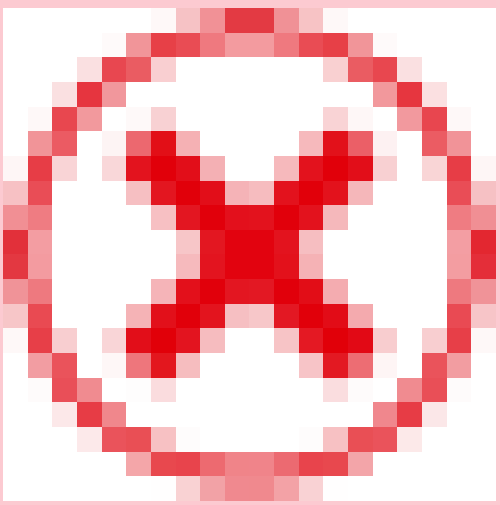
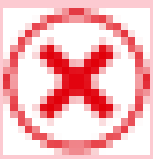
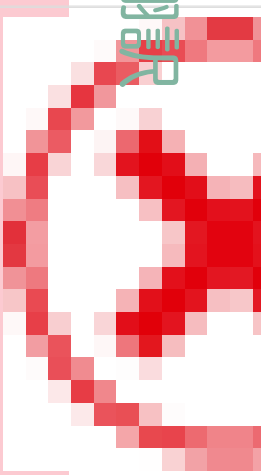
モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

(続く)

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
テスト				
自分の承認				

テスト結果

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

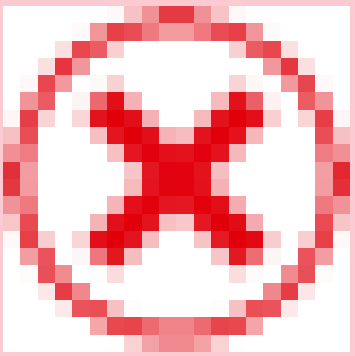
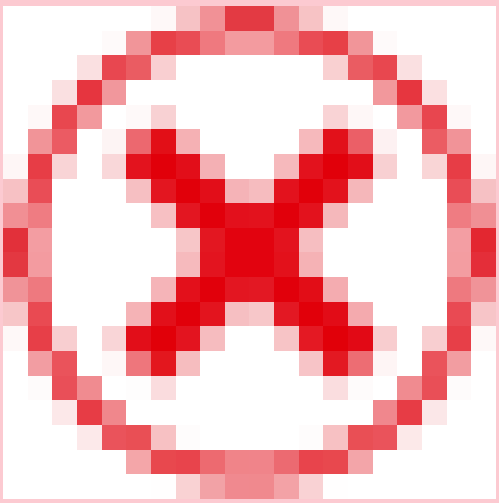
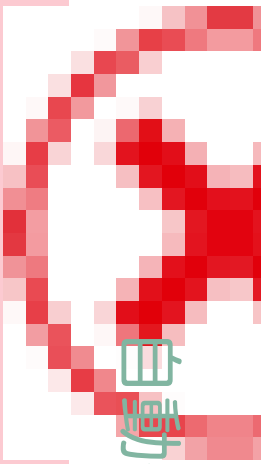
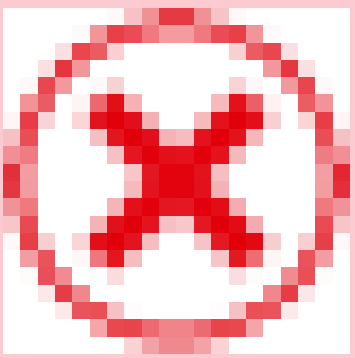
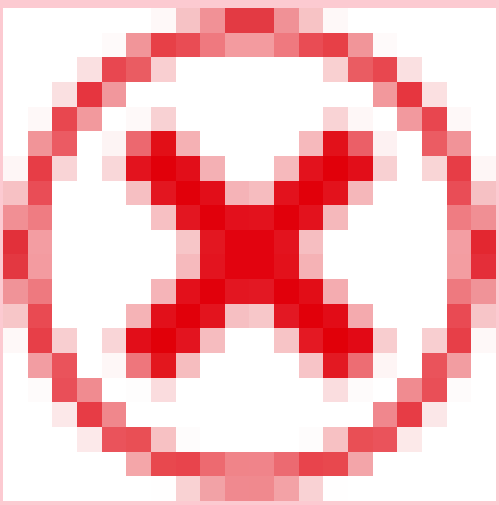
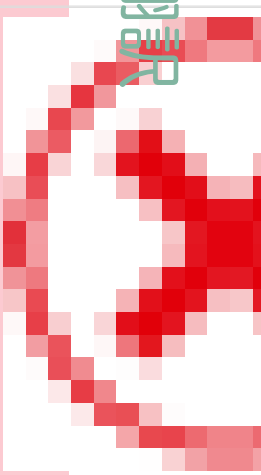
モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

(続く)

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
未トリアージのテスト結果				
自分のオープンなテスト結果				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

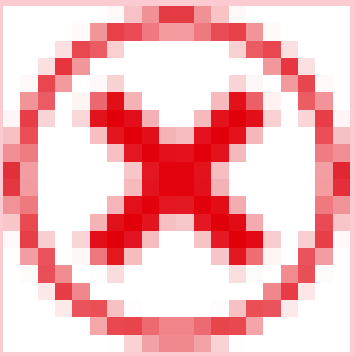
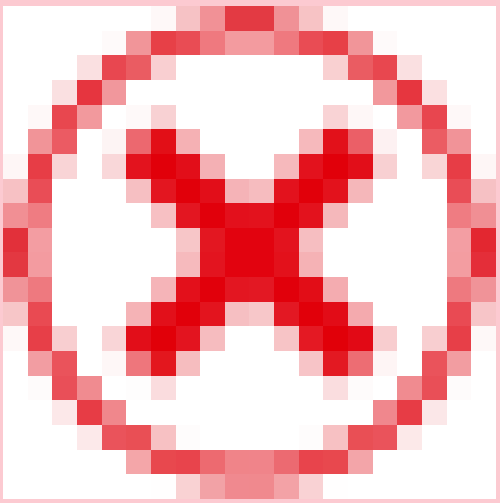
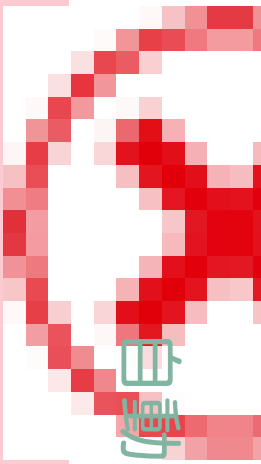
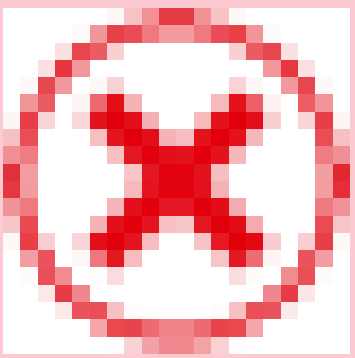
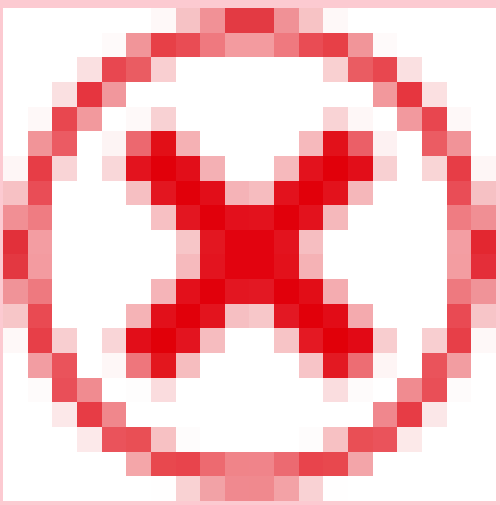
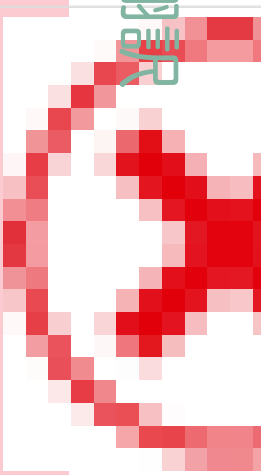
モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

(続く)

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
テスト結果を開く				
該当 CI 確認中				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

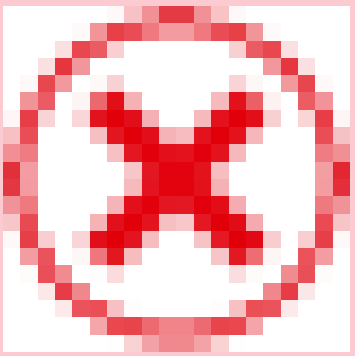
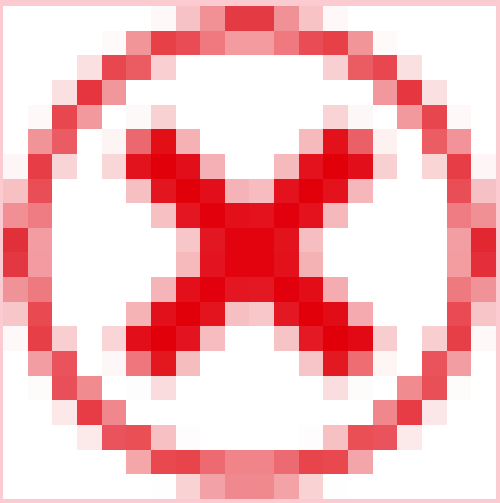
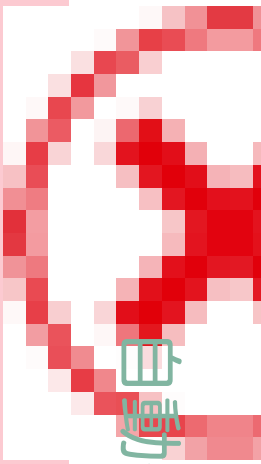
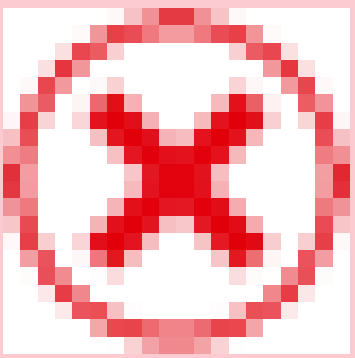
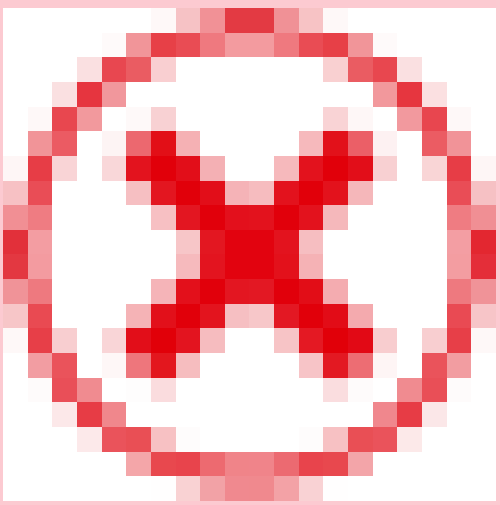
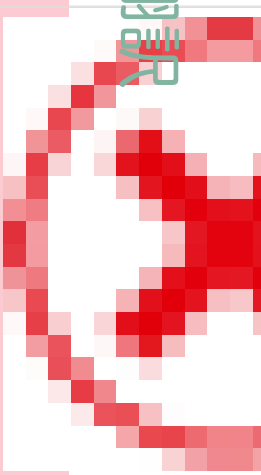
モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

(続く)

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
CI 不明				
未アサイン				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

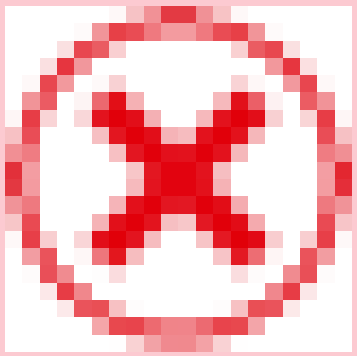
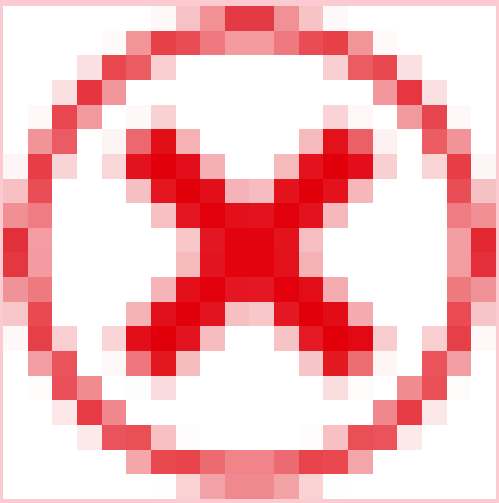
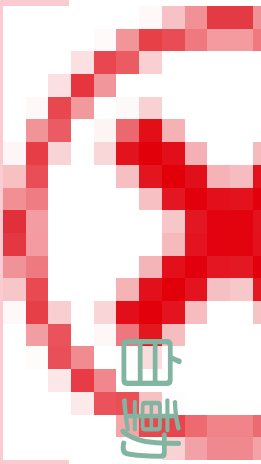
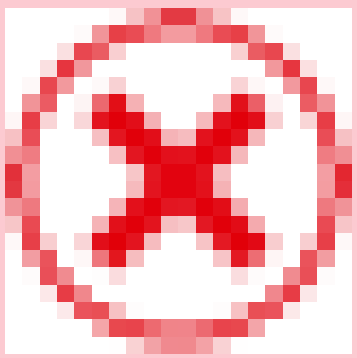
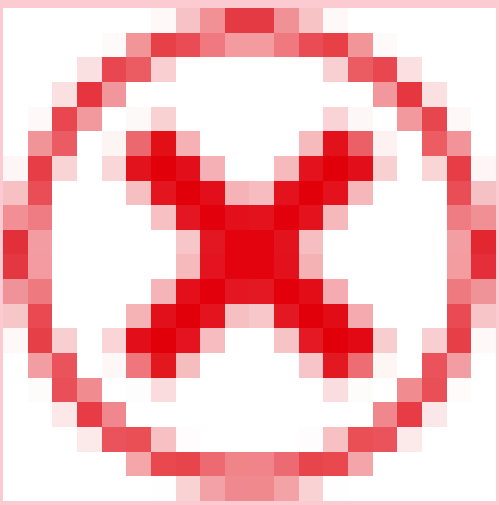
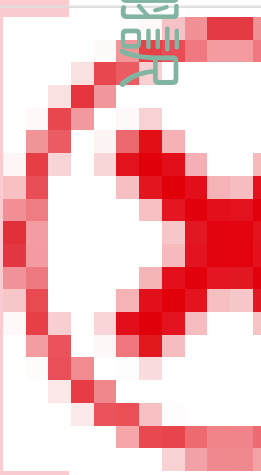
モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

(続く)

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
複数の保留				
すべて				

テスト結果グループ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

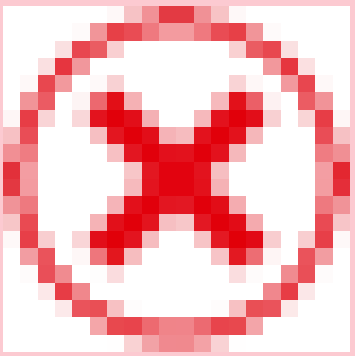
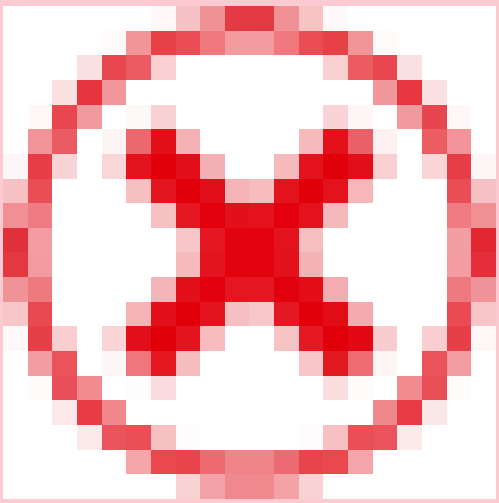
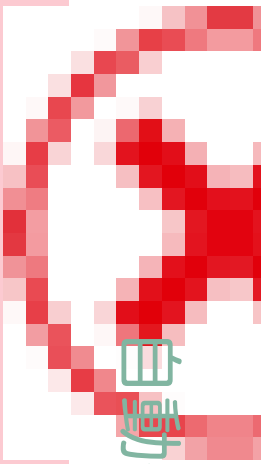
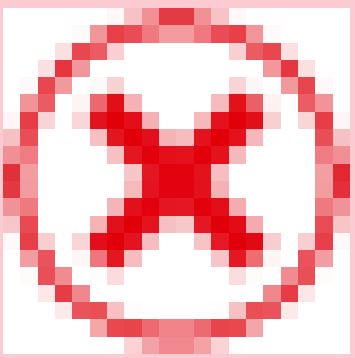
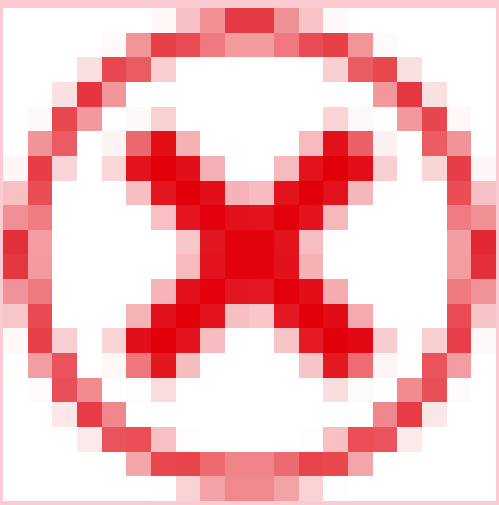
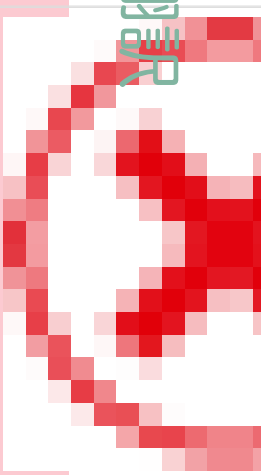
モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

(続く)

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
自分のオープングループ				
すべてのオープングループ				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

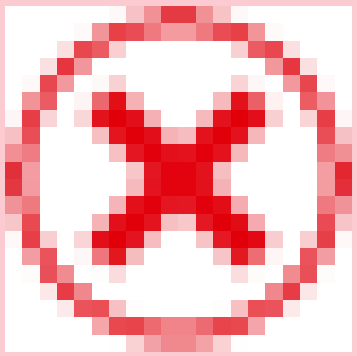
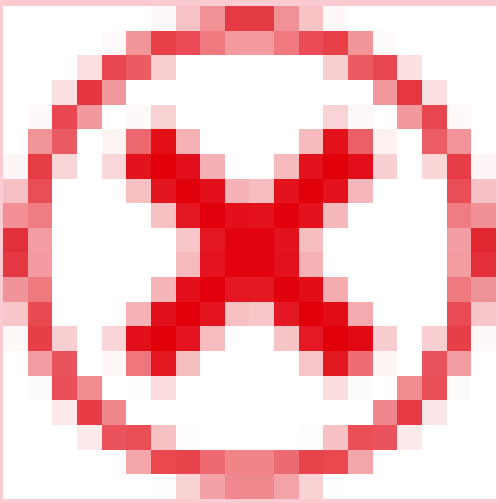
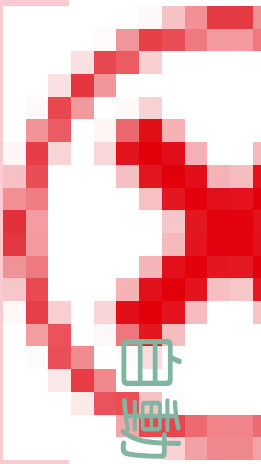
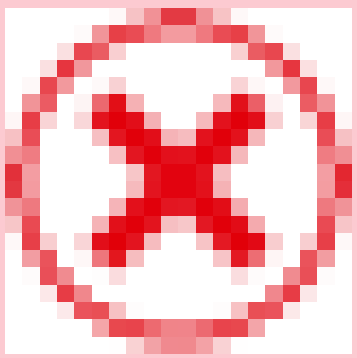
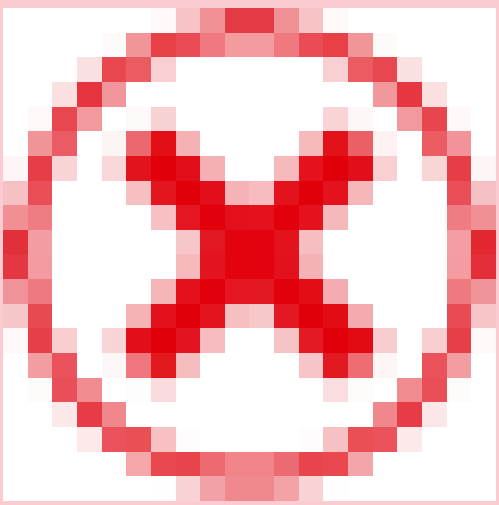
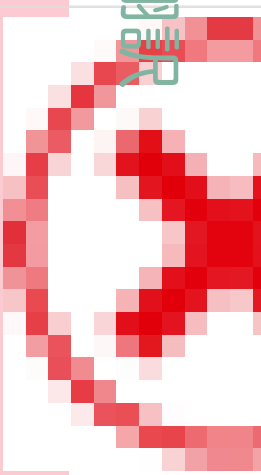
モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

(続く)

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
複数の保留				
すべてのグループ				

提出データ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

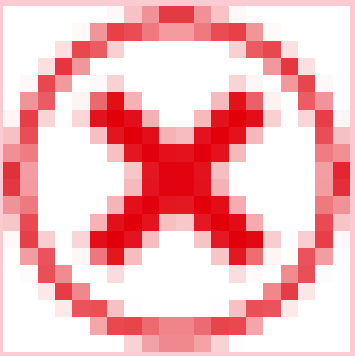
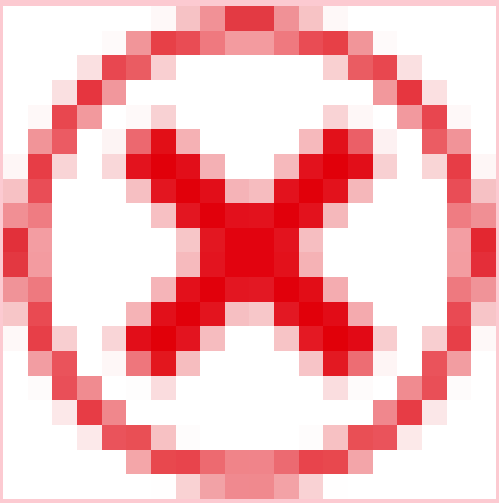
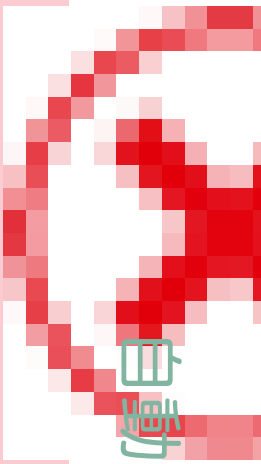
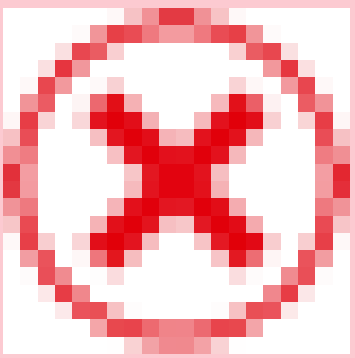
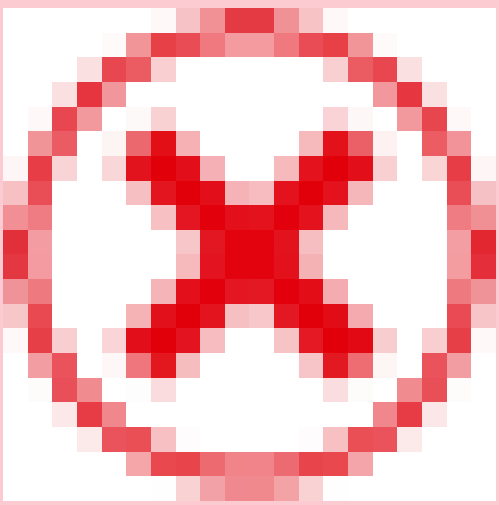
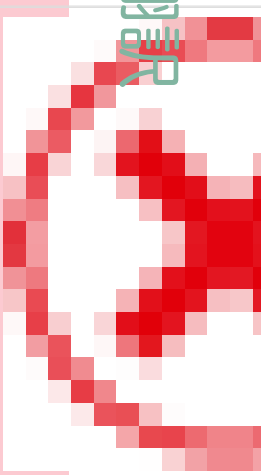
モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

(続く)

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
信頼できるソース				
テクノロジー				
管理				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

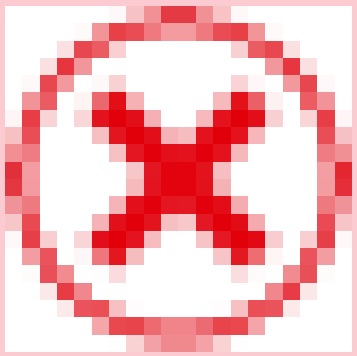
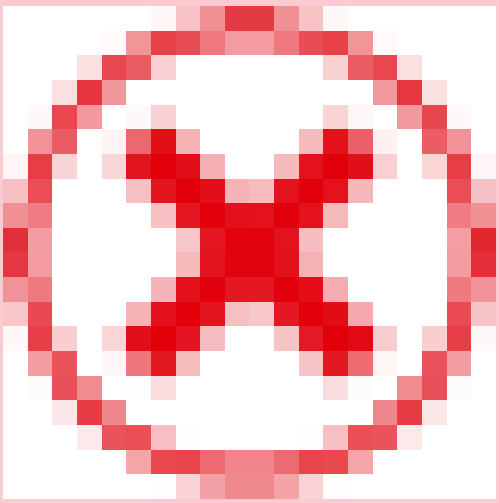
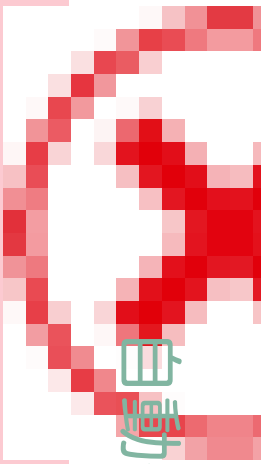
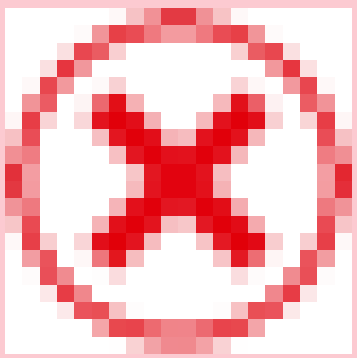
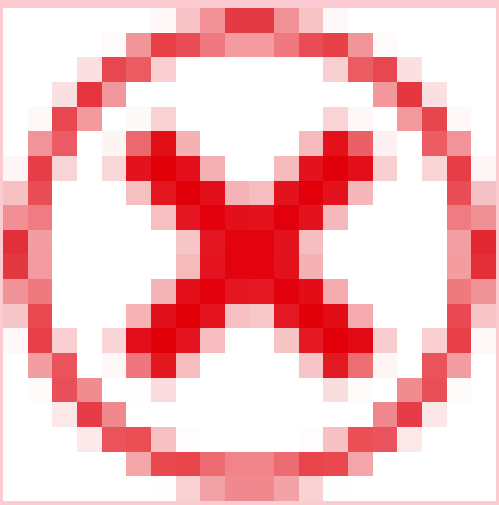
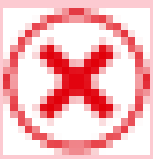
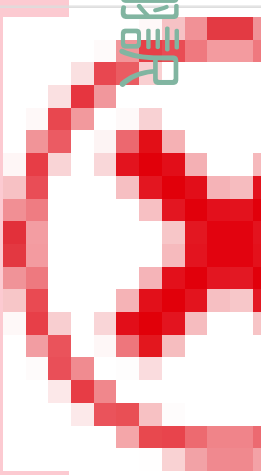
モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

(続く)

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
アサインルール				
古いテスト結果の自動クローズ				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

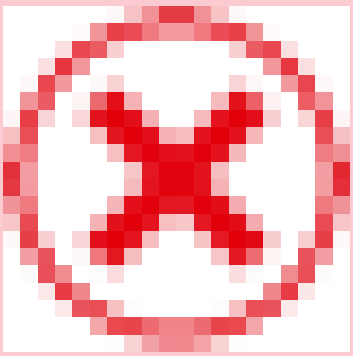
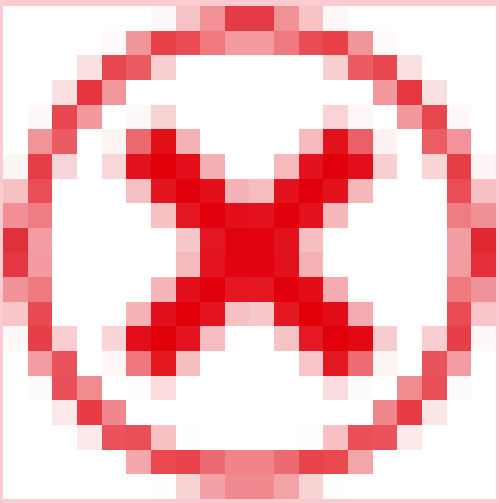
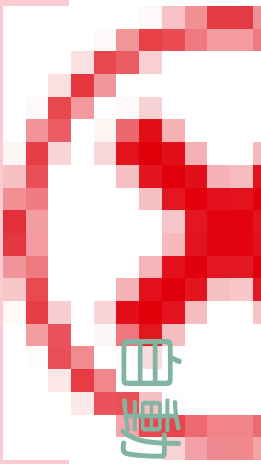
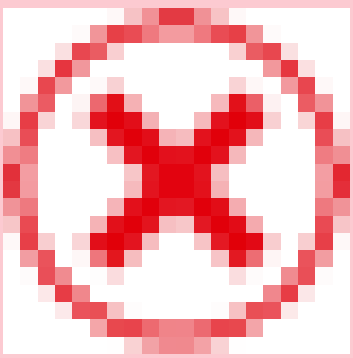
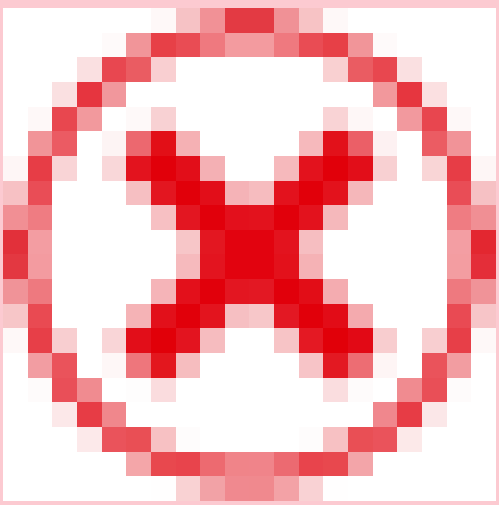
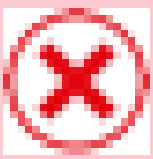
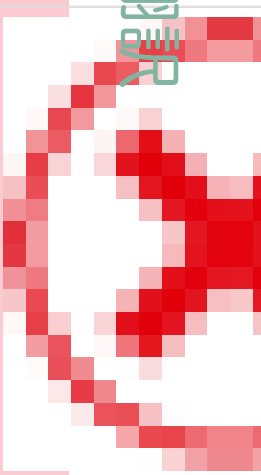
モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

(続く)

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
グループルール				
自動例外ルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

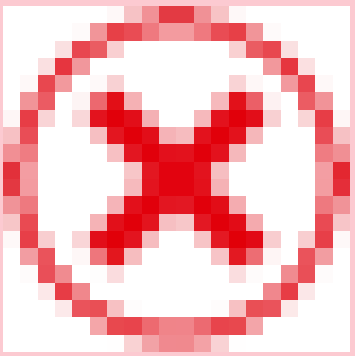
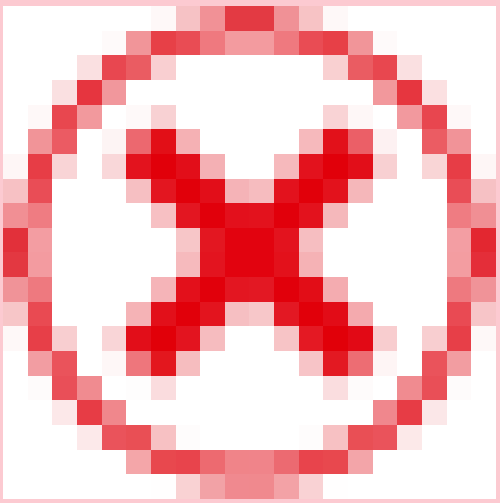
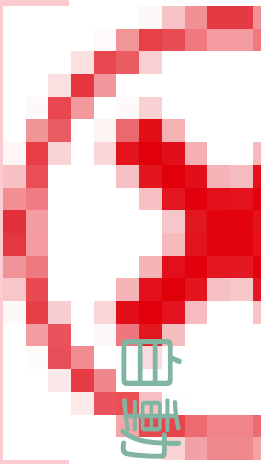
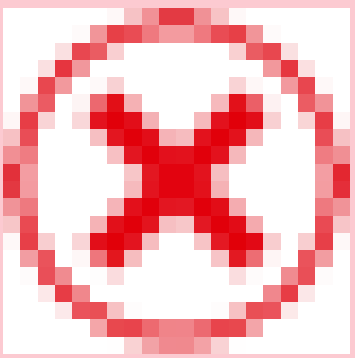
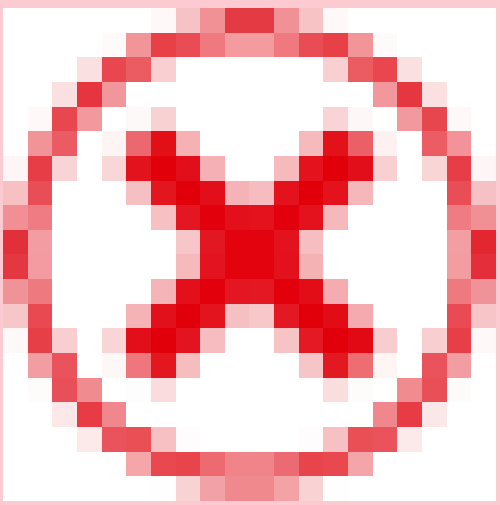
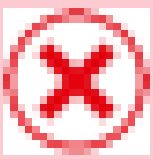
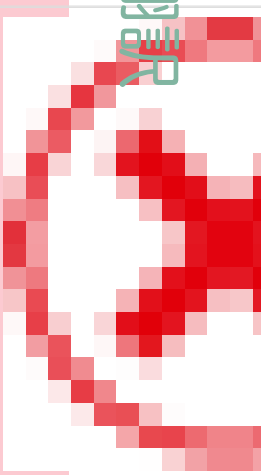
モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

(続く)

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
承認ルール				
リスク算出				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

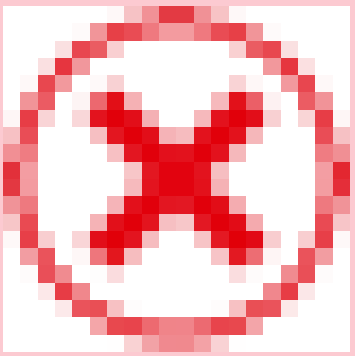
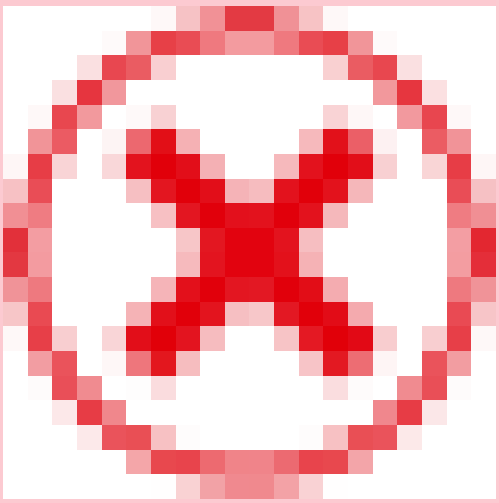
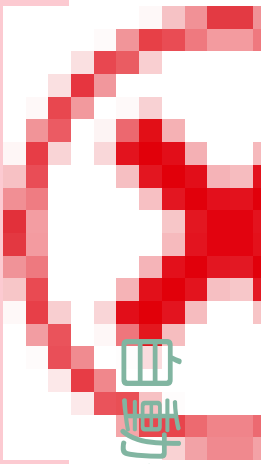
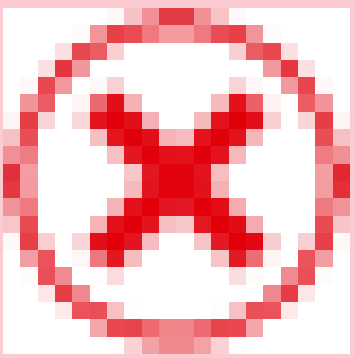
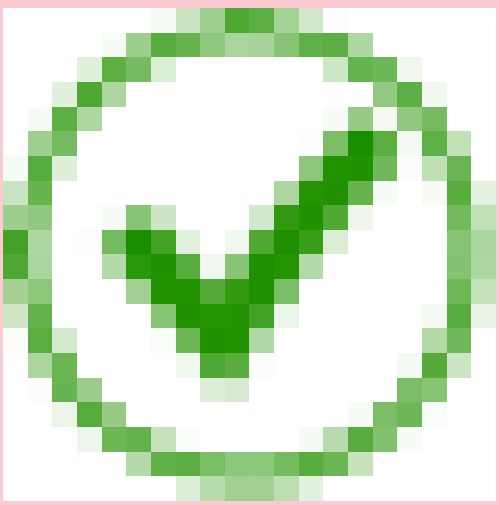
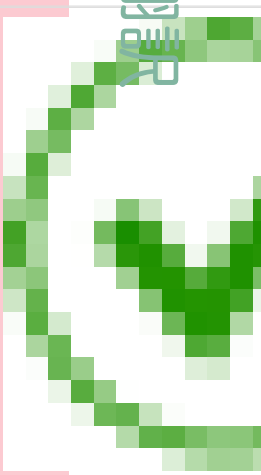
モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

(続く)

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
リスクスコアロールアップ算出				
修復ターゲットルール				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

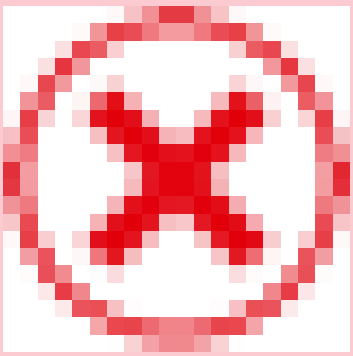
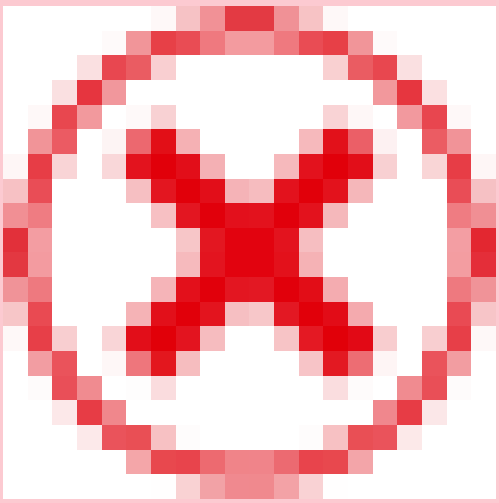
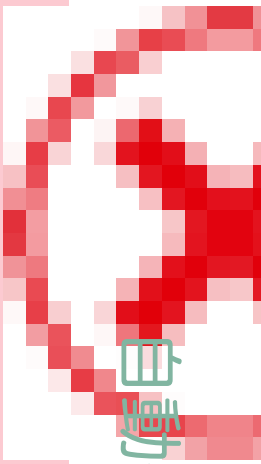
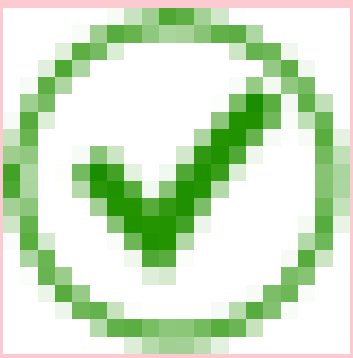
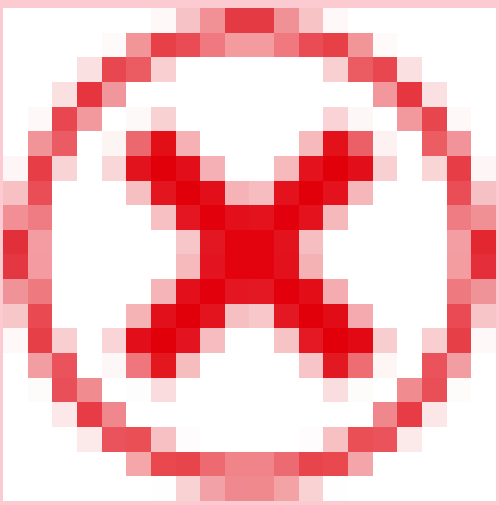
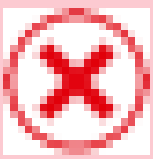
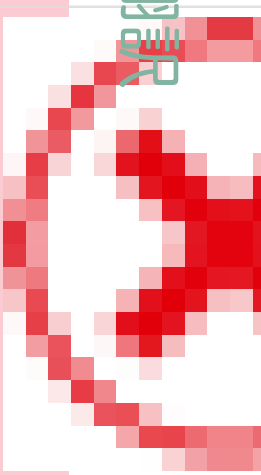
モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

(続く)

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
重要度マッピング				
通知				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

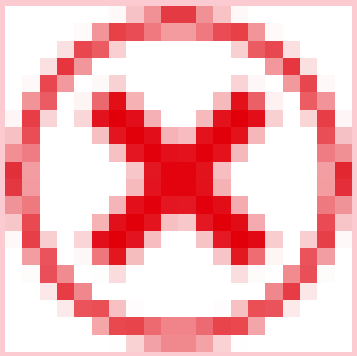
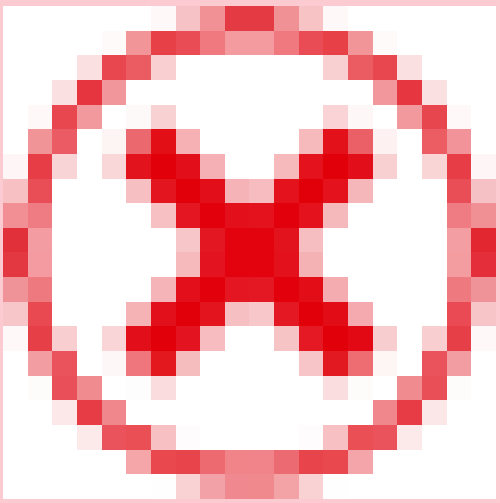
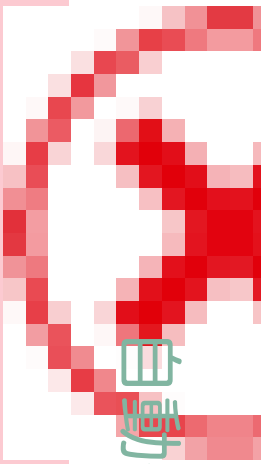
モジュールアクセス：
sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、sn_vulc.read_rem

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.remediation_owner

(続く)

モジュール	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read_remedia
例外管理				

モジュールアクセス：**sn_vulc.remediation_owner**

モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

モジュール	sn_vulc.remediation_owner
(メインアプリグループ)	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

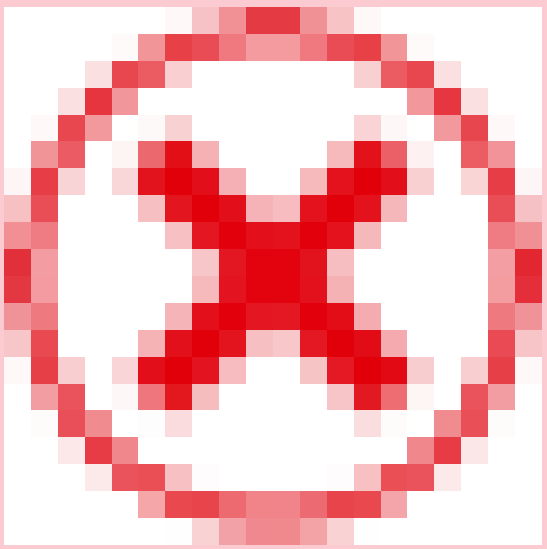
モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

(続く)

モジュール	sn_vulc.remediation_owner
概要	
ポリシー	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

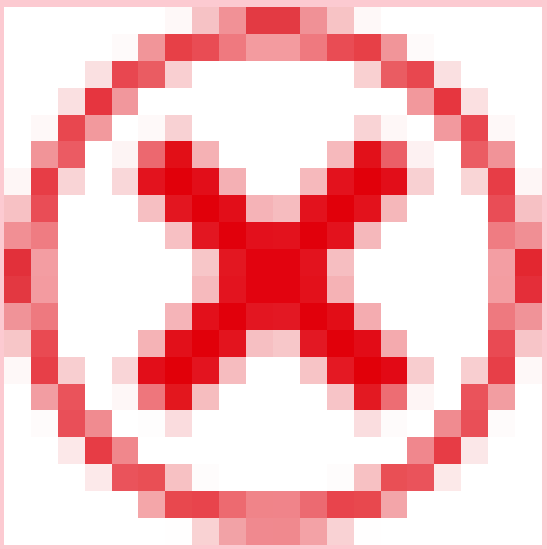
モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

(続く)

モジュール	sn_vulc.remediation_owner
テスト	
自分の承認	
テスト結果	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

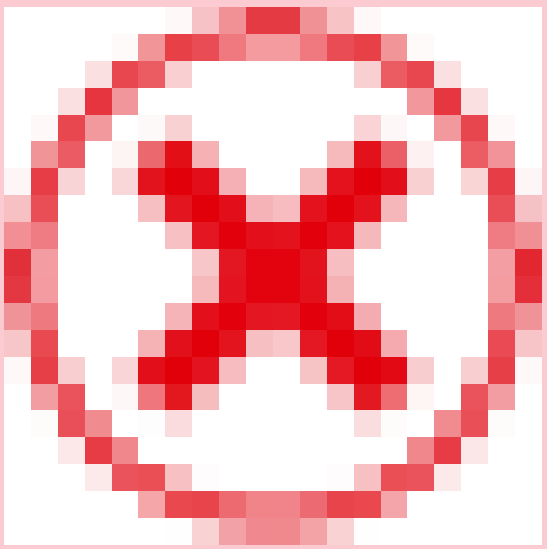
モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

(続く)

モジュール	sn_vulc.remediation_owner
未トリアージのテスト結果	
自分のオープンなテスト結果	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

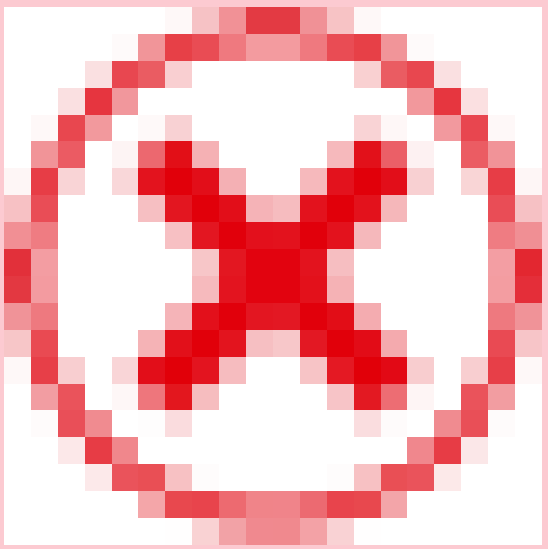
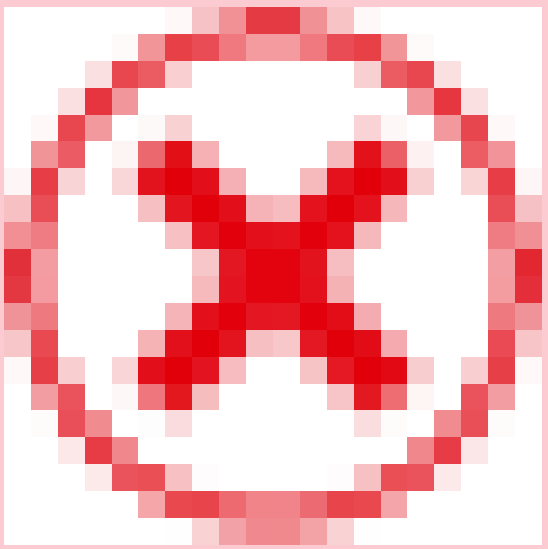
モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

(続く)

モジュール	sn_vulc.remediation_owner
テスト結果を開く	
該当 CI 確認中	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

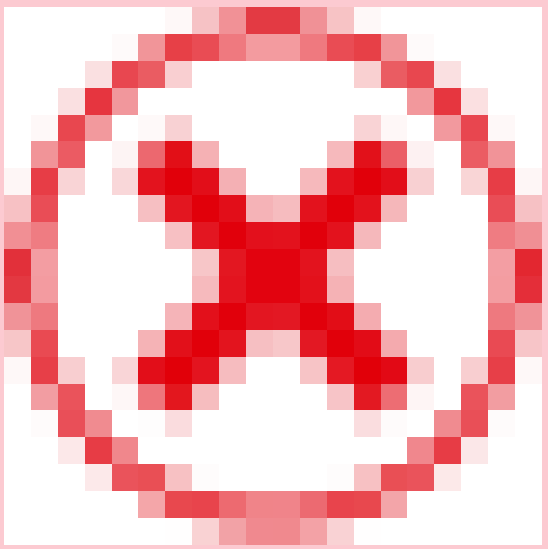
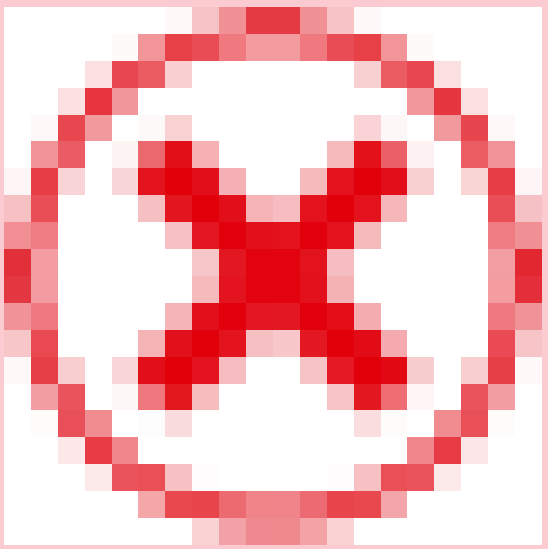
モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

(続く)

モジュール	sn_vulc.remediation_owner
CI 不明	
未アサイン	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

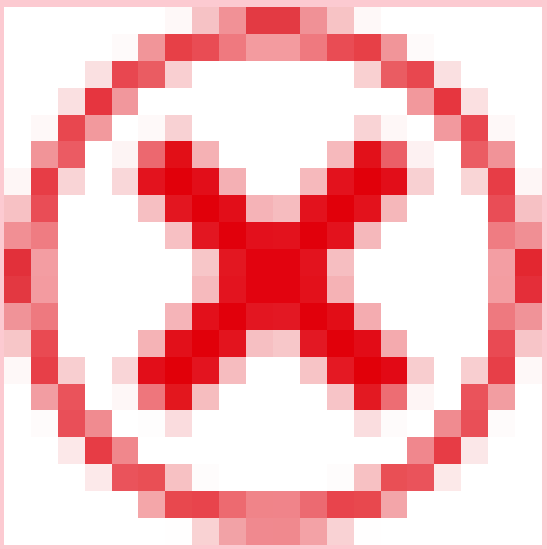
モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

(続く)

モジュール	sn_vulc.remediation_owner
複数の保留	
すべて	
テスト結果グループ	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

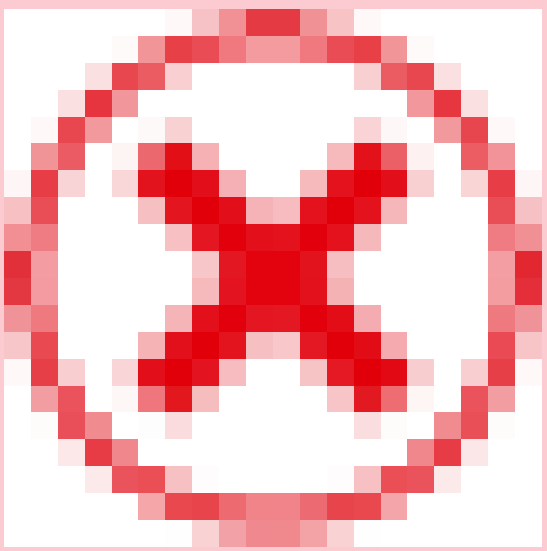
モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

(続く)

モジュール	sn_vulc.remediation_owner
自分のオープングループ	
すべてのオープングループ	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

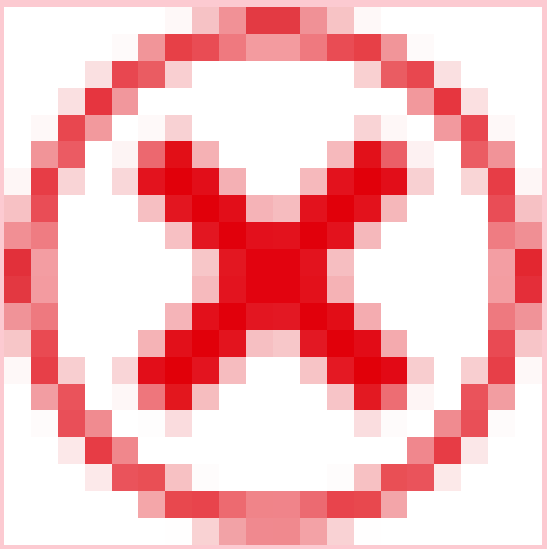
モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

(続く)

モジュール	sn_vulc.remediation_owner
複数の保留	
すべてのグループ	
提出データ	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

(続く)

モジュール	sn_vulc.remediation_owner
信頼できるソース	
テクノロジー	
管理	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

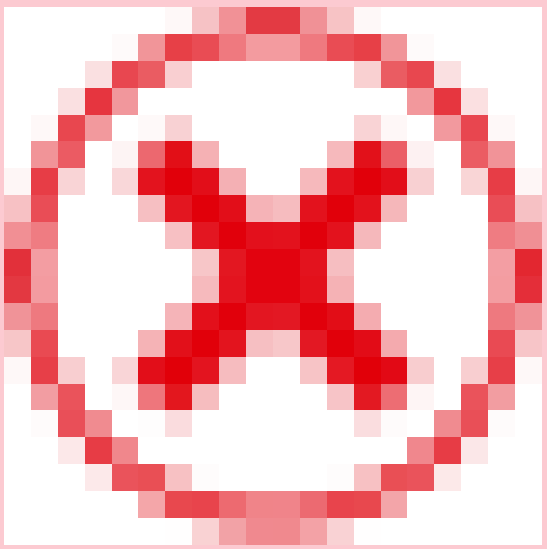
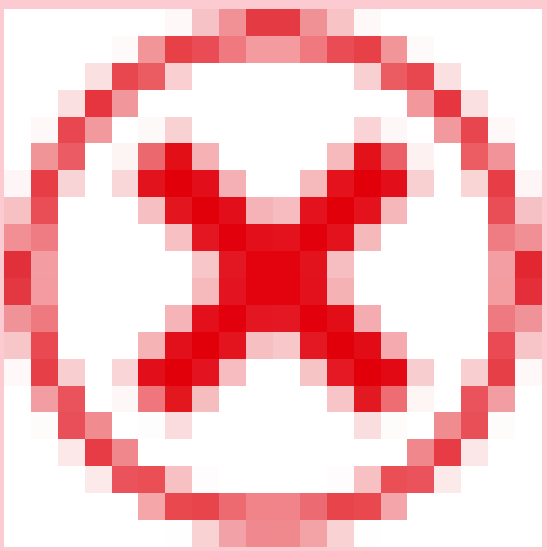
モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

(続く)

モジュール	sn_vulc.remediation_owner
アサインルール	
古いテスト結果の自動クローズ	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

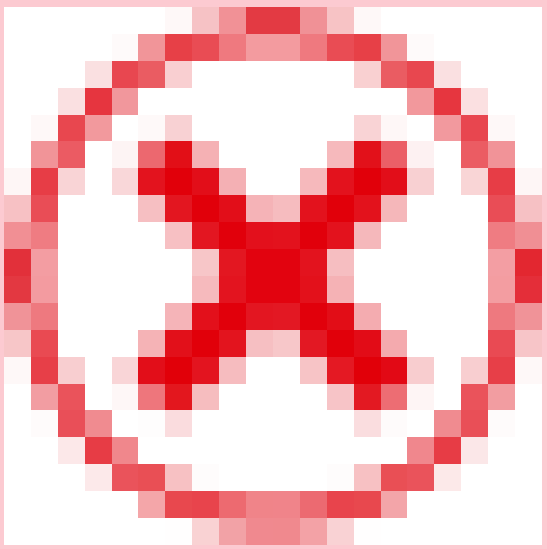
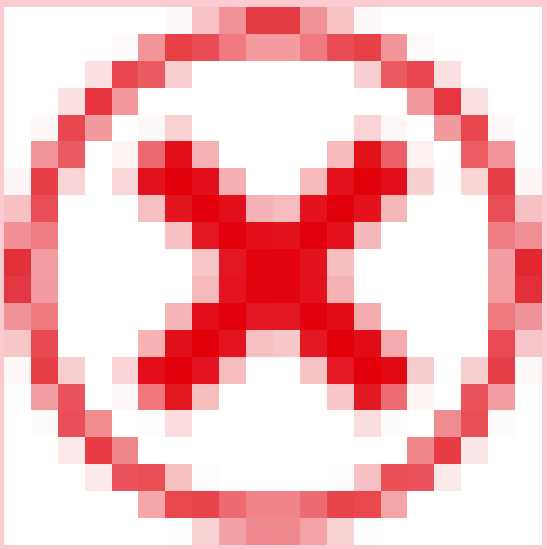
モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

(続く)

モジュール	sn_vulc.remediation_owner
グループルール	
自動例外ルール	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

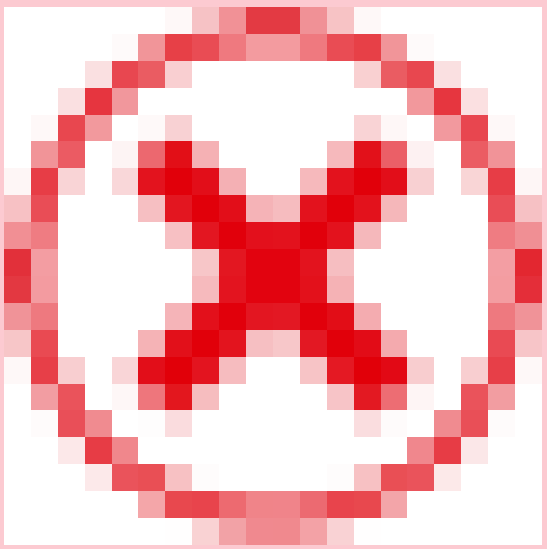
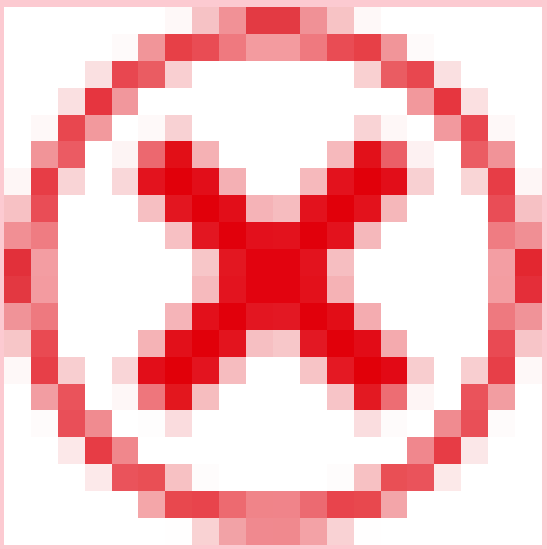
モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

(続く)

モジュール	sn_vulc.remediation_owner
承認ルール	
リスク算出	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

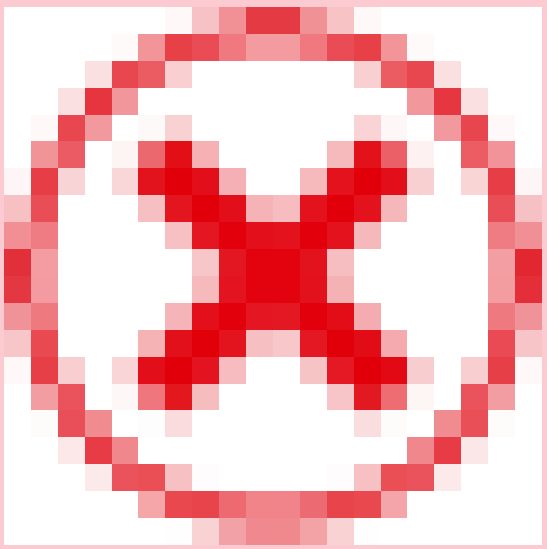
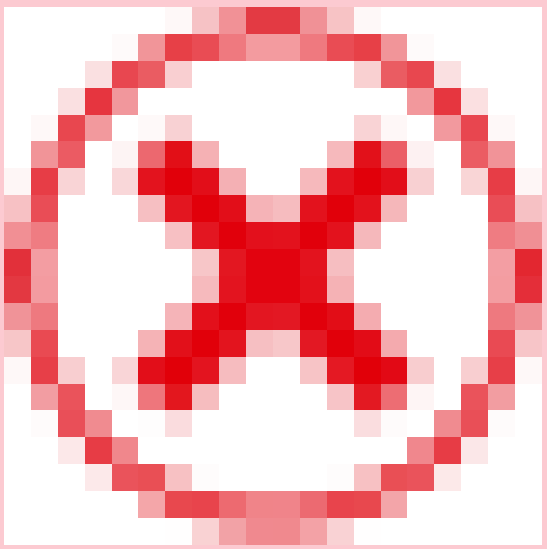
モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

(続く)

モジュール	sn_vulc.remediation_owner
リスクスコアロールアップ算出	
修復ターゲットルール	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

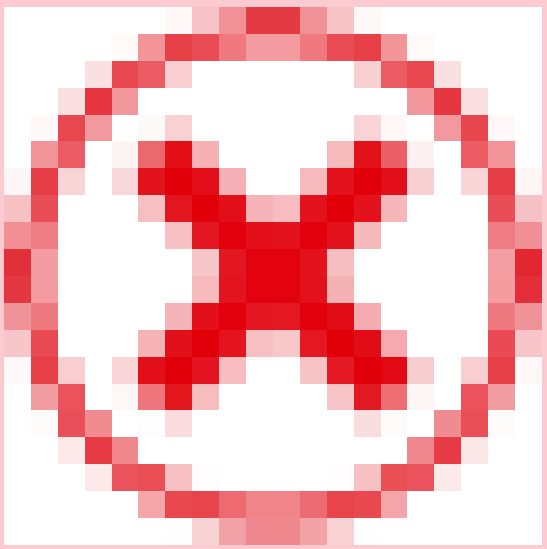
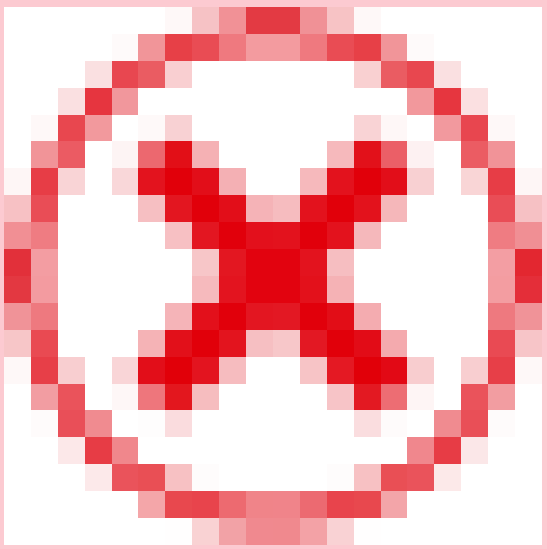
モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

(続く)

モジュール	sn_vulc.remediation_owner
重要度マッピング	
通知	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

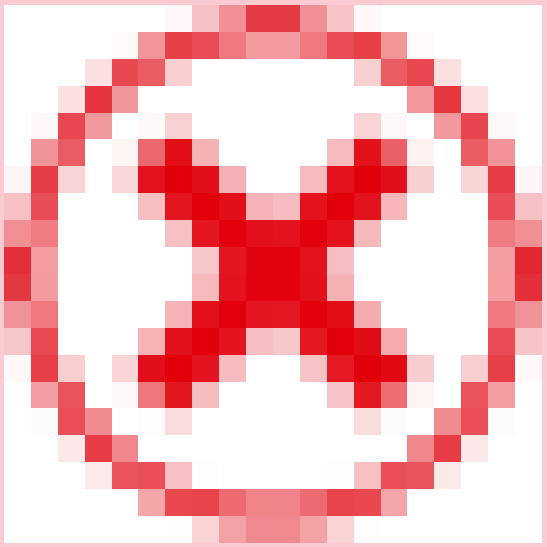
モジュールアクセス：**sn_vulc.remediation_owner**

その他のロールの情報：

sn_vul_qualys.admin、sn_vulc.admin、sn_vulc.exception_approver、sn_vulc.manage_app

sn_vulc.manage_notifications、sn_vulc.manage_remediation_target_rules、sn_vulc.read、

(続く)

モジュール	sn_vulc.remediation_owner
例外管理	

[End]

[store-future: BEGIN review]

コンテナ脆弱性対応のロール別のモジュールアクセス

コンテナ脆弱性対応では、特定のロールがアクセスできるメニューアイテムが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_conta

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_container.configure

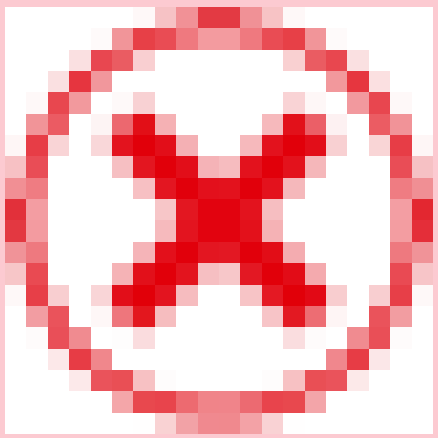
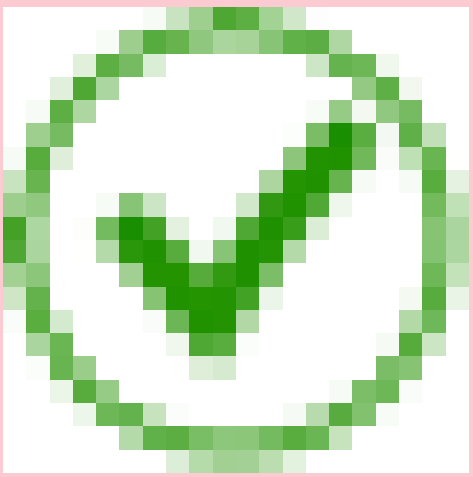
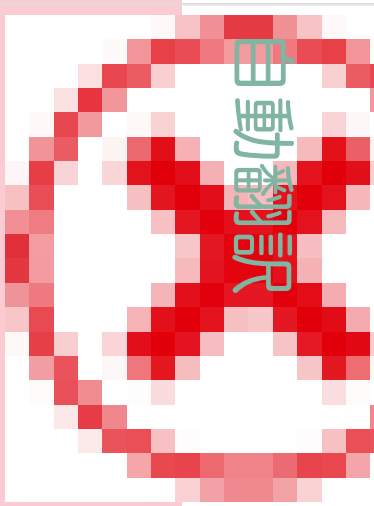
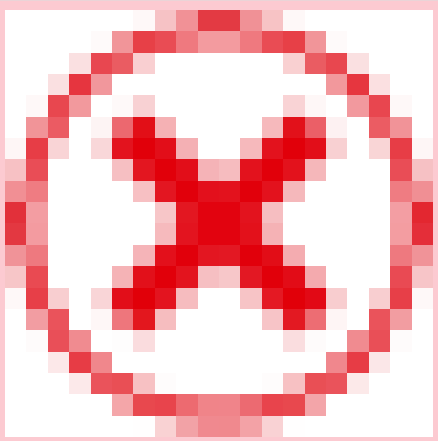
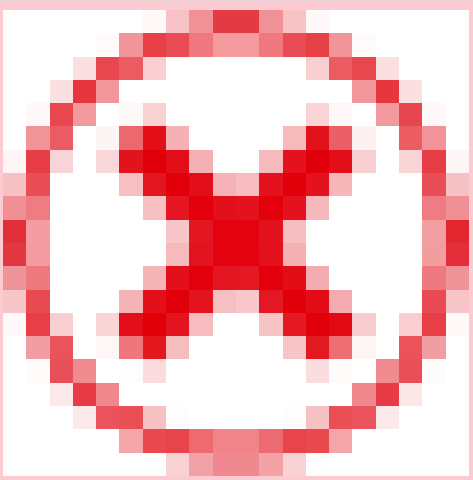
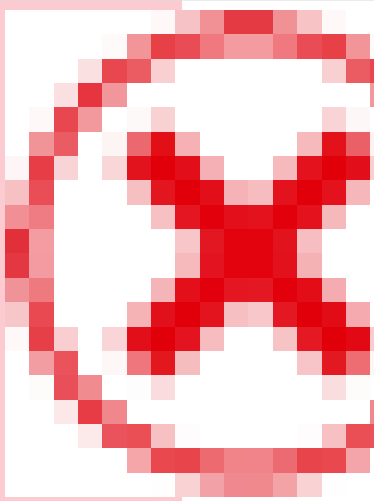
その他のロールの情報：

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_vi_s
(メインアプリグループ)			
概要			
自分の承認			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_container.configure

その他のロールの情報：

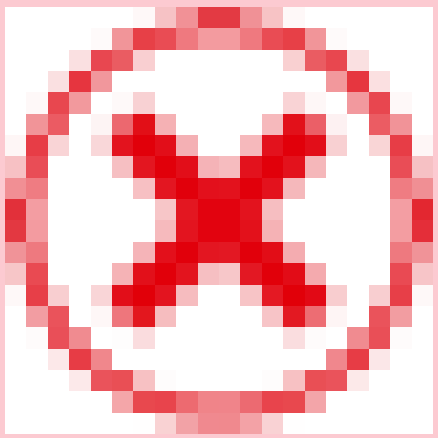
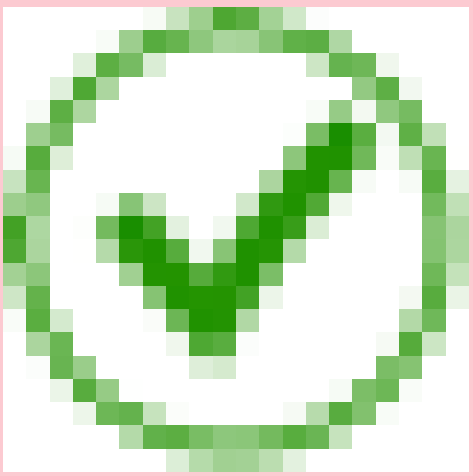
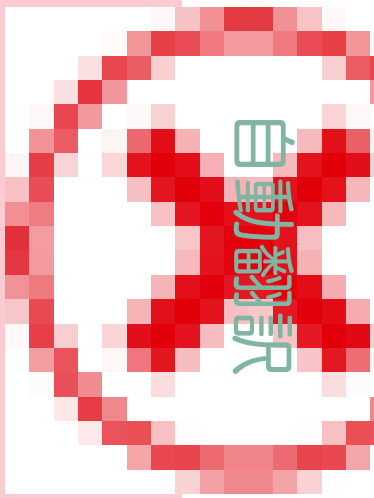
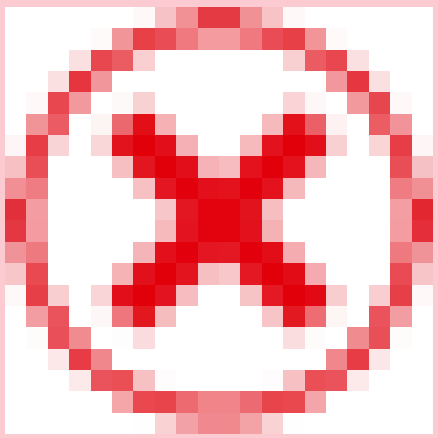
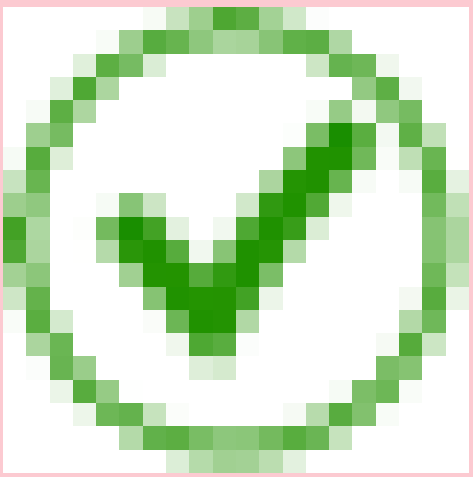
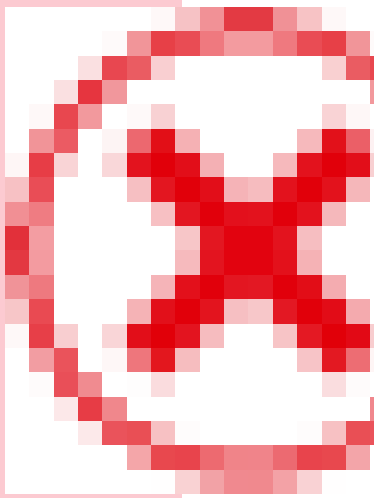
sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_vi_g
コンテナ脆弱性一致アイテム			
自分にアサイン済み			
所属グループにアサイン済み			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_container.configure

その他のロールの情報：

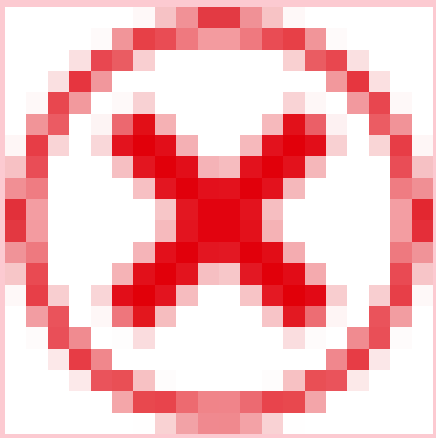
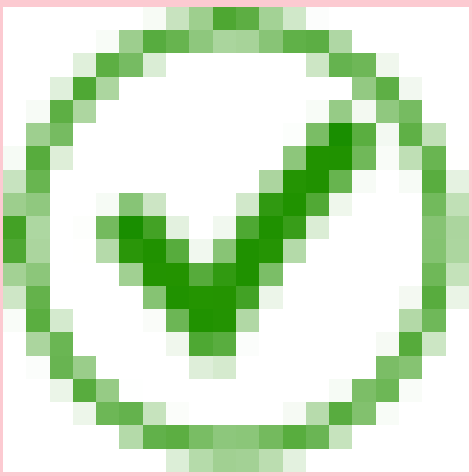
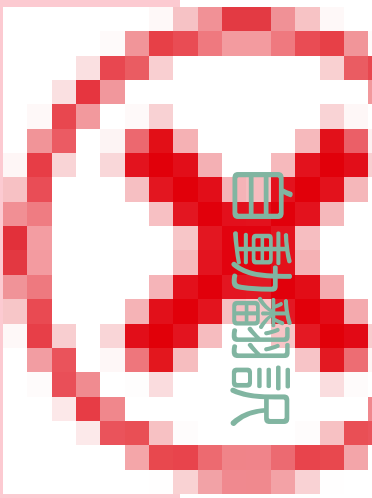
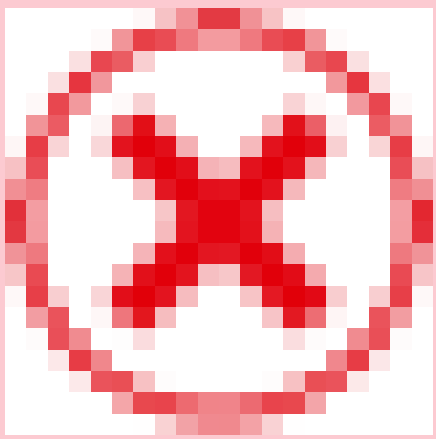
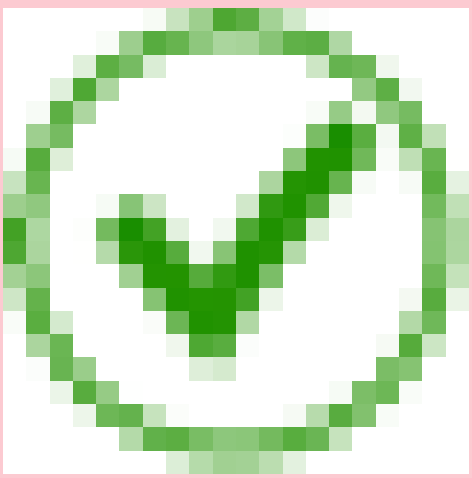
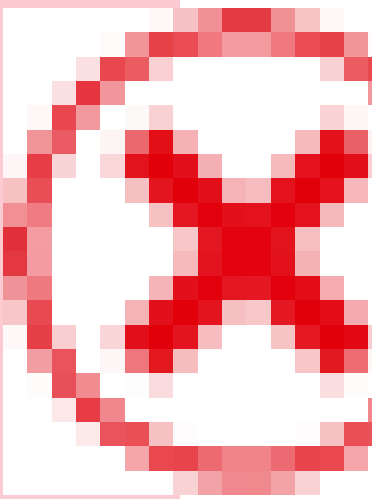
sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_vi_g
重大および高リスク			
エクスプロイト可能			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_container.configure

その他のロールの情報：

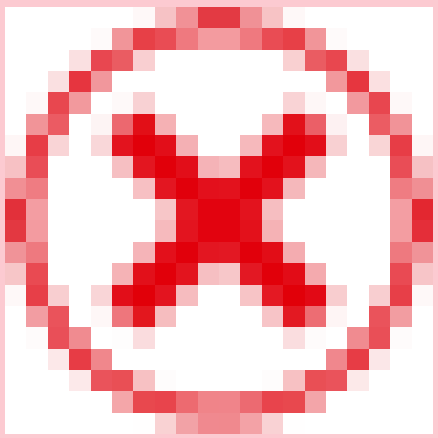
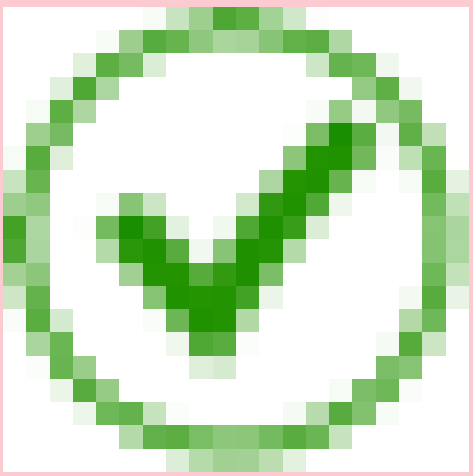
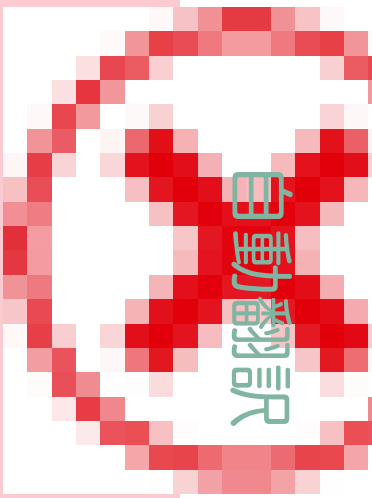
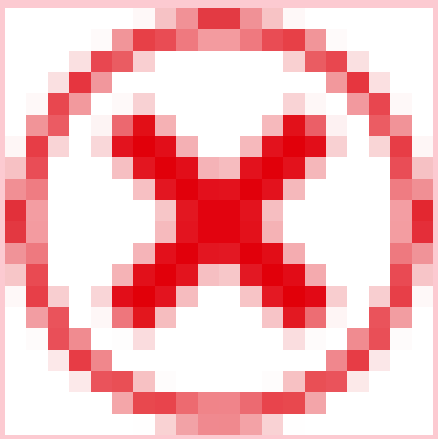
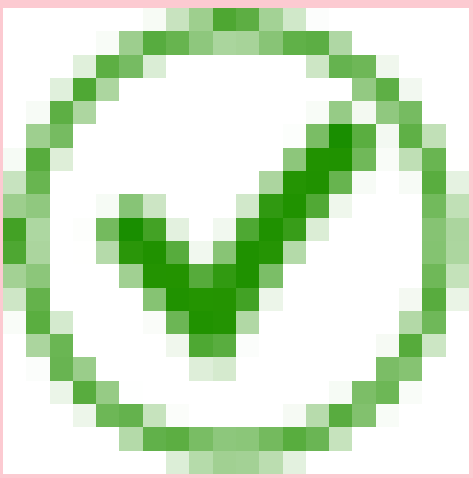
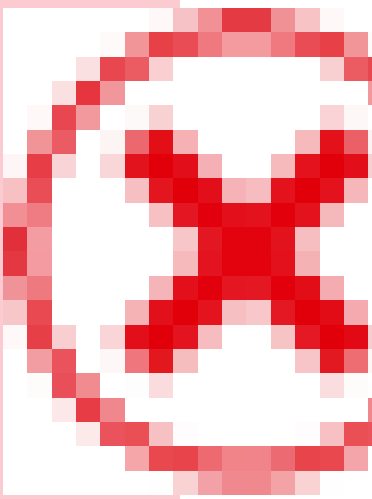
sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_vi_g
該当 CI 確認中			
CI 不明			

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_container.configure

その他のロールの情報：

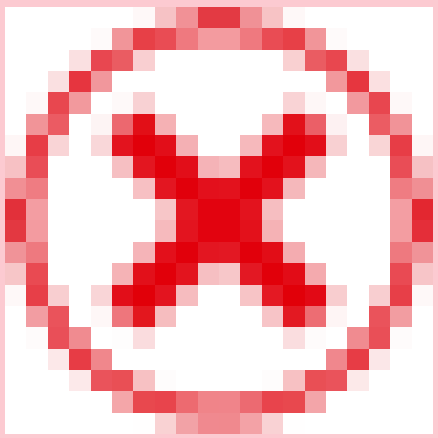
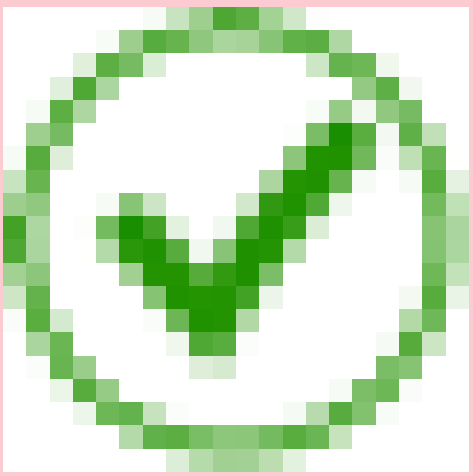
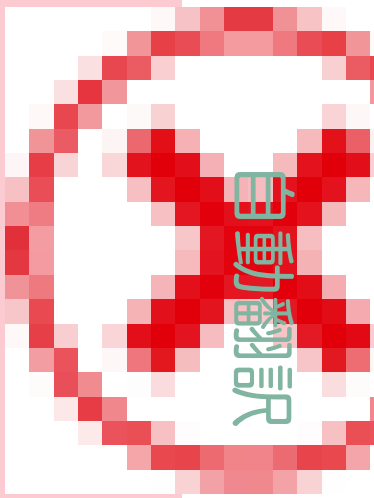
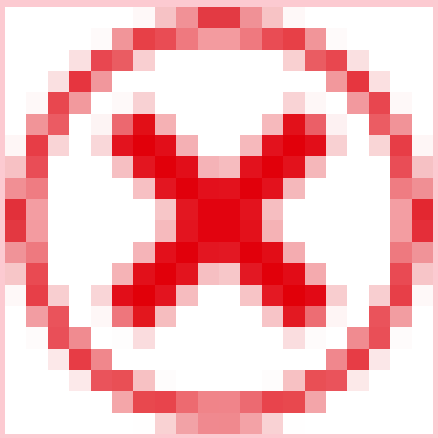
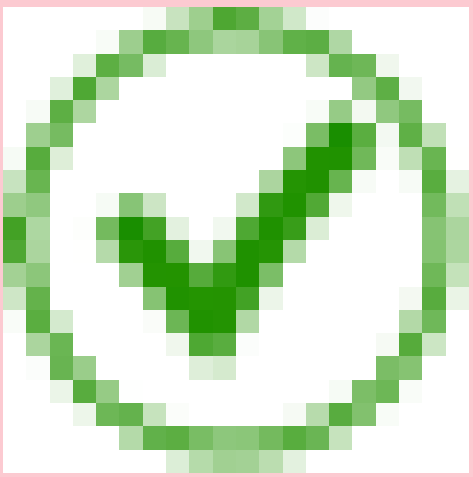
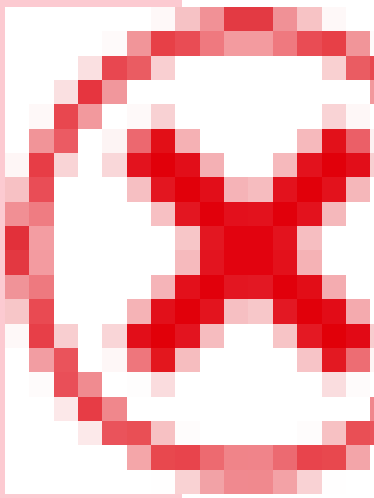
sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_vi_g
すべて			
ライブラリ			
NVD			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_container.configure

その他のロールの情報：

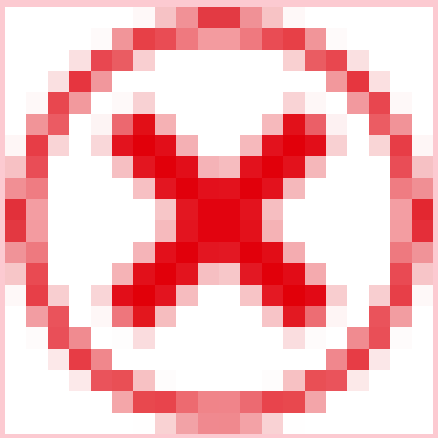
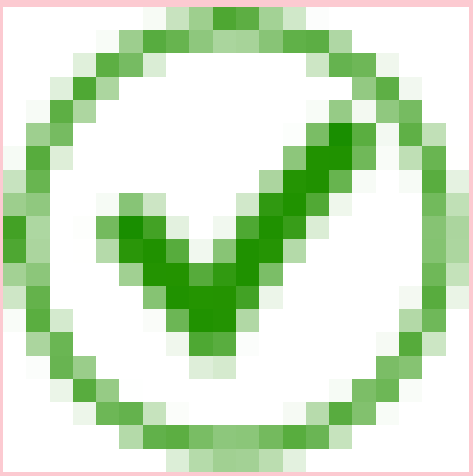
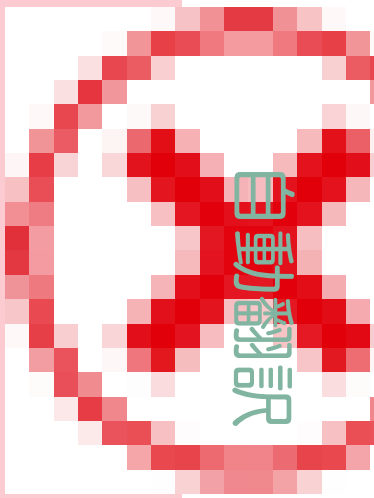
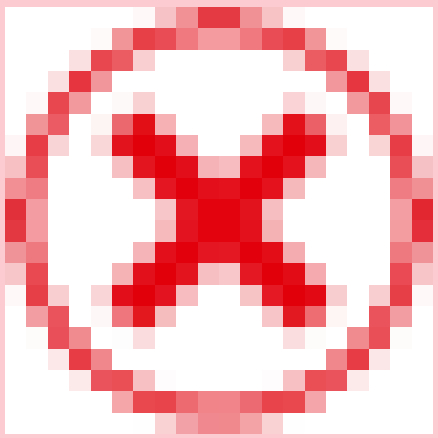
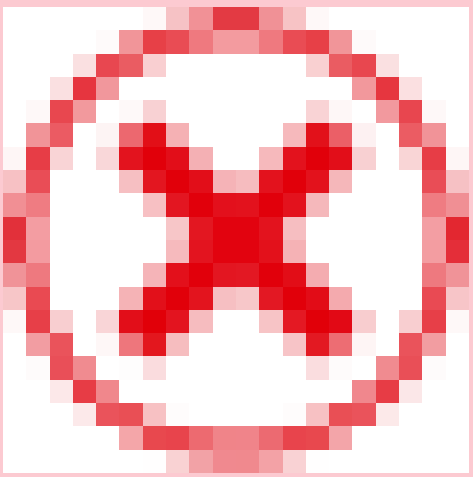
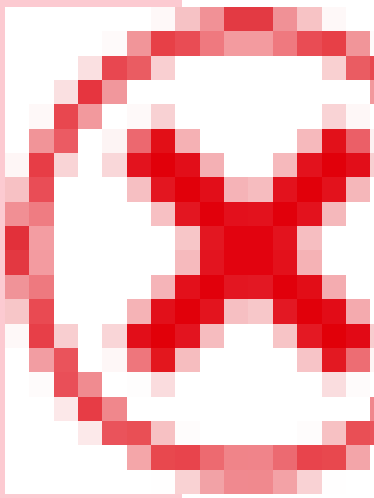
sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_vi_g
サードパーティ			
管理			
アサインルール			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_container.configure

その他のロールの情報：

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_vi_g
脆弱性算出	✗	✗	✗
修復ターゲットルール	✗	✗	✗

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_container.configure

その他のロールの情報：

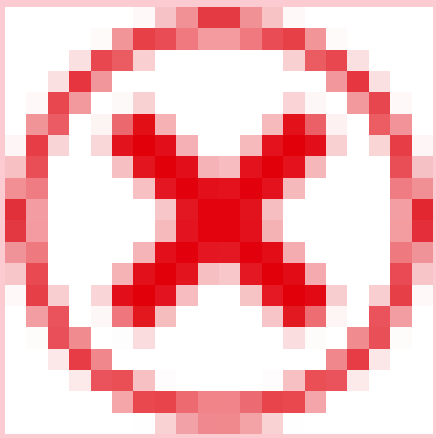
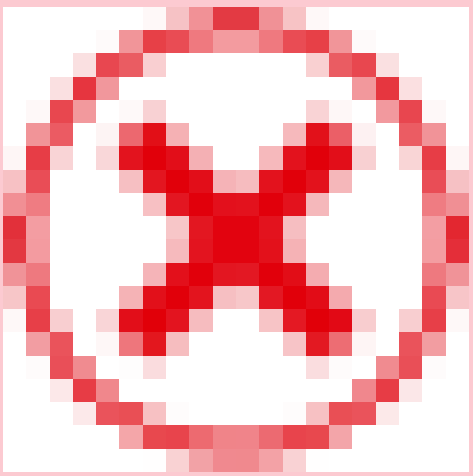
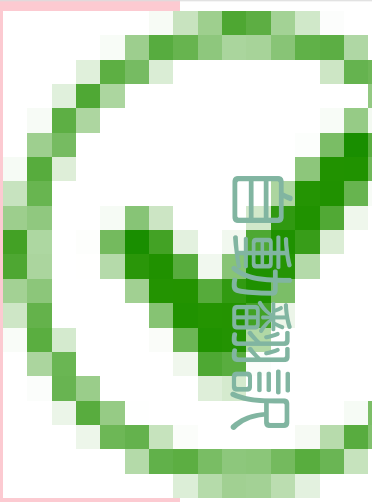
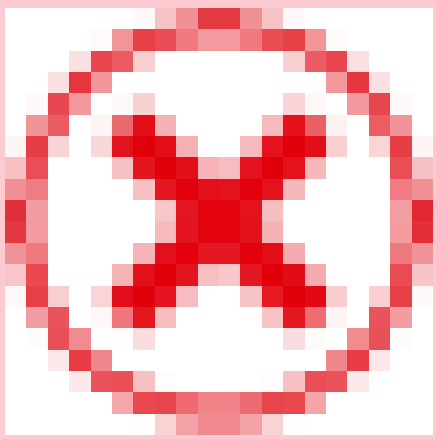
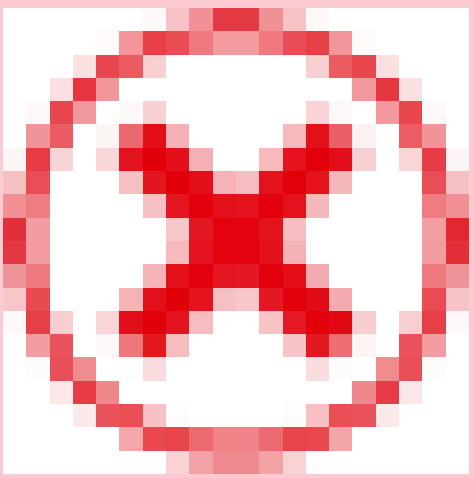
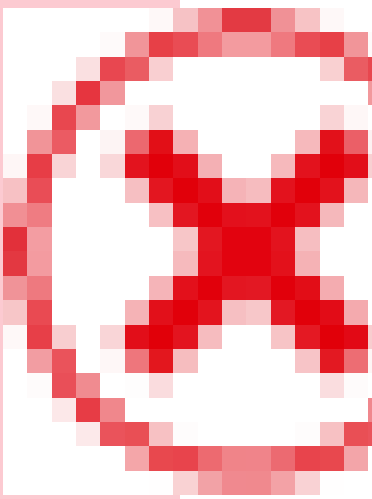
sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_vi_g
VI の粒度の構成			
例外ルール			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_container.configure

その他のロールの情報：

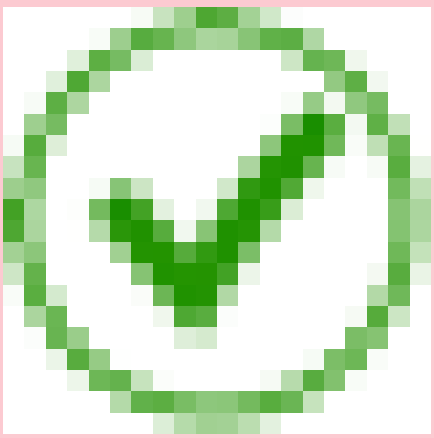
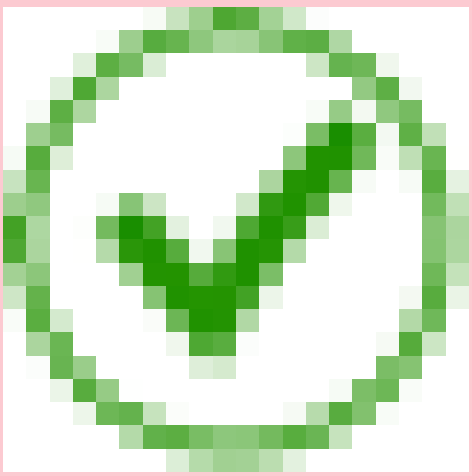
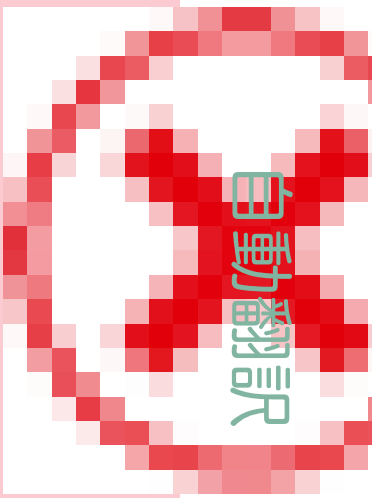
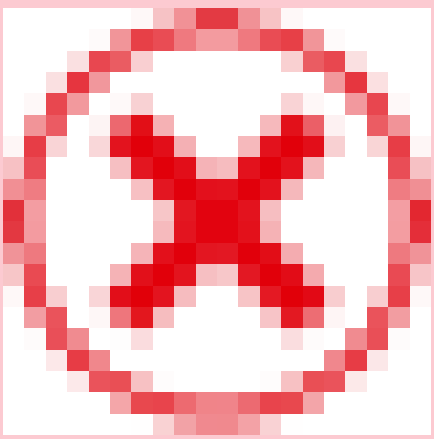
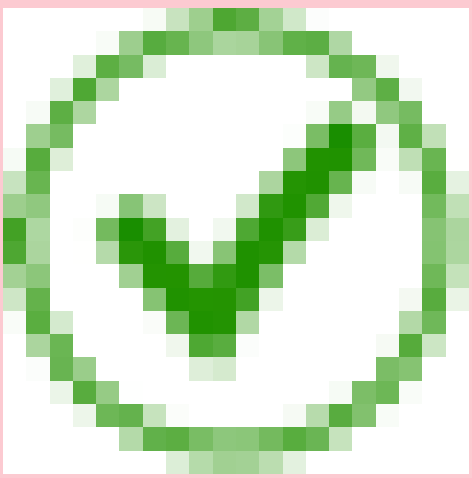
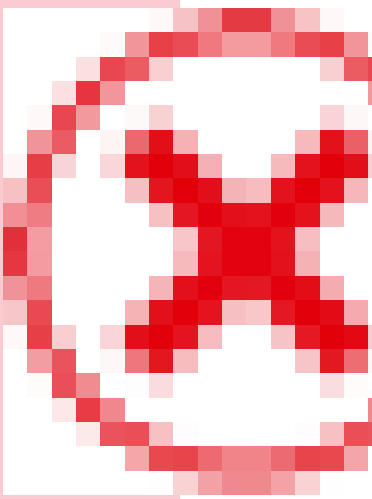
sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_vi_g
承認ルール			
コンテナセキュリティ統合			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_container.configure

その他のロールの情報：

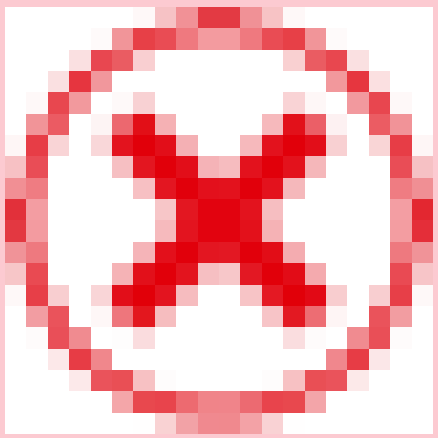
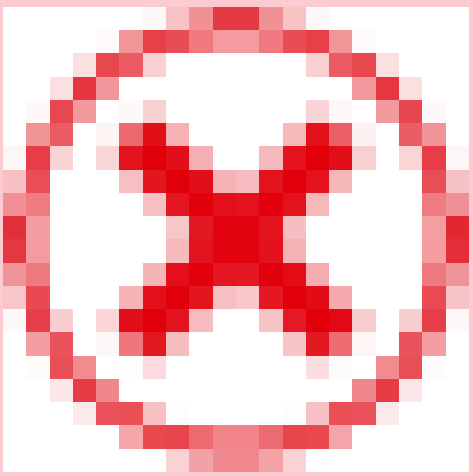
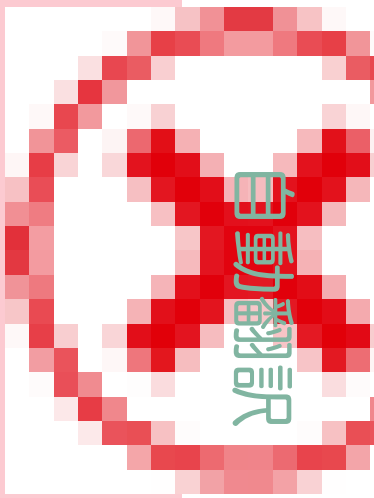
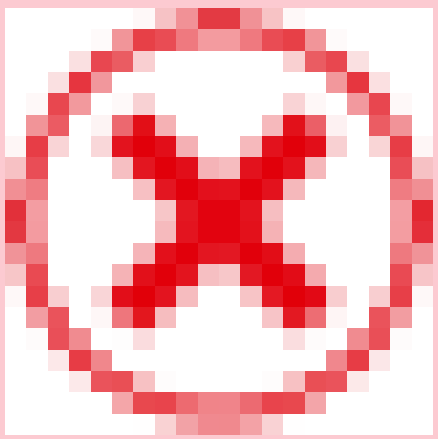
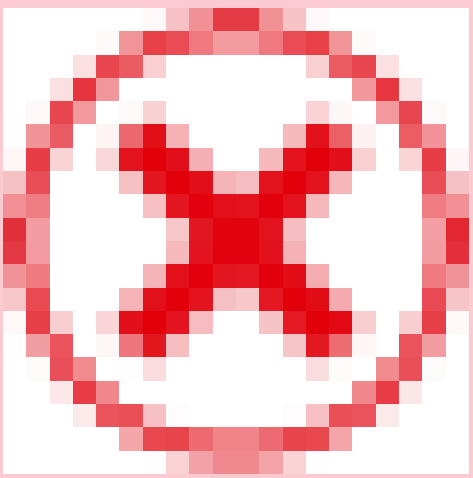
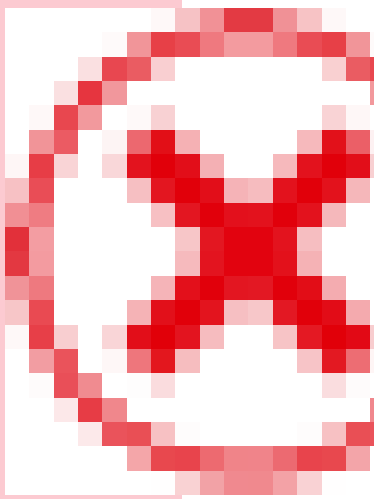
sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_vi_g
脆弱性一致アイテムの自動クローズ			
正規化された重大度マップ			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.exception_approver、sn_vul_container.false_
positive_approver、sn_vul_container.manage_assignment_rules

モジュールアクセス：sn_vul_container.exception_approver、sn_vul_container.false_
positive_approver、sn_vul_container.manage_assignment_rules

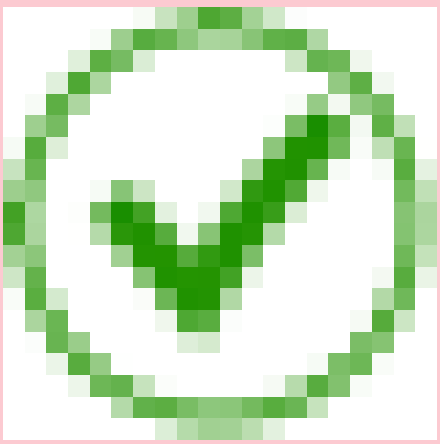
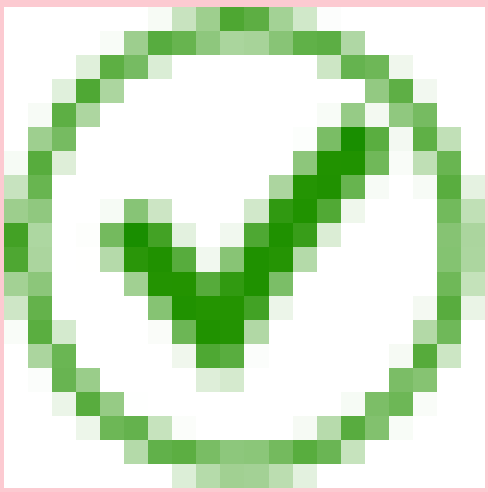
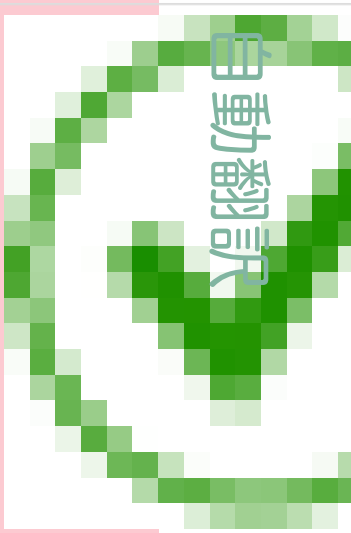
その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

モジュール	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_ass
(メインアプリグループ)			
概要			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

その他のロールの情報：

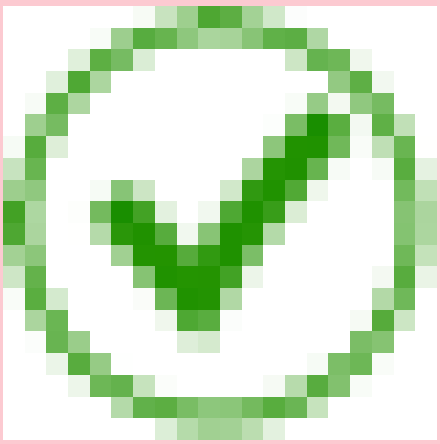
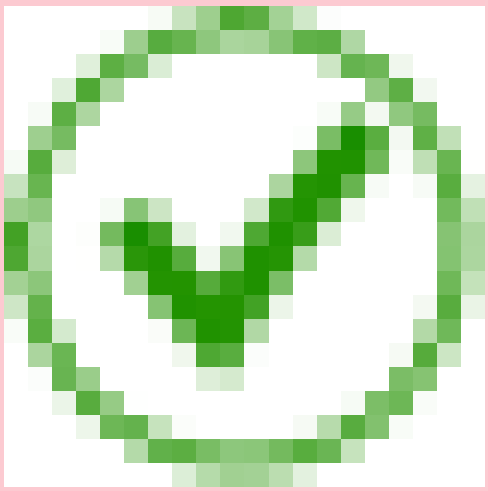
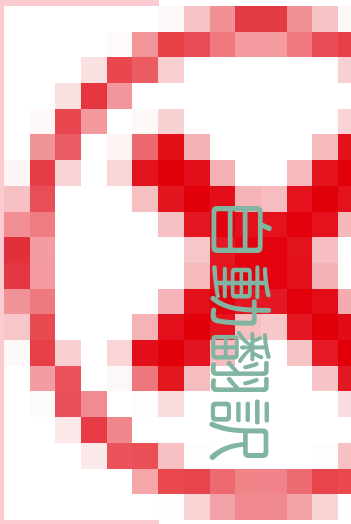
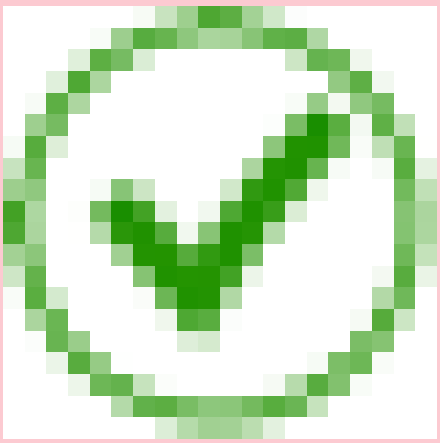
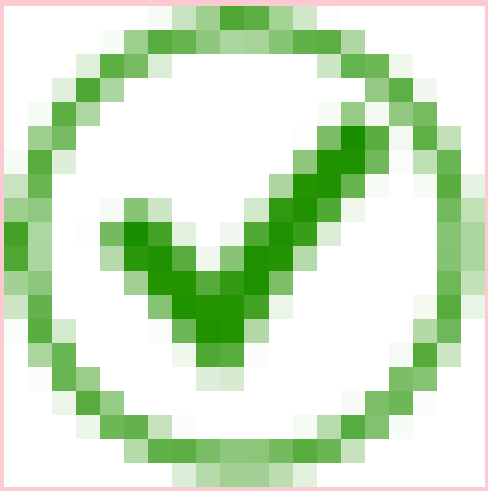
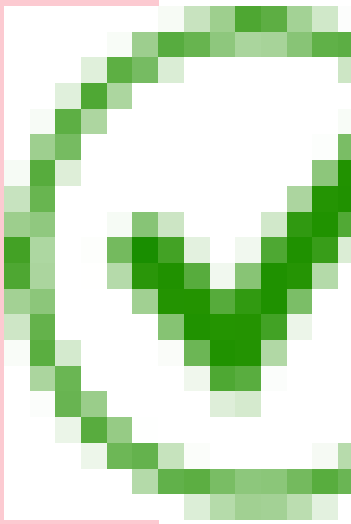
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_ass
自分の承認			
コンテナ脆弱性一致アイテム			
自分にアサイン済み			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

その他のロールの情報：

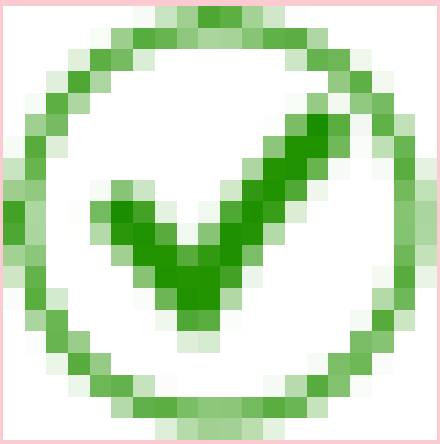
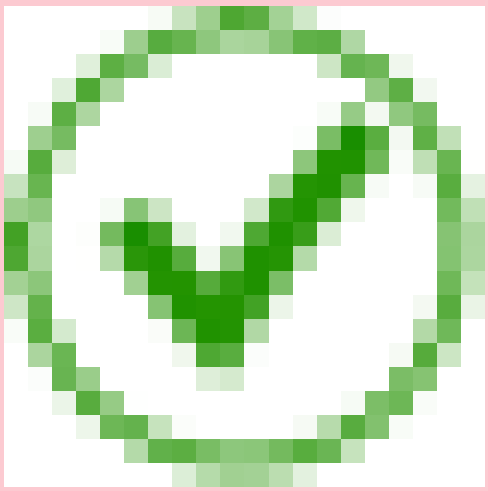
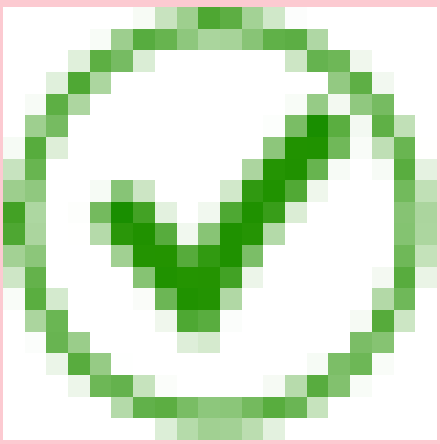
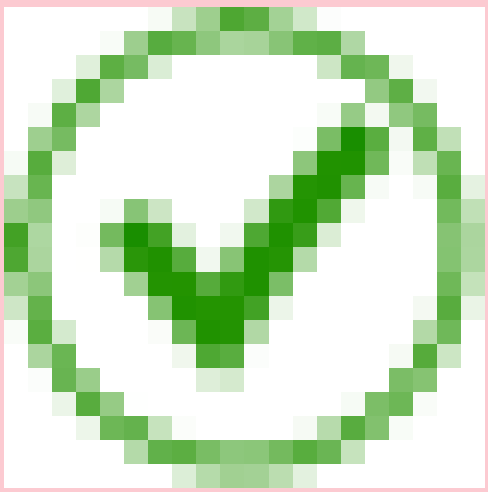
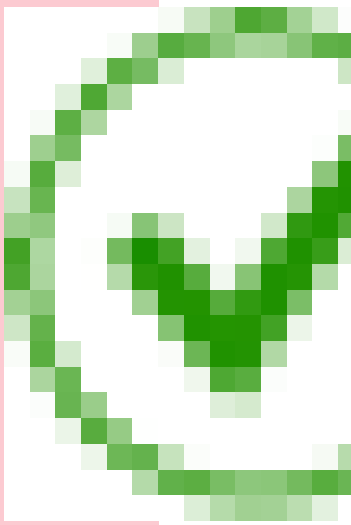
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_ass
所属グループにアサイン済み			
重大および高リスク			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

その他のロールの情報：

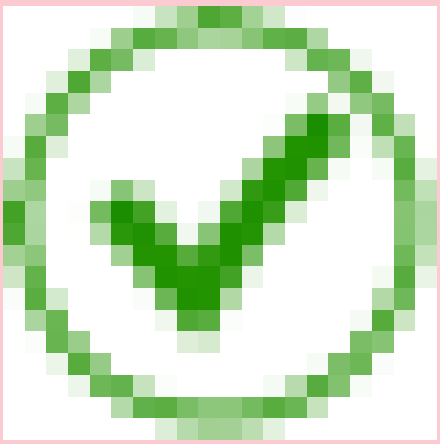
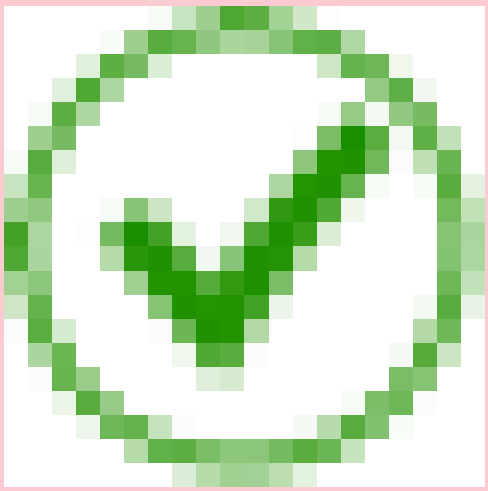
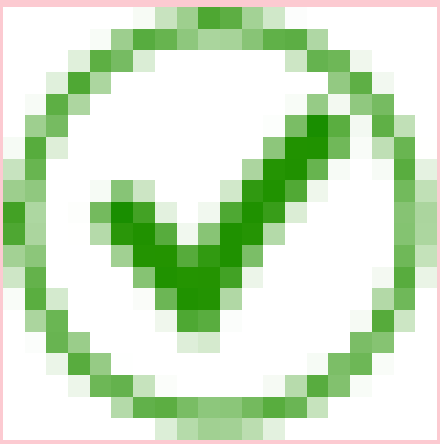
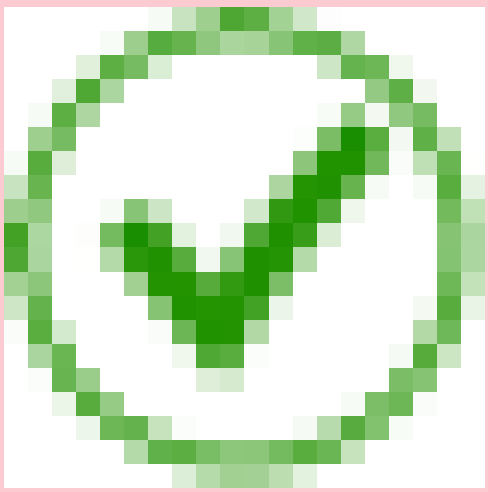
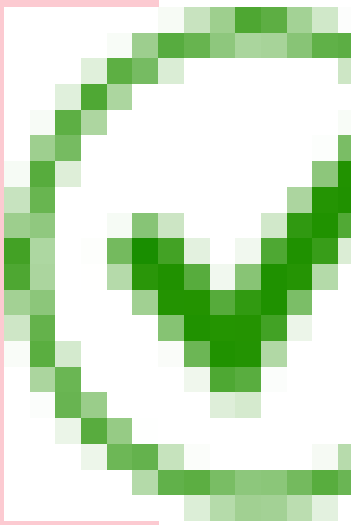
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_ass
エクスプロイト可能			
該当 CI 確認中			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

その他のロールの情報：

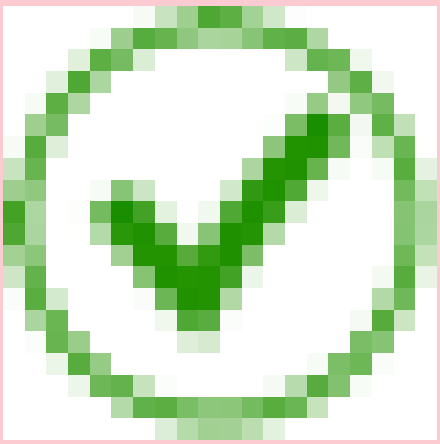
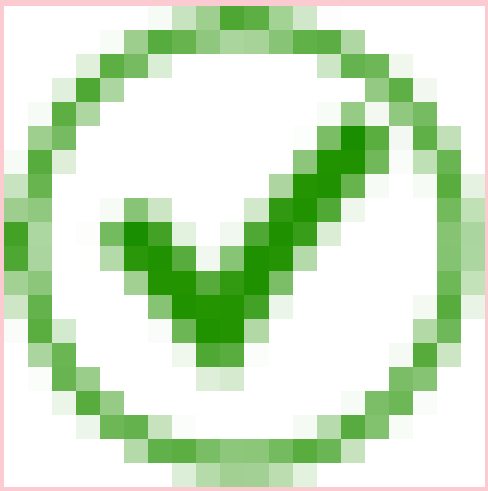
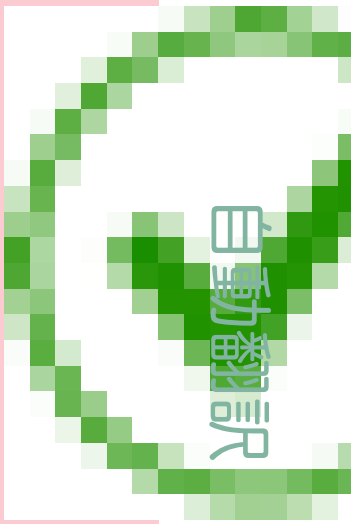
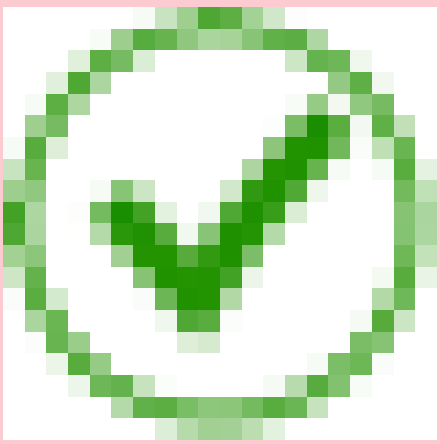
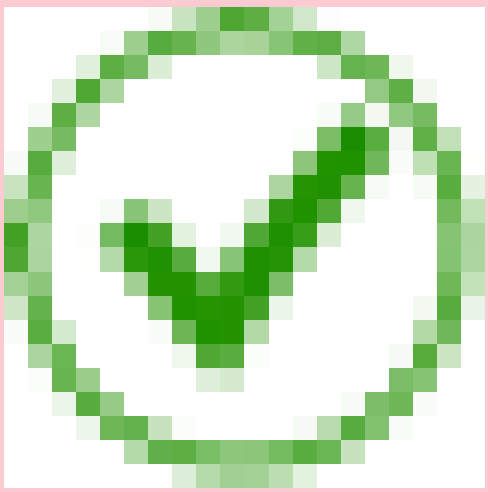
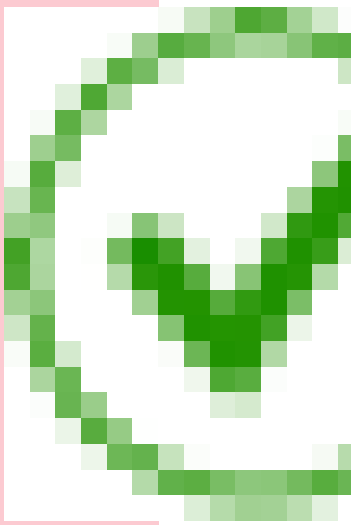
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_ass
CI 不明			
すべて			

ライブラリ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

その他のロールの情報：

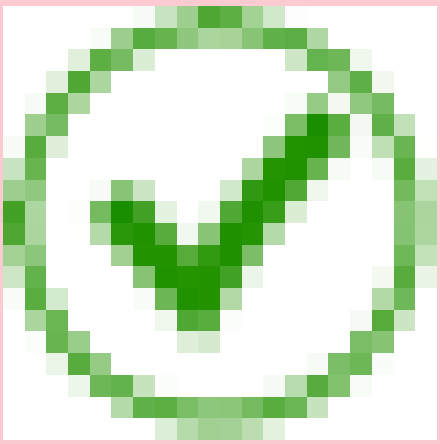
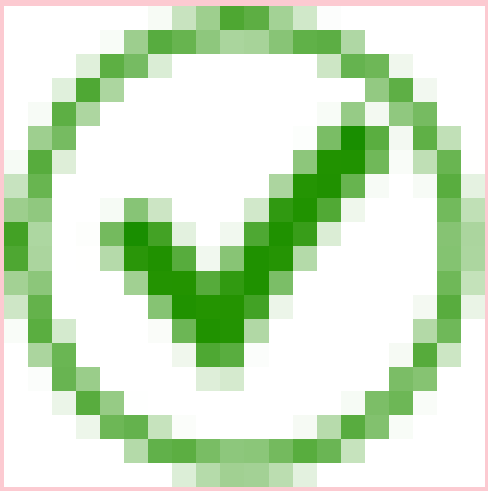
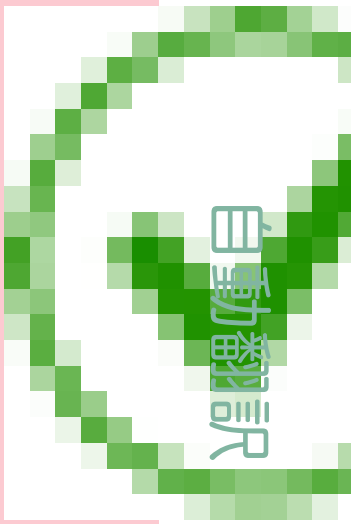
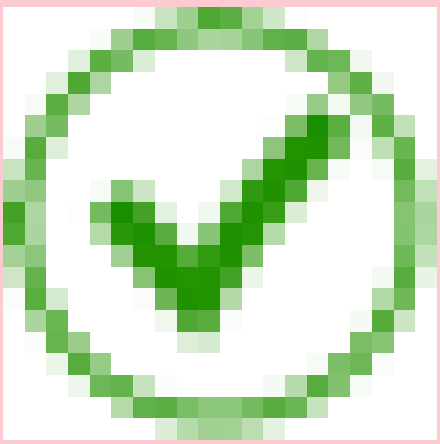
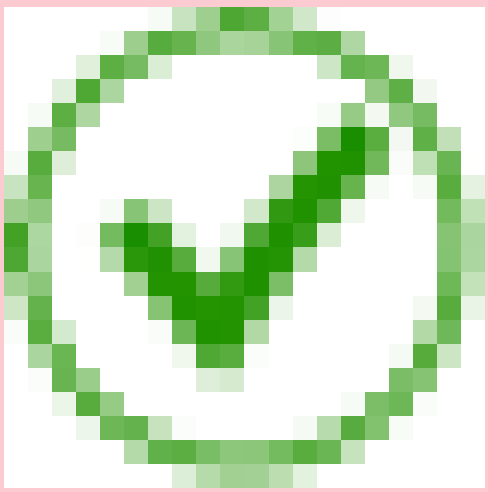
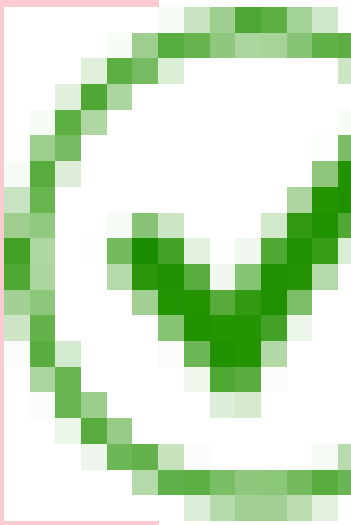
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_ass
NVD			
サードパーティ			

管理

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

その他のロールの情報：

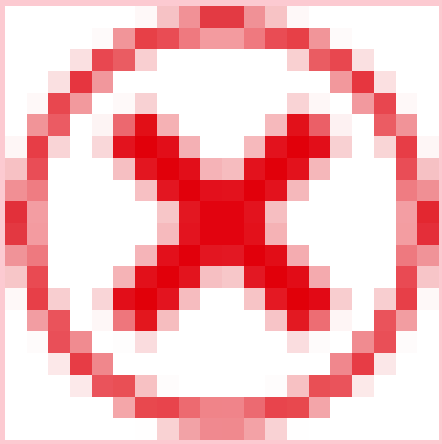
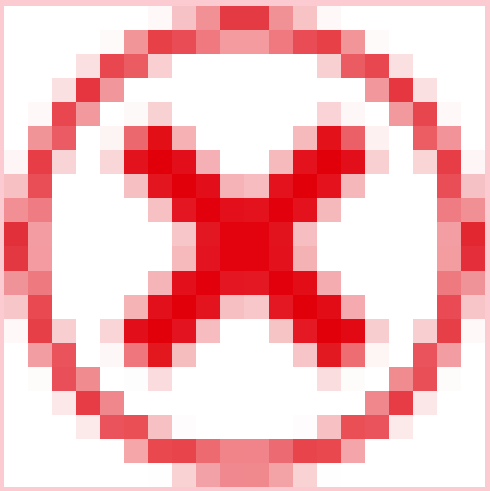
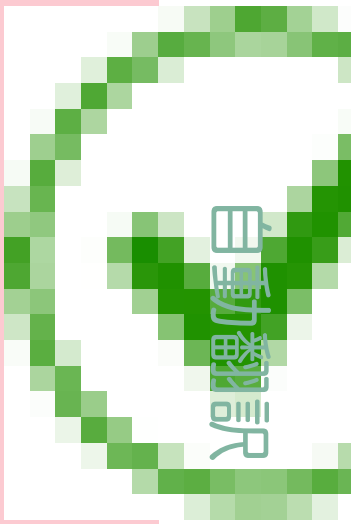
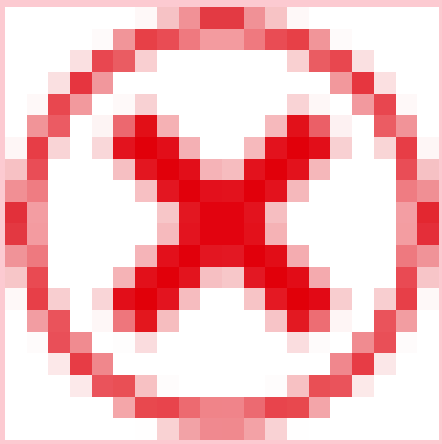
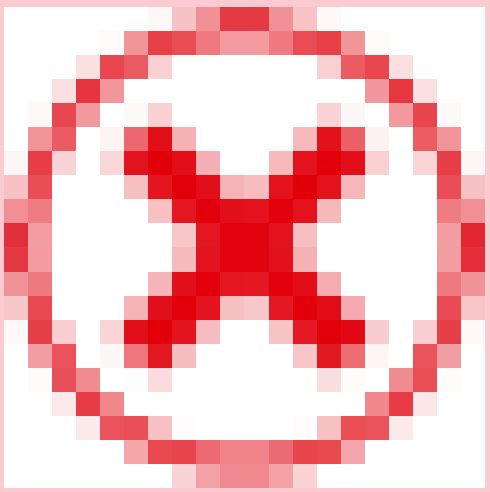
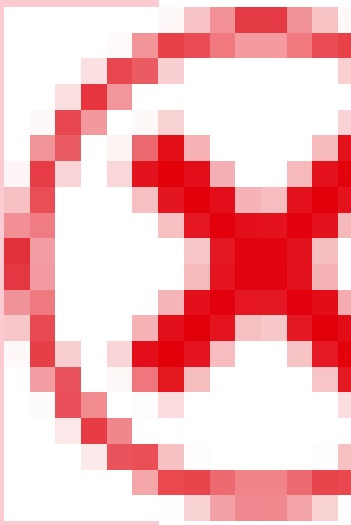
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_ass
アサインルール			
脆弱性算出			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

その他のロールの情報：

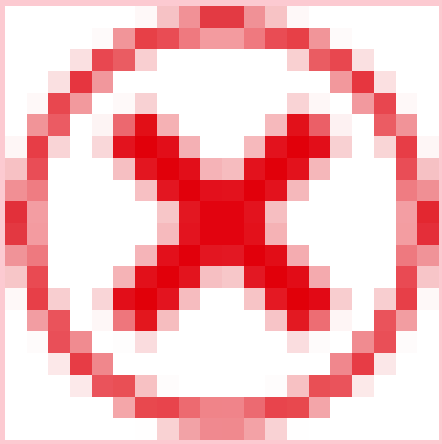
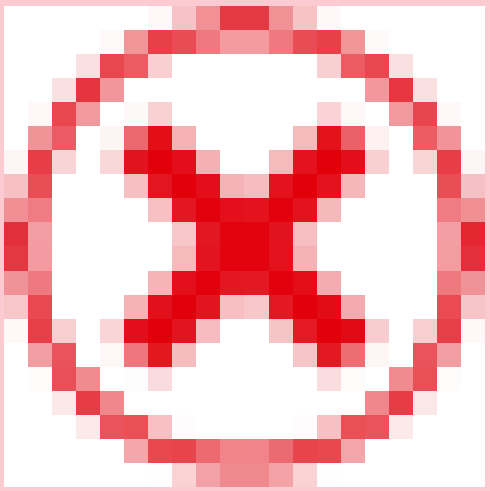
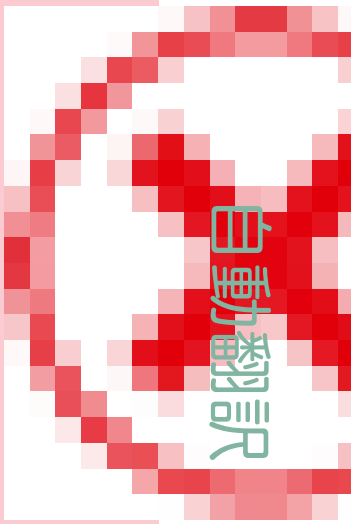
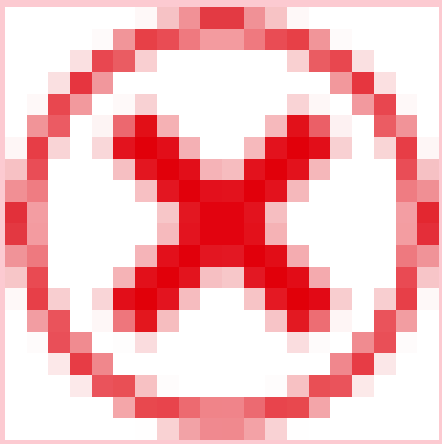
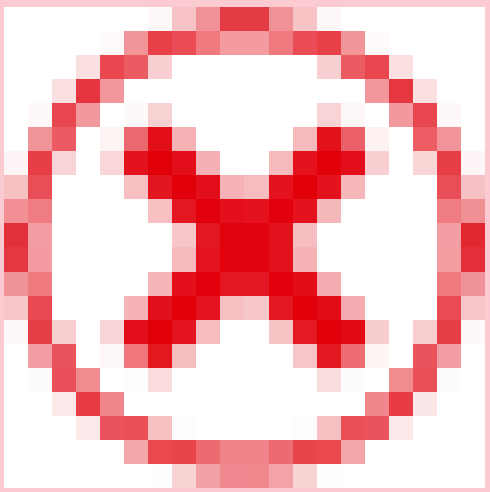
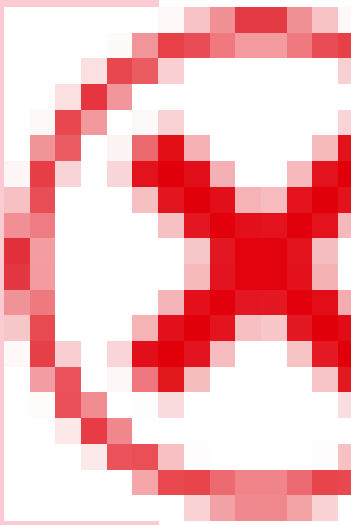
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_ass
修復ターゲットルール			
VI の粒度の構成			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

その他のロールの情報：

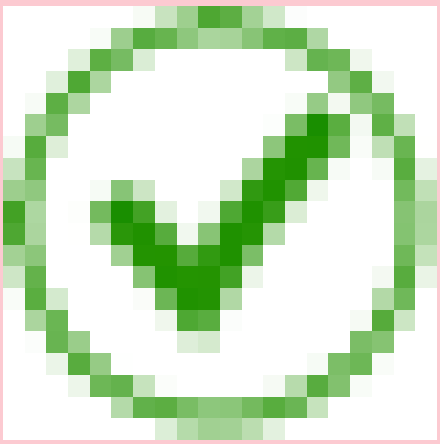
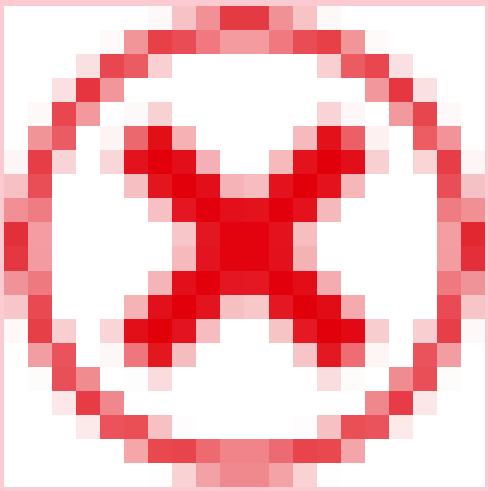
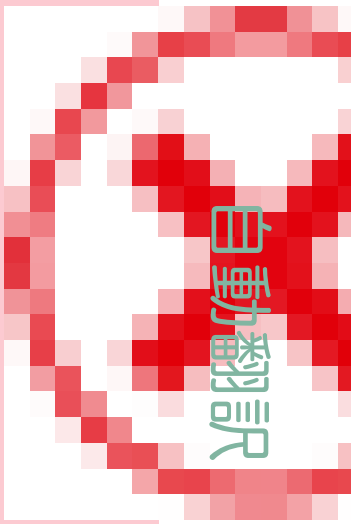
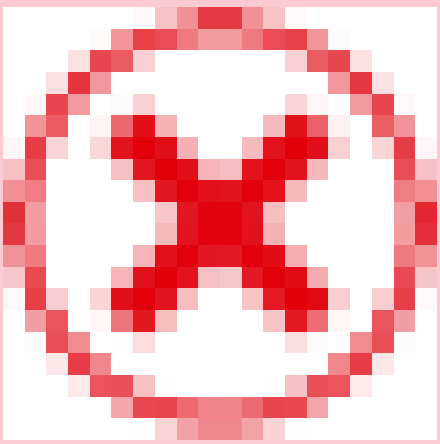
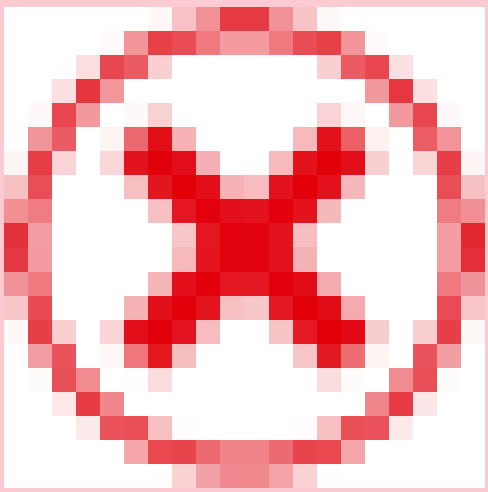
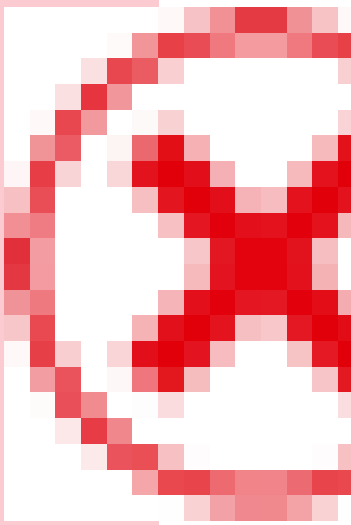
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_ass
例外ルール			
承認ルール			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

その他のロールの情報：

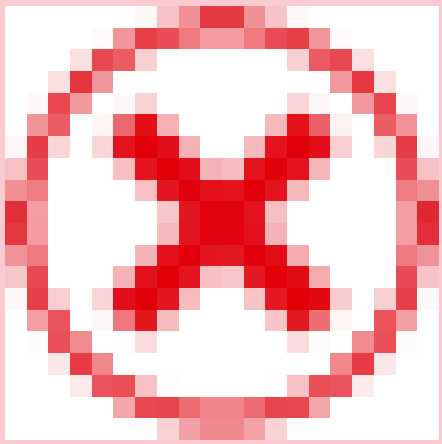
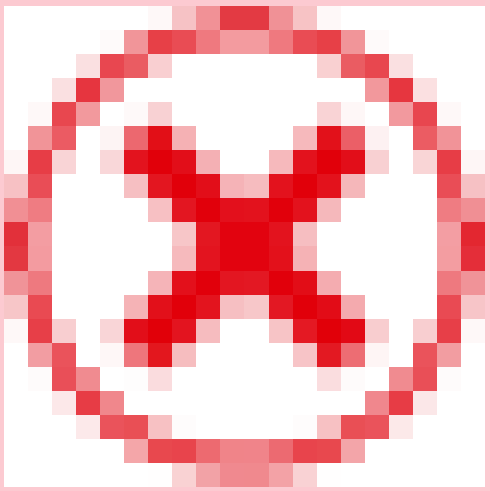
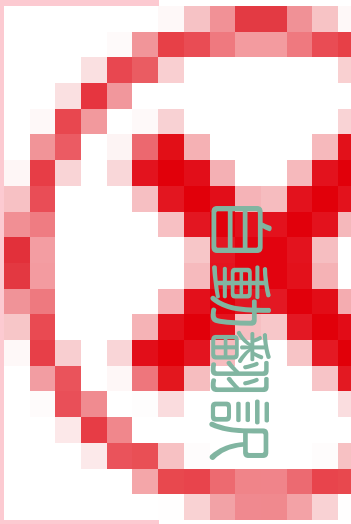
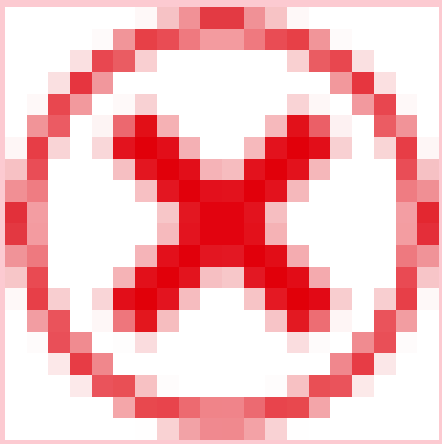
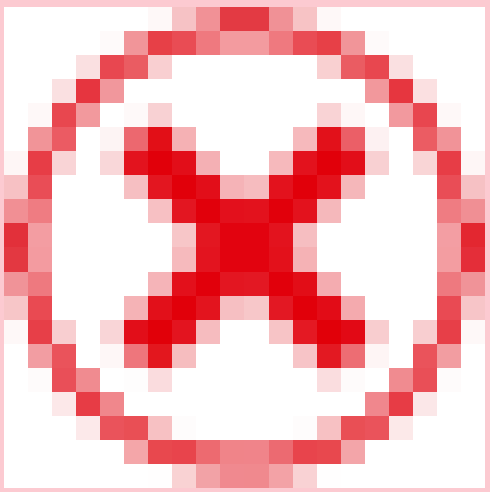
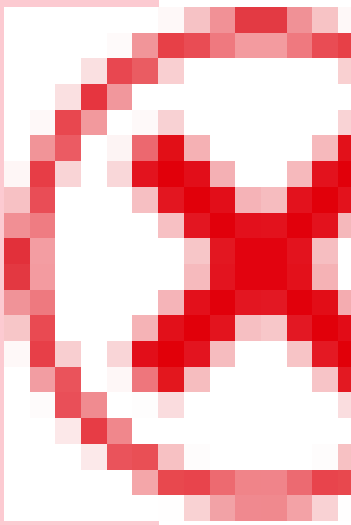
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_ass
コンテナセキュリティ統合			
脆弱性一致アイテムの自動クローズ			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

その他のロールの情報：

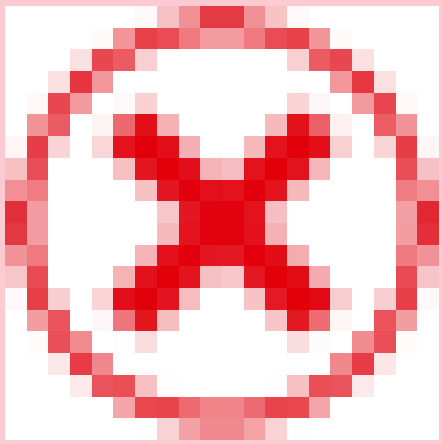
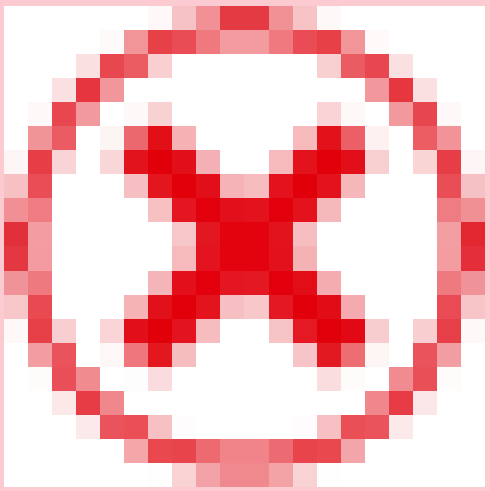
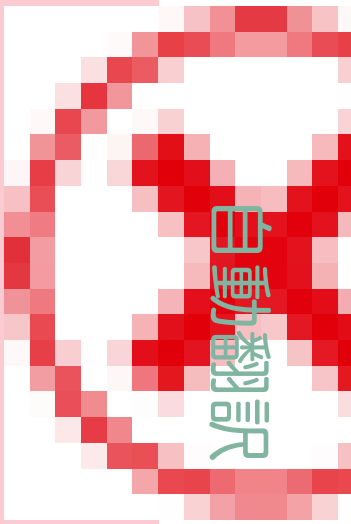
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_ass
正規化された重大度マップ			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

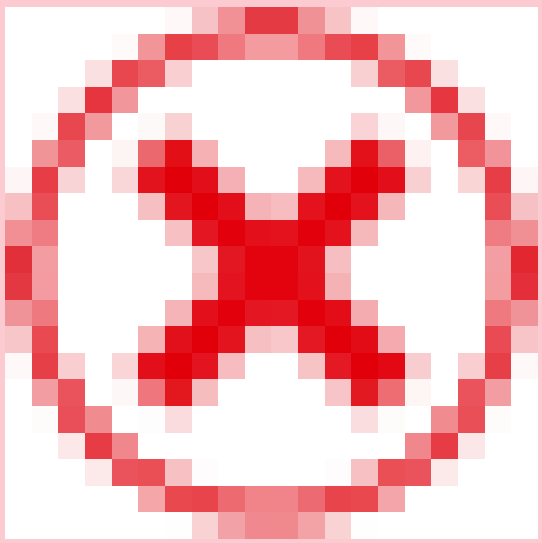
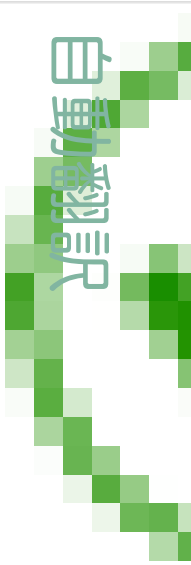
その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
(メインアプリグループ)			
概要			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

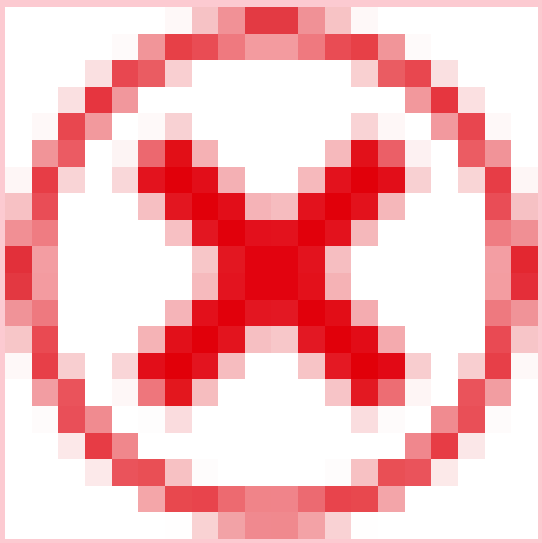
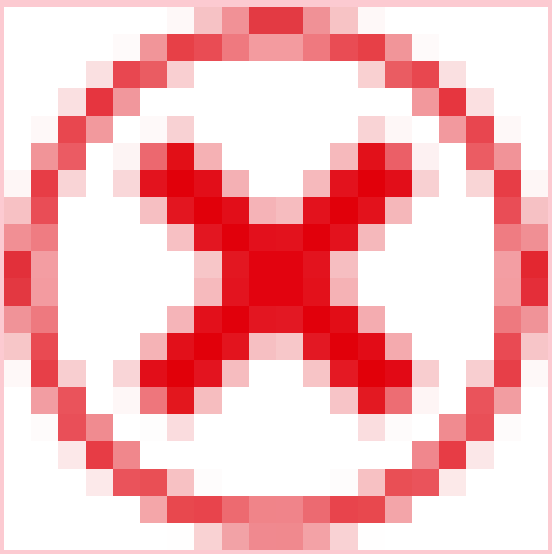
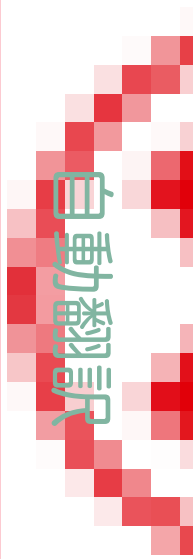
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
自分の承認			
コンテナ脆弱性一致アイテム			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

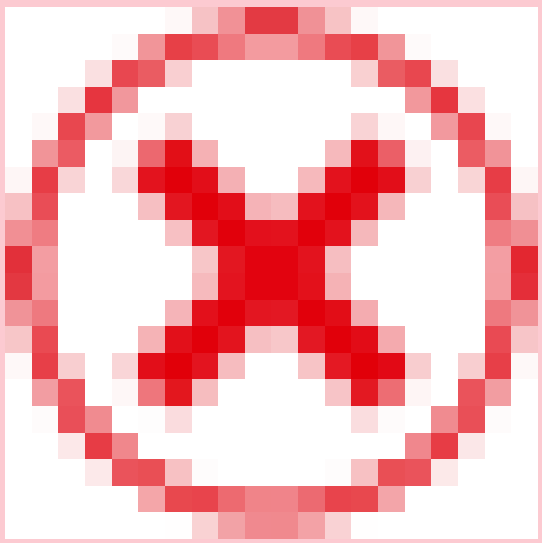
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
自分にアサイン済み			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

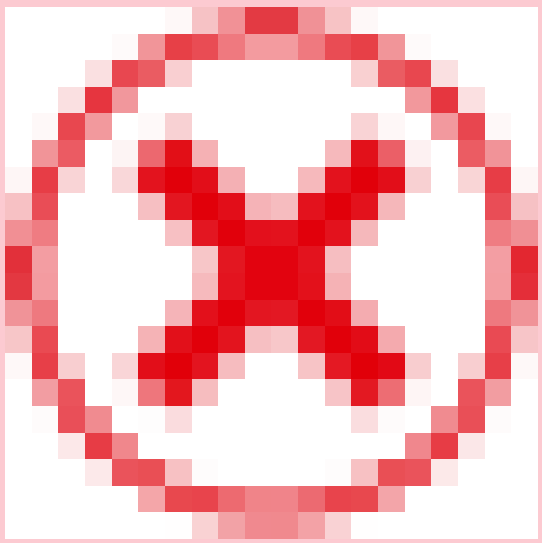
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
所属グループにアサイン済み			

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

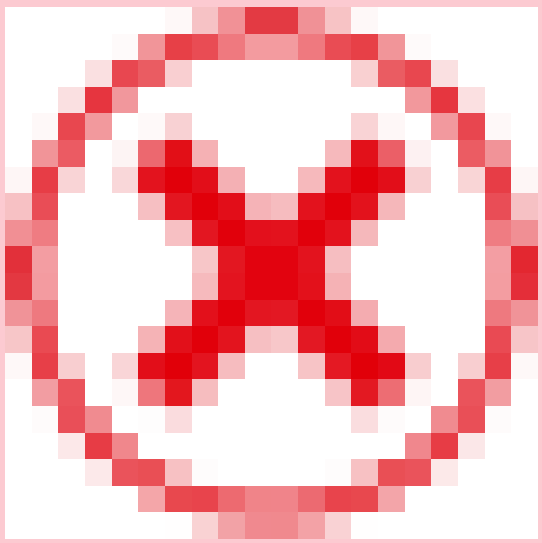
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
重大および高リスク			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

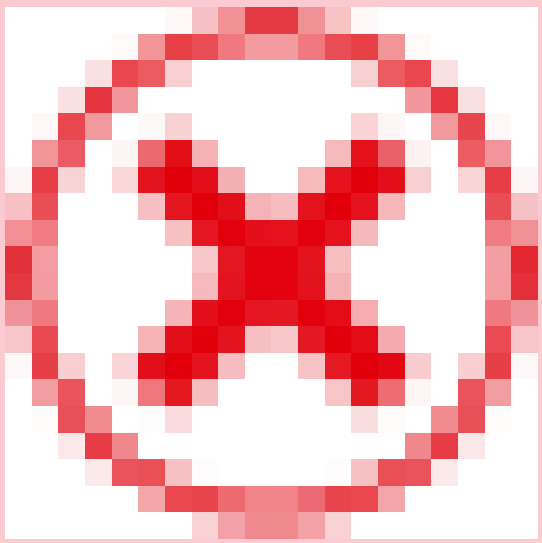
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
エクスプロイト可能			

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

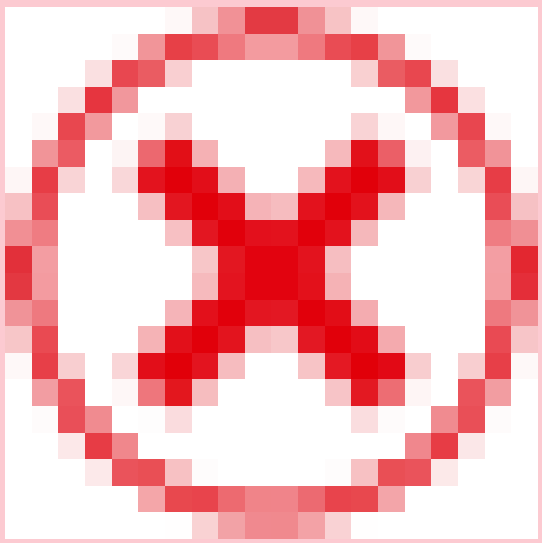
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
該当 CI 確認中			

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

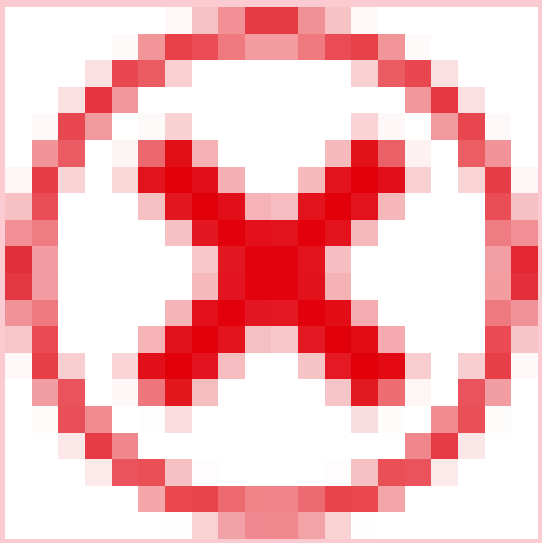
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
CI 不明			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

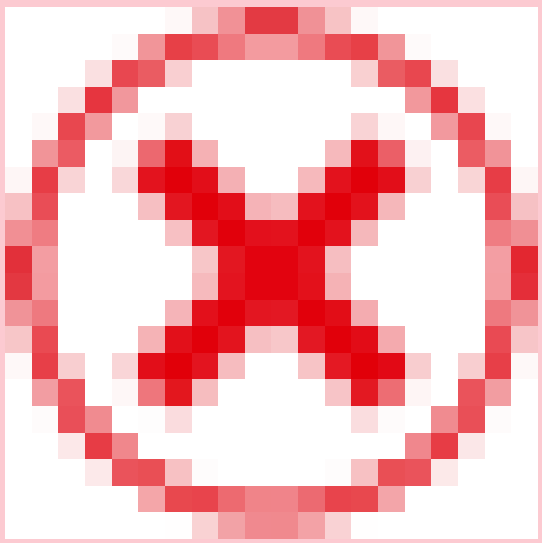
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
すべて			

ライブラリ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

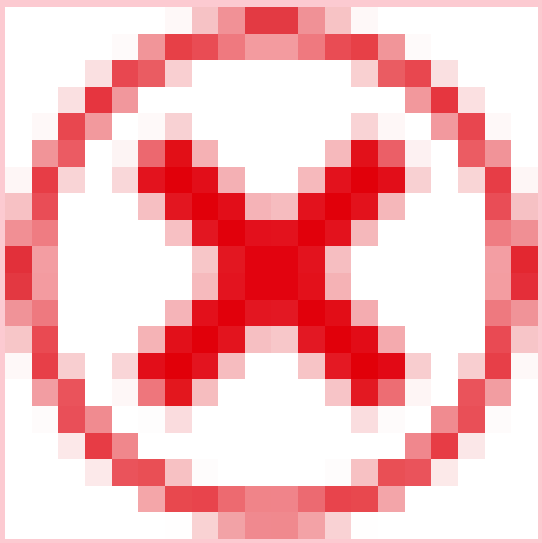
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
NVD			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

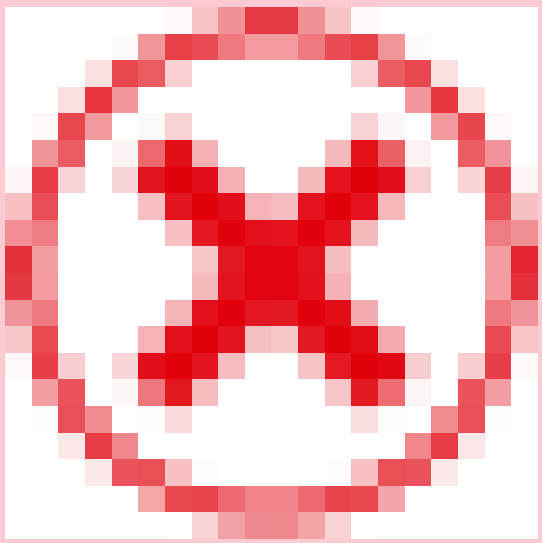
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
サードパーティ			
管理			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

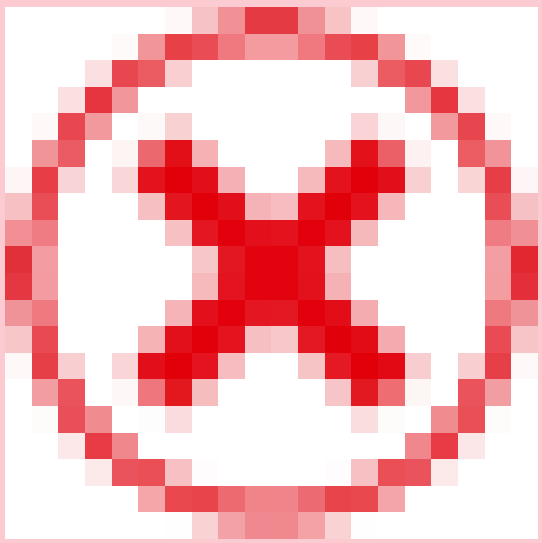
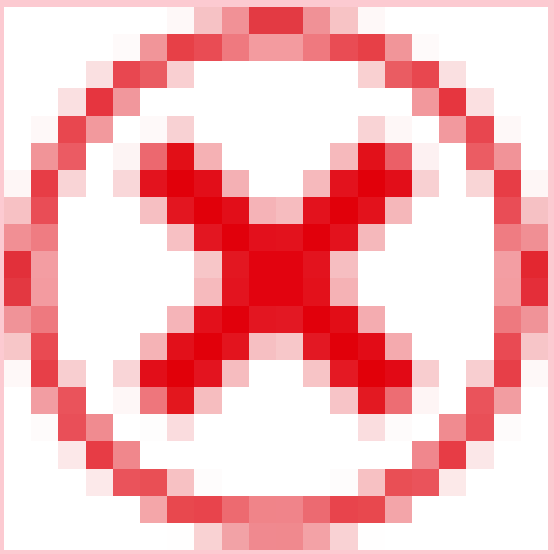
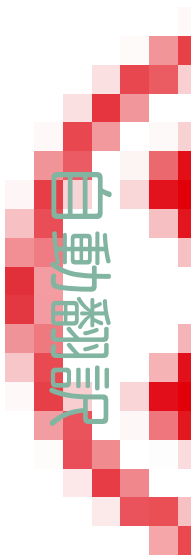
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
アサインルール			

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

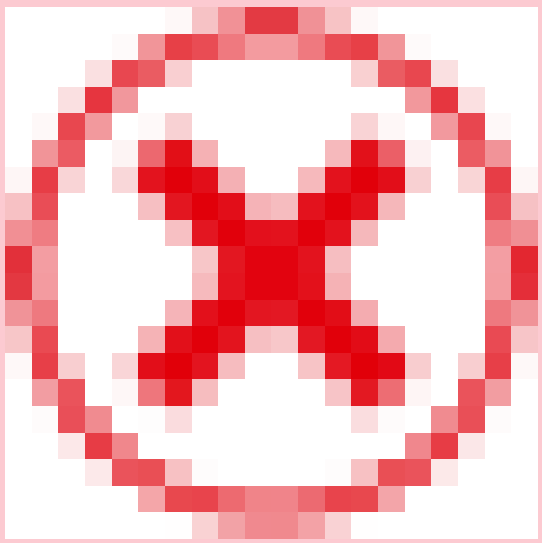
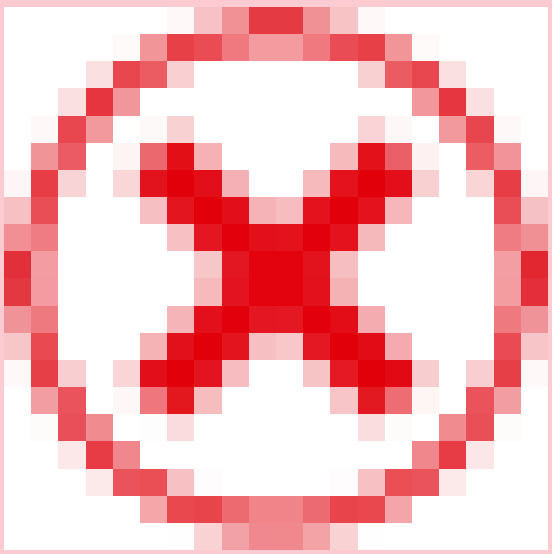
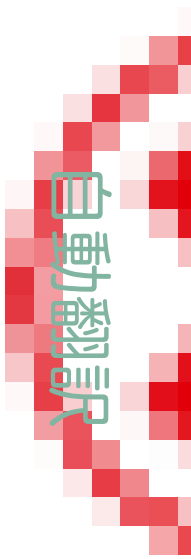
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
脆弱性算出			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

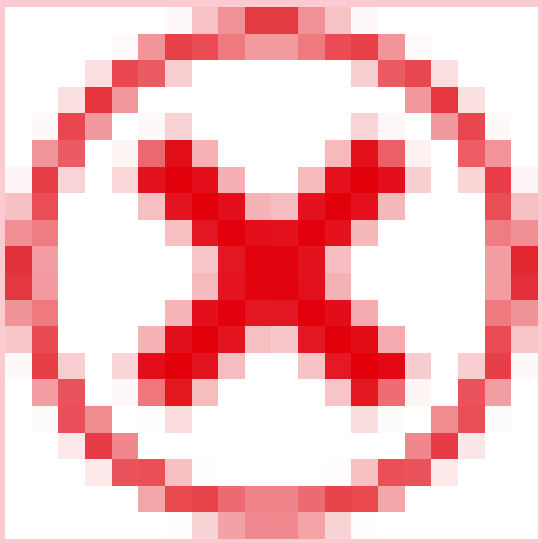
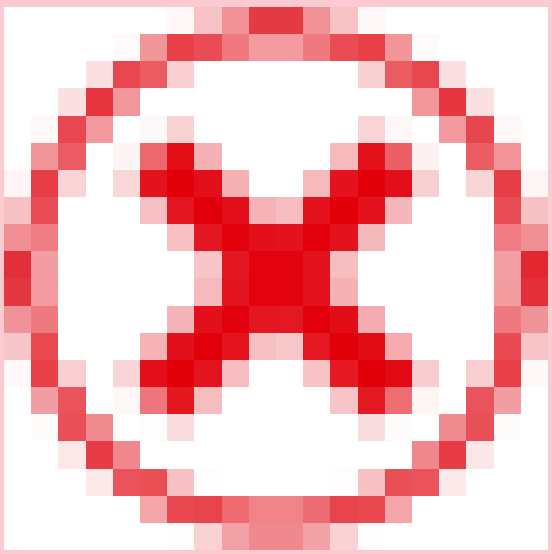
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
修復ターゲットルール			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

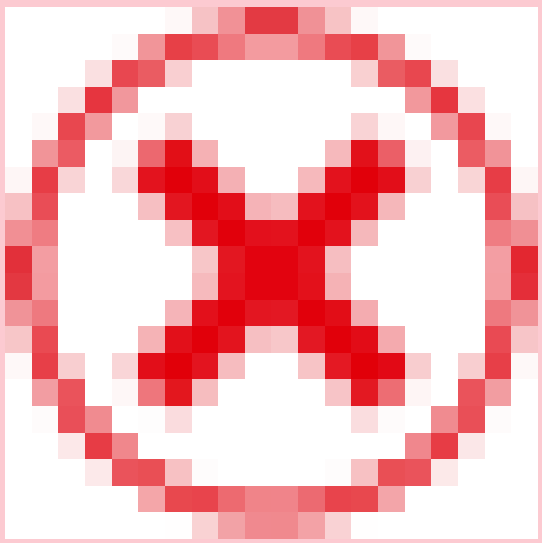
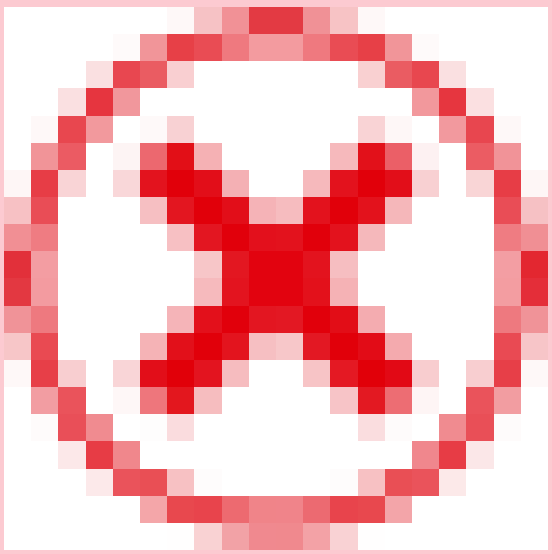
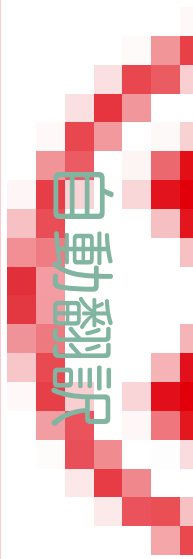
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
VI の粒度の構成			

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

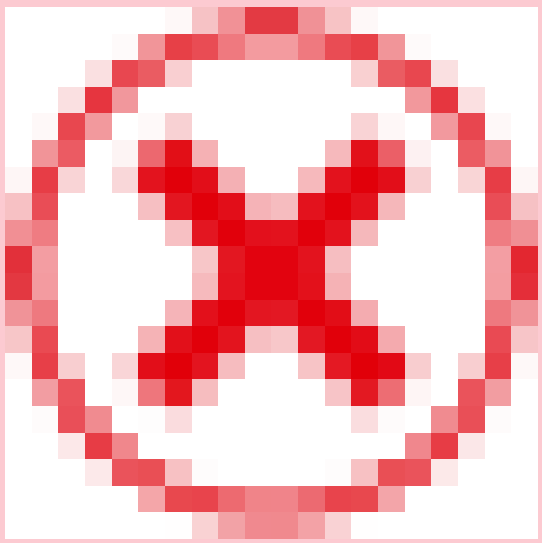
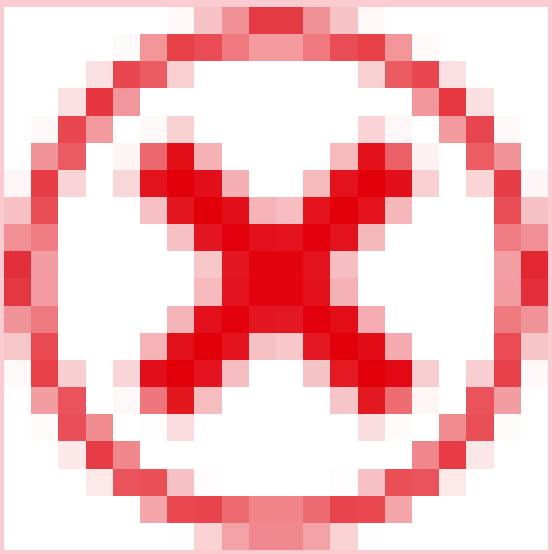
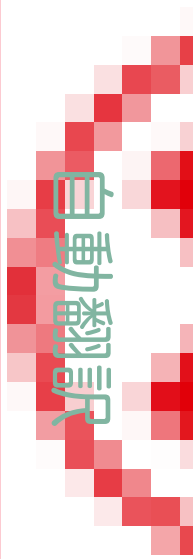
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
例外ルール			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

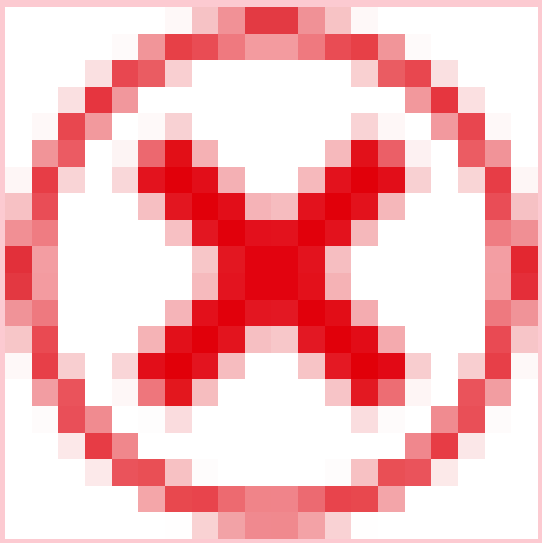
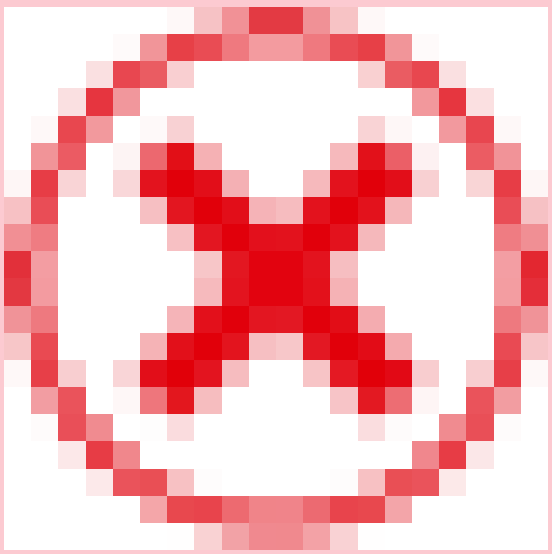
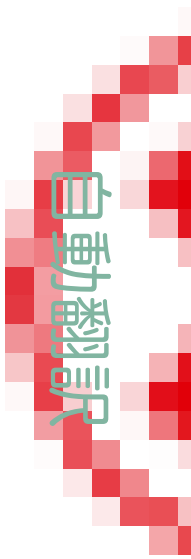
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
承認ルール			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

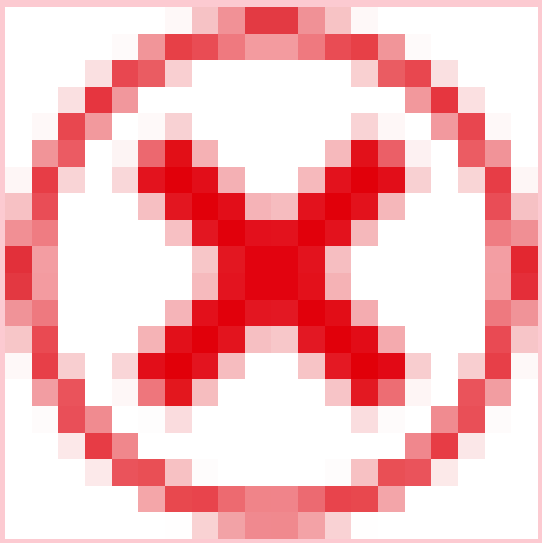
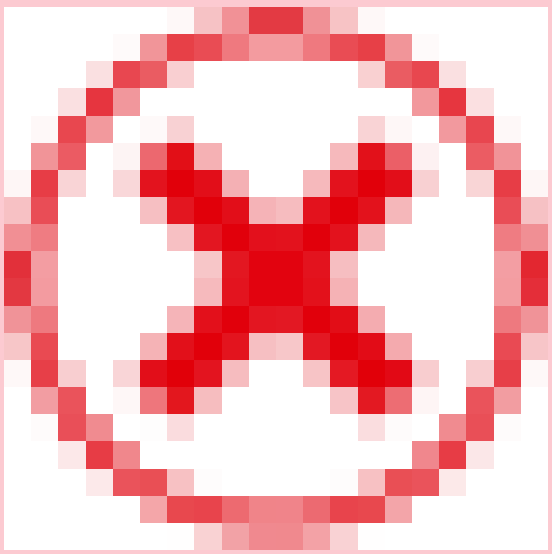
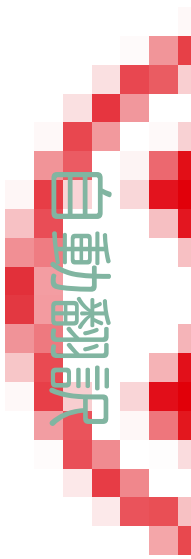
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
コンテナセキュリティ統合			

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

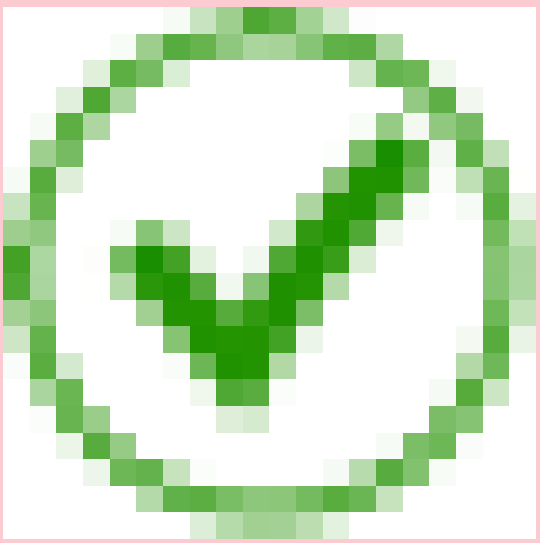
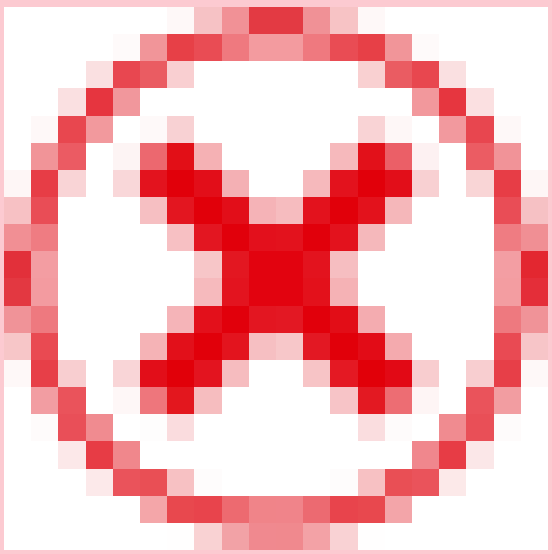
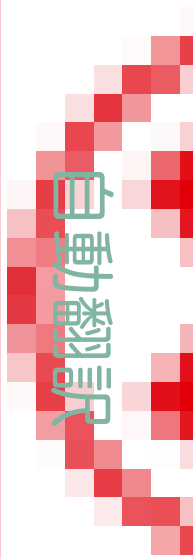
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
脆弱性一致アイテムの自動クローズ			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_severity、sn_vul_cont

その他のロールの情報：

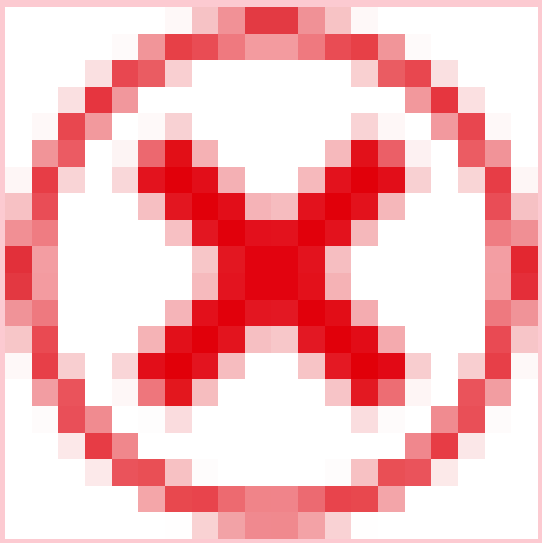
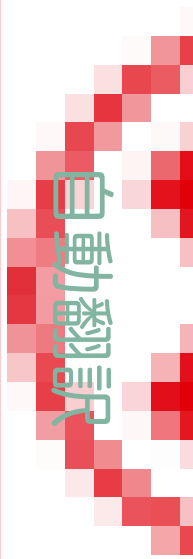
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_containe manage_remedi
正規化された重大度マップ			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_conta

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

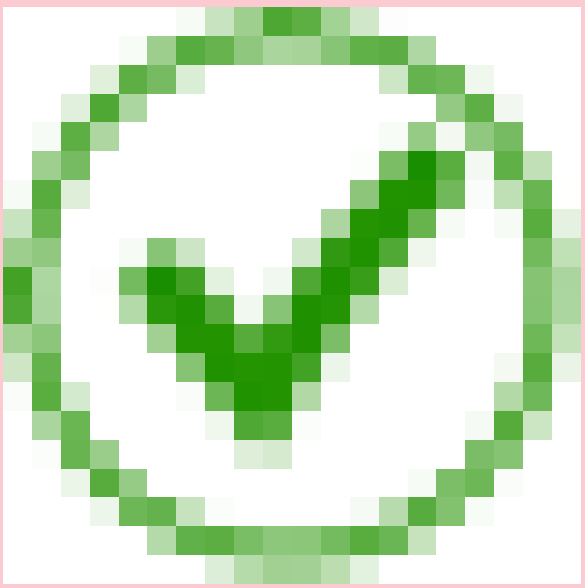
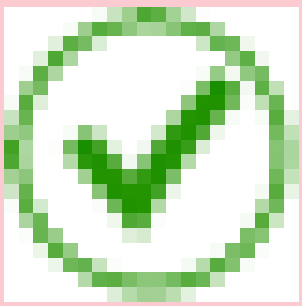
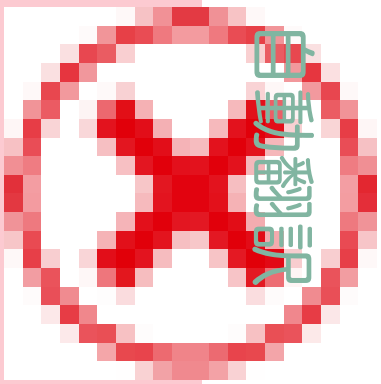
その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
(メインアプリグループ)			
概要			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

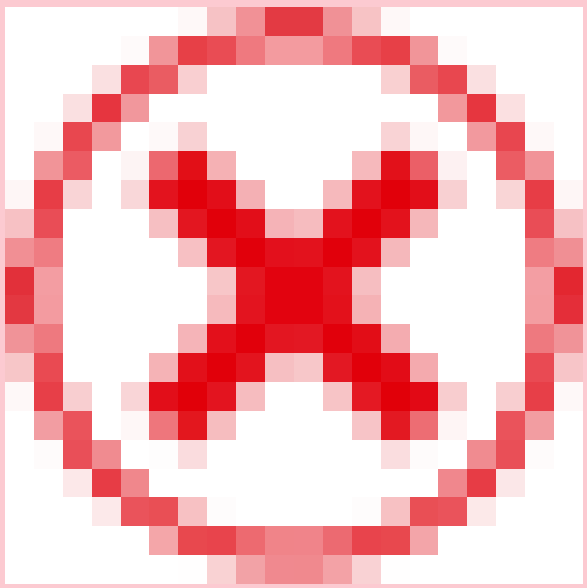
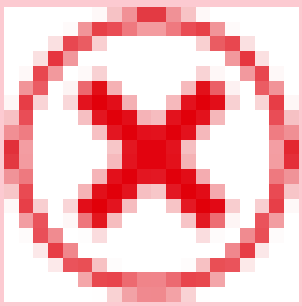
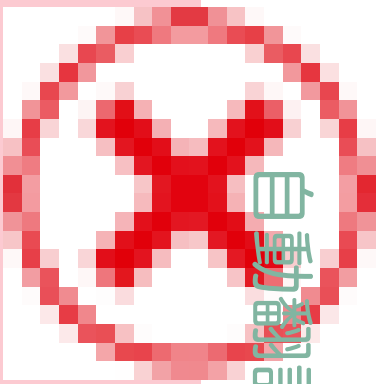
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
自分の承認			

コンテナ脆弱性一致アイテム

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

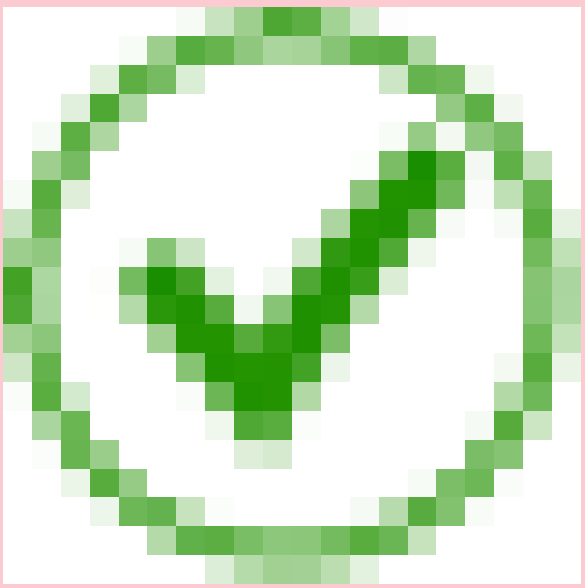
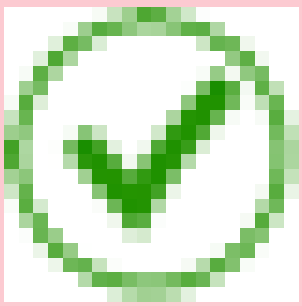
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
自分にアサイン済み			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

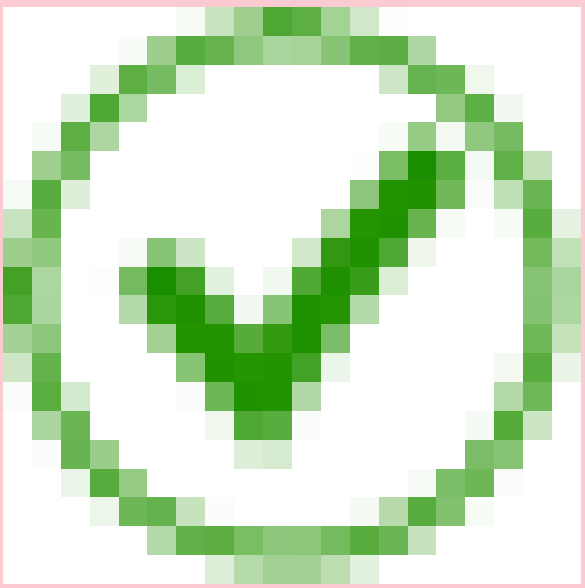
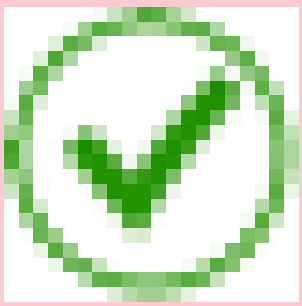
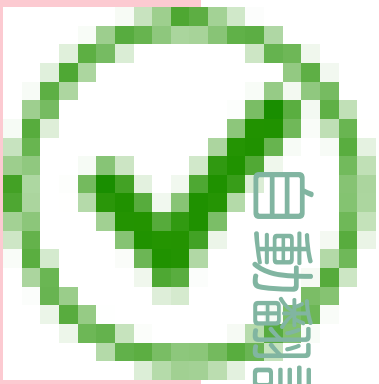
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
所属グループにアサイン済み			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

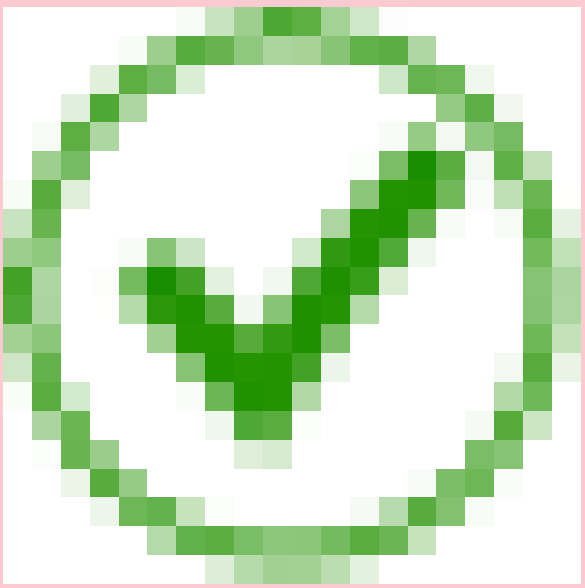
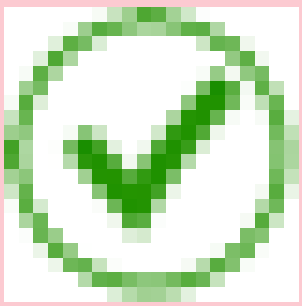
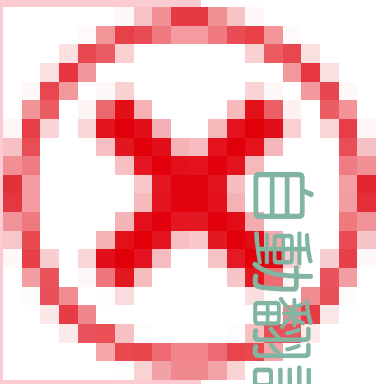
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
重大および高リスク			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

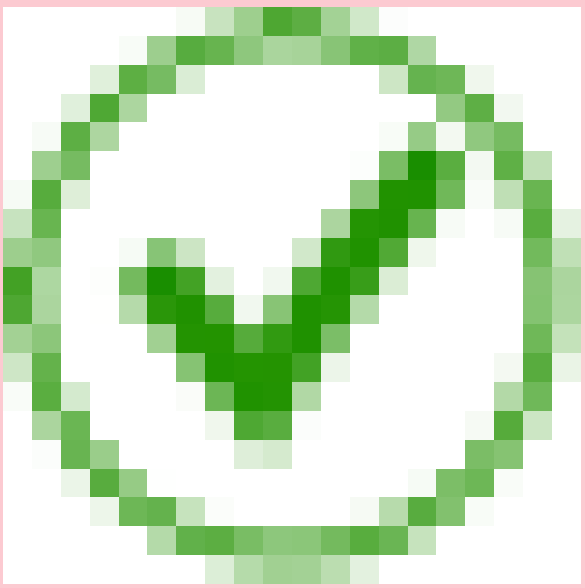
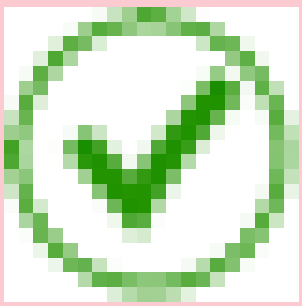
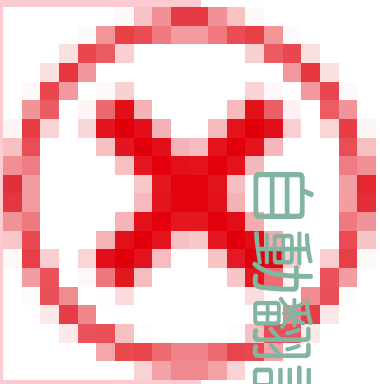
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
エクスプロイト可能			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

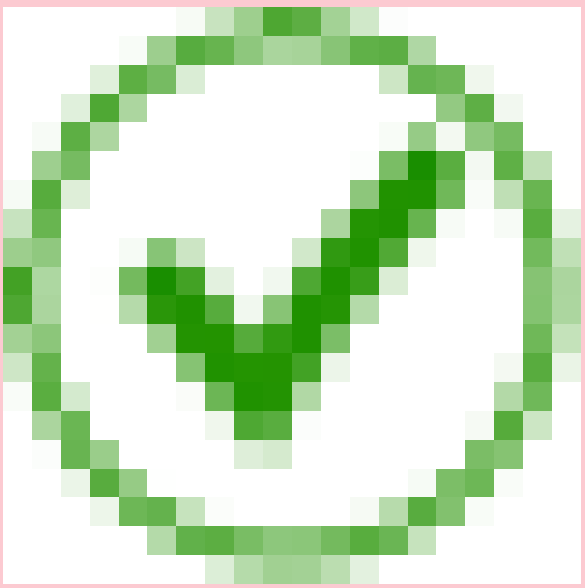
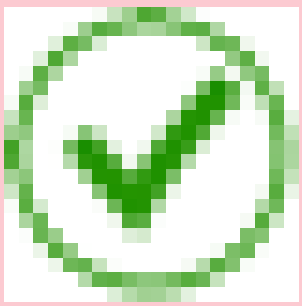
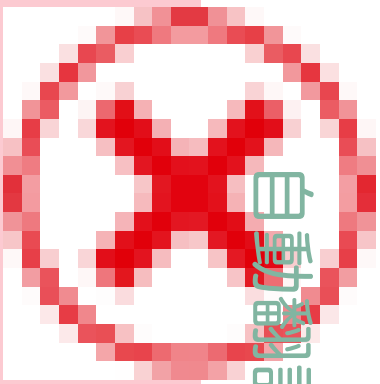
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
該当 CI 確認中			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

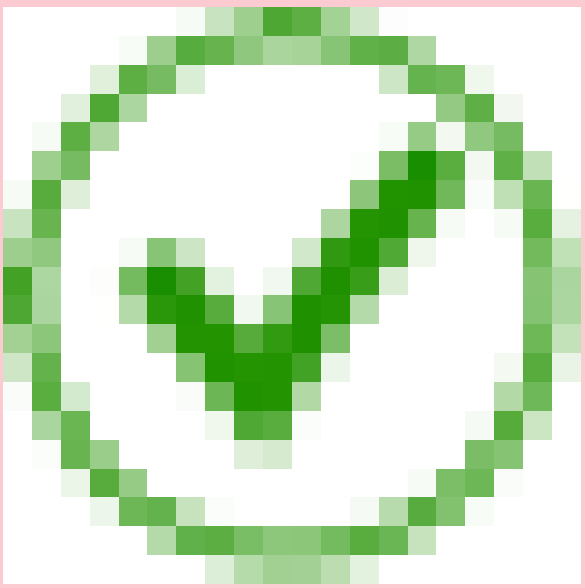
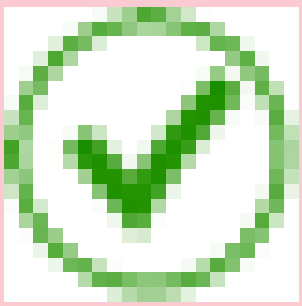
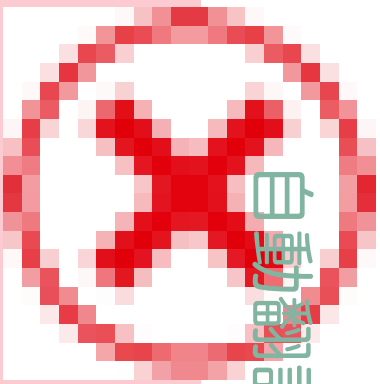
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
CI 不明			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

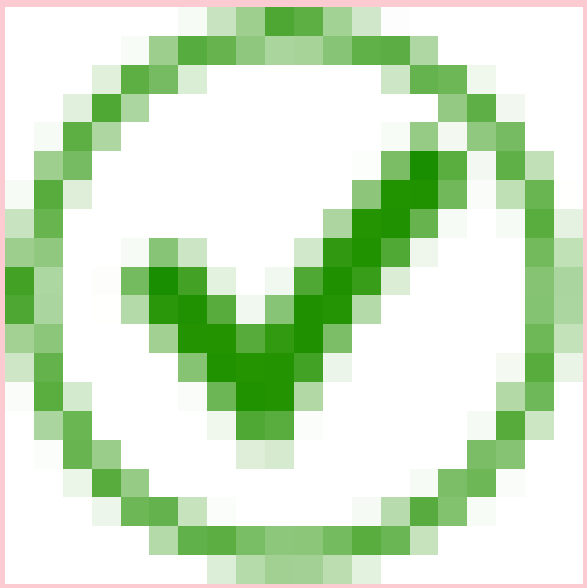
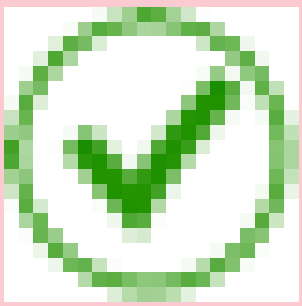
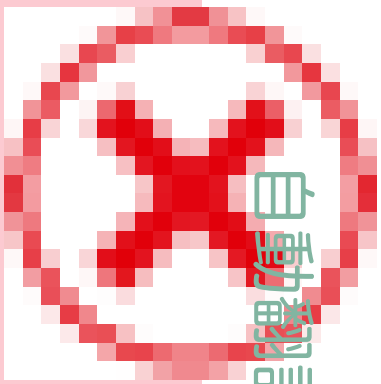
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
すべて			
ライブラリ			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

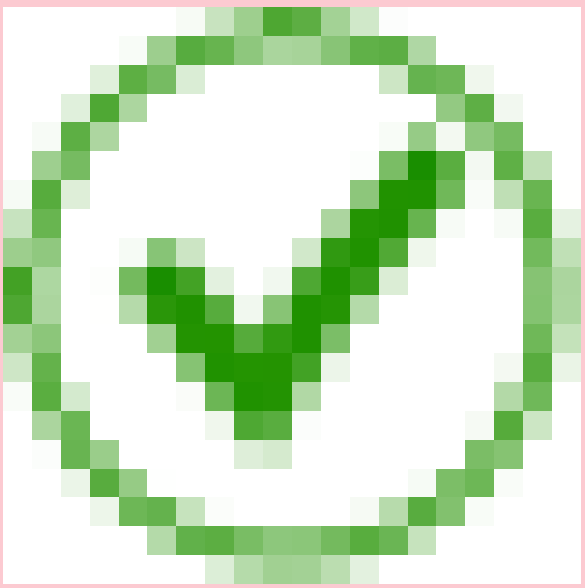
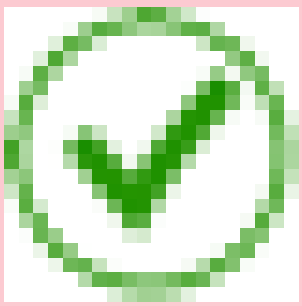
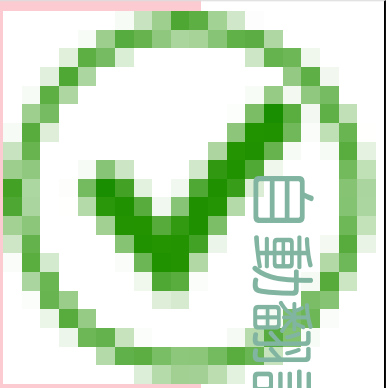
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
NVD			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

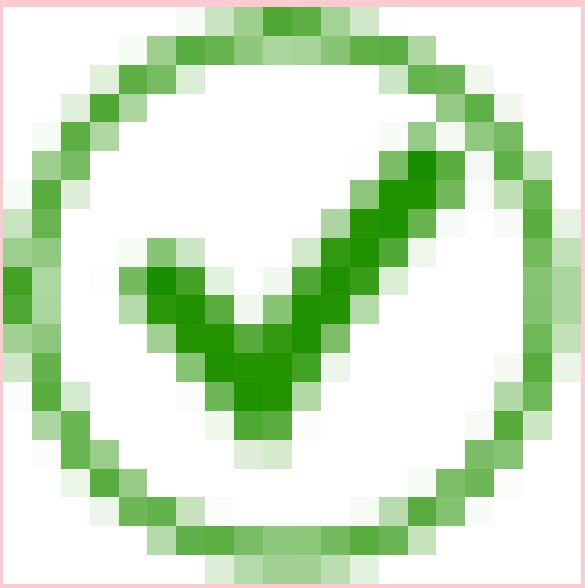
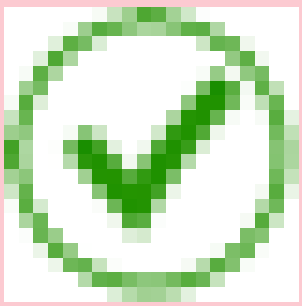
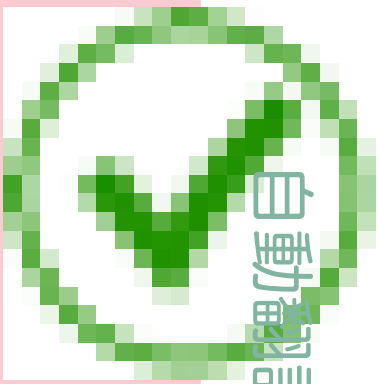
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
サードパーティ			
管理			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

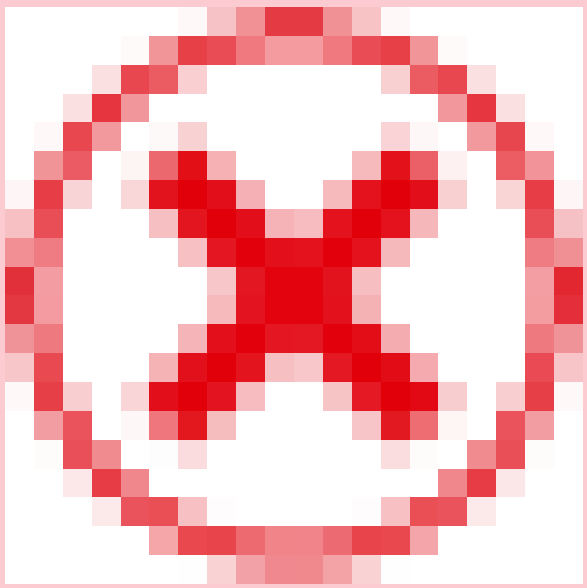
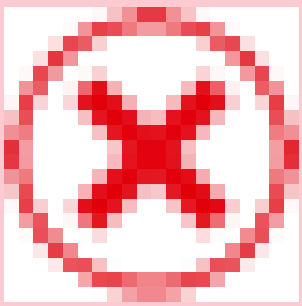
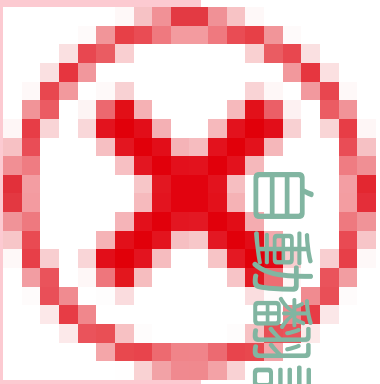
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
アサインルール			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

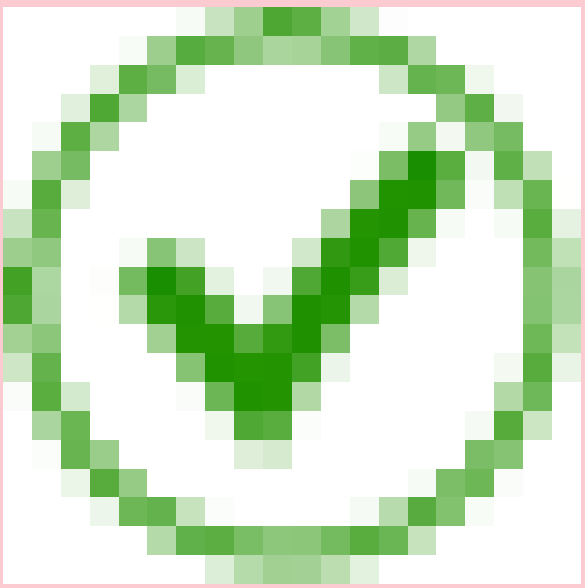
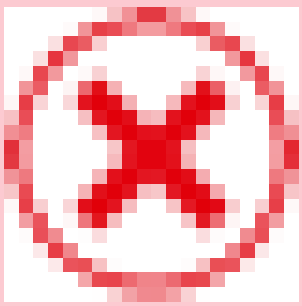
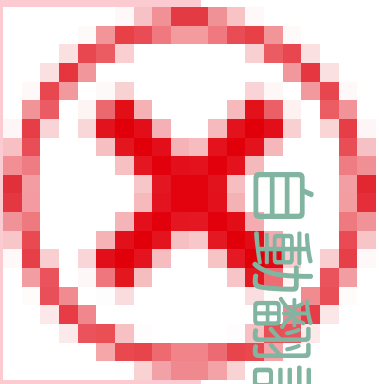
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
脆弱性算出			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

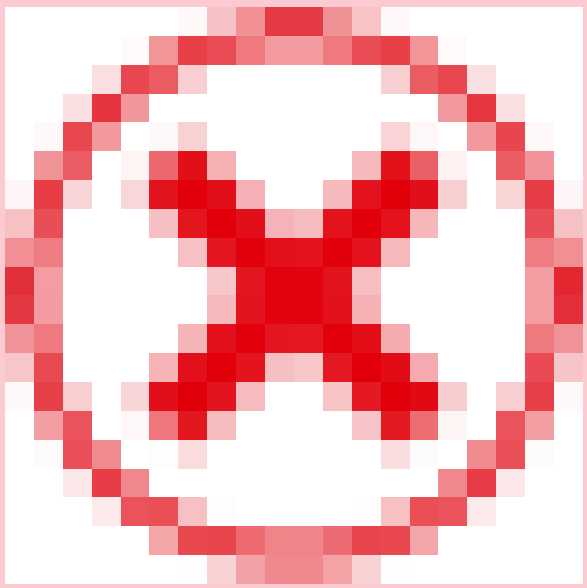
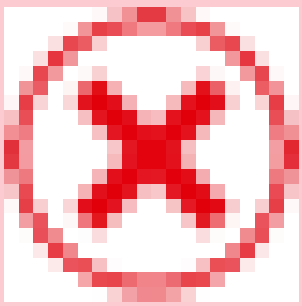
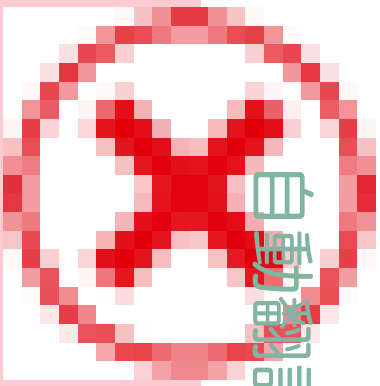
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
修復ターゲットルール			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

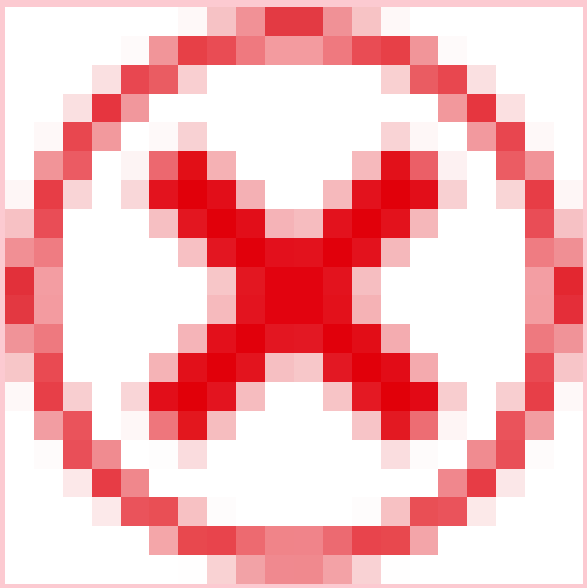
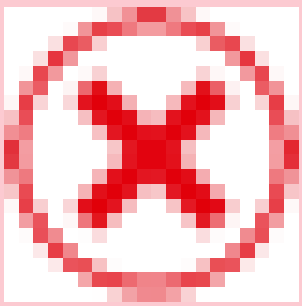
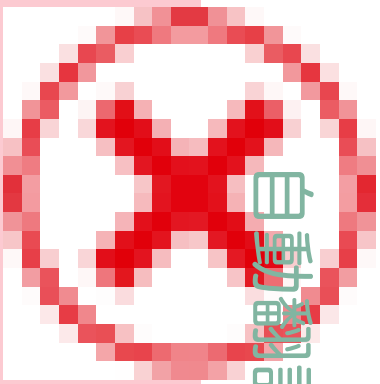
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
VI の粒度の構成			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

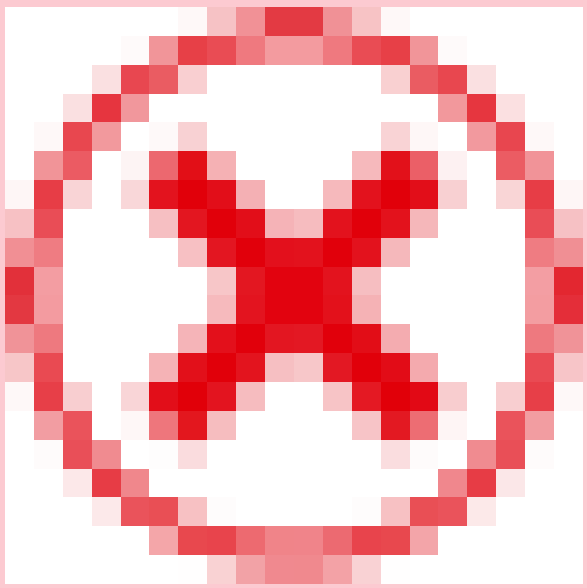
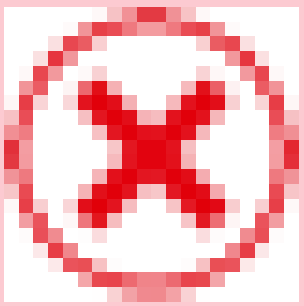
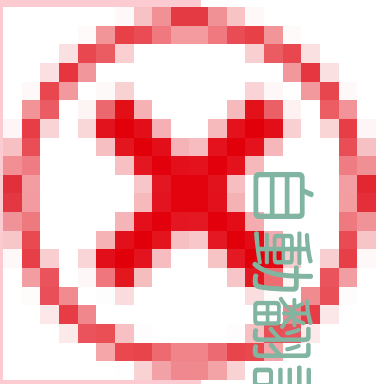
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
例外ルール			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

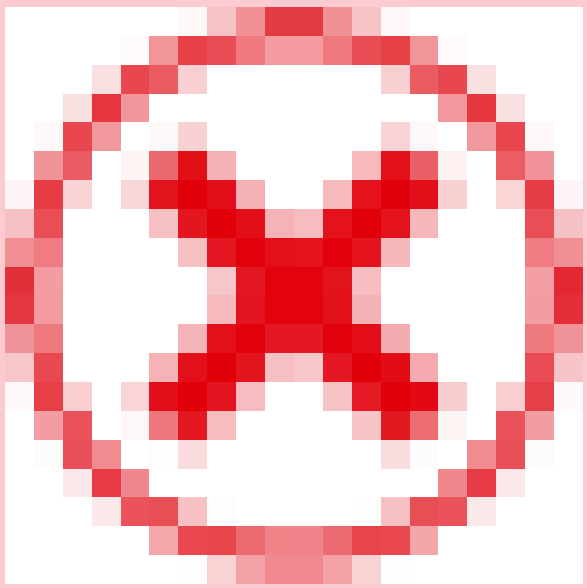
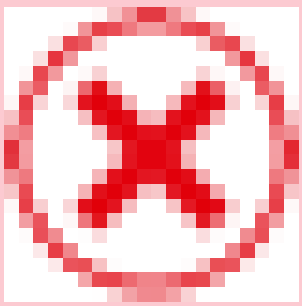
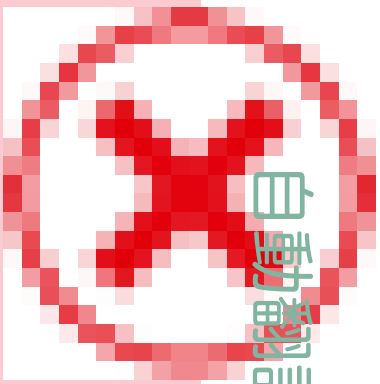
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
承認ルール			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

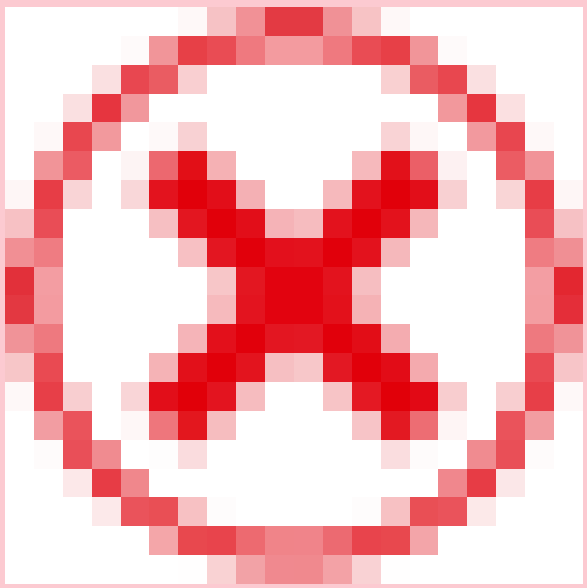
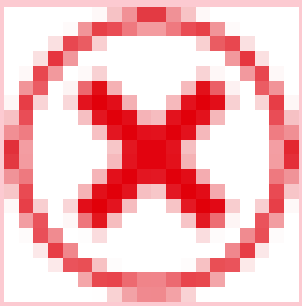
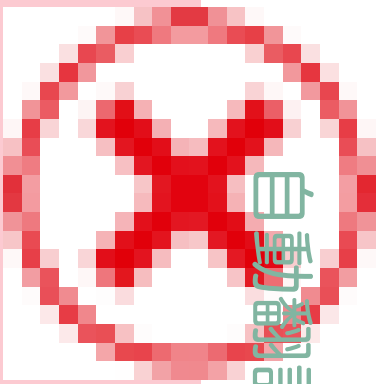
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
コンテナセキュリティ統合			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

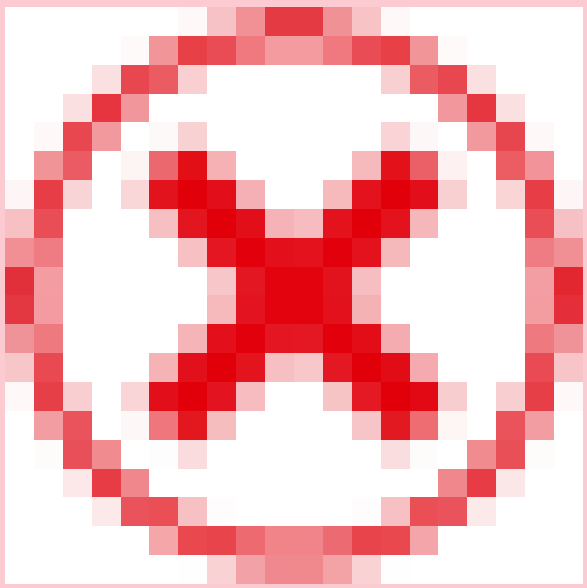
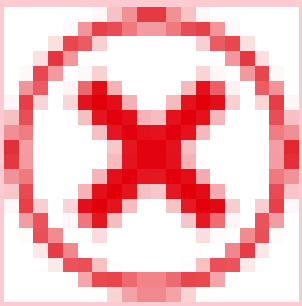
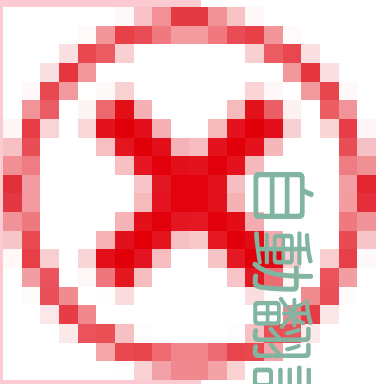
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
脆弱性一致アイテムの自動クローズ			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_container.read_assig

その他のロールの情報：

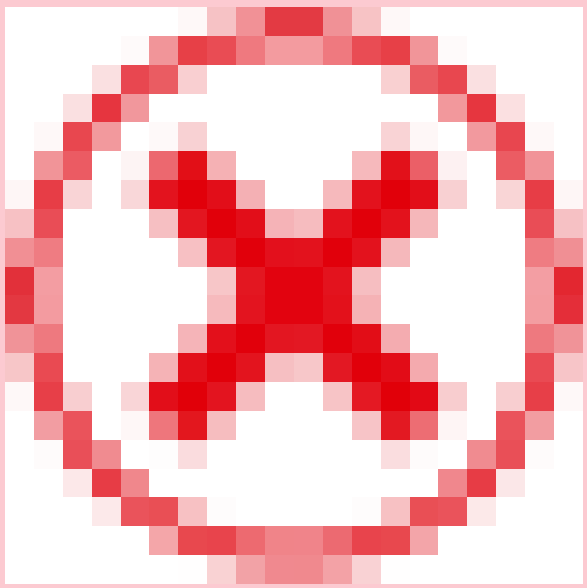
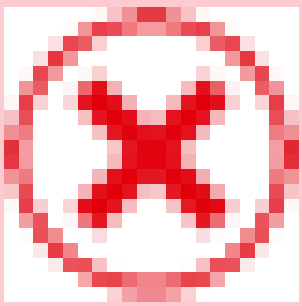
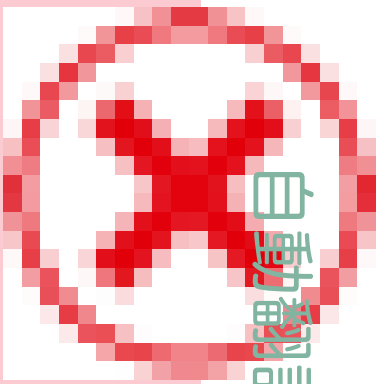
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.read_auto_exception_rule

(続く)

モジュール	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assigned
正規化された重大度マップ			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：**sn_vul_container.read_auto_exception_rule**

モジュールアクセス：**sn_vul_container.read_auto_exception_rule**

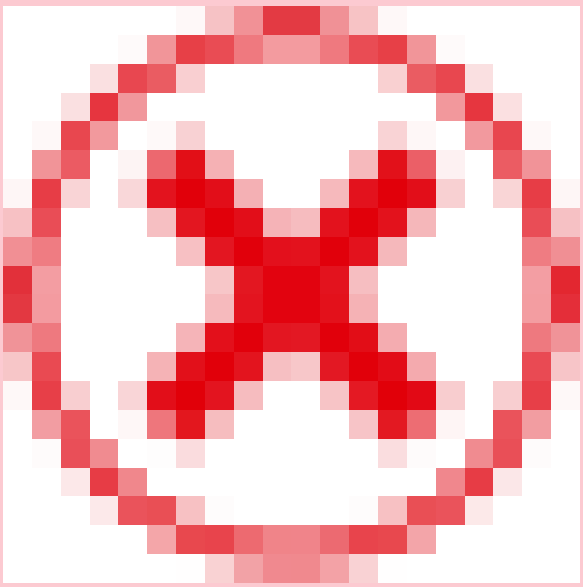
その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

モジュール	**sn_vul_container.read_auto_exception_rule**
(メインアプリグループ)	
概要	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：**sn_vul_container.read_auto_exception_rule**

その他のロールの情報：

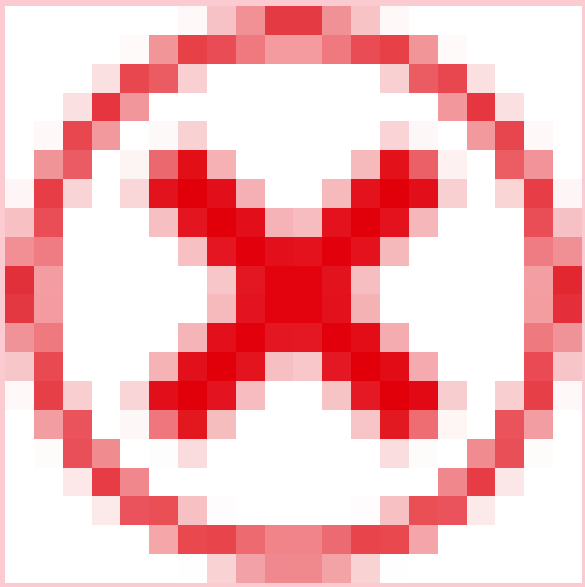
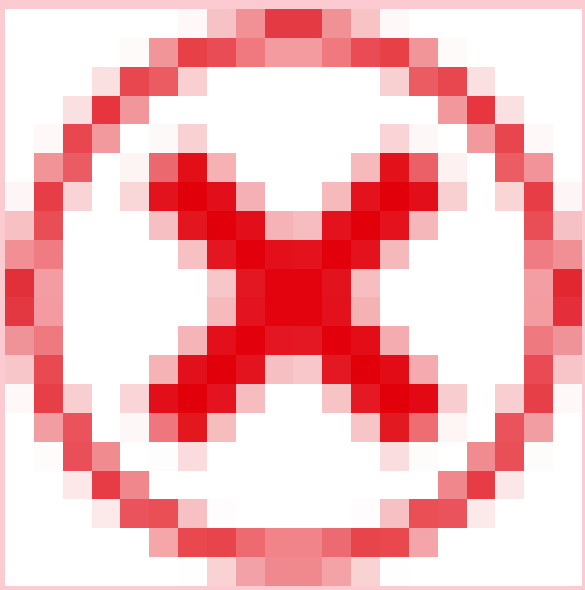
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

(続く)

モジュール	sn_vul_container.read_auto_exception_rule
自分の承認	
コンテナ脆弱性一致アイテム	
自分にアサイン済み	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：**sn_vul_container.read_auto_exception_rule**

その他のロールの情報：

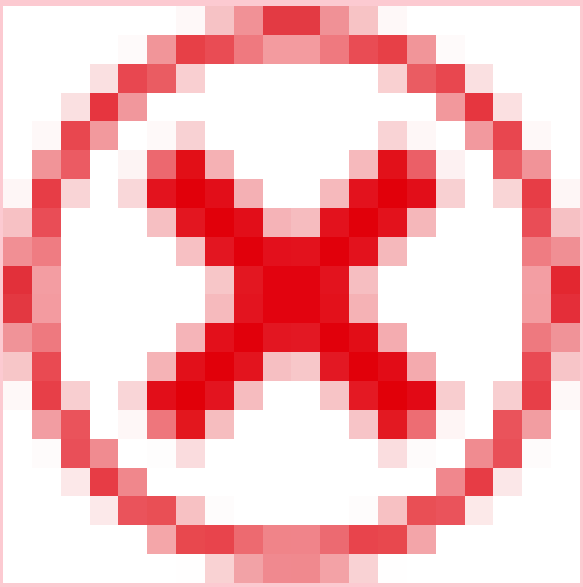
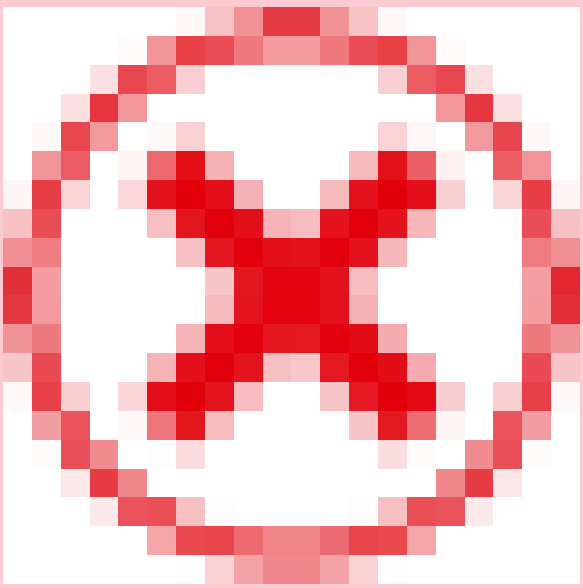
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

(続く)

モジュール	sn_vul_container.read_auto_exception_rule
所属グループにアサイン済み	
重大および高リスク	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：**sn_vul_container.read_auto_exception_rule**

その他のロールの情報：

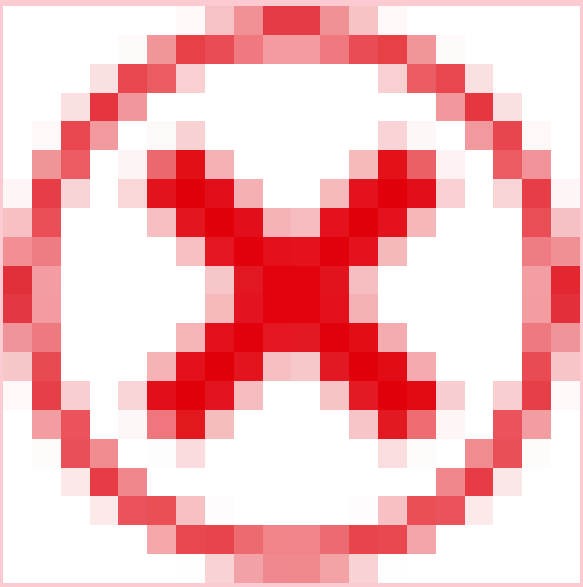
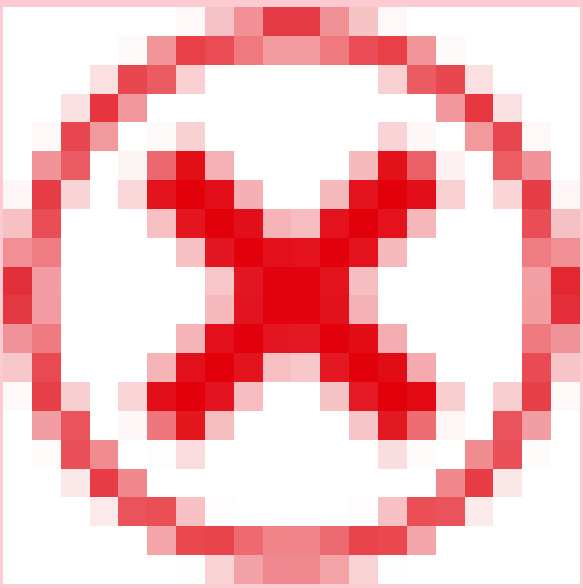
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

(続く)

モジュール	sn_vul_container.read_auto_exception_rule
エクスプロイト可能	
該当 CI 確認中	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：**sn_vul_container.read_auto_exception_rule**

その他のロールの情報：

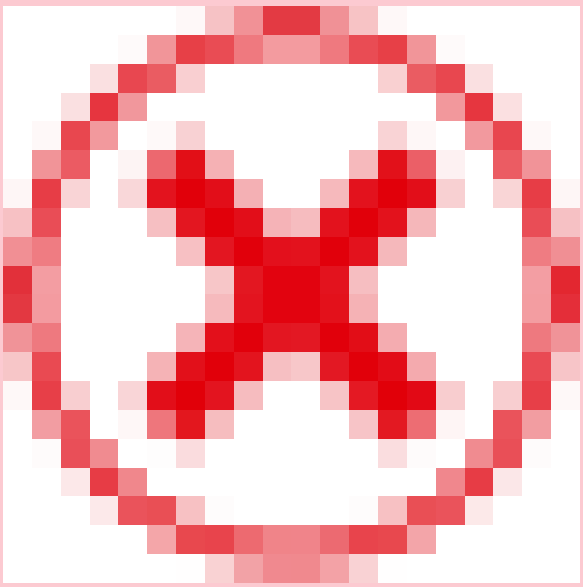
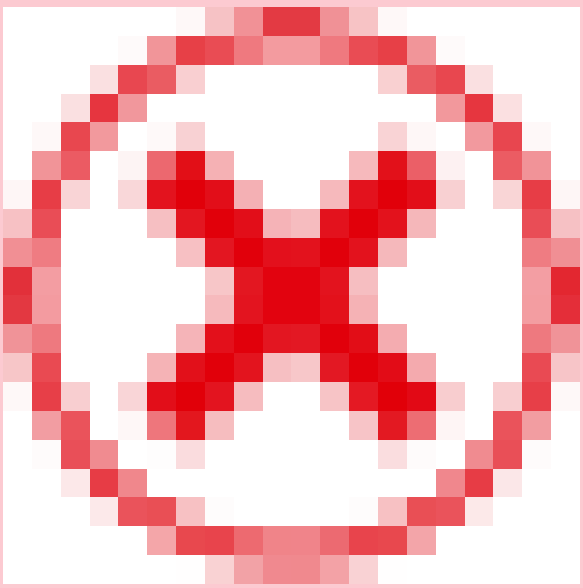
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

(続く)

モジュール	**sn_vul_container.read_auto_exception_rule**
CI 不明	
すべて	
ライブラリ	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：**sn_vul_container.read_auto_exception_rule**

その他のロールの情報：

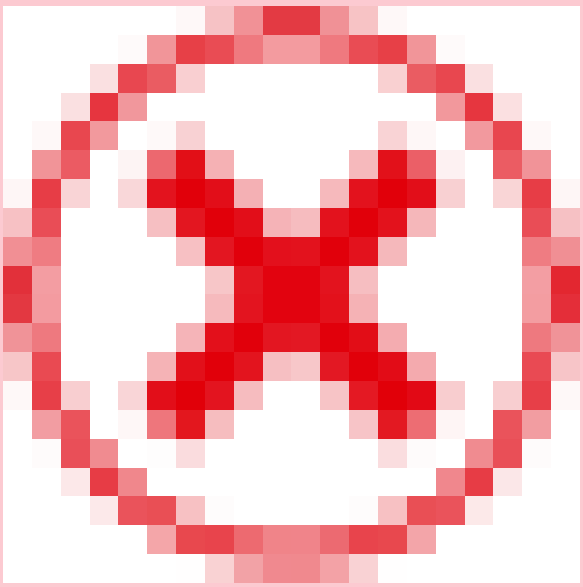
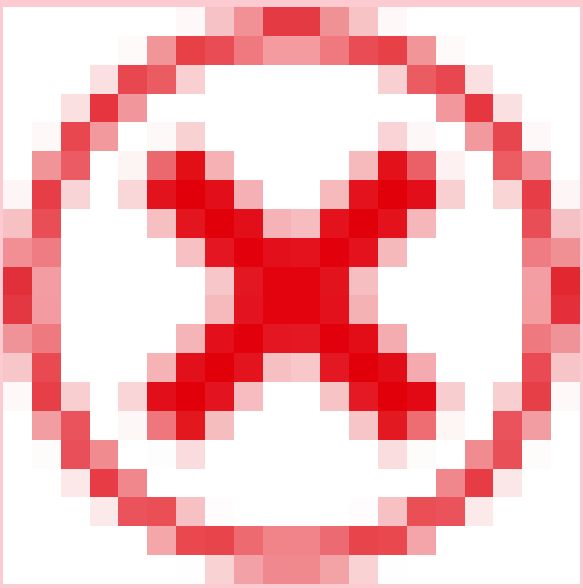
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

(続く)

モジュール	**sn_vul_container.read_auto_exception_rule**
NVD	
サードパーティ	
管理	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：**sn_vul_container.read_auto_exception_rule**

その他のロールの情報：

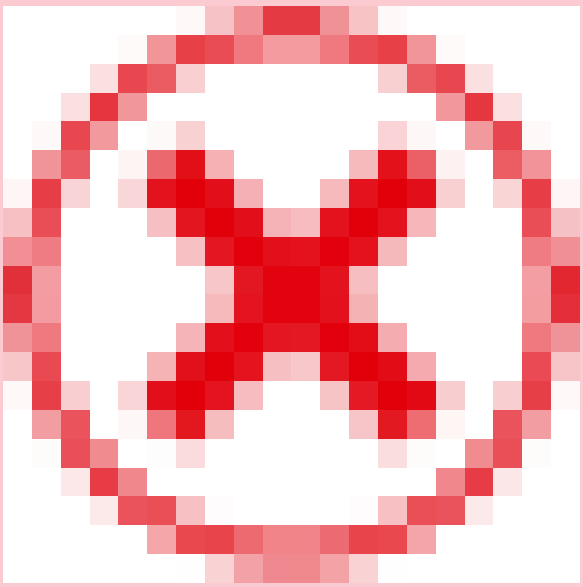
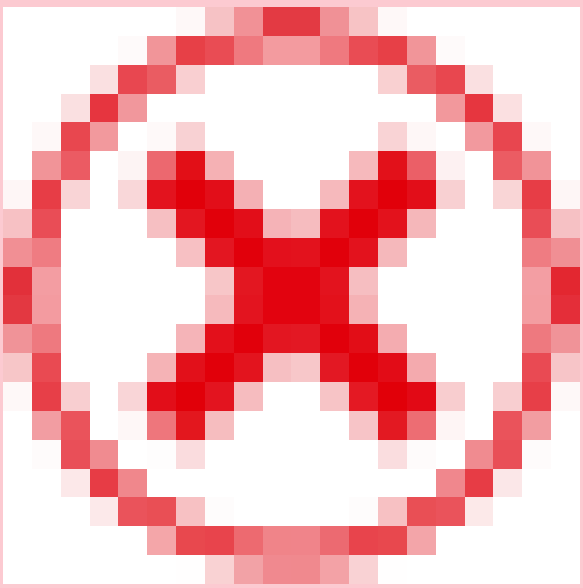
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

(続く)

モジュール	sn_vul_container.read_auto_exception_rule
アサインルール	
脆弱性算出	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：**sn_vul_container.read_auto_exception_rule**

その他のロールの情報：

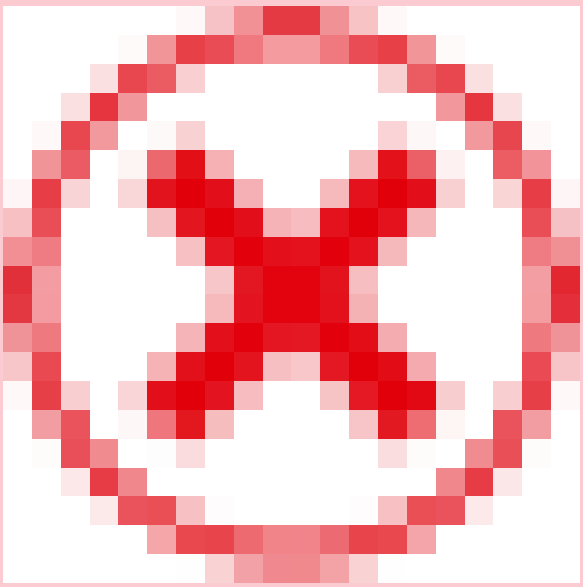
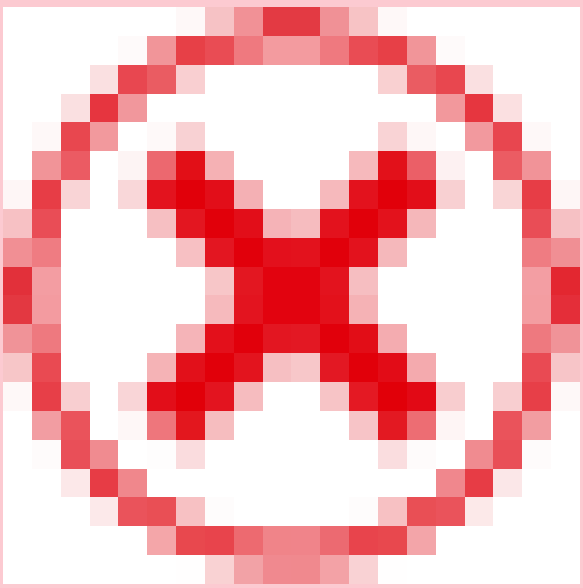
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

(続く)

モジュール	**sn_vul_container.read_auto_exception_rule**
修復ターゲットルール	
VI の粒度の構成	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：**sn_vul_container.read_auto_exception_rule**

その他のロールの情報：

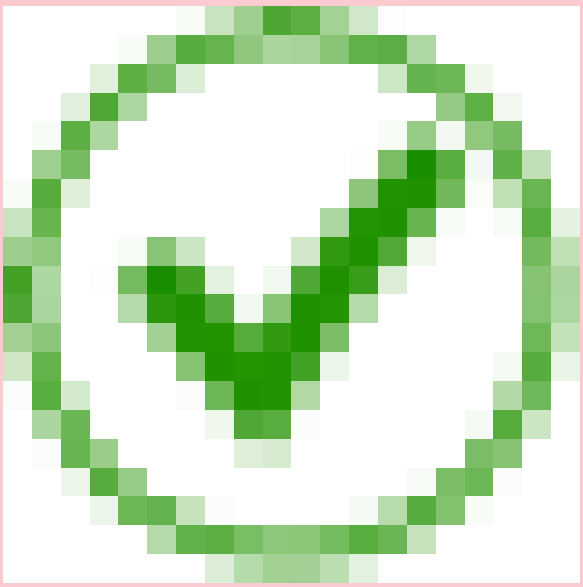
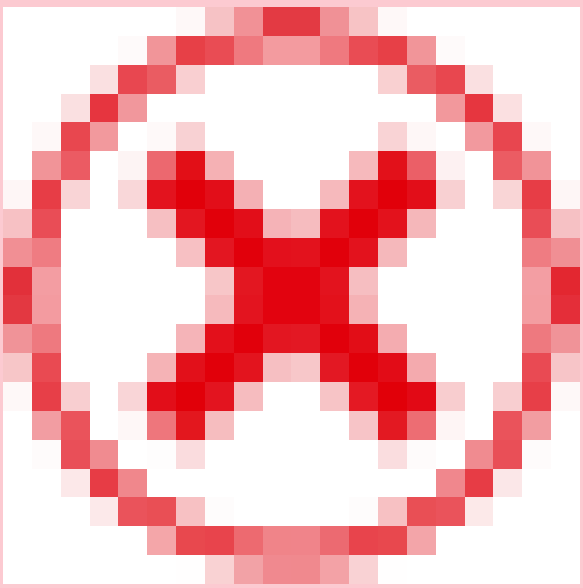
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

(続く)

モジュール	sn_vul_container.read_auto_exception_rule
例外ルール	
承認ルール	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：**sn_vul_container.read_auto_exception_rule**

その他のロールの情報：

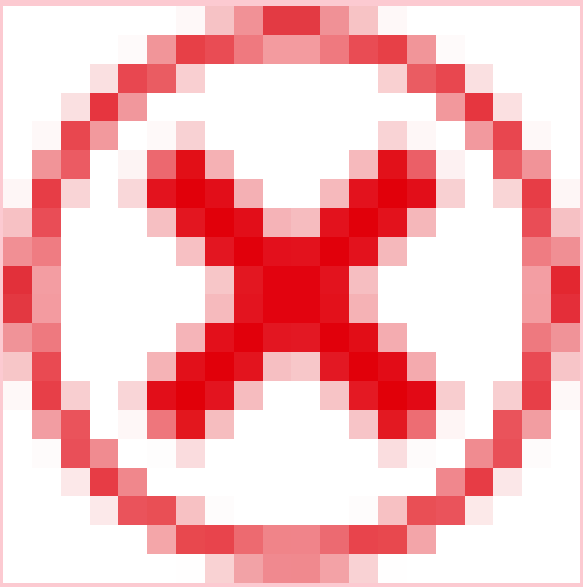
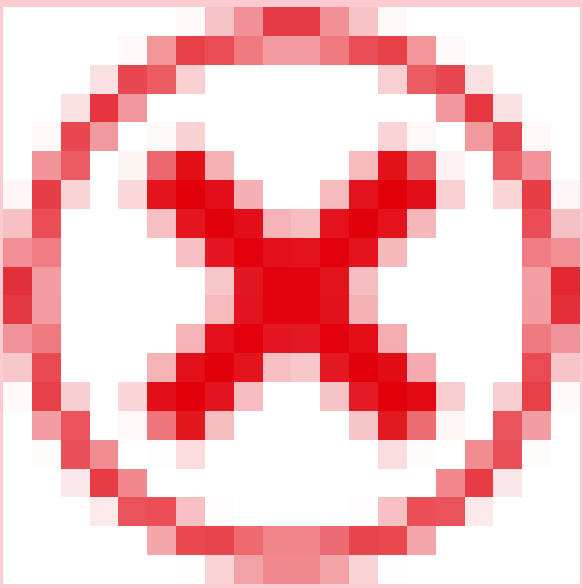
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

(続く)

モジュール	sn_vul_container.read_auto_exception_rule
コンテナセキュリティ統合	
脆弱性一致アイテムの自動クローズ	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：**sn_vul_container.read_auto_exception_rule**

その他のロールの情報：

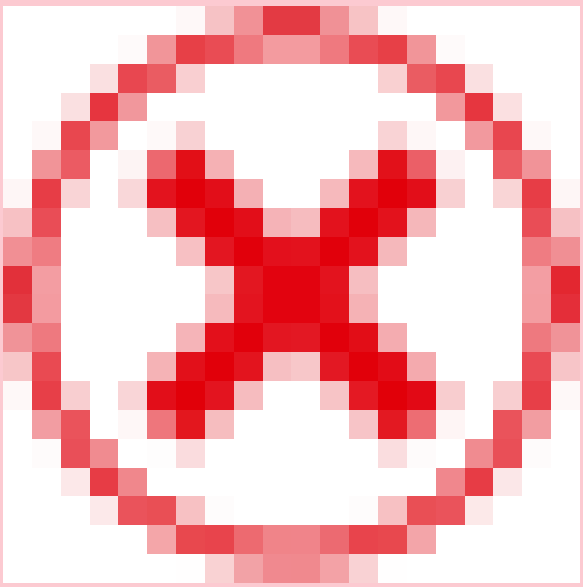
sn_sec_cmn.manage_approval_rules、sn_vul_container.configure_integrations、sn_vul_co

sn_vul_container.exception_approver、sn_vul_container.false_positive_approver、sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi、sn_vul_container.manage_normalized_seve

sn_vul_container.manage_risk_score_configuration、sn_vul_container.read_all、sn_vul_co

(続く)

モジュール	sn_vul_container.read_auto_exception_rule
正規化された重大度マップ	

自動翻訳

[End]

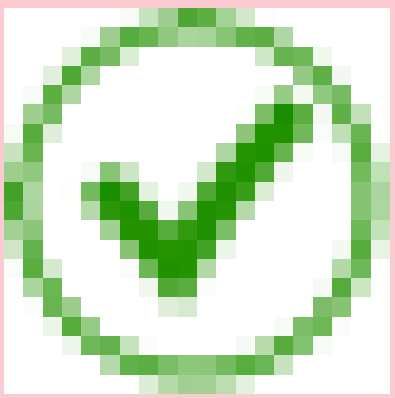
[store-future: BEGIN review]

DLP 管理のロール別のモジュールアクセス

DLP 管理では、特定のロールがアクセスできるメニューアイテムが表示されます。

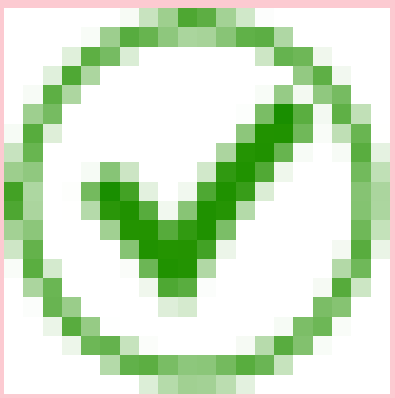
モジュール	sn_dlir.analyst
(メインアプリグループ)	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_dlir.analyst
デフォルト構成	
アサインルール	
応答期日ルール	
メールテンプレート	

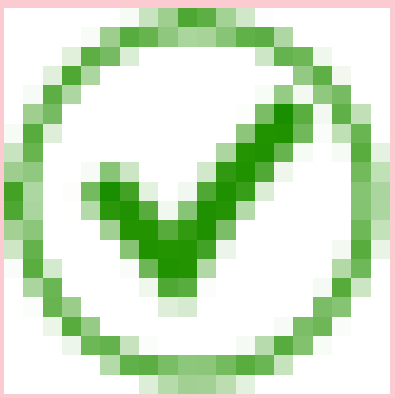
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_dlir.analyst
アセスメント	
インシデント応答オプション	
年齢グラフ構成	
委任者構成	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_dlir.analyst
カスタム状況	
反復違反識別ルール	
カスタムフィールド	
詳細設定	
インシデントアクセス制限	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

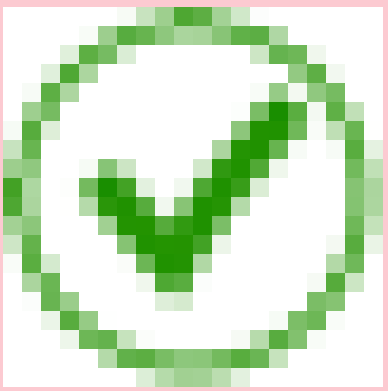
モジュール	sn_dlir.analyst
レコードレベル制限	
フィールドレベル制限	

[End]

[store-future: BEGIN review]

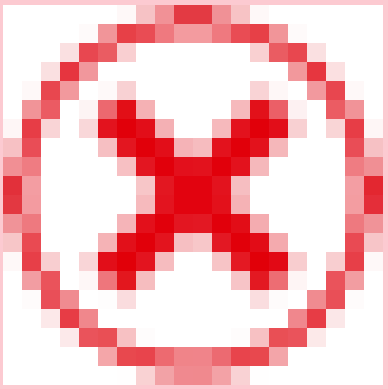
DLP インシデント管理のロール別のモジュールアクセス

DLP インシデント管理では、特定のロールがアクセスできるメニューアイテムが表示されます。

モジュール	sn_dlir.analyst
(メインアプリグループ)	
DLP 運用ポータル	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

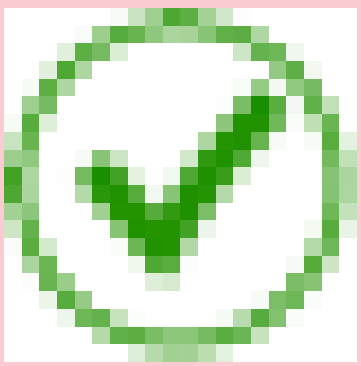
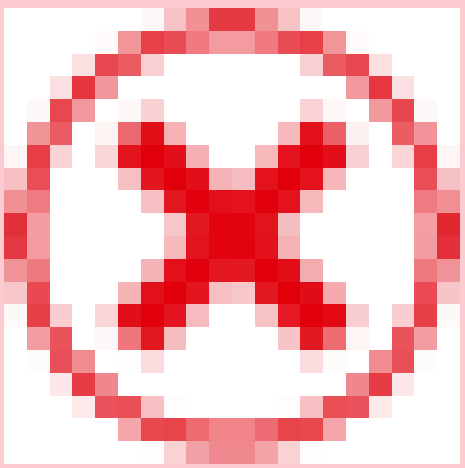
モジュール	sn_dlir.analyst
DLP エンドユーザーポータル	
DLP ダッシュボード	

[End]

[store-future: BEGIN review]

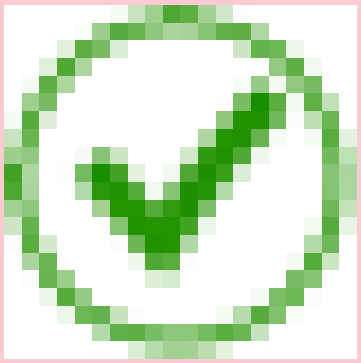
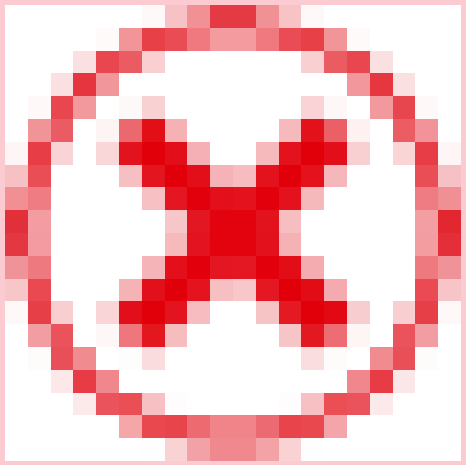
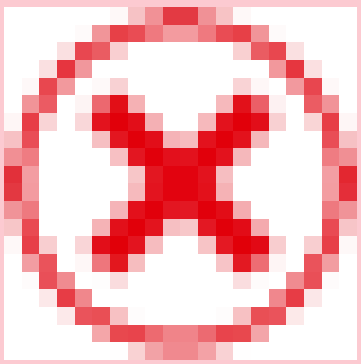
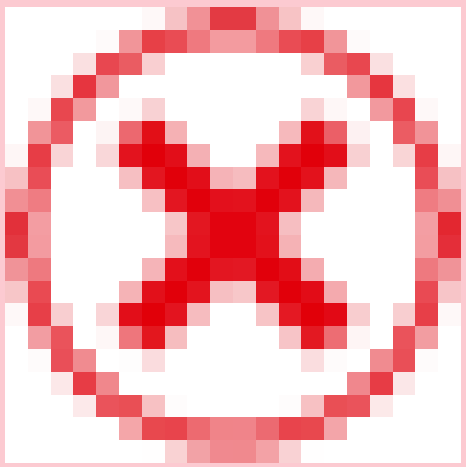
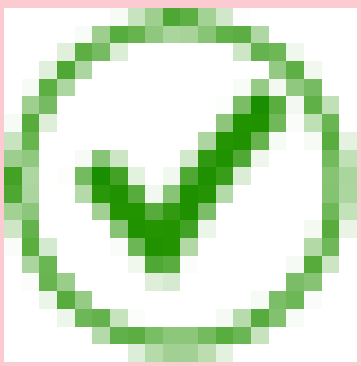
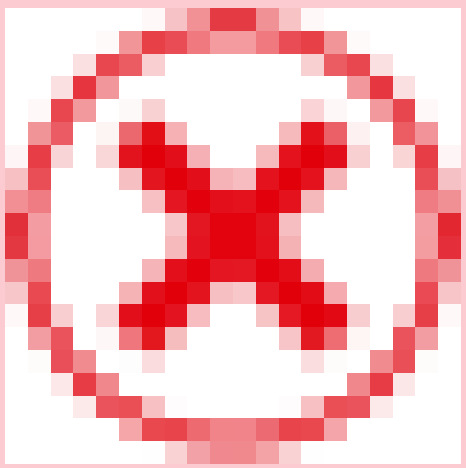
データ認定のロール別のモジュールアクセス

データ認定では、特定のロールがアクセスできるメニューアイテムが表示されます。

モジュール	certification_admin	certification_filter_admin
(メインアプリグループ)		
概要		

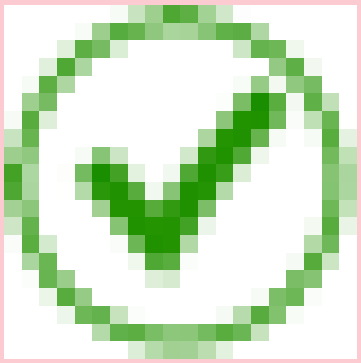
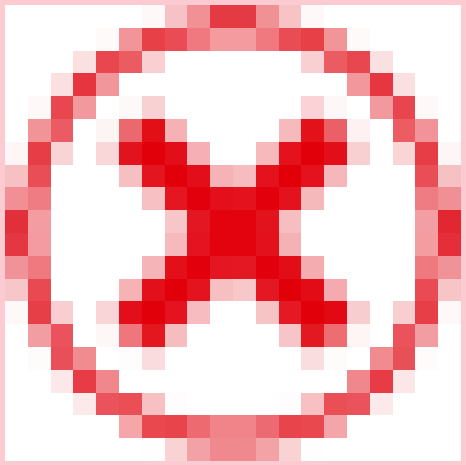
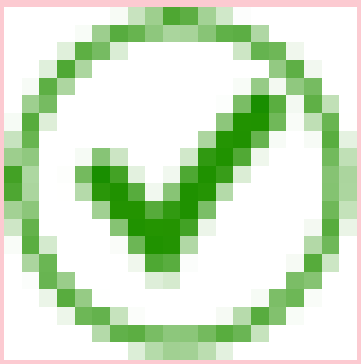
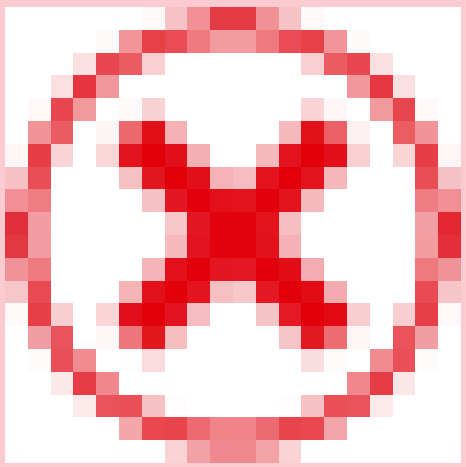
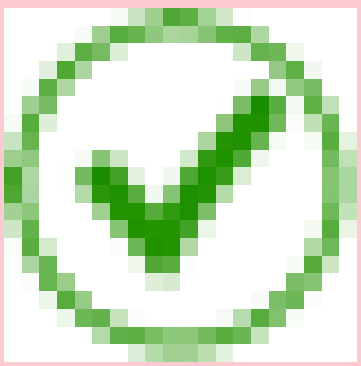
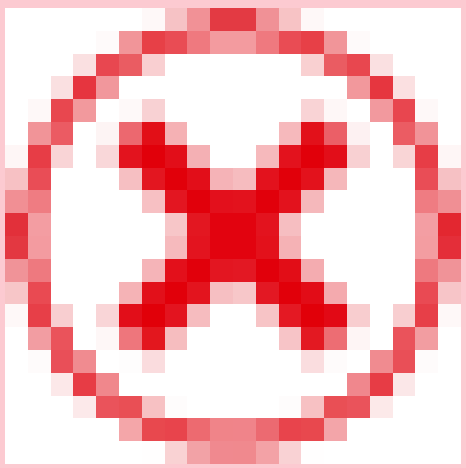
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	certification_admin	certification_filter_admin
はじめに		
タスク		
自分のタスク		
オープン		

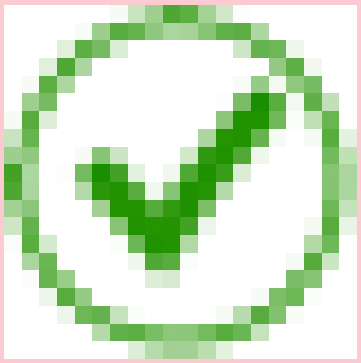
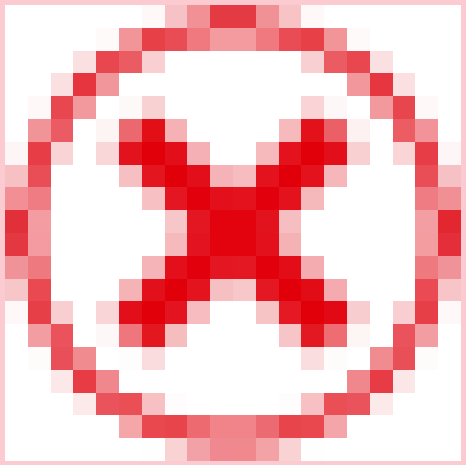
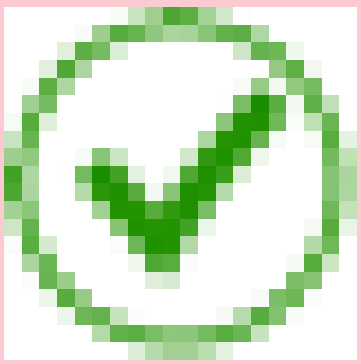
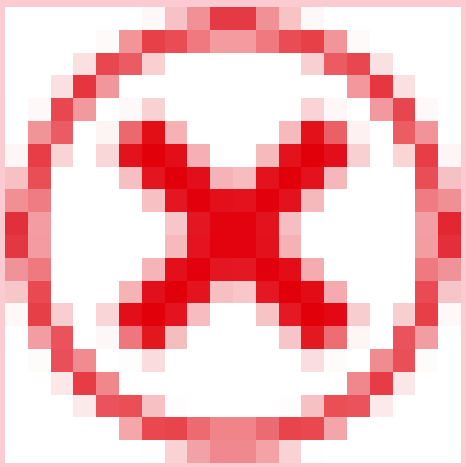
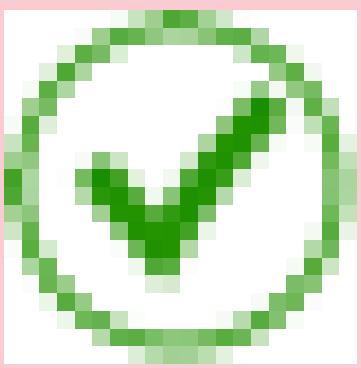
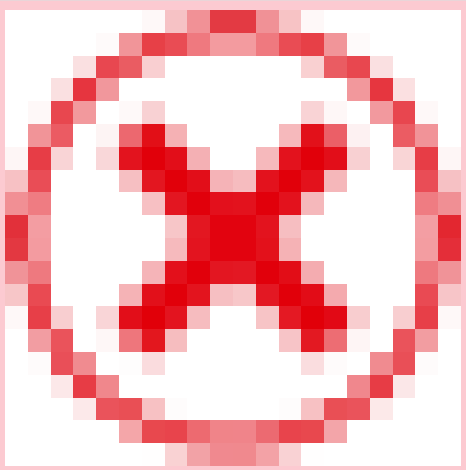
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	certification_admin	certification_filter_admin
すべてのタスク		
認定		
認定		
処理待ち		

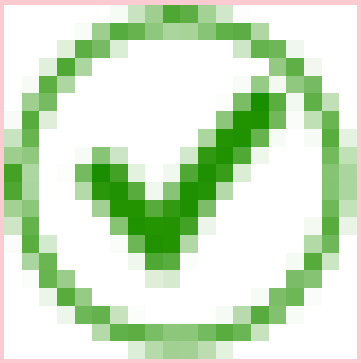
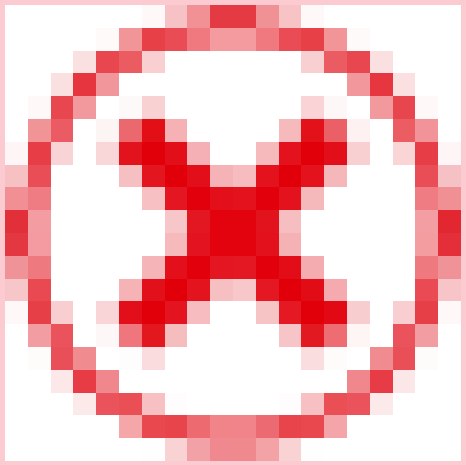
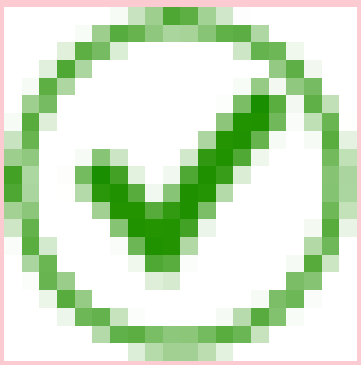
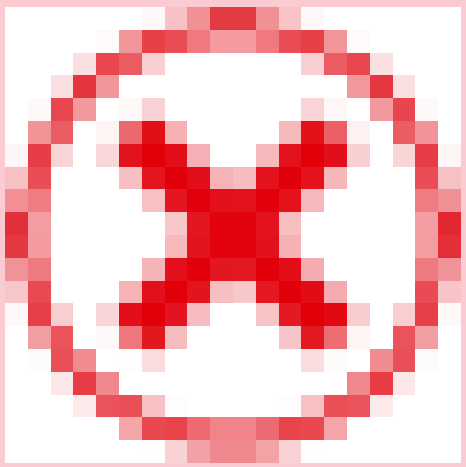
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	certification_admin	certification_filter_admin
すべて		
スケジュール		
新規作成		
スケジュール定義		

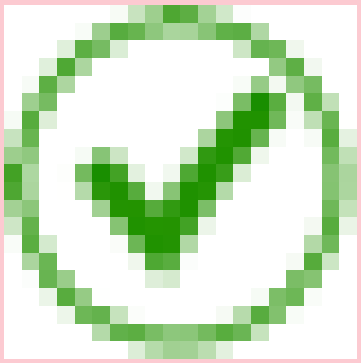
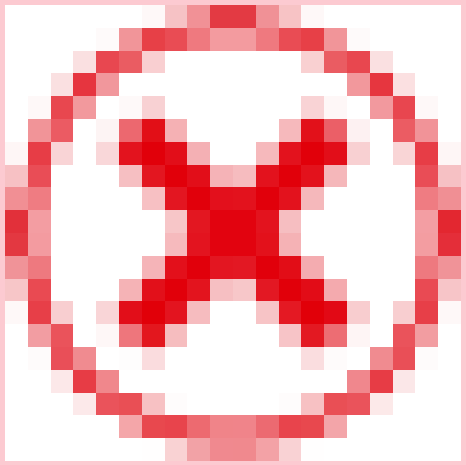
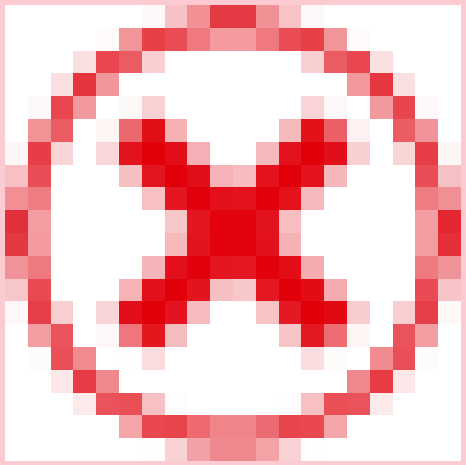
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	certification_admin	certification_filter_admin
認定フィルター		
インスタンス		
監査結果		
監査		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	certification_admin	certification_filter_admin
監査定義		
監査インスタンス		

[End]

[store-future: BEGIN review]

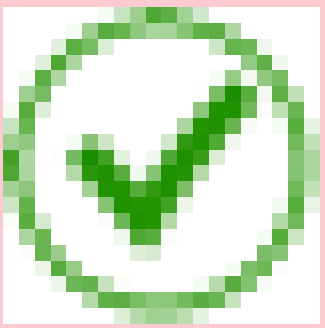
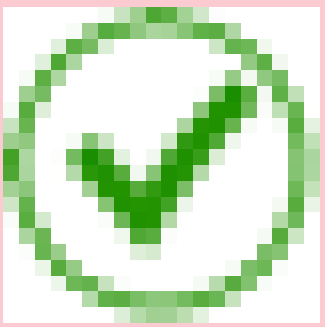
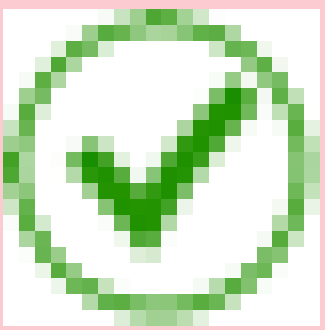
IBM QRadar 統合のロール別のモジュールアクセス

IBM QRadar 統合では、特定のロールがアクセスできるメニューアイテムが表示されます。

モジュール	sn_si.analyst
(メインアプリグループ)	
IBM QRadar プロファイル	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_si.analyst
IBM QRadar 違反インポート	
タスクに対する IBM QRadar 違反	
IBM QRadar フィールド変換	
IBM QRadar 統合の設定	

[End]

[store-future: BEGIN review]

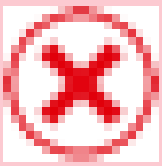
MISP 統合のロール別のモジュールアクセス

MISP 統合では、特定のロールがアクセスできるメニューアイテムが表示されます。

モジュール	sn_si.admin	sn_si.analyst	sn_ti.admin	sn_ti.read	sn_ti.write
(メインアプリグループ)					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_si.admin	sn_si.analyst	sn_ti.admin	sn_ti.read	sn_ti.write
統合の設定					
サイティング検索構成					
イベントの自動作成プロファイル					
イベントの自動作成キュー					
MISP イベントデータ					
関連付けられた MISP イベント					
MISP ユーザー情報					

[End]

[store-future: BEGIN review]

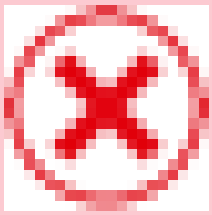
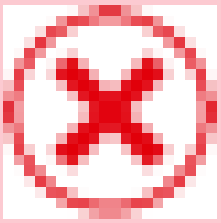
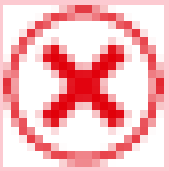
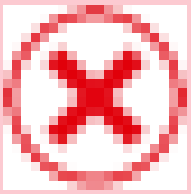
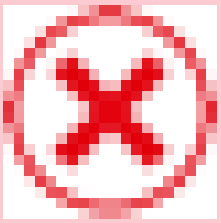
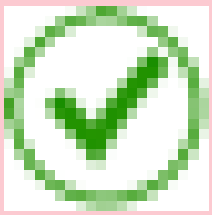
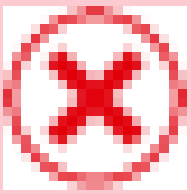
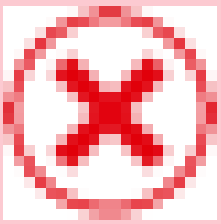
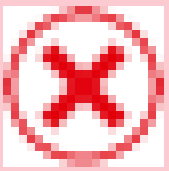
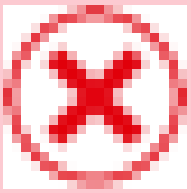
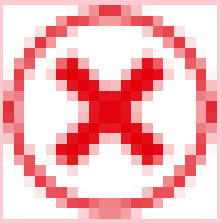
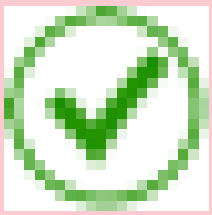
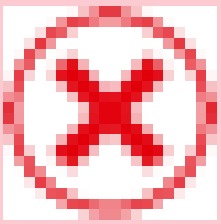
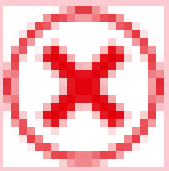
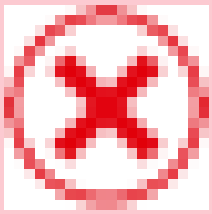
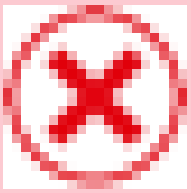
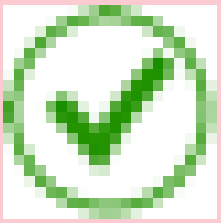
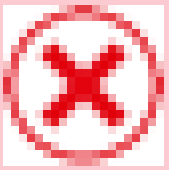
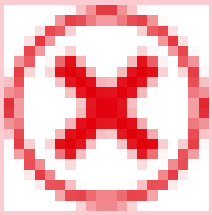
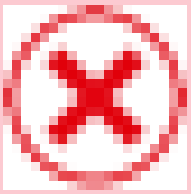
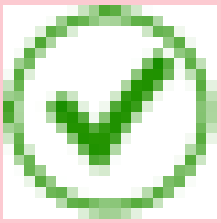
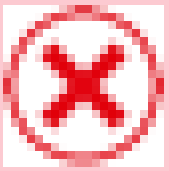
Microsoft Azure Defender for IoT のロール別のモジュールアクセス

Microsoft Azure Defender for IoT では、特定のロールがアクセスできるメニューアイテムが表示されます。

モジュール	cmdb_inst_admin	cmdb_ot_admin	connection_admin	import_admin
(メインアプリグループ)				

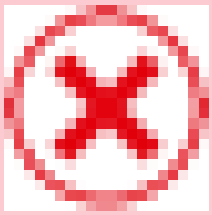
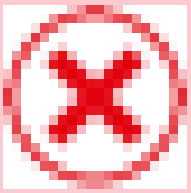
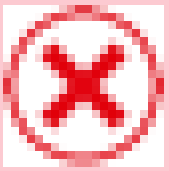
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	cmdb_inst_admin	cmdb_ot_admin	connection_admin	import_admin
セットアップ				
データソース				
統合ハブ ETL				
スケジュールをインポート				
プロパティ				
接続および資格情報				
接続および資格情報エイリアス				
認証情報				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

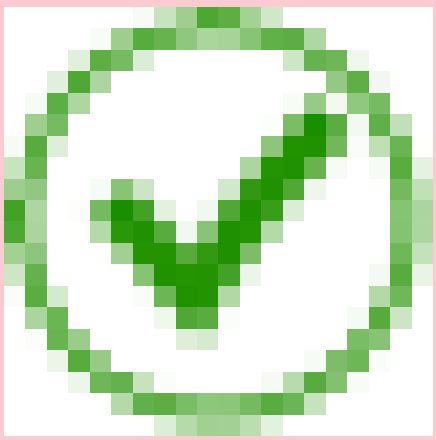
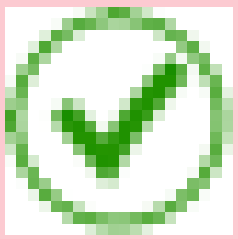
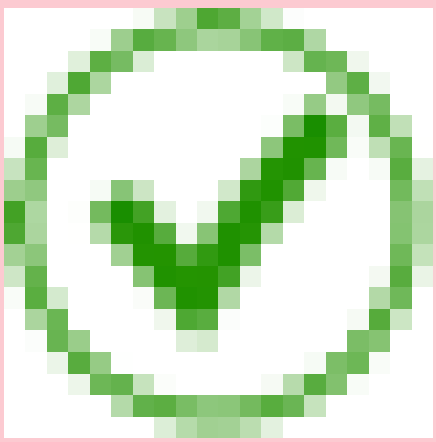
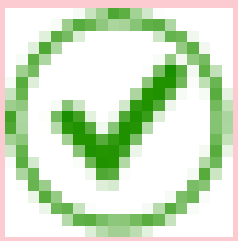
モジュール	cmdb_inst_admin	cmdb_ot_admin	connection_admin	import_admin
接続				

[End]

[store-future: BEGIN review]

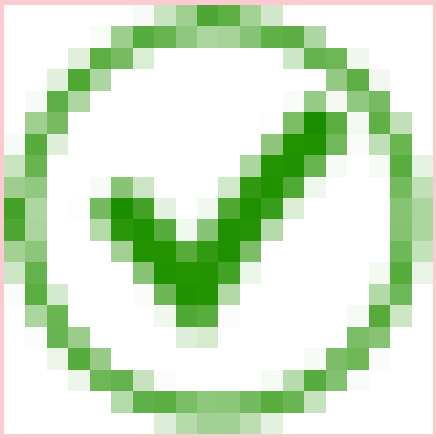
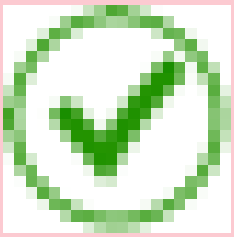
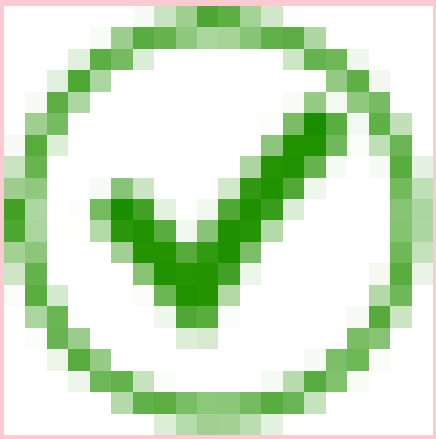
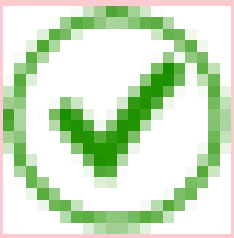
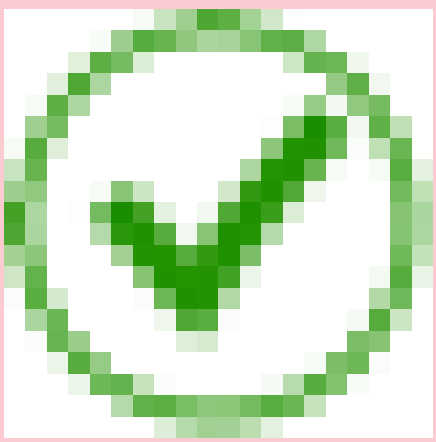
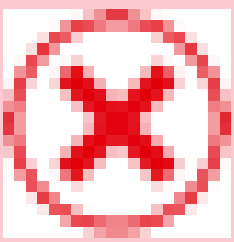
Qualys Vulnerability Integration のロール別のモジュールアクセス

Qualys Vulnerability Integration では、特定のロールがアクセスできるメニューアイテムが表示されます。

モジュール	sn_vul.configure_qualys_integration	sn_vul_qualys.read
(メインアプリグループ)		
概要		
統合実行状況		

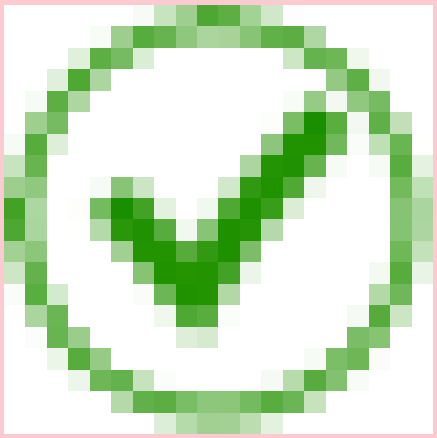
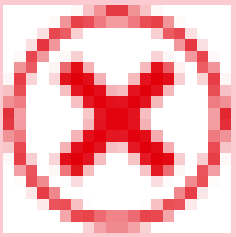
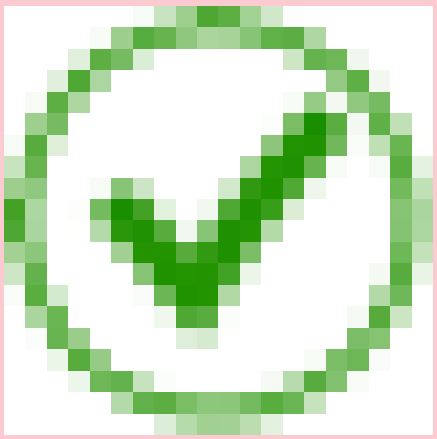
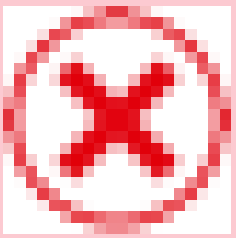
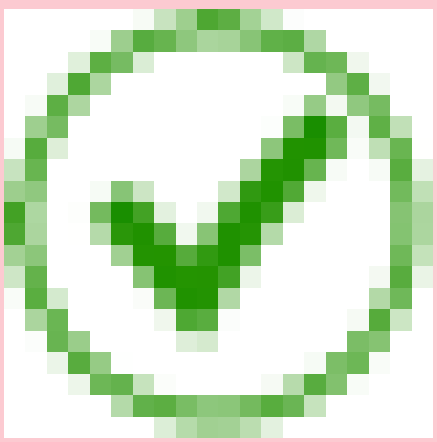
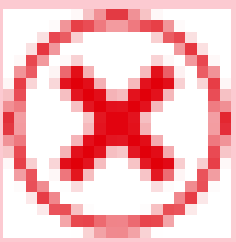
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_vul.configure_qualys_integration	sn_vul_qualys.read
スキャナーアプライアンス		
検索リスト		
管理		
統合インスタンス		

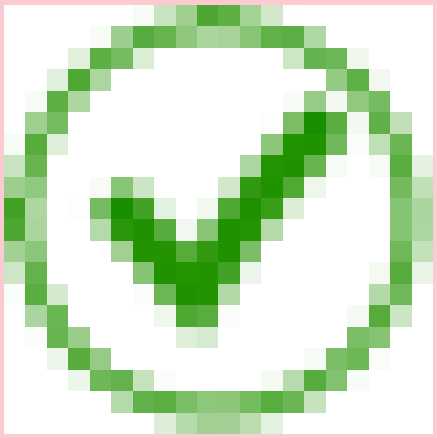
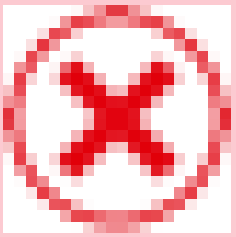
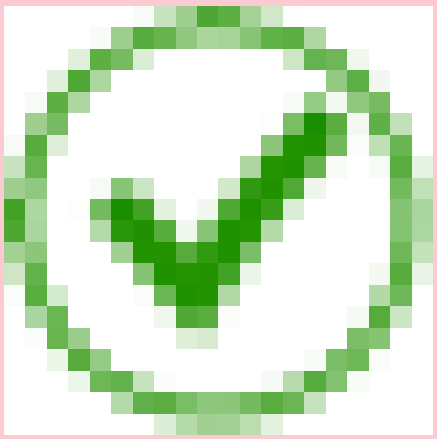
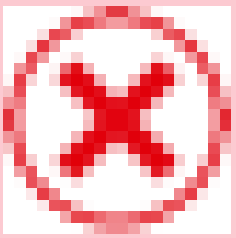
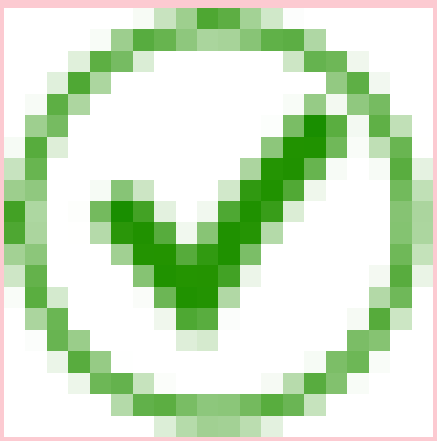
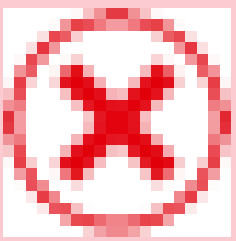
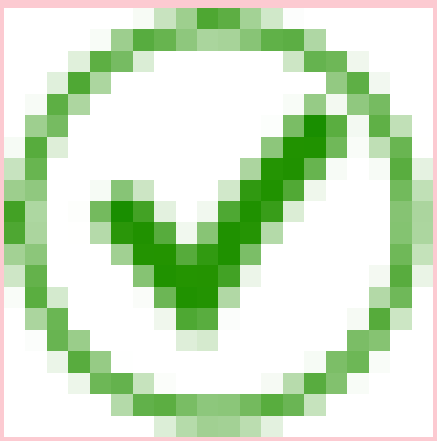
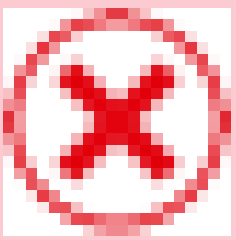
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_vul.configure_qualys_integration	sn_vul_qualys.read
プライマリ統合		
サポート統合		
インポートセットテーブル		
ホストインポート		

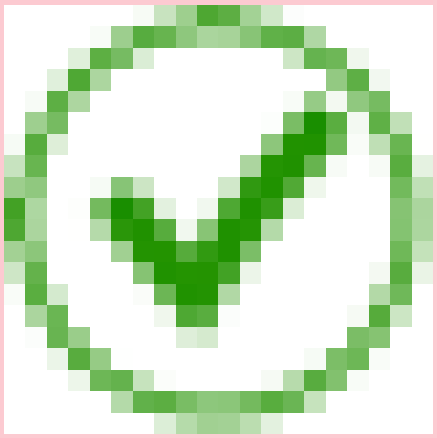
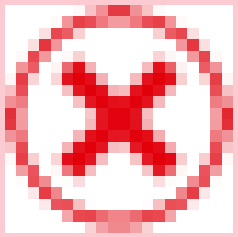
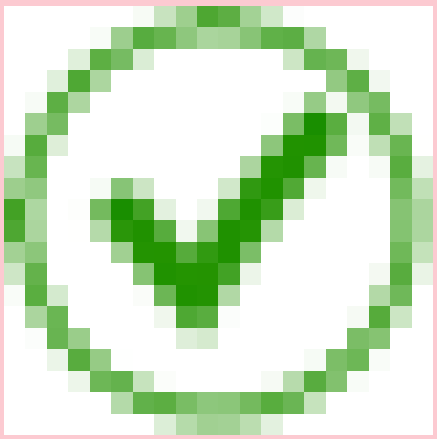
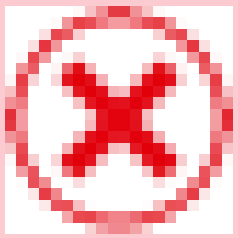
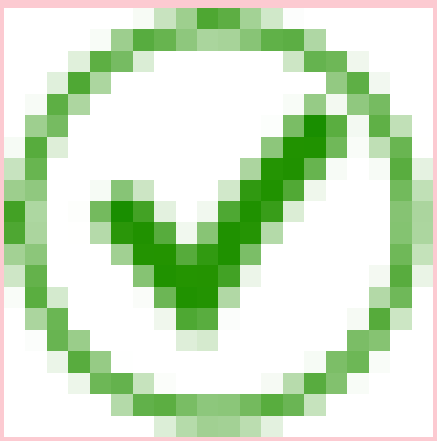
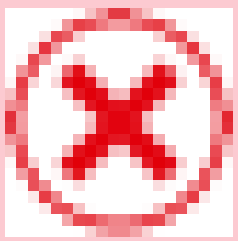
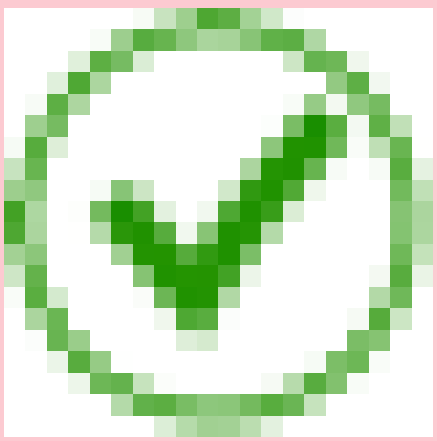
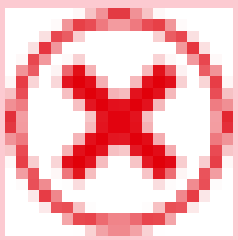
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_vul.configure_qualys_integration	sn_vul_qualys.read
ホスト検出リストインポート		
ナレッジベースのインポート		
チケットリストのインポート		
動的検索リストインポート		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_vul.configure_qualys_integration	sn_vul_qualys.read
静的検索リストインポート		
資産グループインポート		
アプライアンスインポート		
ホスト検出ページネーションインポート		

自動翻訳

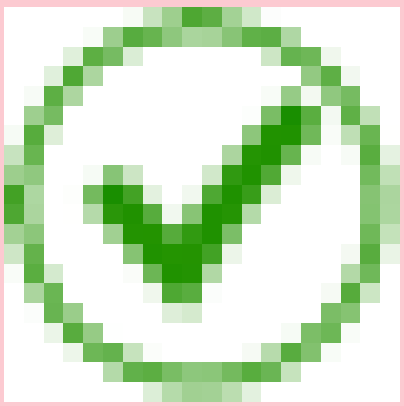
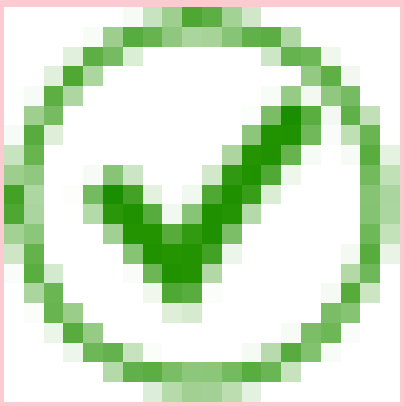
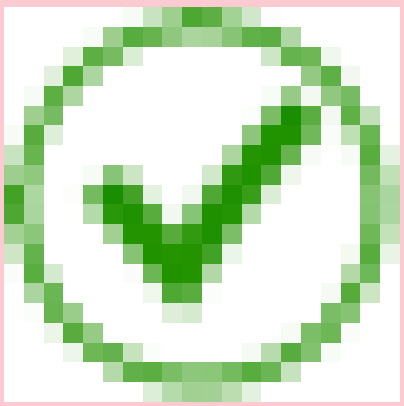
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[End]

[store-future: BEGIN review]

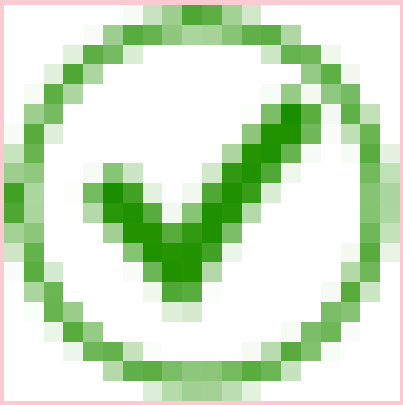
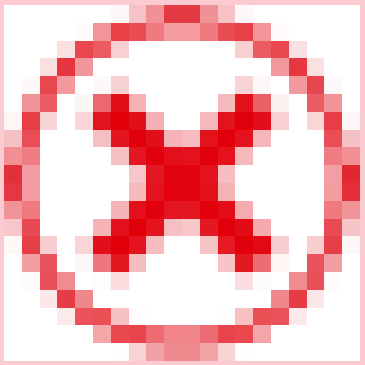
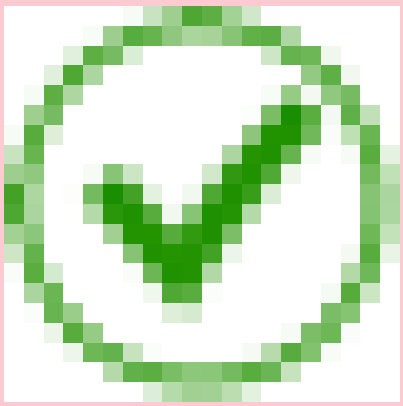
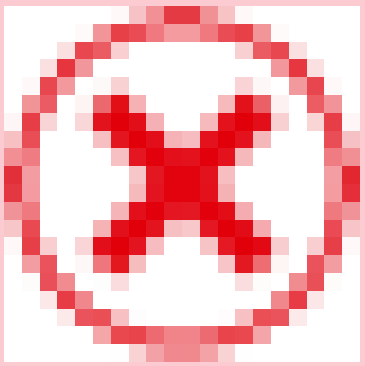
Rapid7 脆弱性統合のロール別のモジュールアクセス

Rapid7 脆弱性統合では、特定のロールがアクセスできるメニューアイテムが表示されます。

モジュール	sn_vul_r7.admin	sn_vul_r7.read
(メインアプリグループ)		
統合実行状況		
サイト		
ソリューション		
管理		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_vul_r7.admin	sn_vul_r7.read
統合		
構成		

[End]

[store-future: BEGIN review]

セキュリティインシデントのロール別のモジュールアクセス

セキュリティインシデントでは、特定のロールがアクセスできるメニューアイテムが表示されます。

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_admin、sn_si.n

その他のロールの情報：

sn_si.special_access、sn_si_approver_user

モジュール	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.external	sn_si.knowledge_admin	sn_si
(メインアプリグループ)							

自動翻訳

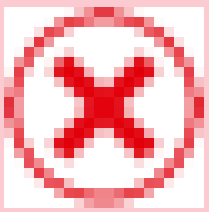
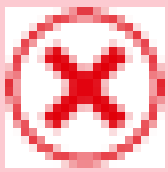
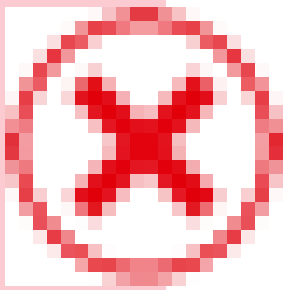
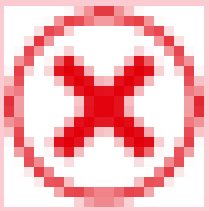
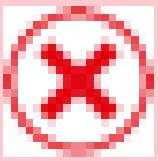
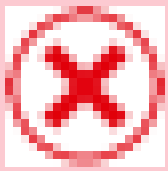
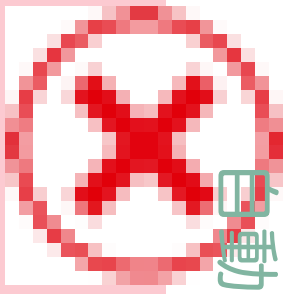
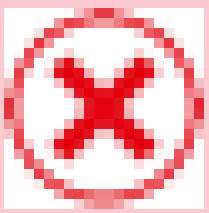
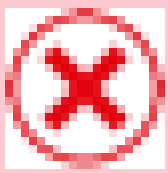
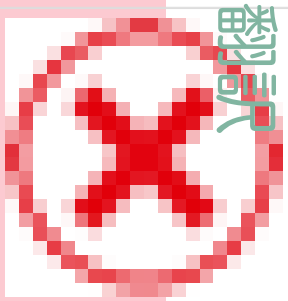
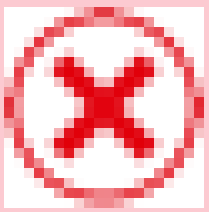
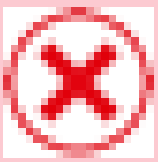
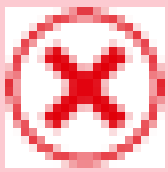
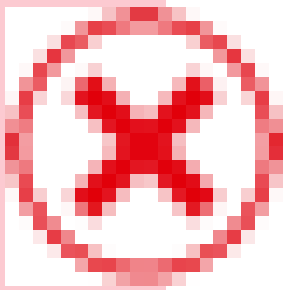
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_admin、sn_si.m

その他のロールの情報：

sn_si.special_access、sn_si_approver_user

(続く)

モジュール	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.external	sn_si.knowledge_admin	sn_si
インシデント新規 UI							
サービスへの影響							
概要							
リアルタイム							
インシデント							

自動翻訳

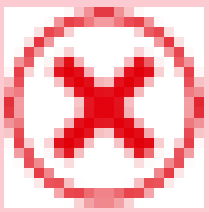
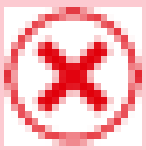
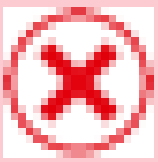
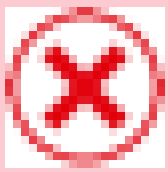
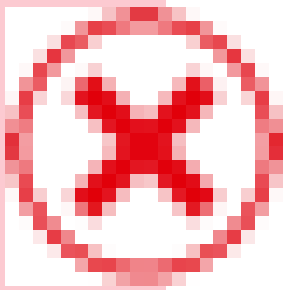
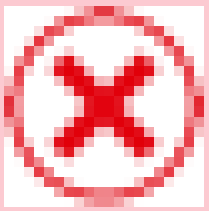
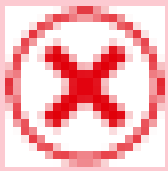
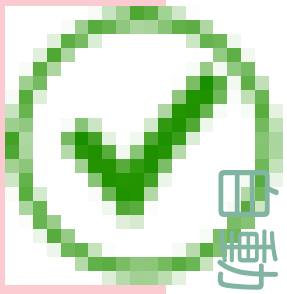
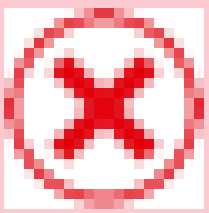
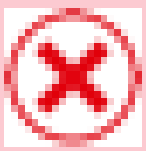
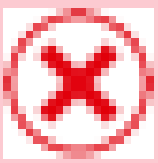
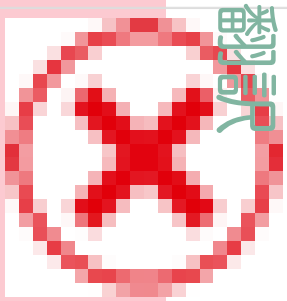
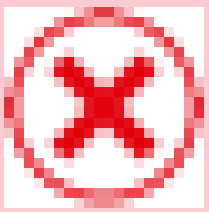
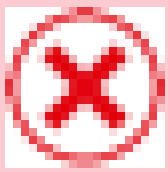
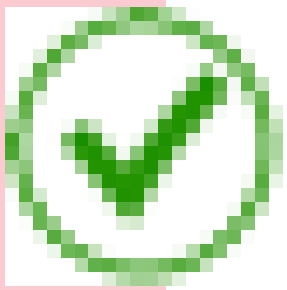
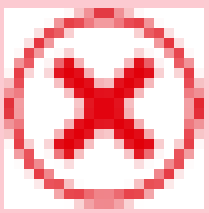
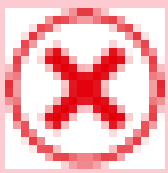
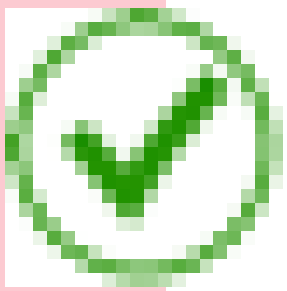
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_admin、sn_si.m

その他のロールの情報：

sn_si.special_access、sn_si_approver_user

(続く)

モジュール	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.external	sn_si.knowledge_admin	sn_si
閲覧可能なインシデント							
自分にアサイン済み							
My Work							
チームにアサイン済み							
オープンインシデントを表示							

自動翻訳

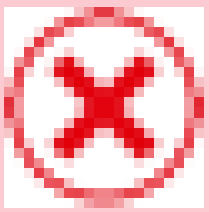
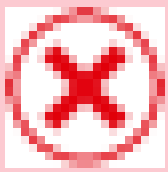
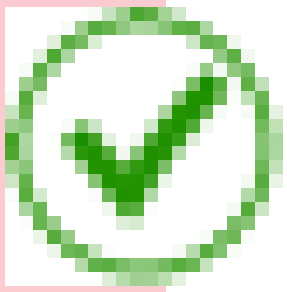
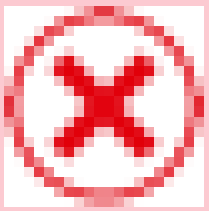
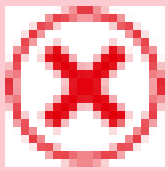
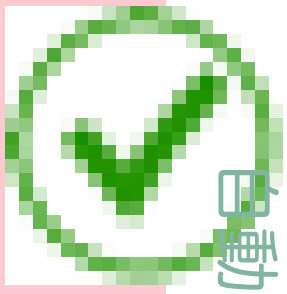
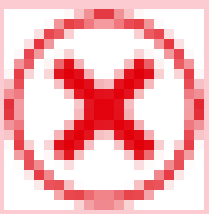
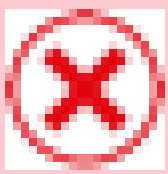
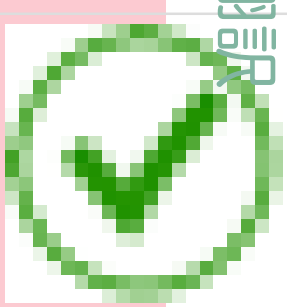
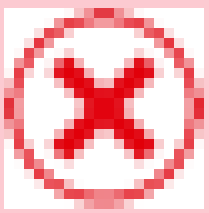
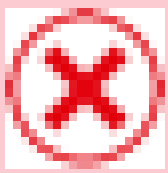
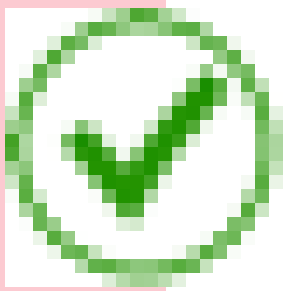
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_admin、sn_si.m

その他のロールの情報：

sn_si.special_access、sn_si_approver_user

(続く)

モジュール	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.external	sn_si.knowledge_admin	sn_si
すべてのインシデントを表示							
未アサインのインシデント							
応答タスク							
自分にアサイン済み							
チームにアサイン済み							

自動翻訳

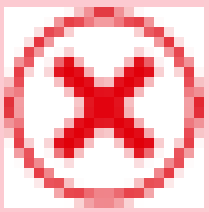
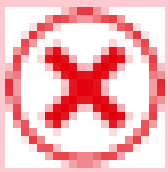
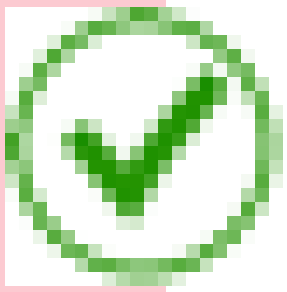
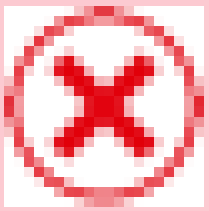
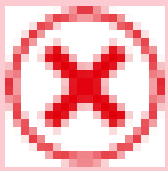
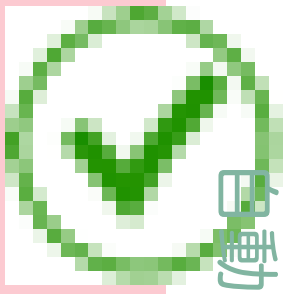
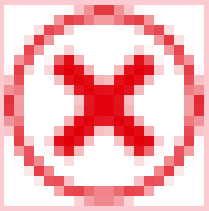
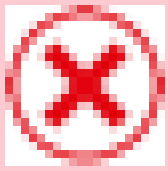
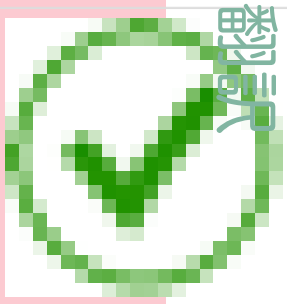
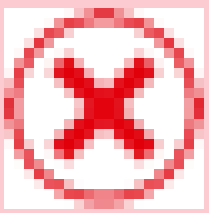
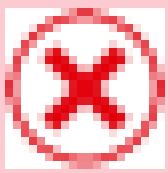
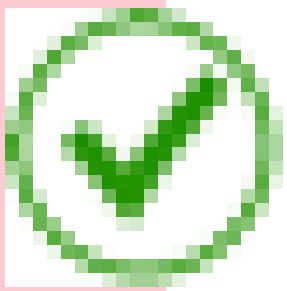
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_admin、sn_si.m

その他のロールの情報：

sn_si.special_access、sn_si_approver_user

(続く)

モジュール	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.external	sn_si.knowledge_admin	sn_si
オープンタスクを表示							
すべてのタスクを表示							
未アサインタスク							
受け付けた要求							
自分にアサイン済み							

自動翻訳

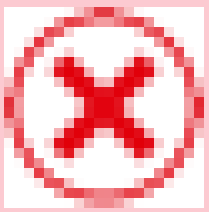
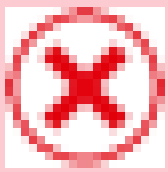
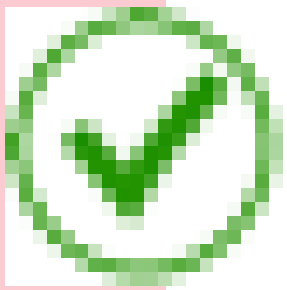
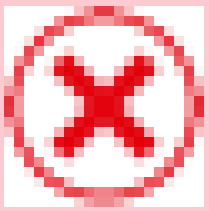
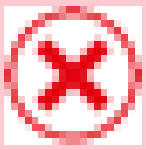
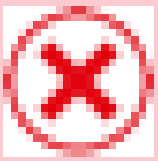
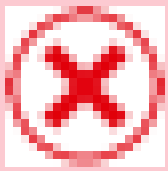
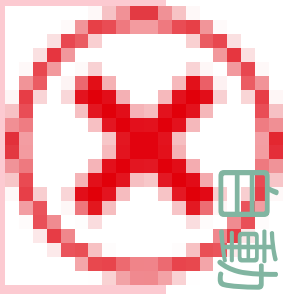
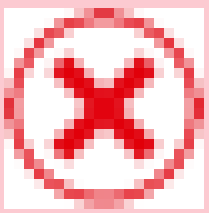
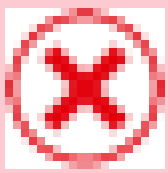
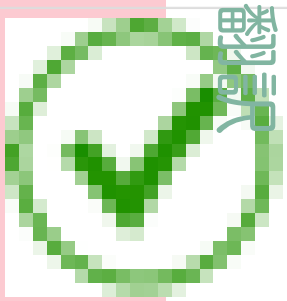
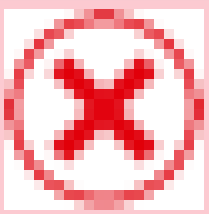
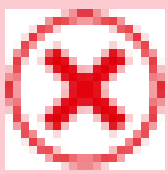
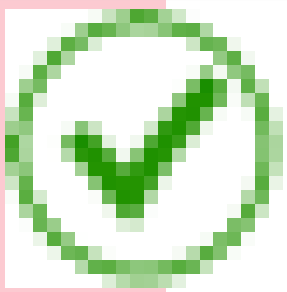
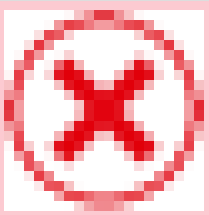
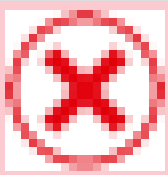
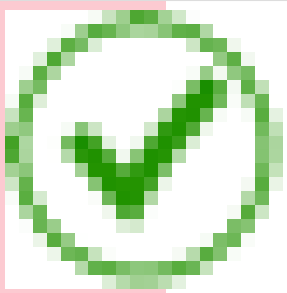
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_admin、sn_si.m

その他のロールの情報：

sn_si.special_access、sn_si_approver_user

(続く)

モジュール	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.external	sn_si.knowledge_admin	sn_si
チームにアサイン済み							
自分の承認							
対応中要求を表示							
全ての要求を表示							
未アサインの要求 (Unassigned Requests)							

自動翻訳

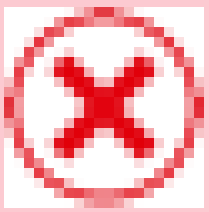
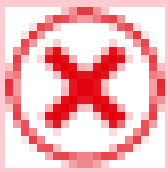
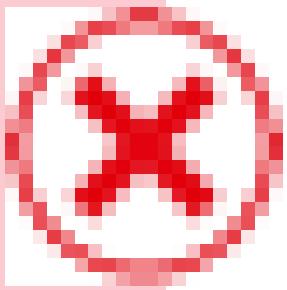
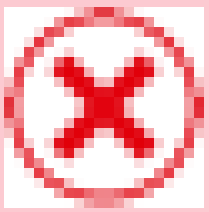
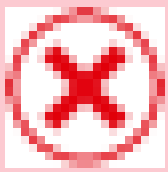
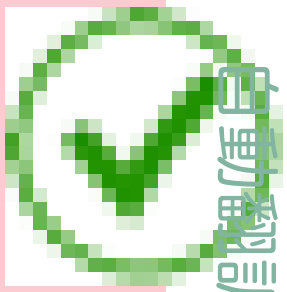
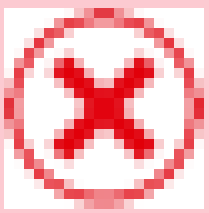
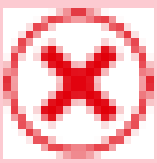
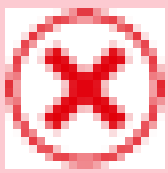
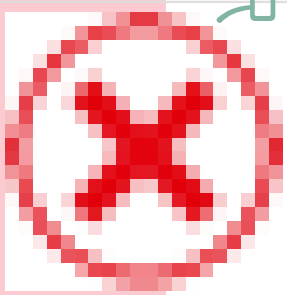
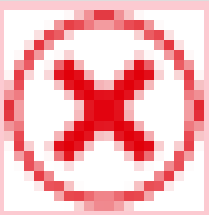
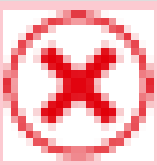
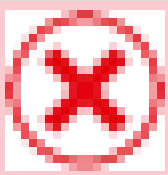
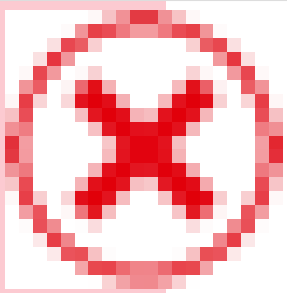
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_admin、sn_si.m

その他のロールの情報：

sn_si.special_access、sn_si_approver_user

(続く)

モジュール	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.external	sn_si.knowledge_admin	sn_si
自分のマップ							
アラートとイベント							
インシデントの事後レビュー							
自分の処理待ちのレビュー							
チームのレビュー処理待ち							
すべての未完了レビュー							
セットアップ							

自動翻訳

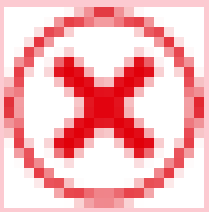
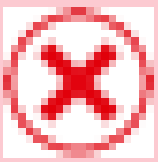
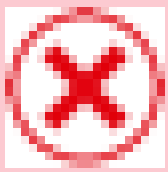
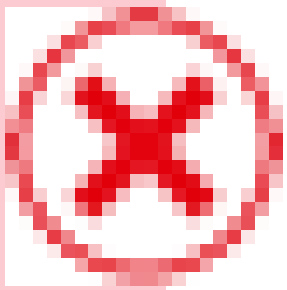
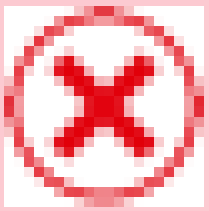
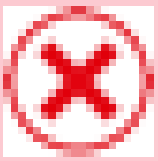
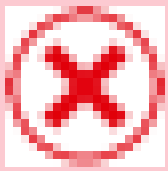
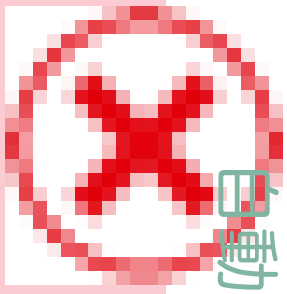
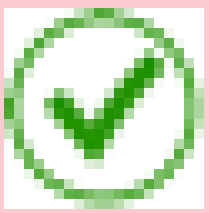
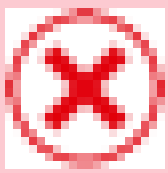
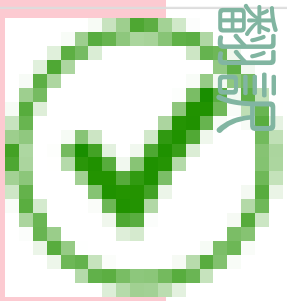
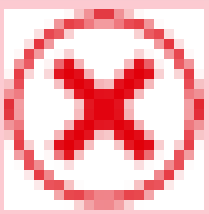
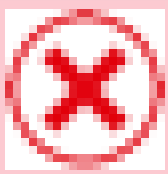
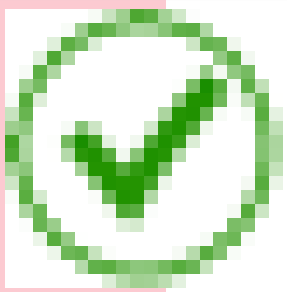
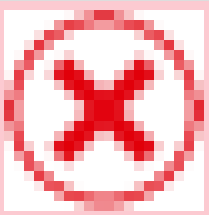
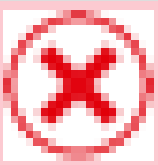
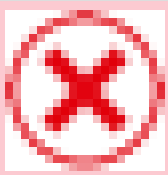
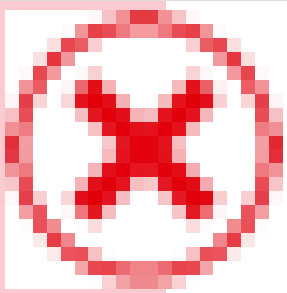
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_admin、sn_si.m

その他のロールの情報：

sn_si.special_access、sn_si_approver_user

(続く)

モジュール	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.external	sn_si.knowledge_admin	sn_si
セキュリティインシデント算出グループ							
重大度算出							
リスクスコア設定							
ニュースフィード設定							
グループ							

自動翻訳

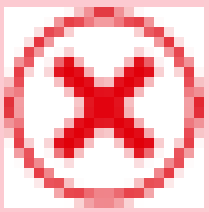
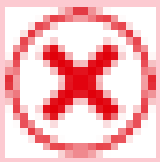
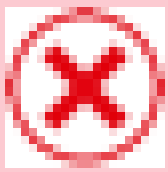
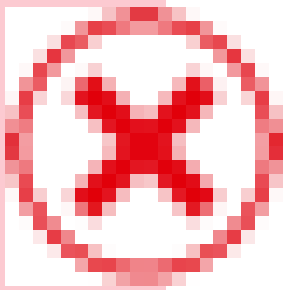
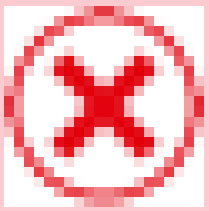
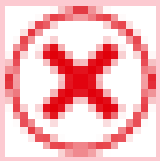
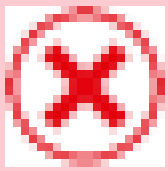
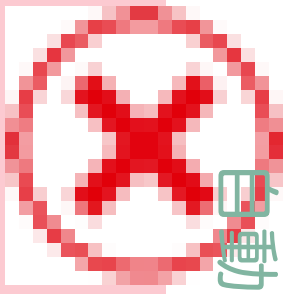
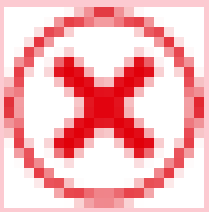
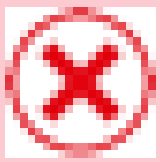
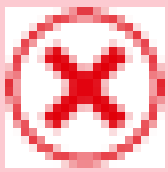
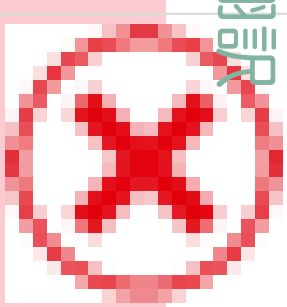
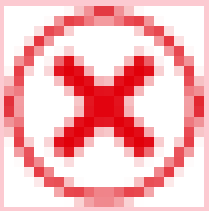
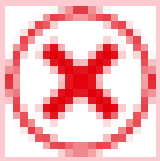
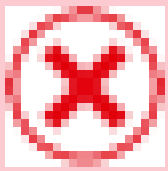
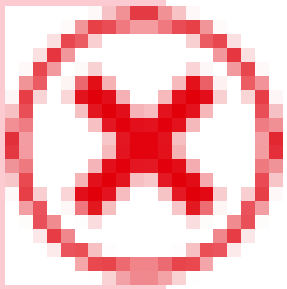
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_admin、sn_si.m

その他のロールの情報：

sn_si.special_access、sn_si_approver_user

(続く)

モジュール	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.external	sn_si.knowledge_admin	sn_si
ロール							
SLA							
アナリストワークスペースセットアップ (新規 UI)							
セットアップアシスタント							
ランディングページのフィルター構成							

自動翻訳

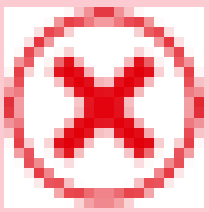
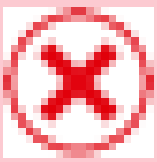
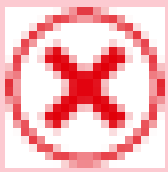
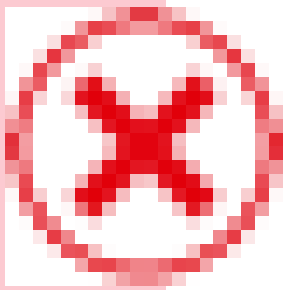
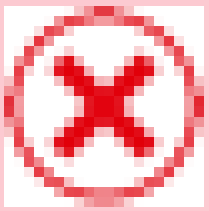
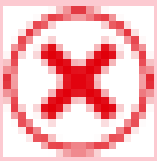
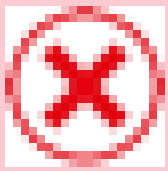
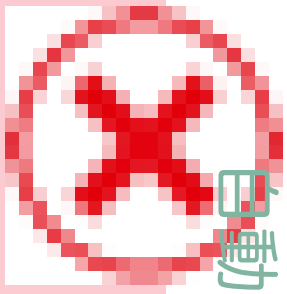
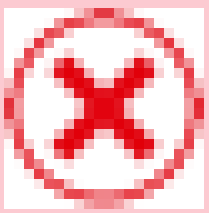
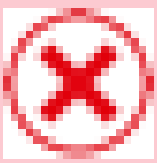
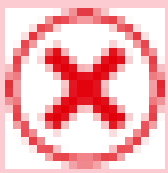
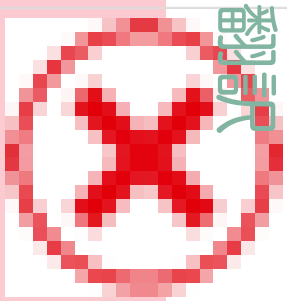
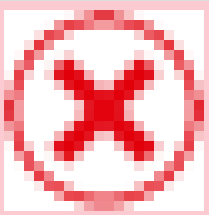
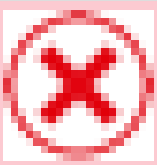
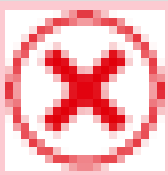
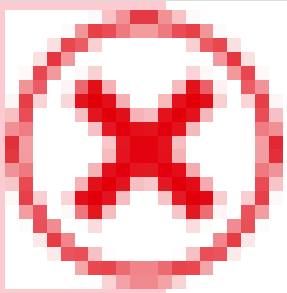
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_admin、sn_si.m

その他のロールの情報：

sn_si.special_access、sn_si_approver_user

(続く)

モジュール	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.external	sn_si.knowledge_admin	sn_si
フォーム UI アクション							
関連リストの構成							
アナリストワークスペースのプロパティ							
カタログとナレッジ							
セキュリティインシデントテンプレート							

自動翻訳

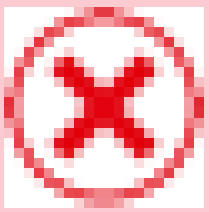
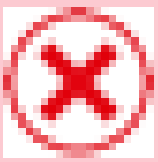
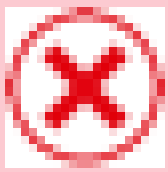
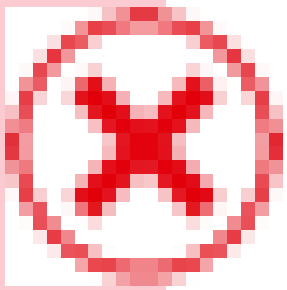
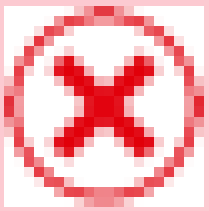
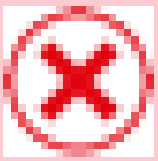
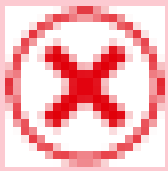
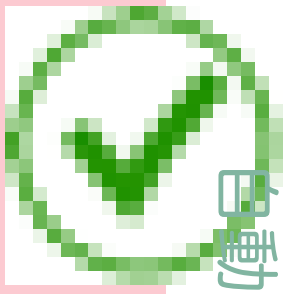
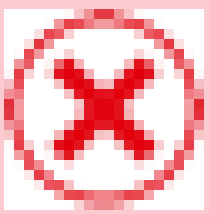
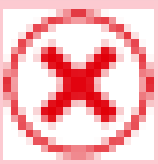
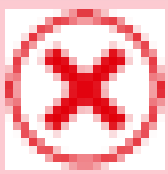
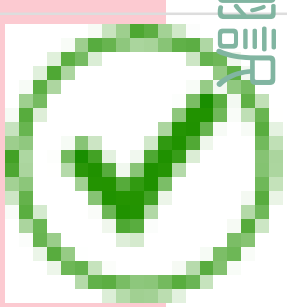
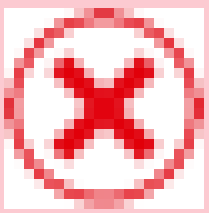
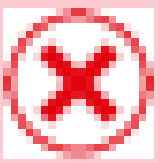
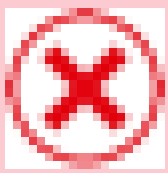
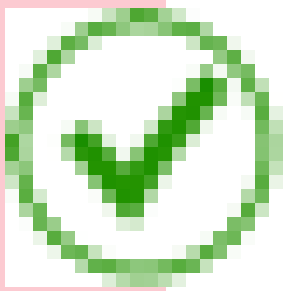
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_admin、sn_si.m

その他のロールの情報：

sn_si.special_access、sn_si_approver_user

(続く)

モジュール	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.external	sn_si.knowledge_admin	sn_si
カタログアイテムの管理							
ナレッジ							
手動 Runbook							
新しい Runbook を作成							
Runbook ドキュメントを表示							
管理							

自動翻訳

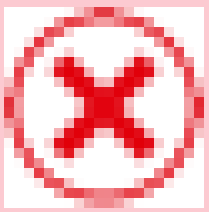
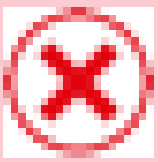
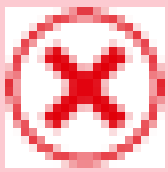
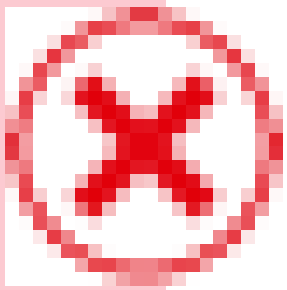
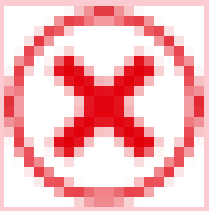
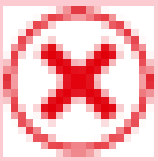
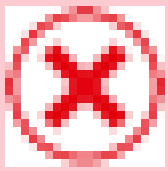
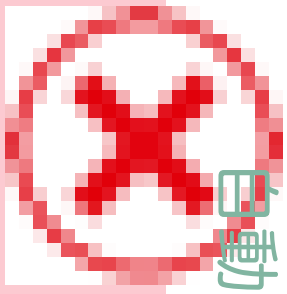
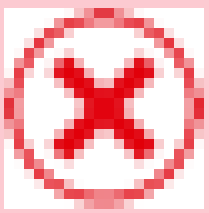
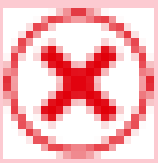
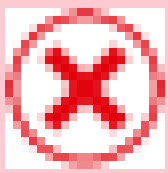
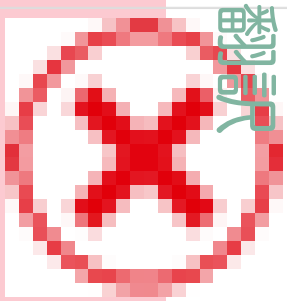
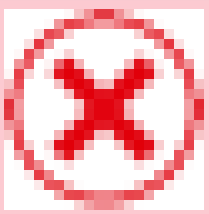
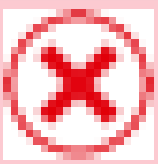
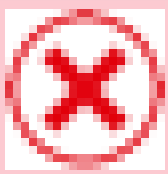
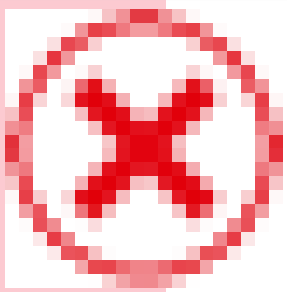
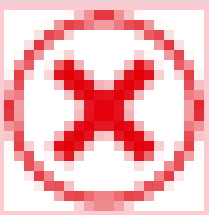
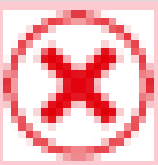
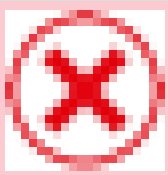
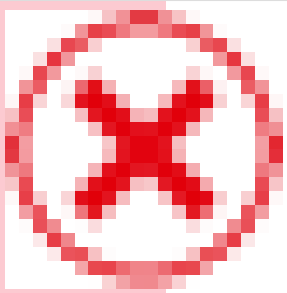
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_admin、sn_si.m

その他のロールの情報：

sn_si.special_access、sn_si_approver_user

(続く)

モジュール	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.external	sn_si.knowledge_admin	sn_si
プロパティ							
構成							
通知							
サービス重要度レポートの定義							
サービス重要度の定義							

自動翻訳

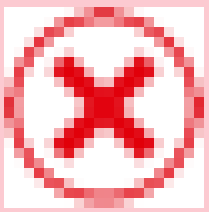
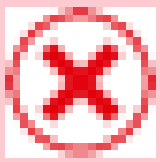
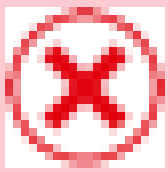
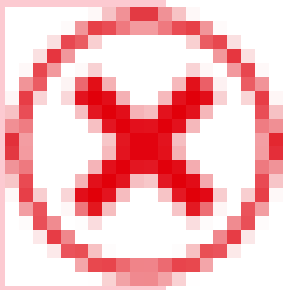
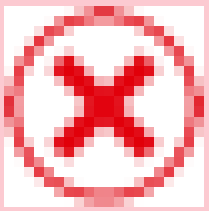
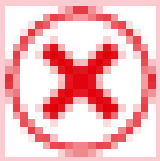
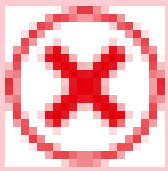
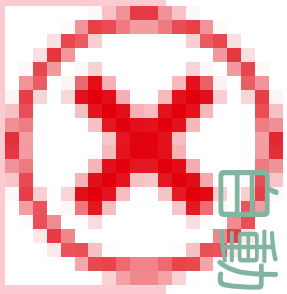
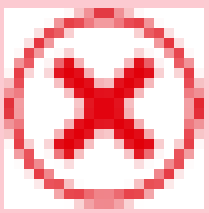
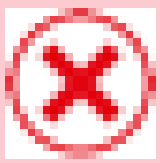
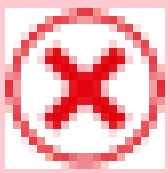
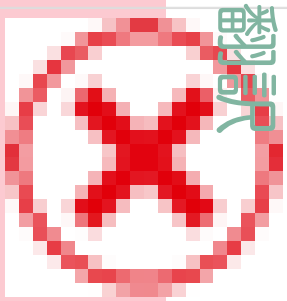
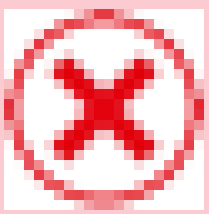
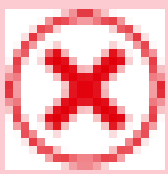
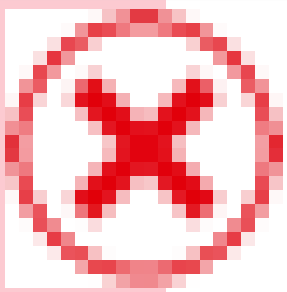
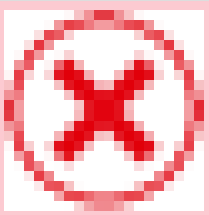
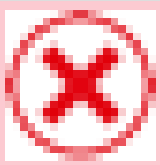
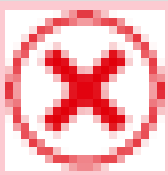
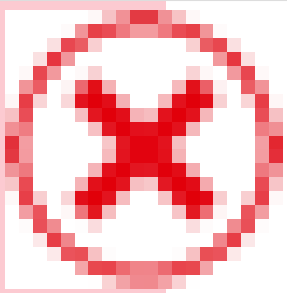
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_admin、sn_si.m

その他のロールの情報：

sn_si.special_access、sn_si_approver_user

(続く)

モジュール	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.external	sn_si.knowledge_admin	sn_si
サービス影響度の定義							
インシデントの事後レビューアセスメントセットアップ							
インシデントの事後レビューレポートセットアップ							
リアルタイム定義							
プロセスの選択							

自動翻訳

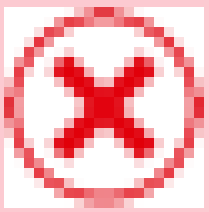
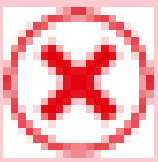
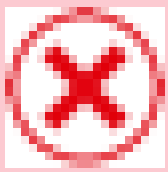
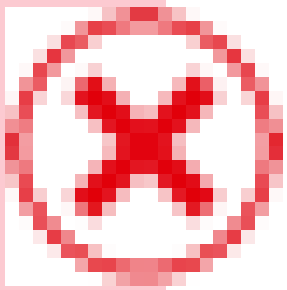
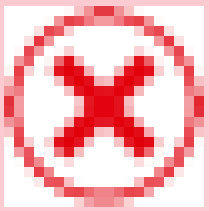
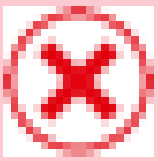
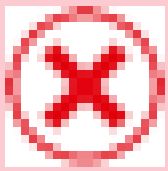
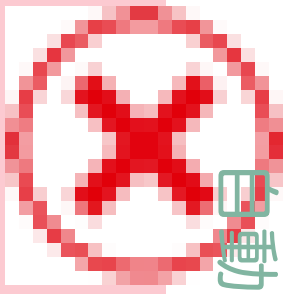
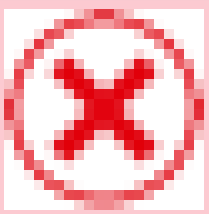
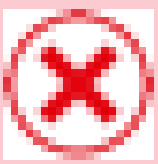
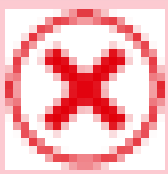
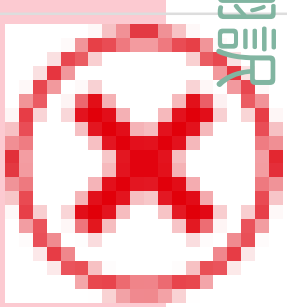
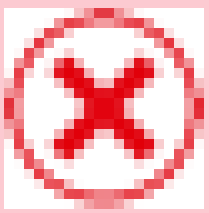
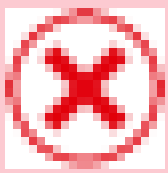
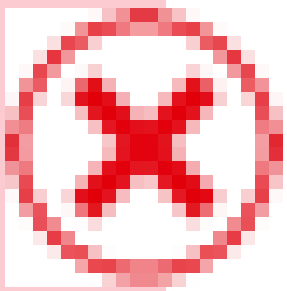
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_admin、sn_si.m

その他のロールの情報：

sn_si.special_access、sn_si_approver_user

(続く)

モジュール	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.external	sn_si.knowledge_admin	sn_si
プロセス定義							
テンプレートワークフロー結果エバリュエータ							
フィッシングメール							
ライセンス管理							
フィッシングメールを報告							

自動翻訳

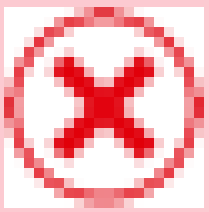
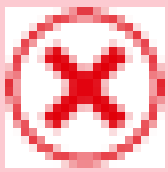
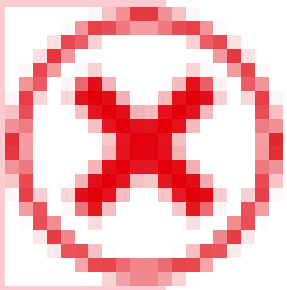
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowledge_admin、sn_si.m

その他のロールの情報：

sn_si.special_access、sn_si_approver_user

(続く)

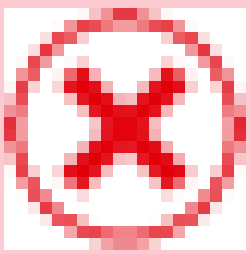
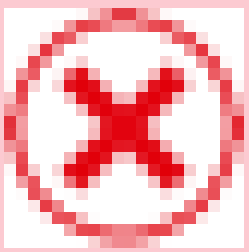
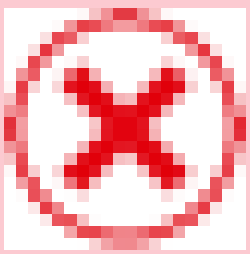
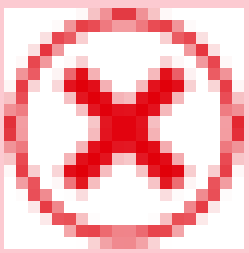
モジュール	sn_sec_cmn.read	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.external	sn_si.knowledge_admin	sn_si
すべての フィッシング メールを表示							

モジュールアクセス：sn_si.special_access、sn_si_approver_user

モジュールアクセス：sn_si.special_access、sn_si_approver_user

その他のロールの情報：

sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowled

モジュール	sn_si.special_access	sn_si_approver_user
(メインアプリグループ)		
インシデント新規 UI		
サービスへの影響		

自動翻訳

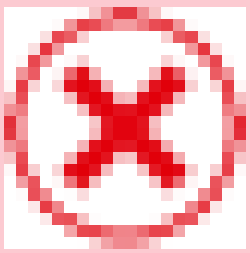
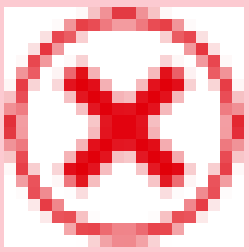
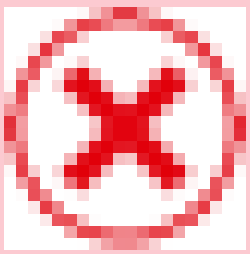
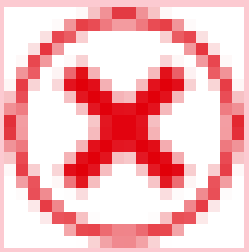
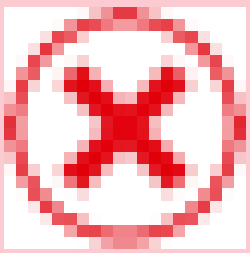
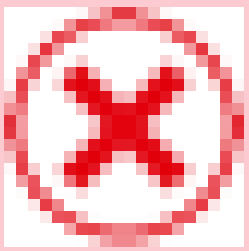
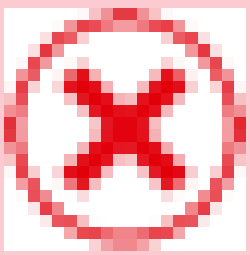
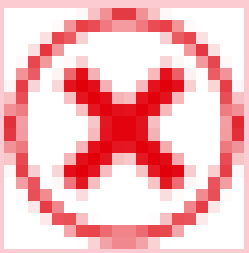
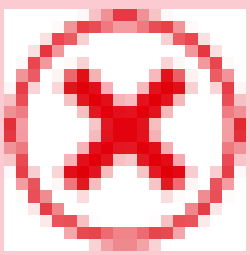
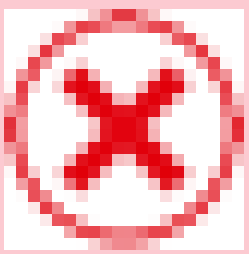
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_si.special_access、sn_si_approver_user

その他のロールの情報：

sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowled

(続く)

モジュール	sn_si.special_access	sn_si_approver_user
概要		
リアルタイム		
インシデント		
閲覧可能なインシデント		
自分にアサイン済み		
My Work		

自動翻訳

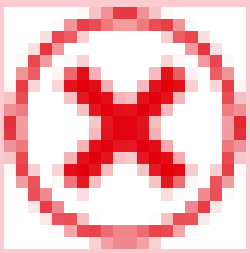
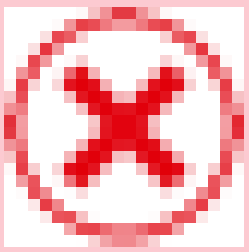
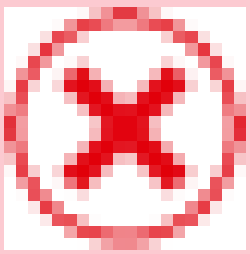
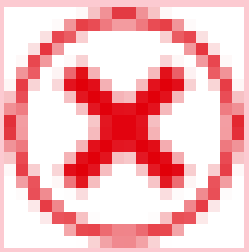
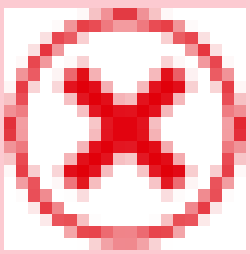
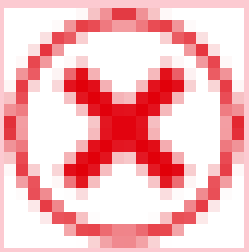
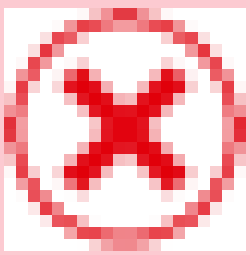
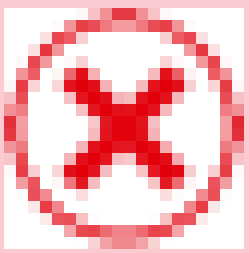
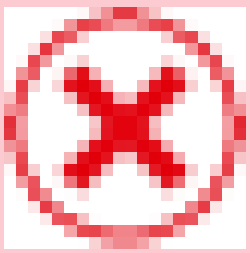
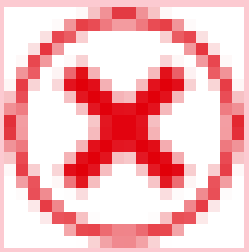
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_si.special_access、sn_si_approver_user

その他のロールの情報：

sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowled

(続く)

モジュール	sn_si.special_access	sn_si_approver_user
チームにアサイン済み		
オープンインシデントを表示		
すべてのインシデントを表示		
未アサインのインシデント		
応答タスク		
自分にアサイン済み		

自動翻訳

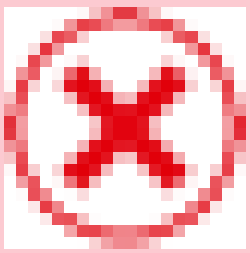
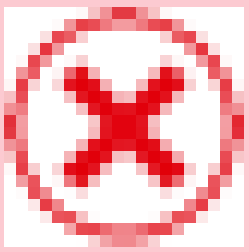
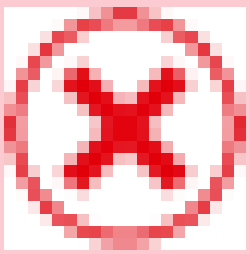
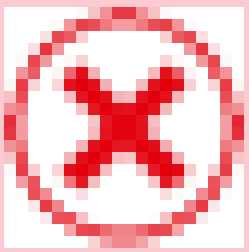
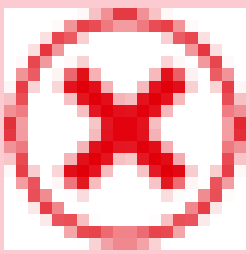
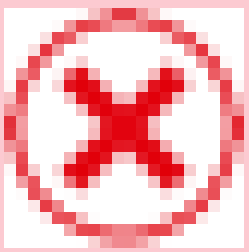
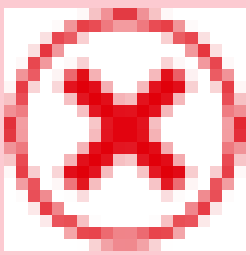
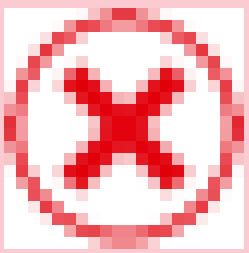
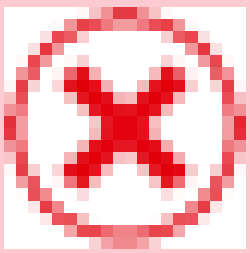
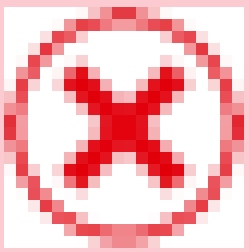
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_si.special_access、sn_si_approver_user

その他のロールの情報：

sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowled

(続く)

モジュール	sn_si.special_access	sn_si_approver_user
チームにアサイン済み		
オープンタスクを表示		
すべてのタスクを表示		
未アサインタスク		
受け付けた要求		
自分にアサイン済み		

自動翻訳

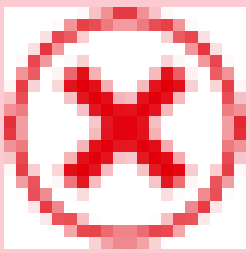
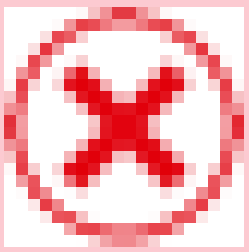
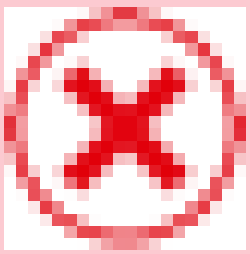
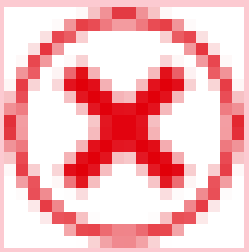
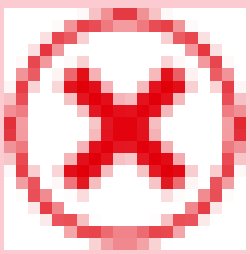
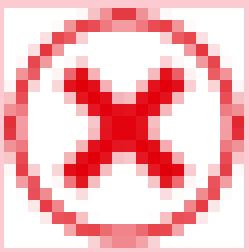
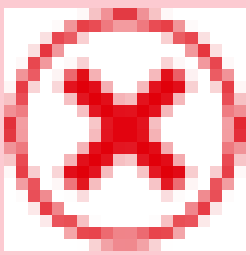
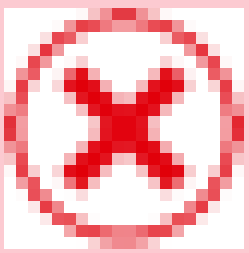
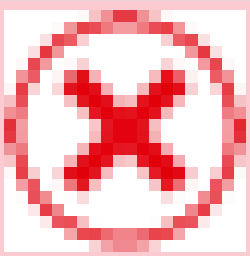
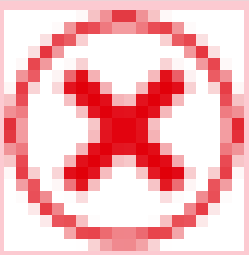
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_si.special_access、sn_si_approver_user

その他のロールの情報：

sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowled

(続く)

モジュール	sn_si.special_access	sn_si_approver_user
チームにアサイン済み		
自分の承認		
対応中要求を表示		
全ての要求を表示		
未アサインの要求 (Unassigned Requests)		

自動翻訳

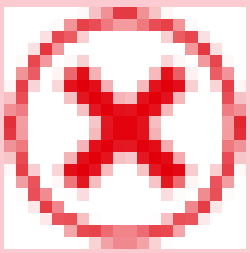
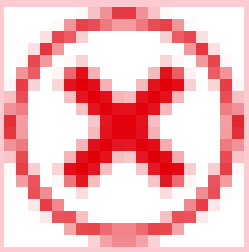
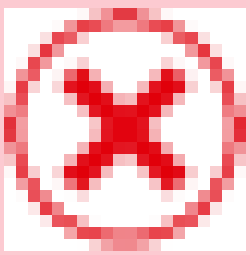
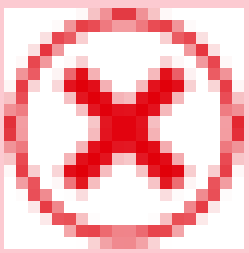
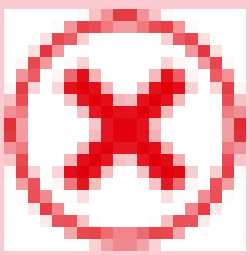
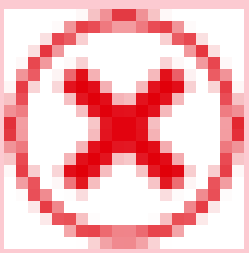
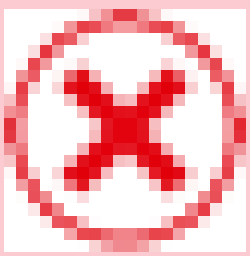
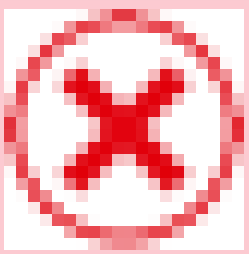
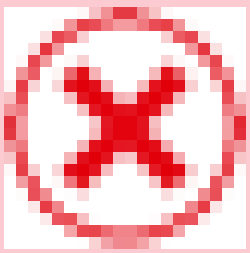
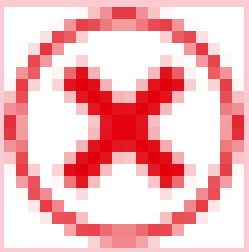
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_si.special_access、sn_si_approver_user

その他のロールの情報：

sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowled

(続く)

モジュール	sn_si.special_access	sn_si_approver_user
自分のマップ		
アラートとイベント		
インシデントの事後レビュー		
自分の処理待ちのレビュー		
チームのレビュー処理待ち		
すべての未完了レビュー		
セットアップ		
セキュリティインシデント算出グループ		

自動翻訳

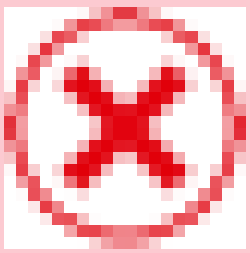
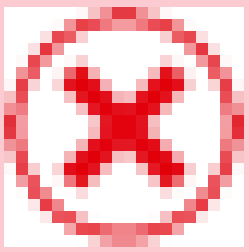
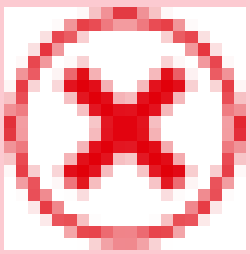
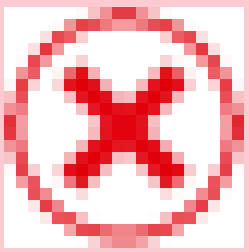
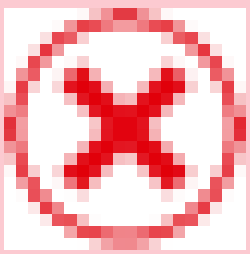
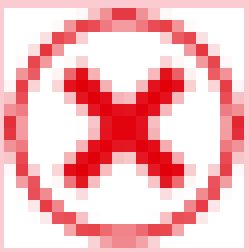
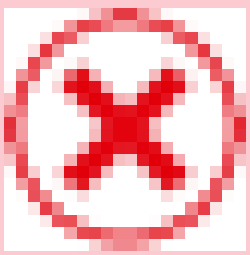
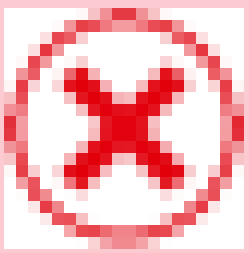
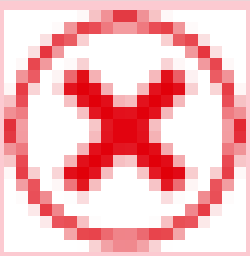
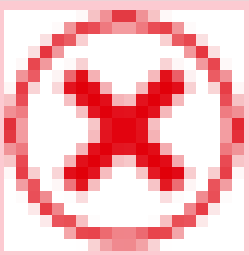
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_si.special_access、sn_si_approver_user

その他のロールの情報：

sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowled

(続く)

モジュール	sn_si.special_access	sn_si_approver_user
重大度算出		
リスクスコア設定		
ニュースフィード設定		
グループ		
ロール		

自動翻訳

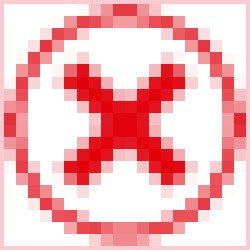
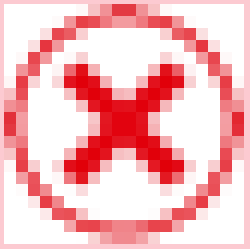
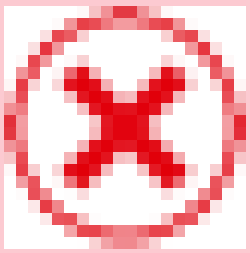
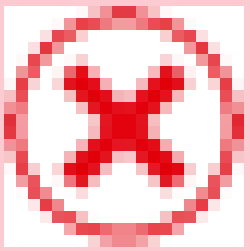
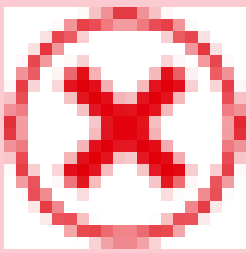
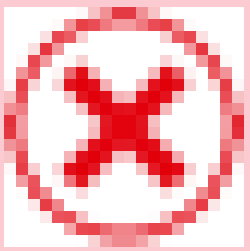
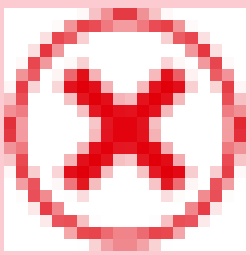
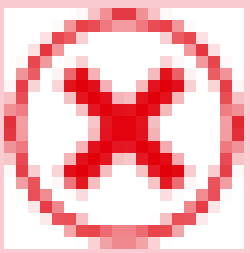
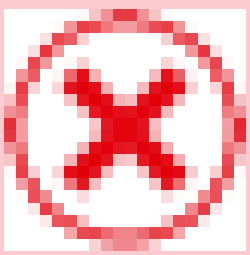
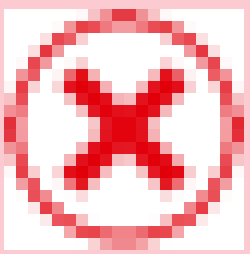
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_si.special_access、sn_si_approver_user

その他のロールの情報：

sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowled

(続く)

モジュール	sn_si.special_access	sn_si_approver_user
SLA		
アナリストワークスペースセットアップ (新規 UI)		
セットアップアシスタント		
ランディングページのフィルター構成		
フォーム UI アクション		
関連リストの構成		

自動翻訳

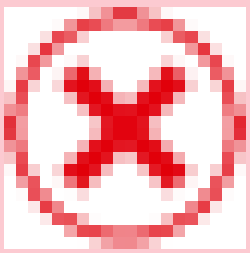
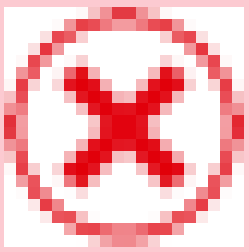
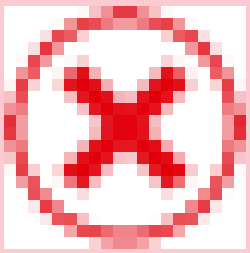
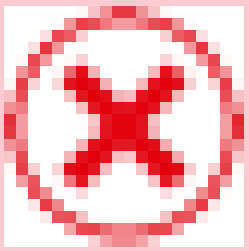
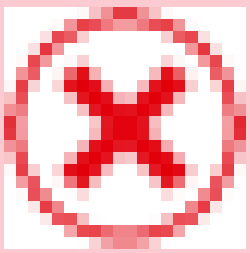
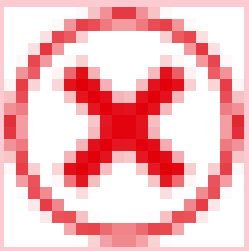
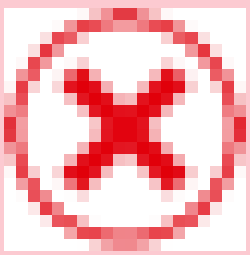
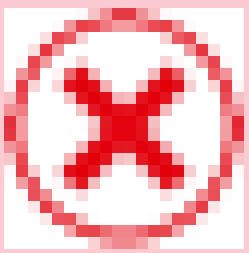
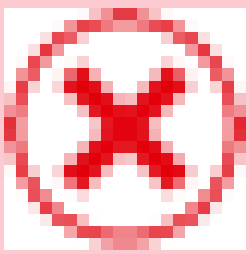
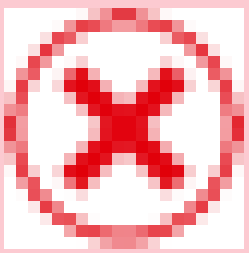
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_si.special_access、sn_si_approver_user

その他のロールの情報：

sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowled

(続く)

モジュール	sn_si.special_access	sn_si_approver_user
アナリストワークスペースのプロパティ		
カタログとナレッジ		
セキュリティインシデントテンプレート		
カタログアイテムの管理		
ナレッジ		
手動 Runbook		
新しい Runbook を作成		

自動翻訳

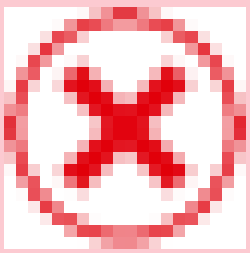
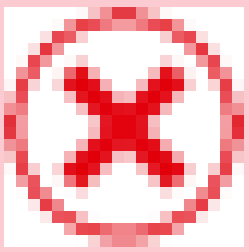
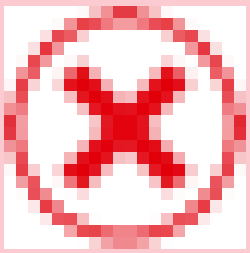
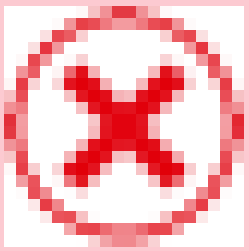
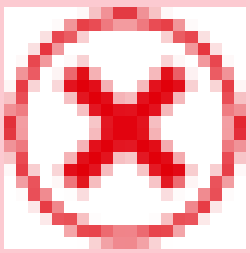
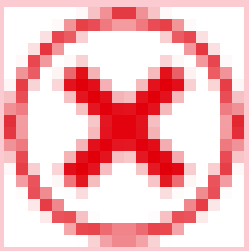
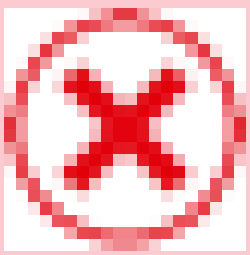
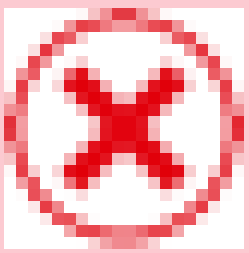
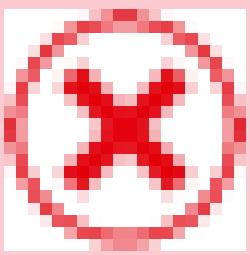
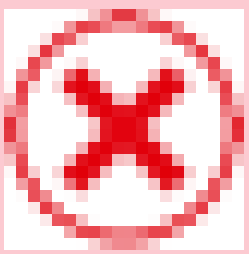
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_si.special_access、sn_si_approver_user

その他のロールの情報：

sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowled

(続く)

モジュール	sn_si.special_access	sn_si_approver_user
Runbook ドキュメントを表示		
管理		
プロパティ		
構成		
通知		
サービス重要度レポートの定義		

自動翻訳

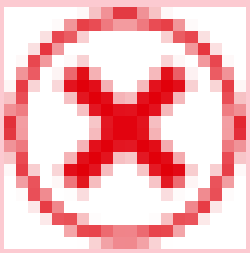
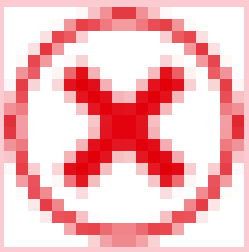
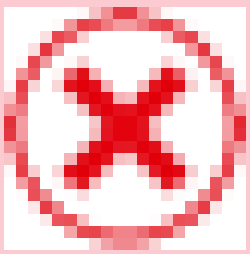
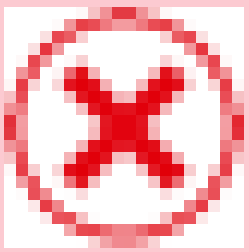
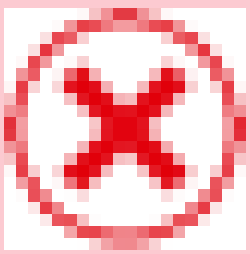
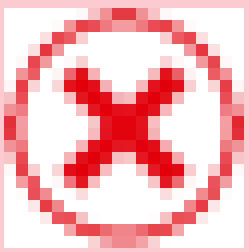
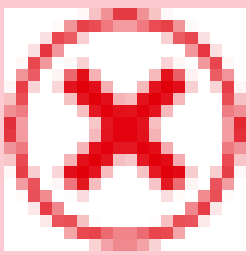
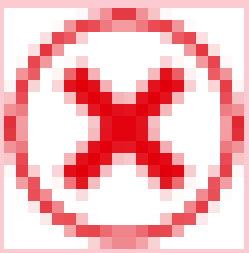
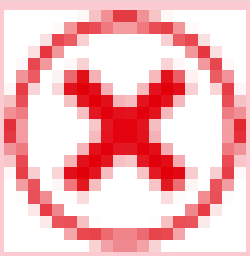
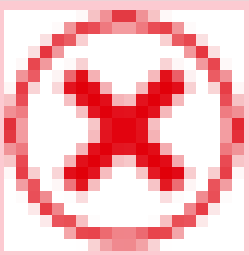
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_si.special_access、sn_si_approver_user

その他のロールの情報：

sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowled

(続く)

モジュール	sn_si.special_access	sn_si_approver_user
サービス重要度の定義		
サービス影響度の定義		
インシデントの事後レビューアセスメントセットアップ		
インシデントの事後レビューレポートセットアップ		
リアルタイム定義		

自動翻訳

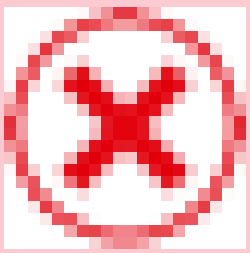
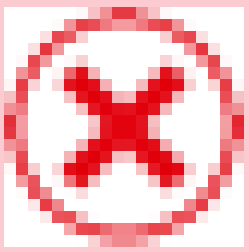
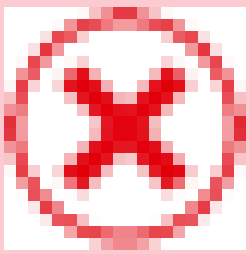
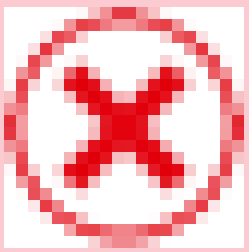
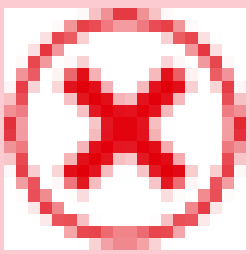
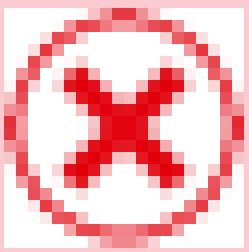
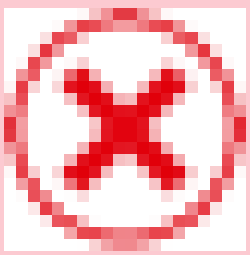
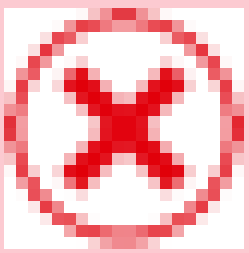
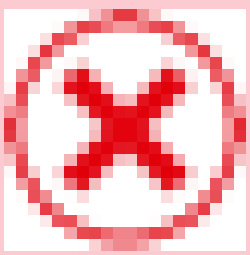
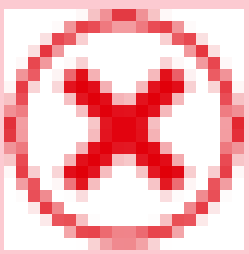
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_si.special_access、sn_si_approver_user

その他のロールの情報：

sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowled

(続く)

モジュール	sn_si.special_access	sn_si_approver_user
プロセスの選択		
プロセス定義		
テンプレートワークフロー結果エバリュエータ		
フィッシングメール		
ライセンス管理		
フィッシングメールを報告		

自動翻訳

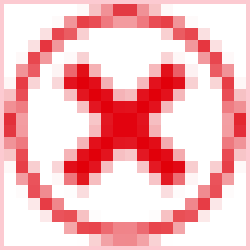
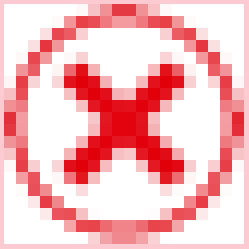
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_si.special_access、sn_si_approver_user

その他のロールの情報：

sn_sec_cmn.read、sn_si.admin、sn_si.analyst、sn_si.ciso、sn_si.external、sn_si.knowled

(続く)

モジュール	sn_si.special_access	sn_si_approver_user
すべてのフィッシングメールを表示		

[End]

[store-future: BEGIN review]

Security Operations のロール別モジュールアクセス

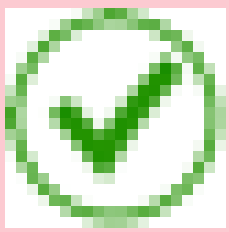
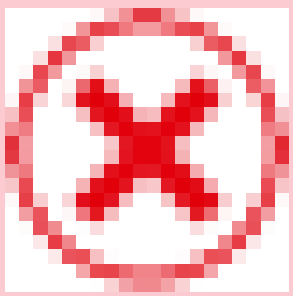
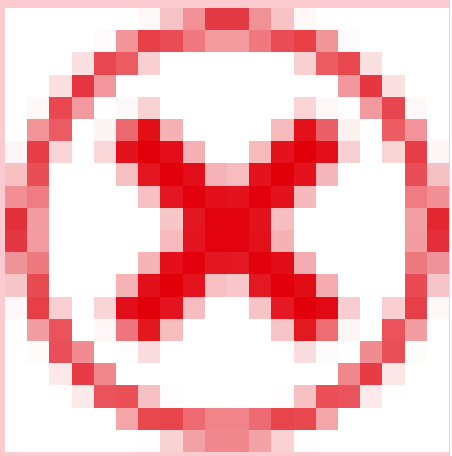
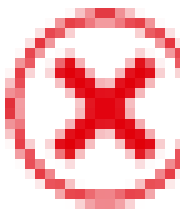
Security Operations では、特定のロールがアクセスできるメニューアイテムが表示されます。

モジュールアクセス：
admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_backgr**ound_job**

モジュールアクセス：
admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_job、sn_sec_cmn

その他のロールの情報：

sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_it

モジュール	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_cmn.re
(メインアプリグループ)					
統合					

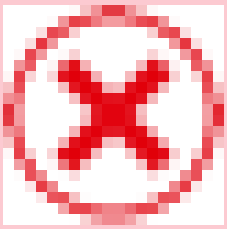
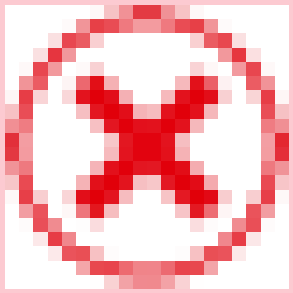
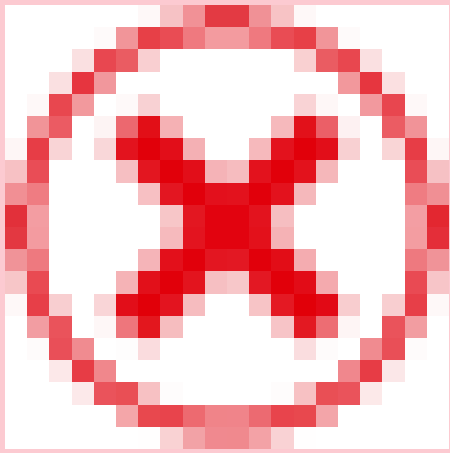
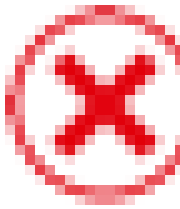
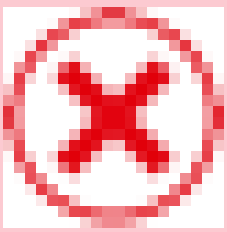
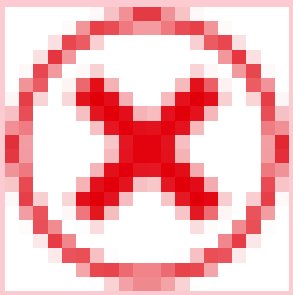
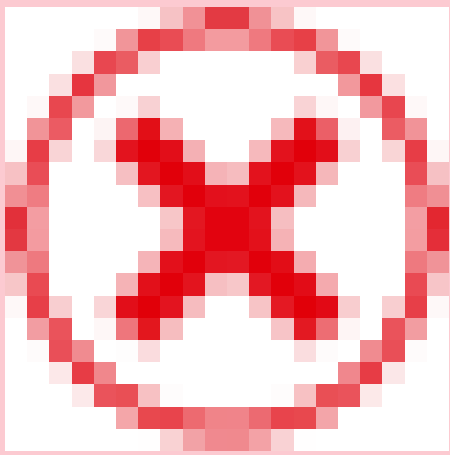
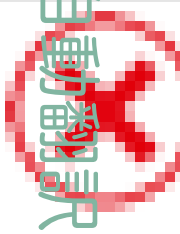
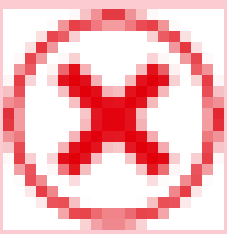
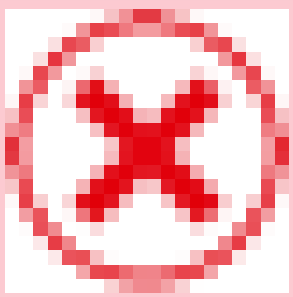
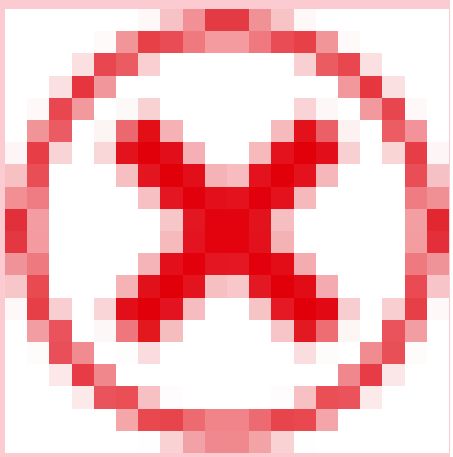
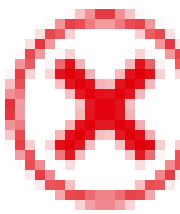
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_job、sn_sec_cmn.

その他のロールの情報：

sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_it

(続く)

モジュール	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_cmn.re
統合機能フロー					
機能実行					
機能実装レート制限					

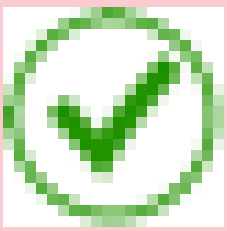
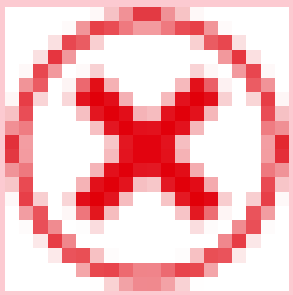
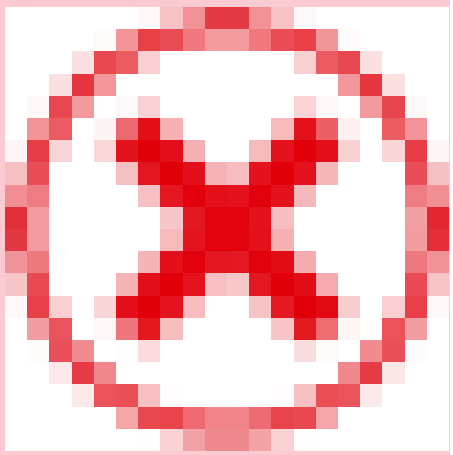
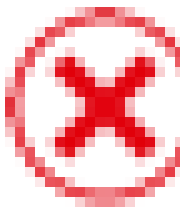
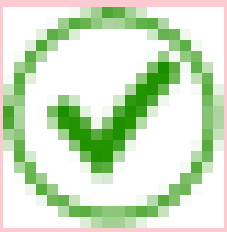
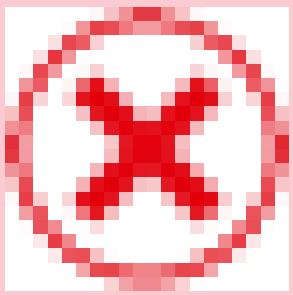
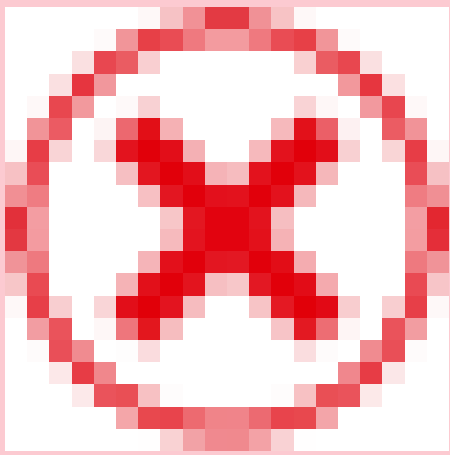
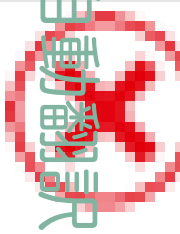
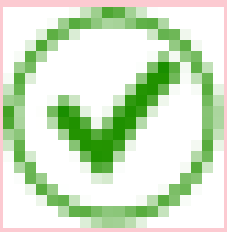
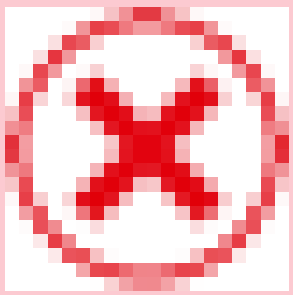
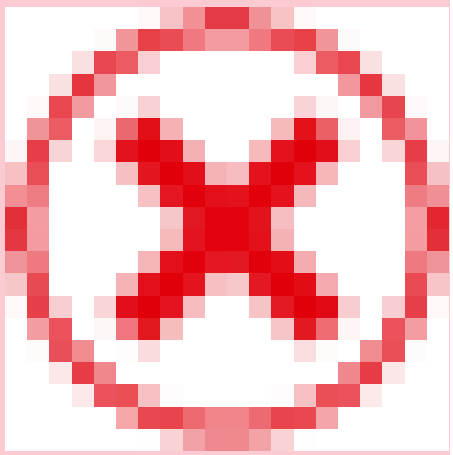
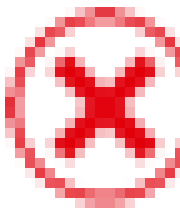
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_job、sn_sec_cmn.

その他のロールの情報：

sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_it

(続く)

モジュール	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_cmn.re
統合構成					
サイティング検索構成					
統合機能					
統合					

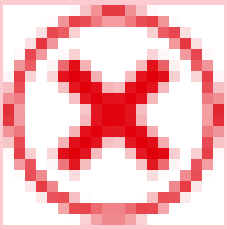
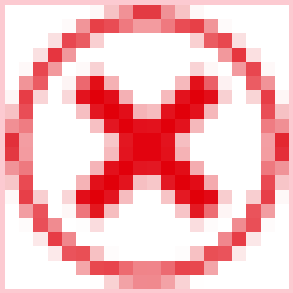
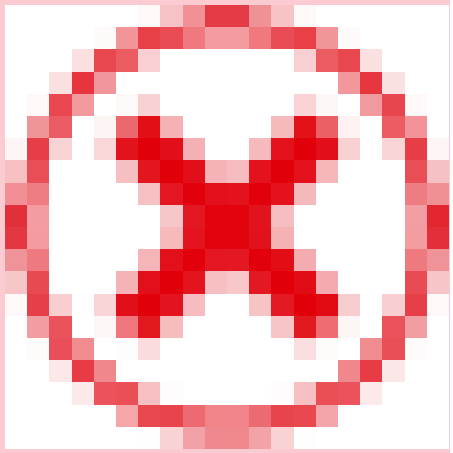
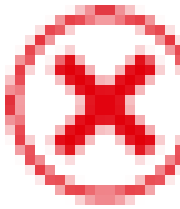
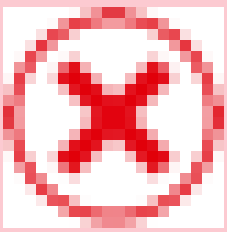
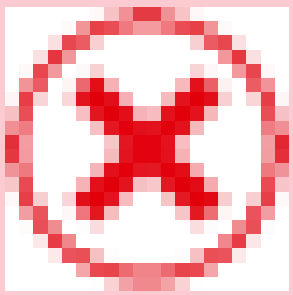
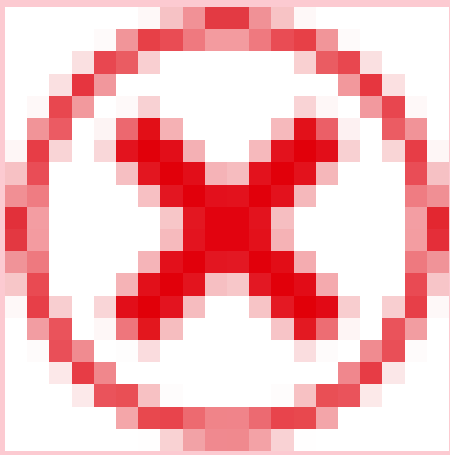
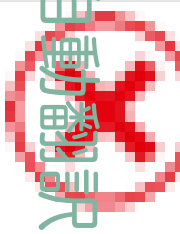
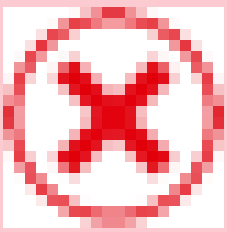
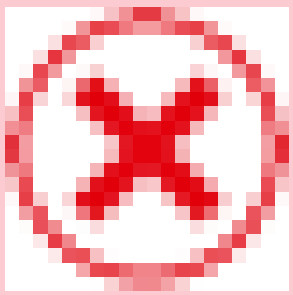
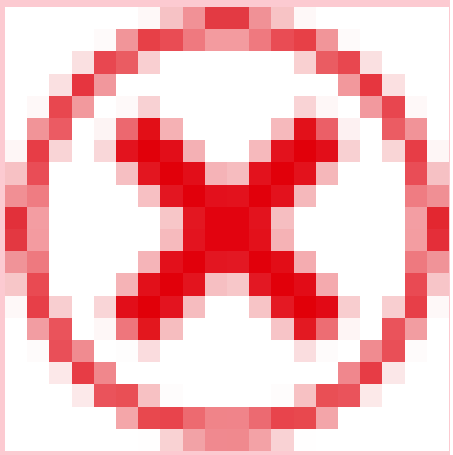
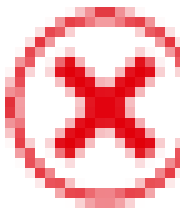
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_job、sn_sec_cmn.

その他のロールの情報：

sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_it

(続く)

モジュール	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_cmn.re
統合機能フロー					
機能実行					
機能実装レート制限					

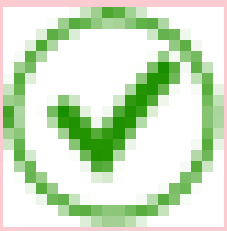
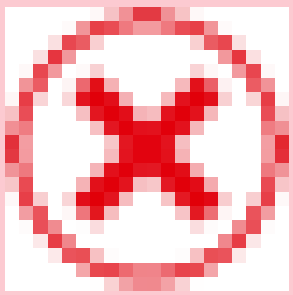
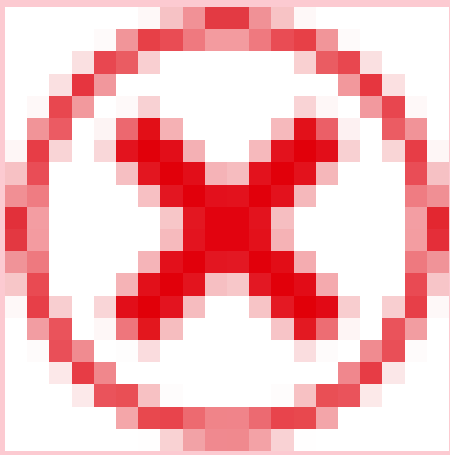
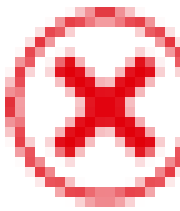
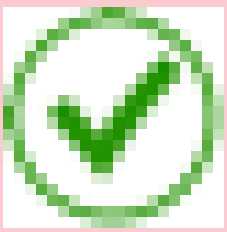
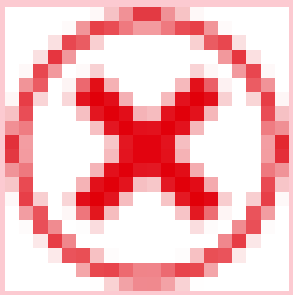
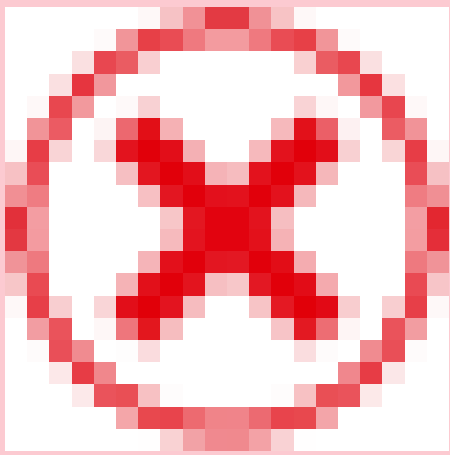
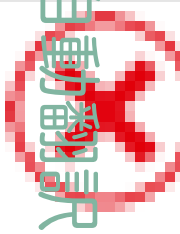
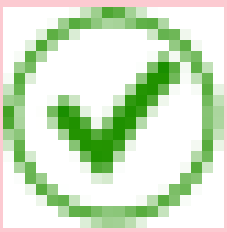
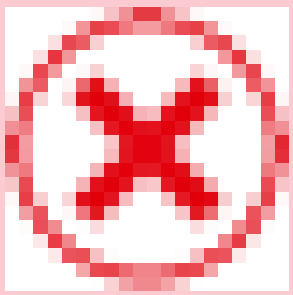
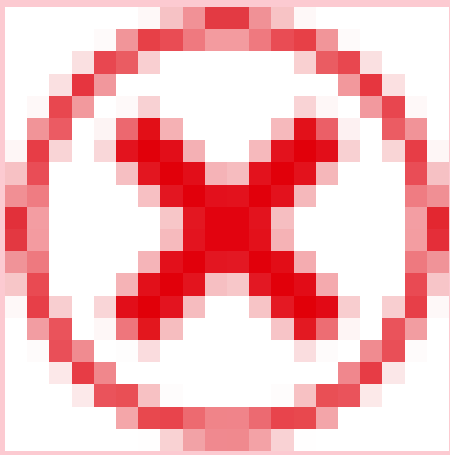
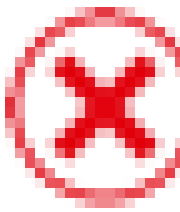
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_job、sn_sec_cmn.

その他のロールの情報：

sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_it

(続く)

モジュール	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_cmn.re
統合構成					
サイティング検索構成					
統合機能					
メール処理					

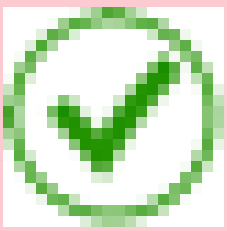
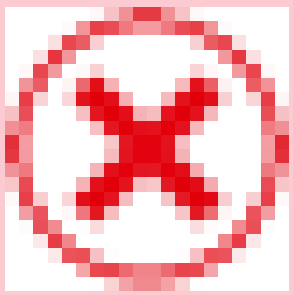
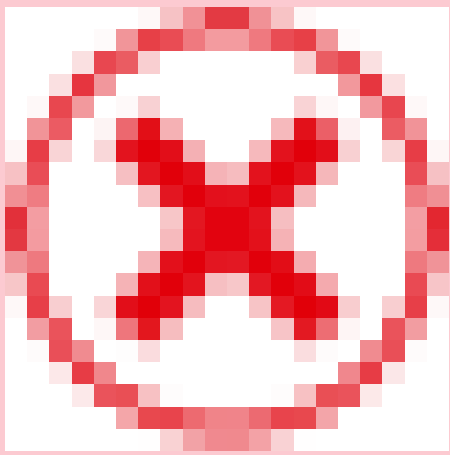
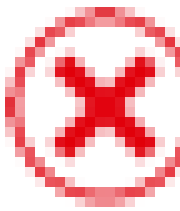
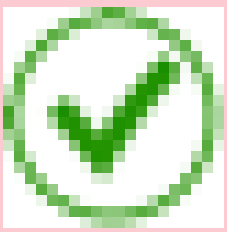
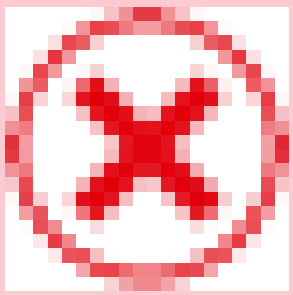
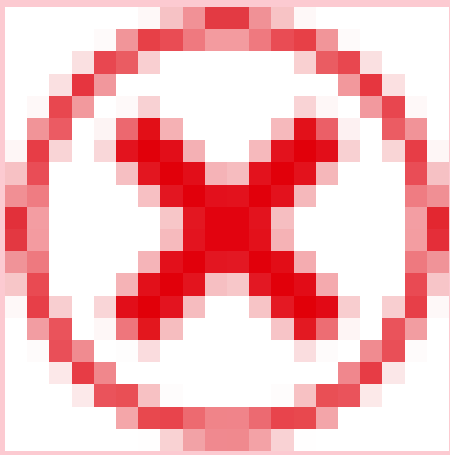
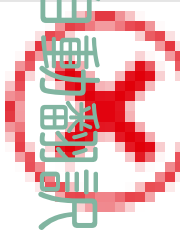
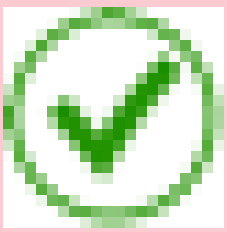
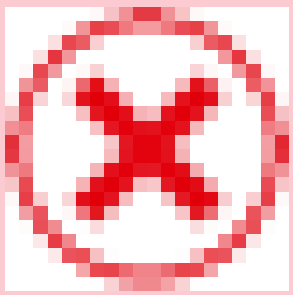
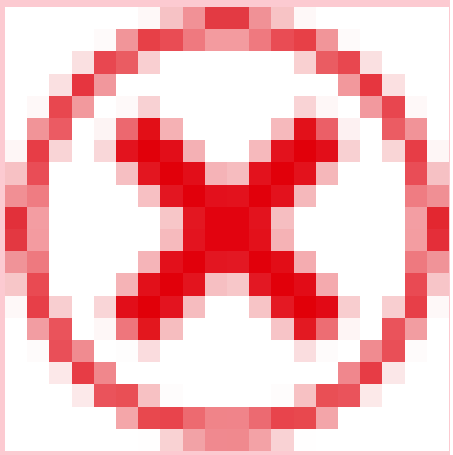
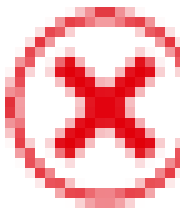
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_job、sn_sec_cmn.

その他のロールの情報：

sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_it

(続く)

モジュール	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_cmn.re
メール解析					
重複ルール					
プロパティ					

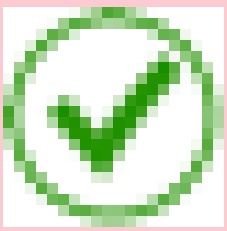
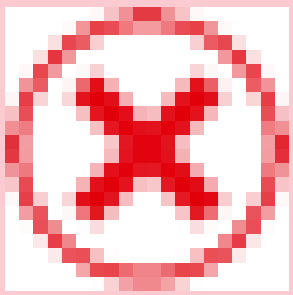
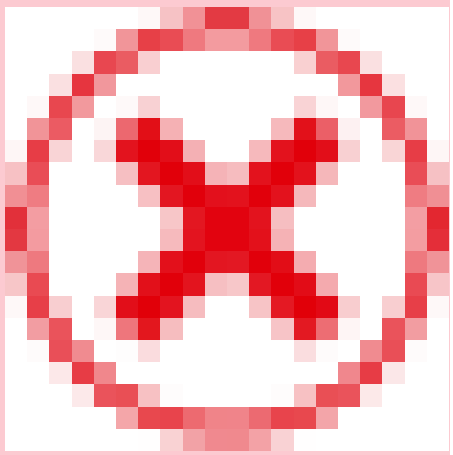
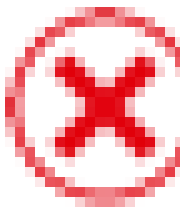
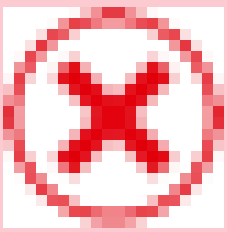
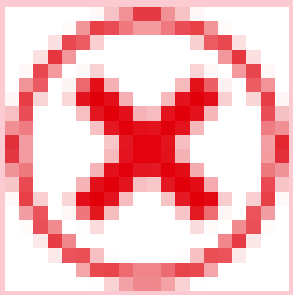
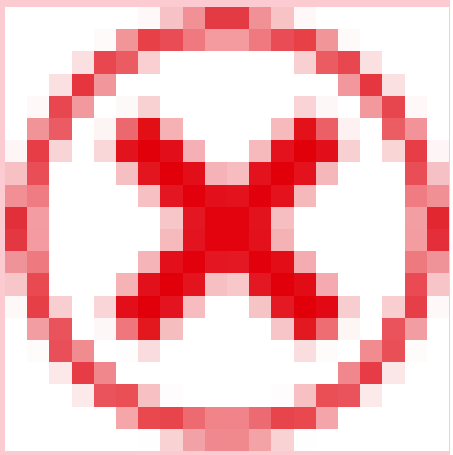
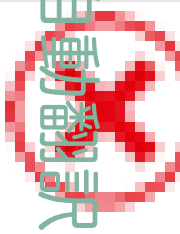
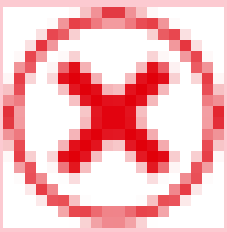
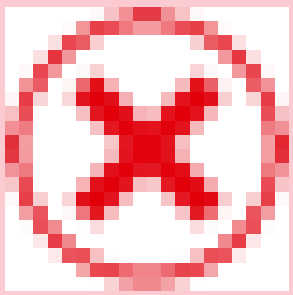
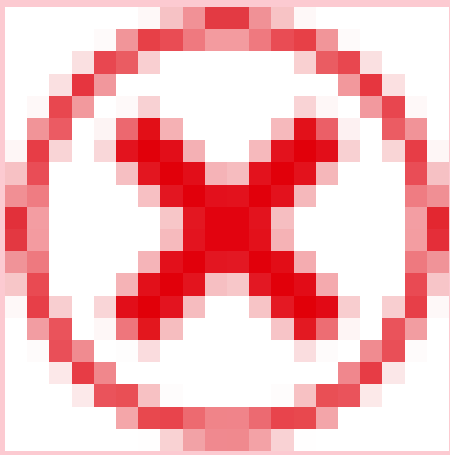
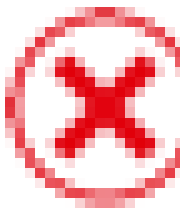
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_job、sn_sec_cmn.

その他のロールの情報：

sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_it

(続く)

モジュール	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_cmn.re
一致しないメール					
取り込みルール - ユーザーから報告されたフィッシング					
ユーザーから報告されたフィッシングプロパティ					
グループ					

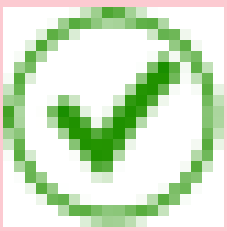
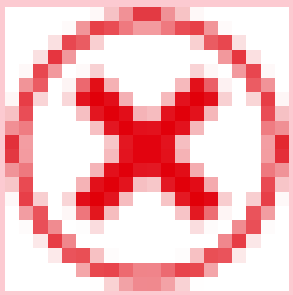
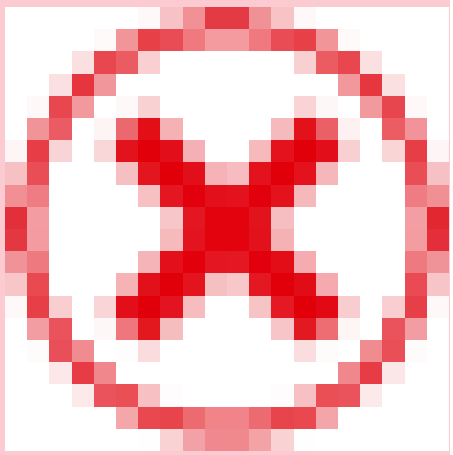
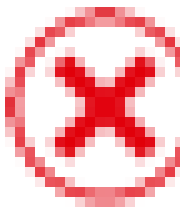
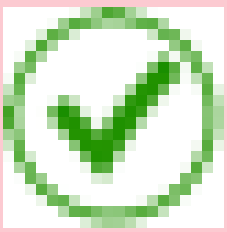
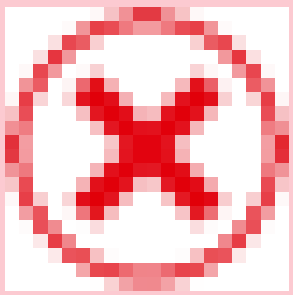
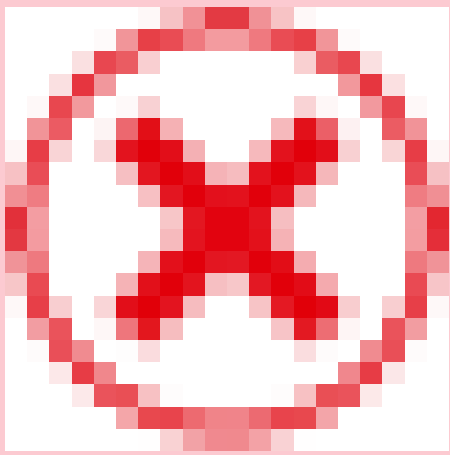
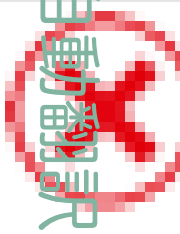
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_job、sn_sec_cmn.

その他のロールの情報：

sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_it

(続く)

モジュール	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_cmn.re
フィルターグループ					
エスカレーション					
データ拡張					
セキュリティタグ					

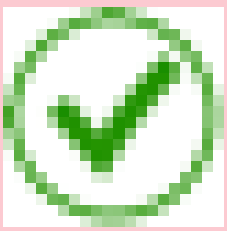
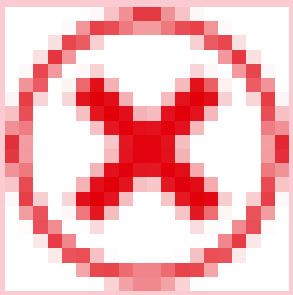
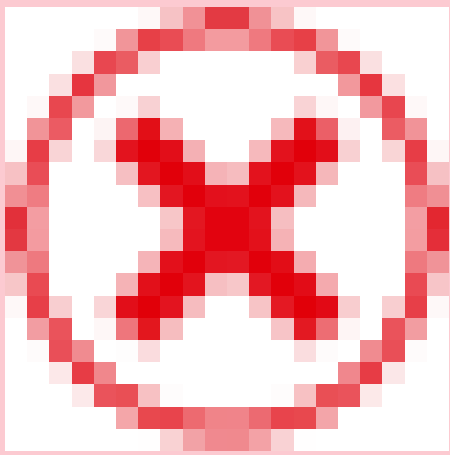
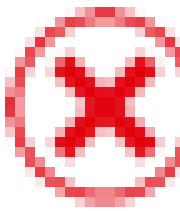
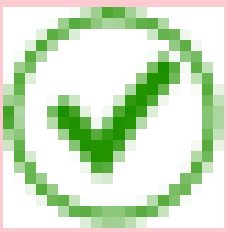
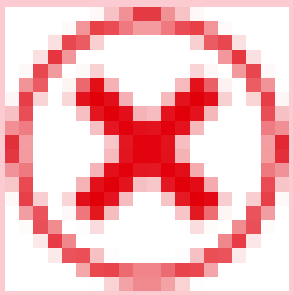
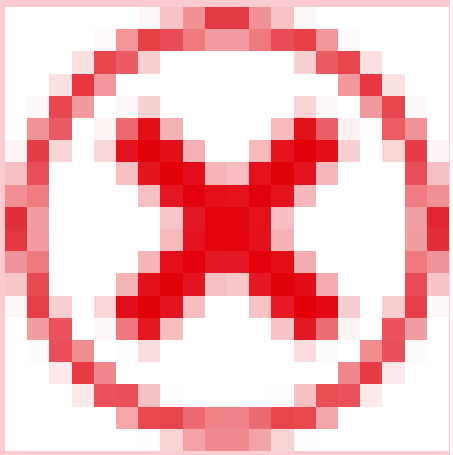
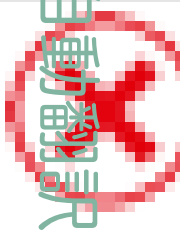
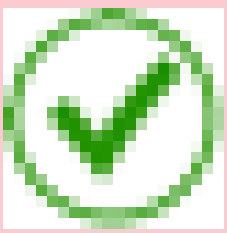
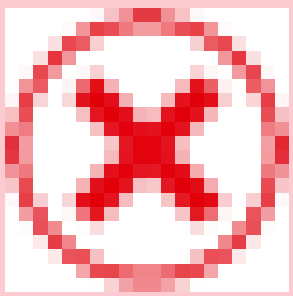
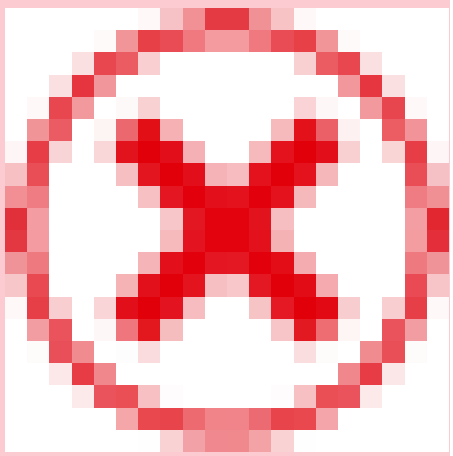
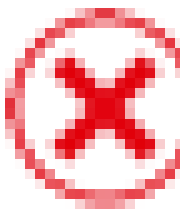
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_job、sn_sec_cmn.

その他のロールの情報：

sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_it

(続く)

モジュール	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_cmn.re
グループ					
Tags					
ワークフロー					
実行トラッキング					

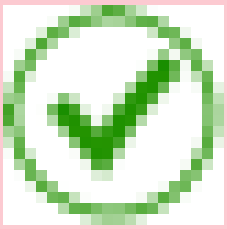
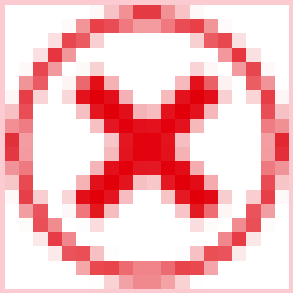
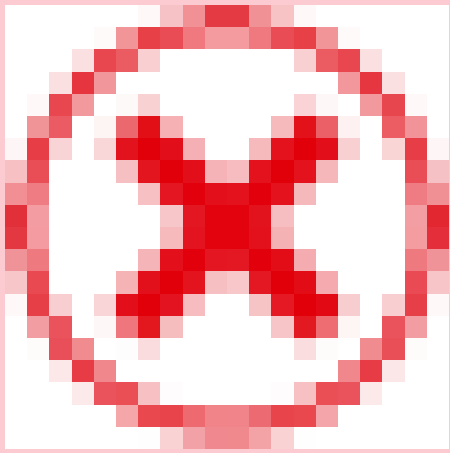
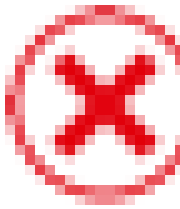
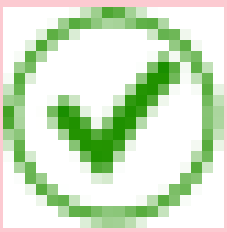
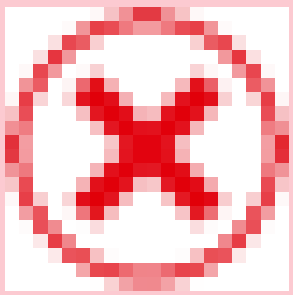
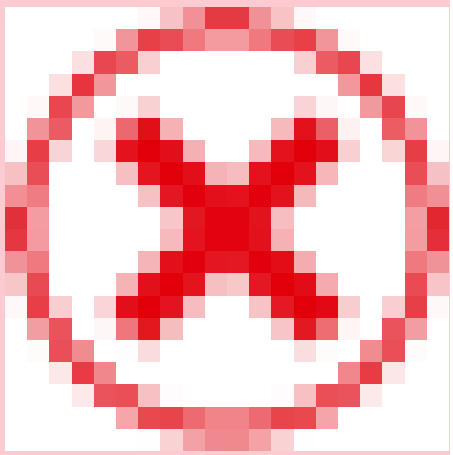
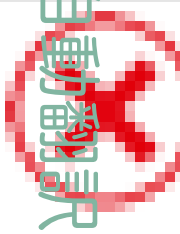
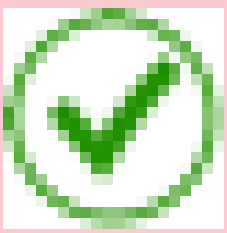
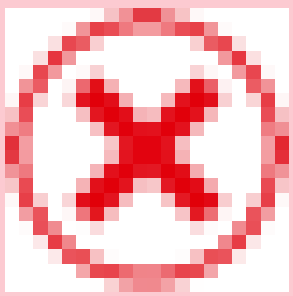
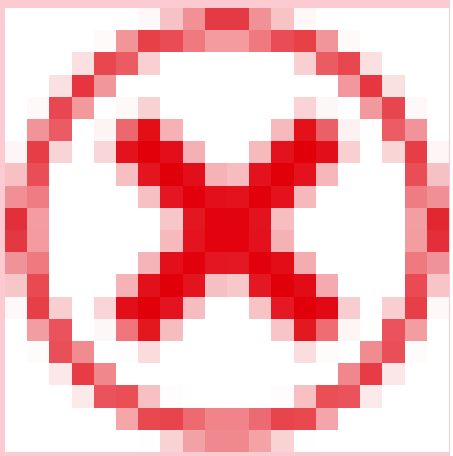
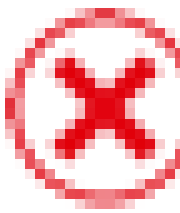
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_job、sn_sec_cmn.

その他のロールの情報：

sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_it

(続く)

モジュール	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_cmn.re
セキュリティワークフローを表示					
ワークフロートリガー					
ユーティリティ					
拡張データマッピング					

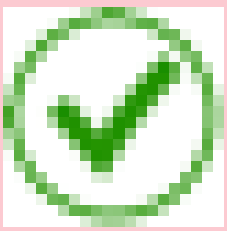
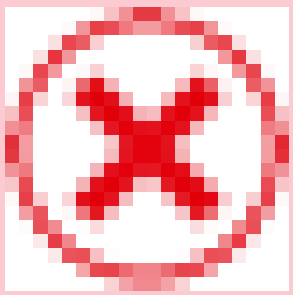
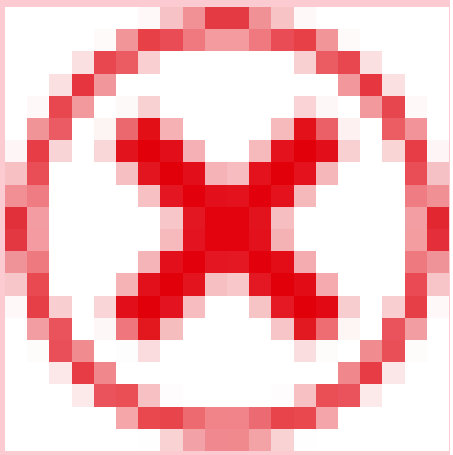
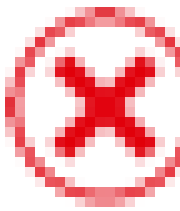
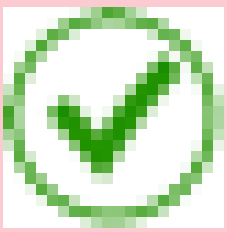
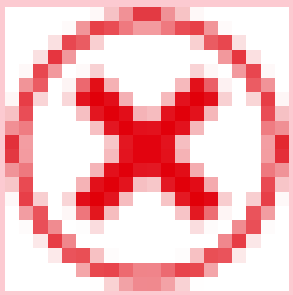
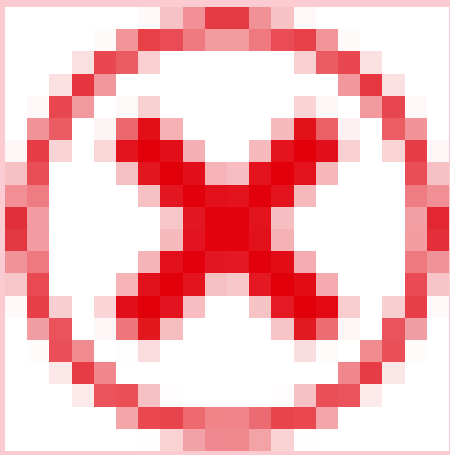
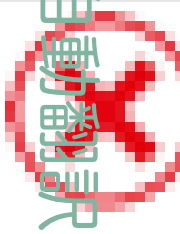
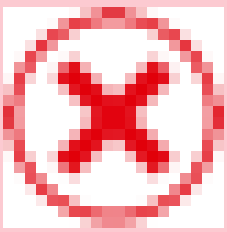
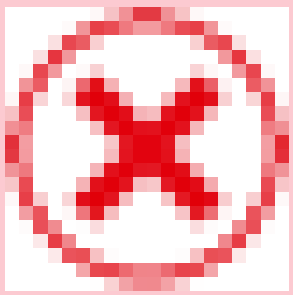
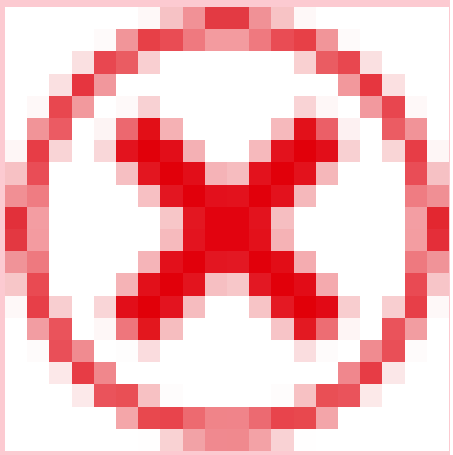
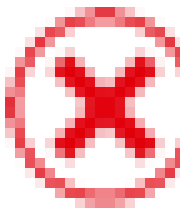
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_job、sn_sec_cmn.

その他のロールの情報：

sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_it

(続く)

モジュール	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_cmn.re
フィールド値変換					
フィールドマッピング					
オンデマンドオーケストレーション					

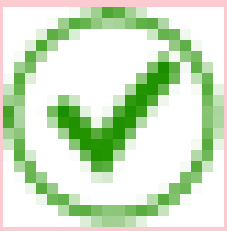
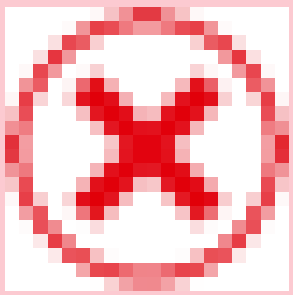
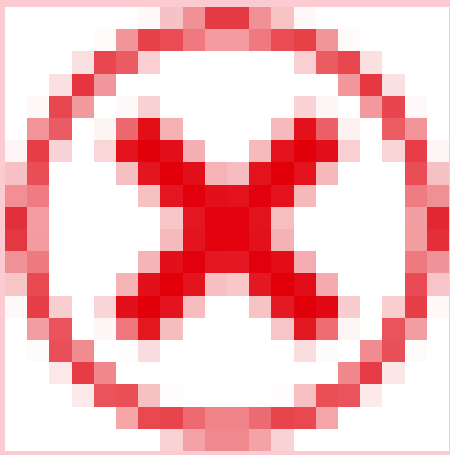
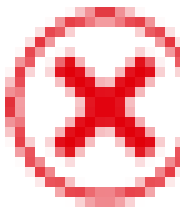
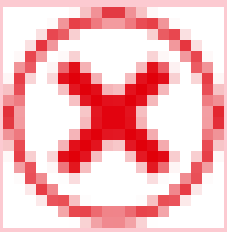
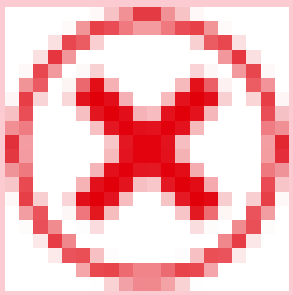
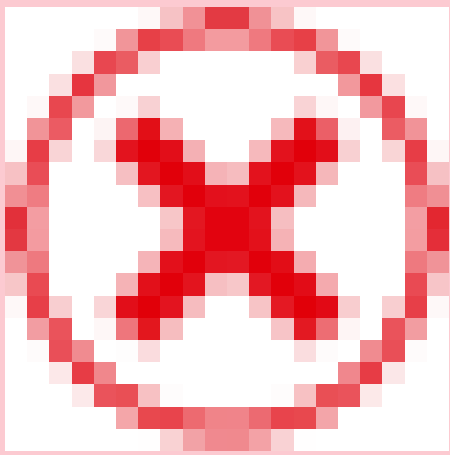
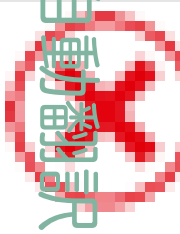
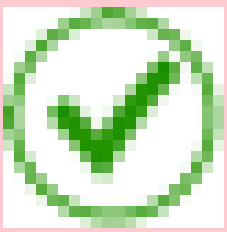
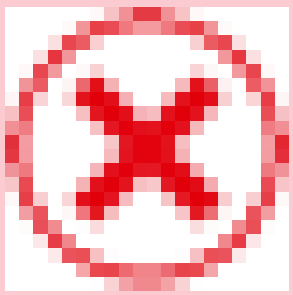
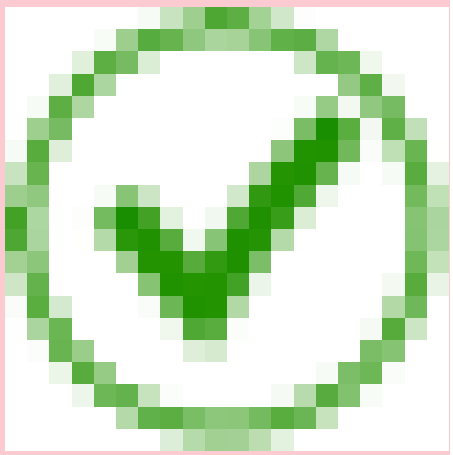
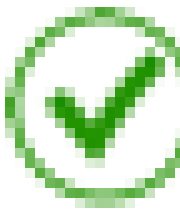
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_job、sn_sec_cmn.

その他のロールの情報：

sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_it

(続く)

モジュール	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_cmn.re
オペレーティングシステムグループ					
SecOps 登録アプリケーション					
バックグラウンドジョブ構成					
CMDB					

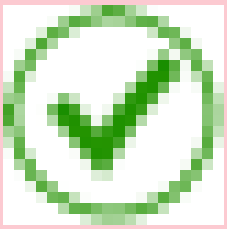
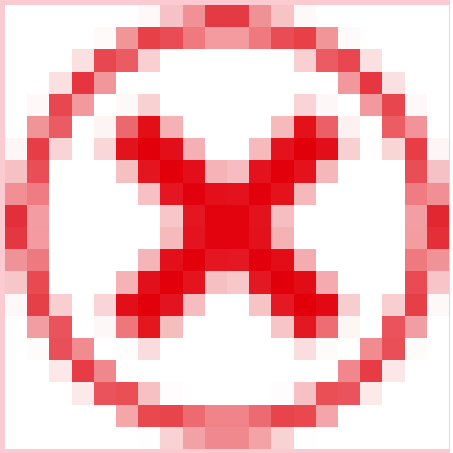
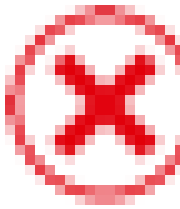
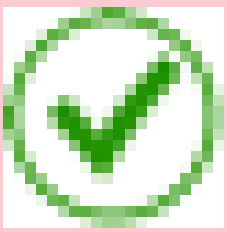
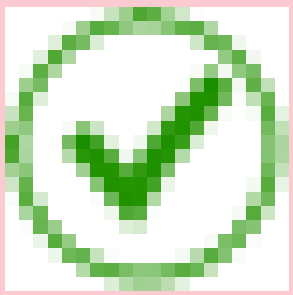
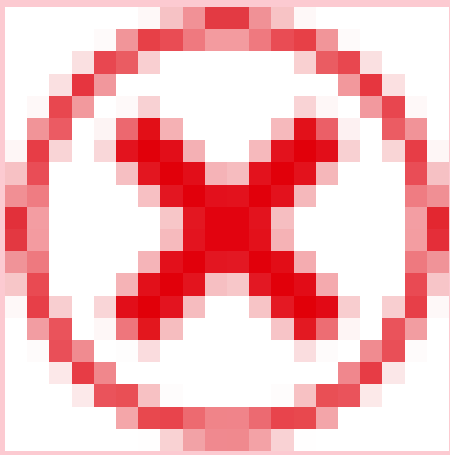
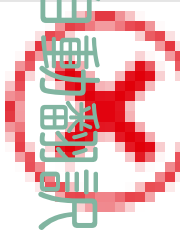
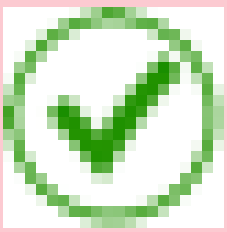
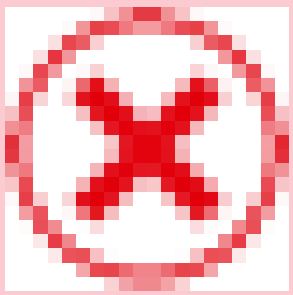
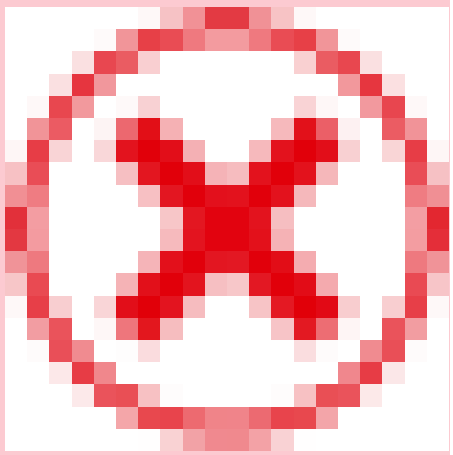
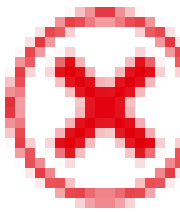
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_job、sn_sec_cmn.

その他のロールの情報：

sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_it

(続く)

モジュール	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_cmn.re
CI ルックアップルール					
検出されたアイテム					
一致しない検出されたアイテムを調整					

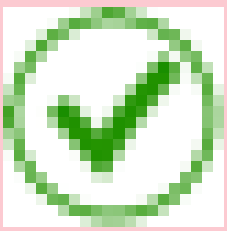
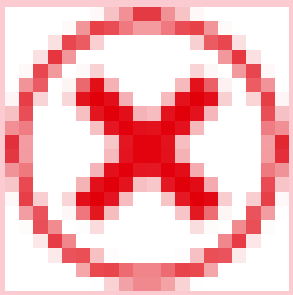
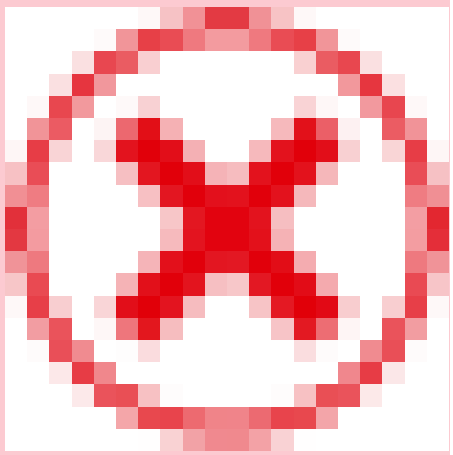
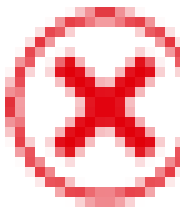
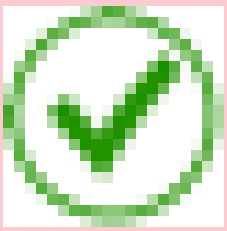
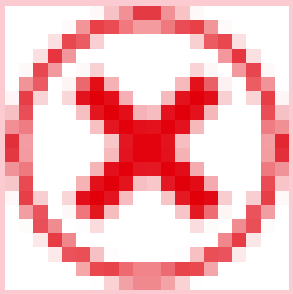
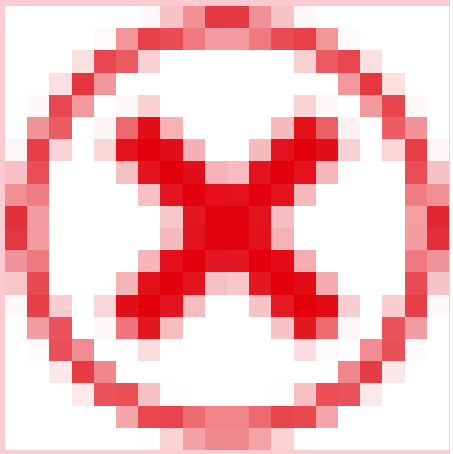
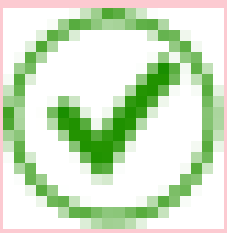
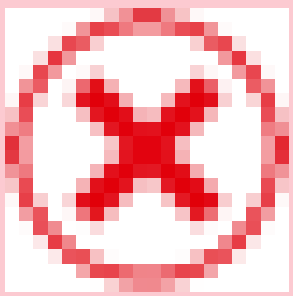
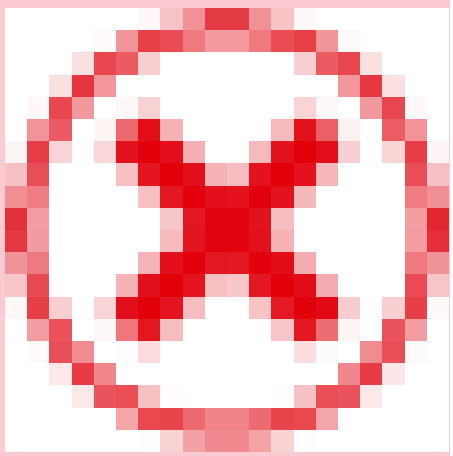
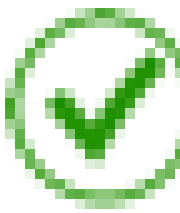
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_job、sn_sec_cmn.

その他のロールの情報：

sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_it

(続く)

モジュール	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_cmn.re
検出されたコンテナイメージ					
WatchDog					
構成					
概要					

自動翻訳

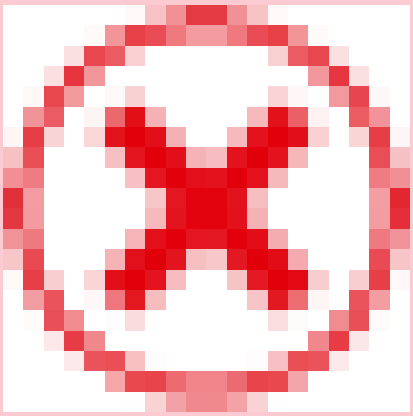
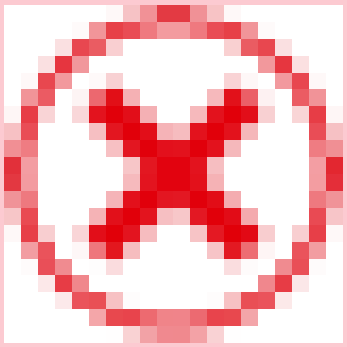
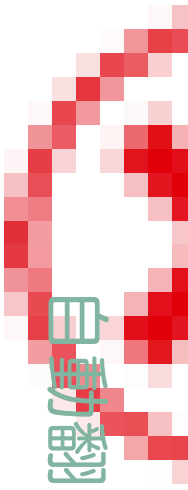
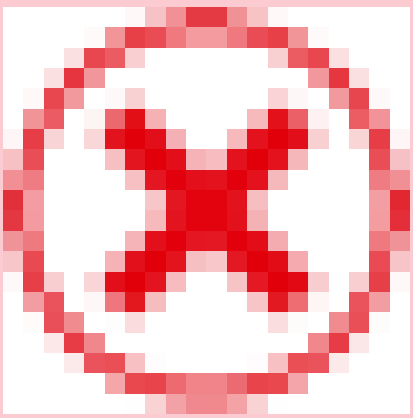
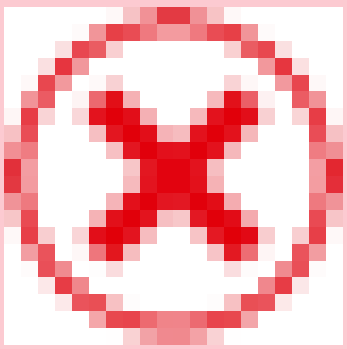
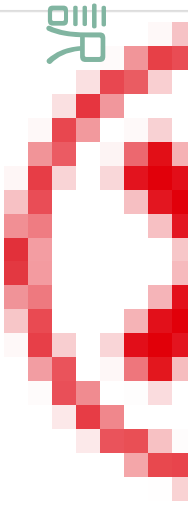
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
(メインアプリグループ)					
統合					
統合機能フロー					

自動翻訳

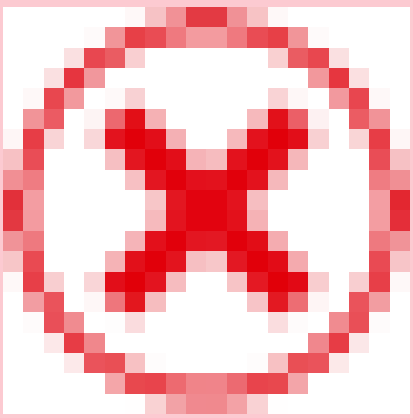
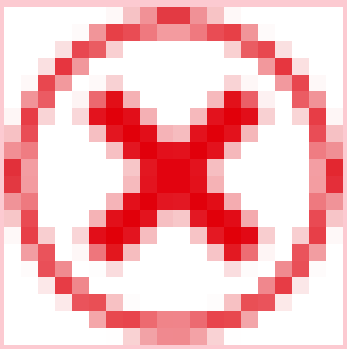
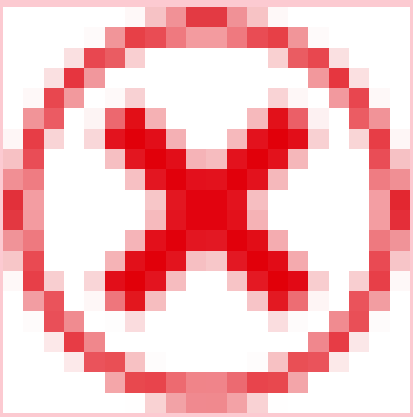
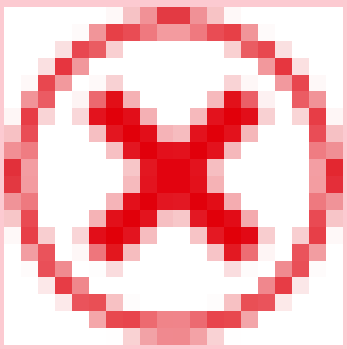
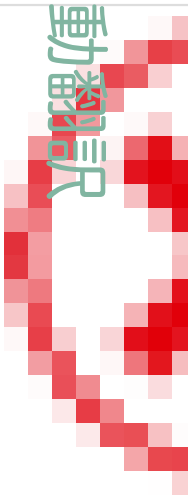
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
機能実行					
機能実装レート制限					

自動翻訳

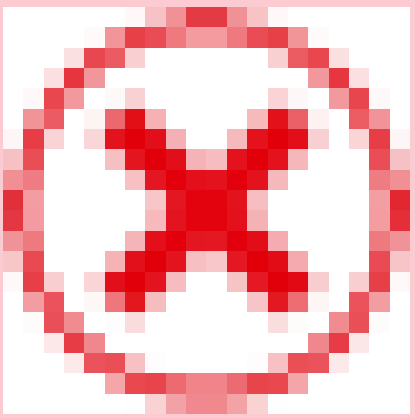
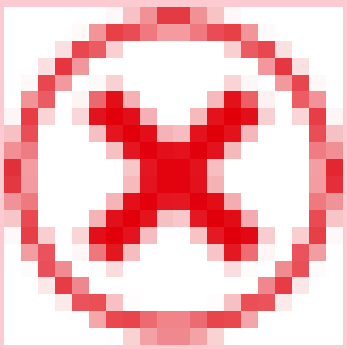
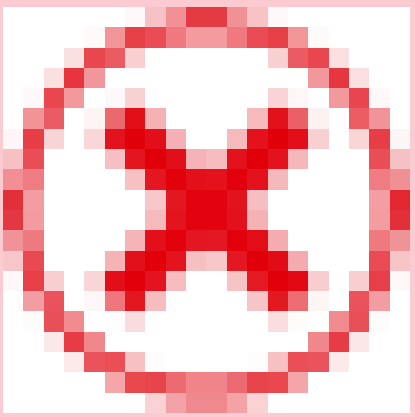
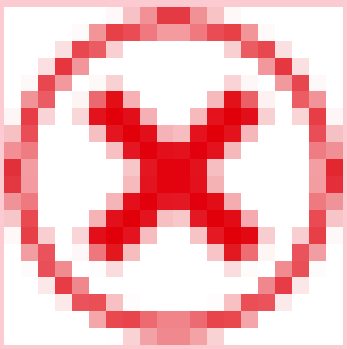
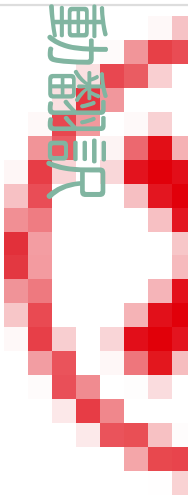
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
統合構成					
サイティング検索構成					

自動翻訳

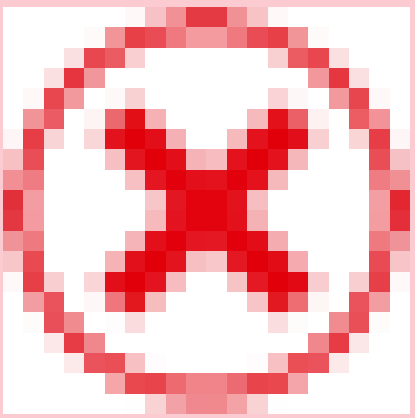
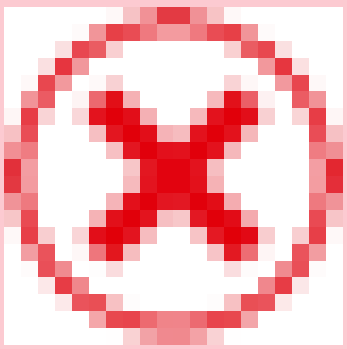
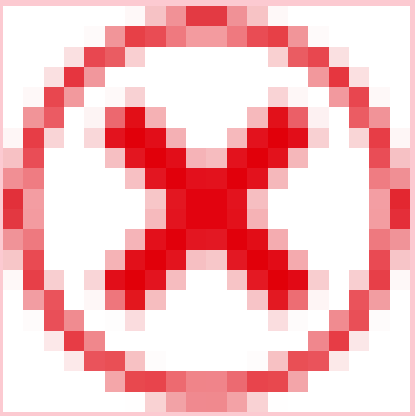
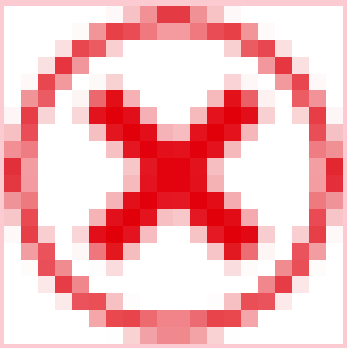
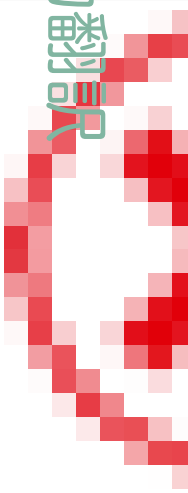
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
統合機能					
統合					
統合機能フロー					

自動翻訳

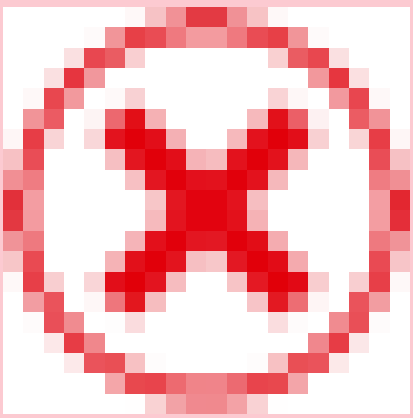
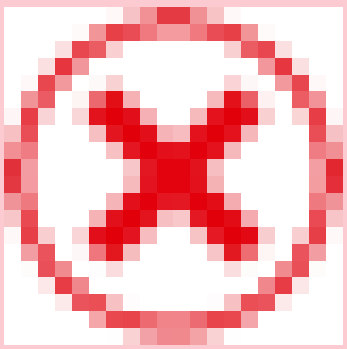
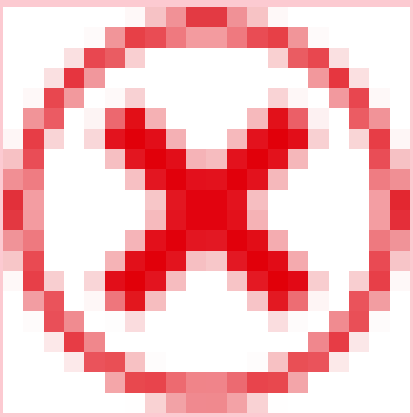
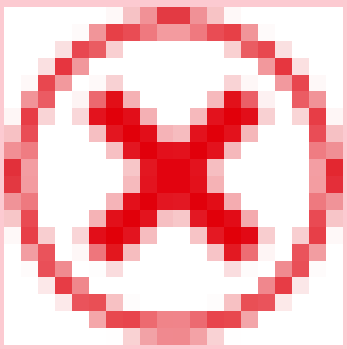
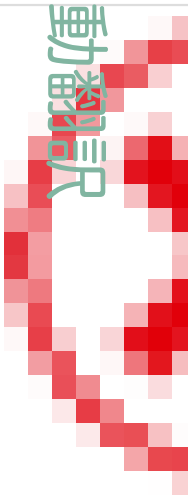
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
機能実行					
機能実装レート制限					

自動翻訳

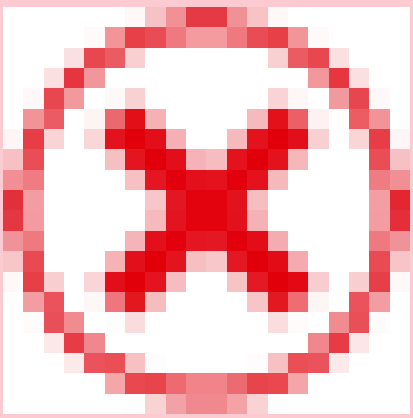
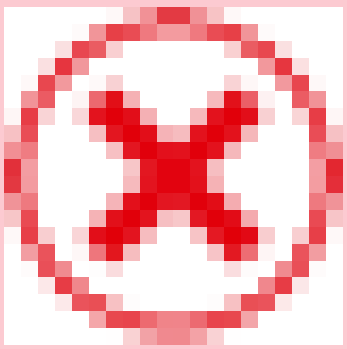
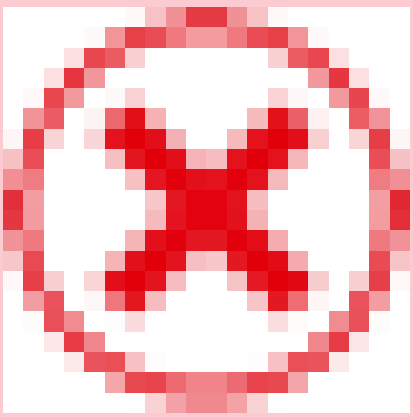
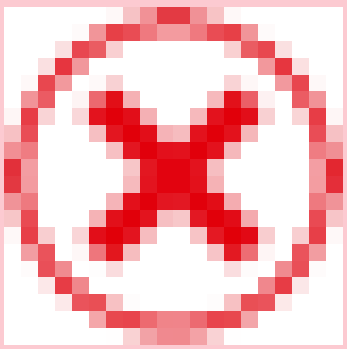
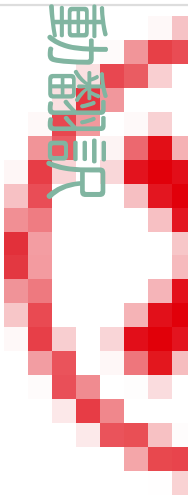
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
統合構成					
サイティング検索構成					

自動翻訳

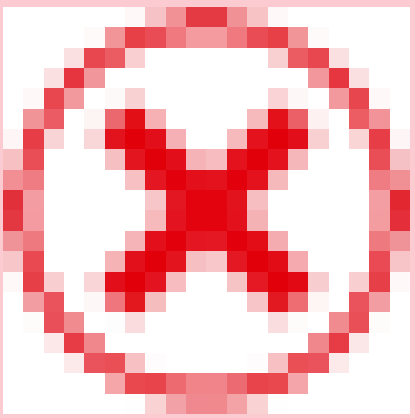
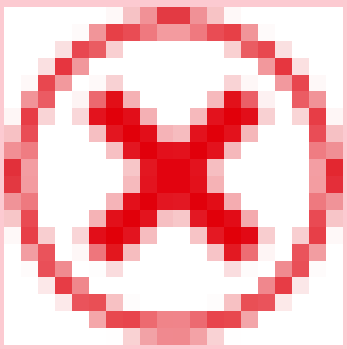
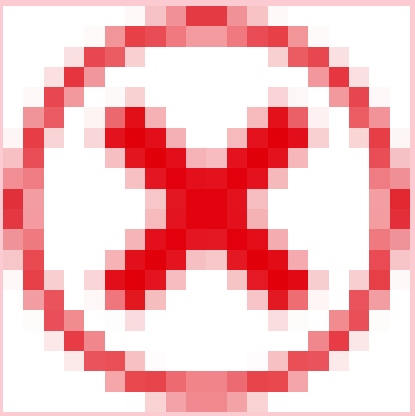
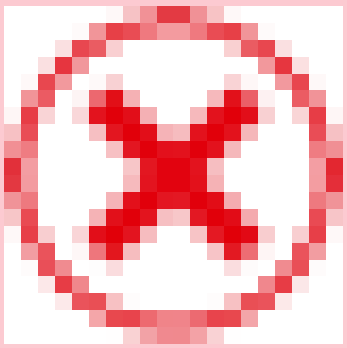
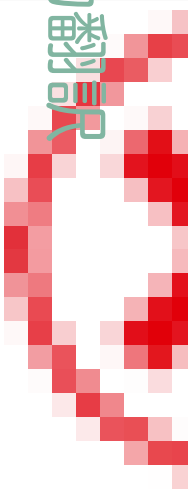
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
統合機能					
メール処理					
メール解析					

自動翻訳

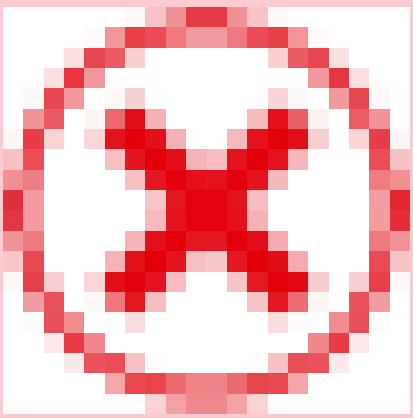
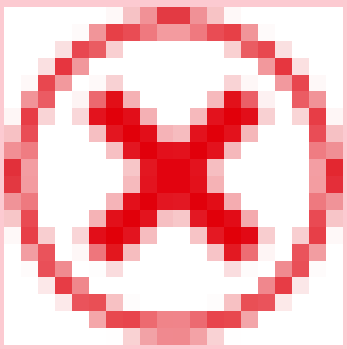
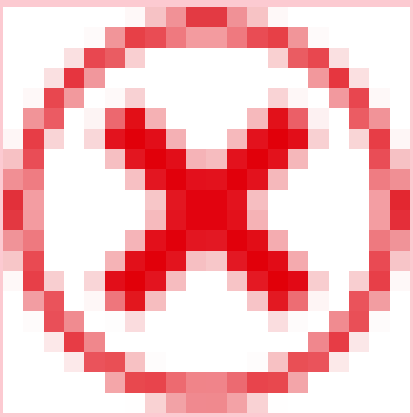
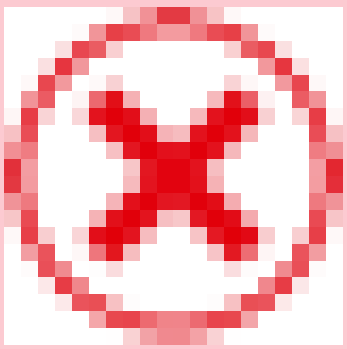
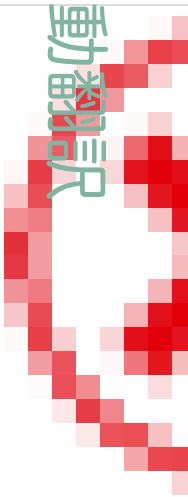
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
重複ルール					
プロパティ					

自動翻訳

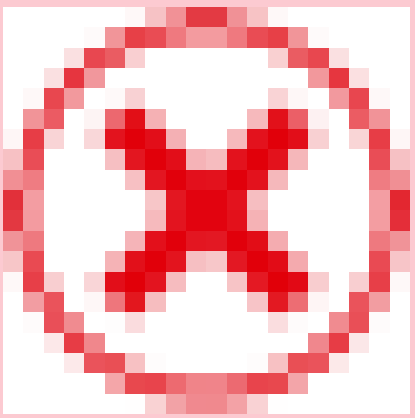
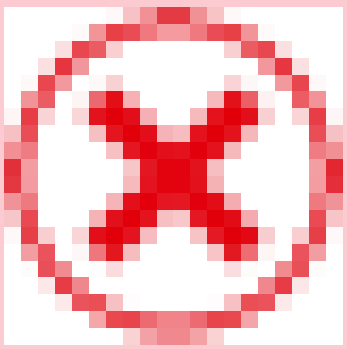
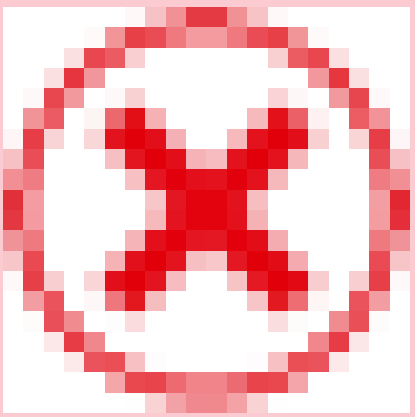
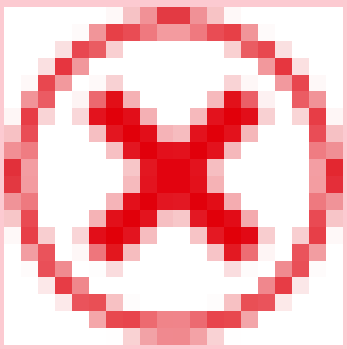
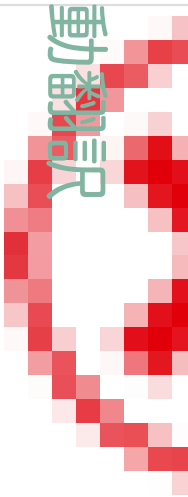
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
一致しないメール					
取り込みルール - ユーザーから報告されたフィッシング					

自動翻訳

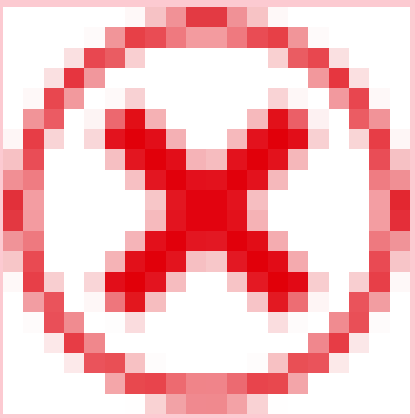
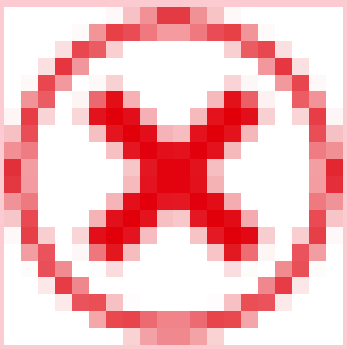
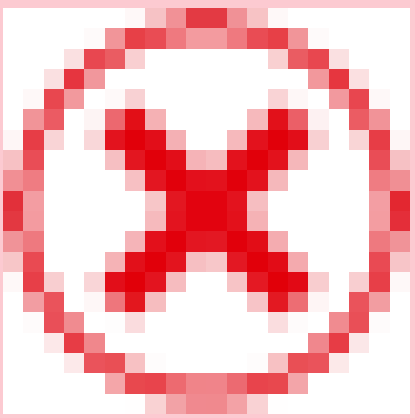
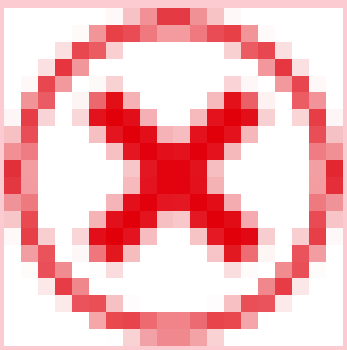
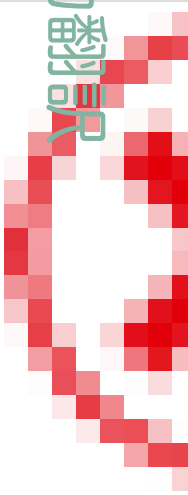
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
ユーザーから報告されたフィッシングプロパティ					
グループ					
フィルターグループ					

自動翻訳

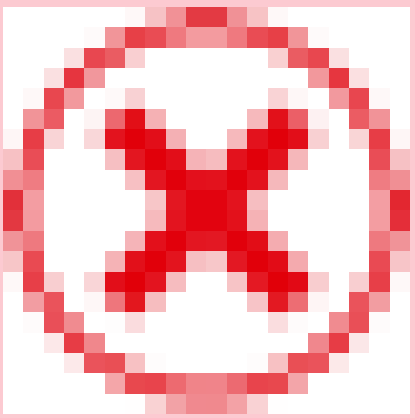
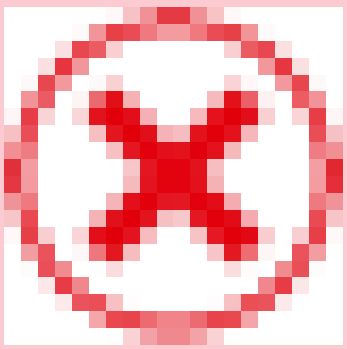
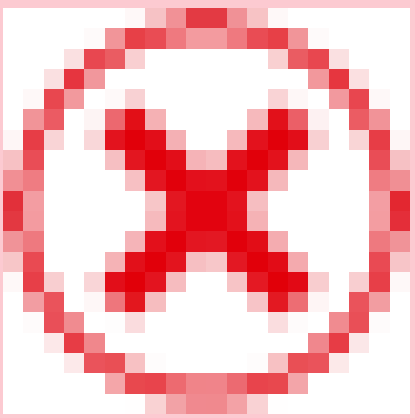
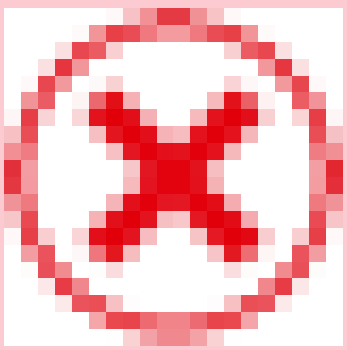
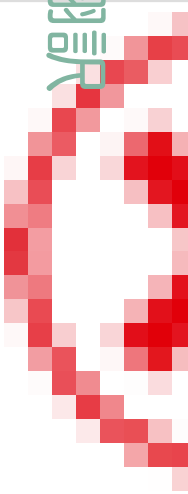
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
エスカレーション					
データ拡張					
セキュリティタグ					
グループ					

自動翻訳

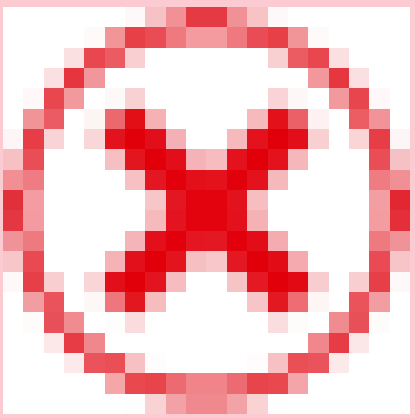
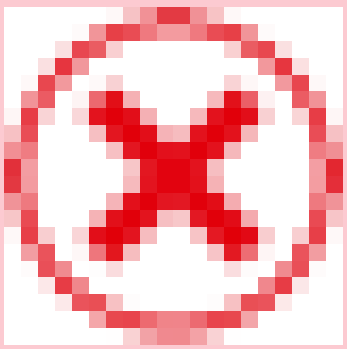
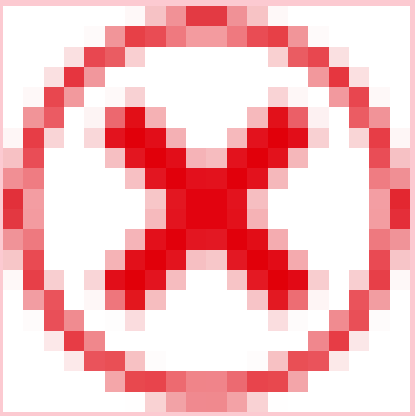
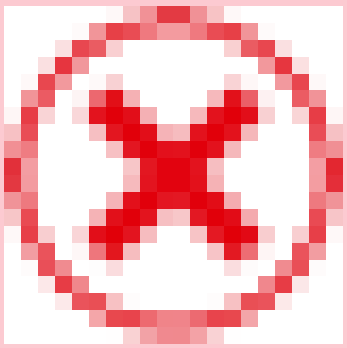
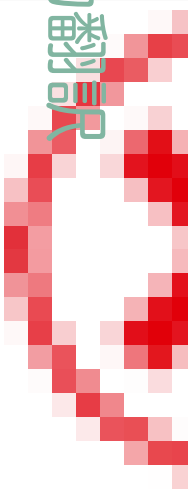
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
Tags					
ワークフロー					
実行トラッキング					

自動翻訳

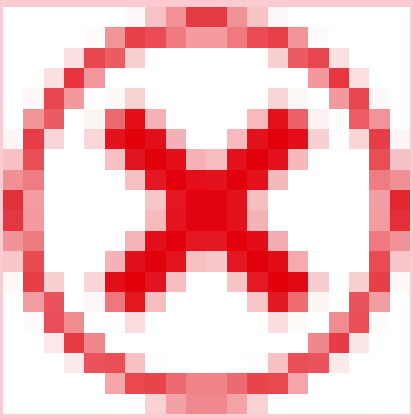
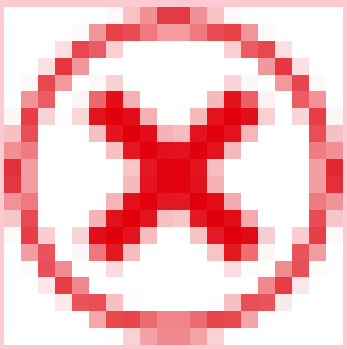
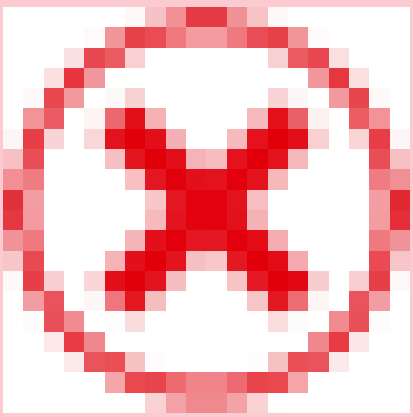
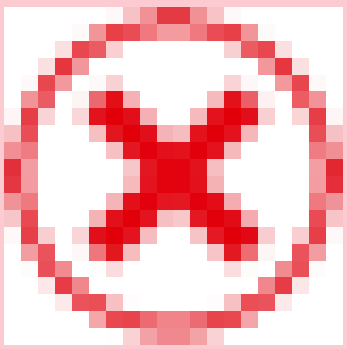
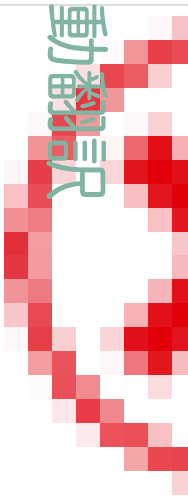
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
セキュリティワークフローを表示					
ワークフロートリガー					
ユーティリティ					

自動翻訳

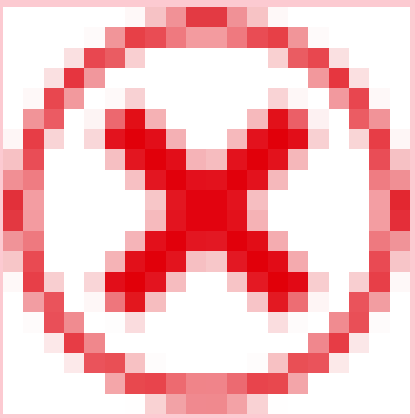
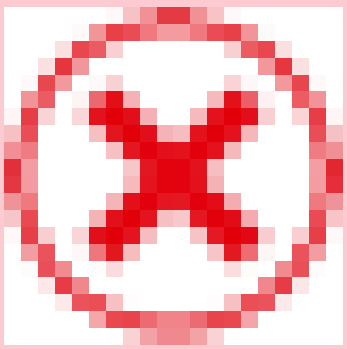
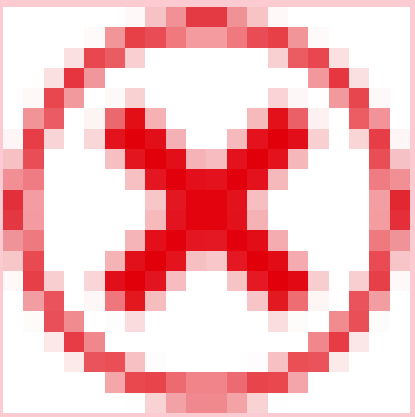
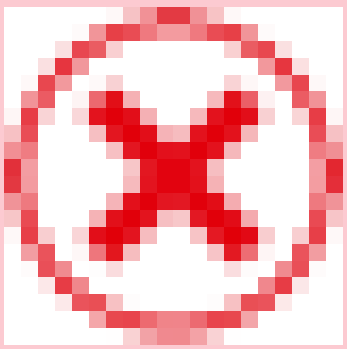
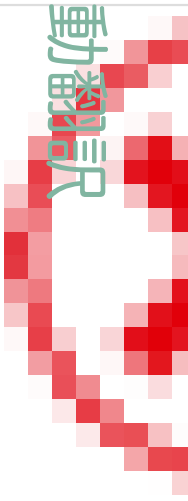
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
拡張データマッピング					
フィールド値変換					

自動翻訳

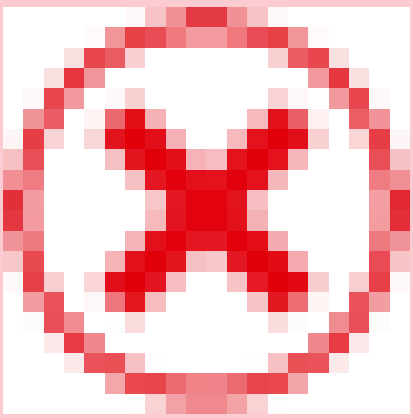
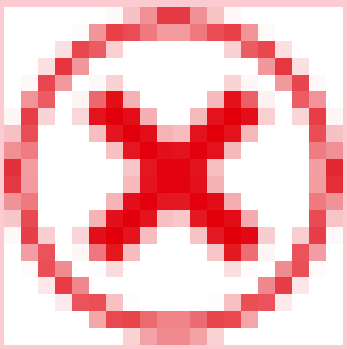
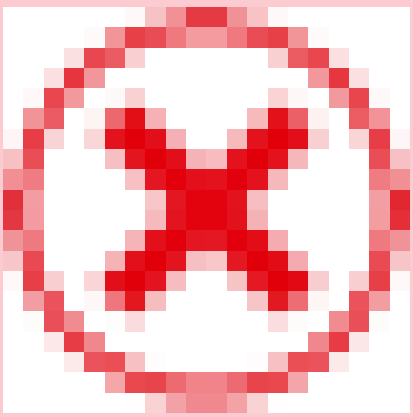
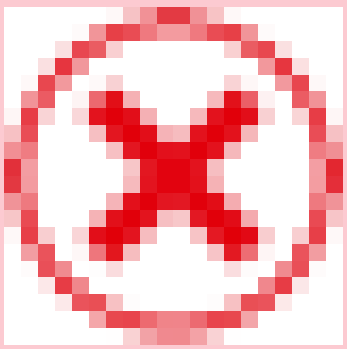
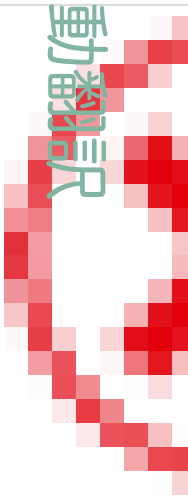
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
フィールドマッピング					
オンデマンドオーケストレーション					

自動翻訳

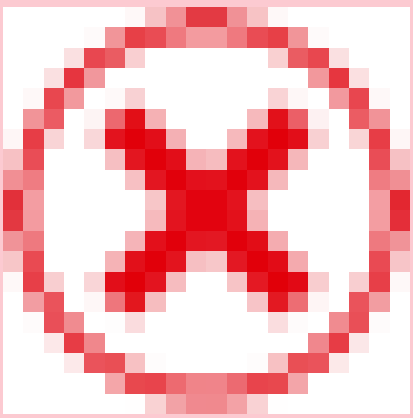
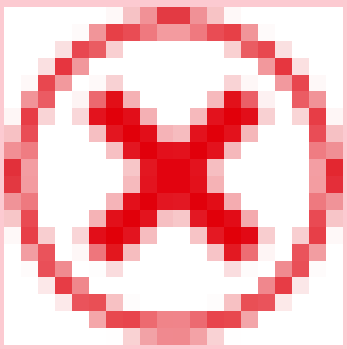
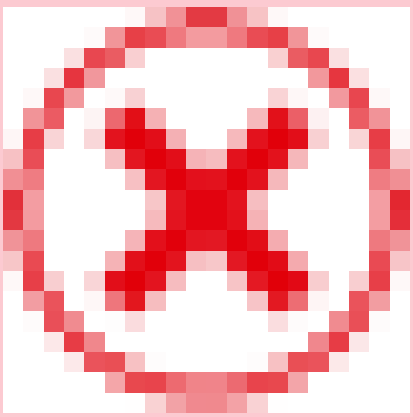
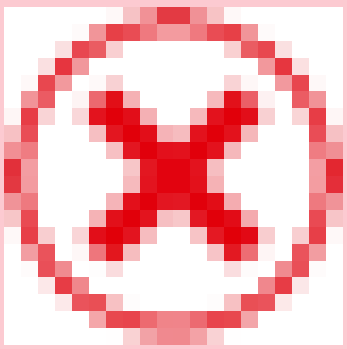
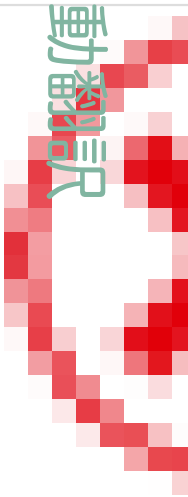
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
オペレーティングシステムグループ					
SecOps 登録アプリケーション					

自動翻訳

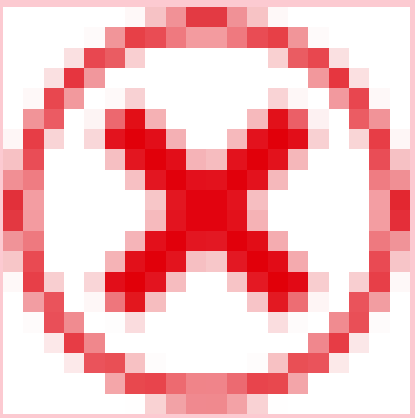
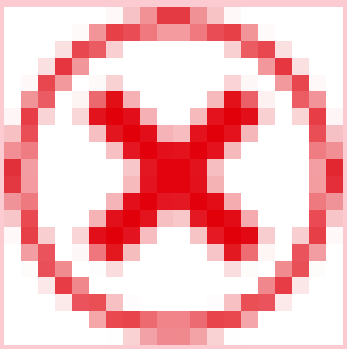
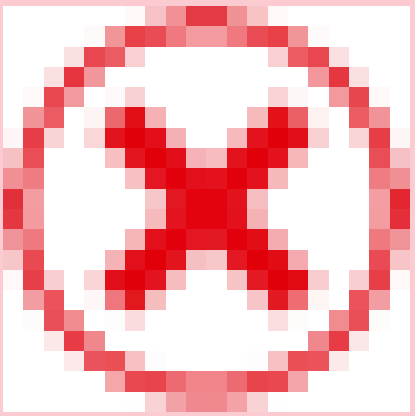
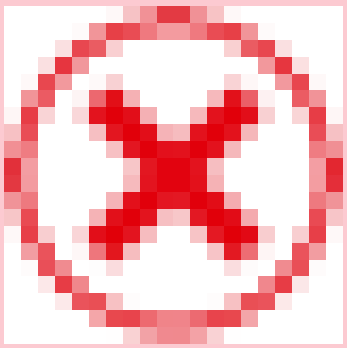
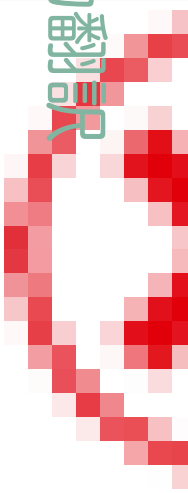
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
バックグラウンドジョブ構成					
CMDB					
CI ルックアップルール					

自動翻訳

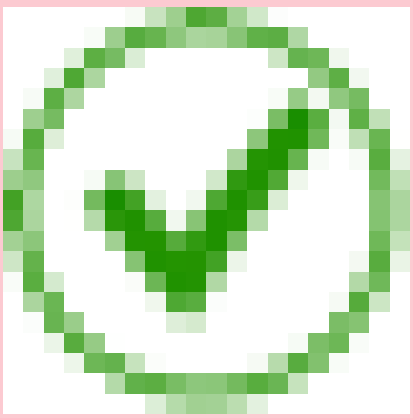
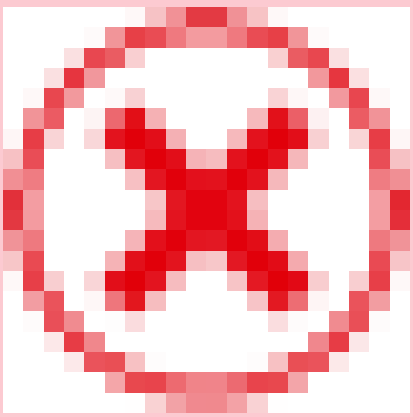
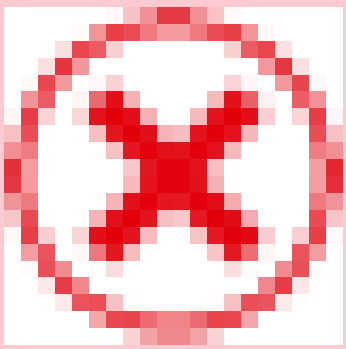
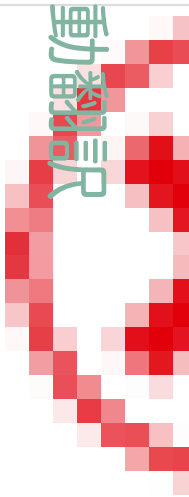
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
検出されたアイテム					
一致しない検出されたアイテムを調整					

自動翻訳

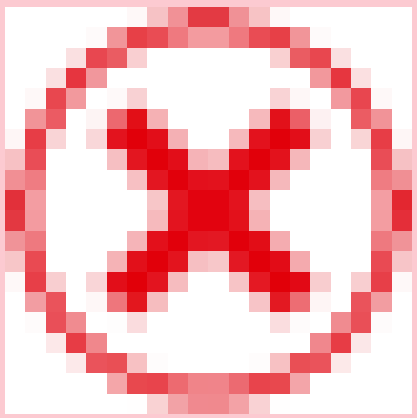
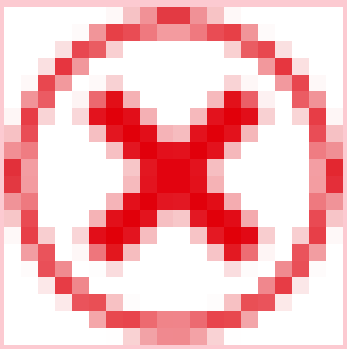
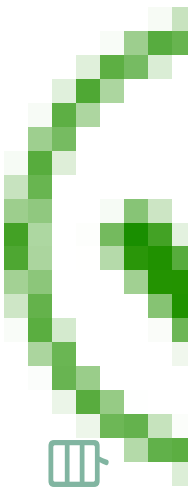
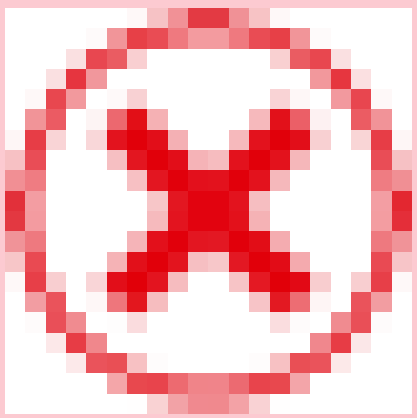
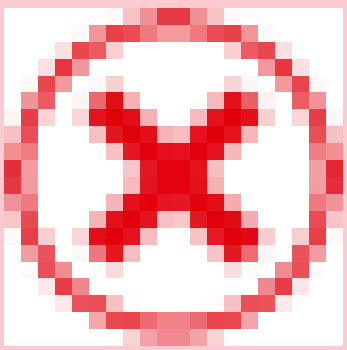
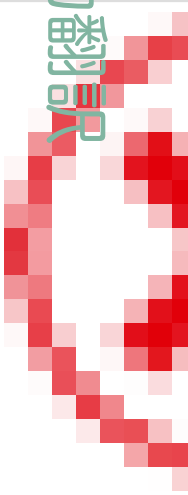
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
検出されたコンテナイメージ					
WatchDog					
構成					

自動翻訳

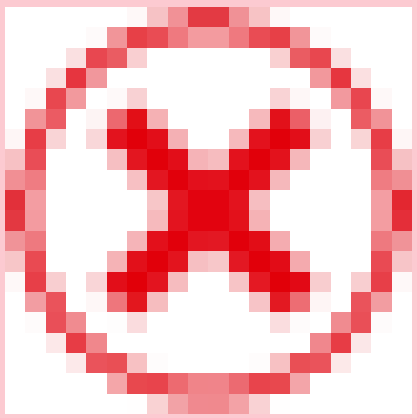
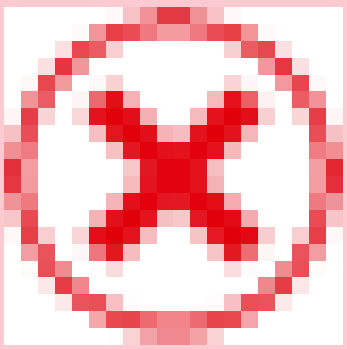
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.reclassify_unmatch_ci、sn_si.admin、sn_si.basic、sn_vul.read_discovered_item、sn_vul_conta

その他のロールの情報：

admin、sn_sec_cmn.admin、sn_sec_cmn.ci_manager、sn_sec_cmn.manage_background_

(続く)

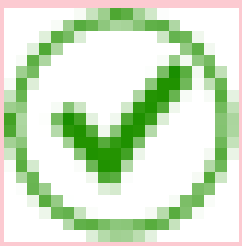
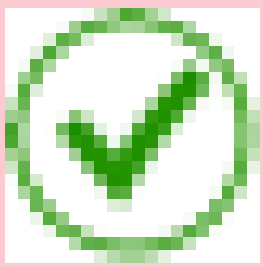
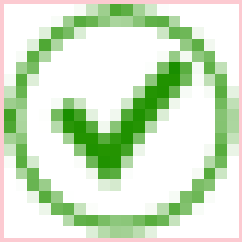
モジュール	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.basic	sn_vul.read_discovered_item	sn_vul_containe
概要					

[End]

[store-future: BEGIN review]

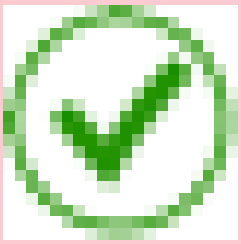
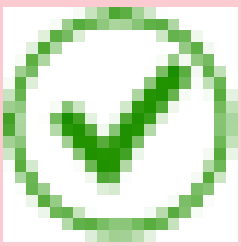
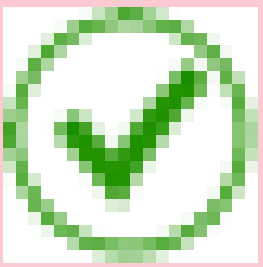
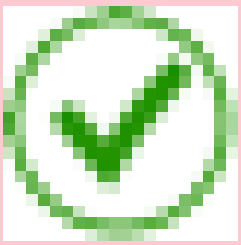
Splunk Integration のロール別のモジュールアクセス

Splunk Integration では、特定のロールがアクセスできるメニューアイテムが表示されます。

モジュール	sn_si.admin	sn_si.analyst
(メインアプリグループ)		
Splunk イベントプロファイル		
Splunk フィールド変換		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

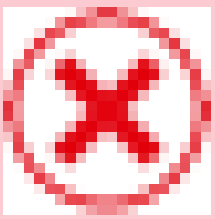
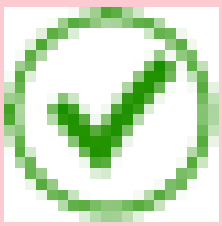
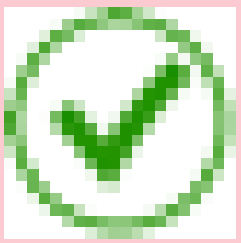
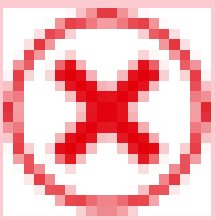
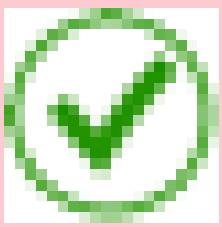
モジュール	sn_si.admin	sn_si.analyst
タスクに対する Splunk イベント		
Splunk イベントインポート		
Splunk Integration 設定		

[End]

[store-future: BEGIN review]

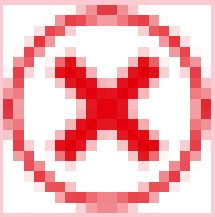
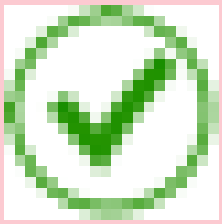
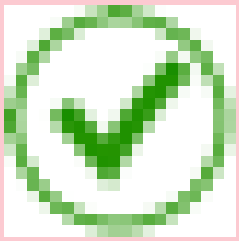
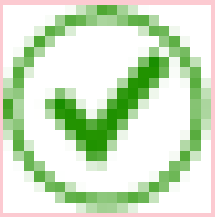
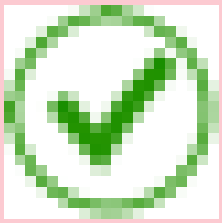
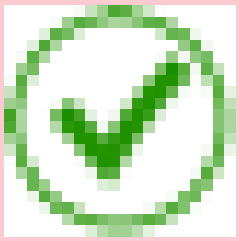
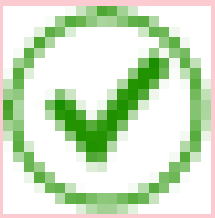
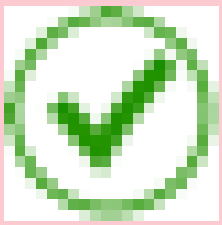
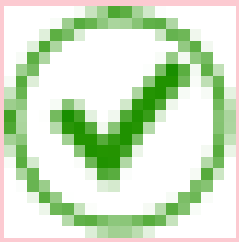
Symantec DLP 統合のロール別のモジュールアクセス

Symantec DLP 統合では、特定のロールがアクセスできるメニューアイテムが表示されます。

モジュール	agent_admin	sn_dlir.admin	sn_dlir.analyst
(メインアプリグループ)			
インシデントプロファイル			
インシデント状況マッピング			

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

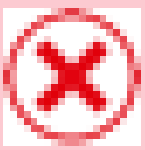
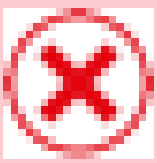
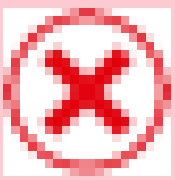
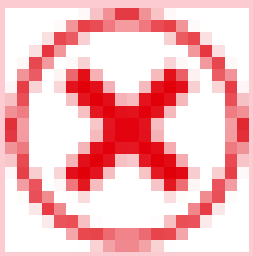
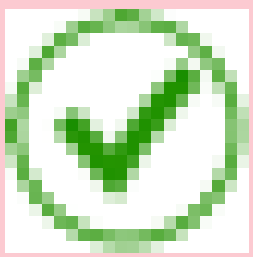
モジュール	agent_admin	sn_dlir.admin	sn_dlir.analyst
設定			
MID アプリケーション			
MID サーバー			

[End]

[store-future: BEGIN review]

脅威インテリジェンスのロール別のモジュールアクセス

脅威インテリジェンスでは、特定のロールがアクセスできるメニューアイテムが表示されます。

モジュール	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read	sn_ti.read	sn_ti.w
(メインアプリグループ)								
オブジェクト								
オブジェクト								
IoC リポジトリ								
攻撃モード/方法								

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read	sn_ti.read	sn_ti.w
インジケーター	✓	✓	✓	✓	✓	✓	✓	✓
観測事象	✓	✓	✓	✓	✓	✓	✓	✓
攻撃パターン	✓	✓	✓	✓	✓	✓	✓	✓
キャンペーン	✓	✓	✓	✓	✓	✓	✓	✓
対処措置	✓	✓	✓	✓	✓	✓	✓	✓
ID	✓	✓	✓	✓	✓	✓	✓	✓

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read	sn_ti.read	sn_ti.w
インフラストラクチャ	✓	✓	✓	✓	✓	✓	✓	✓
場所	✓	✓	✓	✓	✓	✓	✓	✓
マルウェア	✓	✓	✓	✓	✓	✓	✓	✓
侵入セット	✓	✓	✓	✓	✓	✓	✓	✓
攻撃者	✓	✓	✓	✓	✓	✓	✓	✓
マルウェア分析	✓	✓	✓	✓	✓	✓	✓	✓

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read	sn_ti.read	sn_ti.w
観測データ	✓	✓	✓	✓	✓	✓	✓	✓
脅威グループ化	✓	✓	✓	✓	✓	✓	✓	✓
マーキング定義	✓	✓	✓	✓	✓	✓	✓	✓
脅威メモ	✓	✓	✓	✓	✓	✓	✓	✓
脅威に関する意見	✓	✓	✓	✓	✓	✓	✓	✓
脅威レポート	✓	✓	✓	✓	✓	✓	✓	✓

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read	sn_ti.read	sn_ti.w
インジケーターのサイティング	✓	✓	✓	✓	✓	✓	✓	✓
オブジェクトのサイティング	✓	✓	✓	✓	✓	✓	✓	✓
脆弱性	✓	✓	✓	✓	✓	✓	✓	✓
ツール	✓	✓	✓	✓	✓	✓	✓	✓
オブジェクトとオブジェクトの関係	✓	✓	✓	✓	✓	✓	✓	✓
オブジェクトとインジケーターの関係	✓	✓	✓	✓	✓	✓	✓	✓

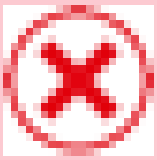
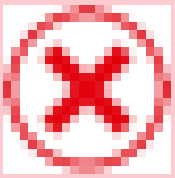
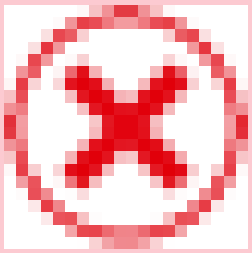
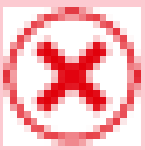
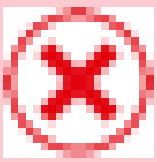
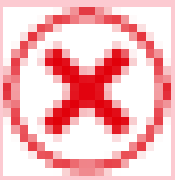
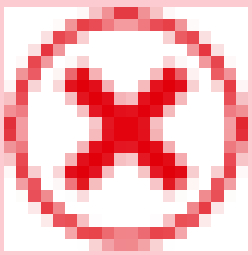
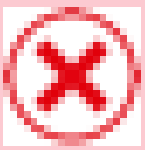
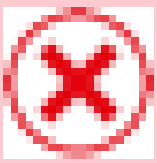
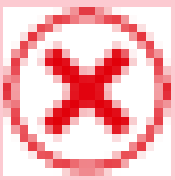
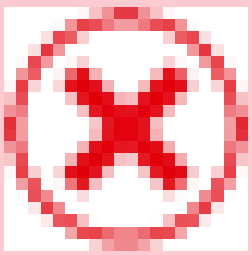
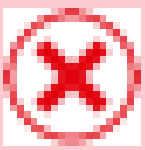
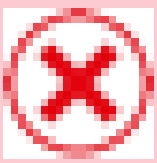
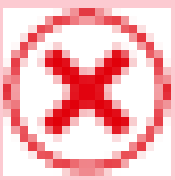
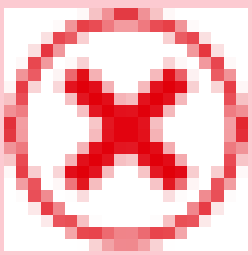
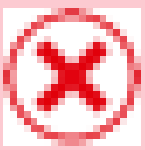
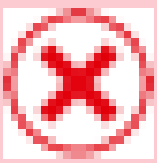
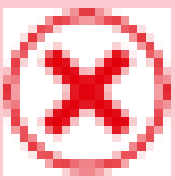
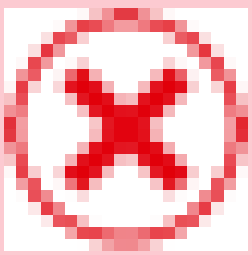
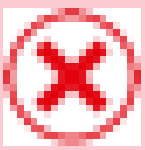
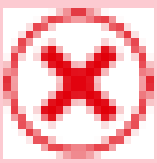
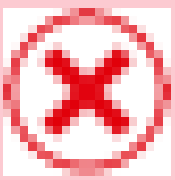
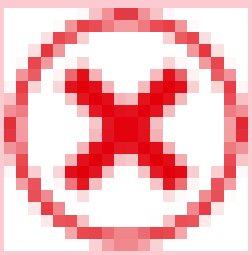
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read	sn_ti.read	sn_ti.w
オブジェクトと観測事象の関係	✓	✓	✓	✓	✓	✓	✓	✓
ソース								
脅威のソース	✗	✗	✗	✗	✓	✗	✗	✓
TAXII プロファイル	✗	✗	✗	✗	✓	✗	✗	✓
外部情報								
データ違反ライブラリ	✓	✓	✓	✓	✓	✓	✓	✓
WHOIS ライブラリ	✓	✓	✓	✓	✓	✓	✓	✓
管理								
プロパティ	✗	✗	✗	✗	✓	✗	✗	✗

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read	sn_ti.read	sn_ti.w
攻撃メカニズム								
攻撃の動機								
ディスカバリー方法								
フィード								
インジケータータイプ								
インフラストラクチャタイプ								

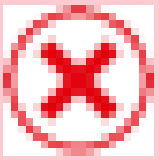
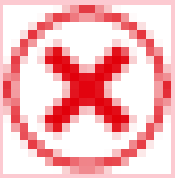
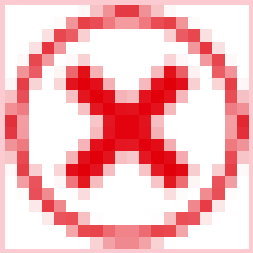
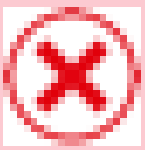
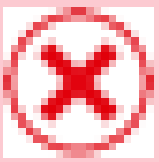
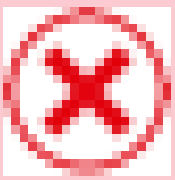
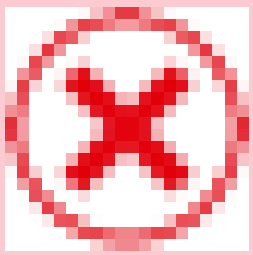
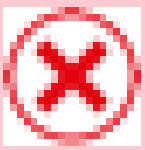
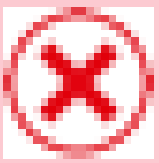
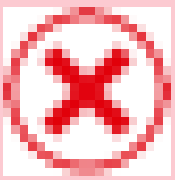
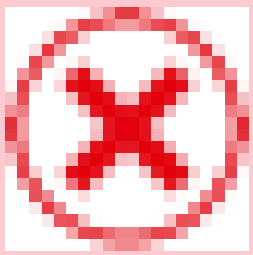
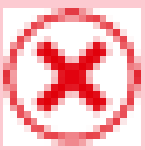
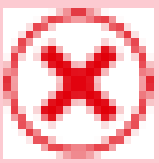
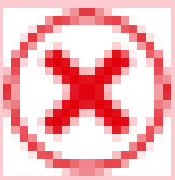
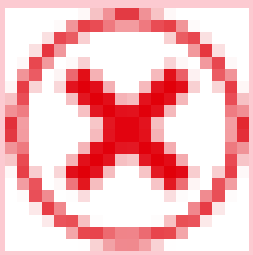
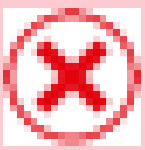
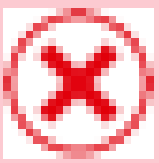
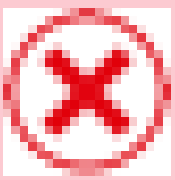
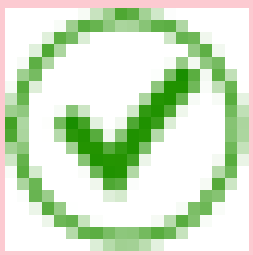
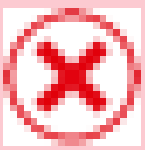
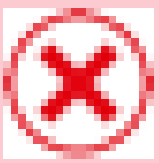
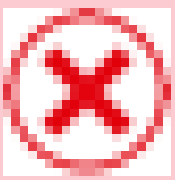
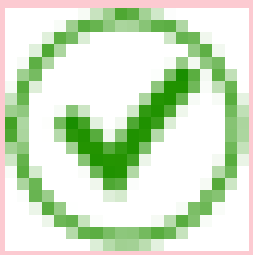
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read	sn_ti.read	sn_ti.w
意図した効果	✗	✗	✗	✗	✓	✗	✗	✗
マルウェア機能	✗	✗	✗	✗	✓	✗	✗	✗
マルウェアタイプ	✗	✗	✗	✗	✓	✗	✗	✗
通知	✗	✗	✗	✗	✓	✗	✗	✗
観測事象タイプ	✗	✗	✗	✗	✓	✗	✗	✗
レート制限定義	✗	✗	✗	✗	✓	✗	✗	✗

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read	sn_ti.read	sn_ti.w
レポートタイプ								
攻撃者ロール								
攻撃者タイプ								
ツールタイプ								
ケース管理								
すべてのケース								
オープンケース								

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read	sn_ti.read	sn_ti.w
自分のケース	✗	✗	✗	✗	✗	✓	✗	✗
MITRE ATT&CK リポジトリ								
概要	✓	✓	✓	✓	✓	✓	✓	✓
マトリクス	✓	✓	✓	✓	✓	✓	✓	✓
テクニック	✓	✓	✓	✓	✓	✓	✓	✓
緩和	✓	✓	✓	✓	✓	✓	✓	✓
グループ	✓	✓	✓	✓	✓	✓	✓	✓

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read	sn_ti.read	sn_ti.w
マルウェア	✓	✓	✓	✓	✓	✓	✓	✓
ツール	✓	✓	✓	✓	✓	✓	✓	✓
MITRE 関係	✓	✓	✓	✓	✓	✓	✓	✓
ヒートマップとナビゲーター	✓	✓	✓	✓	✓	✓	✓	✓
CVE テクニックマッピング	✓	✓	✓	✓	✓	✓	✓	✓
MITRE ATT&CK 管理								
データソースマッピング	✓	✓	✓	✓	✓	✓	✓	✓

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read	sn_ti.read	sn_ti.w
データコンポーネントマッピング	✓	✓	✓	✓	✓	✓	✓	✓
ディスカバリー範囲の定義	✓	✓	✓	✓	✓	✓	✓	✓
ディスカバリー範囲のマッピング	✓	✓	✓	✓	✓	✓	✓	✓
緩和対象範囲の定義	✓	✓	✓	✓	✓	✓	✓	✓
緩和対象範囲計算ツール	✓	✓	✓	✓	✓	✓	✓	✓
緩和対象範囲のマッピング	✓	✓	✓	✓	✓	✓	✓	✓

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュール	sn_si.admin	sn_si.analyst	sn_si.ciso	sn_si.manager	sn_ti.admin	sn_ti.case_user_read	sn_ti.read	sn_ti.w
テクニック抽出ルール	✓	✓	✓	✓	✓	✓	✓	✓
検出ルール - MITRE ATTCK マッピング	✓	✓	✓	✓	✓	✓	✓	✓
脅威グループ - テクニックヒートマップ定義	✓	✓	✓	✓	✓	✓	✓	✓
脅威グループ - MITRE ATTCK テクニックマッピング	✓	✓	✓	✓	✓	✓	✓	✓
プロパティ	✓	✗	✗	✗	✓	✗	✗	✗

[End]

[store-future: BEGIN review]

脆弱性対応のロール別のモジュールアクセス

脆弱性対応では、特定のロールがアクセスできるメニューアイテムが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

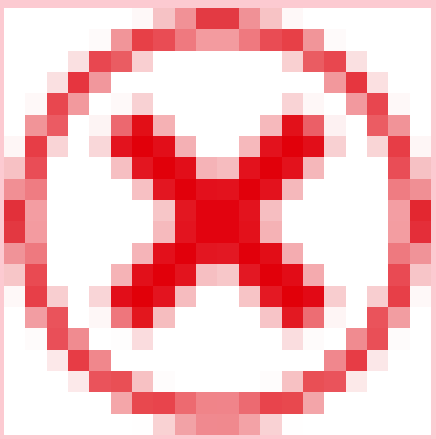
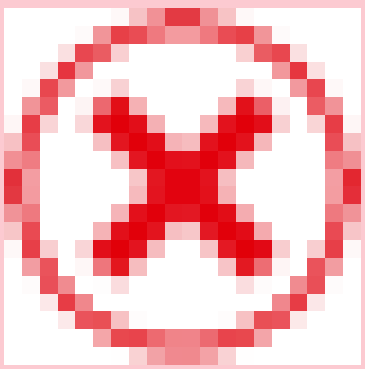
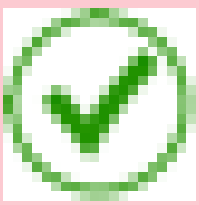
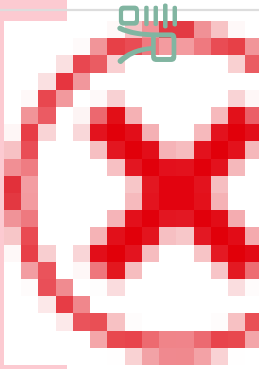
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
(メインアプリグループ)				
CISO ダッシュボード				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

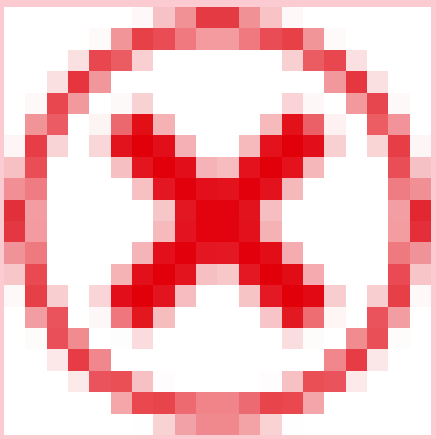
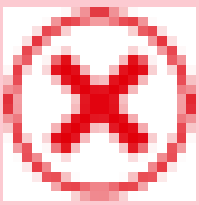
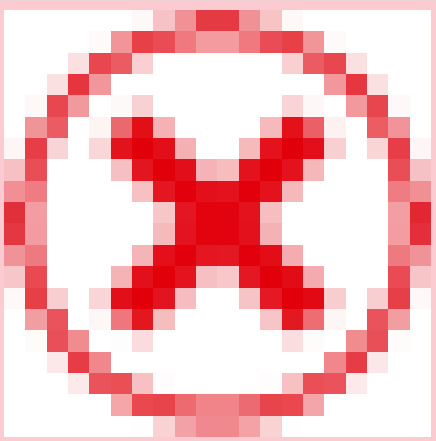
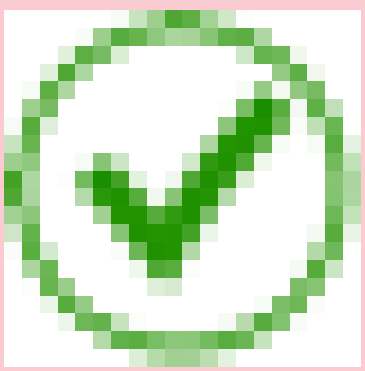
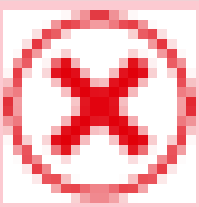
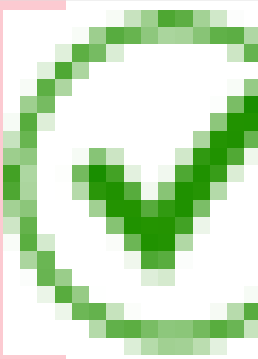
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
修復の概要				
脆弱性マネージャーのワークスペース				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

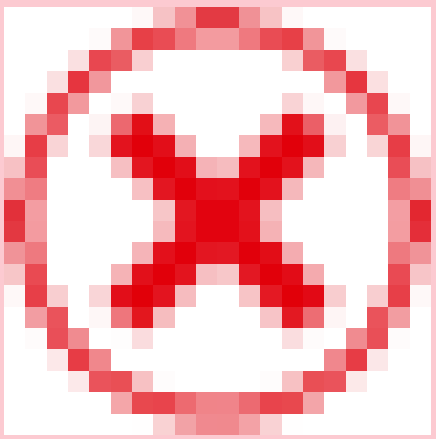
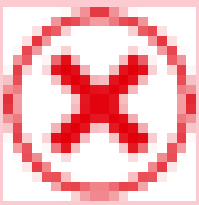
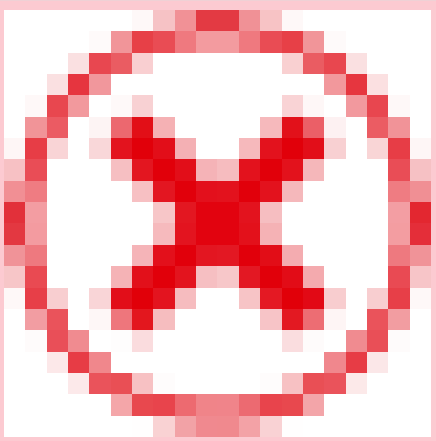
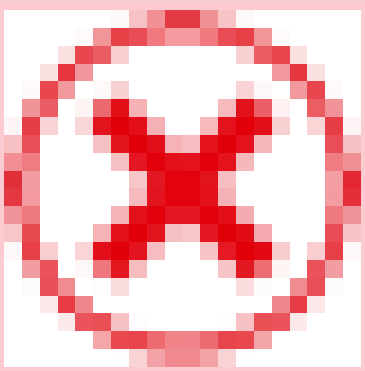
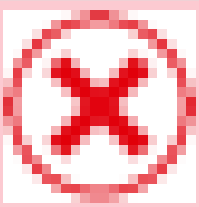
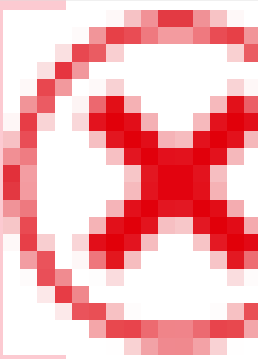
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
概要				
IT 修復ワークスペース				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

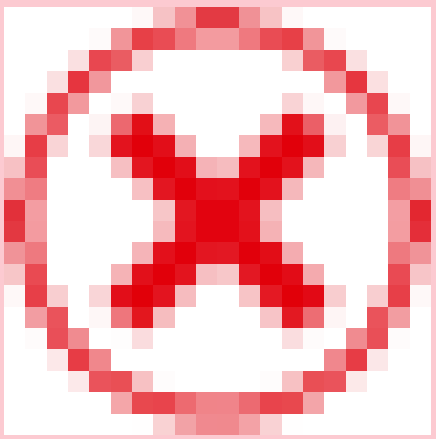
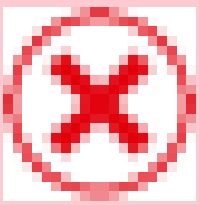
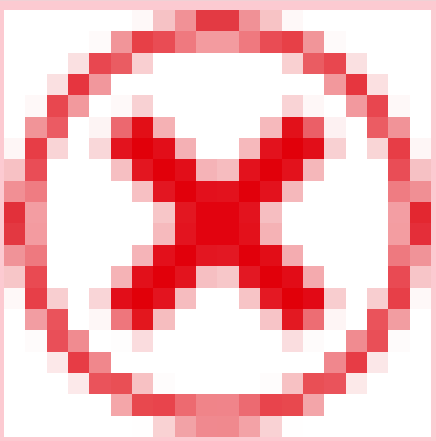
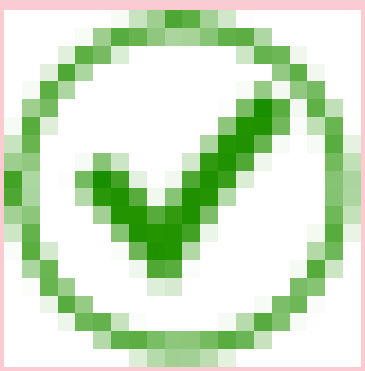
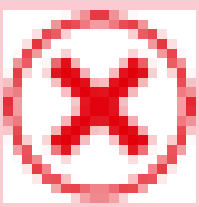
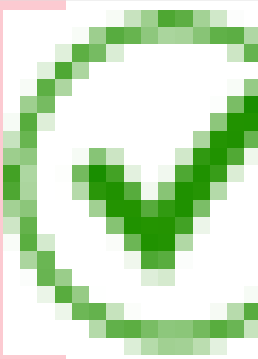
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
承認者の概要				
概要				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

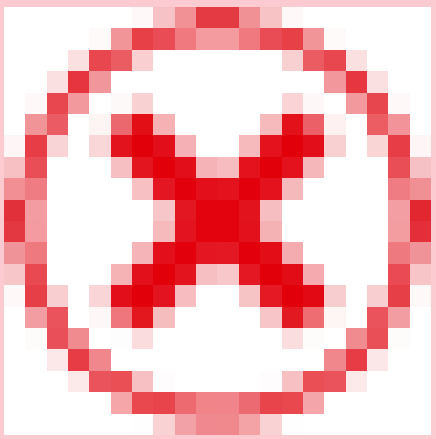
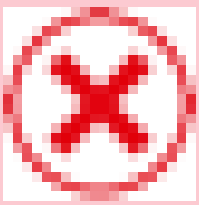
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
自分の承認				
修復タスク				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

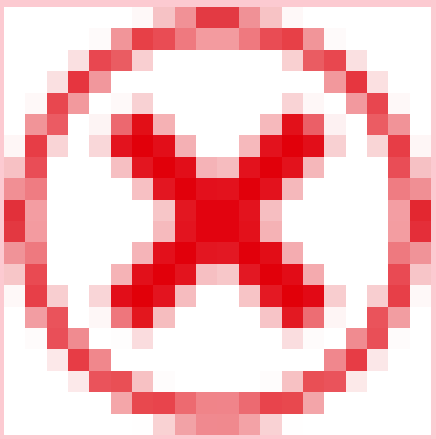
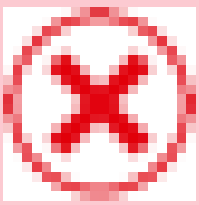
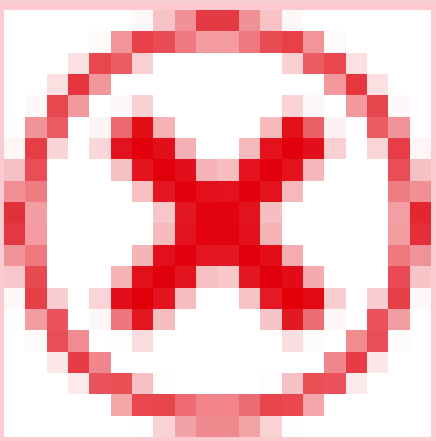
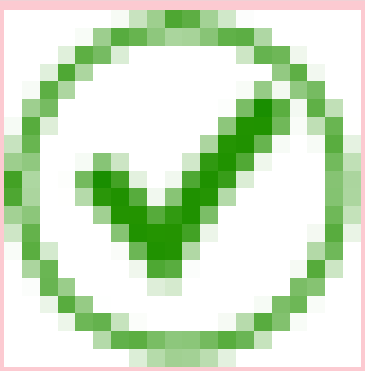
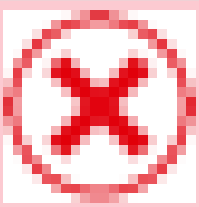
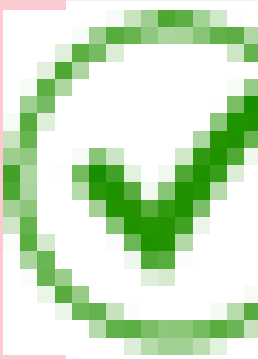
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
有効				
自分にアサイン済み				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

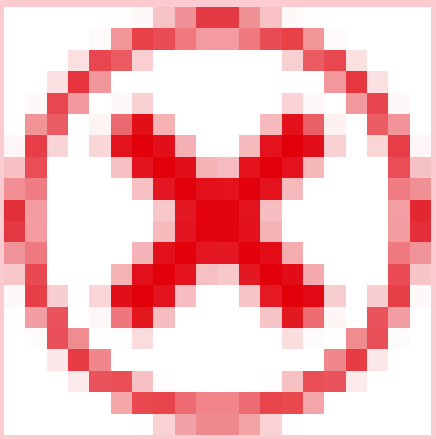
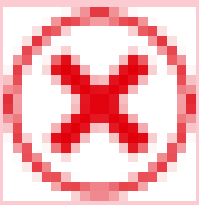
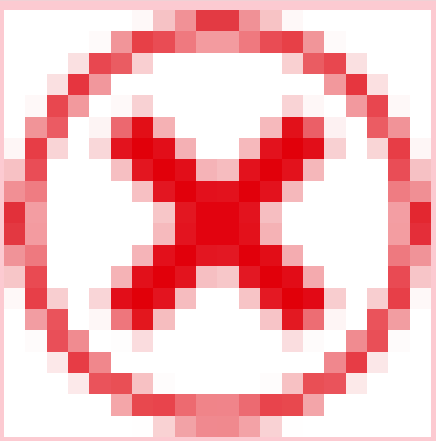
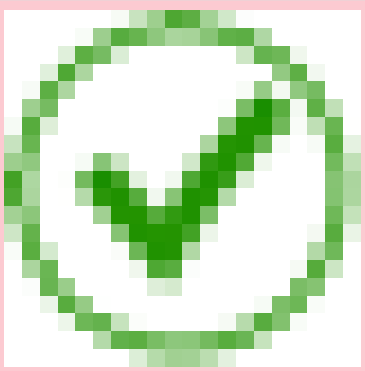
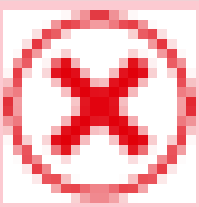
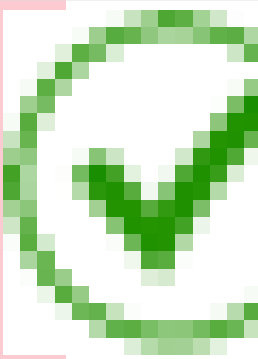
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
所属グループにアサイン済み				
すべて				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

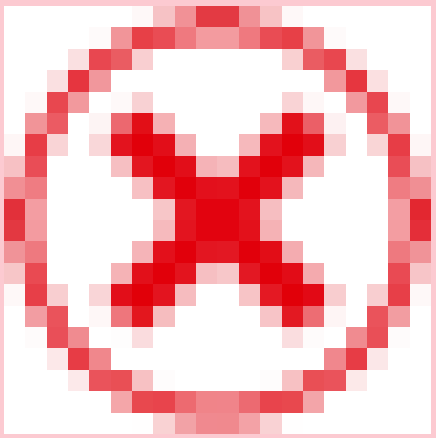
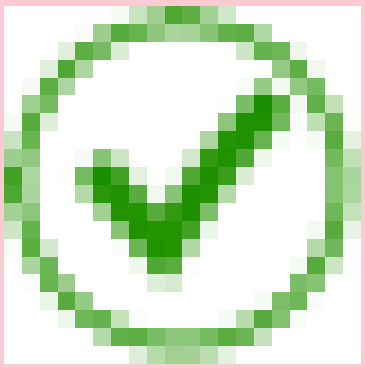
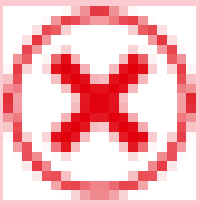
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
脆弱性一致アイテム				
重大なリスク				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

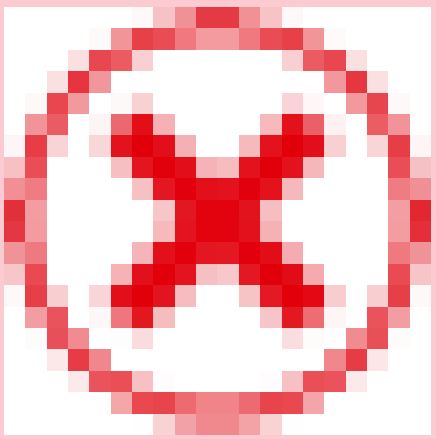
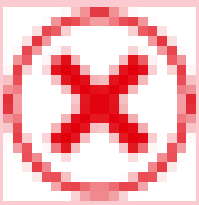
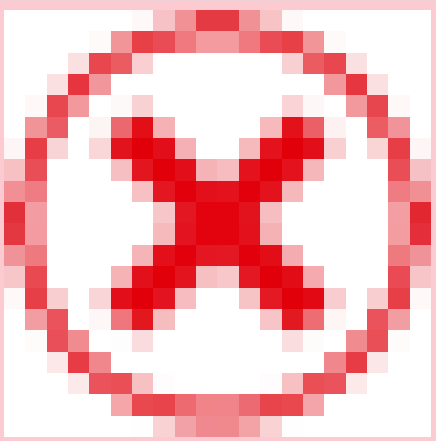
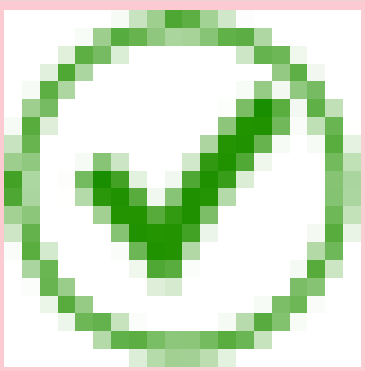
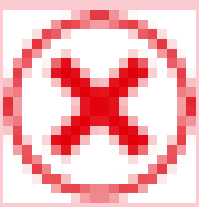
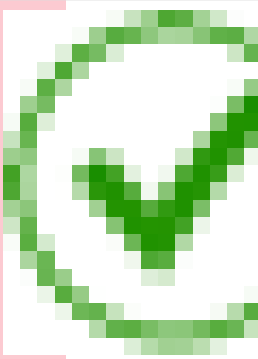
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
高リスク				
エクスプロイト可能				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

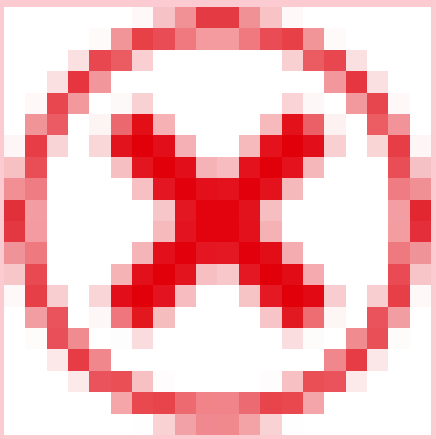
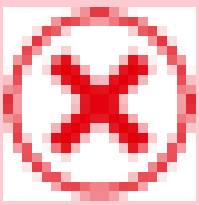
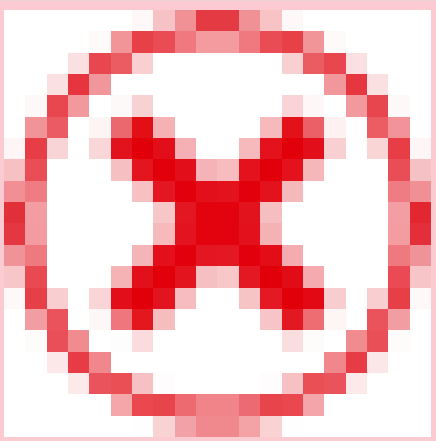
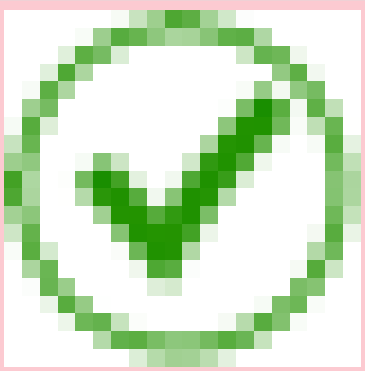
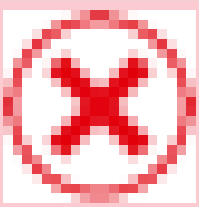
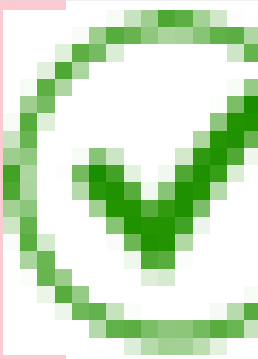
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
該当 CI 確認中				
CI 不明				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

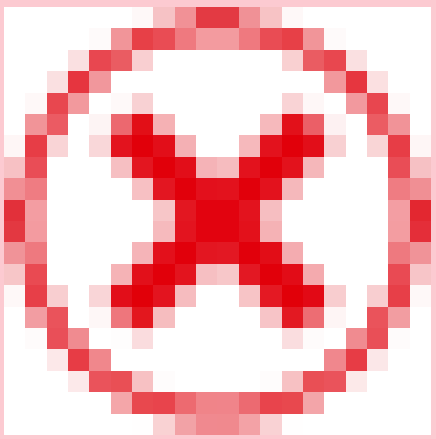
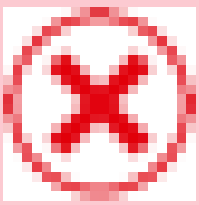
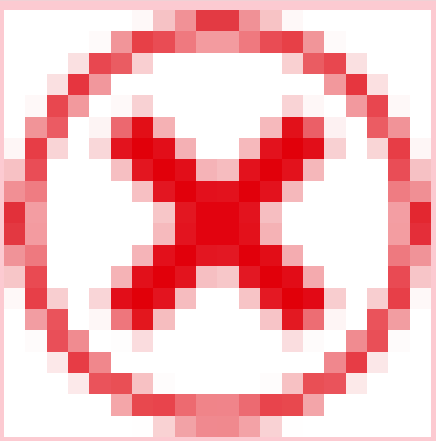
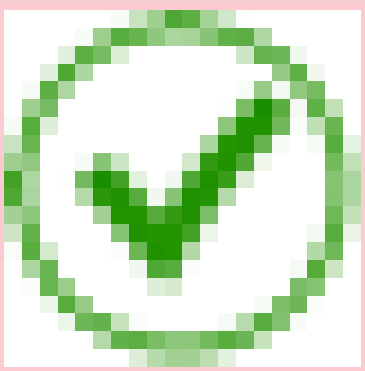
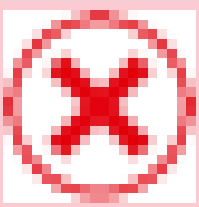
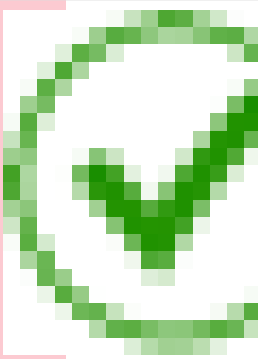
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
過去 90 日以内				
91 日以上前				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

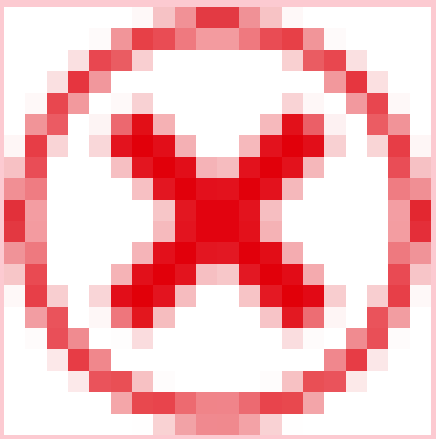
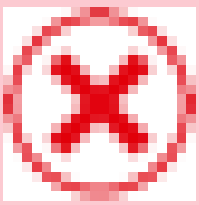
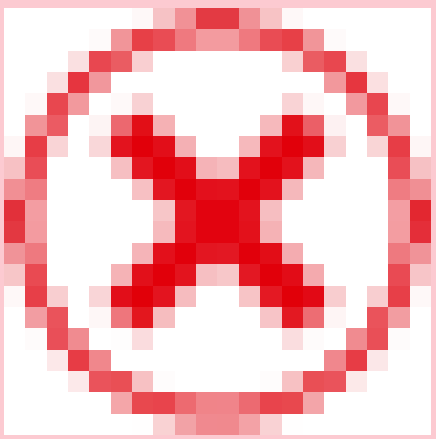
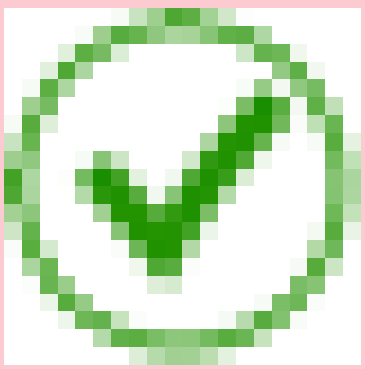
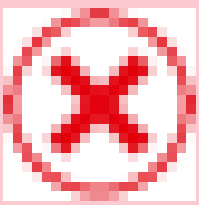
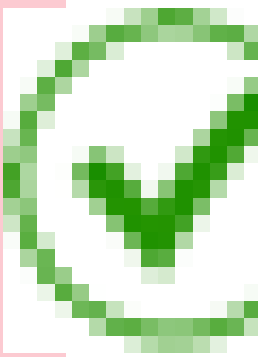
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
未アサイン				
修復タスク未割り当て				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

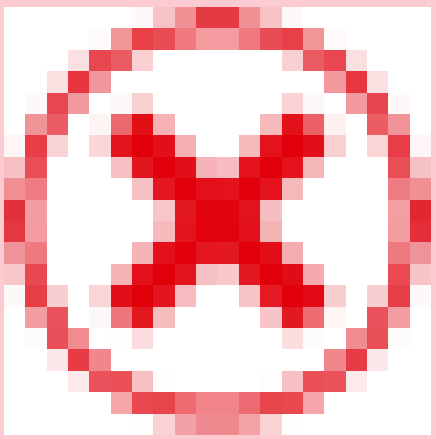
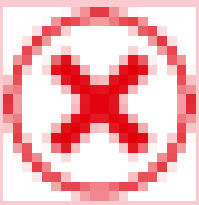
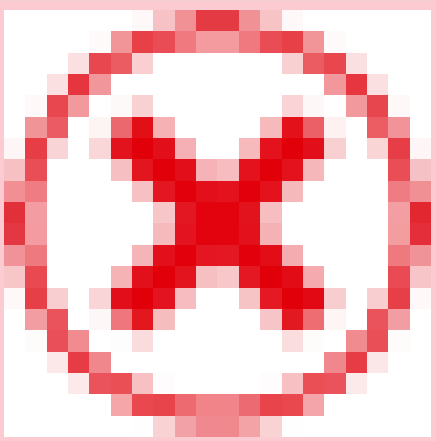
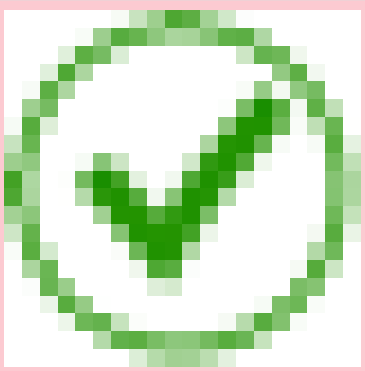
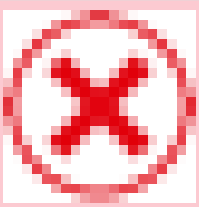
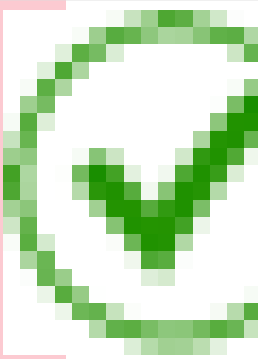
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
廃止				
複数の保留				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

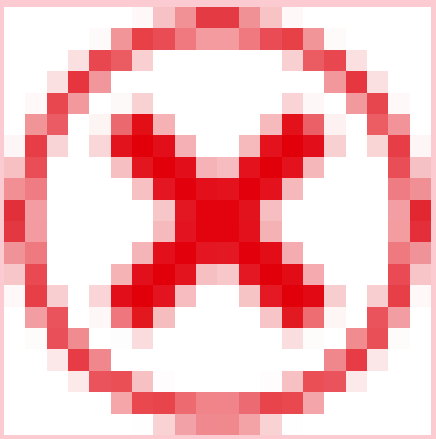
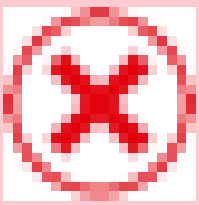
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
すべて				

ソリューション

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

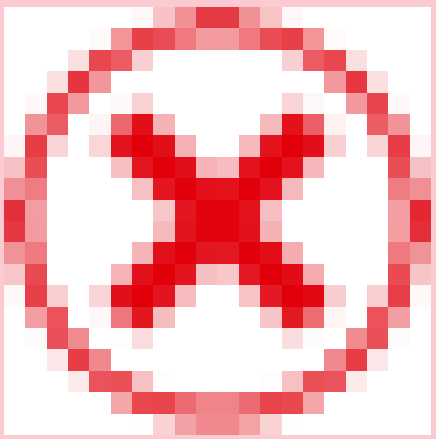
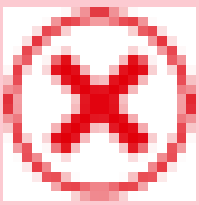
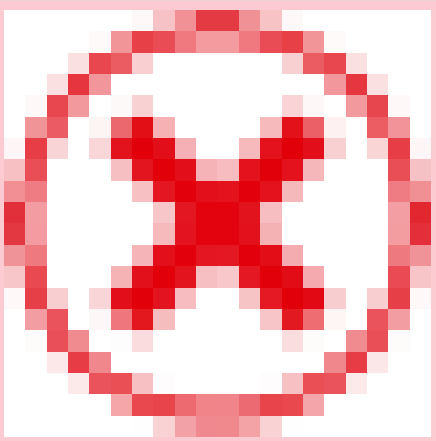
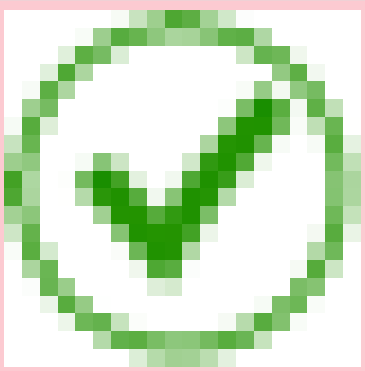
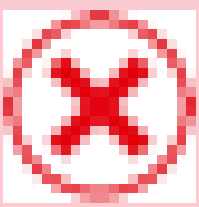
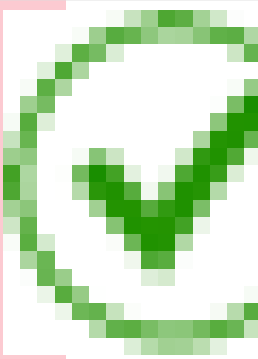
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
すべて				
最高優先度				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
脆弱性一致アイテムを使用	✗	✓	✗	✓

ライブラリ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

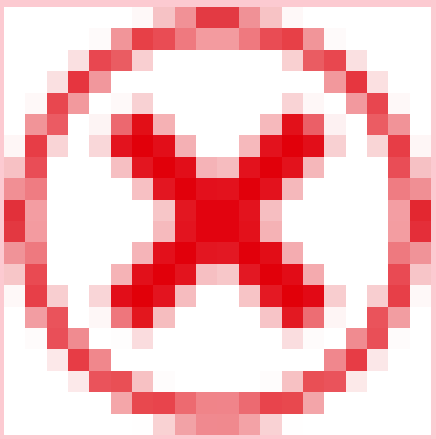
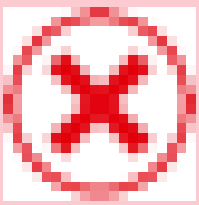
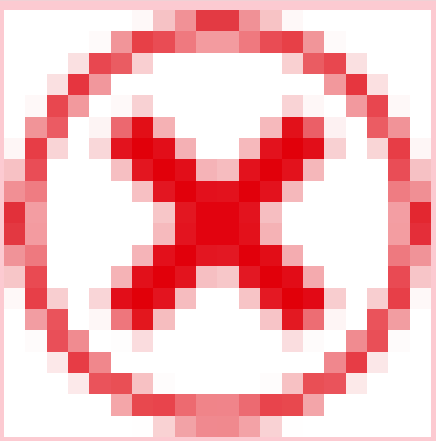
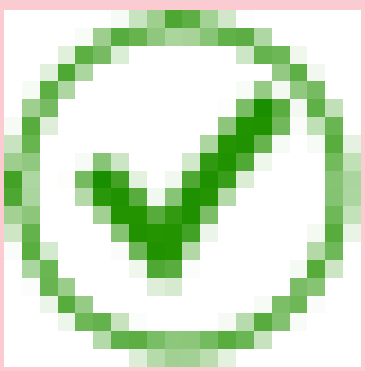
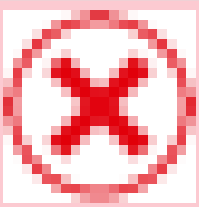
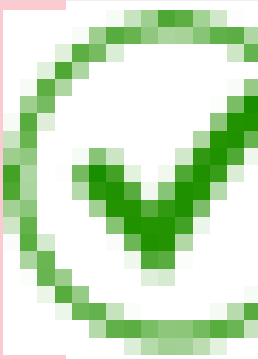
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
NVD				
CWE				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

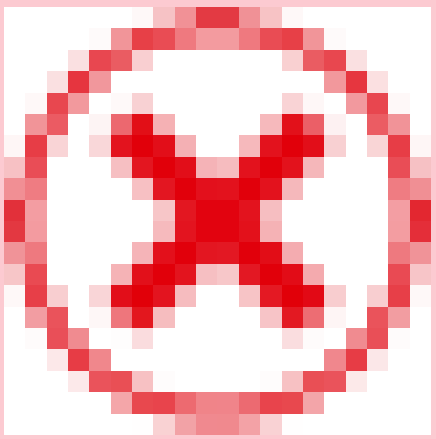
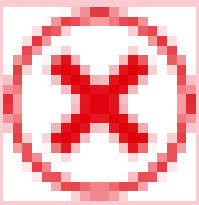
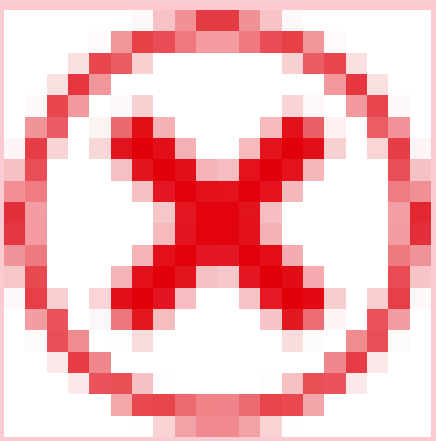
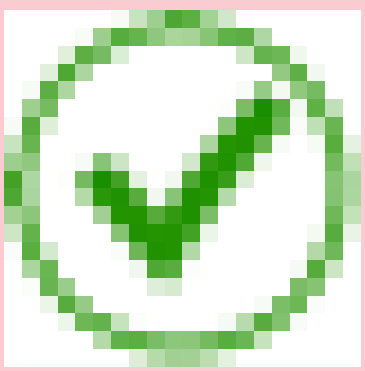
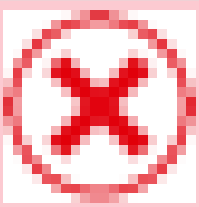
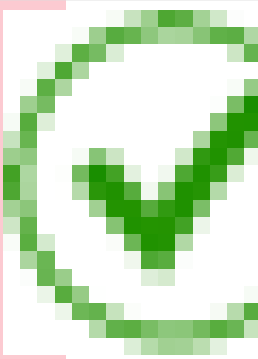
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
サードパーティ				
脆弱なソフトウェア				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

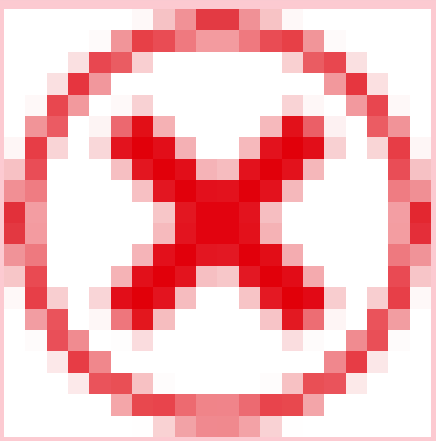
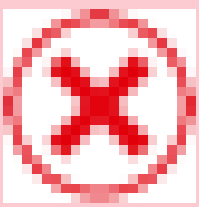
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
脆弱性スキャン				
エクスポージャーアセスメント				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

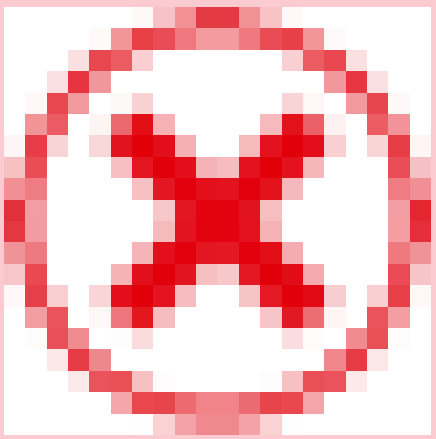
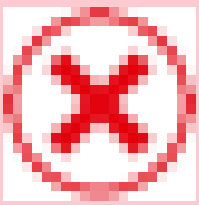
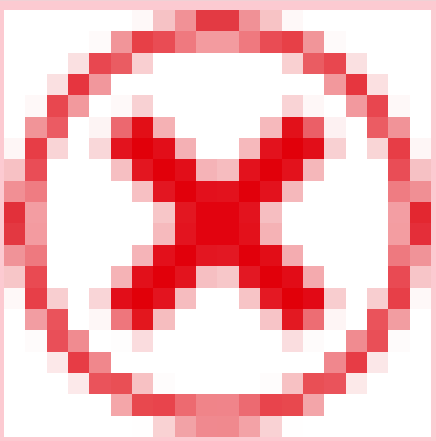
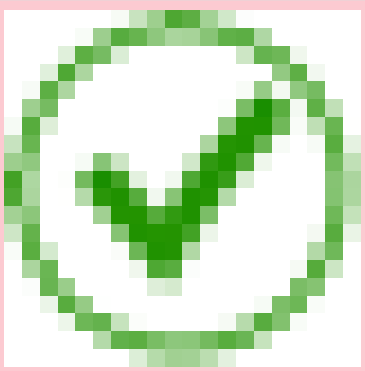
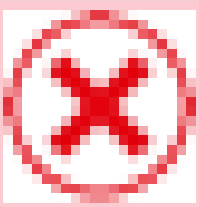
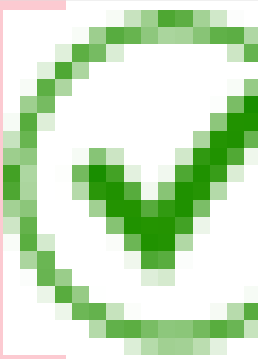
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
スキャン				
スキャナー				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

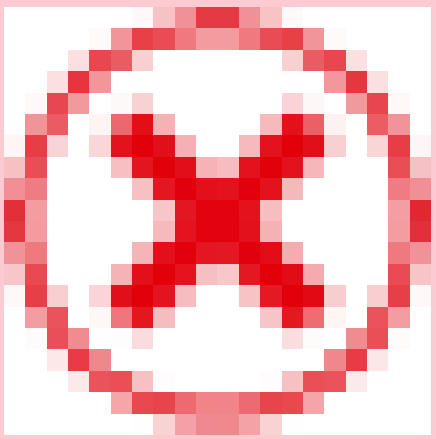
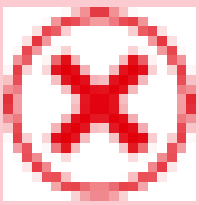
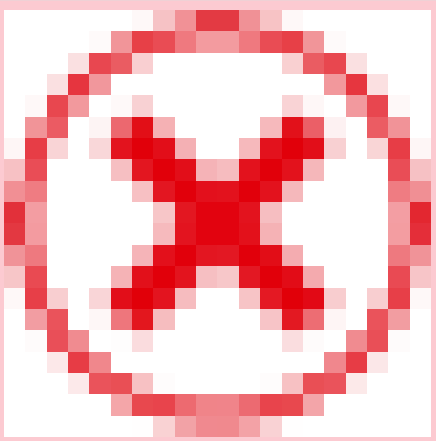
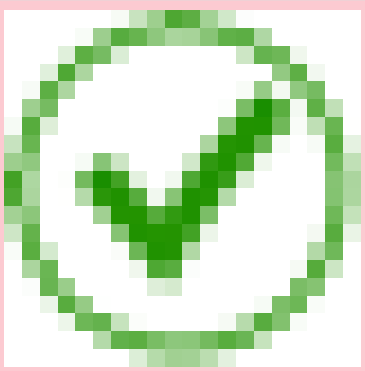
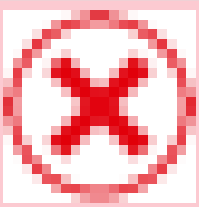
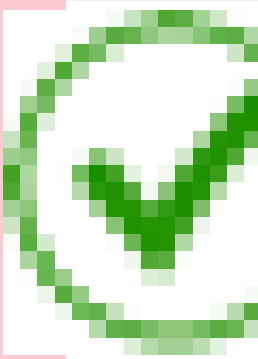
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
スキャンキュー				
スキャナーレート制限				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

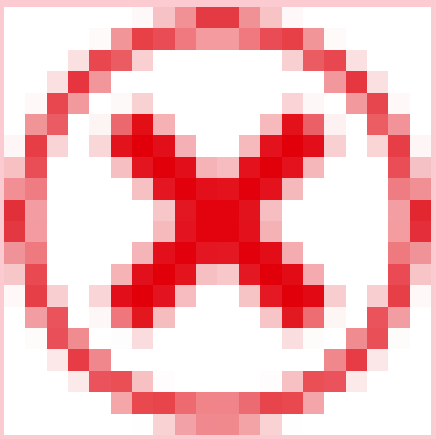
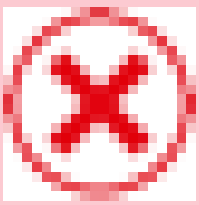
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
レート制限定義				
管理				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

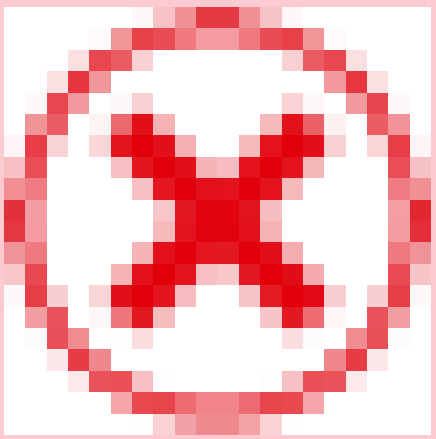
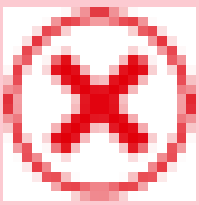
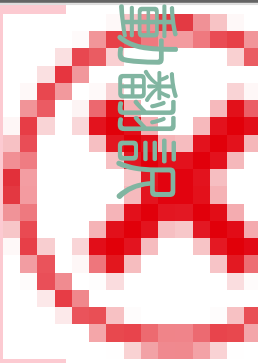
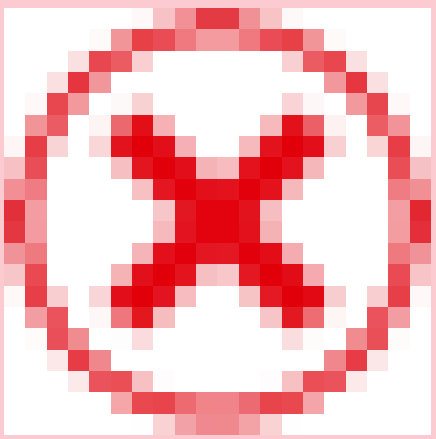
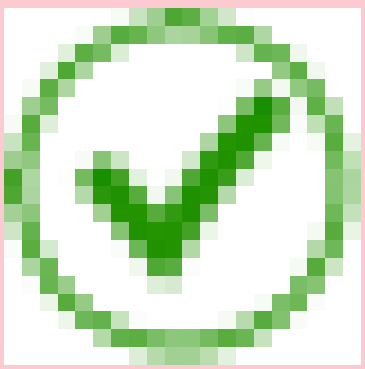
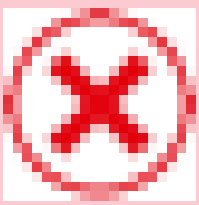
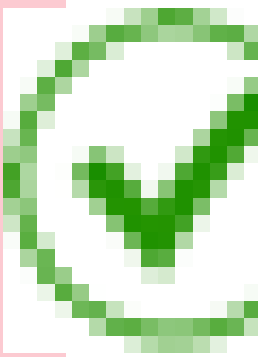
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
セットアップアシスタント				
監視トピック				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

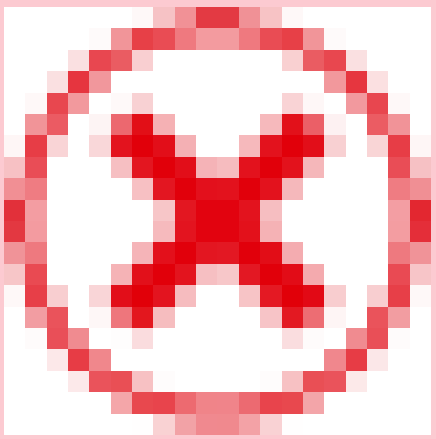
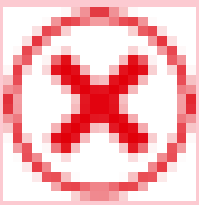
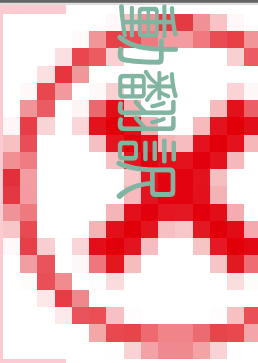
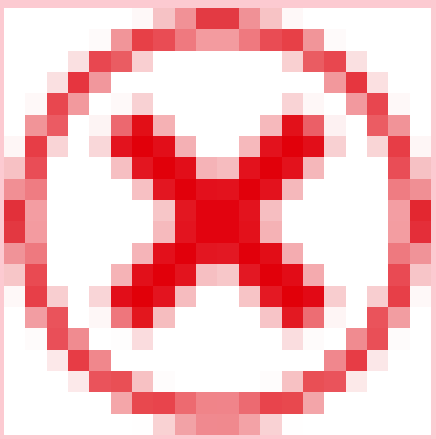
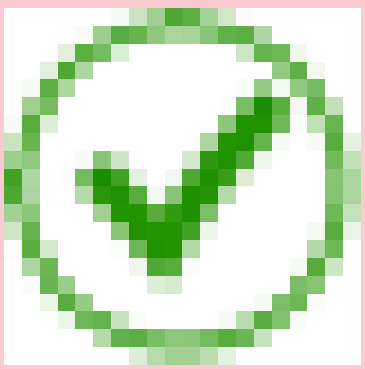
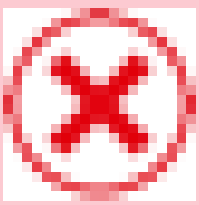
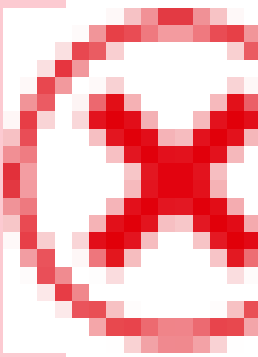
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
アサインルール				
修復タスクルール				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

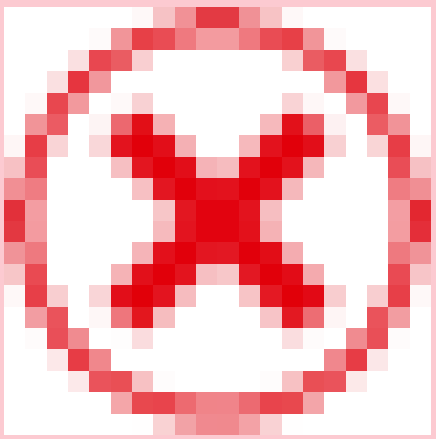
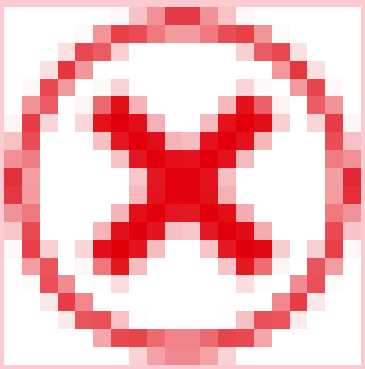
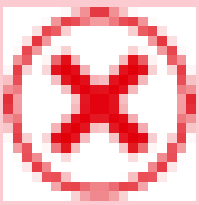
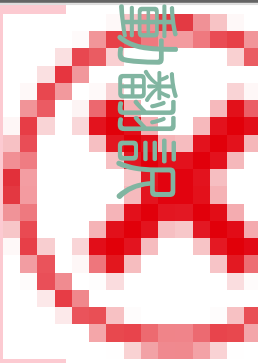
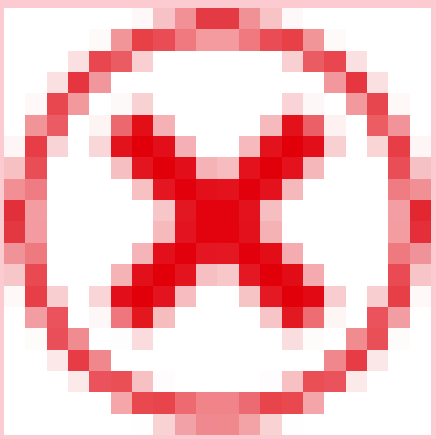
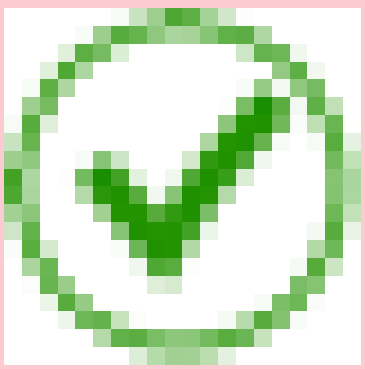
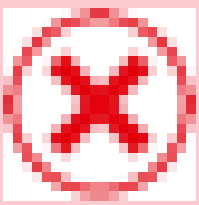
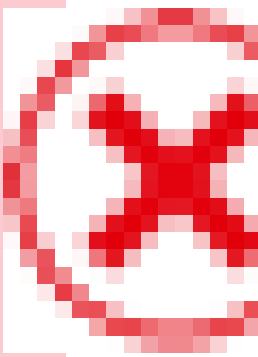
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
アサインの推奨				
脆弱性算出				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

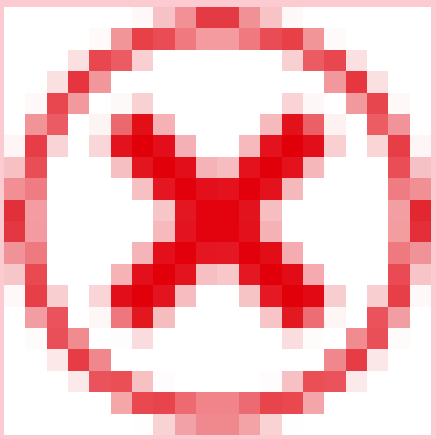
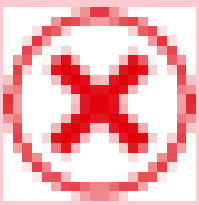
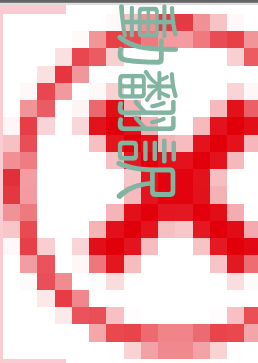
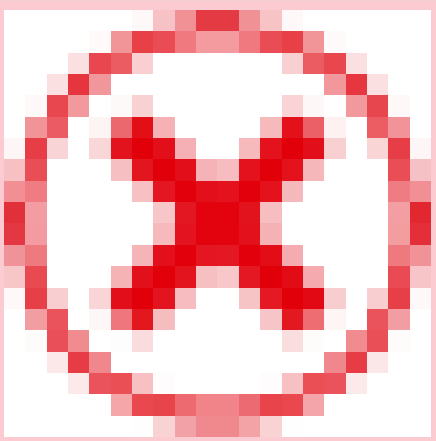
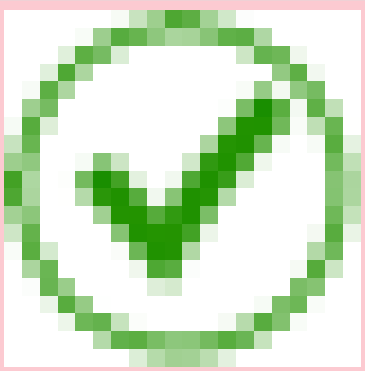
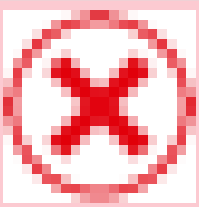
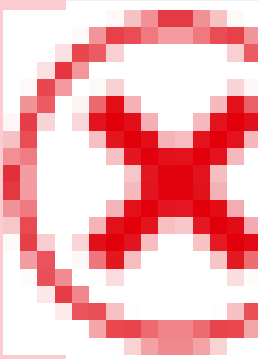
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
脆弱性ロールアップ算出				
修復ターゲットルール				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

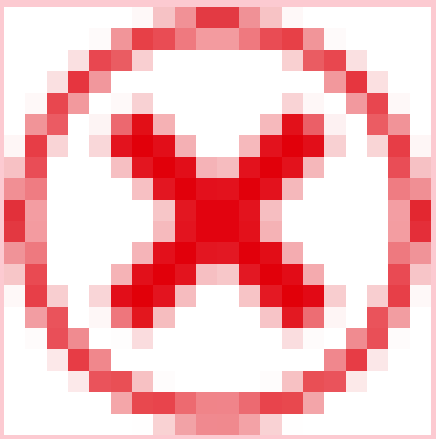
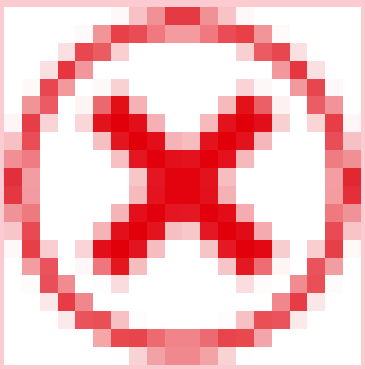
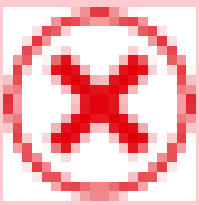
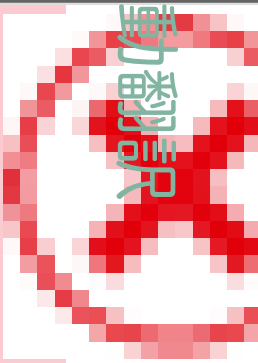
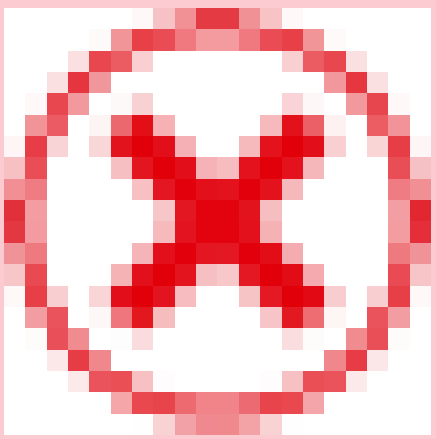
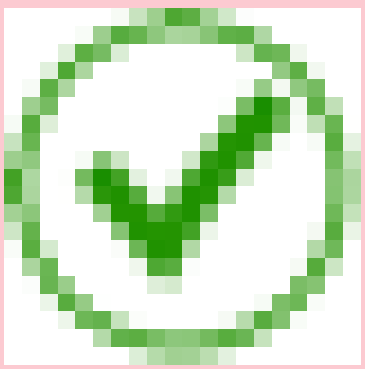
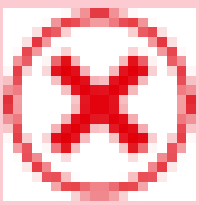
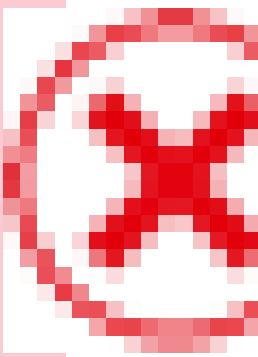
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
自動クローズ構成				
ルールの自動削除				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

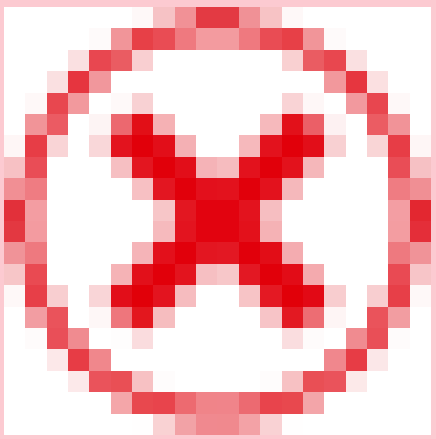
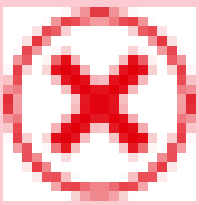
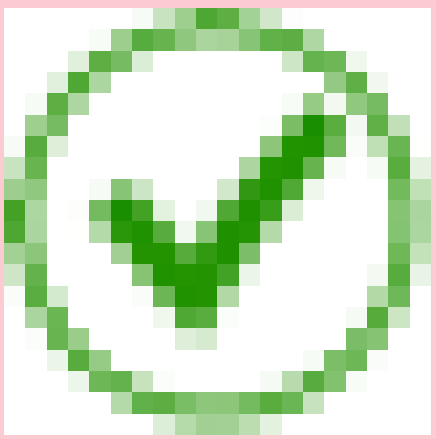
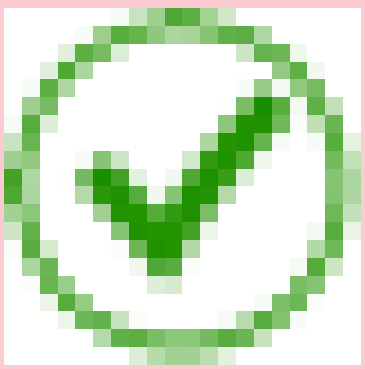
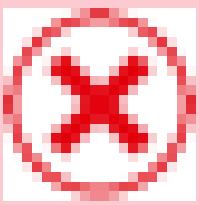
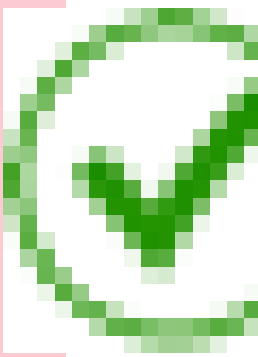
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
例外ルール				
承認ルール				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

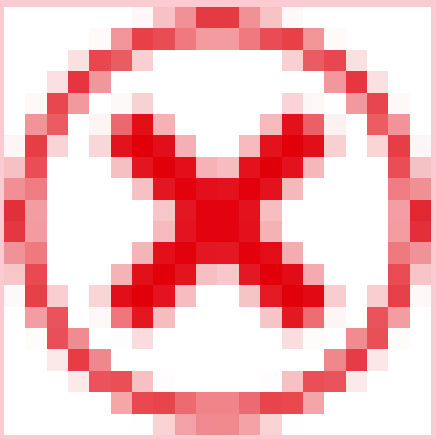
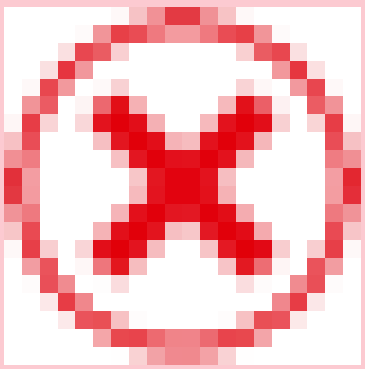
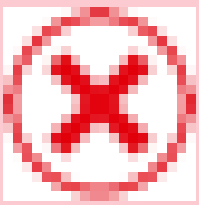
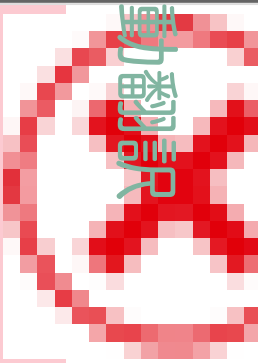
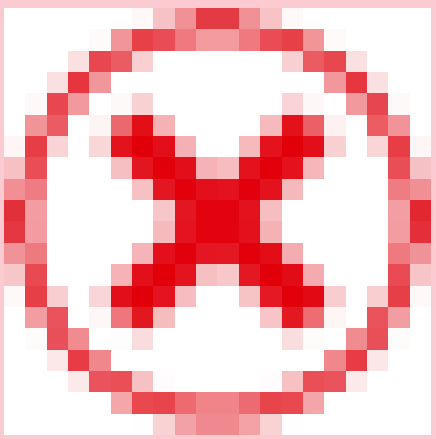
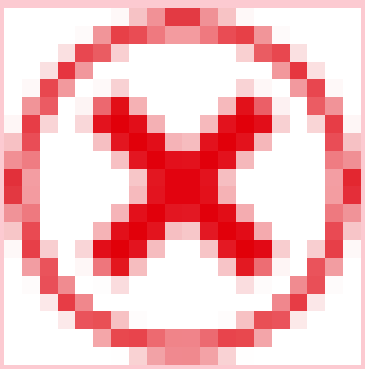
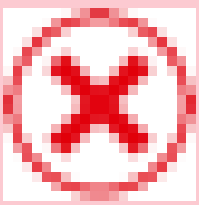
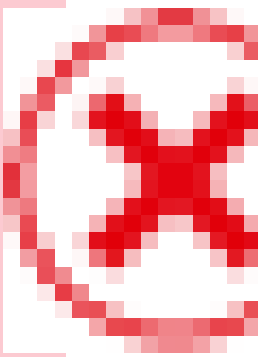
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
分類ルール				
パフォーマンス構成				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

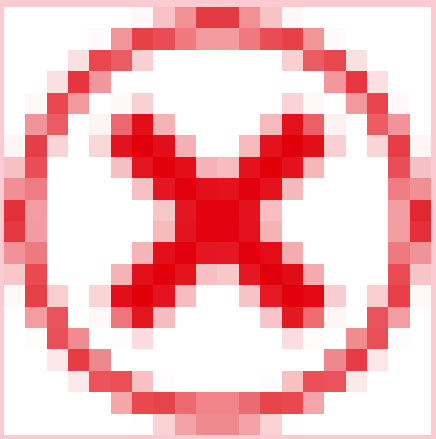
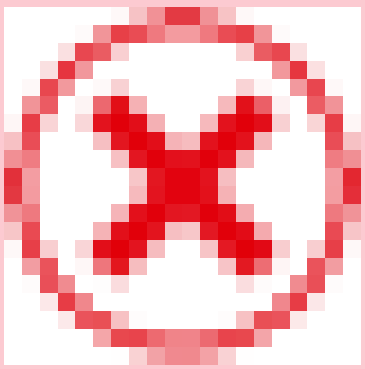
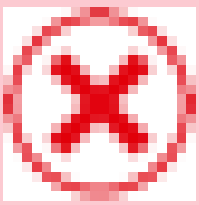
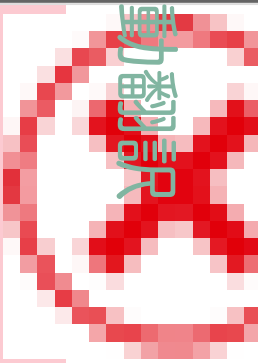
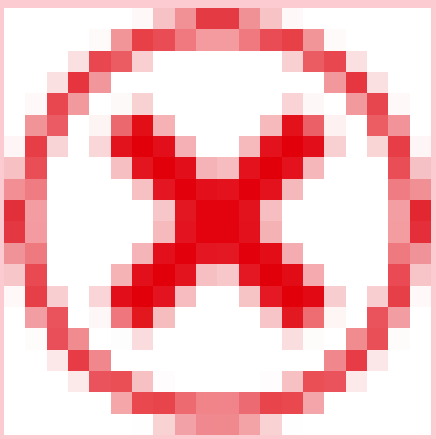
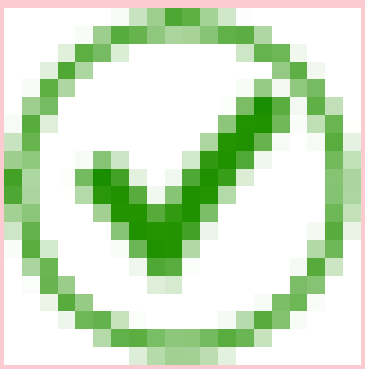
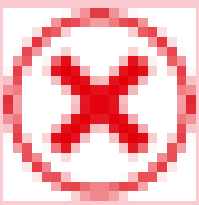
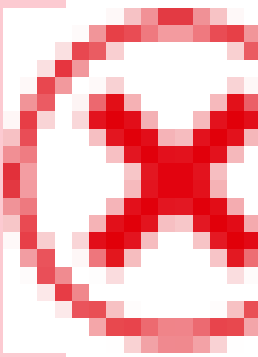
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
VI の粒度の構成				
通知				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

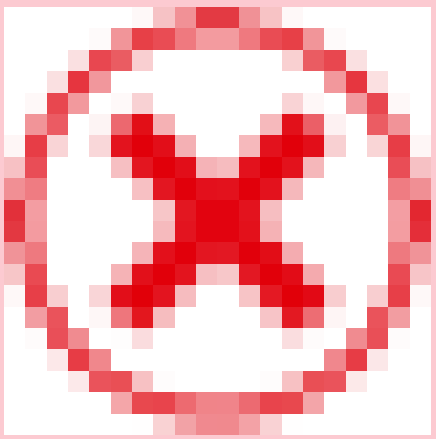
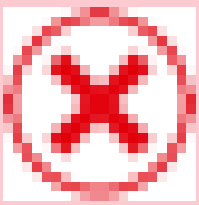
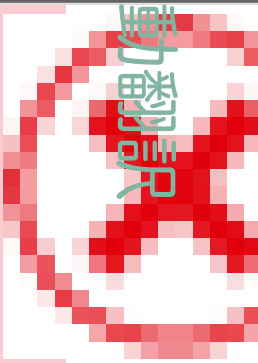
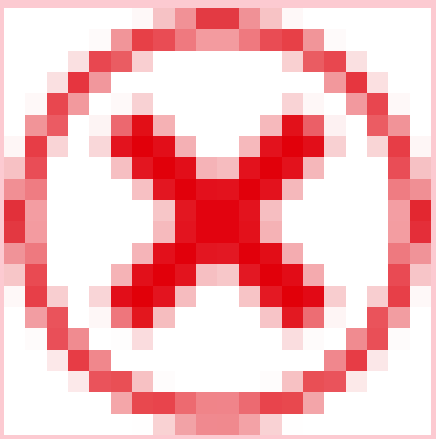
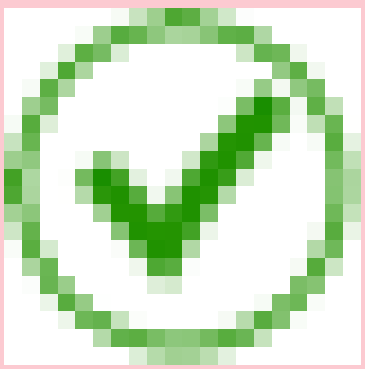
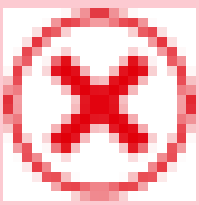
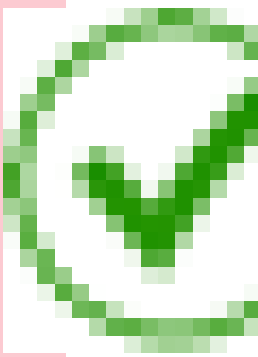
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
メールテンプレート				
キューをインポート				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

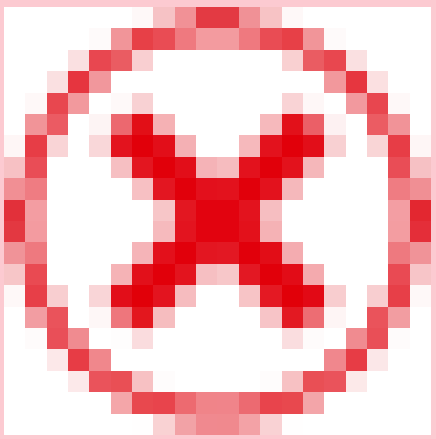
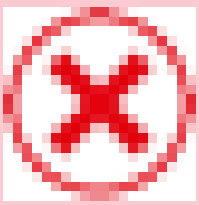
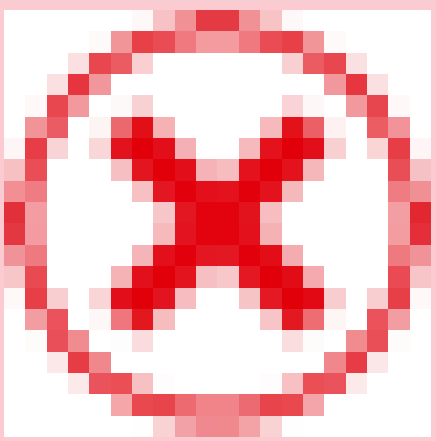
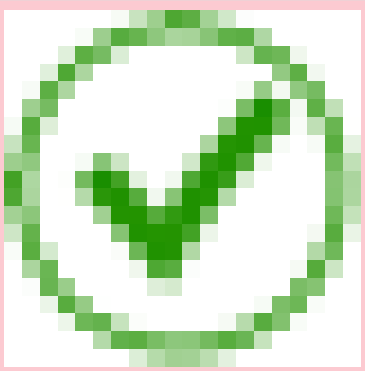
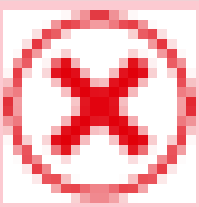
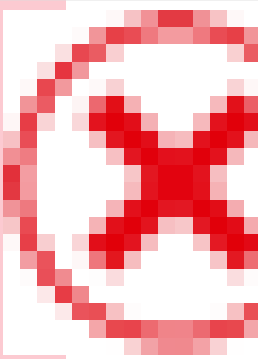
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
統合				
SLA 定義				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

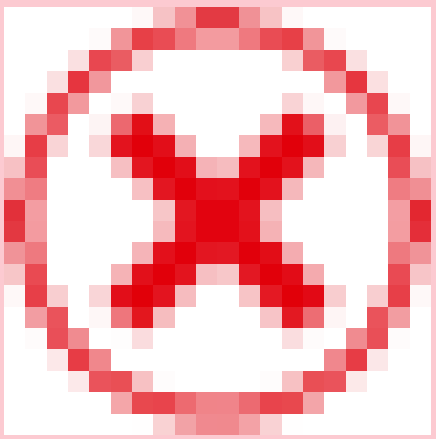
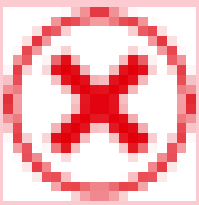
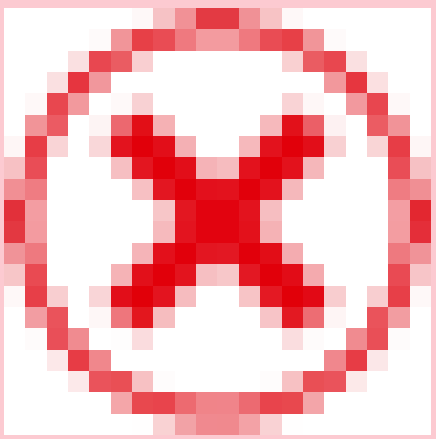
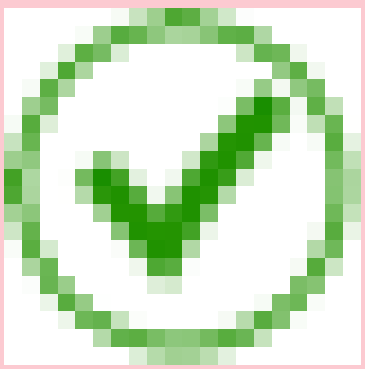
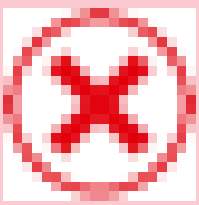
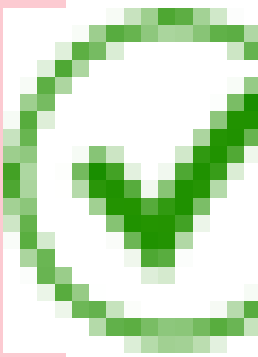
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
SAM NVD の構成				
正規化された重大度マップ				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

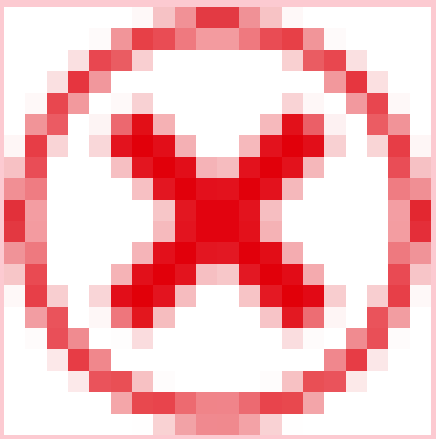
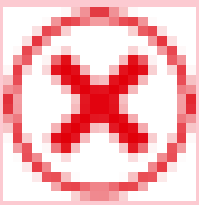
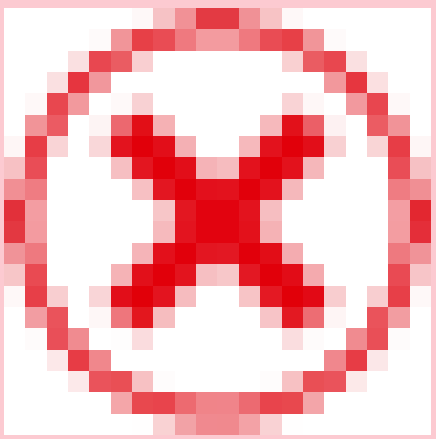
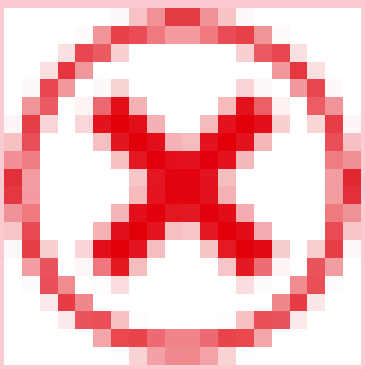
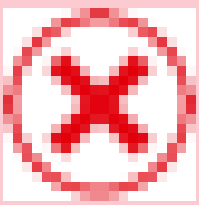
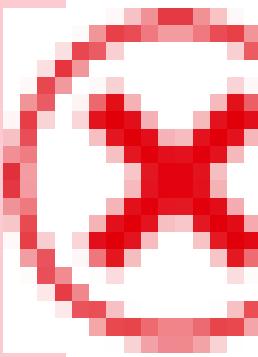
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
スキャン範囲構成				
例外管理				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

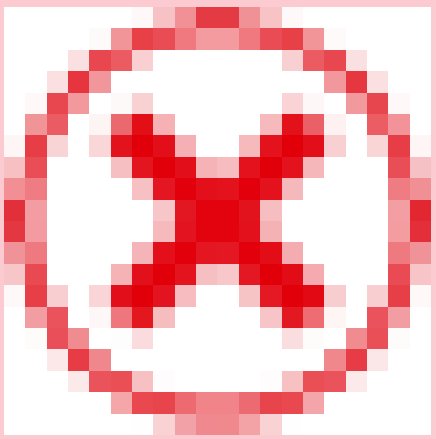
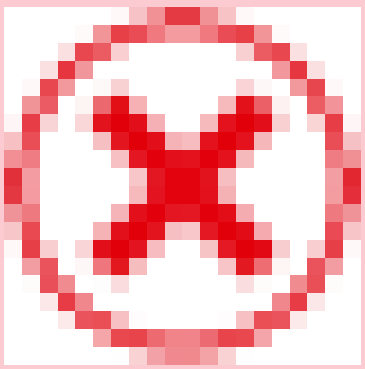
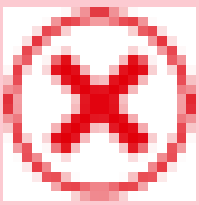
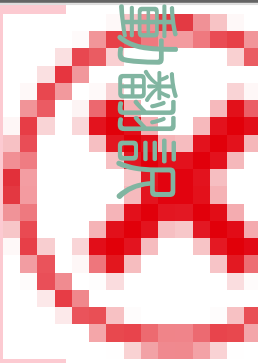
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
使用状況レポート				
診断				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、sn_vul.configure_i

その他のロールの情報：

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

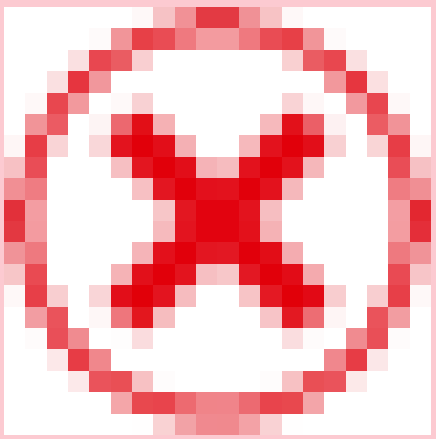
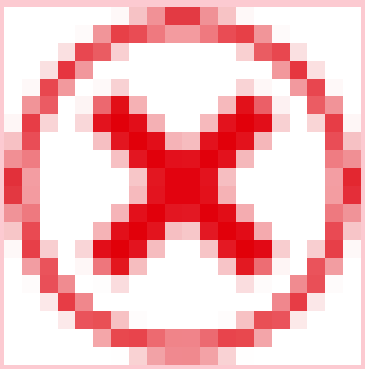
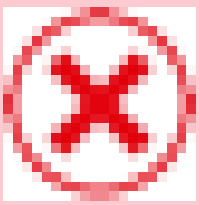
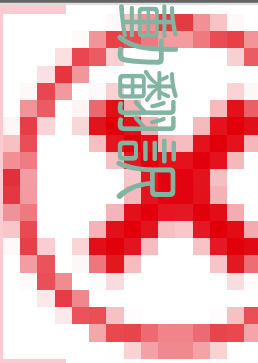
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_integ
チェック				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
(メインアプリグループ)				
CISO ダッシュボード	✗	✗	✗	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

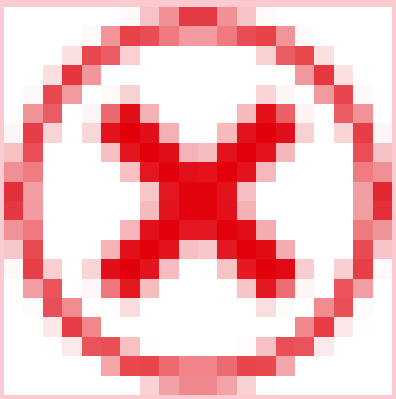
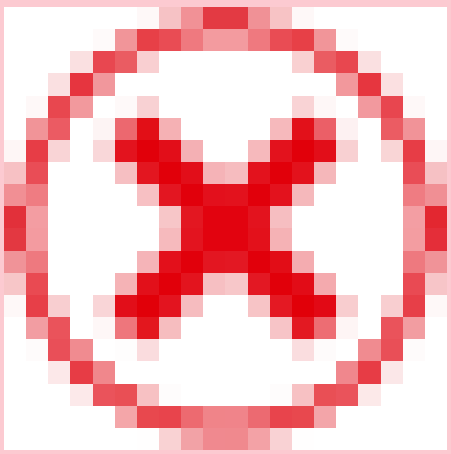
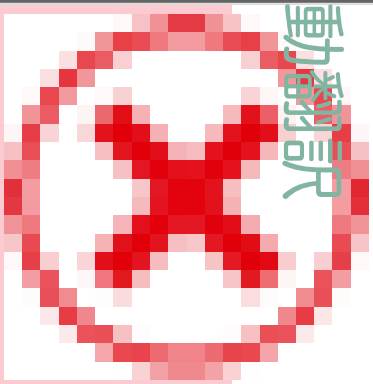
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
修復の概要				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

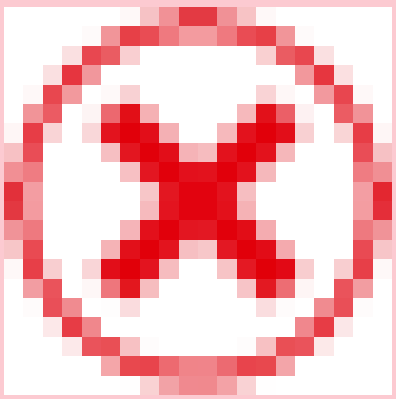
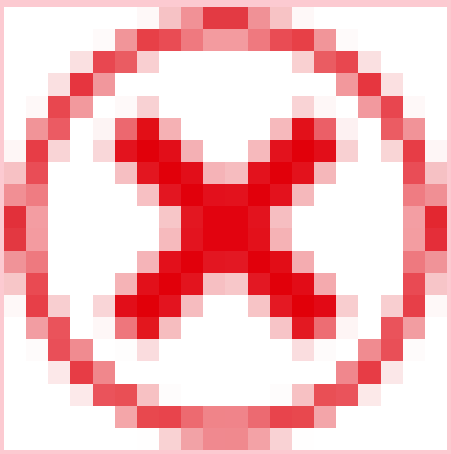
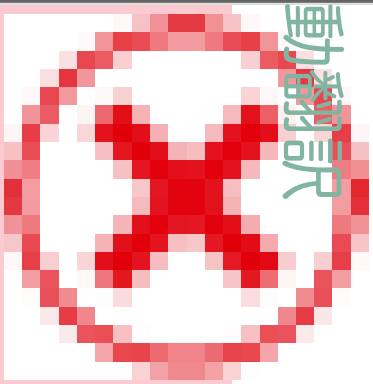
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
脆弱性マネージャーのワークスペース				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

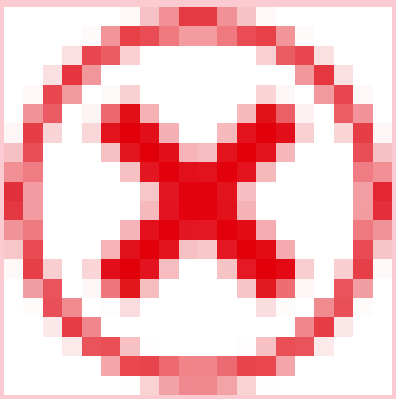
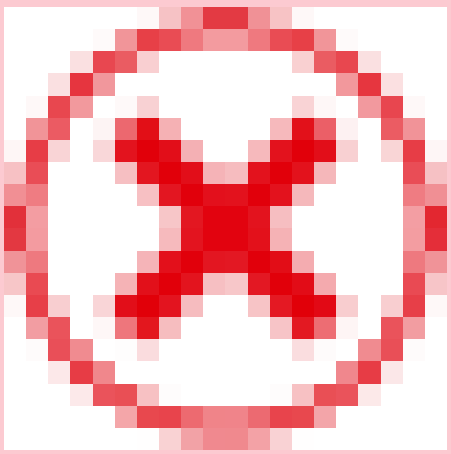
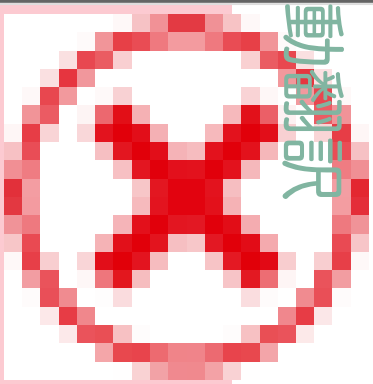
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
概要				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

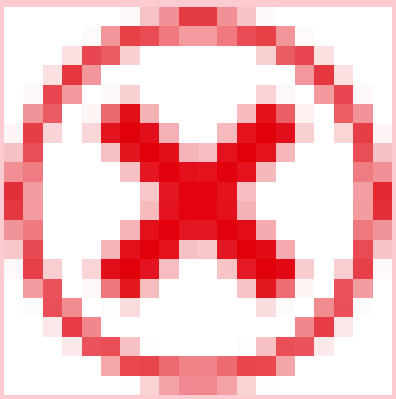
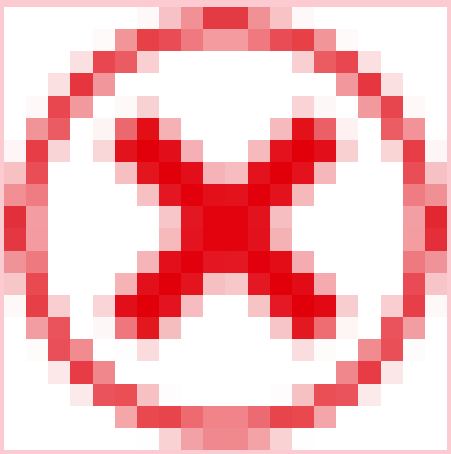
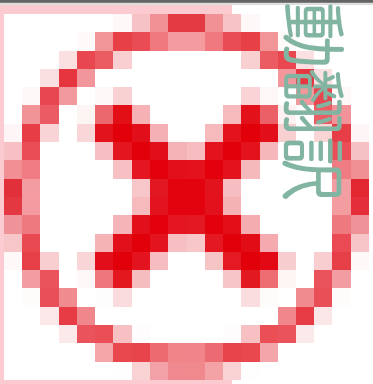
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
IT 修復ワークスペース				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

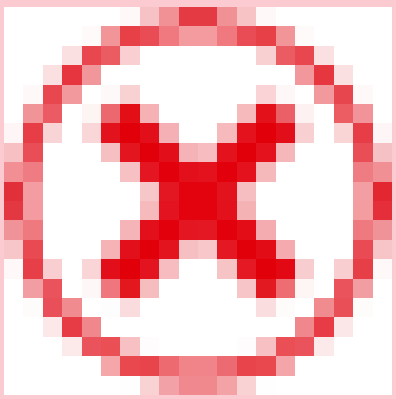
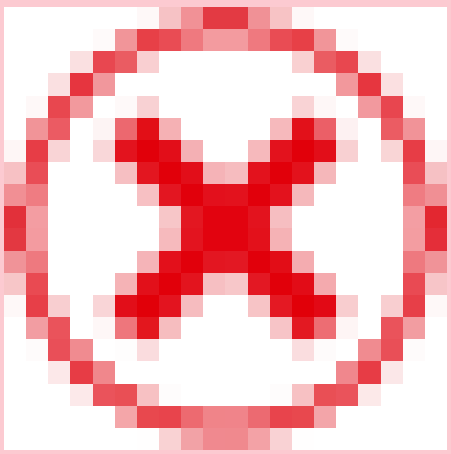
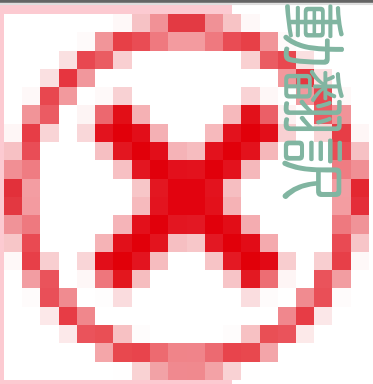
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
承認者の概要				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

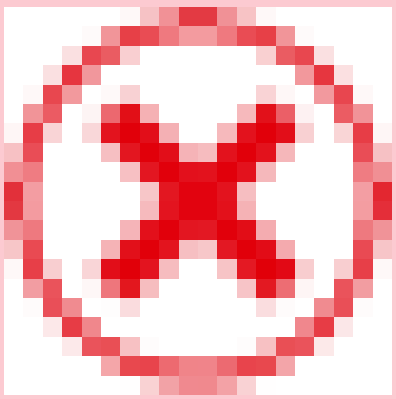
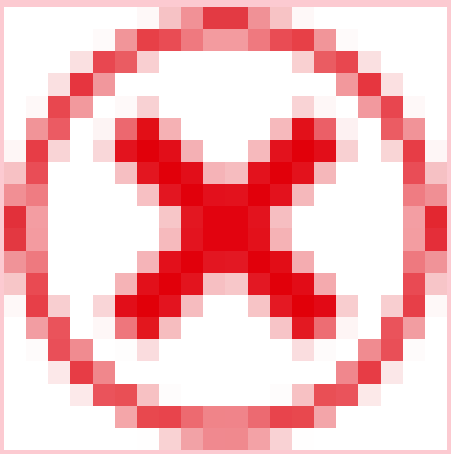
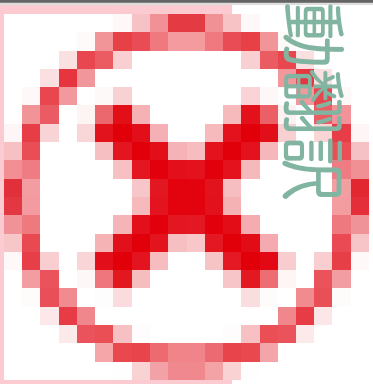
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
概要				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

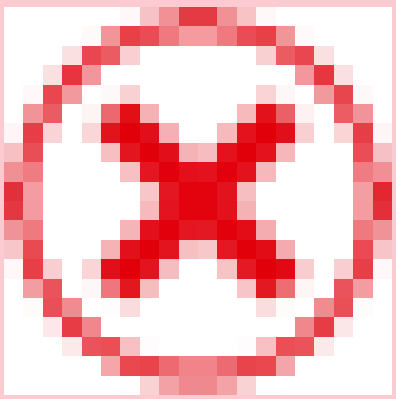
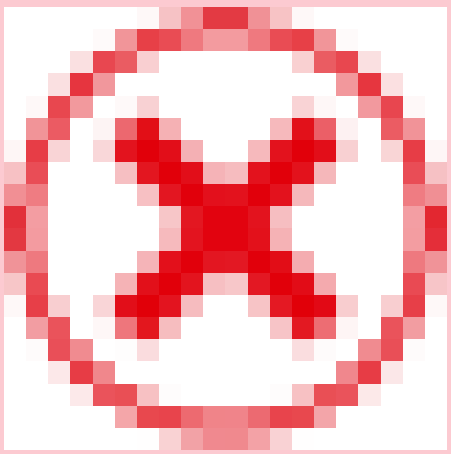
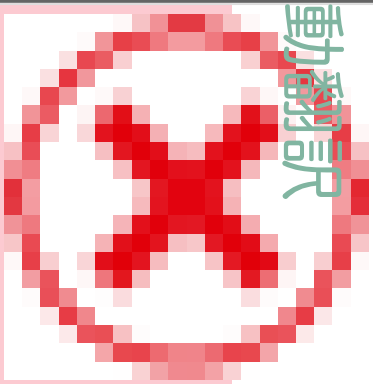
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
自分の承認				

修復タスク

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

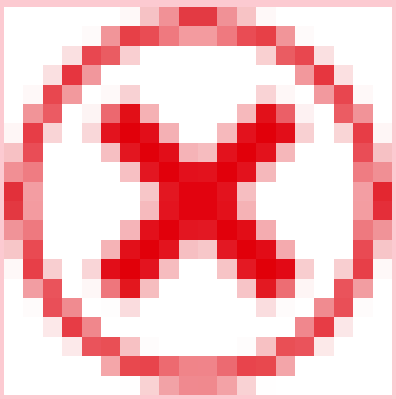
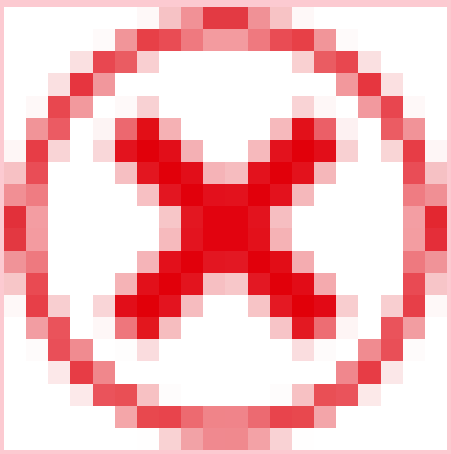
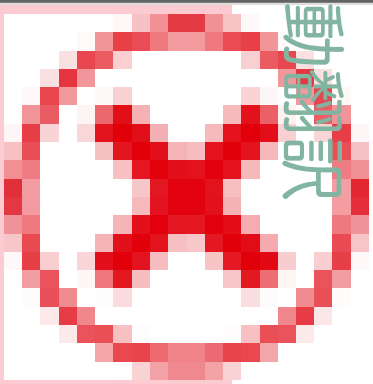
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
有効				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

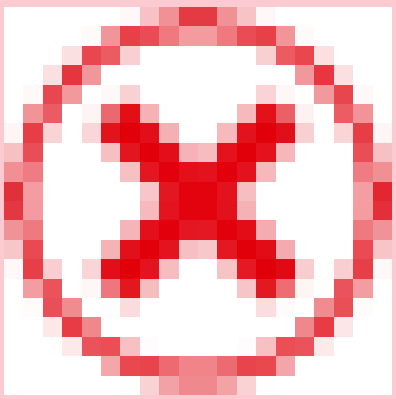
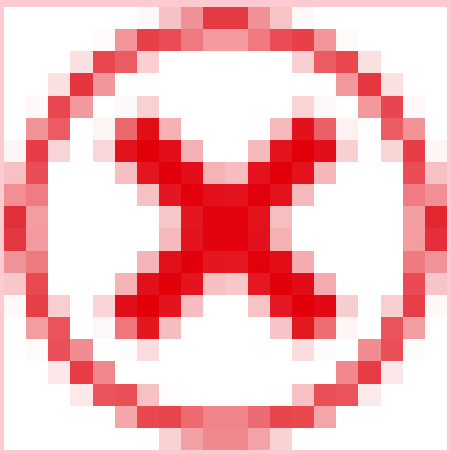
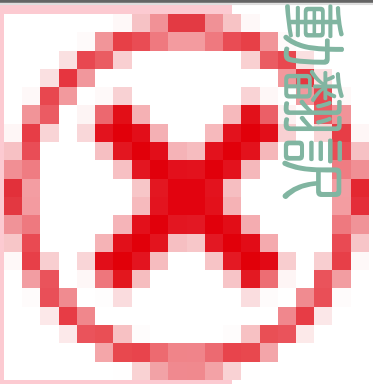
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
自分にアサイン済み				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

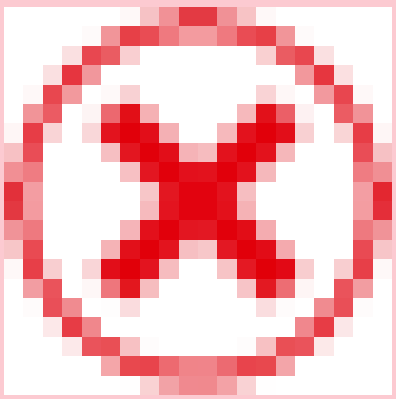
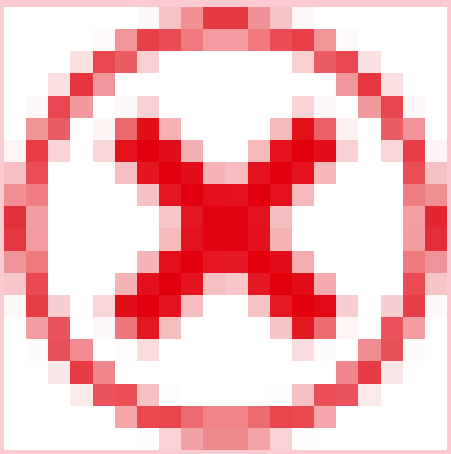
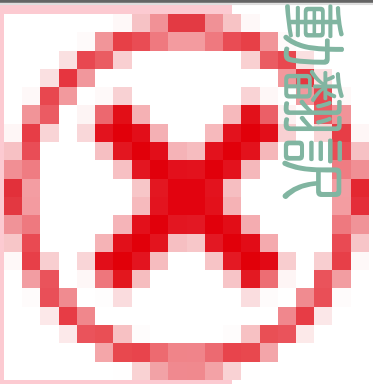
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
所属グループにアサイン済み				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

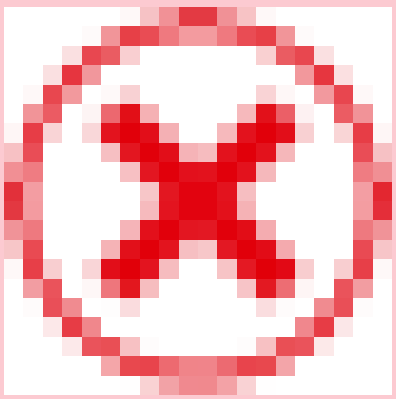
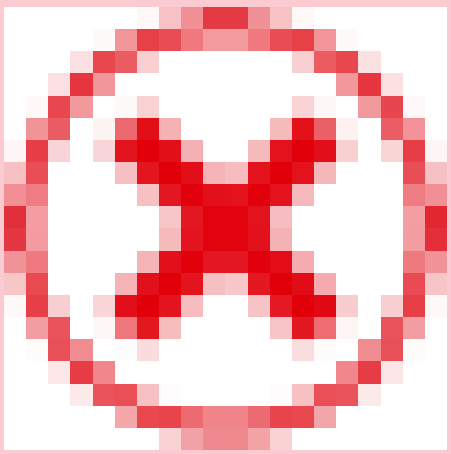
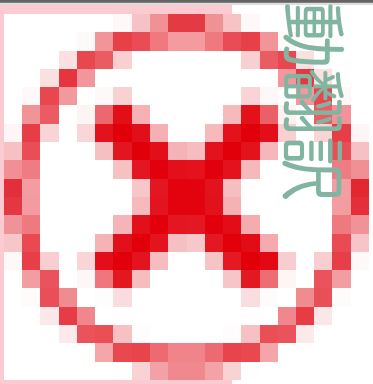
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
すべて				

脆弱性一致アイテム

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

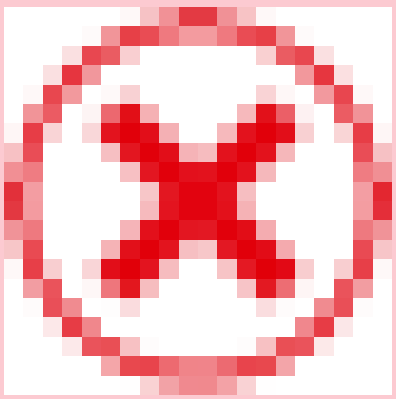
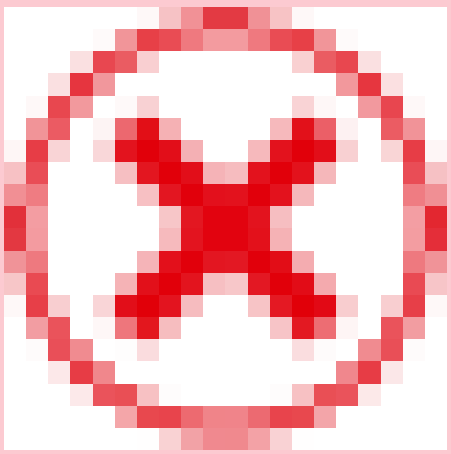
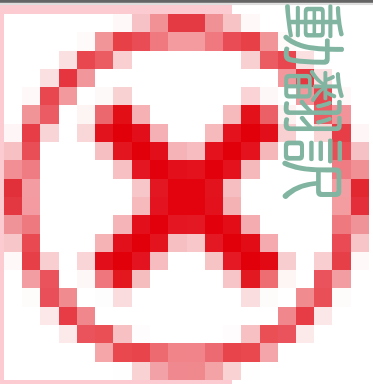
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
重大なリスク				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

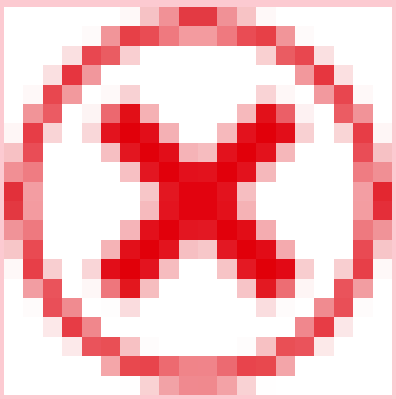
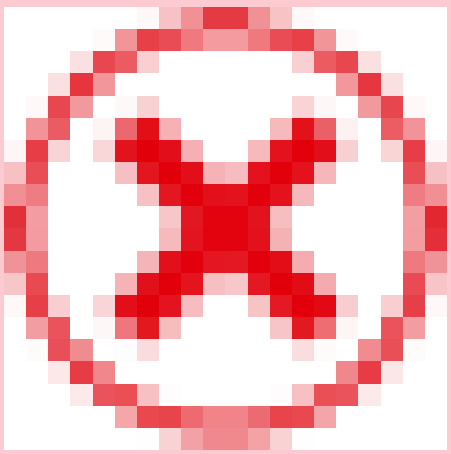
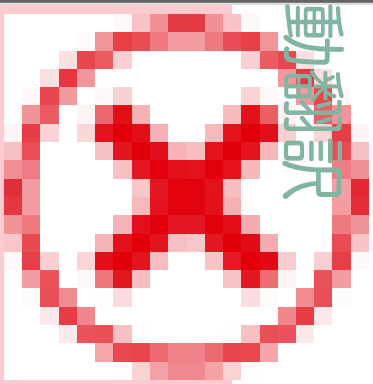
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
高リスク				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

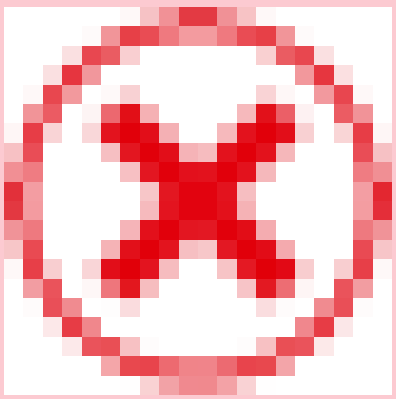
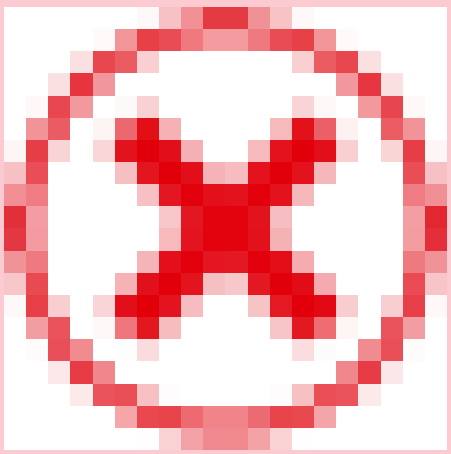
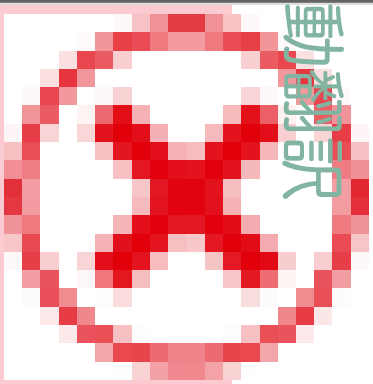
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
エクスプロイト可能				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

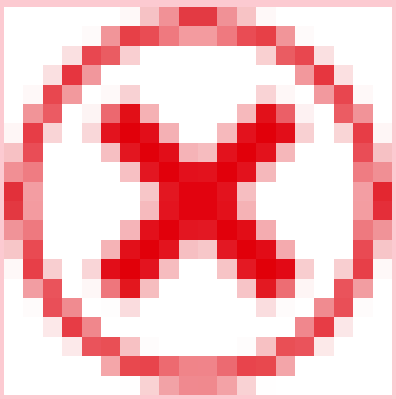
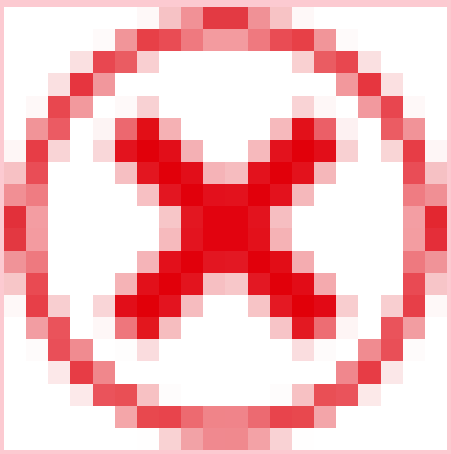
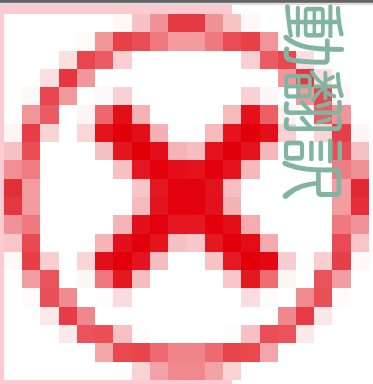
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
該当 CI 確認中				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

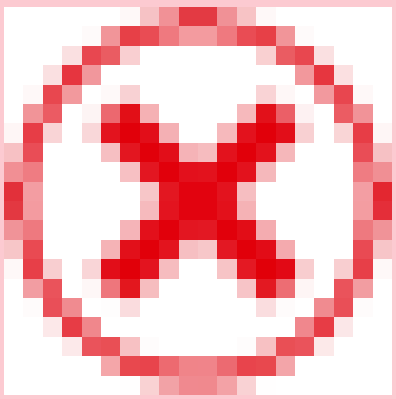
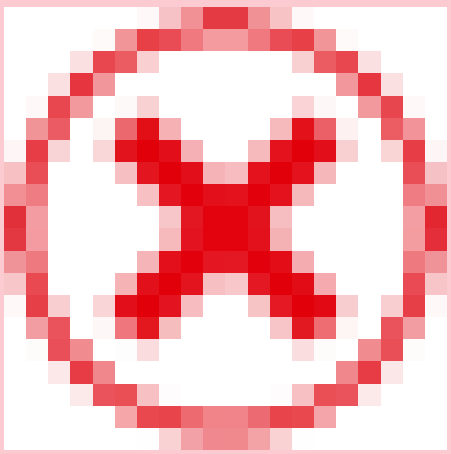
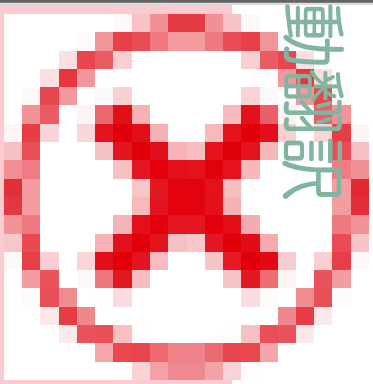
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
CI 不明				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

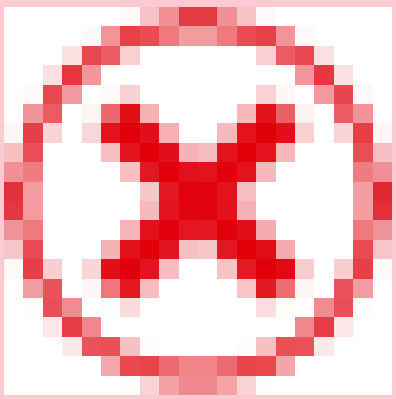
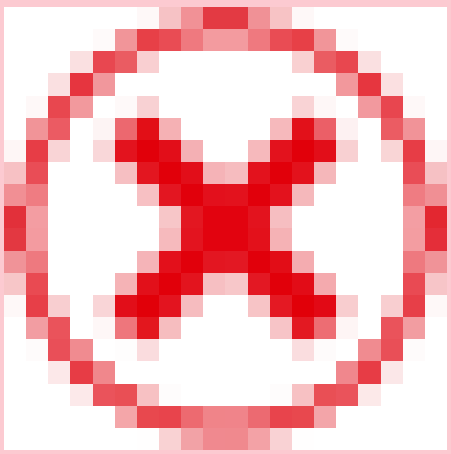
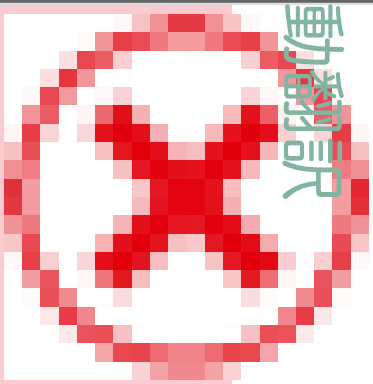
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
過去 90 日以内				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

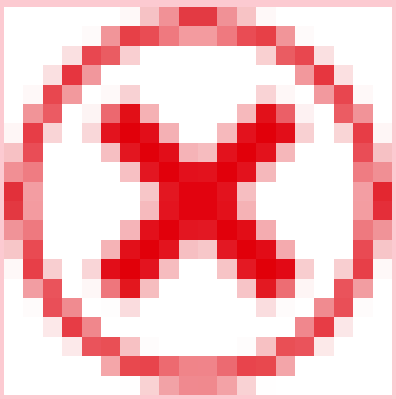
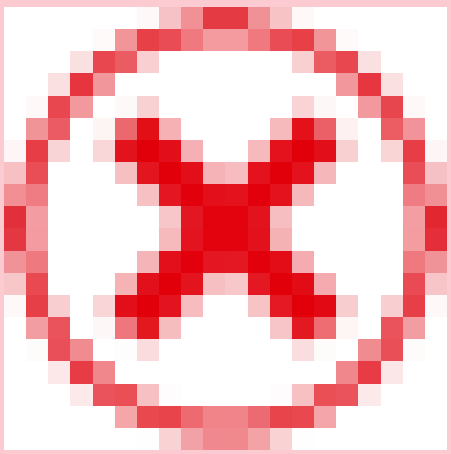
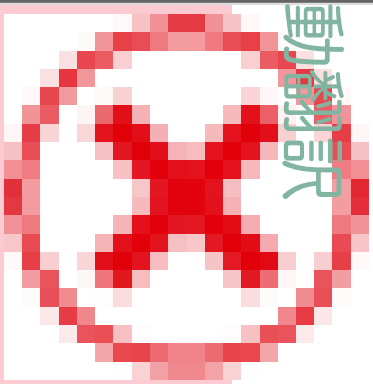
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
91 日以上前				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

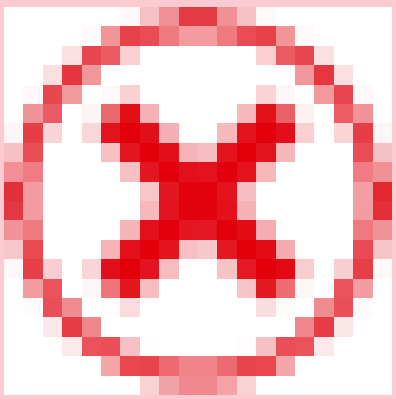
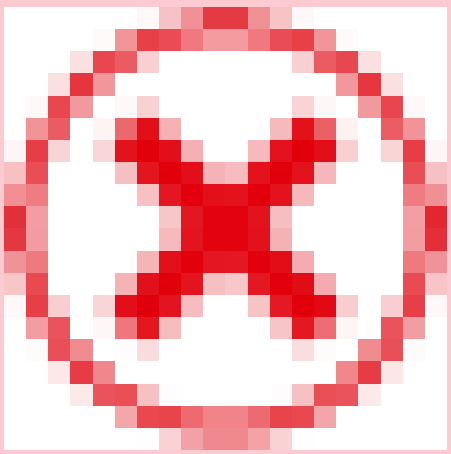
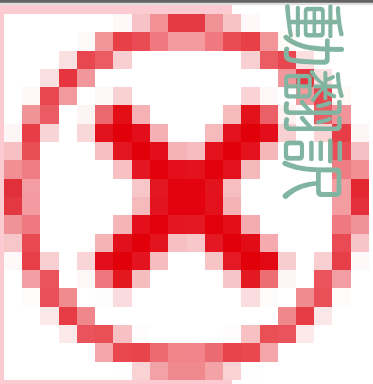
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
未アサイン				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

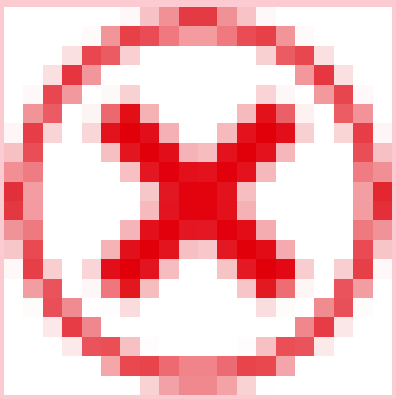
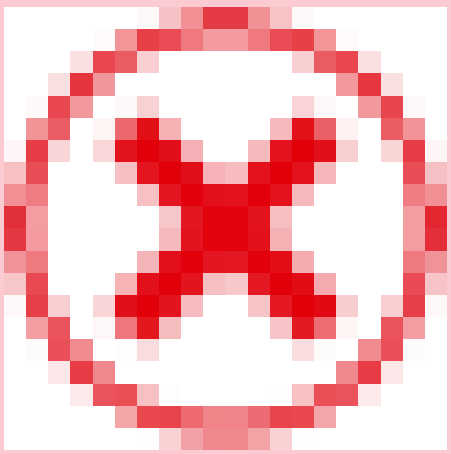
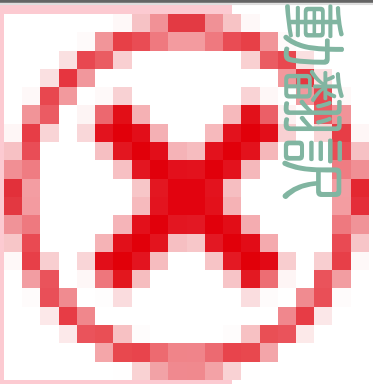
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
修復タスク未割り当て				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

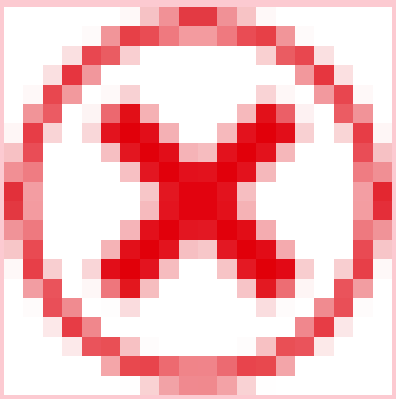
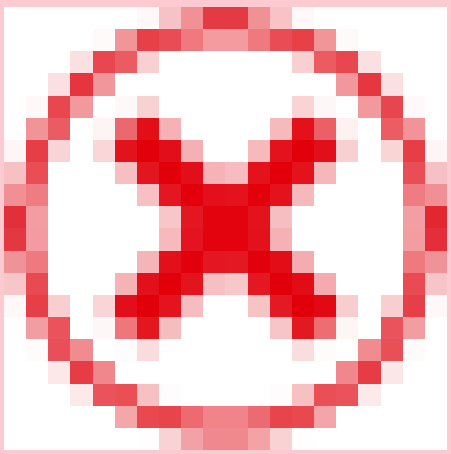
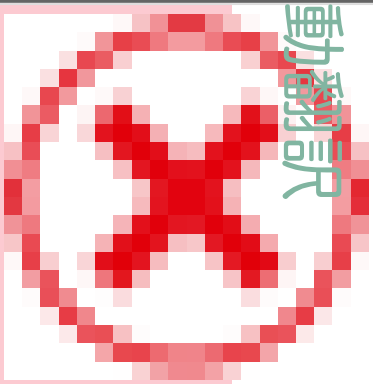
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
廃止				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

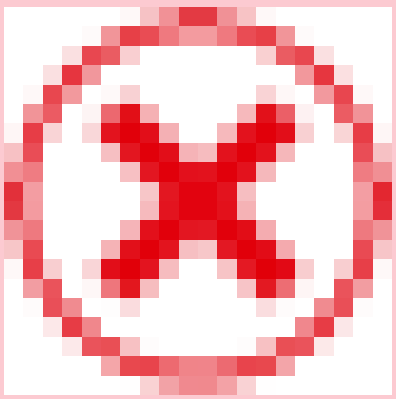
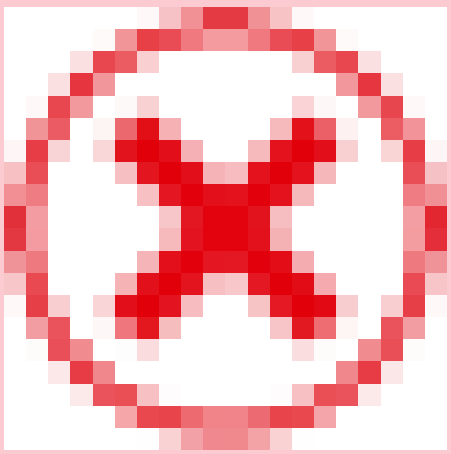
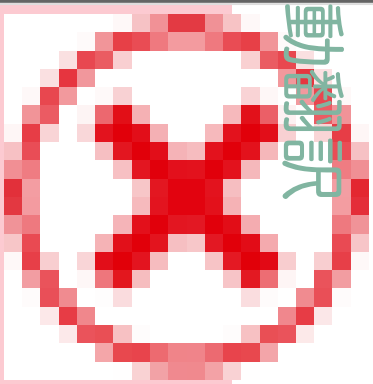
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
複数の保留				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

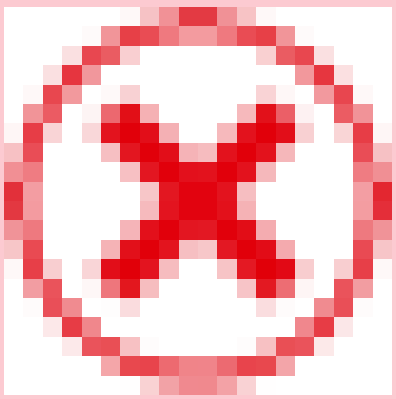
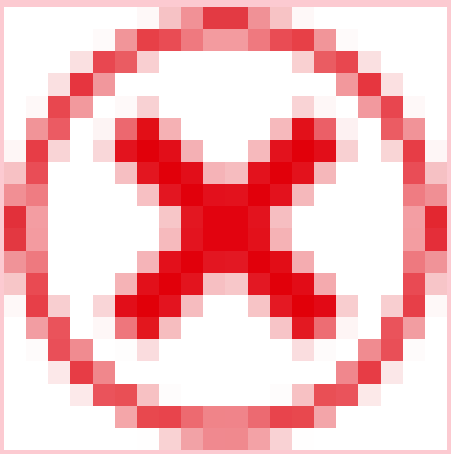
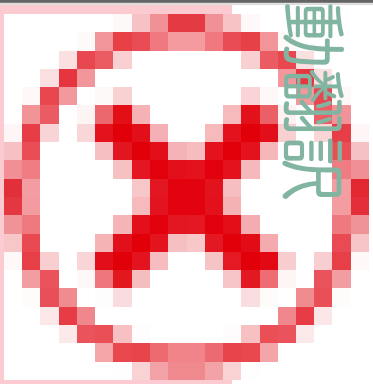
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
すべて				

ソリューション

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

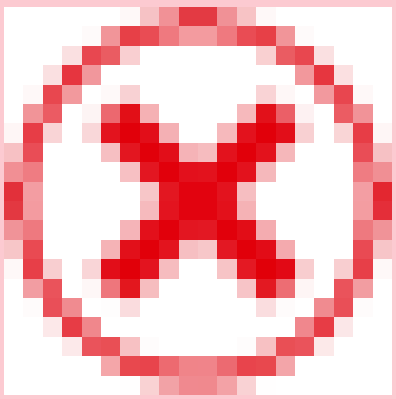
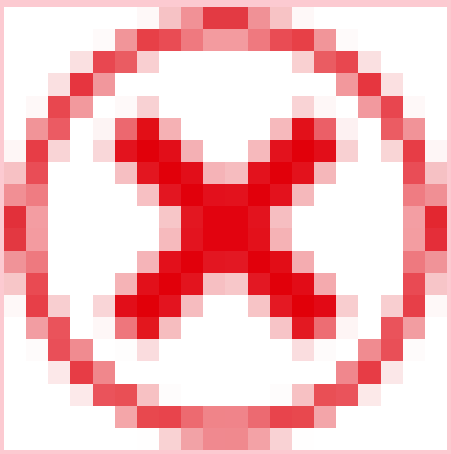
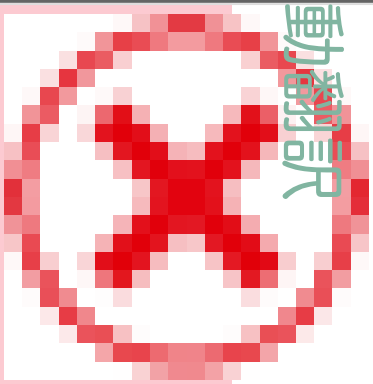
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
すべて				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

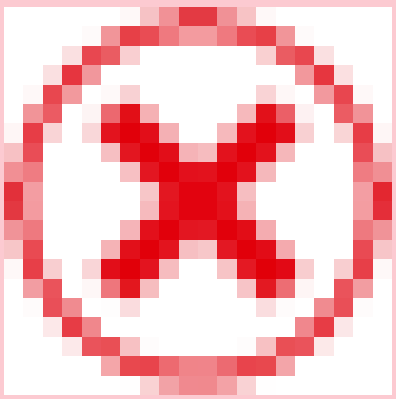
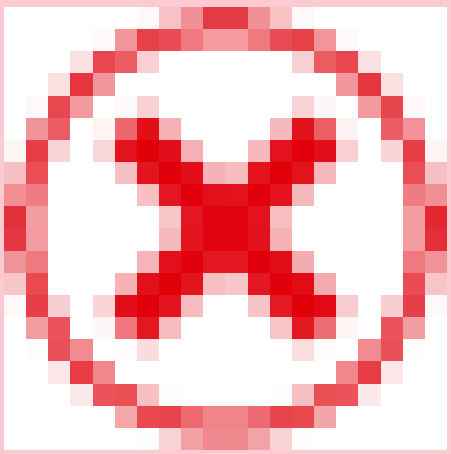
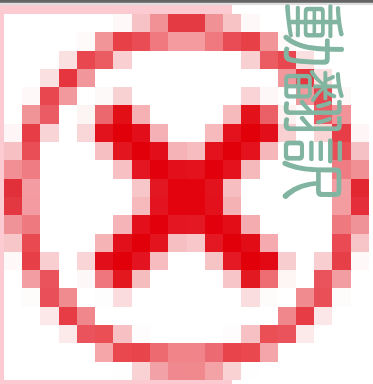
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
最高優先度				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

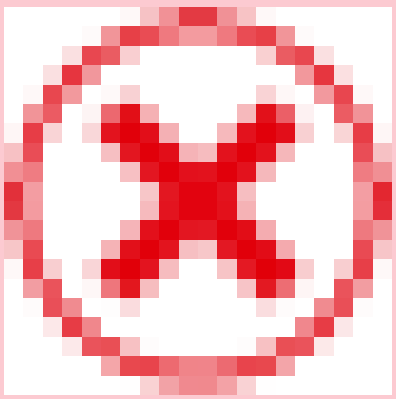
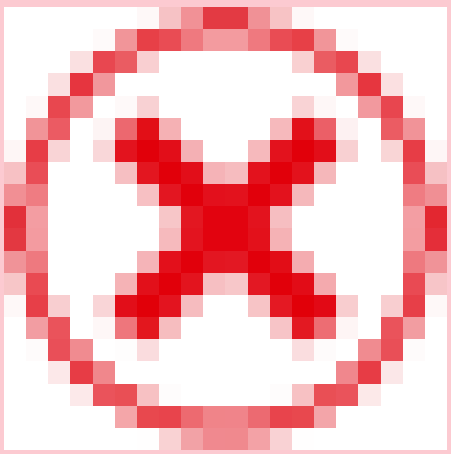
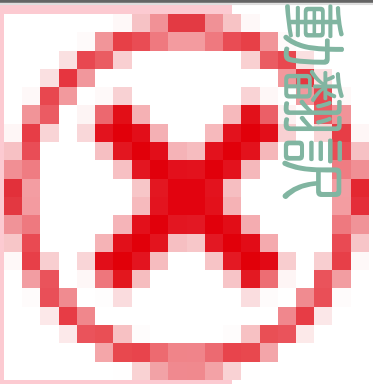
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
脆弱性一致アイテムを使用				

ライブラリ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

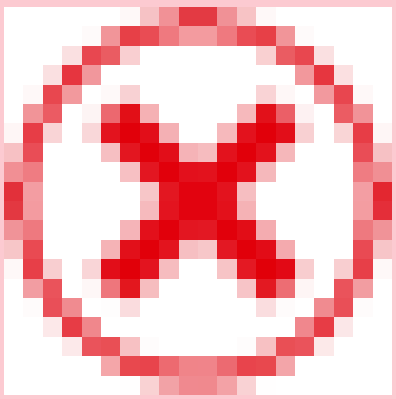
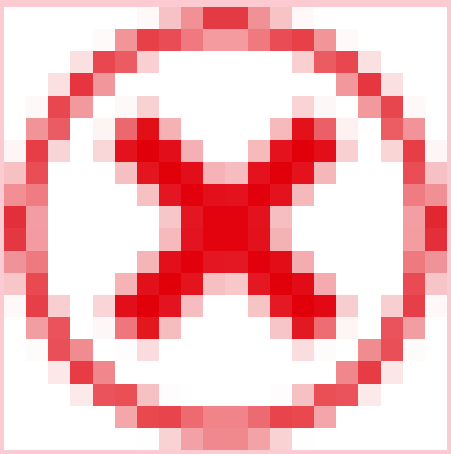
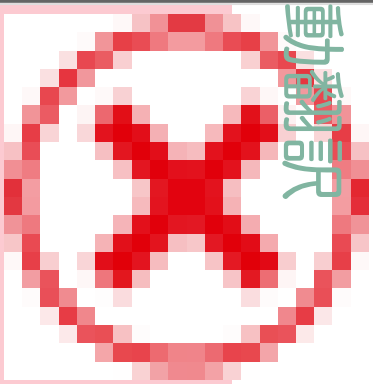
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
NVD				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

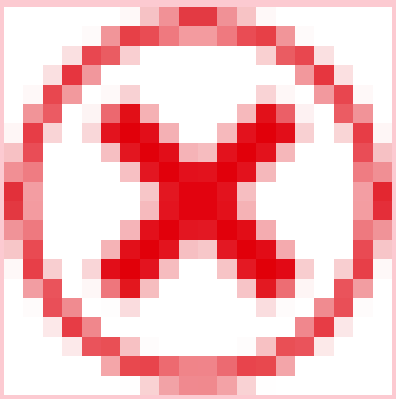
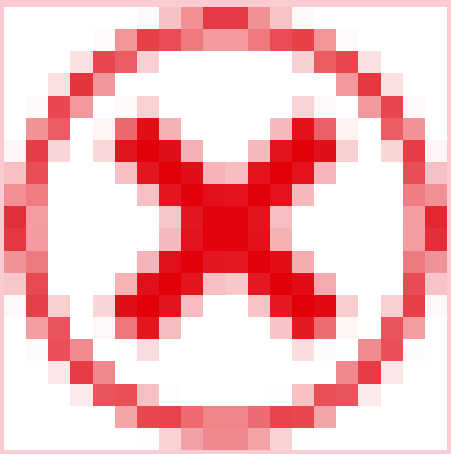
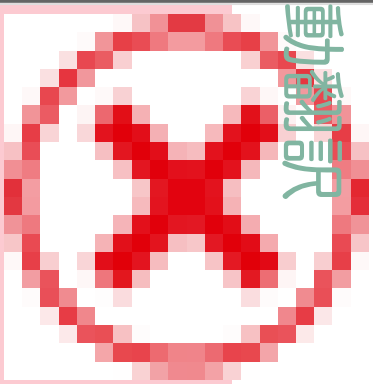
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
CWE				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

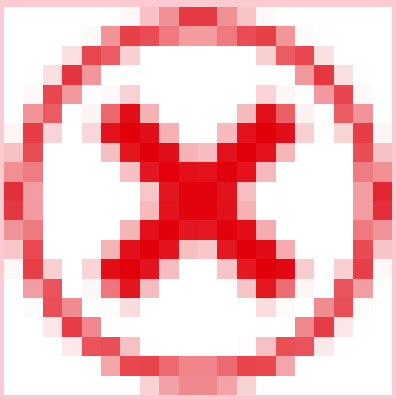
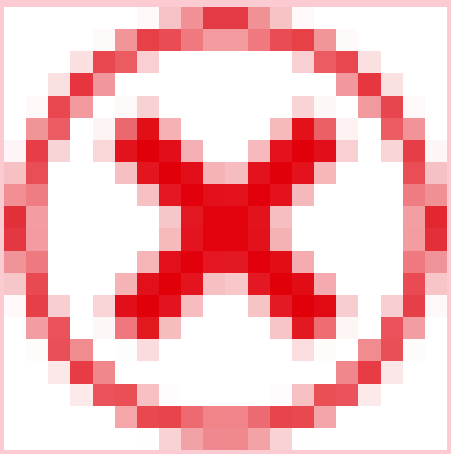
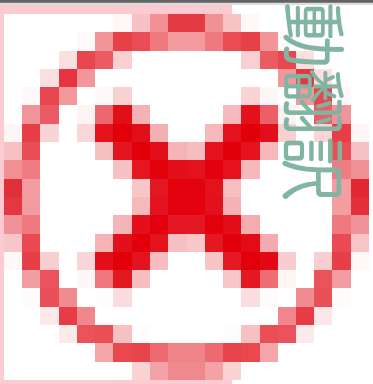
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
サードパーティ				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

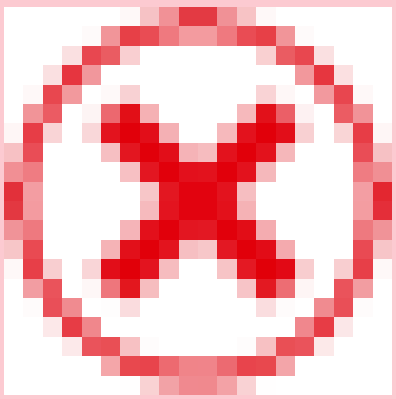
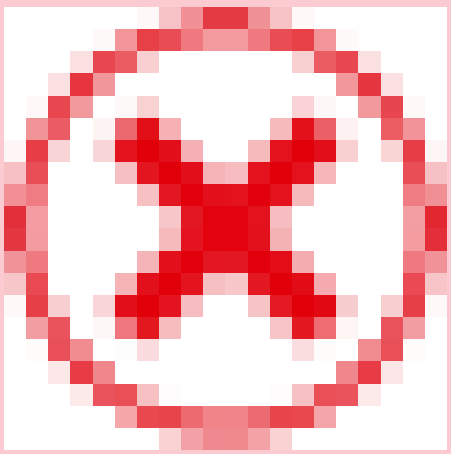
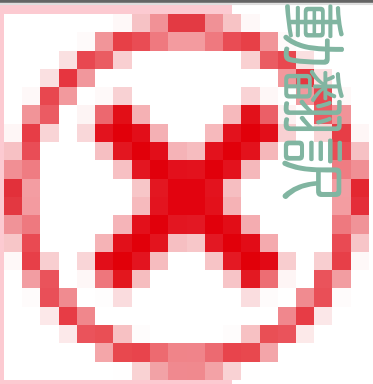
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
脆弱なソフトウェア				
脆弱性スキャン				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

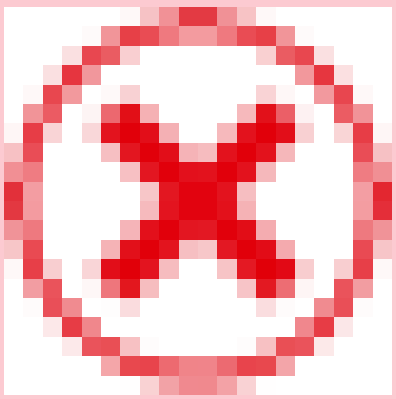
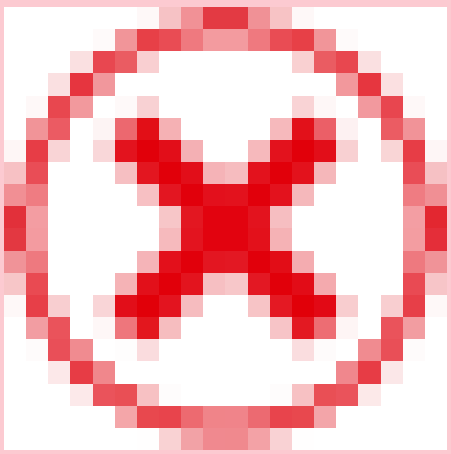
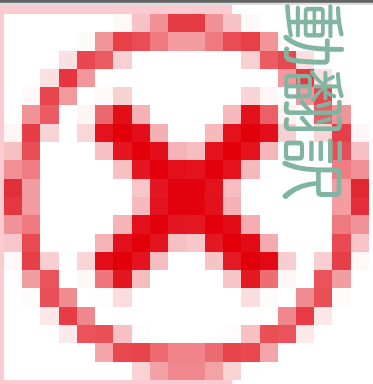
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
エクスポージャーアセスメント				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

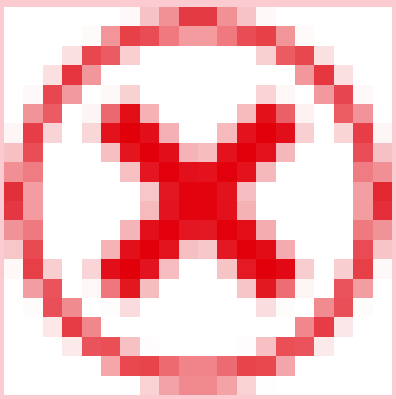
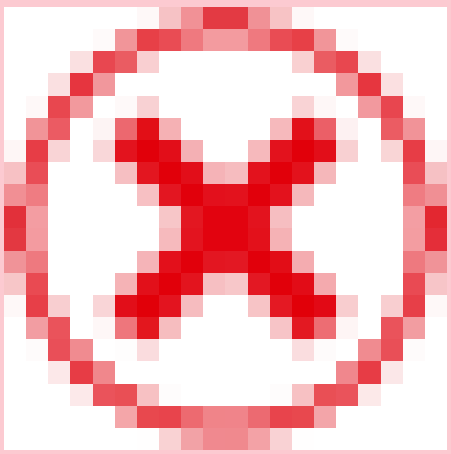
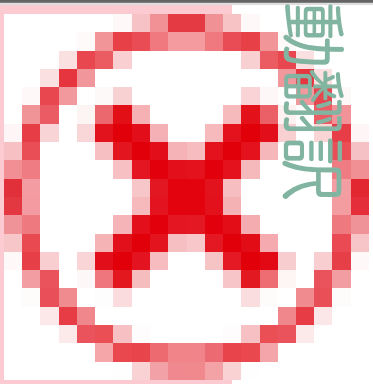
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
スキャン				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

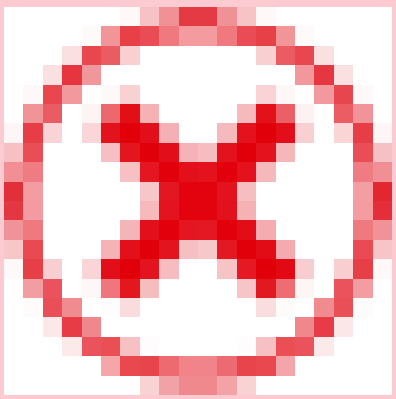
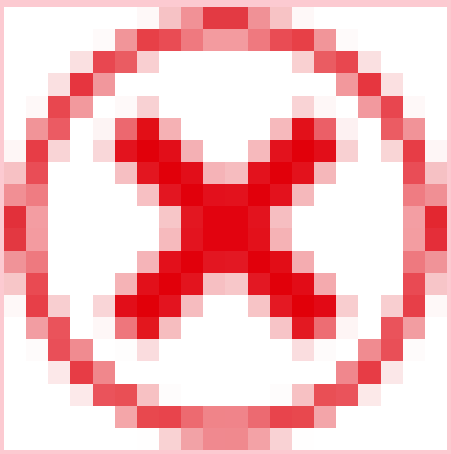
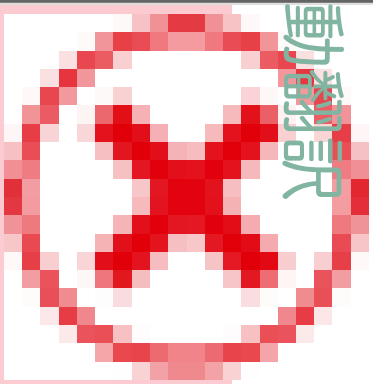
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
スキャナー				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

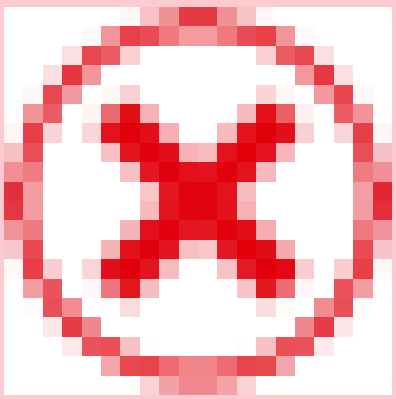
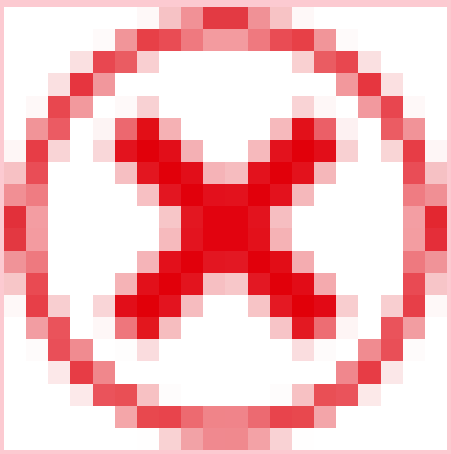
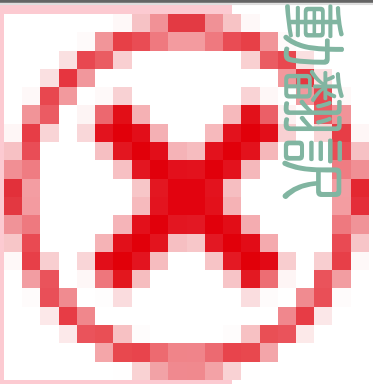
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
スキャンキュー				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

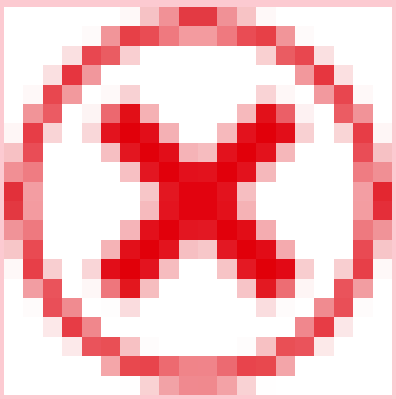
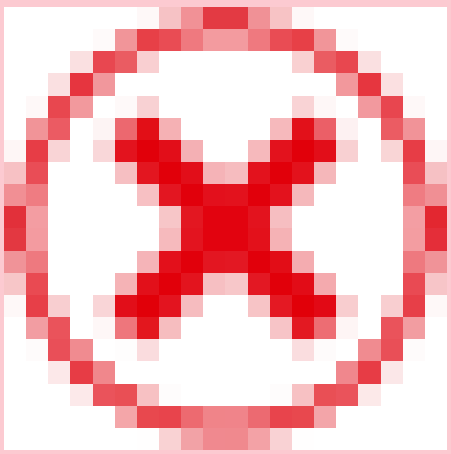
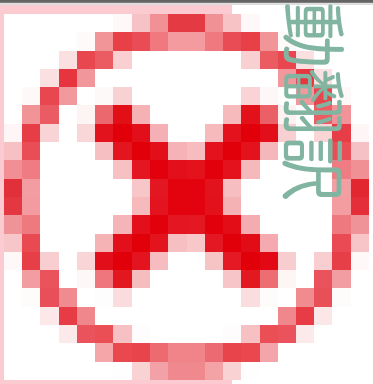
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
スキャナーレート制限				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

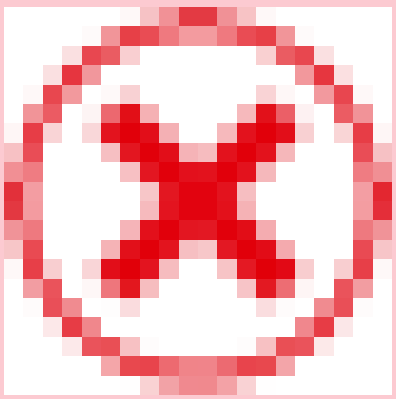
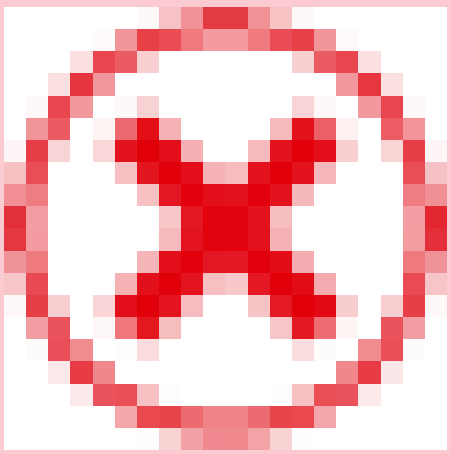
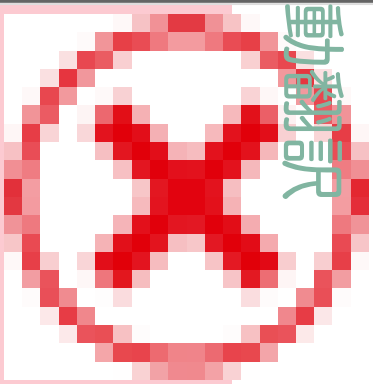
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
レート制限定義				
管理				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

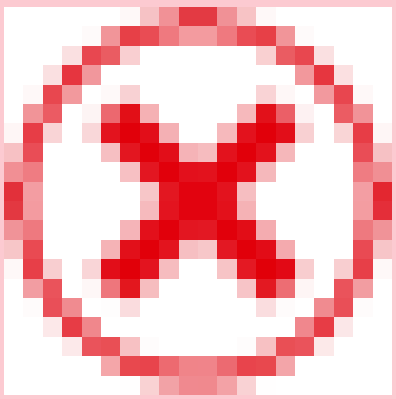
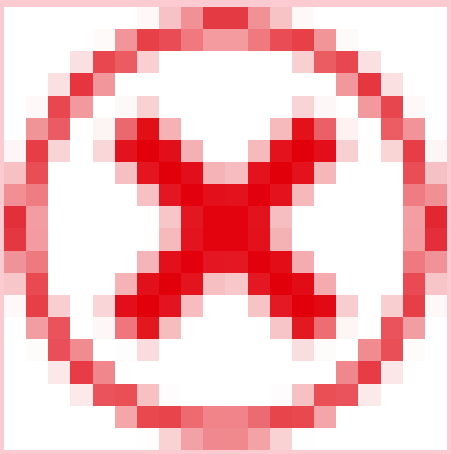
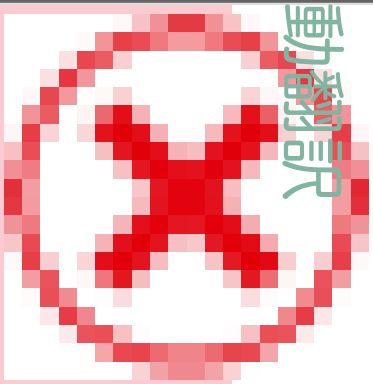
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
セットアップアシスタント				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

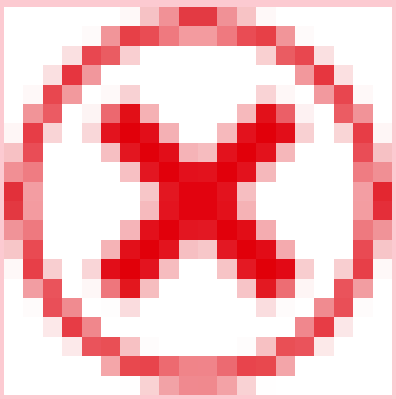
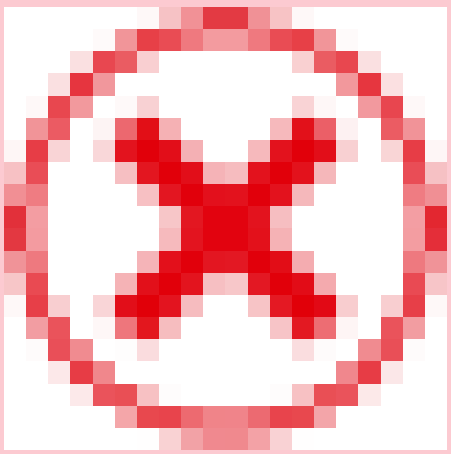
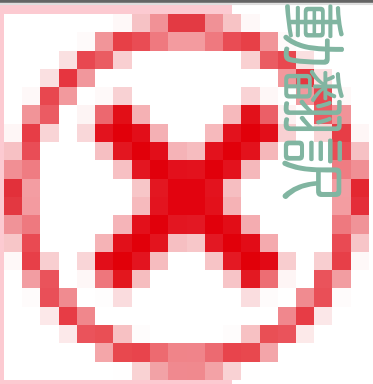
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
監視トピック				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

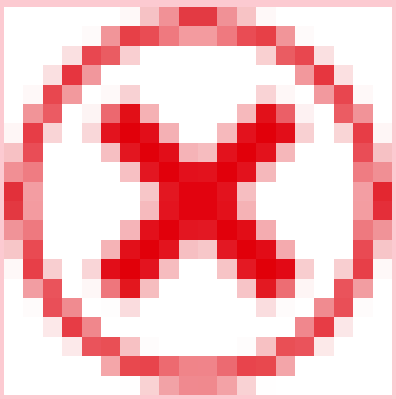
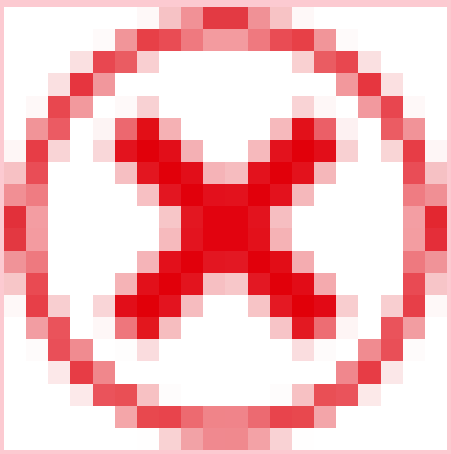
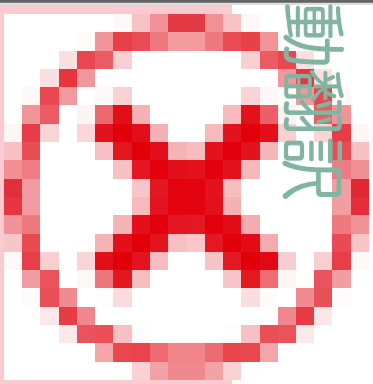
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
アサインルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

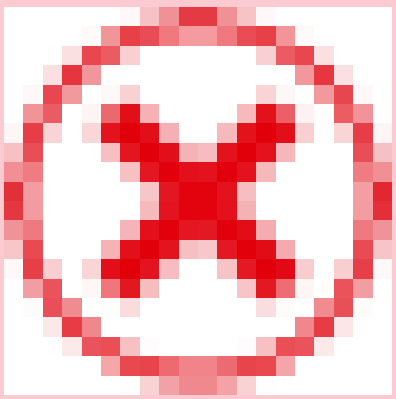
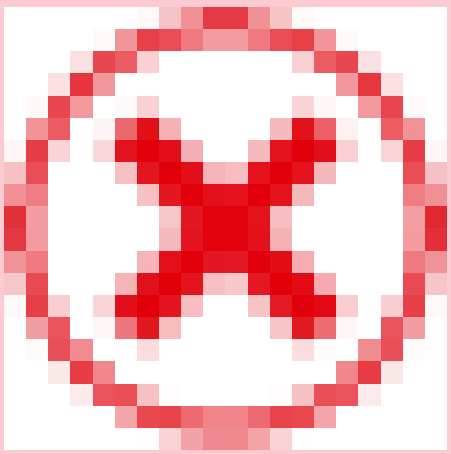
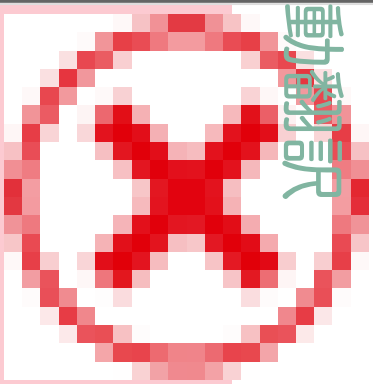
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
修復タスクルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

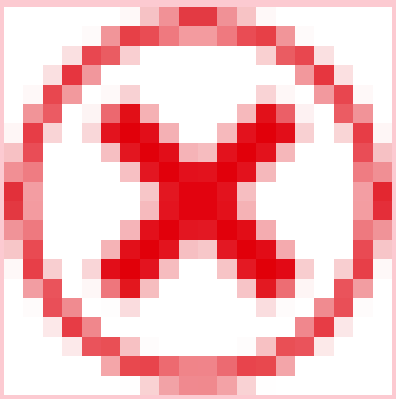
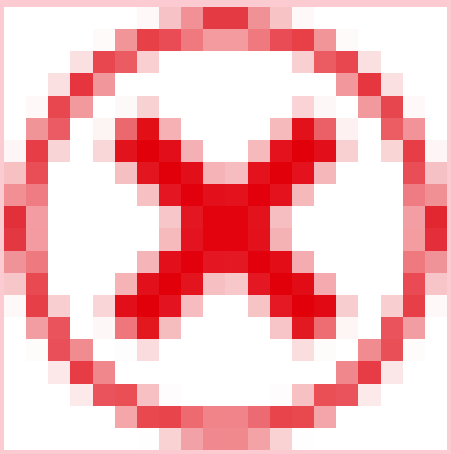
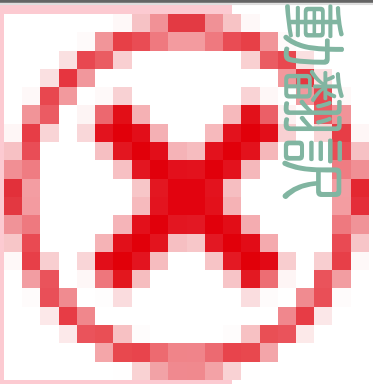
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
アサインの推奨				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

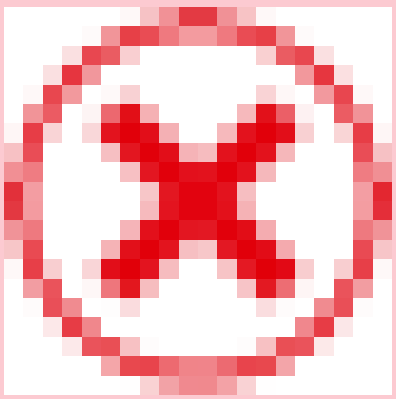
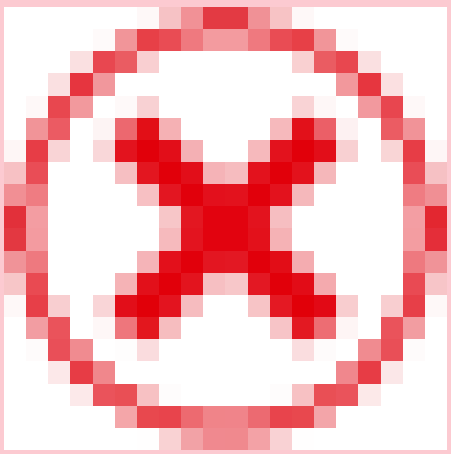
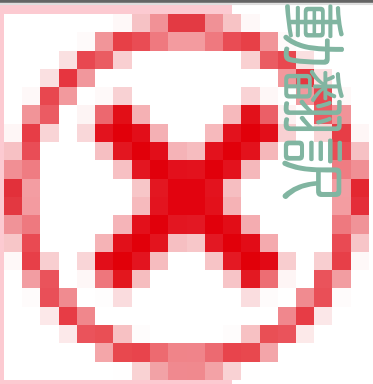
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
脆弱性算出				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

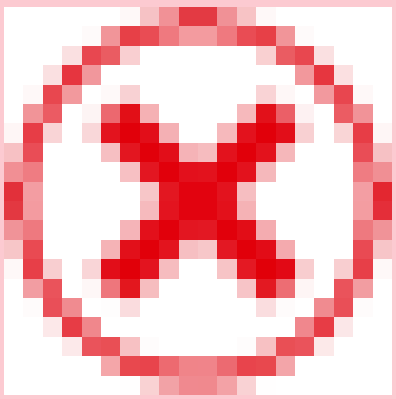
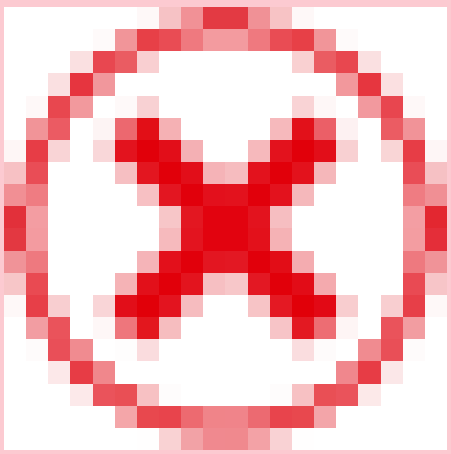
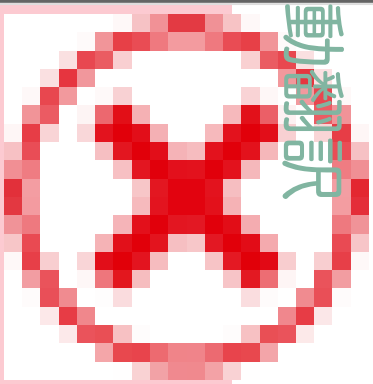
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
脆弱性ロールアップ算出				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

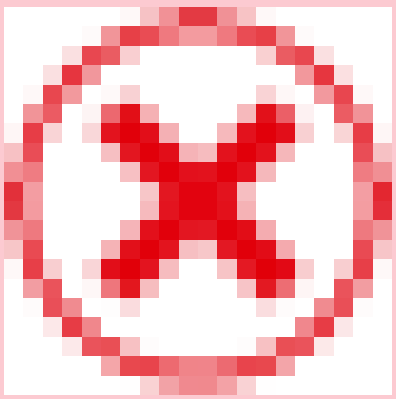
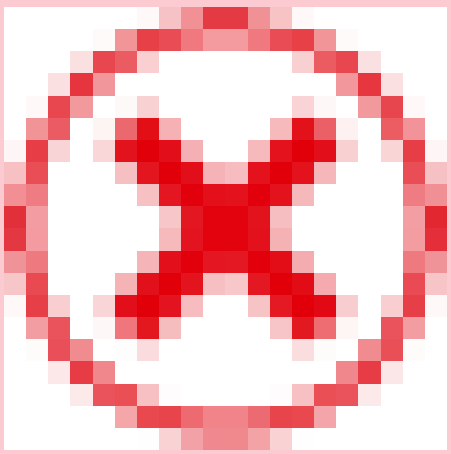
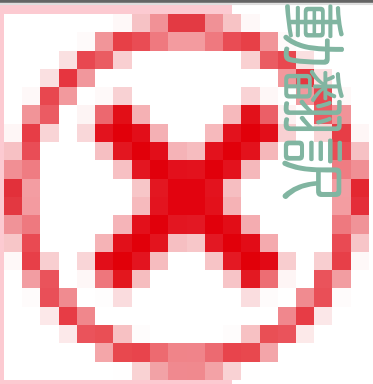
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
修復ターゲットルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

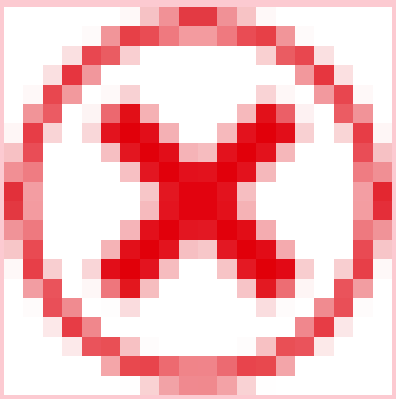
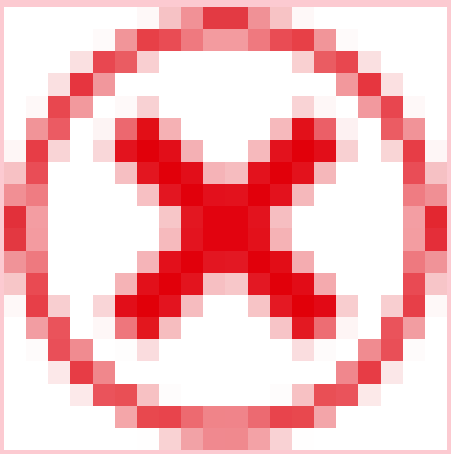
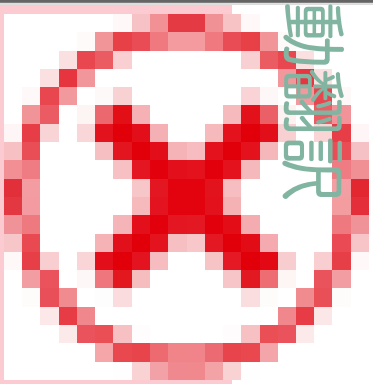
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
自動クローズ構成				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

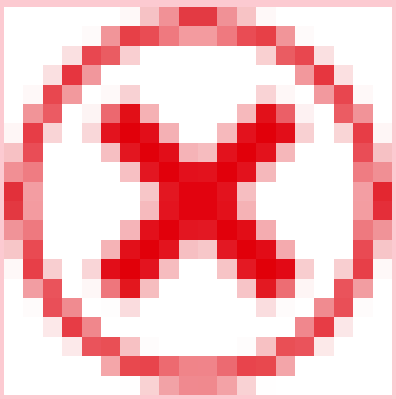
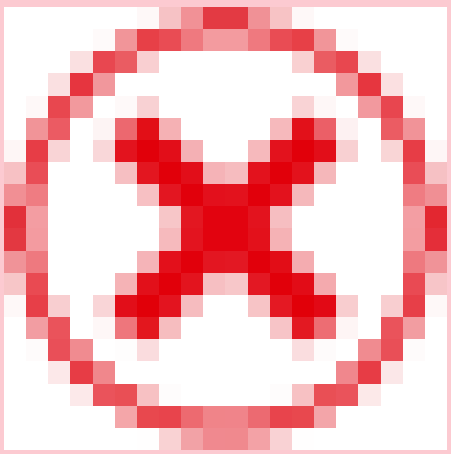
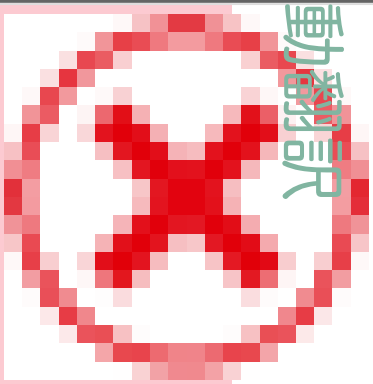
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
ルールの自動削除				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

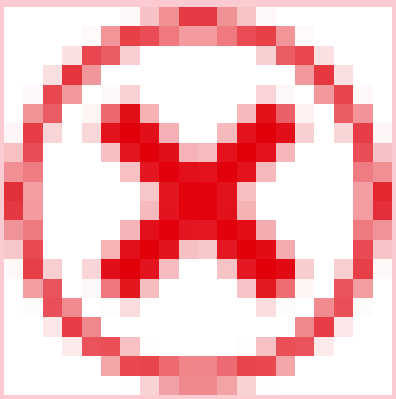
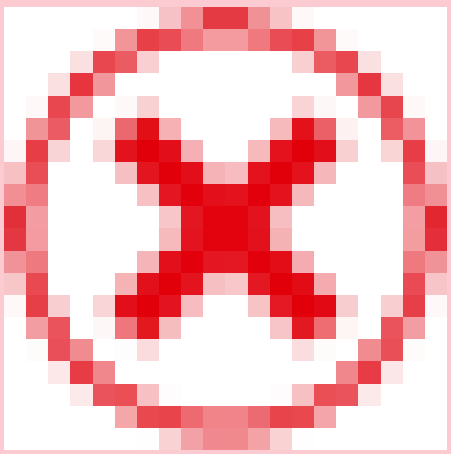
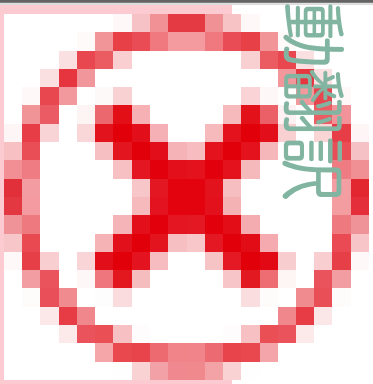
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
例外ルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

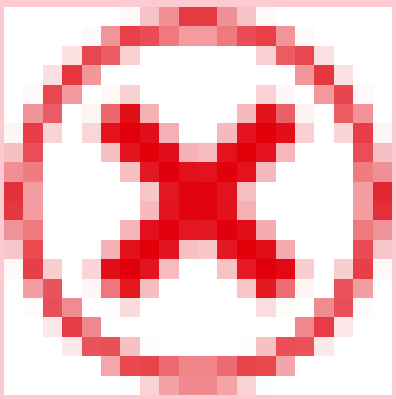
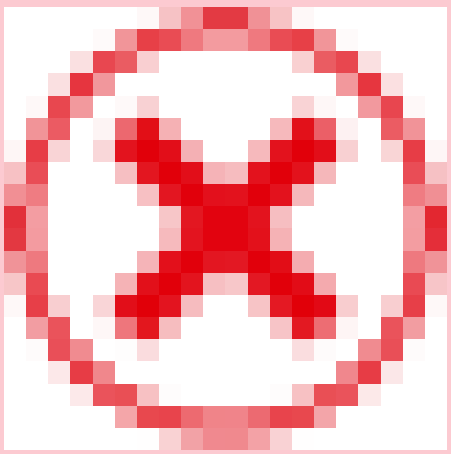
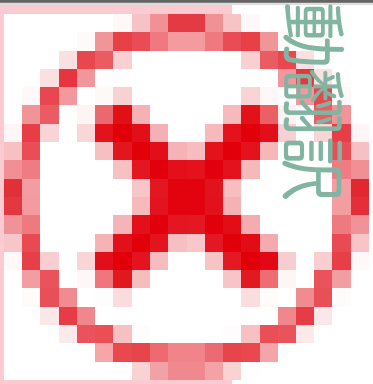
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
承認ルール				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

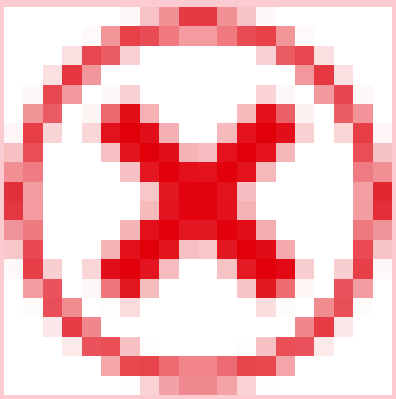
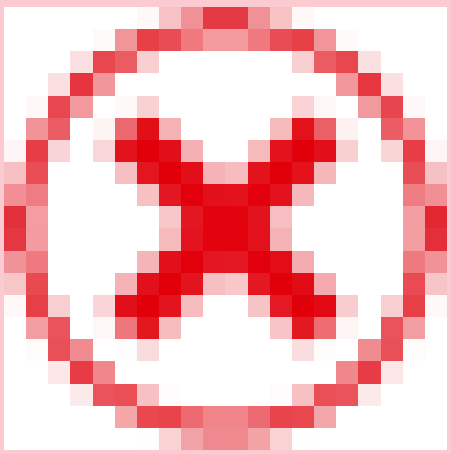
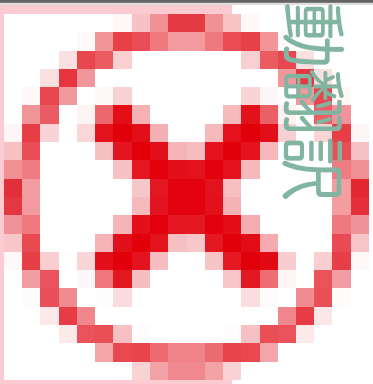
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
分類ルール				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

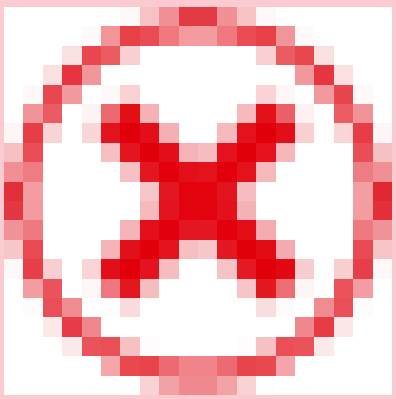
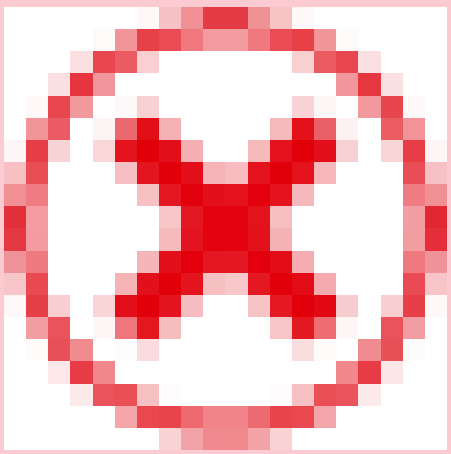
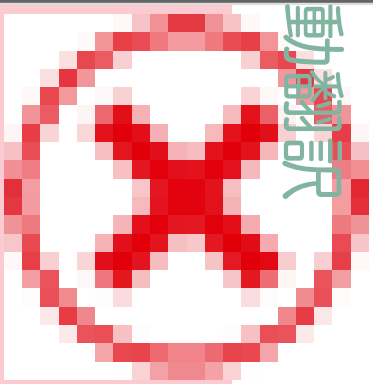
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
パフォーマンス構成				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

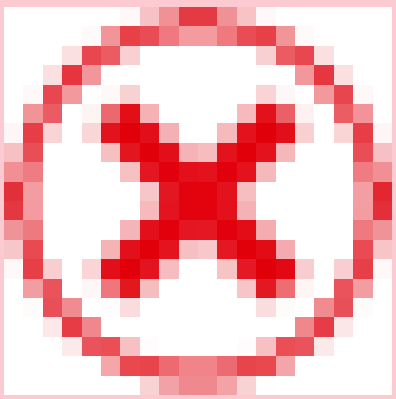
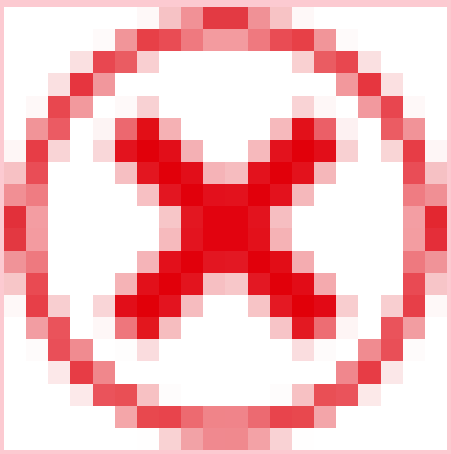
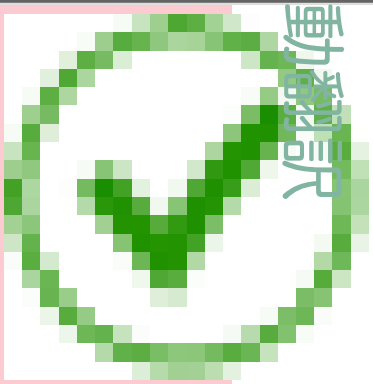
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
VI の粒度の構成				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

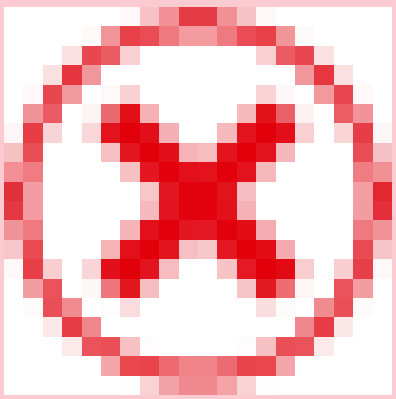
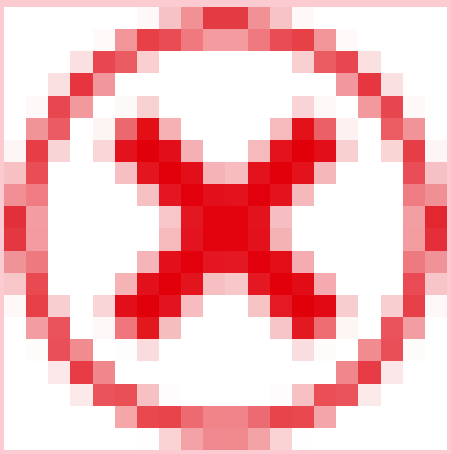
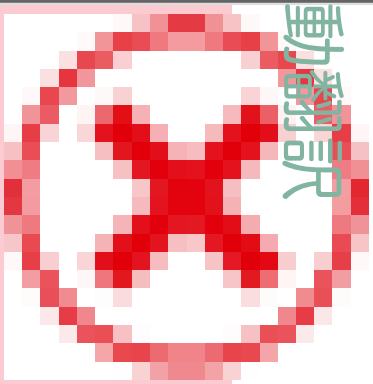
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
通知				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

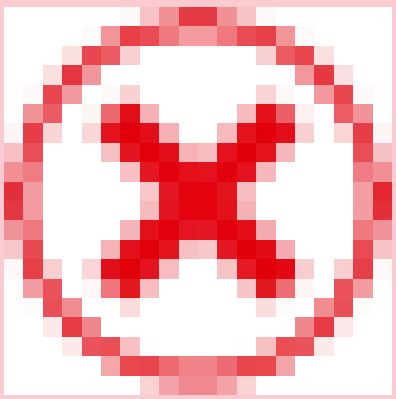
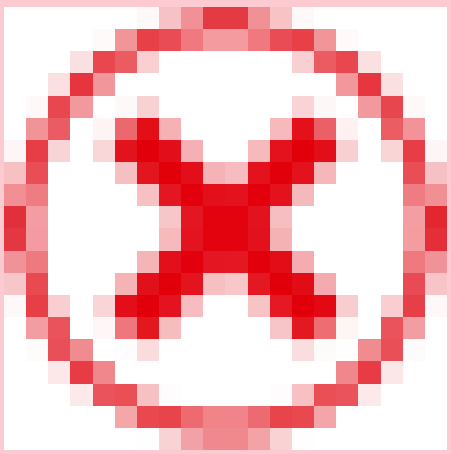
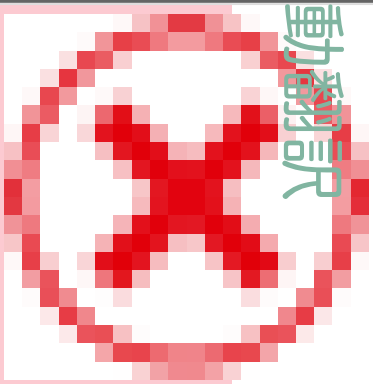
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
メールテンプレート				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

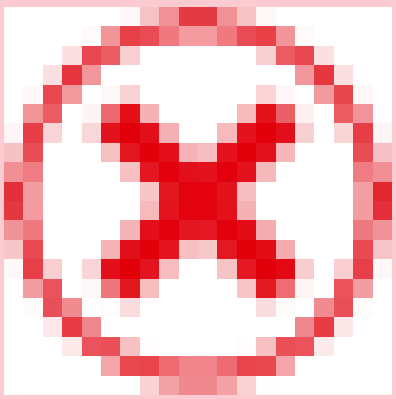
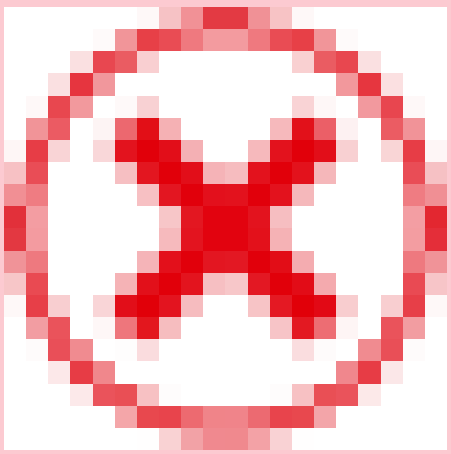
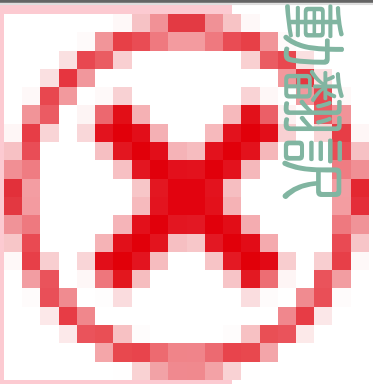
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
キューをインポート				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

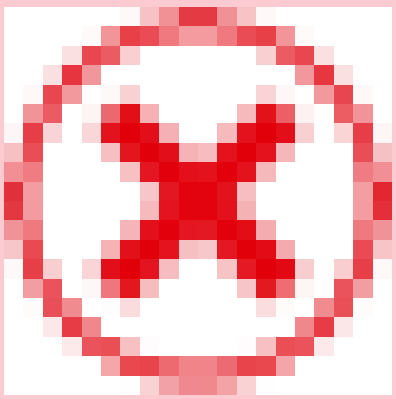
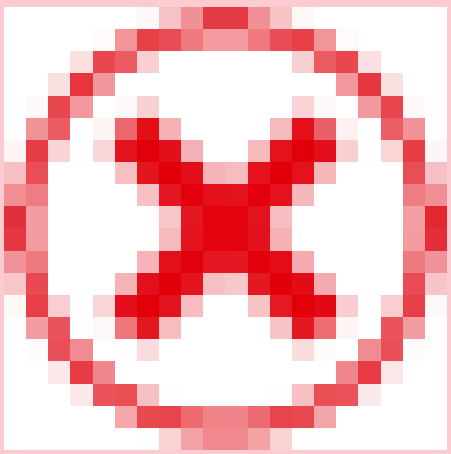
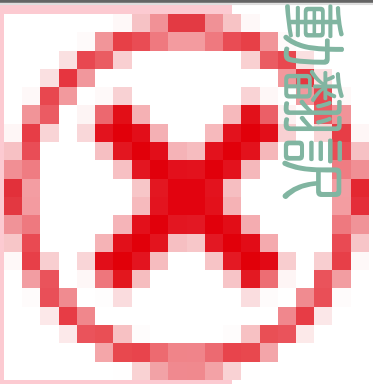
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
統合				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

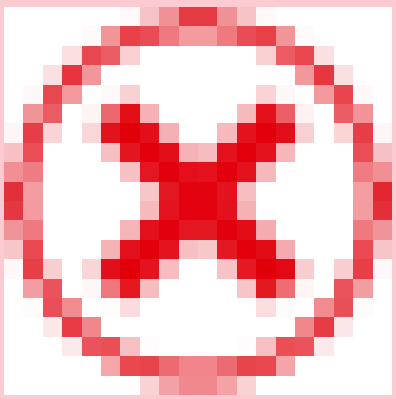
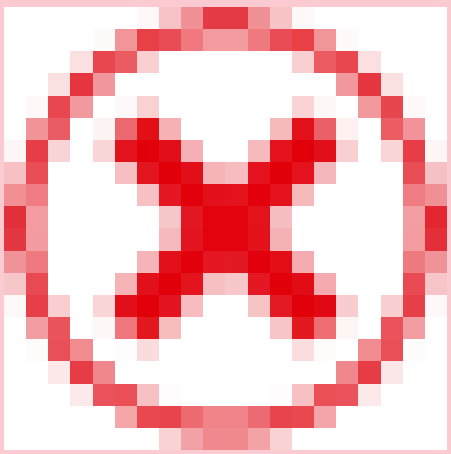
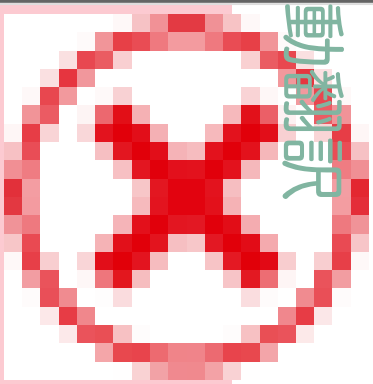
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
SLA 定義				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

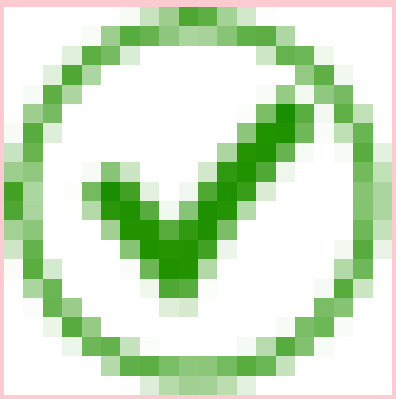
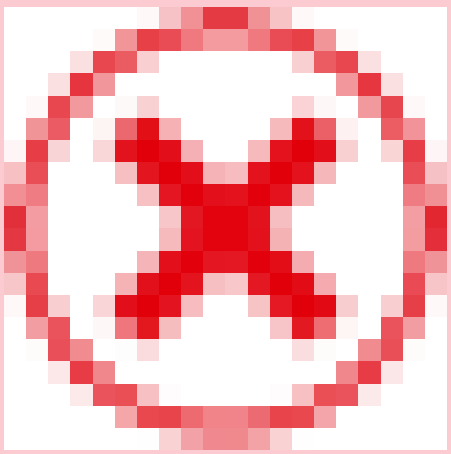
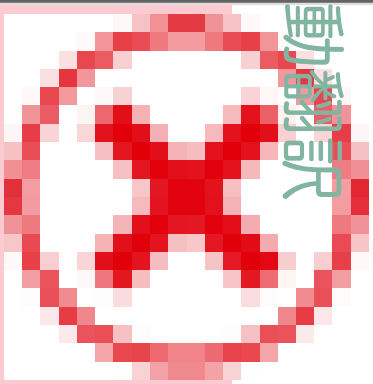
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
SAM NVD の構成				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

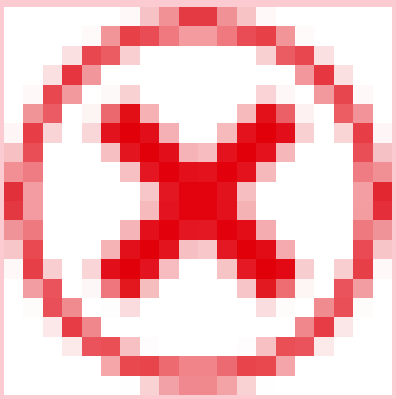
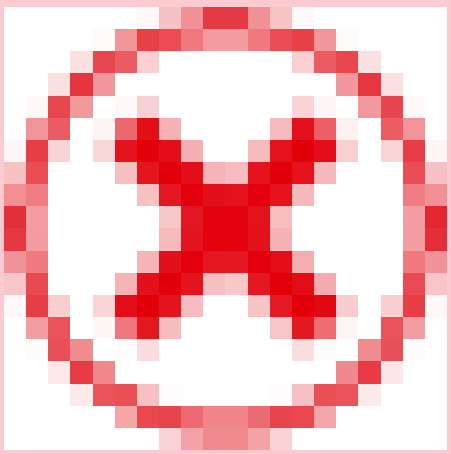
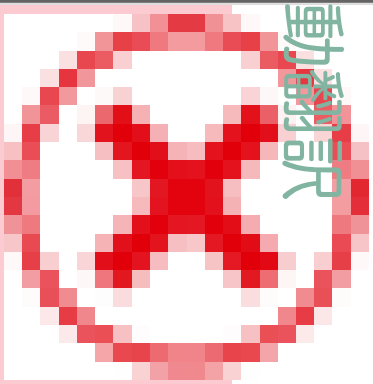
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
正規化された重大度マップ				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

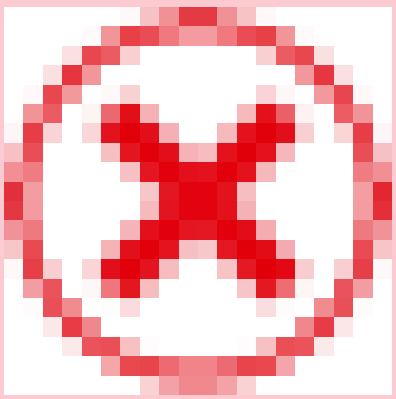
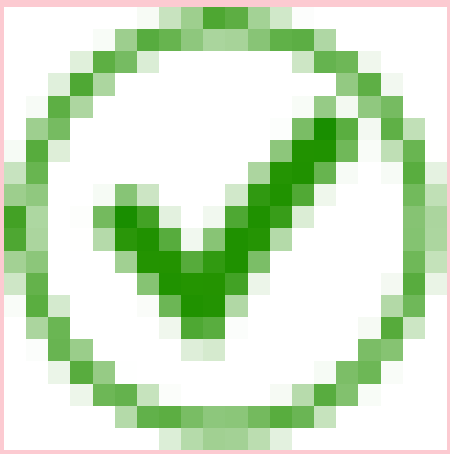
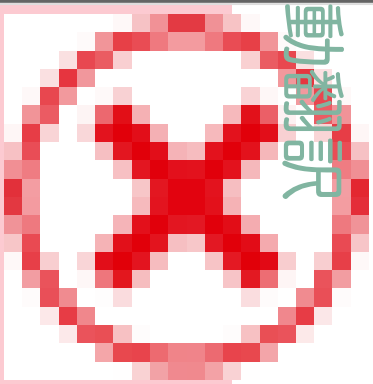
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
スキャン範囲構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

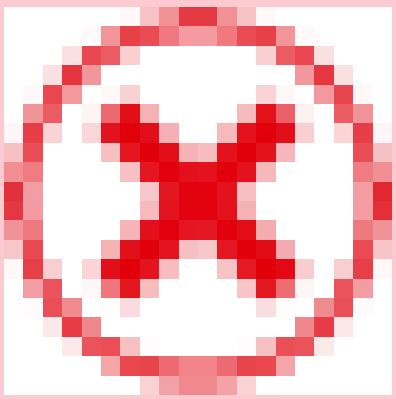
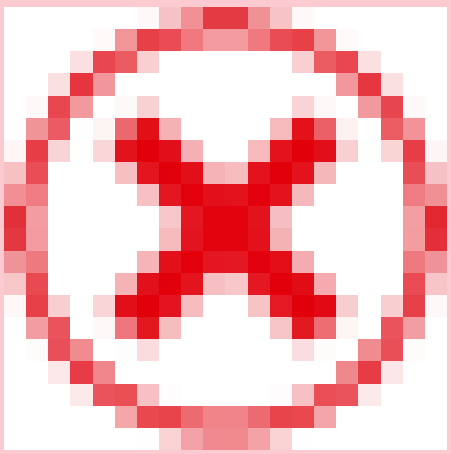
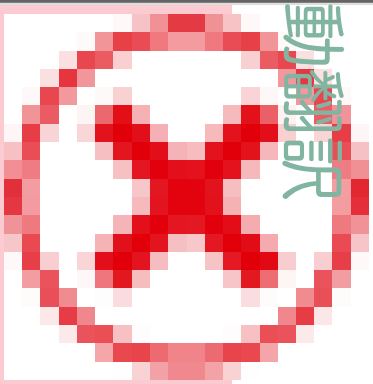
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
例外管理				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

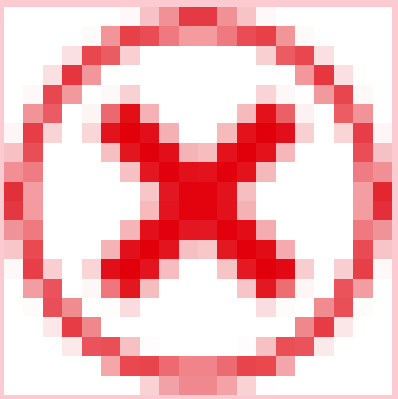
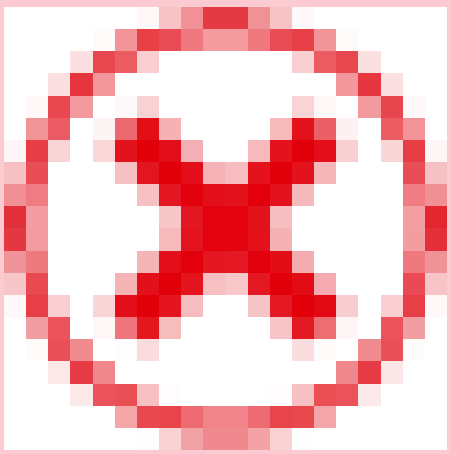
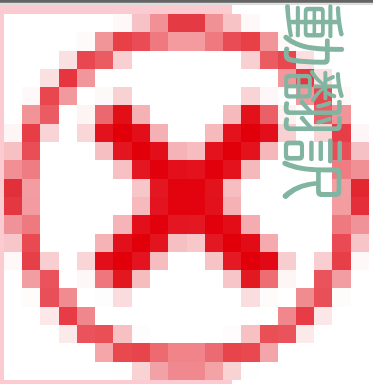
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
使用状況レポート				
診断				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configure_vi_granularity、

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

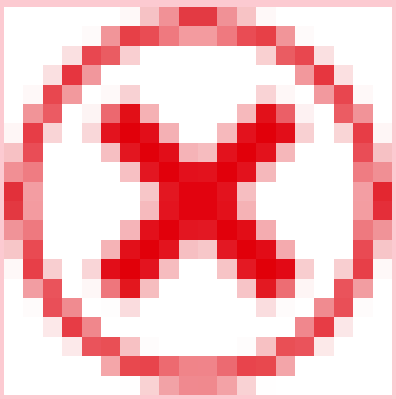
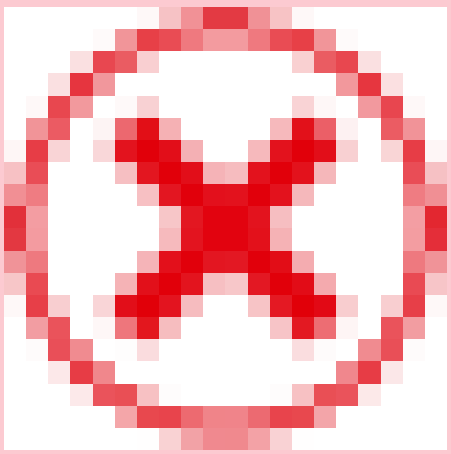
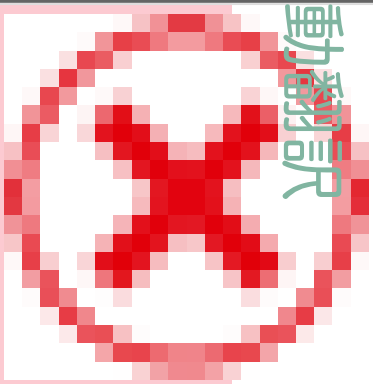
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity	sn_
チェック				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

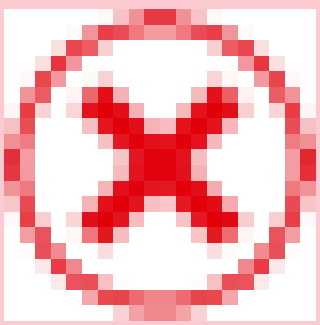
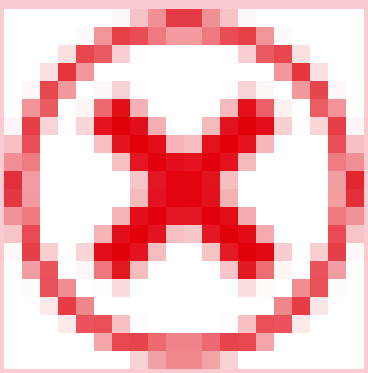
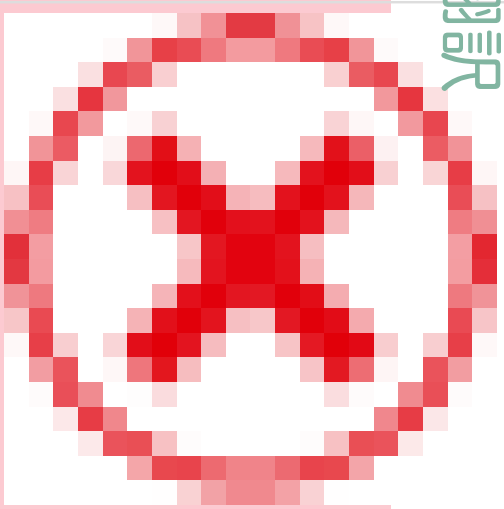
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
(メインアプリグループ)				
CISO ダッシュボード				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

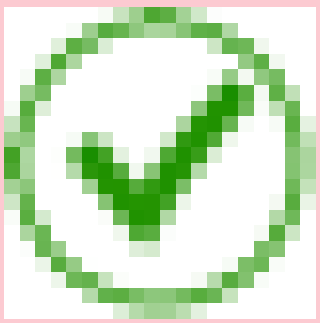
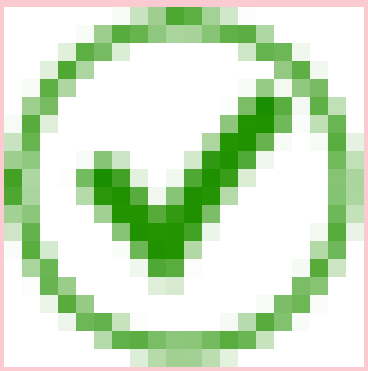
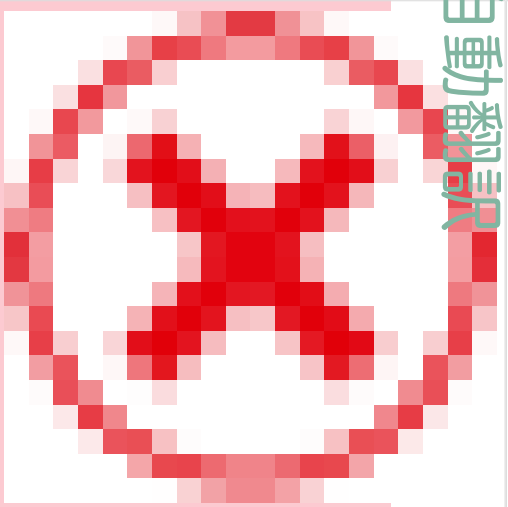
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
修復の概要				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

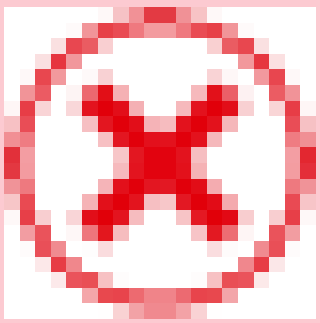
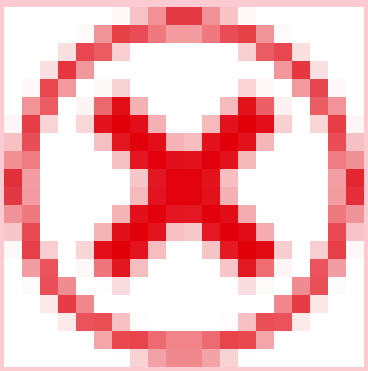
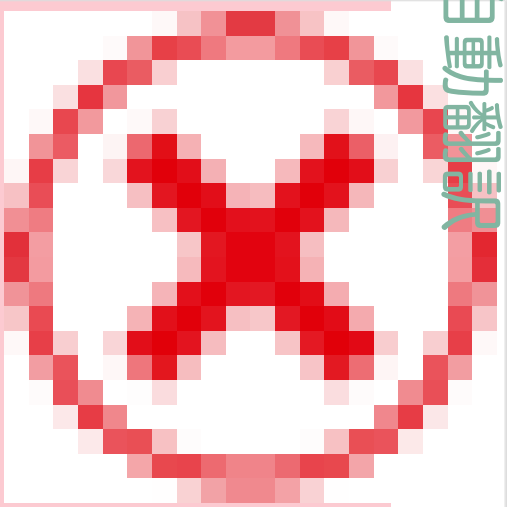
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
脆弱性マネージャーのワークスペース				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

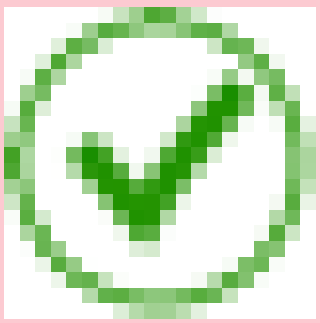
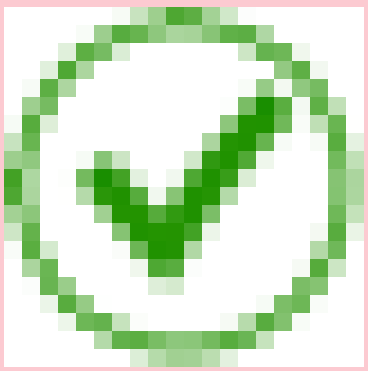
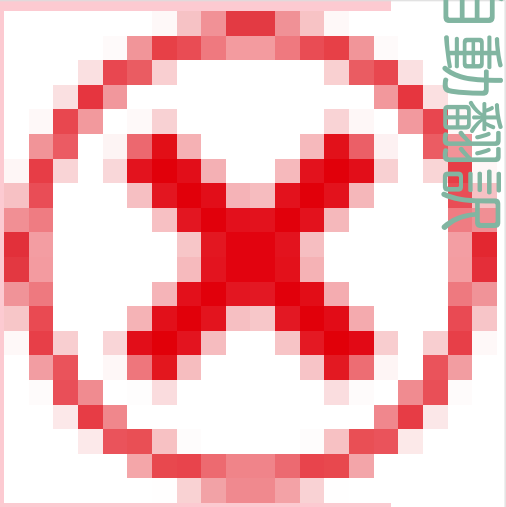
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
概要				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

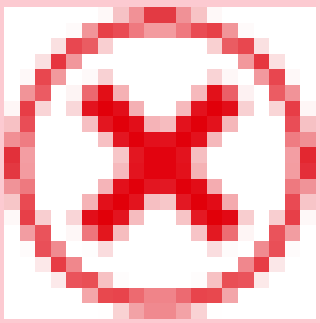
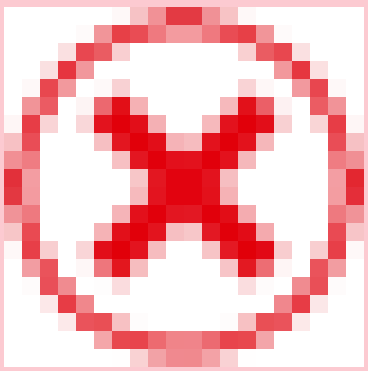
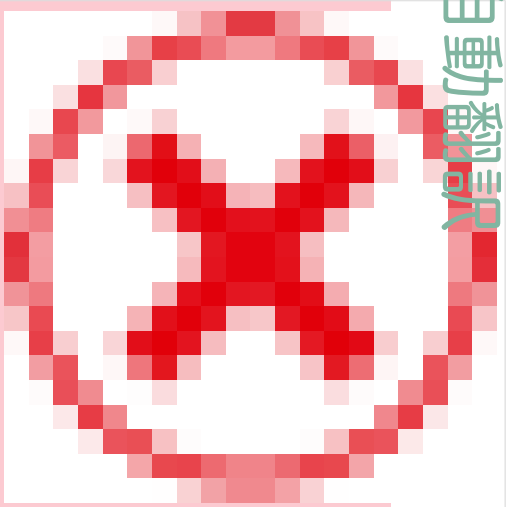
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
IT 修復ワークスペース				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

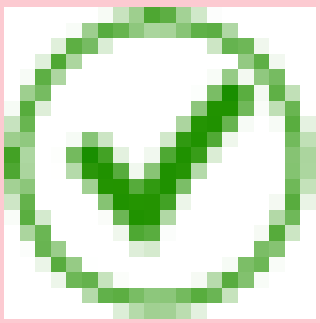
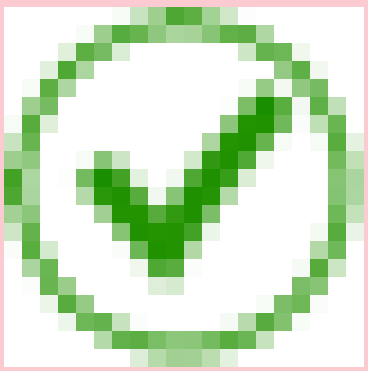
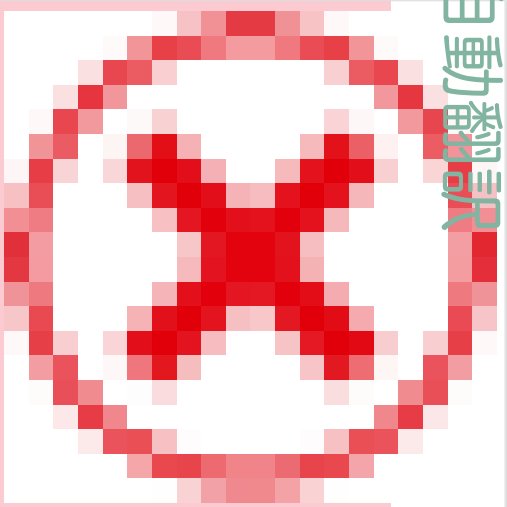
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
承認者の概要				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

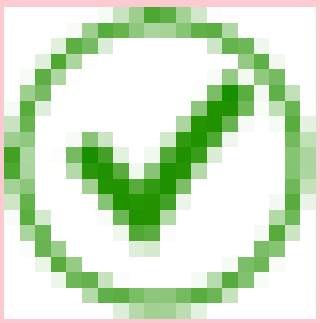
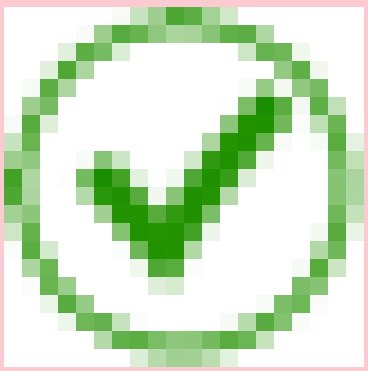
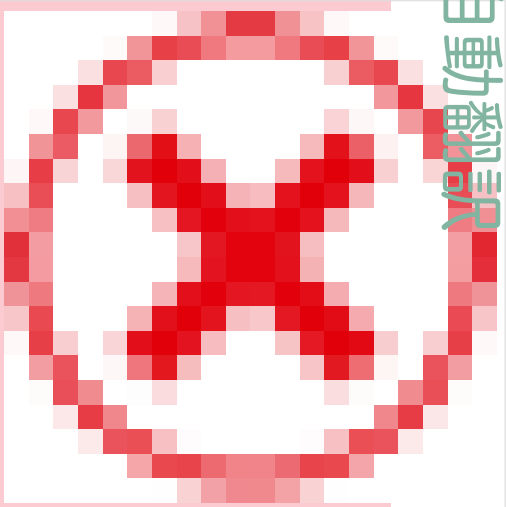
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
概要				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi

sn_vul.manage_exception_configuration

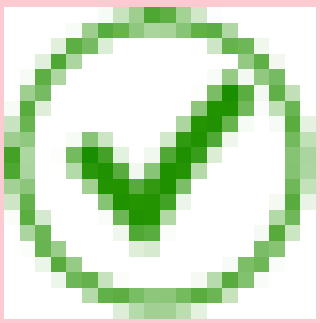
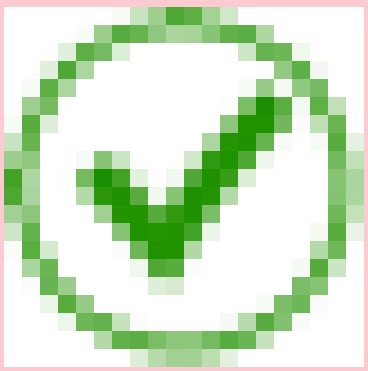
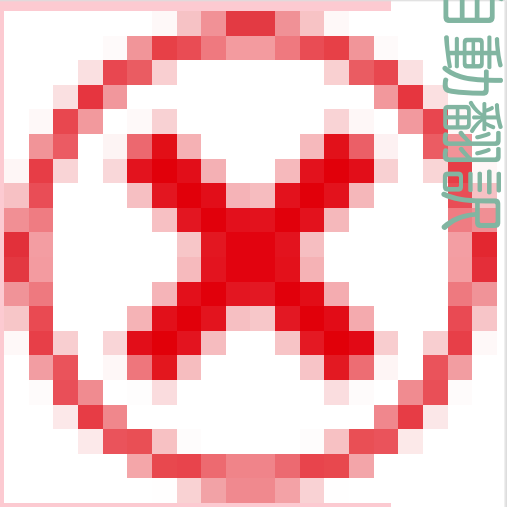
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
自分の承認				

修復タスク

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi

sn_vul.manage_exception_configuration

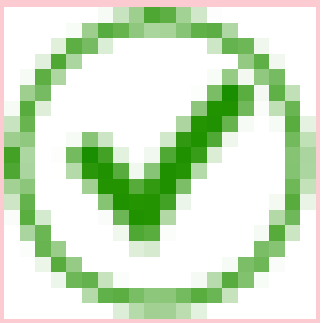
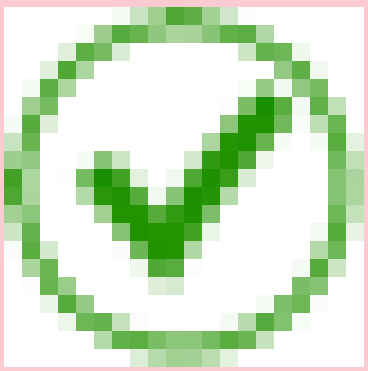
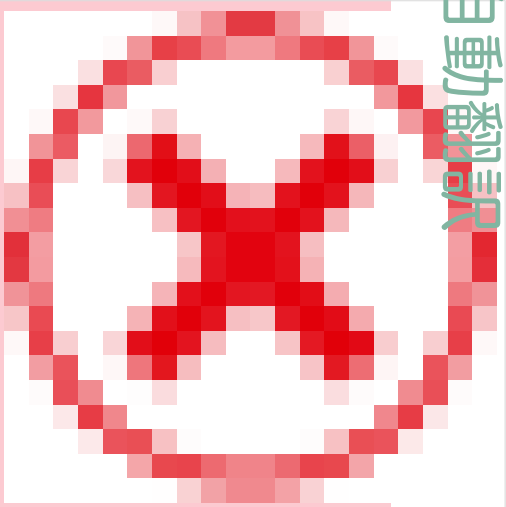
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
有効				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

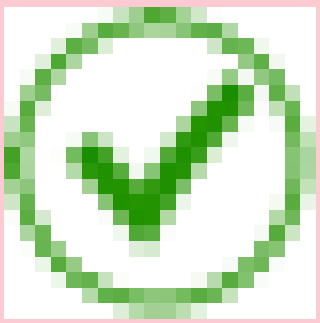
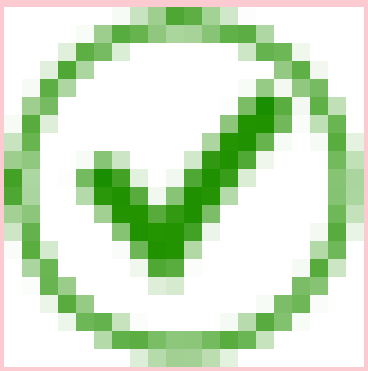
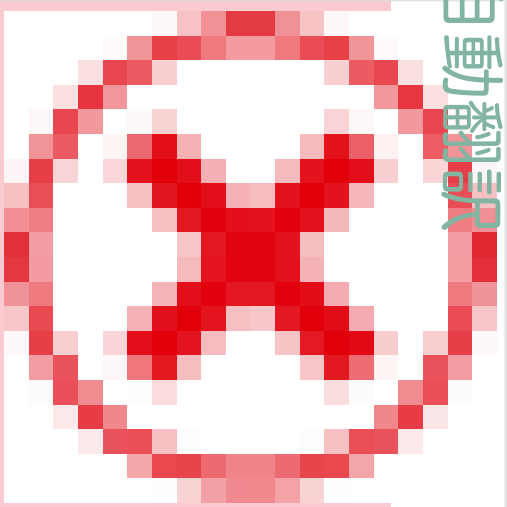
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
自分にアサイン済み				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

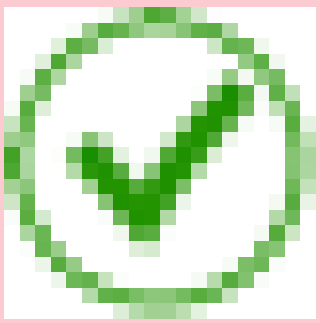
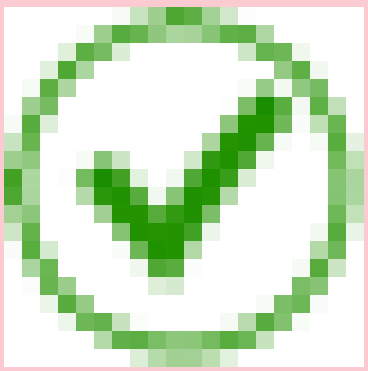
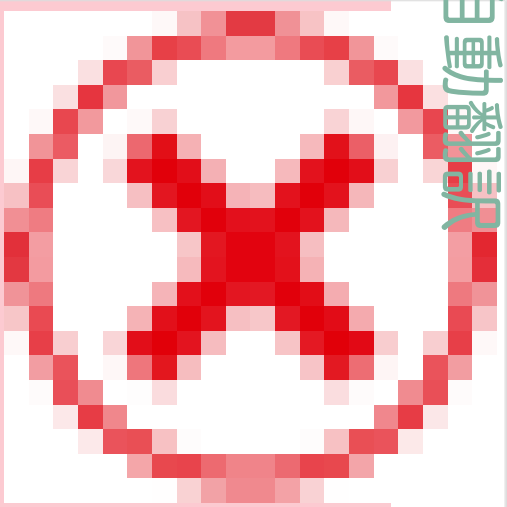
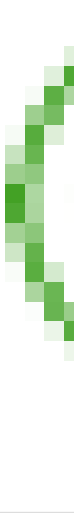
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
所属グループにアサイン済み				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi

sn_vul.manage_exception_configuration

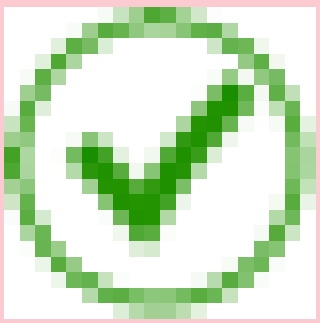
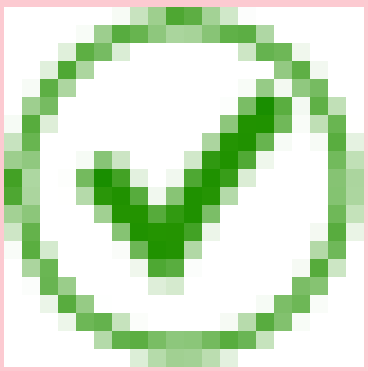
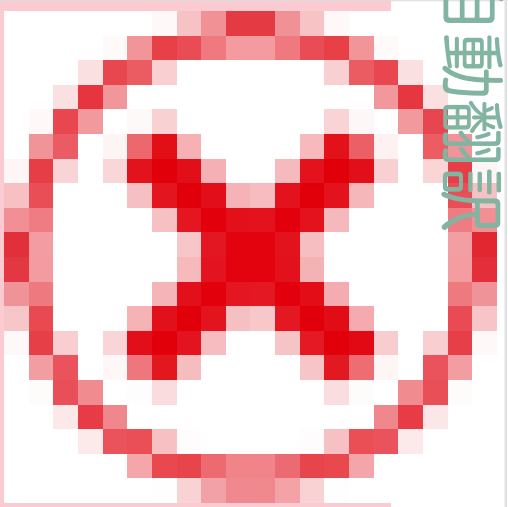
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
すべて				

脆弱性一致アイテム

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

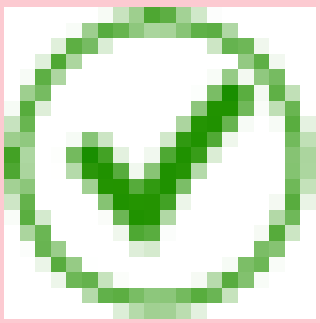
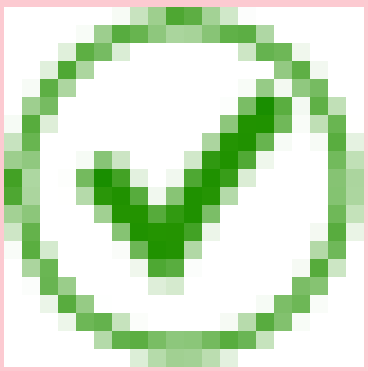
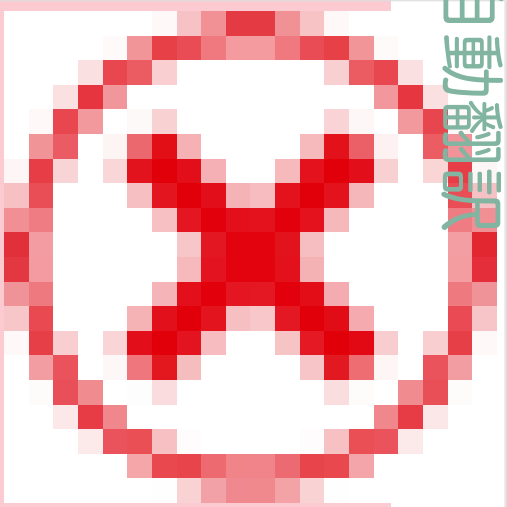
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
重大なリスク				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

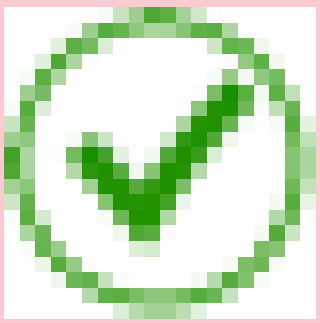
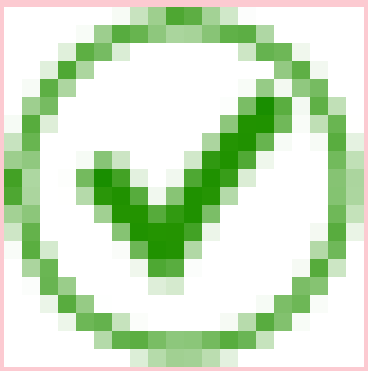
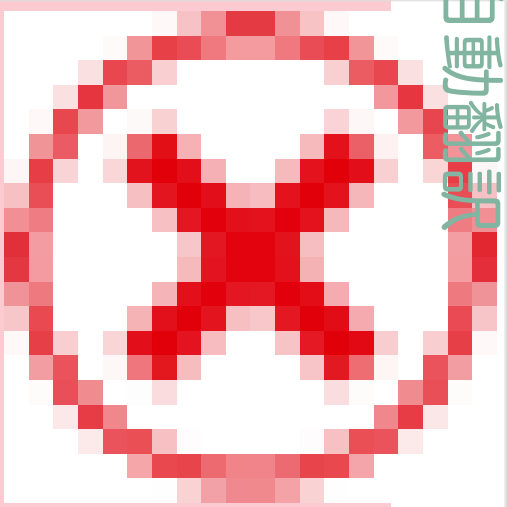
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
高リスク				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

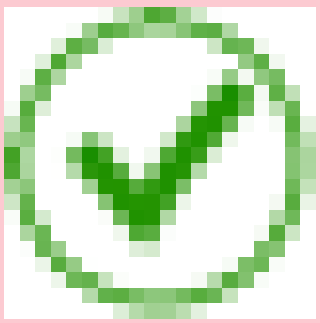
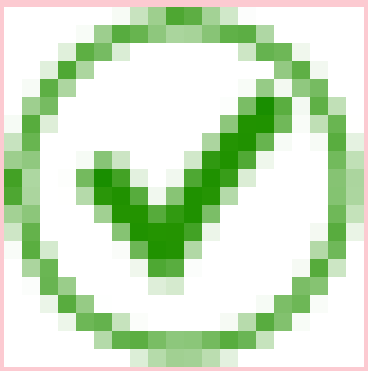
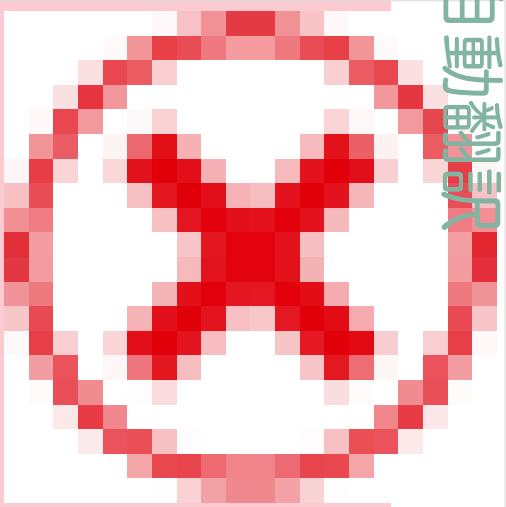
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
エクスプロイト可能				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi

sn_vul.manage_exception_configuration

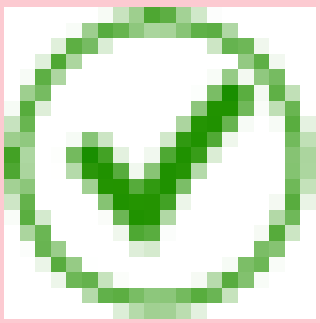
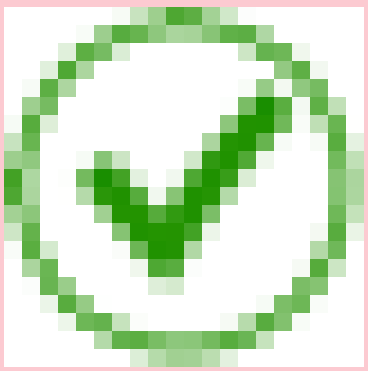
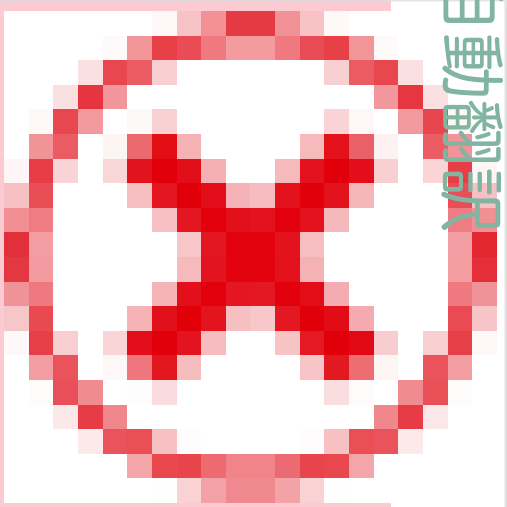
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
該当 CI 確認中				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

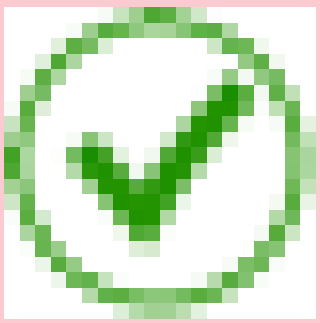
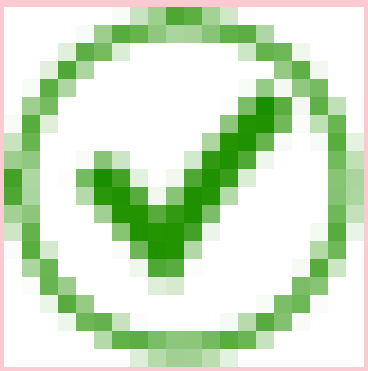
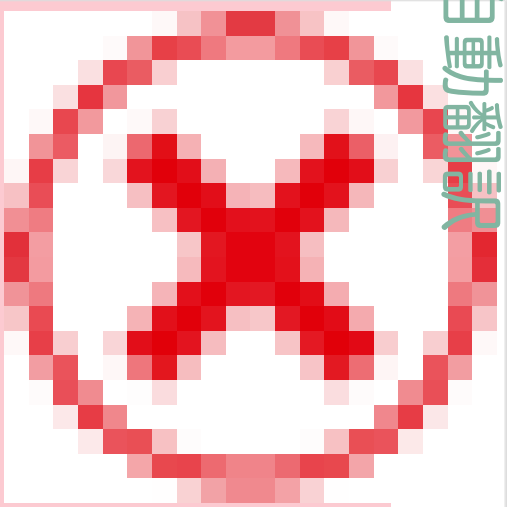
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
CI 不明				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi

sn_vul.manage_exception_configuration

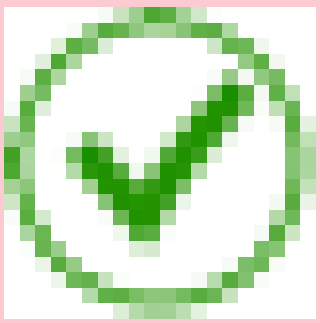
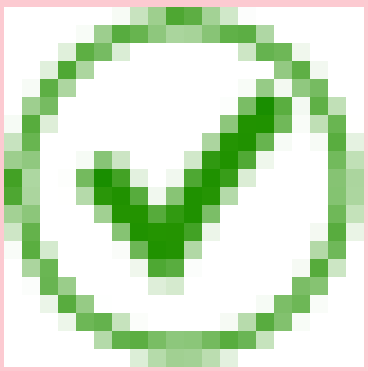
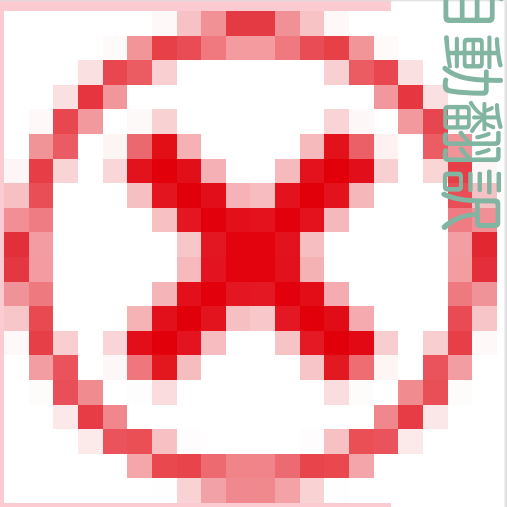
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
過去 90 日以内				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi

sn_vul.manage_exception_configuration

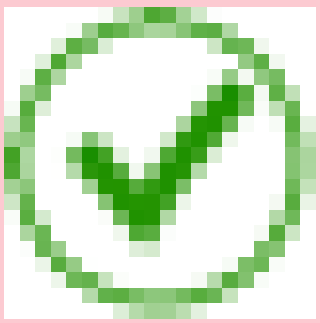
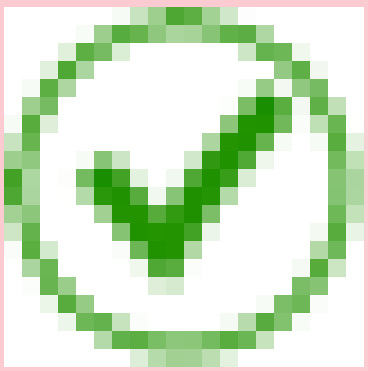
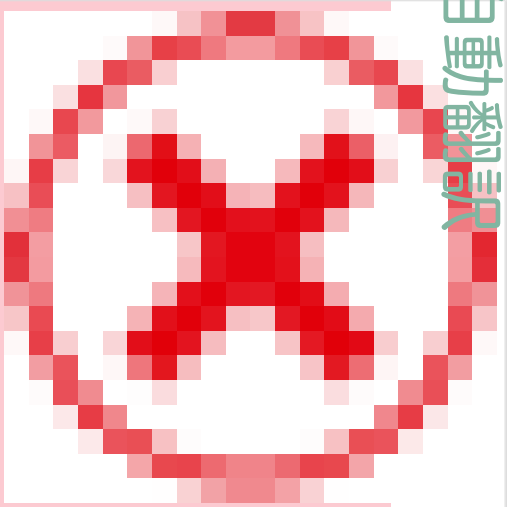
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
91 日以上前				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

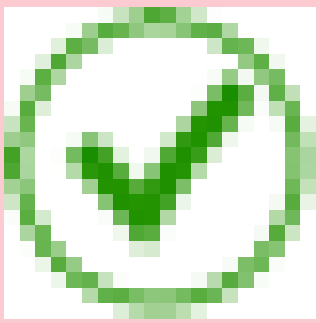
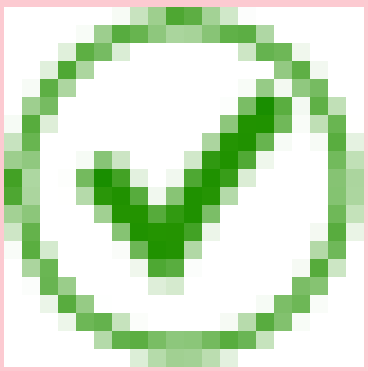
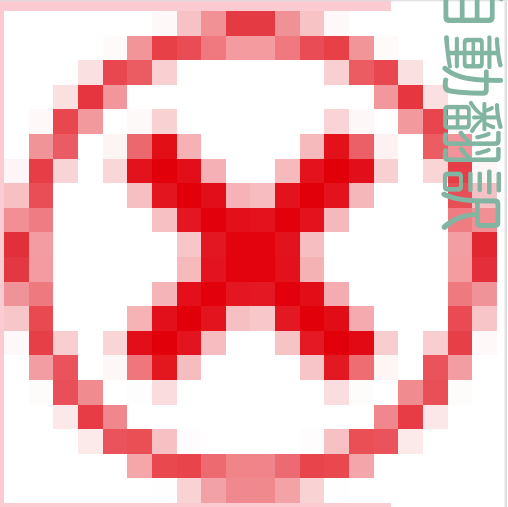
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
未アサイン				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

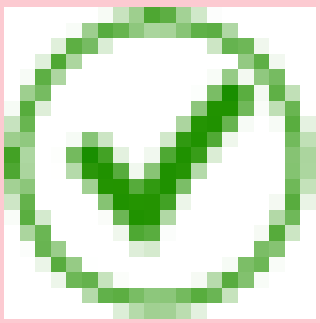
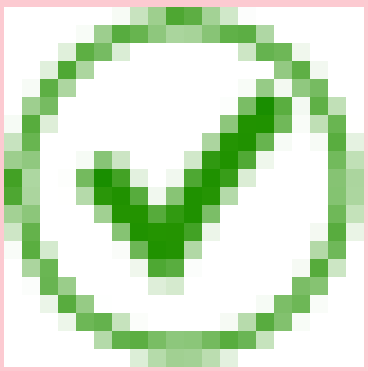
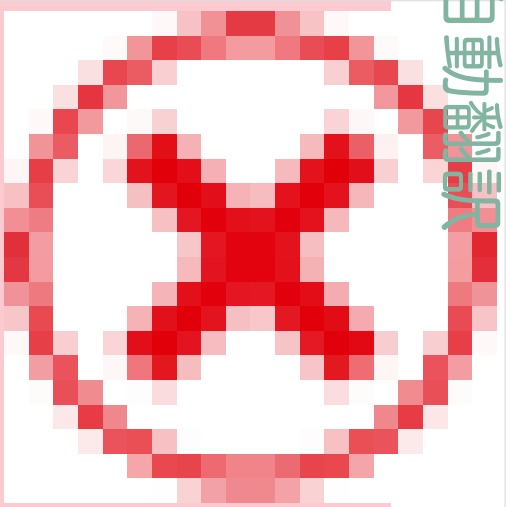
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
修復タスク未割り当て				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

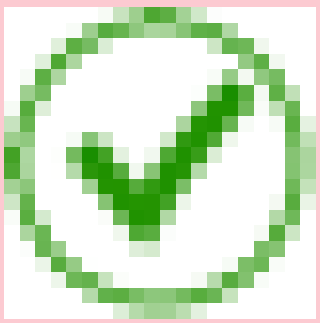
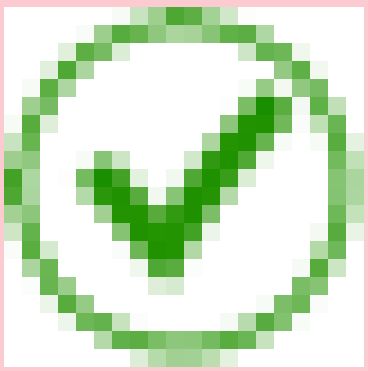
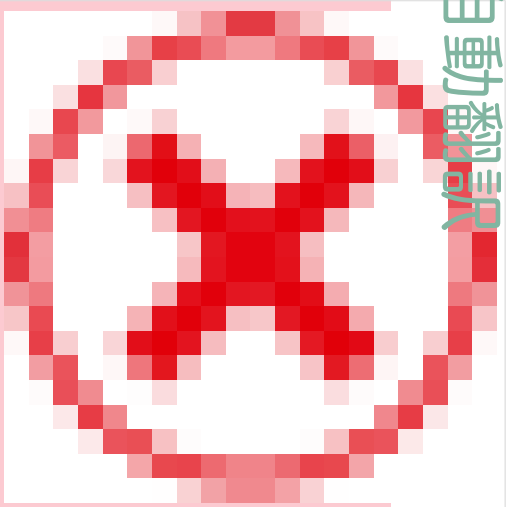
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
廃止				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

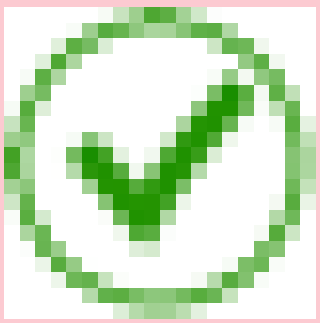
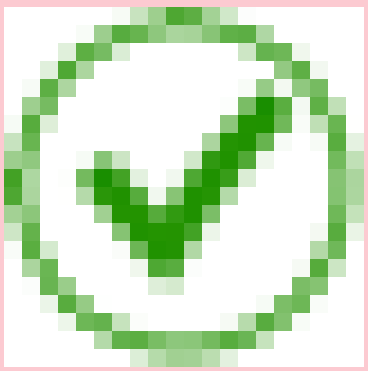
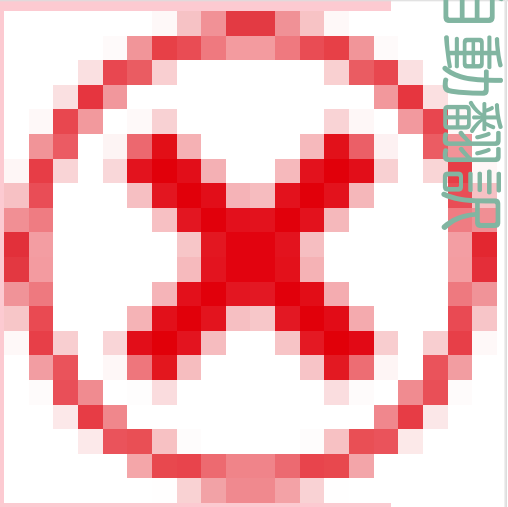
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
複数の保留				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

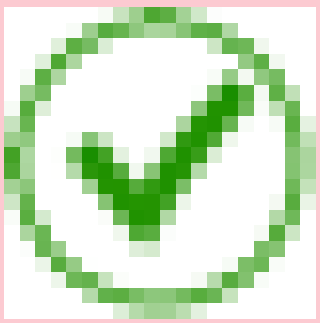
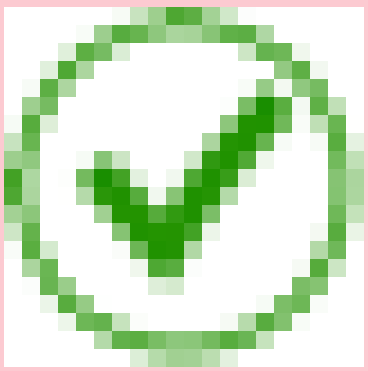
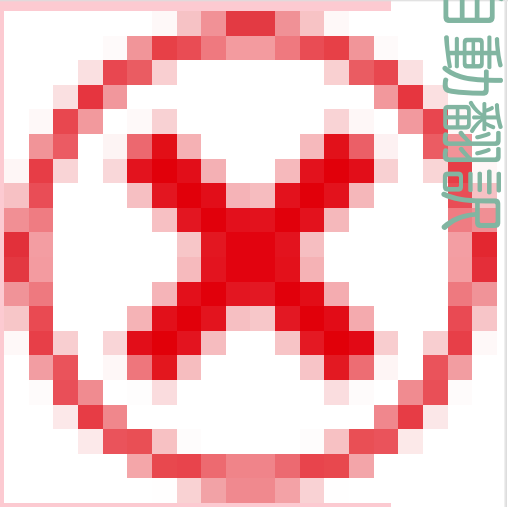
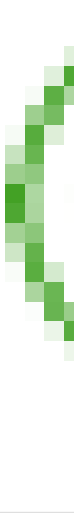
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
すべて				

自動翻訳

ソリューション

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

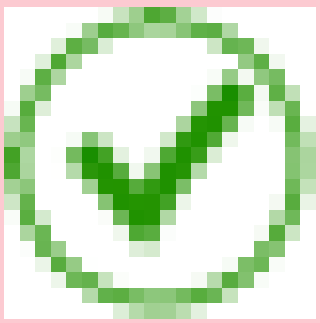
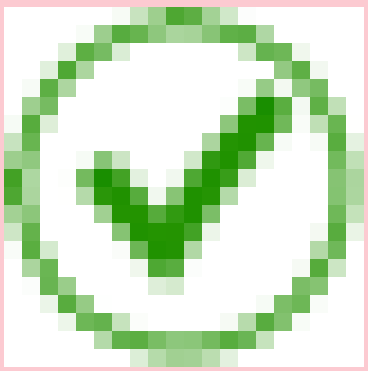
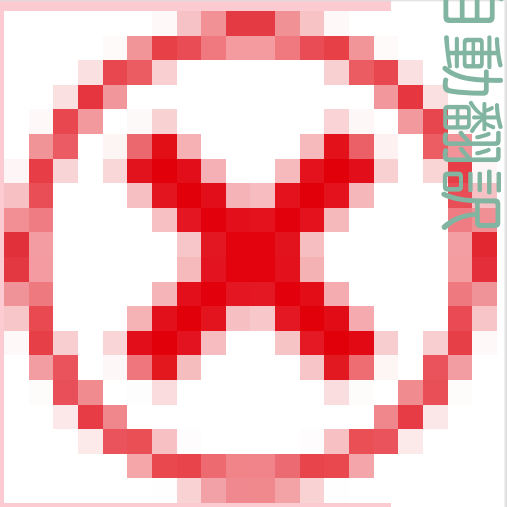
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
すべて				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi

sn_vul.manage_exception_configuration

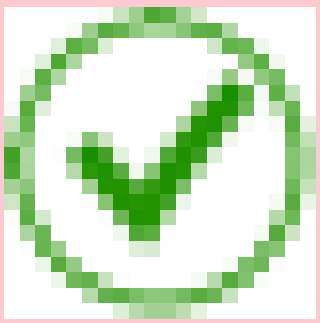
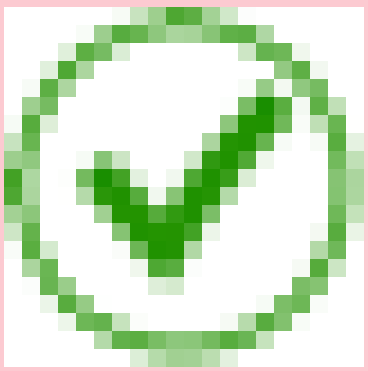
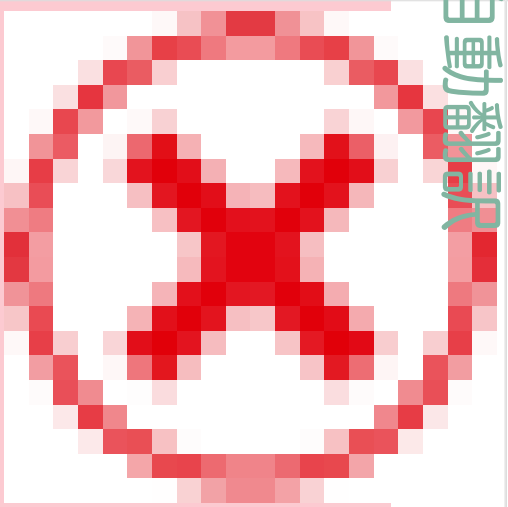
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
最高優先度				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

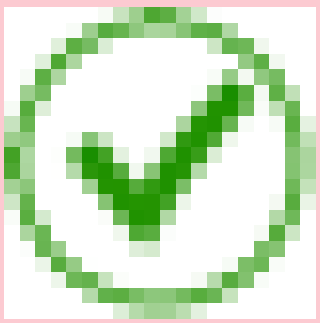
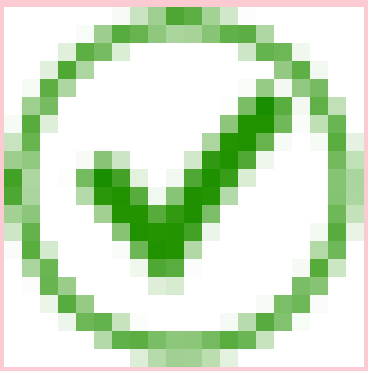
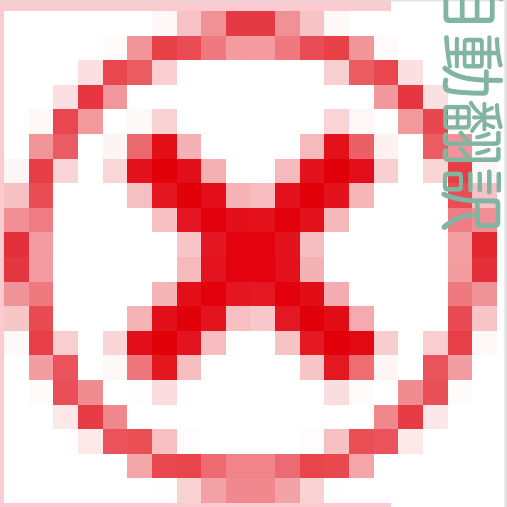
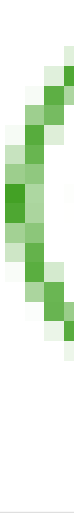
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
脆弱性一致アイテムを使用				

自動翻訳

ライブラリ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

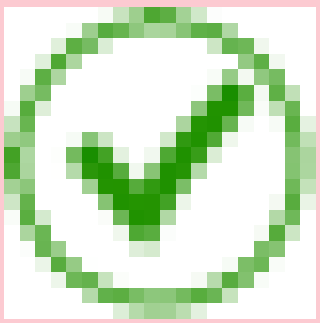
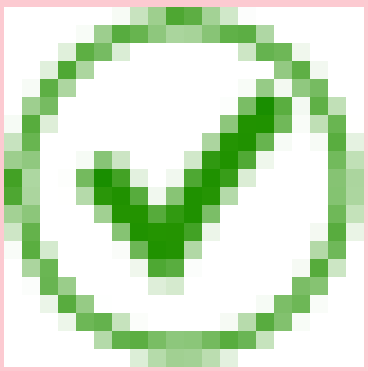
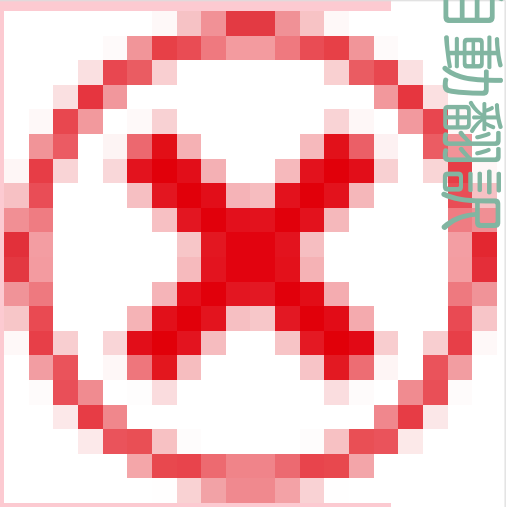
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
NVD				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

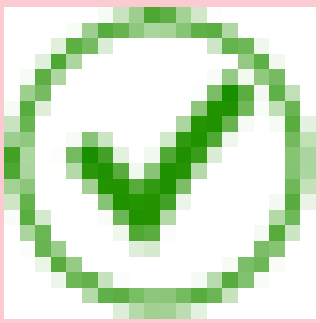
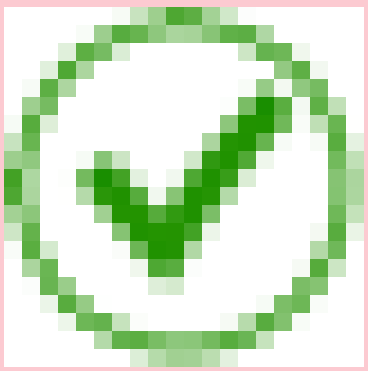
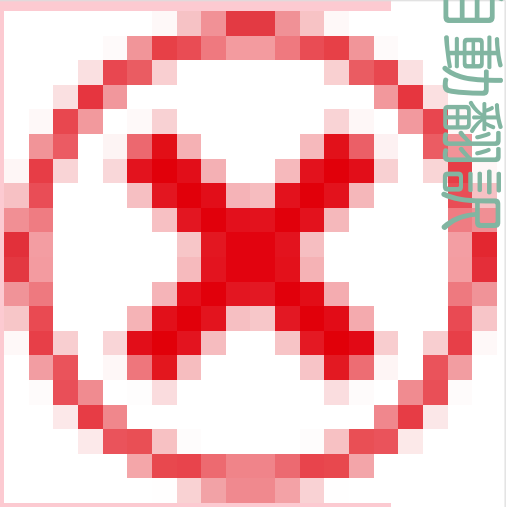
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
CWE				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

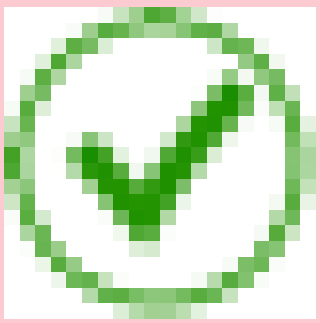
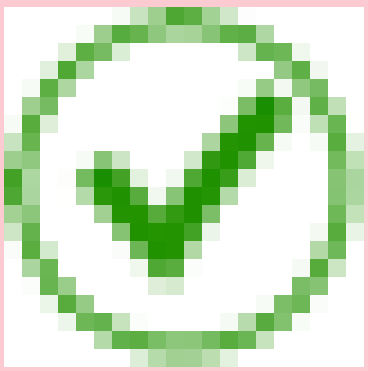
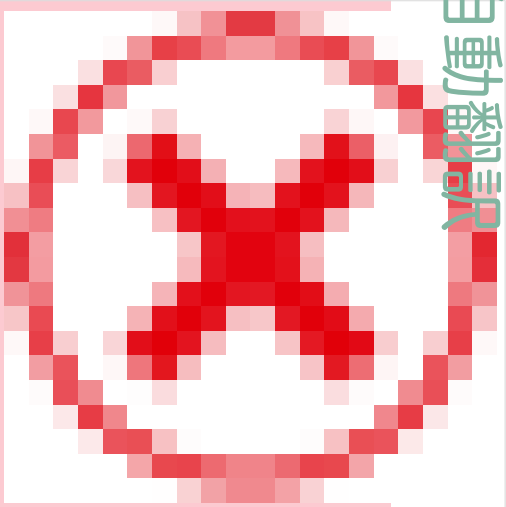
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
サードパーティ				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

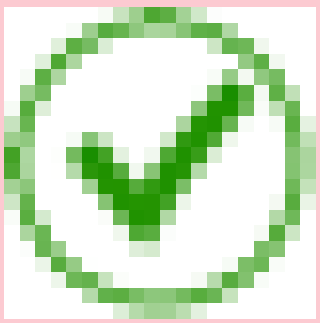
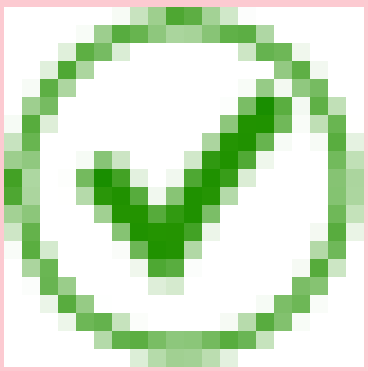
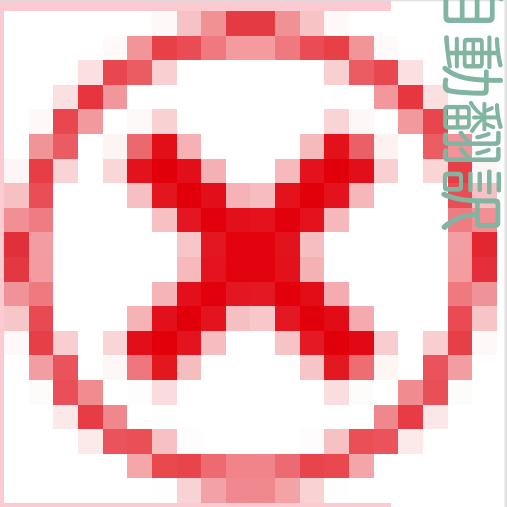
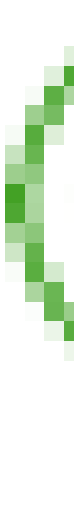
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
脆弱なソフトウェア				

脆弱性スキャン

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

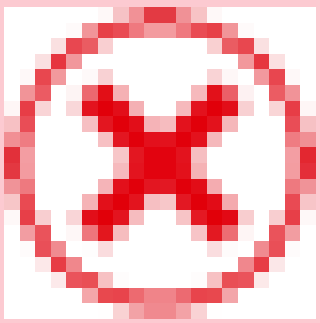
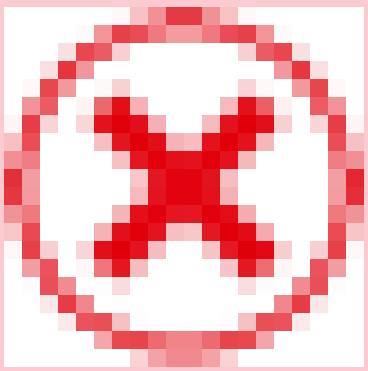
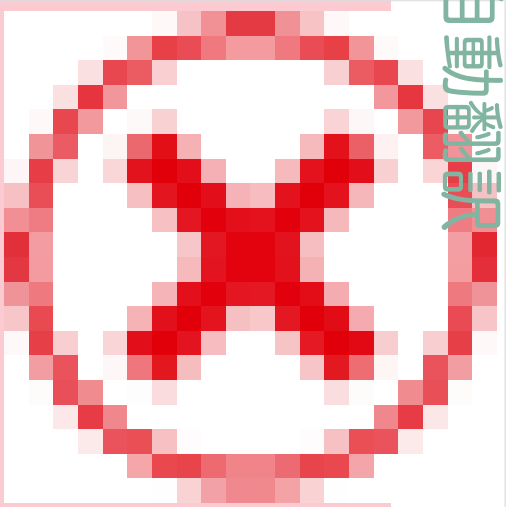
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
エクスポージャーアセスメント				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

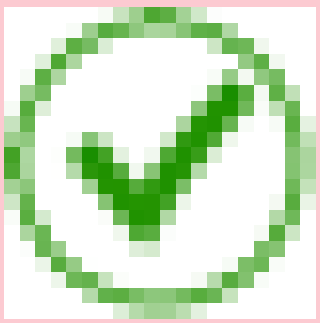
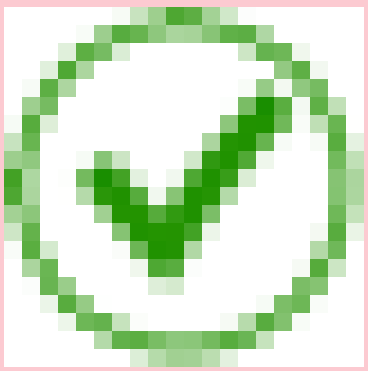
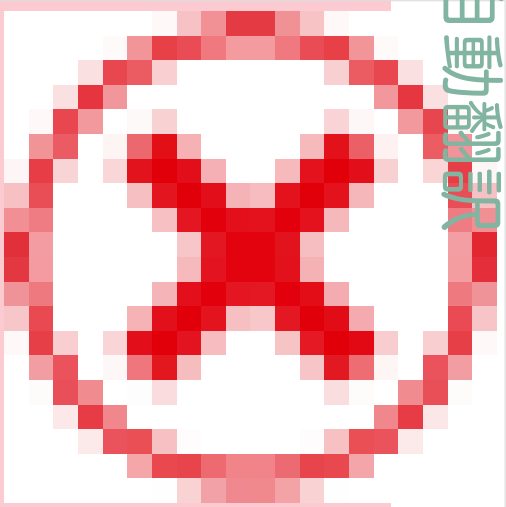
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
スキャン				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

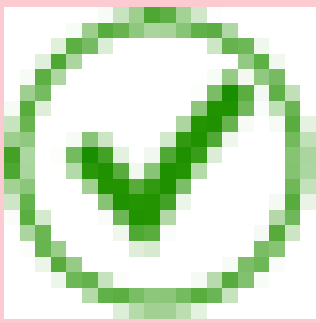
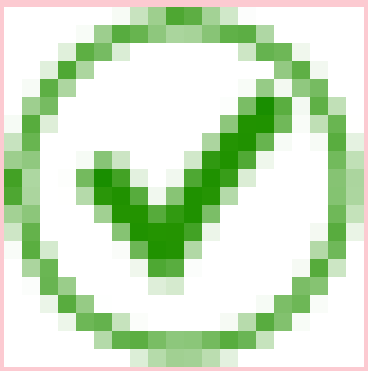
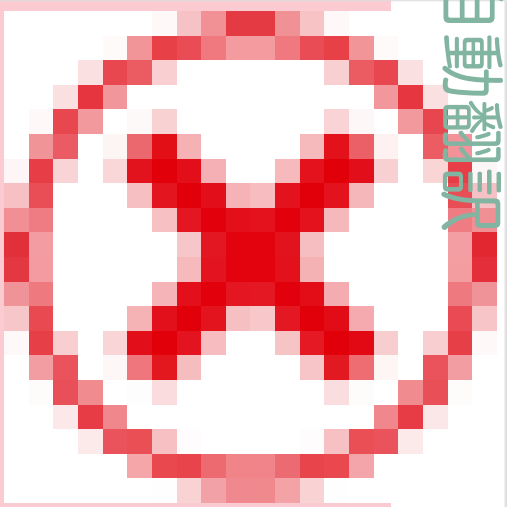
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
スキャナー				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

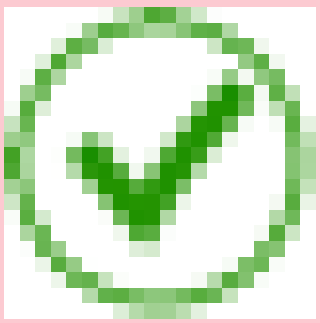
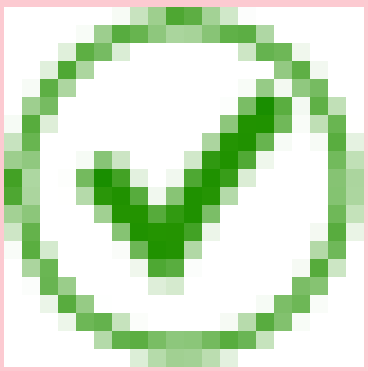
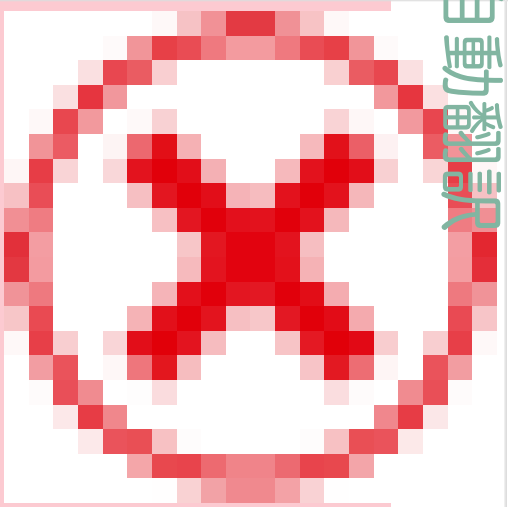
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
スキャンキュー				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

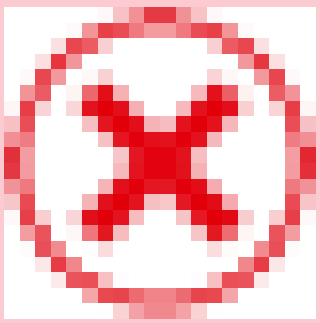
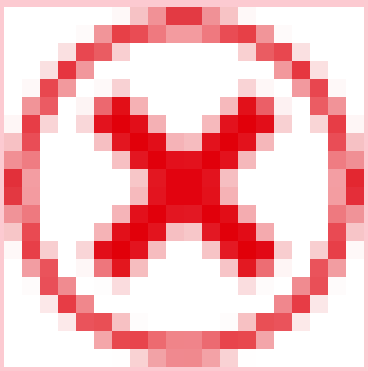
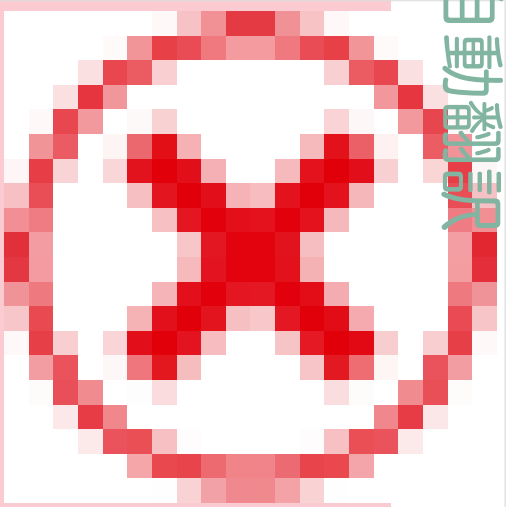
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
スキャナーレート制限				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi

sn_vul.manage_exception_configuration

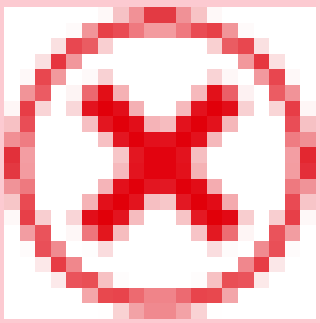
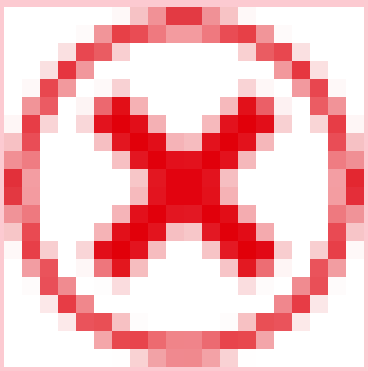
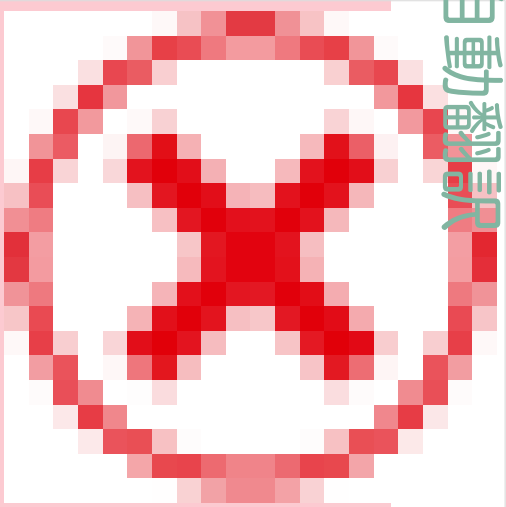
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
レート制限定義				

管理

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

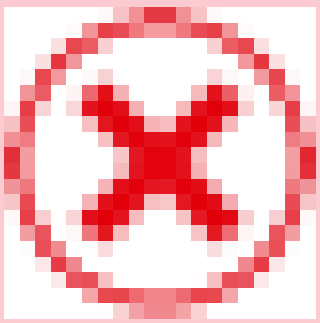
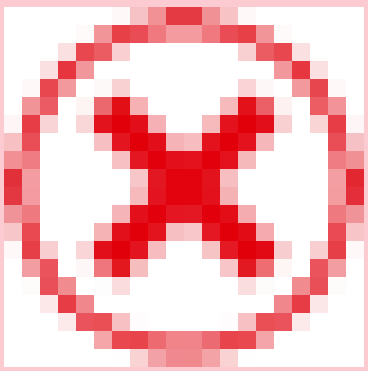
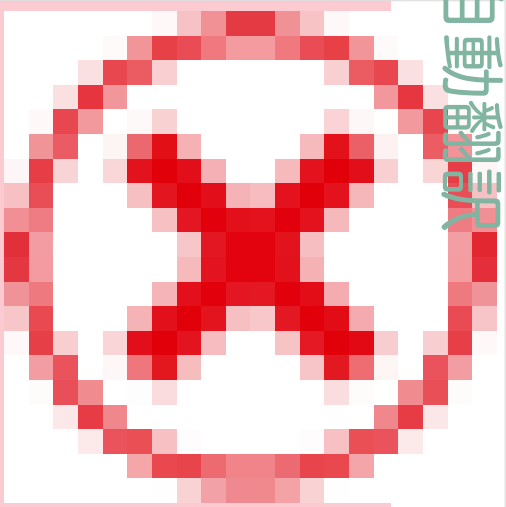
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
セットアップアシスタント				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

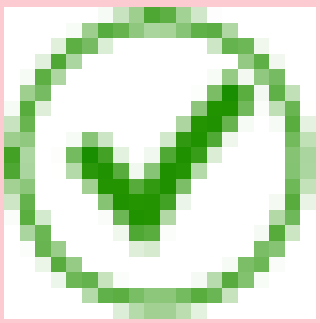
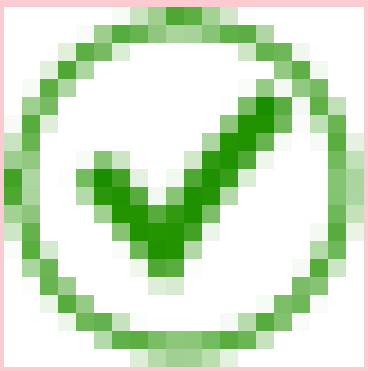
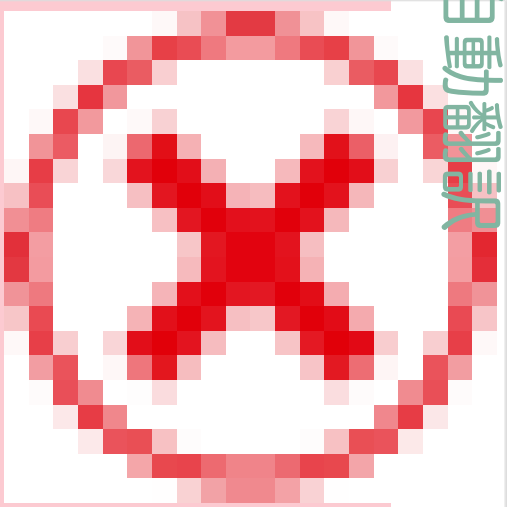
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
監視トピック				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

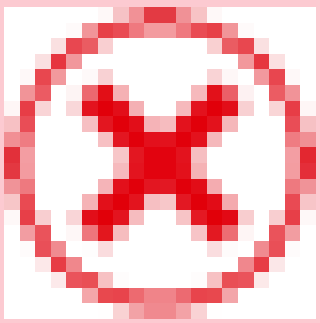
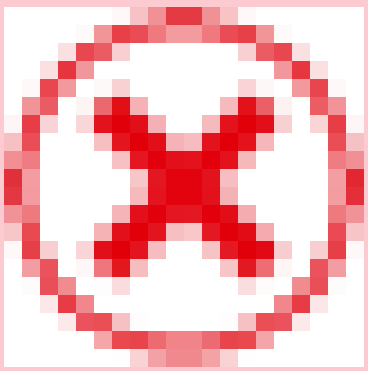
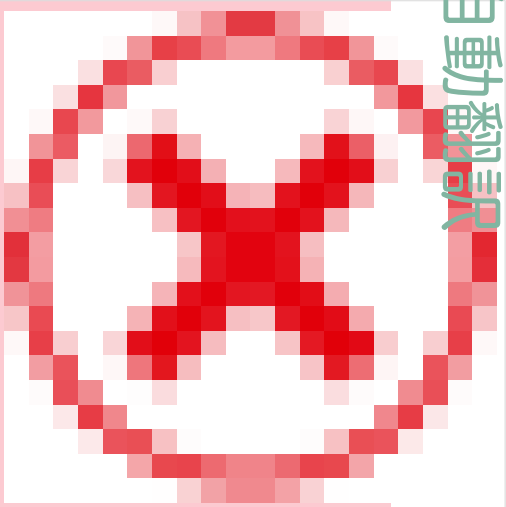
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
アサインルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

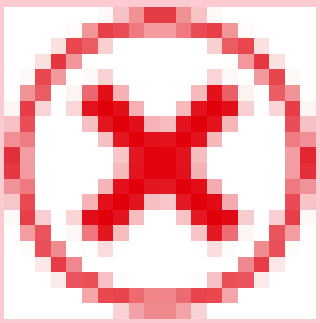
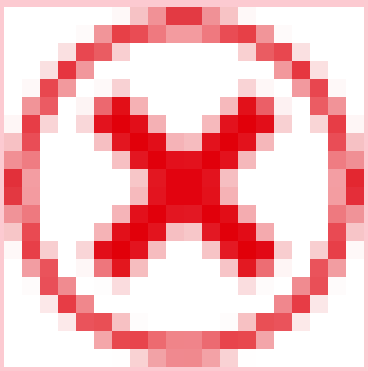
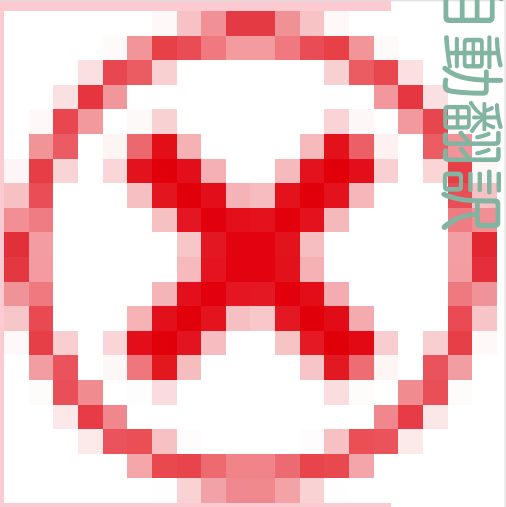
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
修復タスクルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

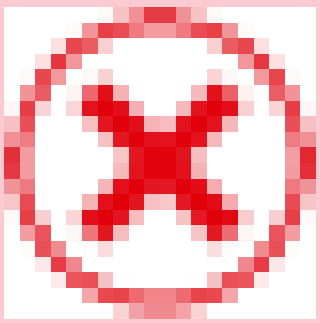
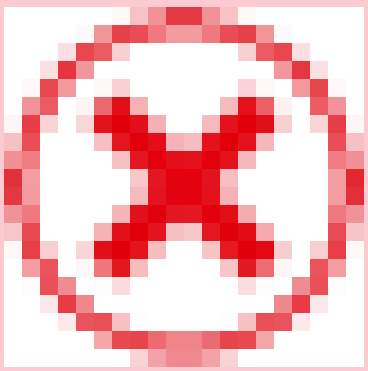
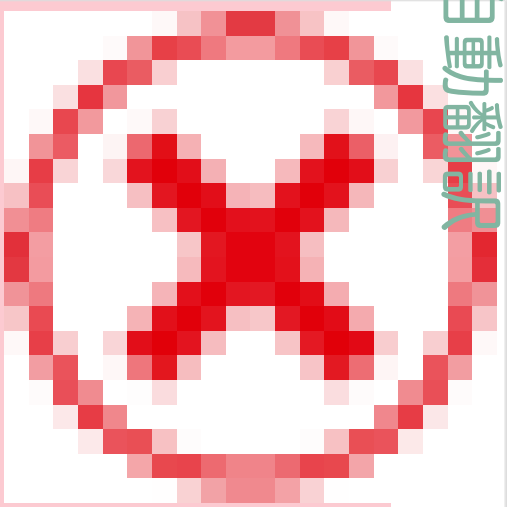
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
アサインの推奨				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

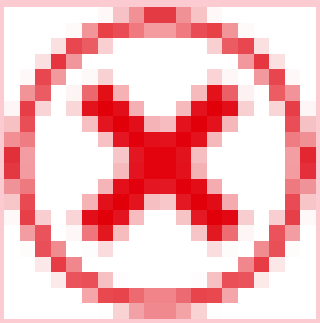
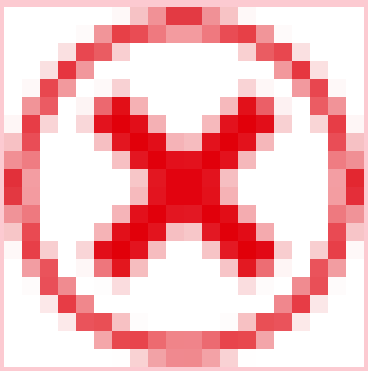
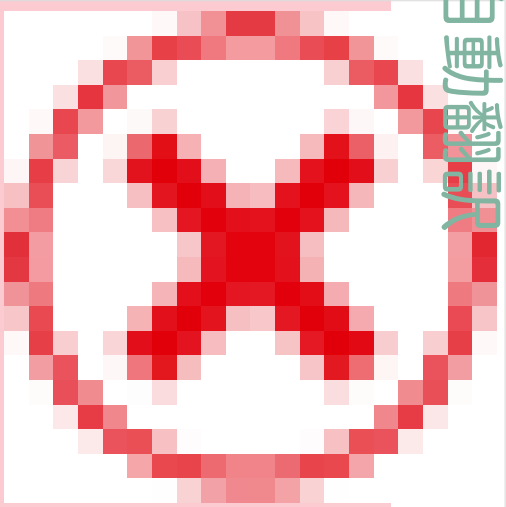
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
脆弱性算出				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

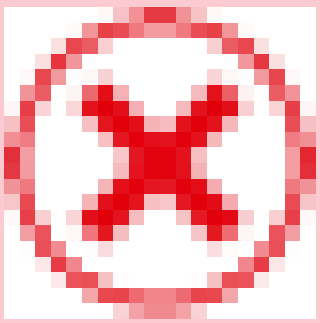
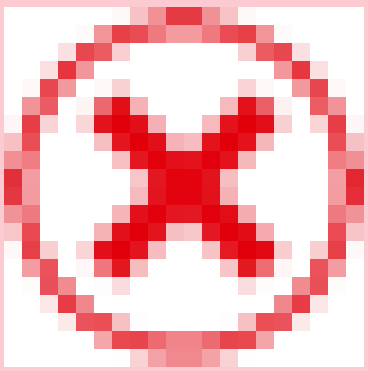
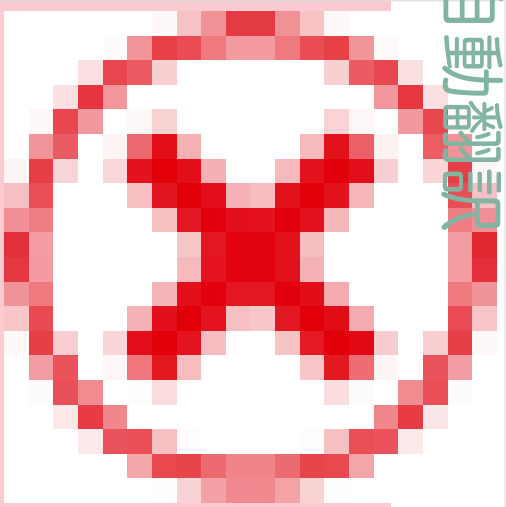
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
脆弱性ロールアップ算出				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

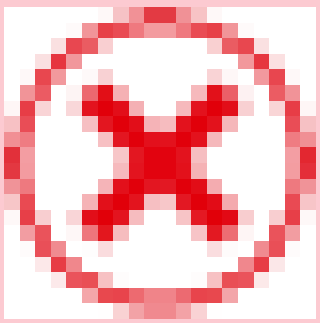
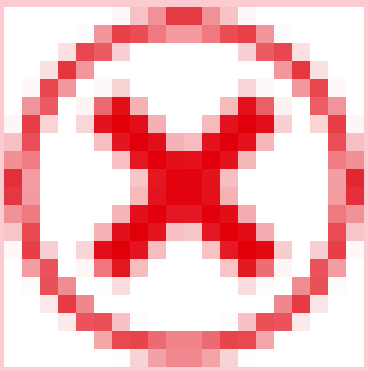
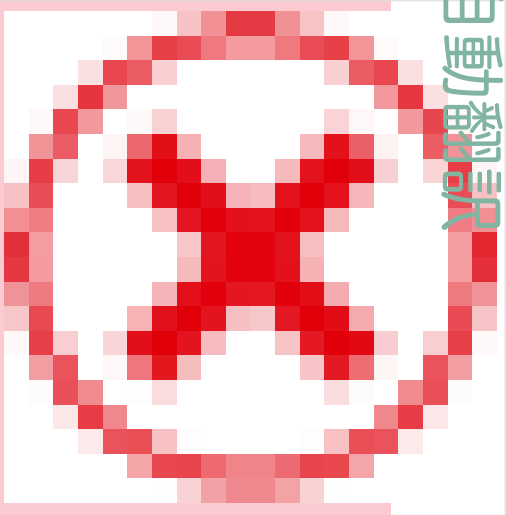
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
修復ターゲットルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

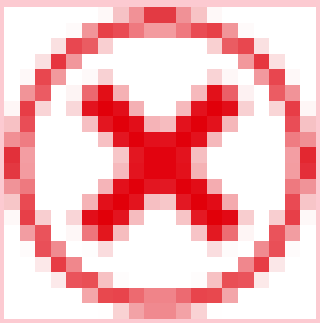
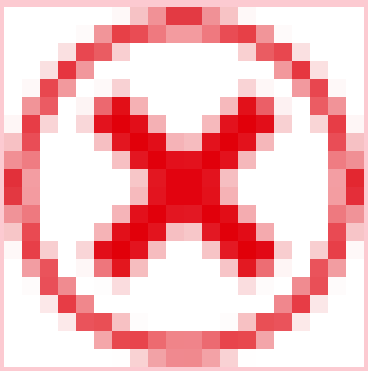
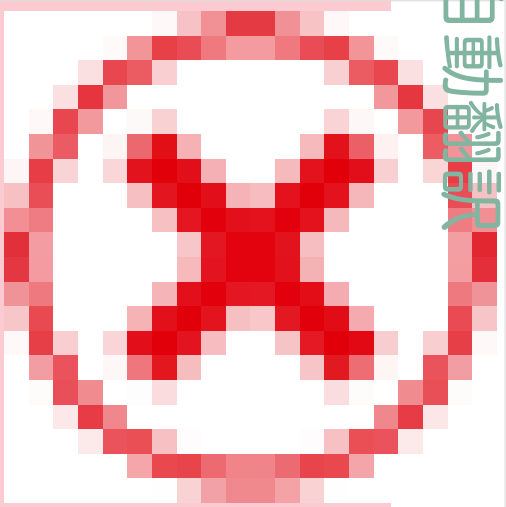
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
自動クローズ構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

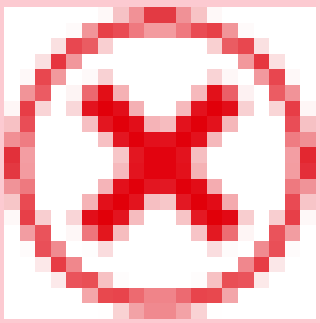
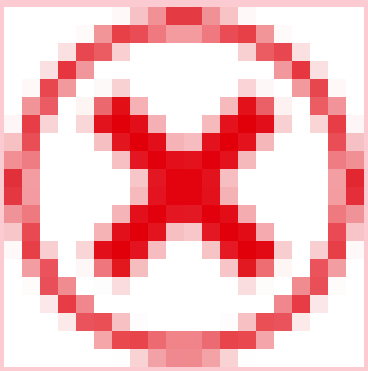
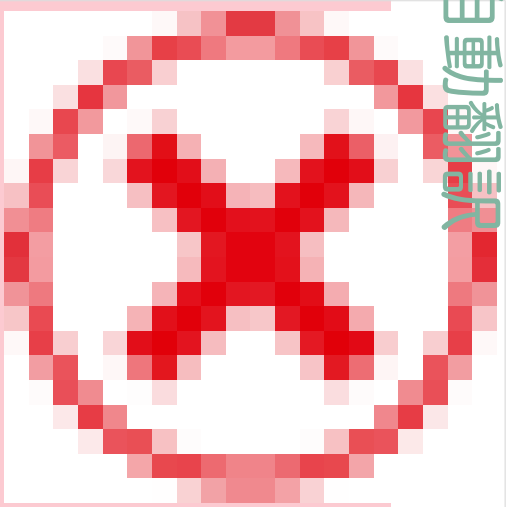
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
ルールの自動削除				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

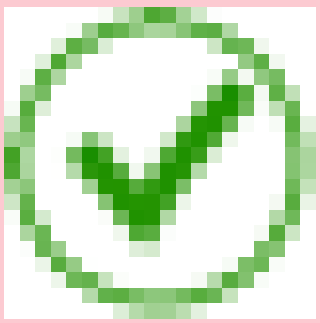
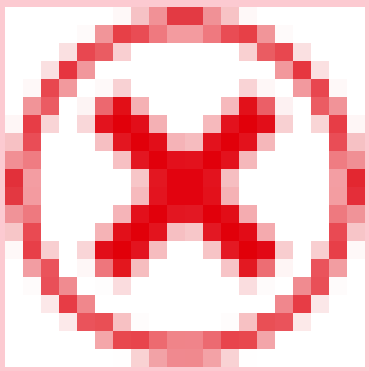
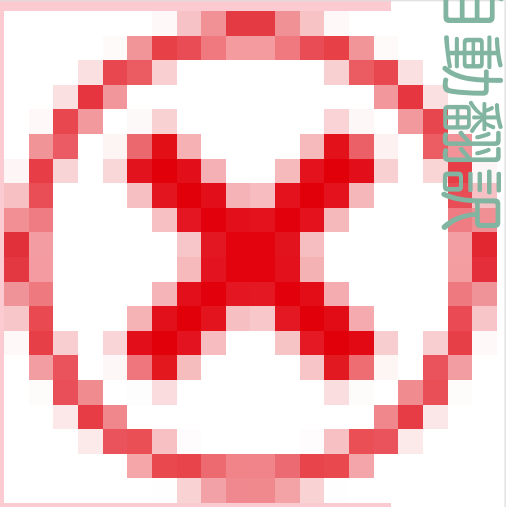
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
例外ルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

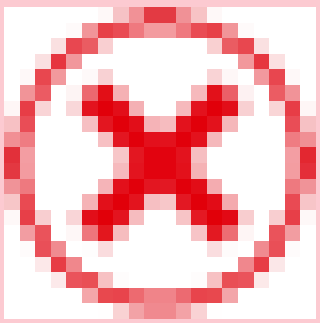
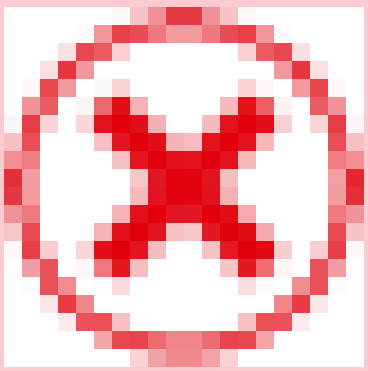
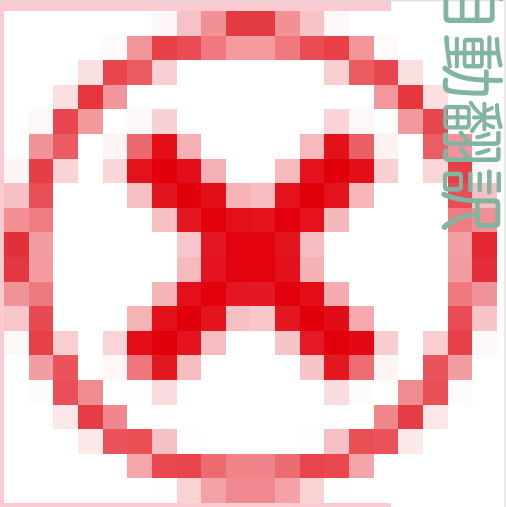
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
承認ルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

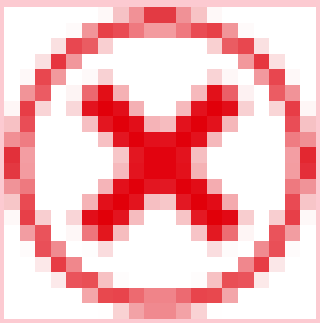
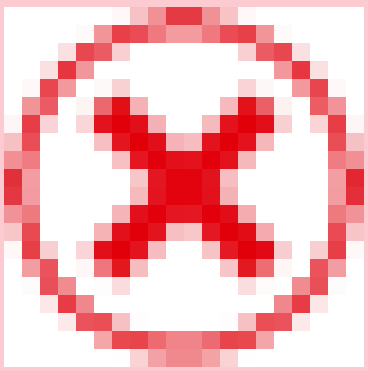
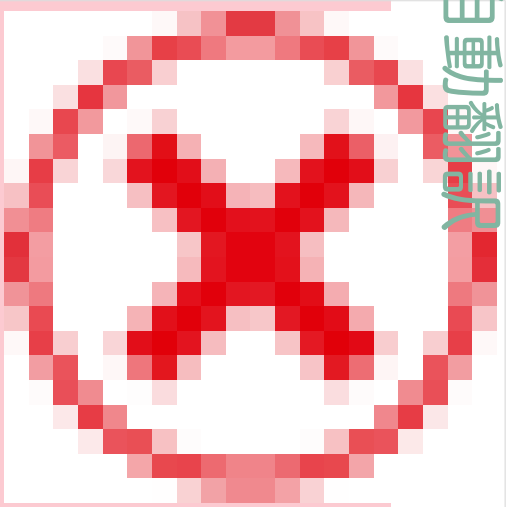
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
分類ルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

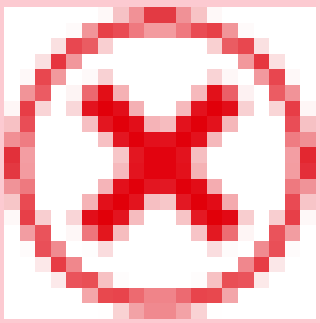
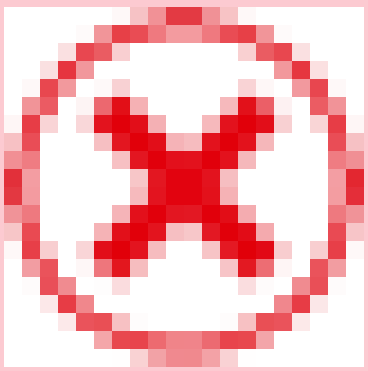
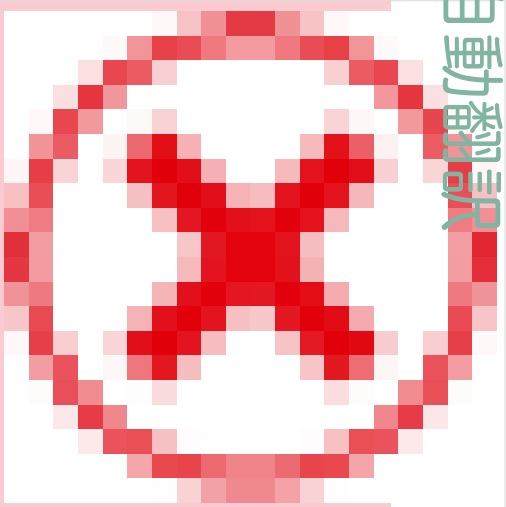
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
パフォーマンス構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

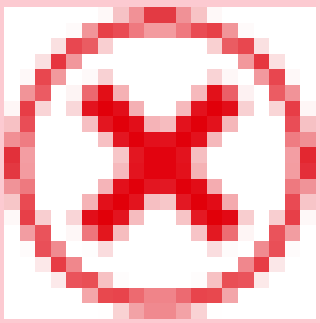
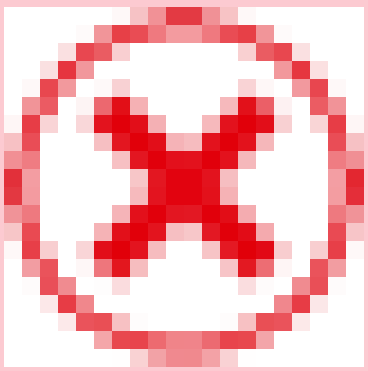
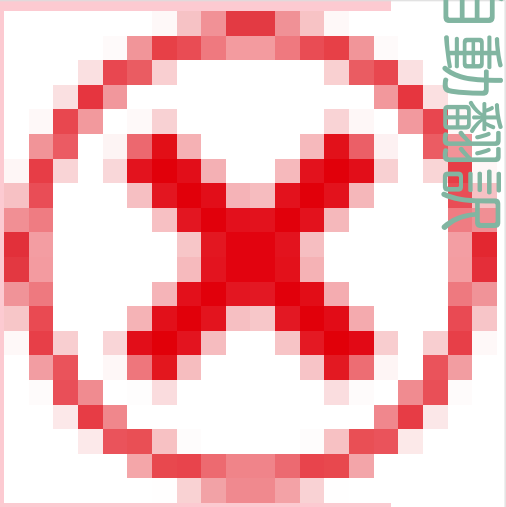
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
VI の粒度の構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

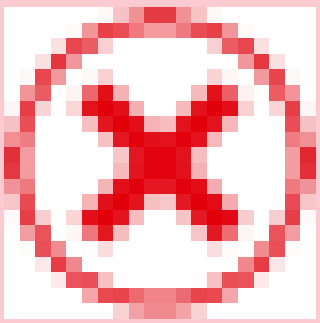
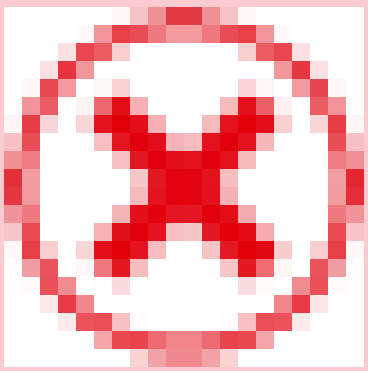
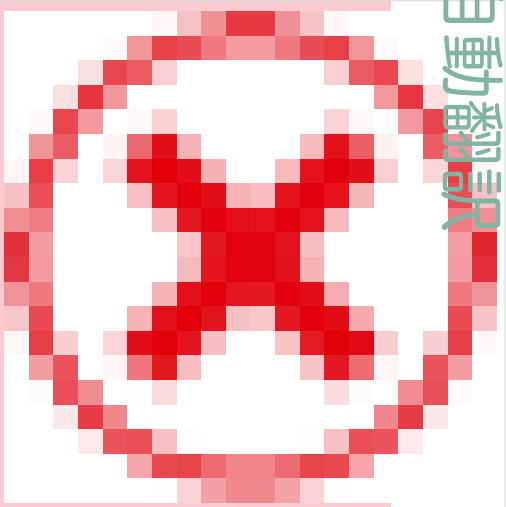
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
通知				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

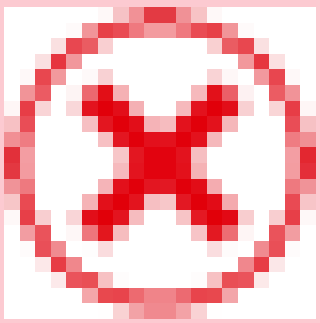
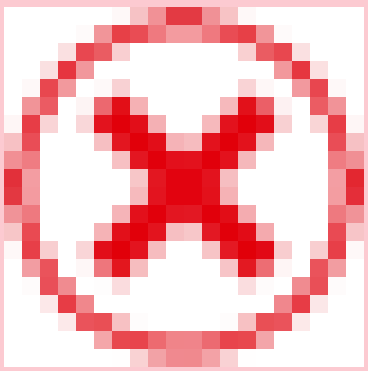
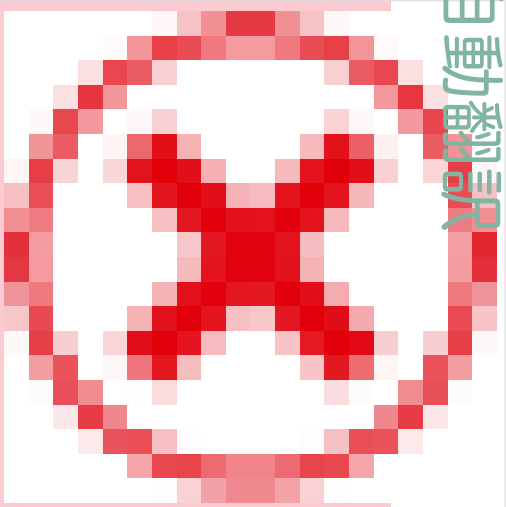
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
メールテンプレート				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

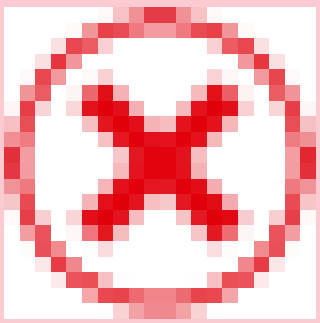
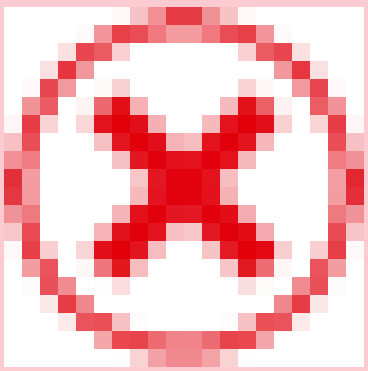
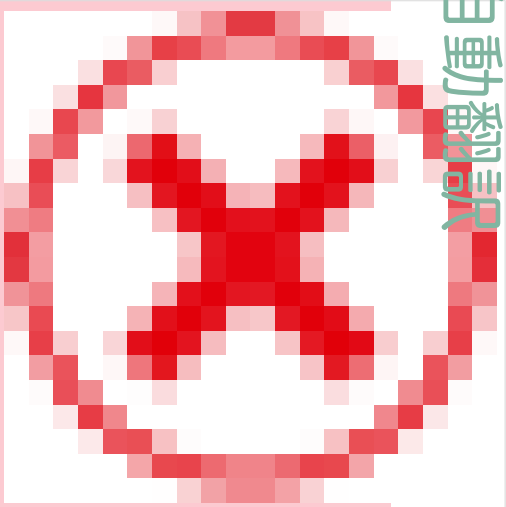
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
キューをインポート				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

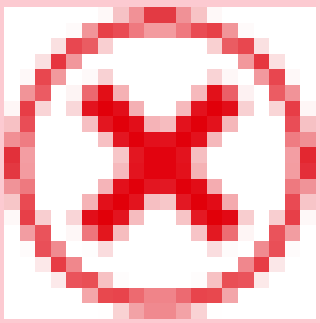
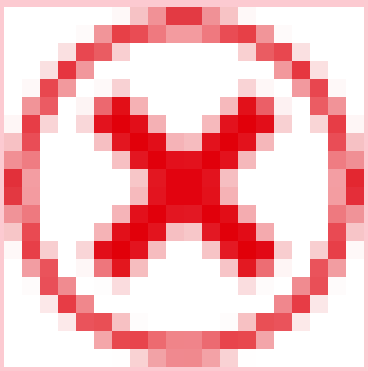
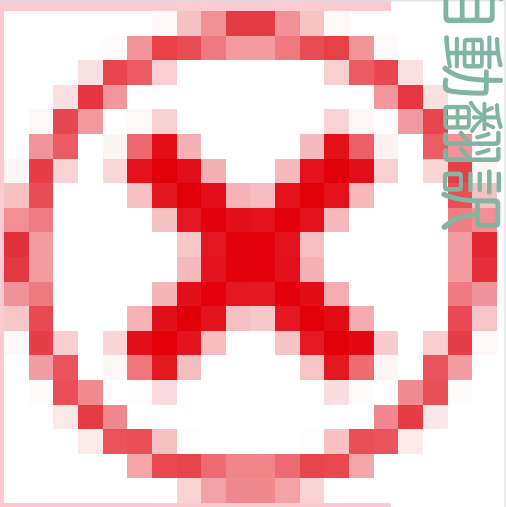
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
統合				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

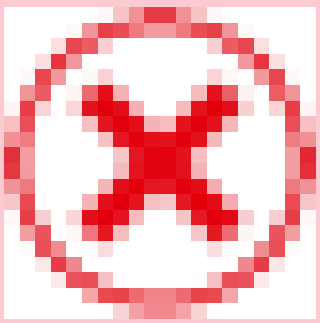
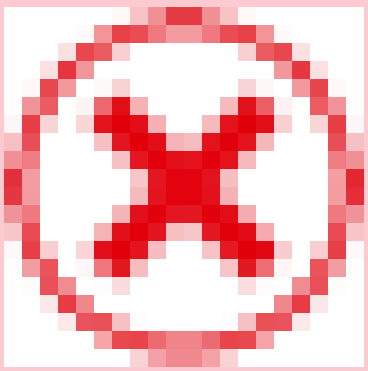
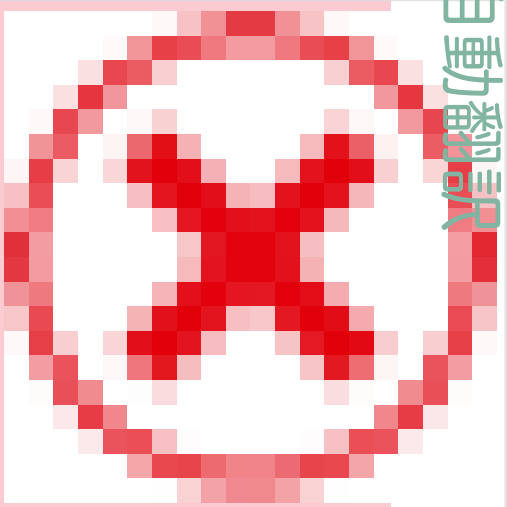
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
SLA 定義				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

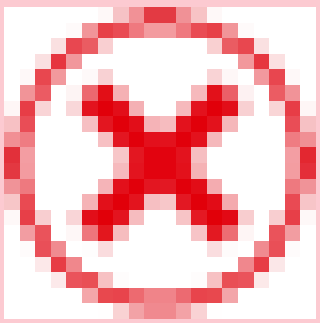
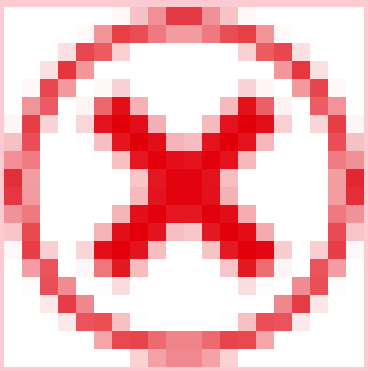
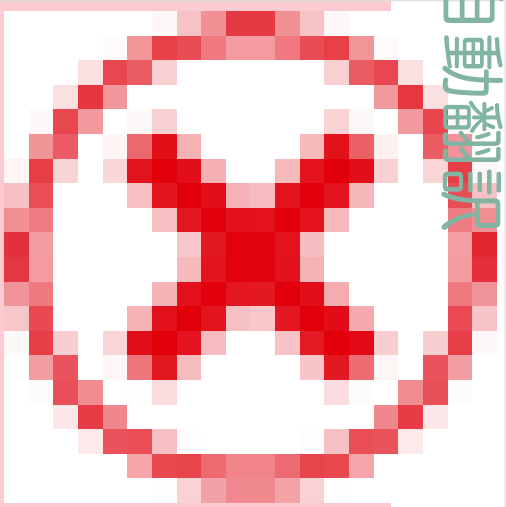
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
SAM NVD の構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

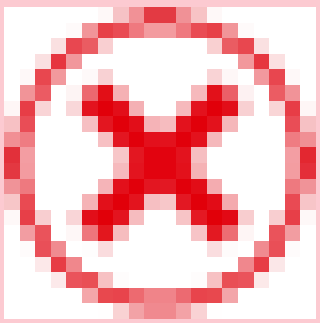
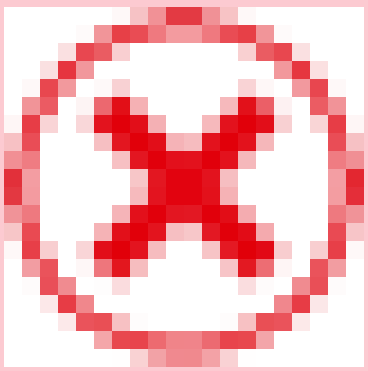
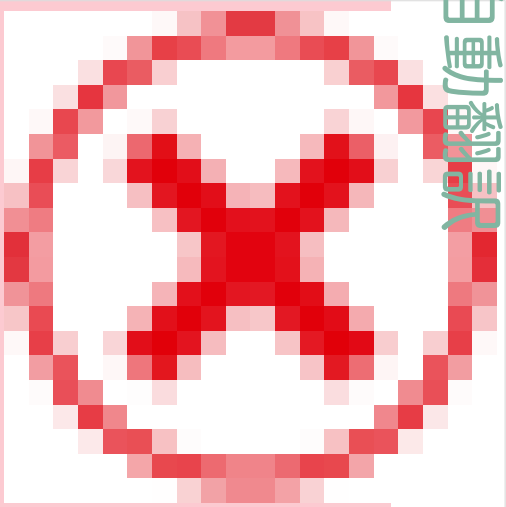
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
正規化された重大度マップ				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

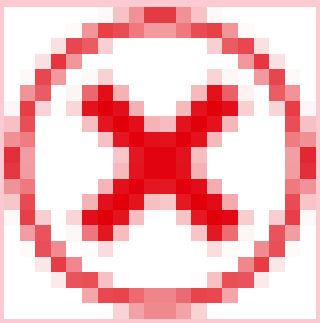
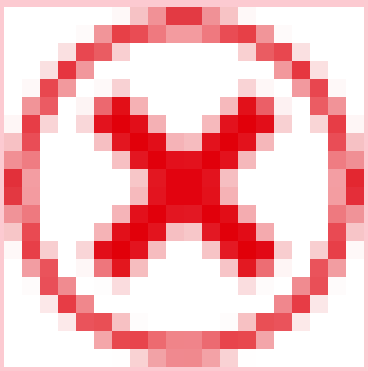
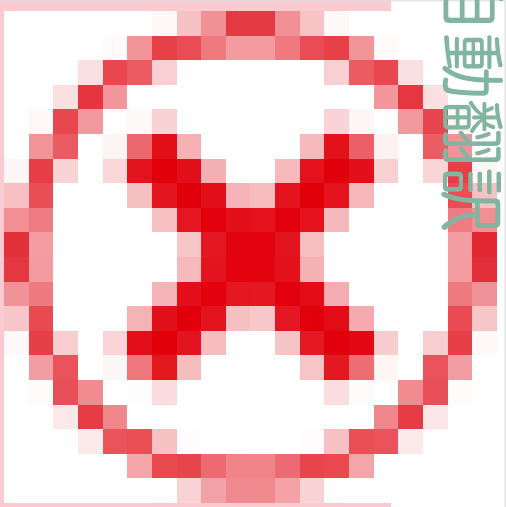
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
スキャン範囲構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

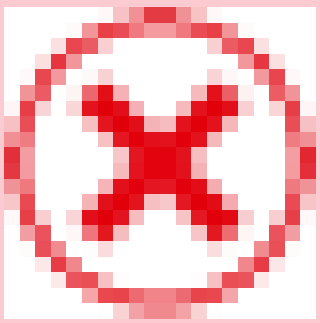
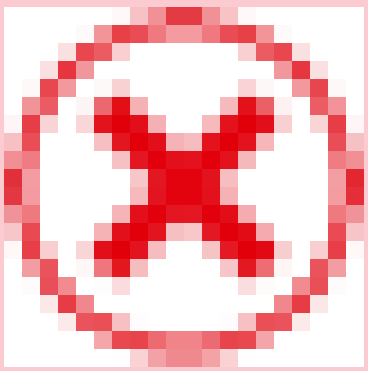
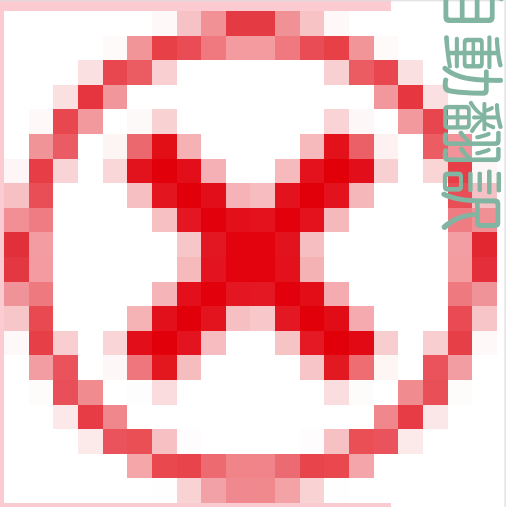
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
例外管理				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

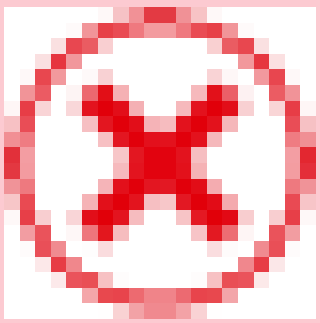
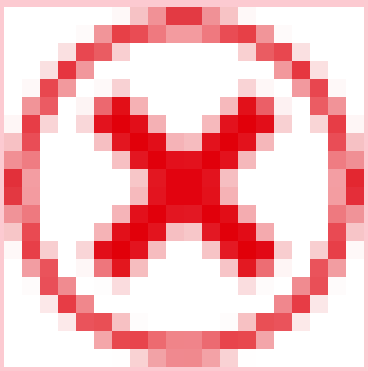
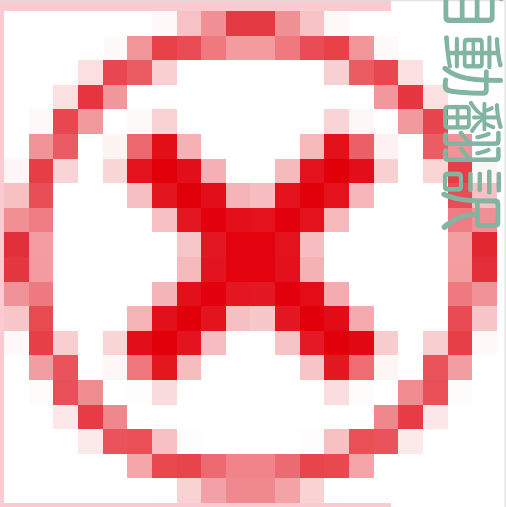
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
使用状況レポート				

自動翻訳

診断

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignment_rules

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	sn_vu
チェック	✗	✗	✗	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classificati
sn_vul.manage_exception_configuration

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、
sn_vul.manage_exception_configuration

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

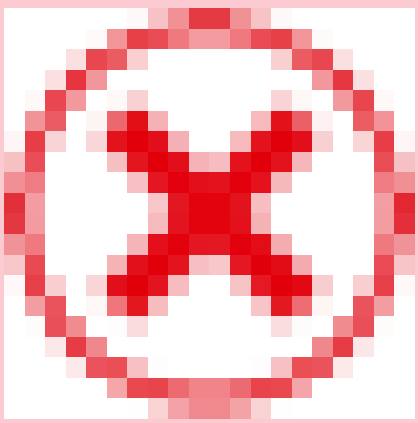
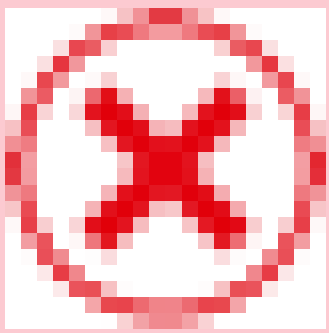
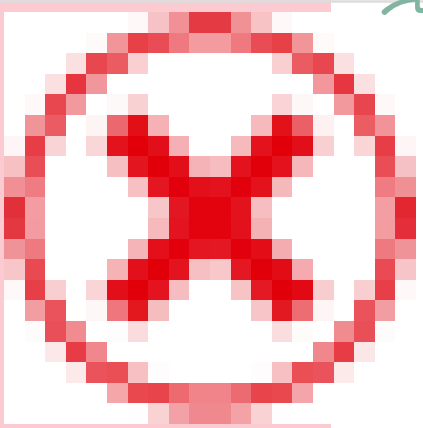
sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rul	sn_vul.r
(メインアプリグループ)				
CISO ダッシュボード				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

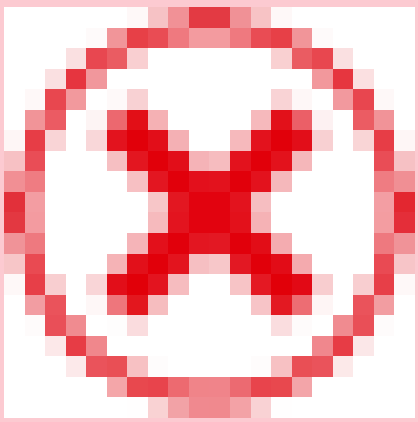
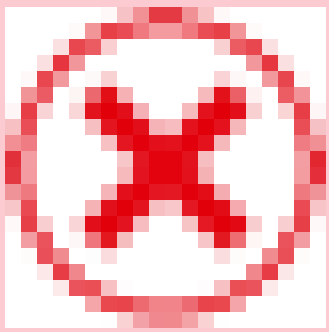
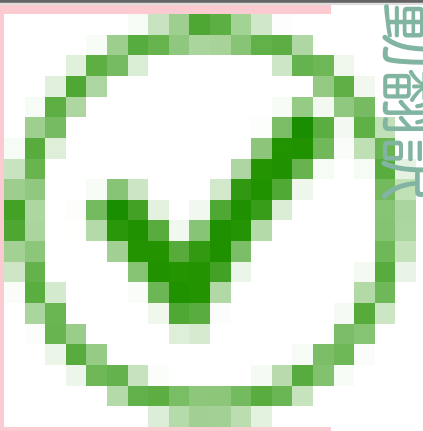
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
修復の概要				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

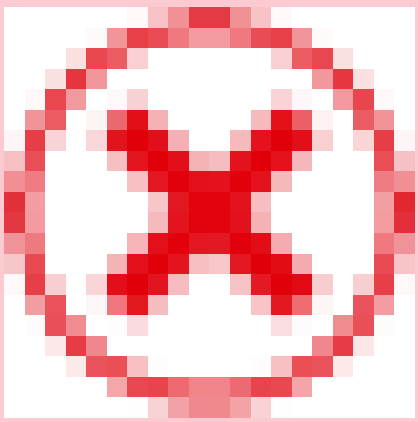
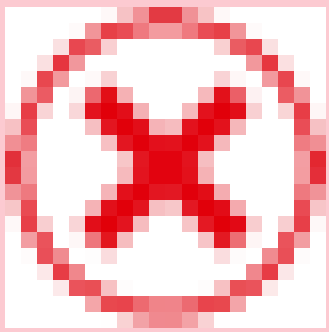
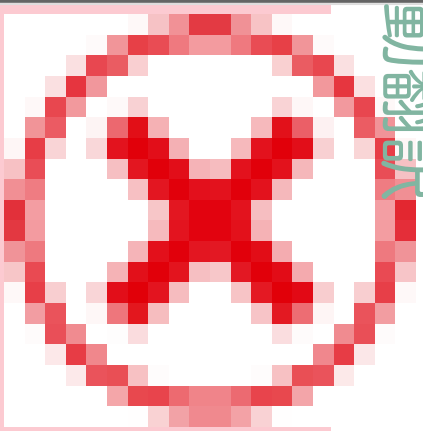
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
脆弱性マネージャーのワークスペース				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

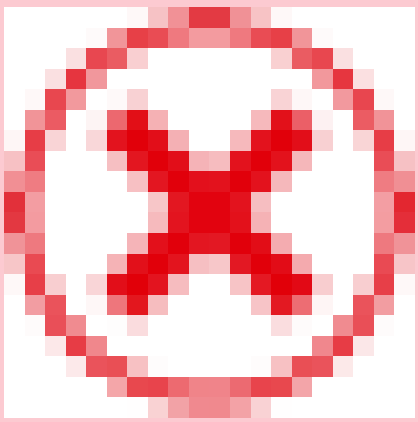
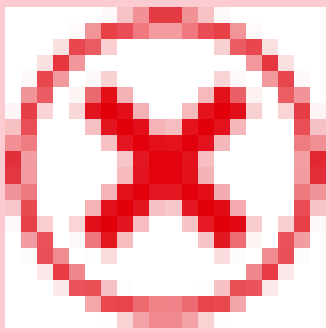
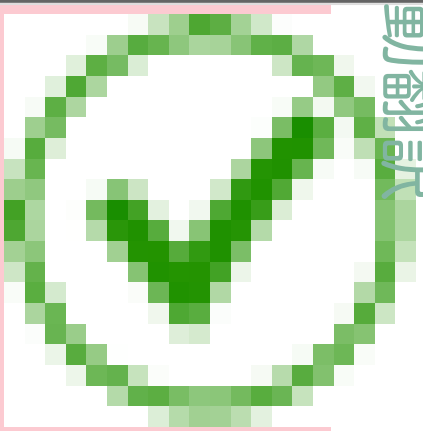
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
概要				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

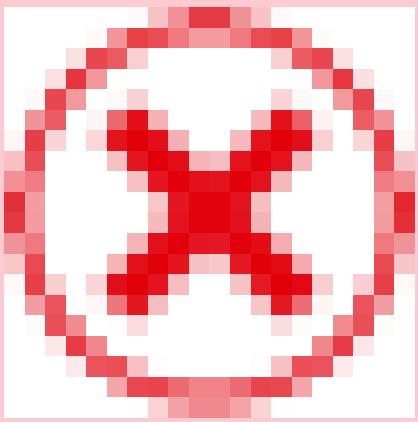
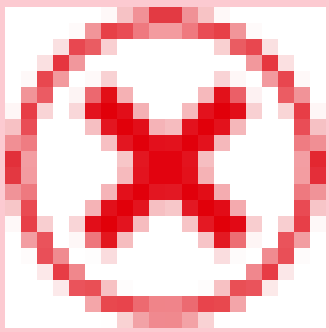
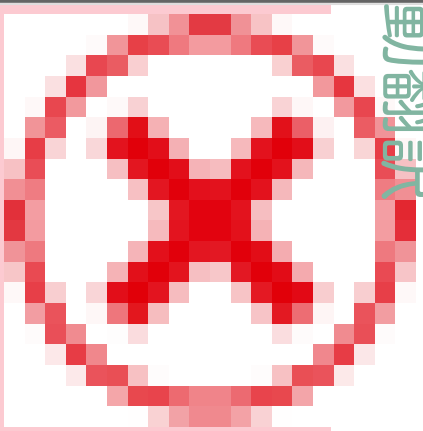
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
IT 修復ワークスペース				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

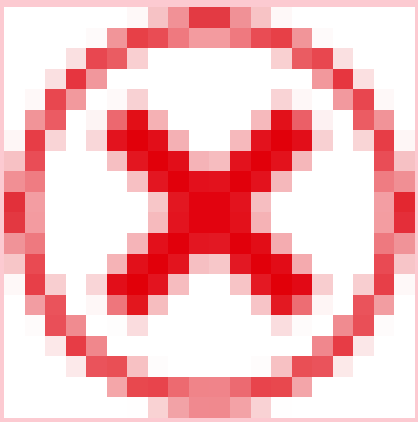
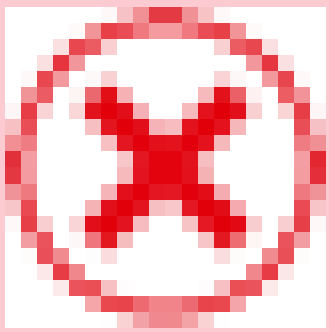
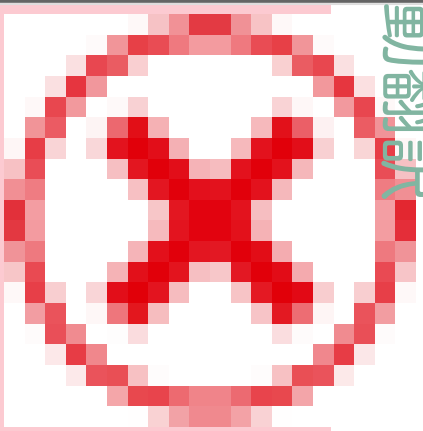
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
承認者の概要				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

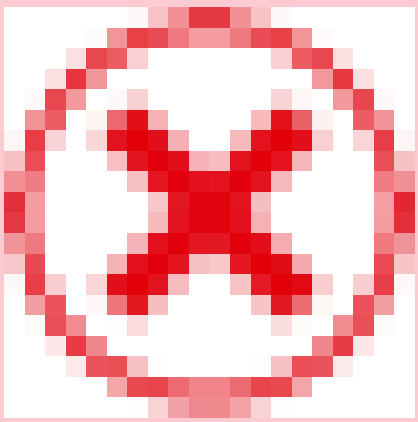
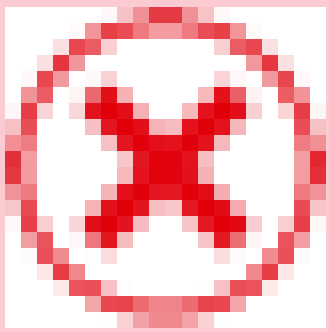
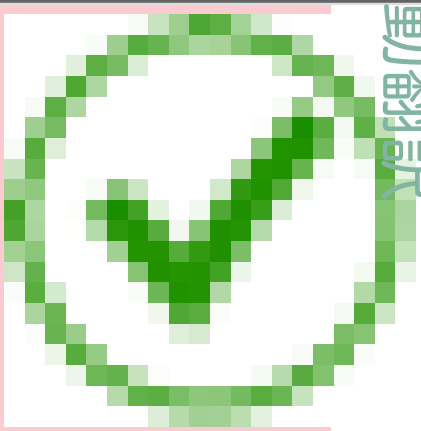
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
概要				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

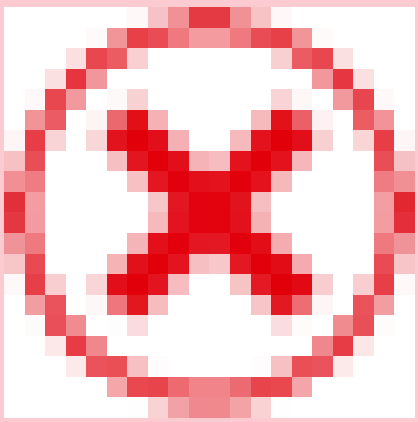
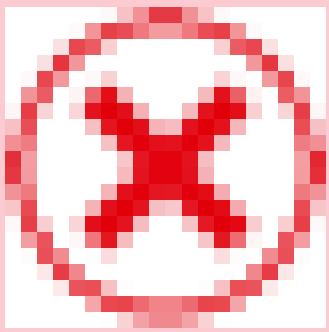
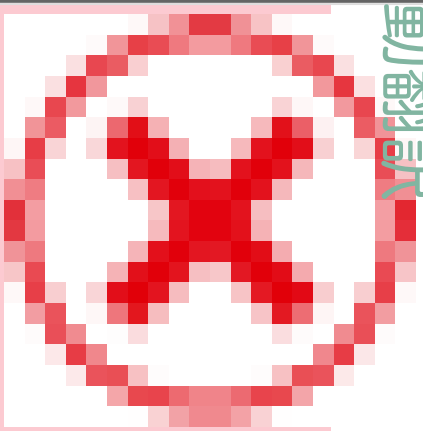
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
自分の承認				

修復タスク

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

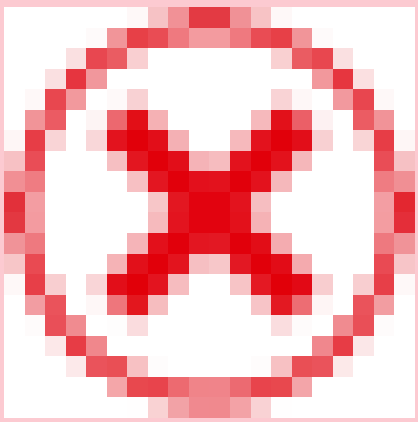
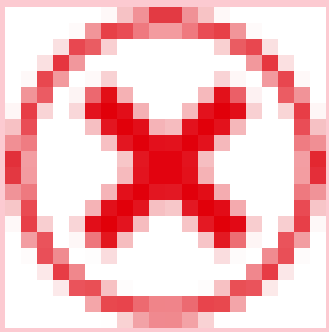
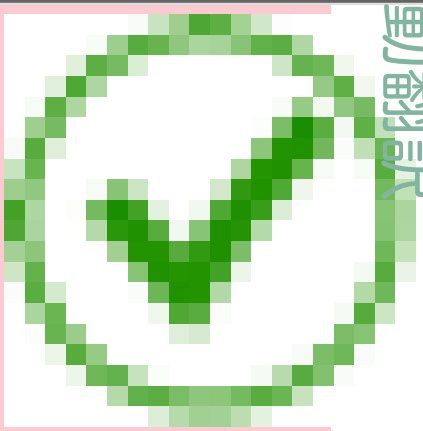
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
有効				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

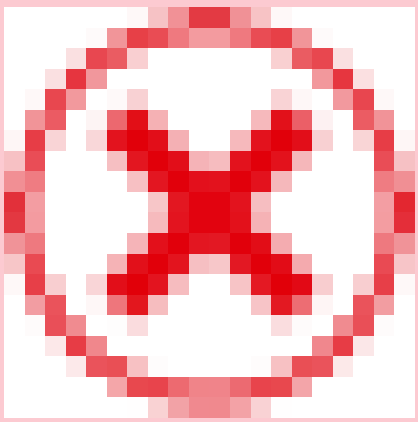
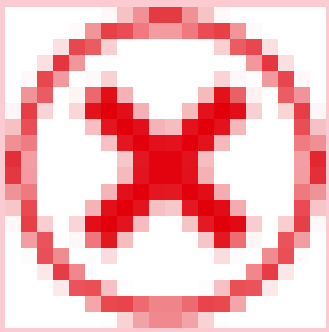
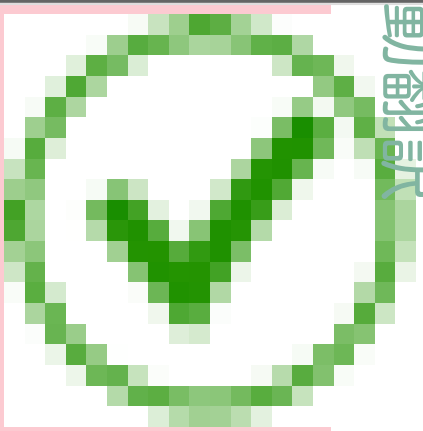
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
自分にアサイン済み				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

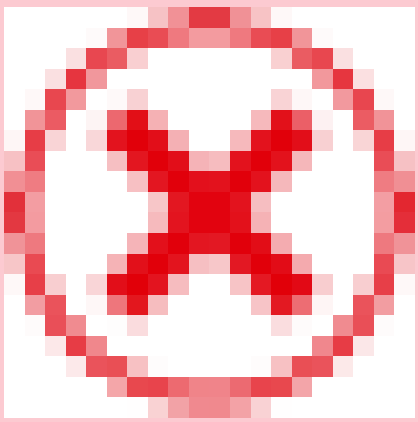
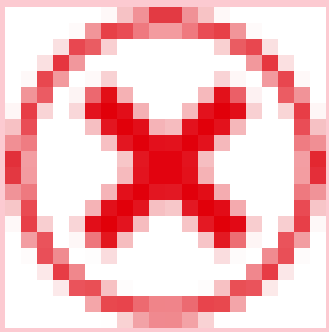
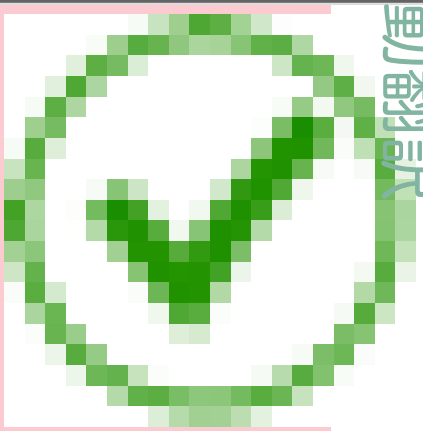
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
所属グループにアサイン済み				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

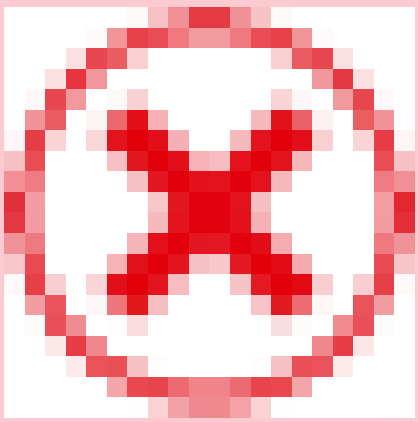
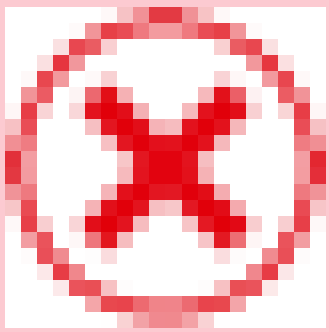
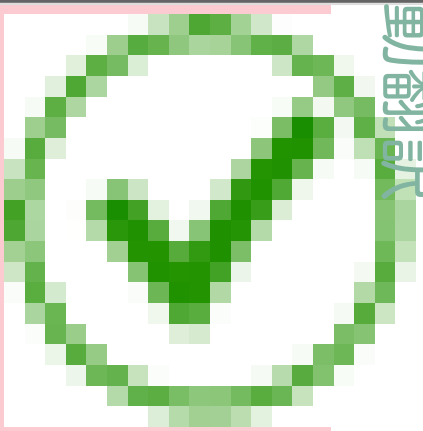
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
すべて				

脆弱性一致アイテム

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

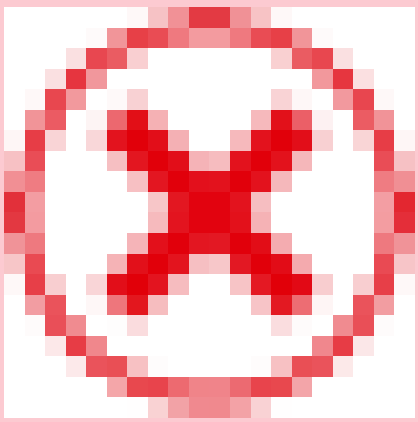
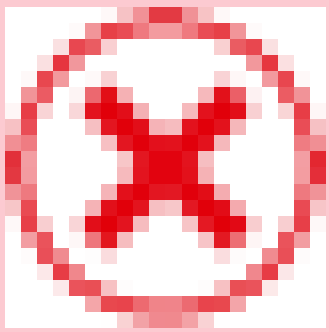
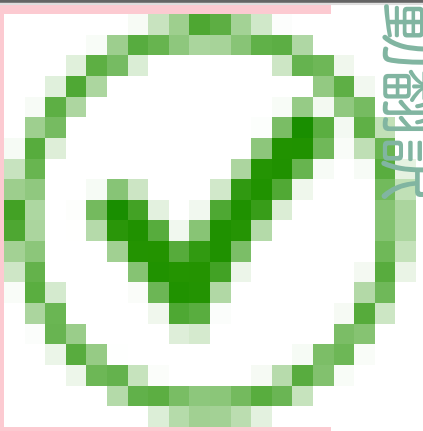
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
重大なリスク				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

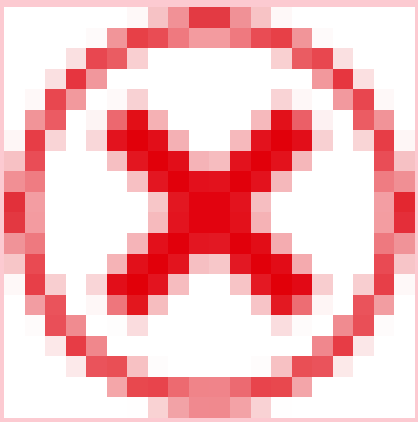
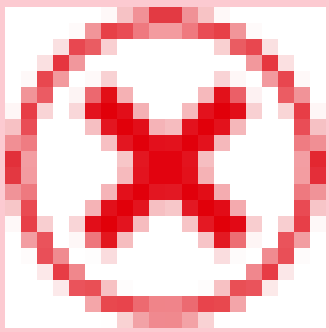
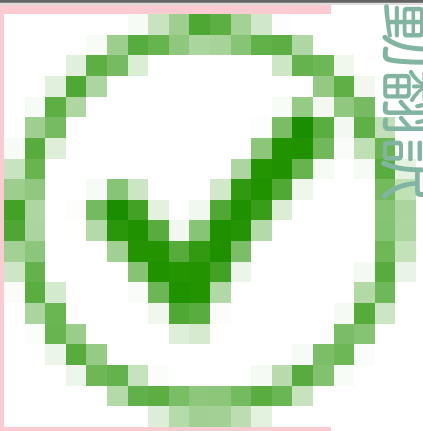
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
高リスク				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

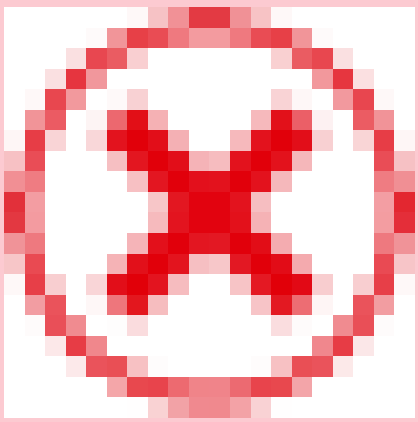
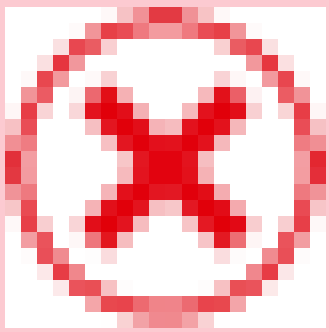
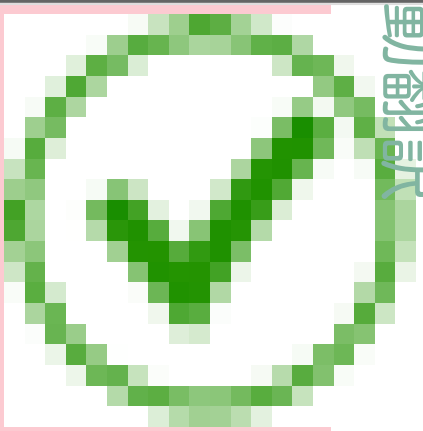
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
エクスプロイト可能				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
該当 CI 確認中	✗	✗	✓	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
CI 不明	✗	✗	✓	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

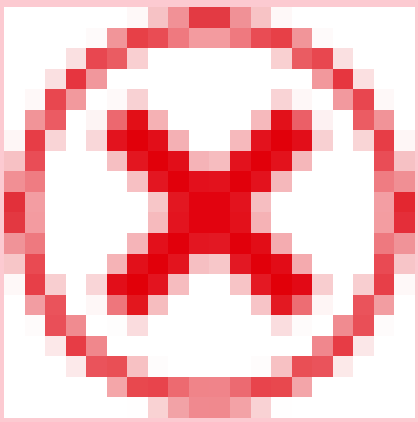
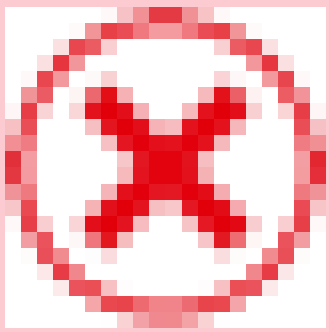
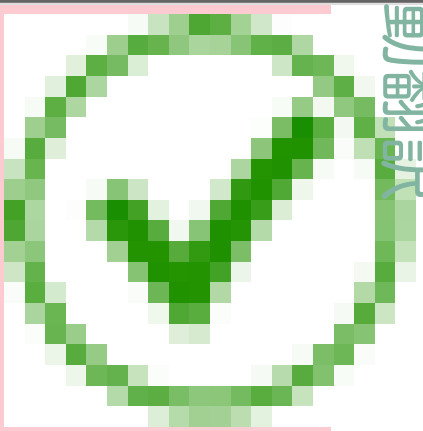
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
過去 90 日以内				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

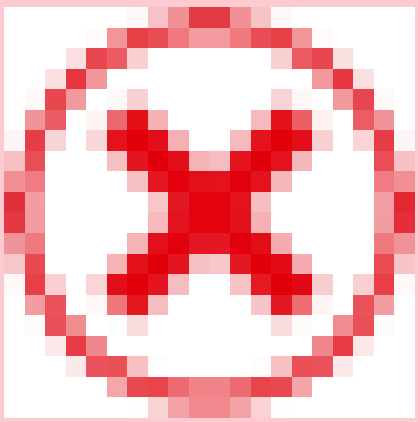
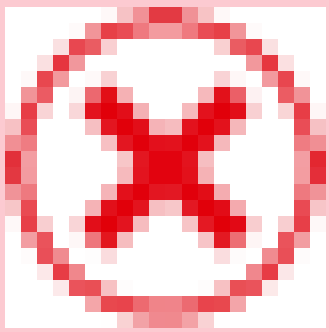
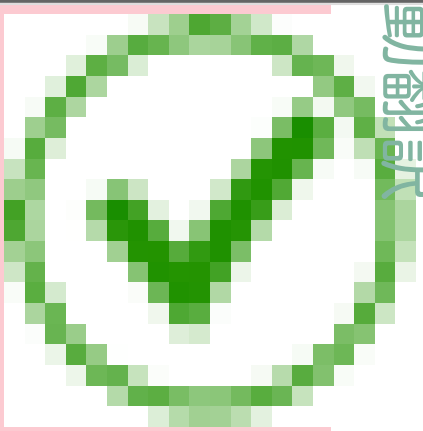
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
91 日以上前				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

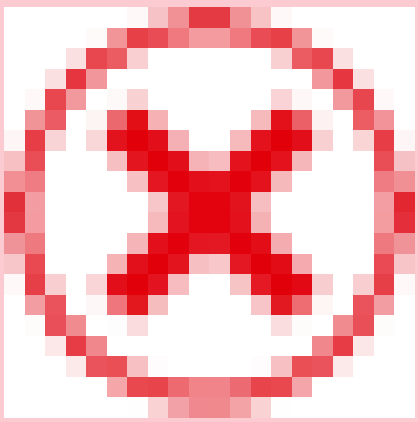
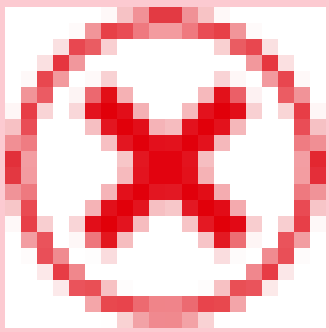
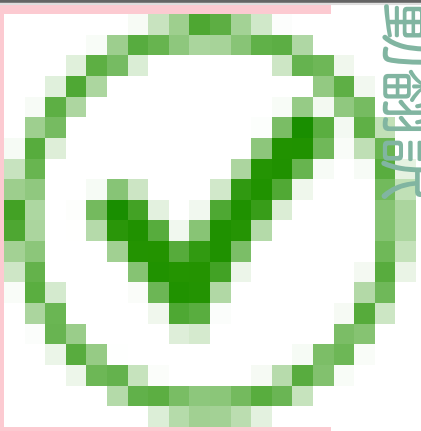
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
未アサイン				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

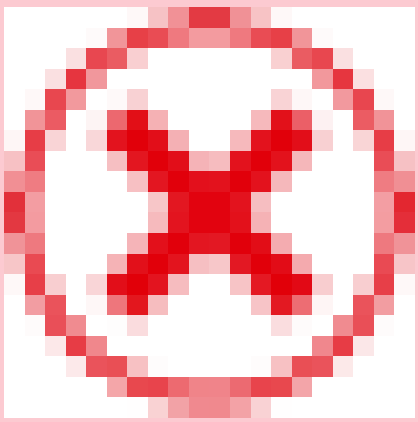
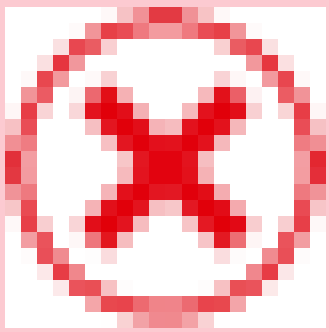
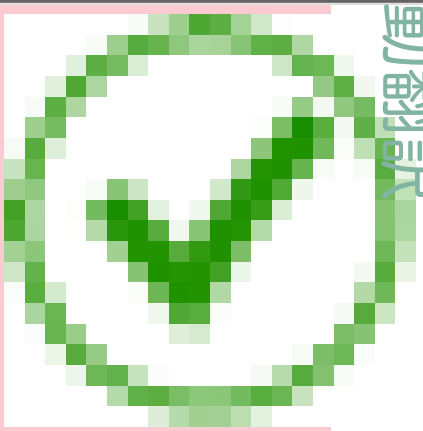
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
修復タスク未割り当て				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

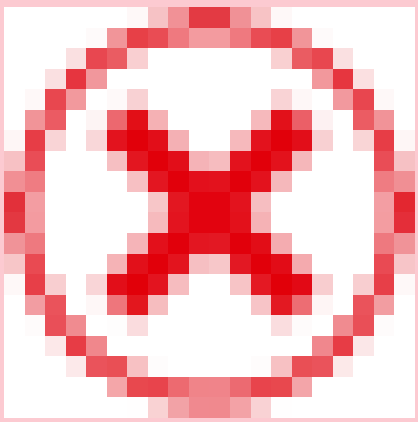
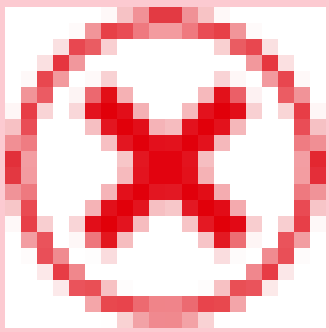
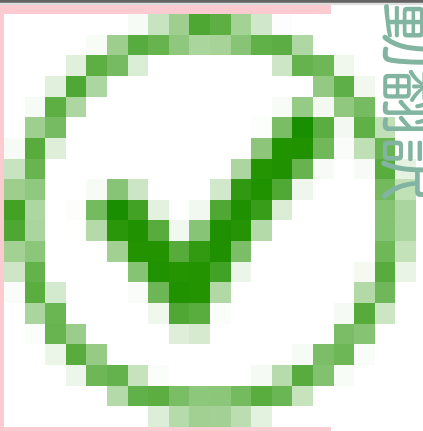
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
廃止				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

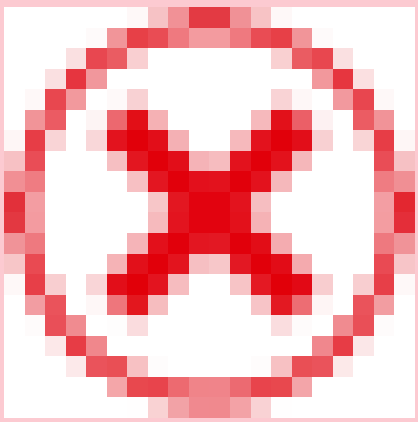
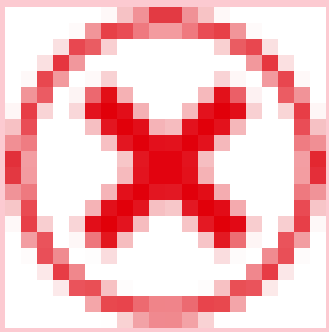
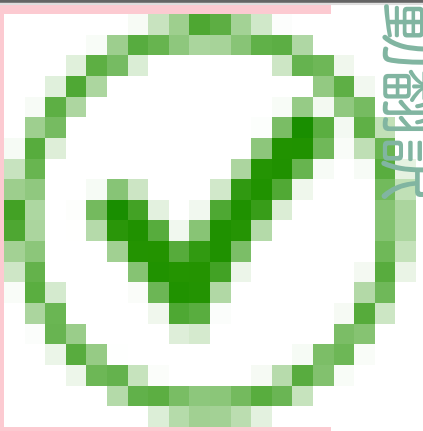
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
複数の保留				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

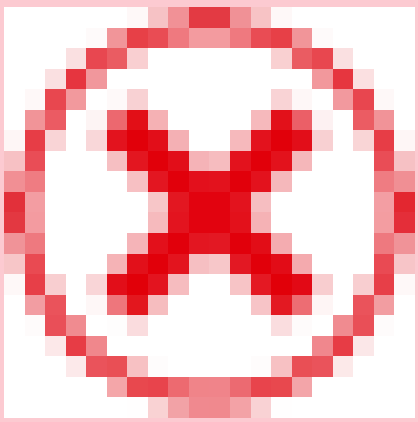
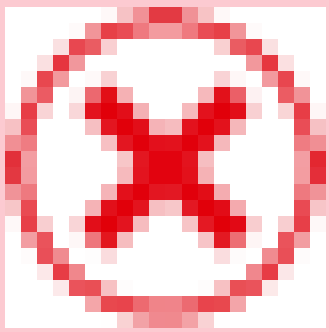
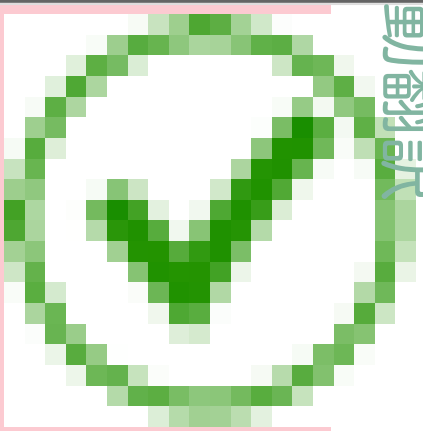
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
すべて				

ソリューション

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

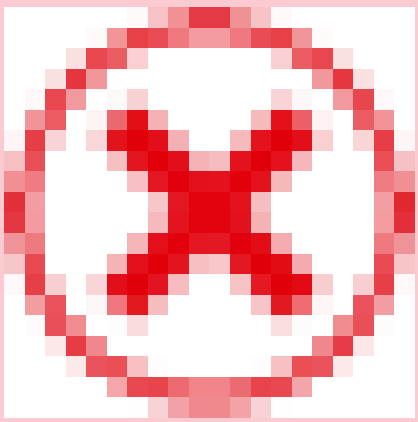
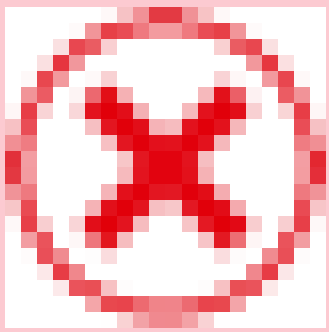
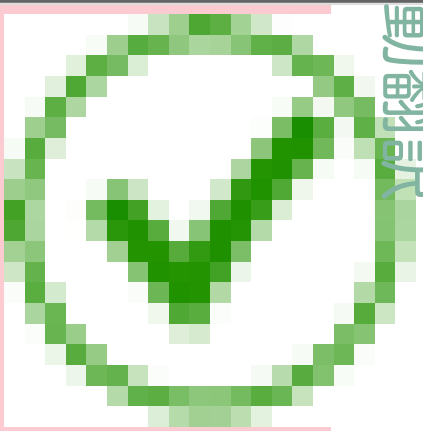
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
すべて				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

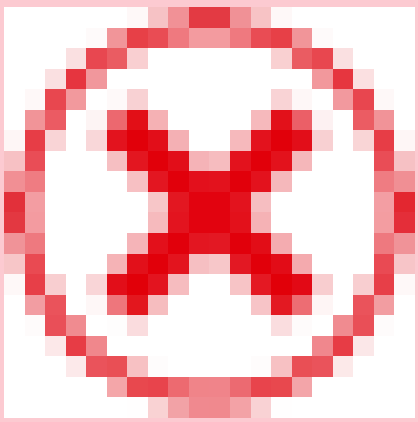
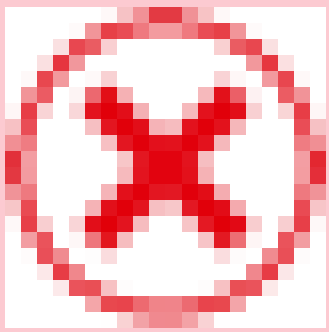
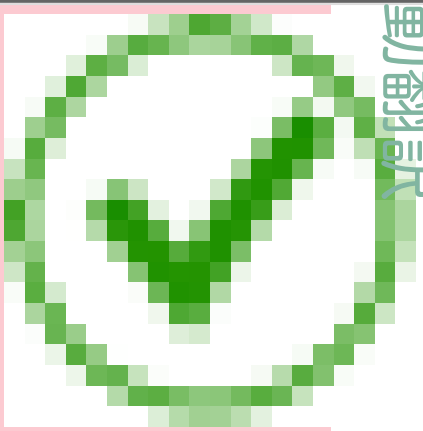
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
最高優先度				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

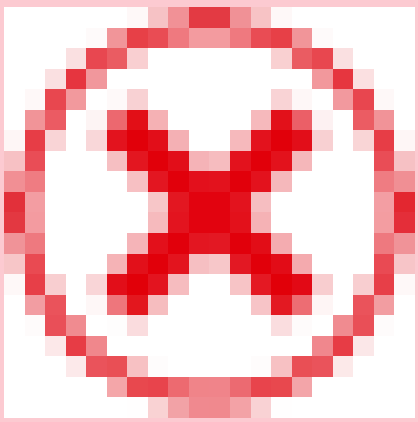
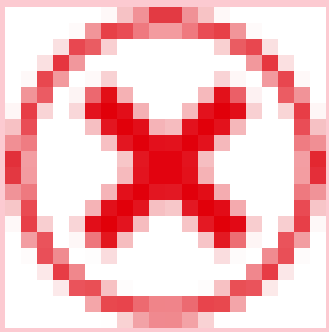
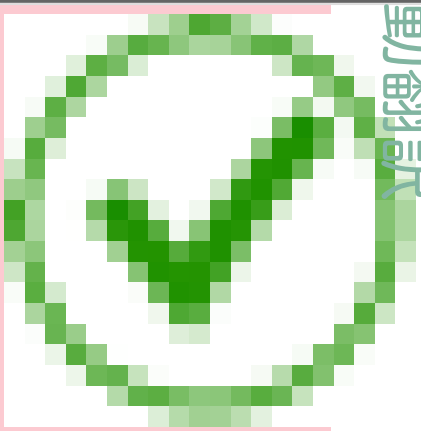
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
脆弱性一致アイテムを使用				

ライブラリ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
NVD	✗	✗	✓	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

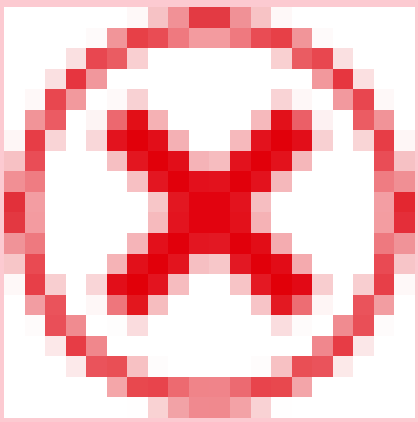
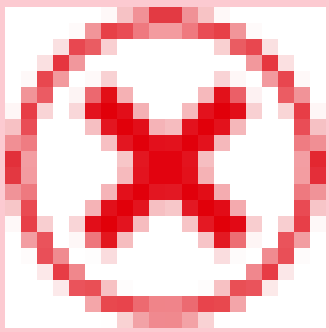
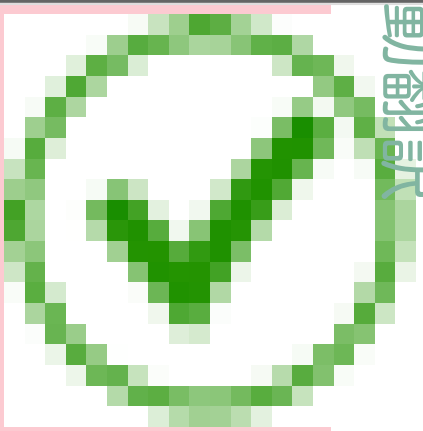
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
CWE				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

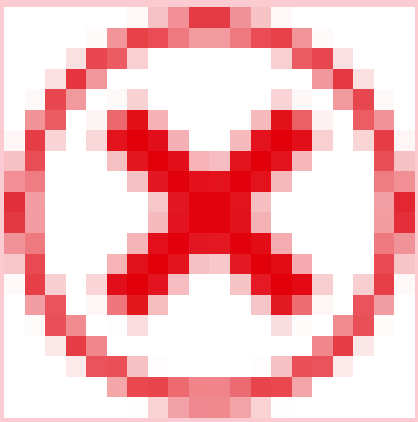
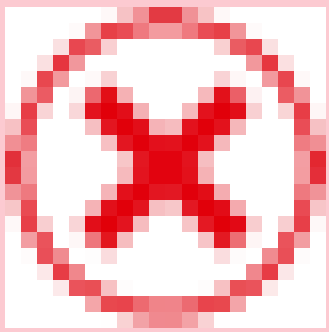
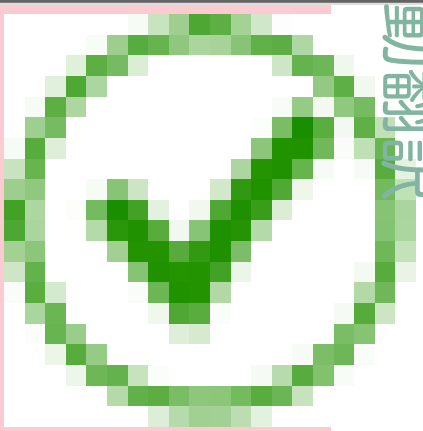
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
サードパーティ				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

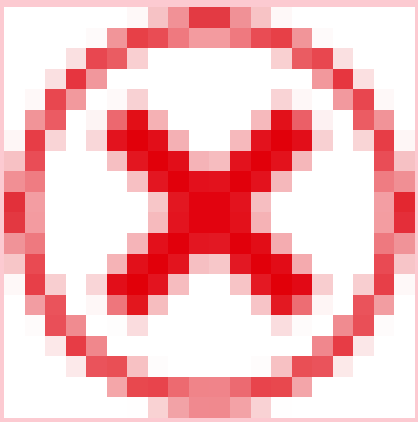
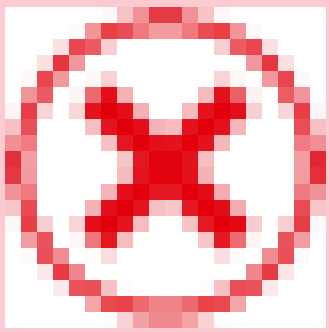
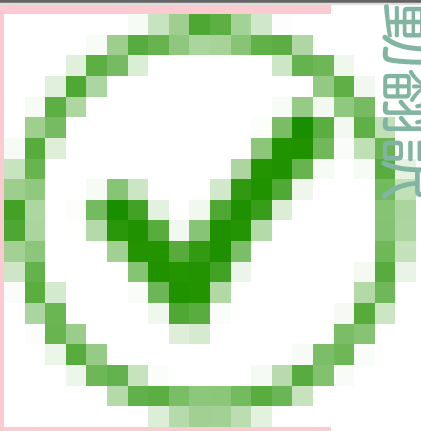
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
脆弱なソフトウェア				
脆弱性スキャン				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
エクスポージャーアセスメント	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

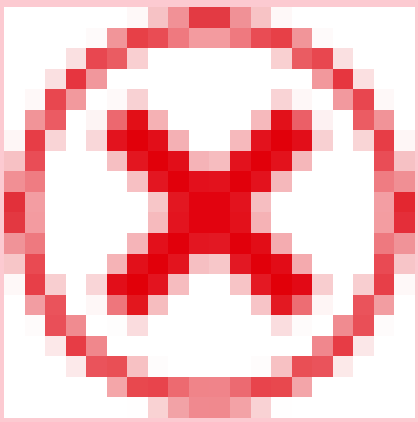
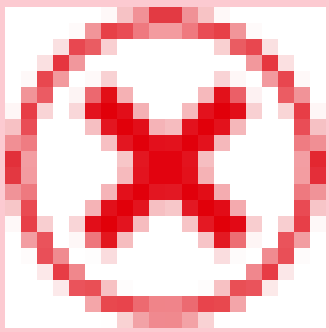
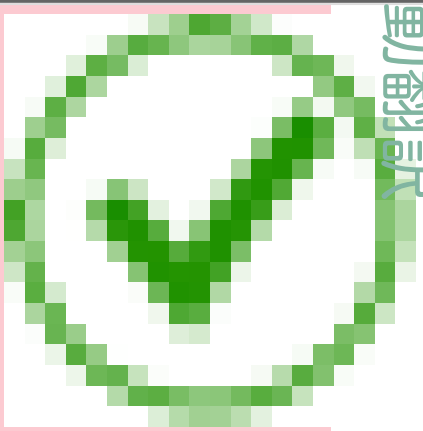
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
スキャン				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

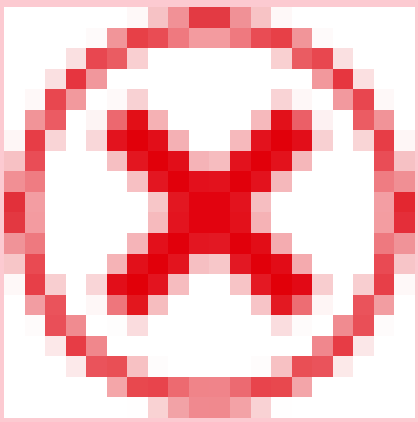
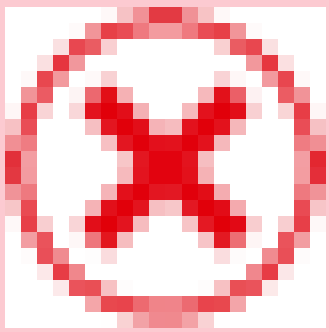
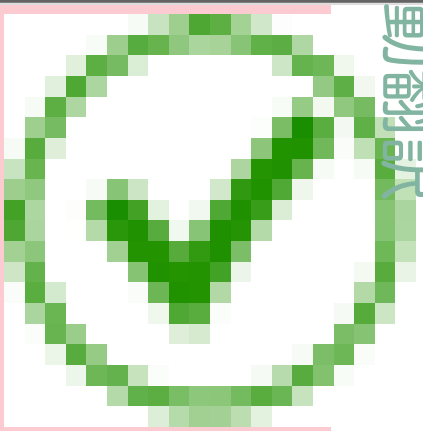
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
スキャナー				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

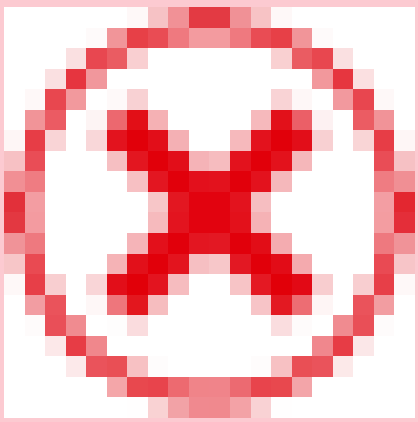
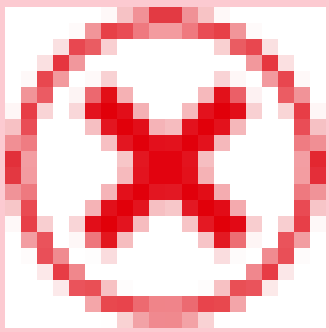
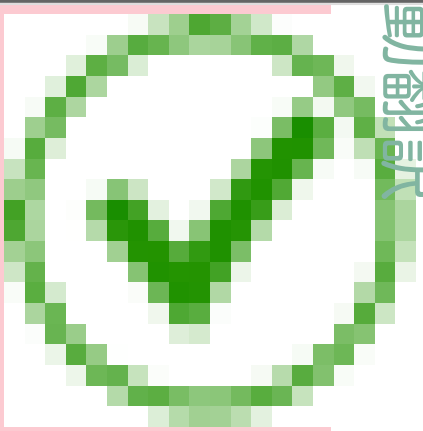
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
スキャンキュー				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

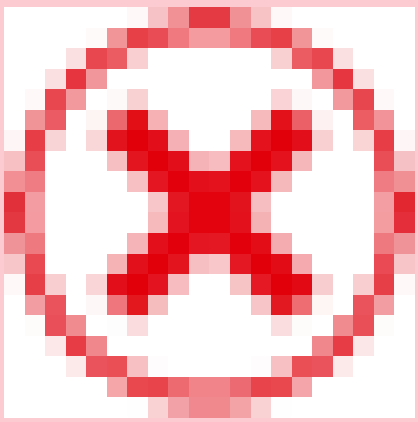
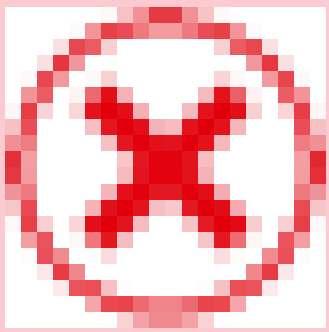
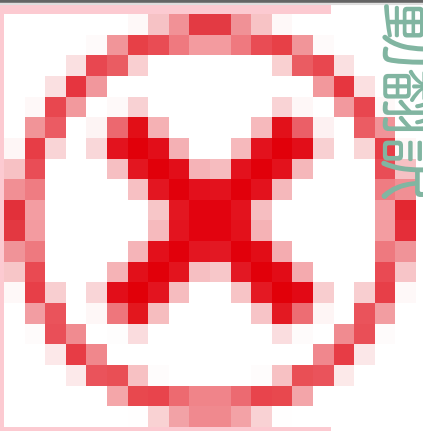
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
スキャナーレート制限				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

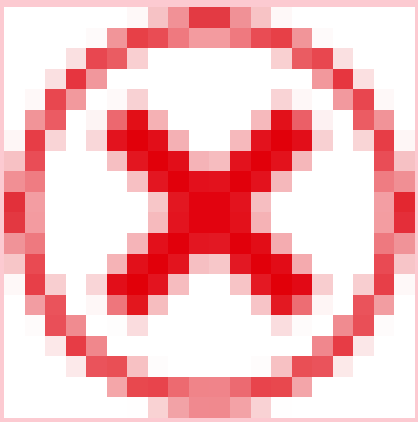
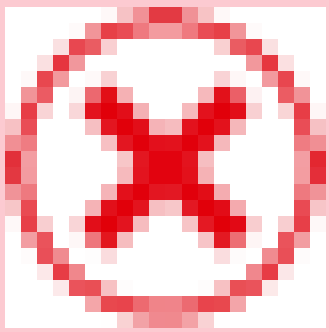
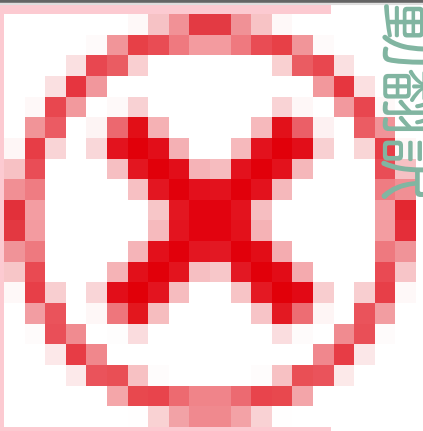
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
レート制限定義				
管理				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
セットアップアシスタント	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
監視トピック	✗	✗	✓	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
アサインルール	✗	✗	✗	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

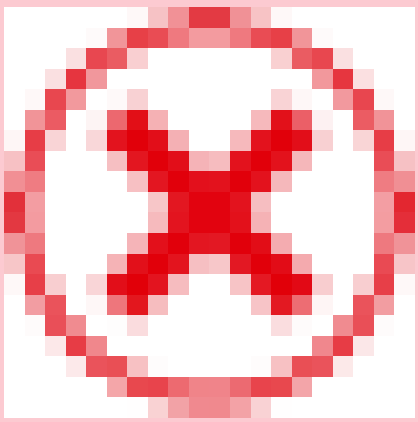
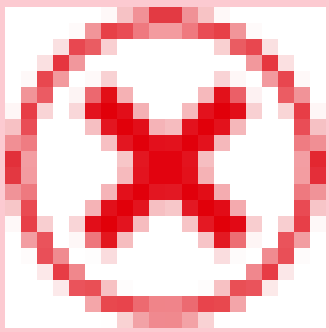
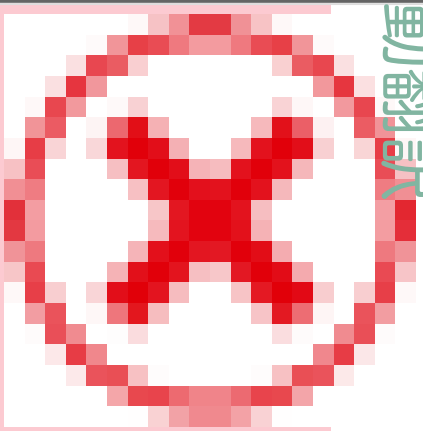
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
修復タスクルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

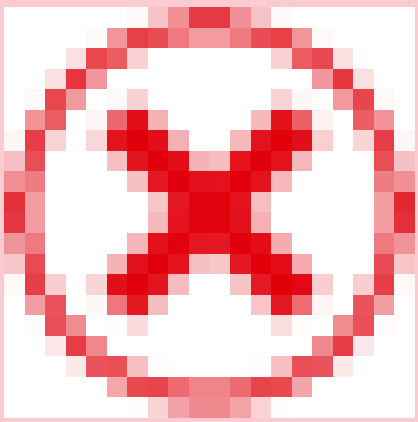
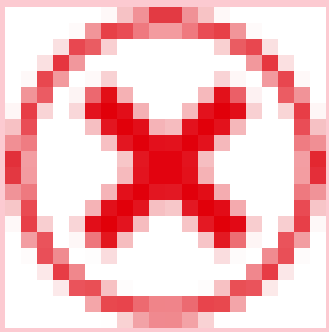
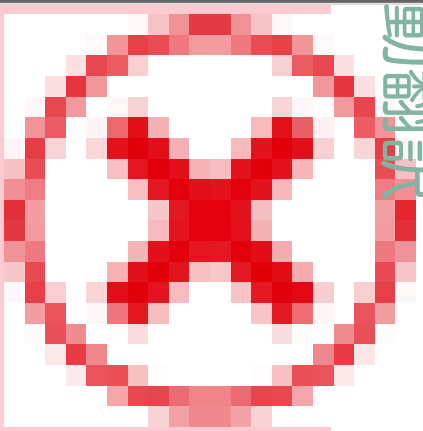
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
アサインの推奨				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

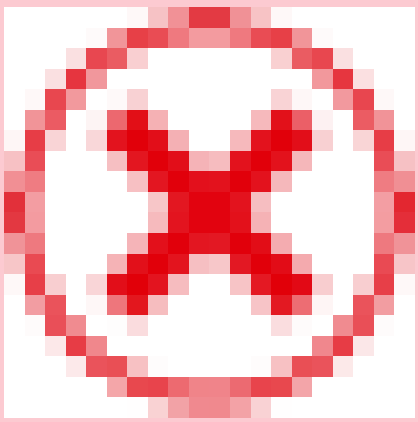
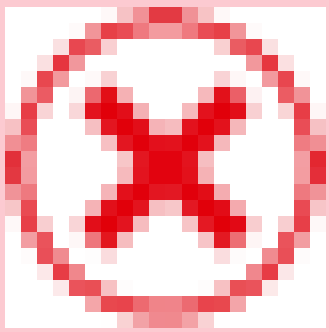
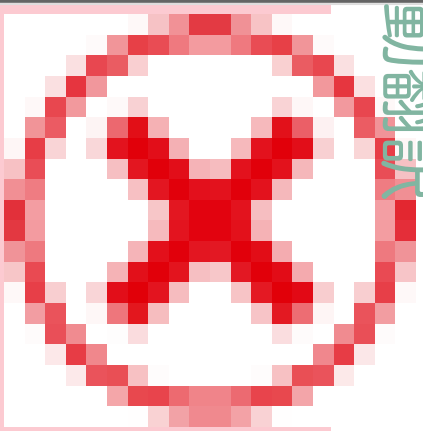
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
脆弱性算出				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

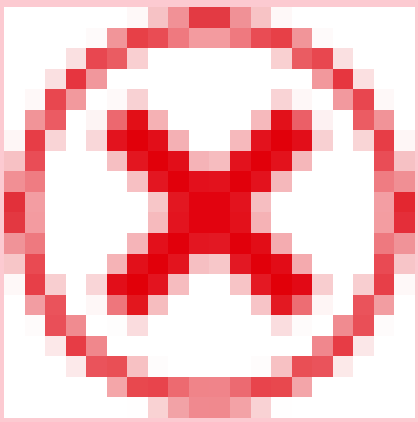
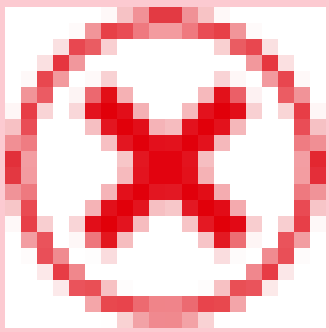
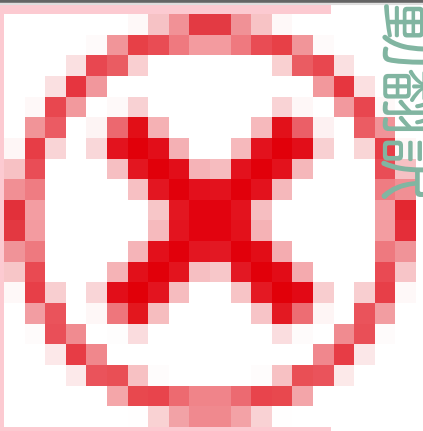
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
脆弱性ロールアップ算出				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
修復ターゲットルール	✗	✗	✗	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

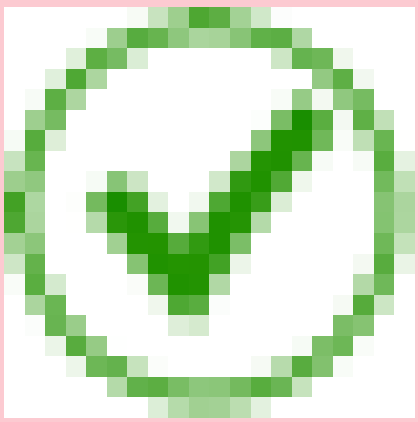
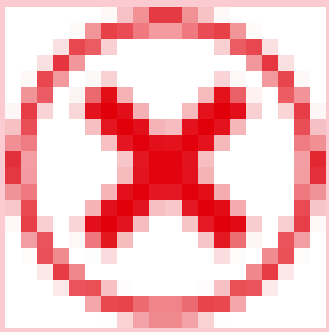
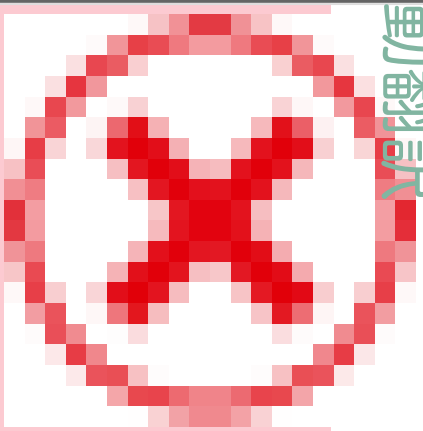
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
自動クローズ構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

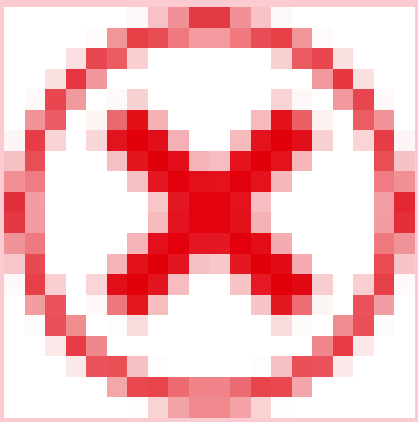
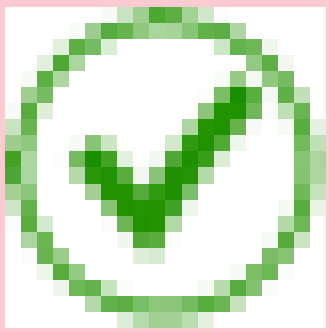
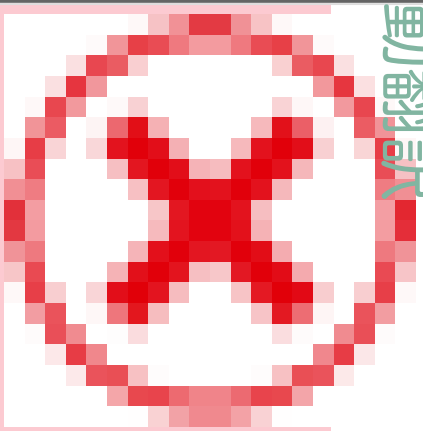
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
ルールの自動削除				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

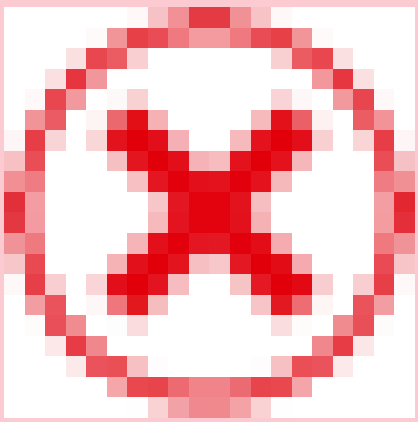
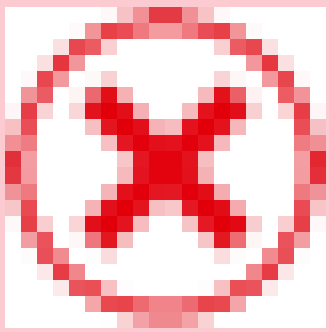
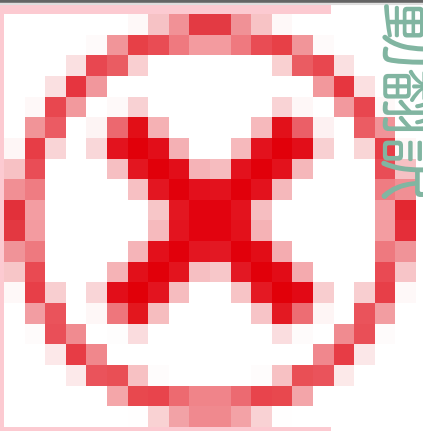
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
例外ルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
承認ルール	✗	✗	✗	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

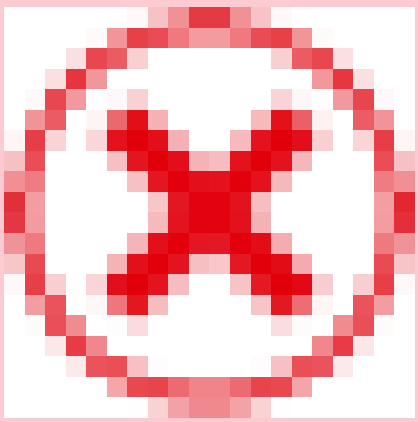
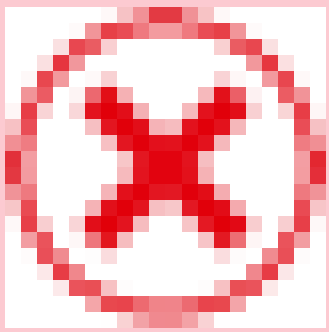
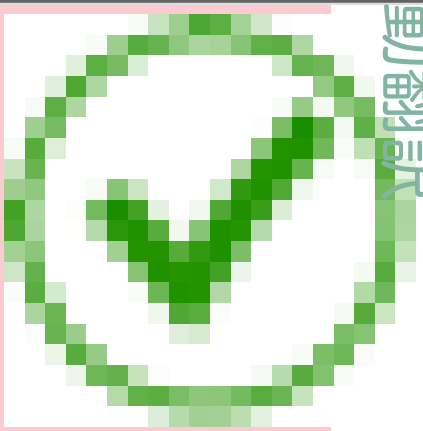
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
分類ルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

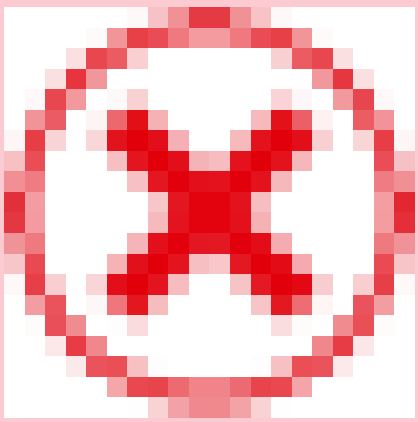
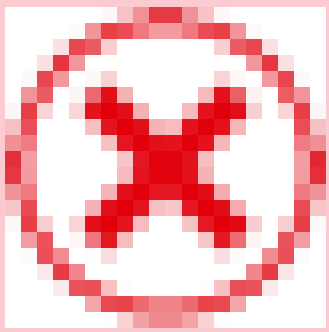
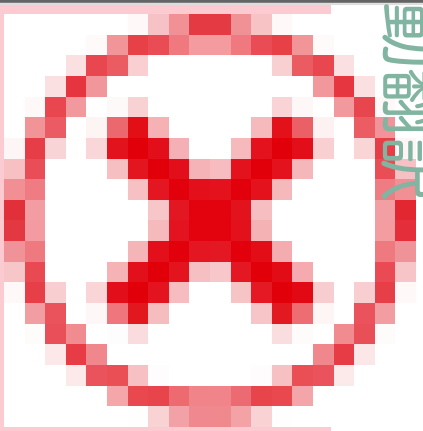
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
パフォーマンス構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

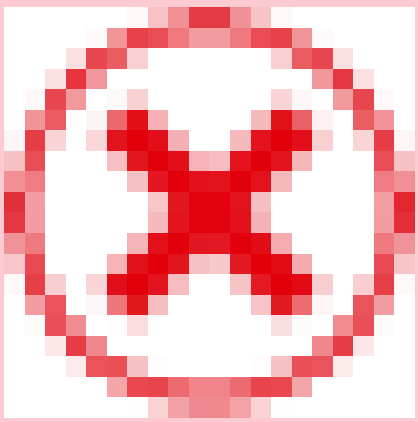
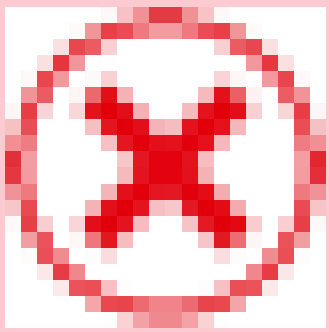
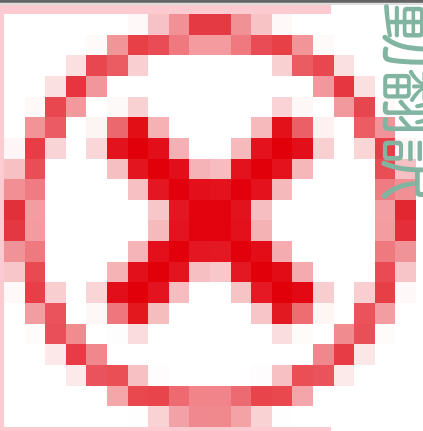
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
VI の粒度の構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
通知	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
メールテンプレート	✗	✗	✗	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

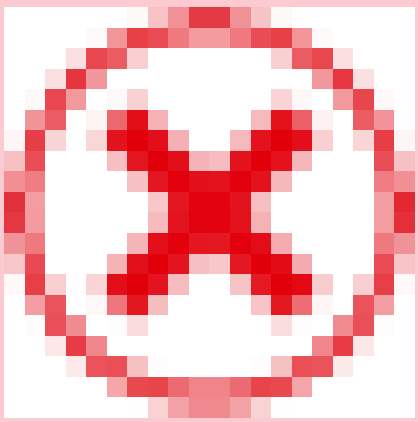
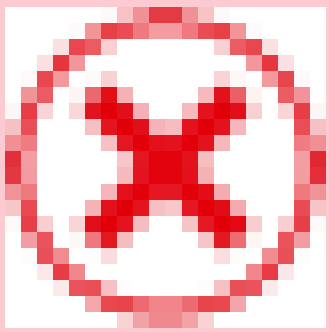
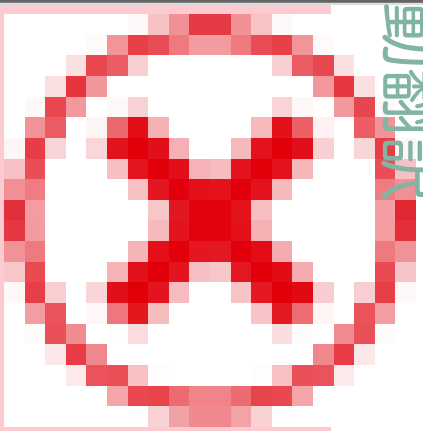
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
キューをインポート				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

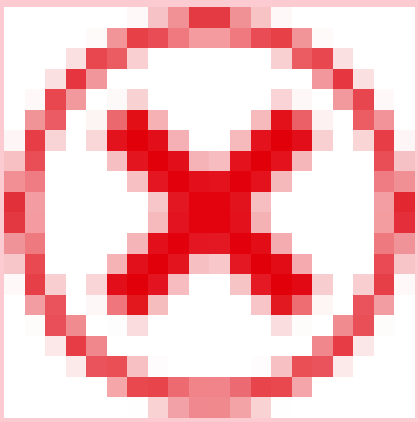
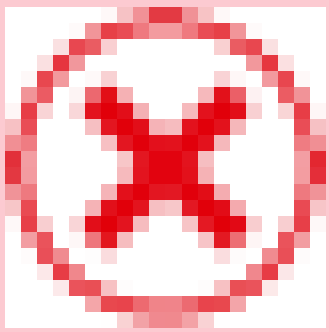
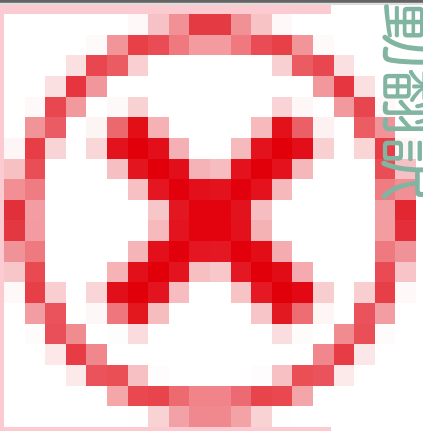
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
統合				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

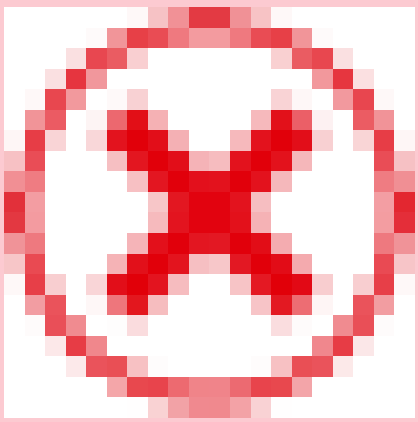
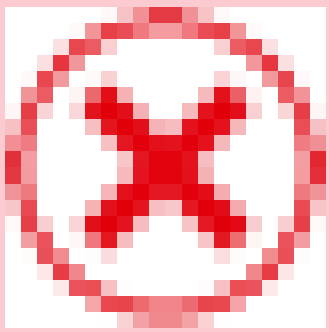
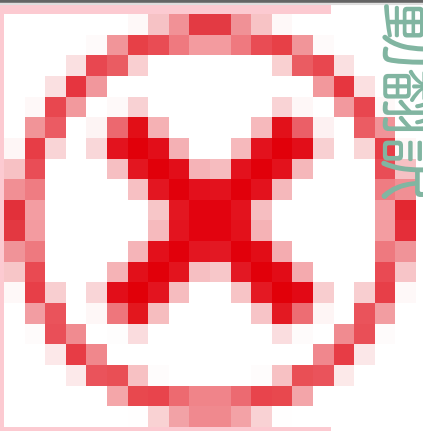
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
SLA 定義				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

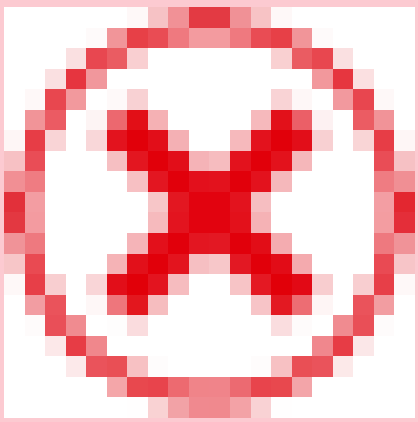
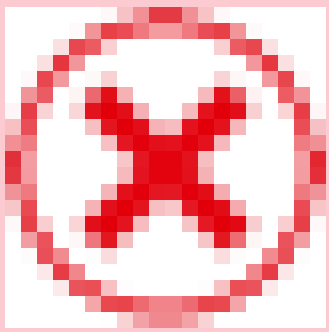
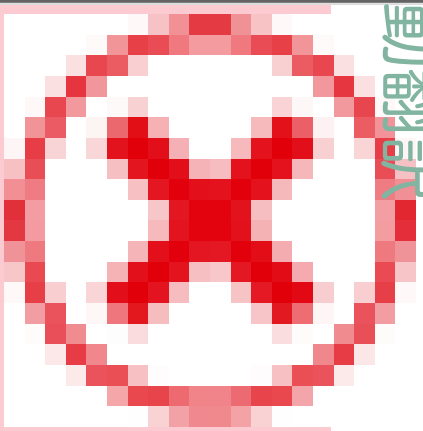
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
SAM NVD の構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

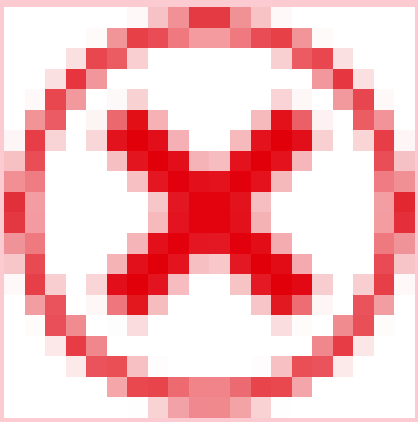
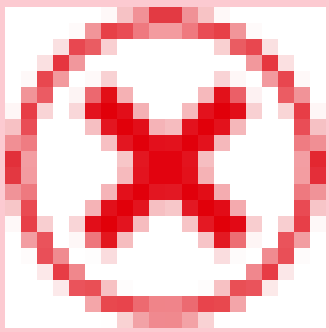
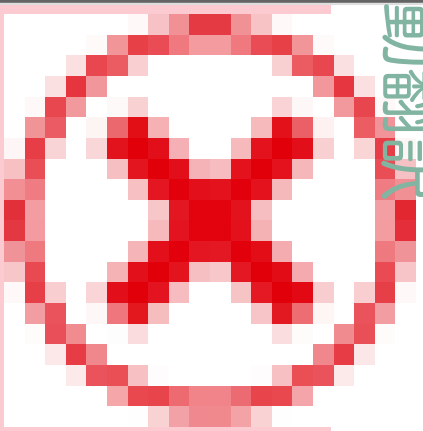
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
正規化された重大度マップ				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

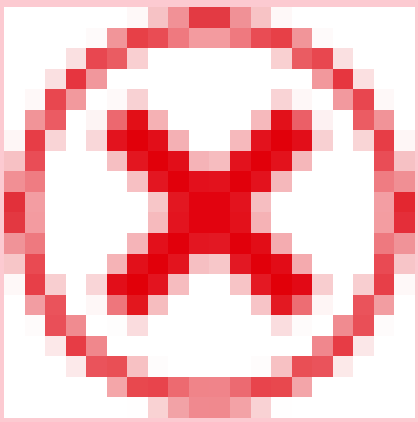
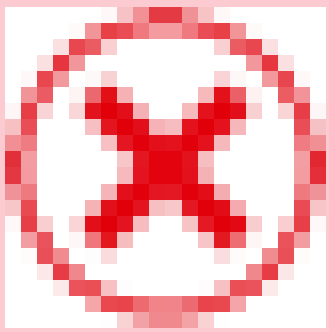
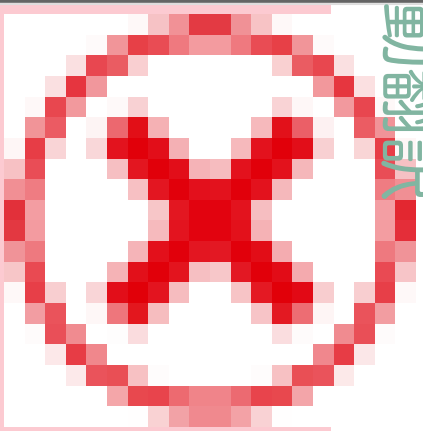
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
スキャン範囲構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

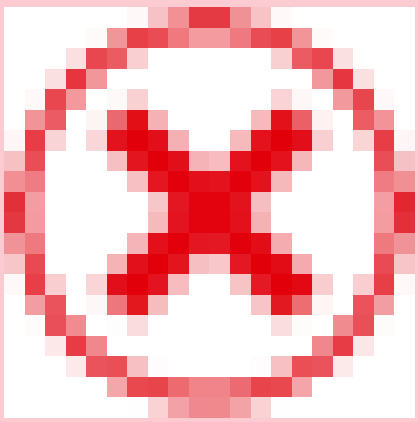
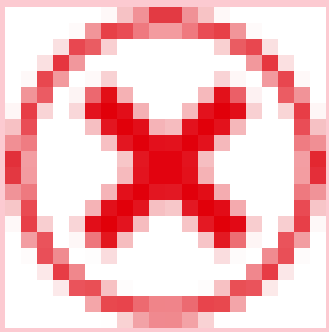
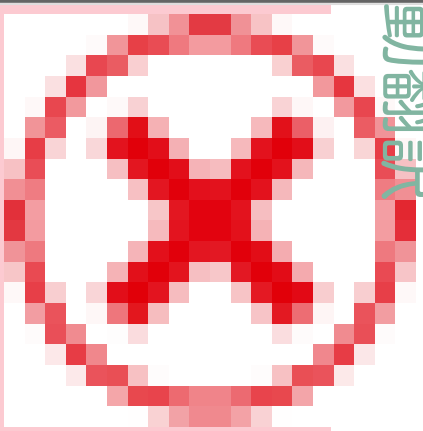
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
例外管理				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

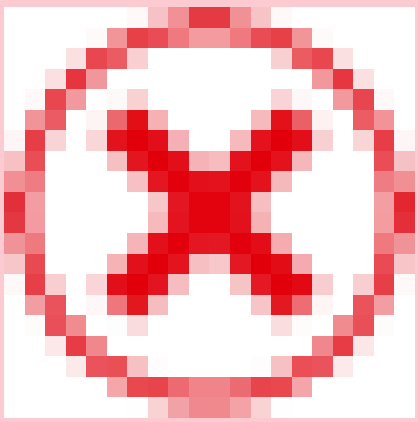
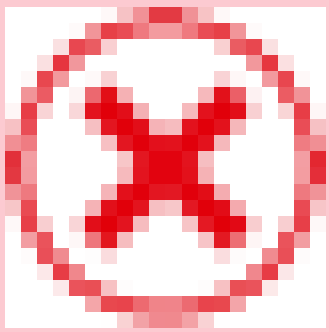
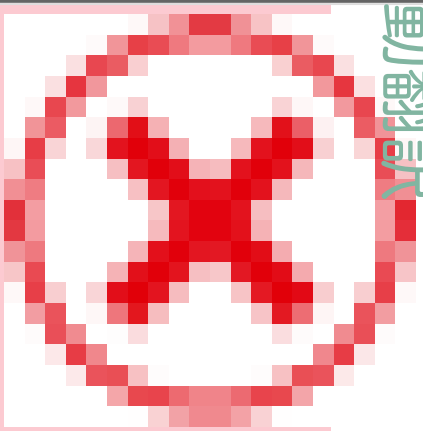
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
使用状況レポート				
診断				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classification_rules、**sn_vul.manage_exception_configuration**

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

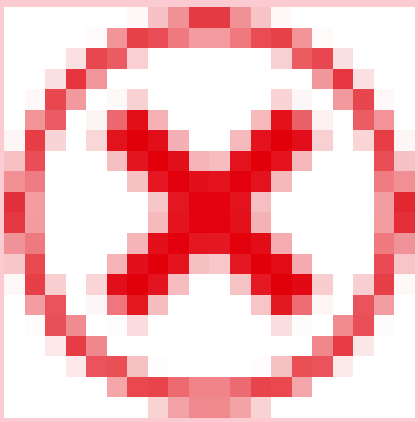
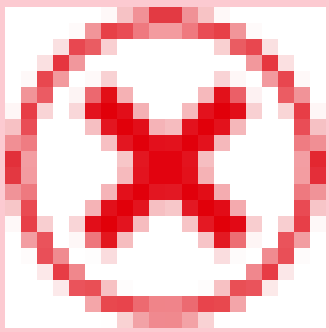
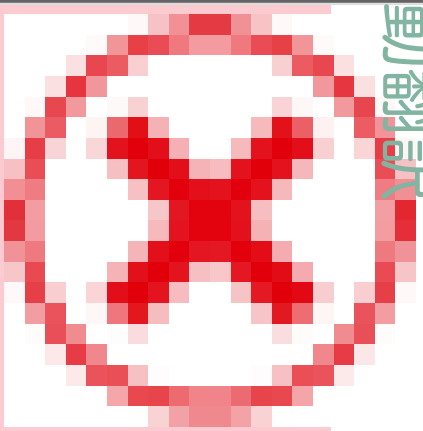
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_vul.r
チェック				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifica

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
(メインアプリグループ)				
CISO ダッシュボード	✗	✗	✗	✗

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

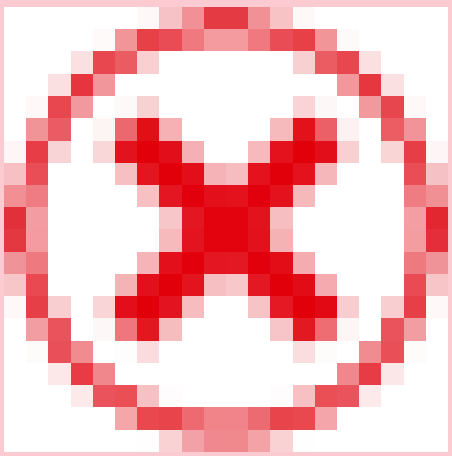
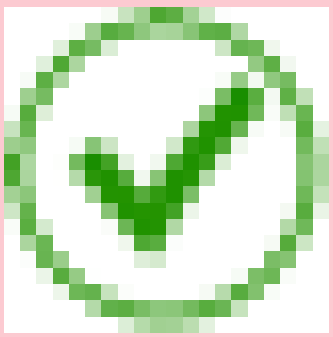
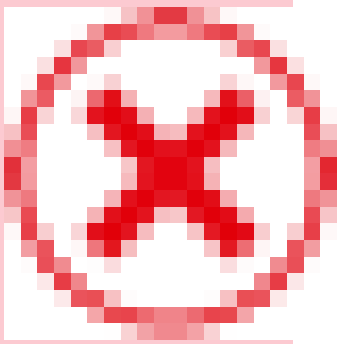
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
修復の概要				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

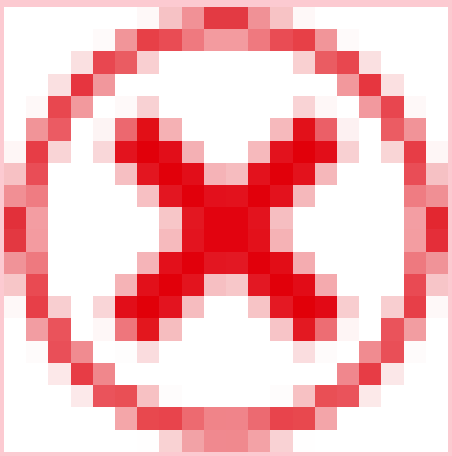
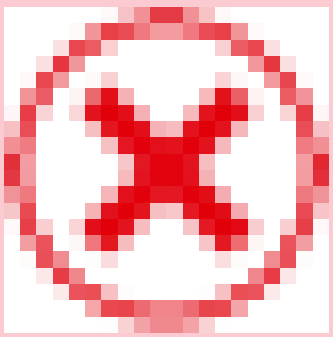
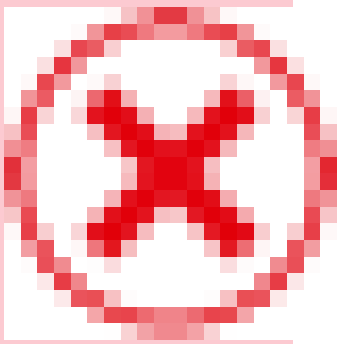
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
脆弱性マネージャーのワークスペース				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

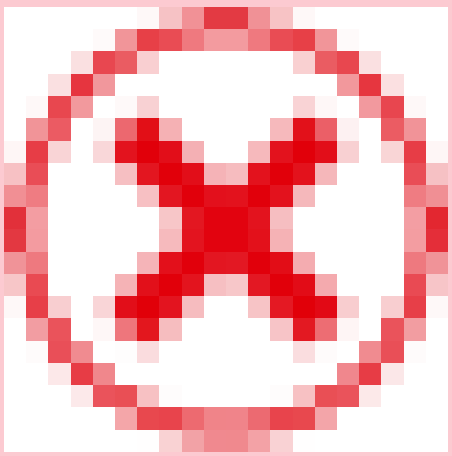
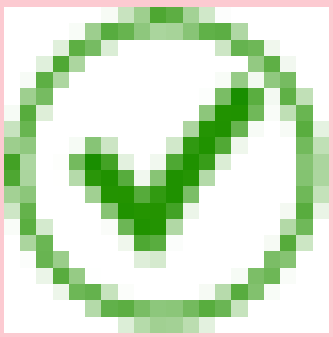
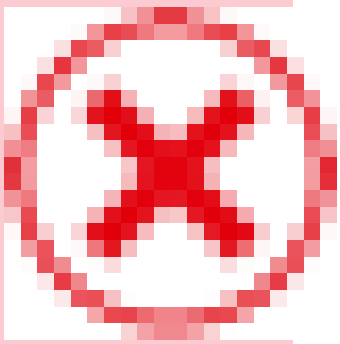
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
概要				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

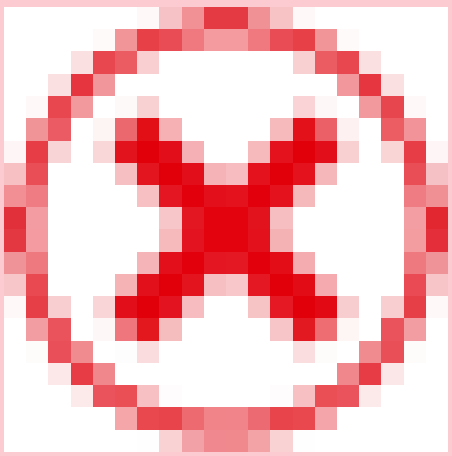
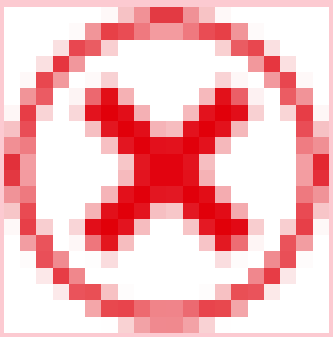
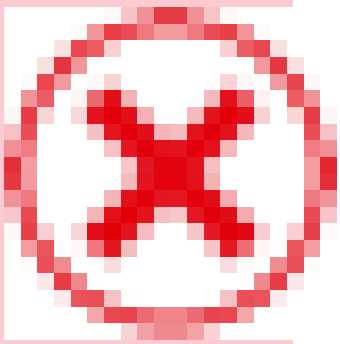
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
IT 修復ワークスペース				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

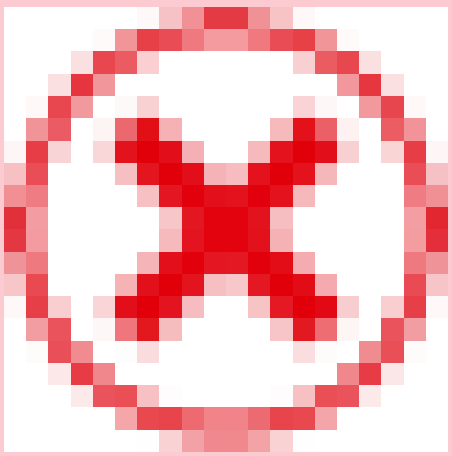
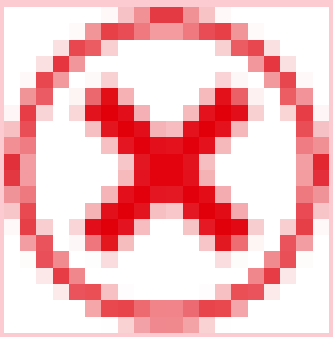
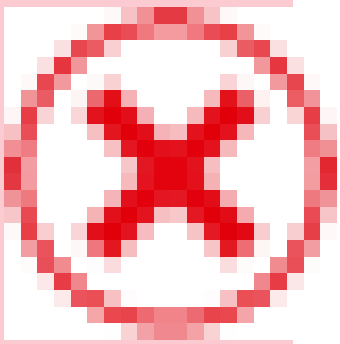
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
承認者の概要				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

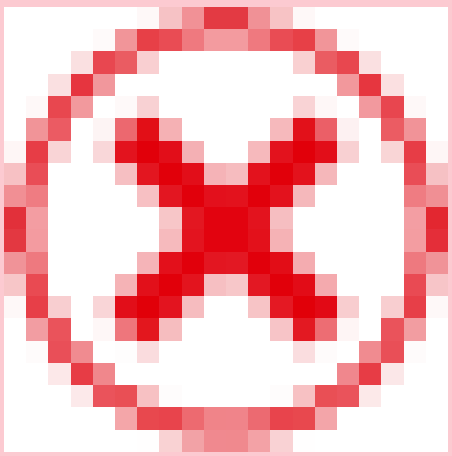
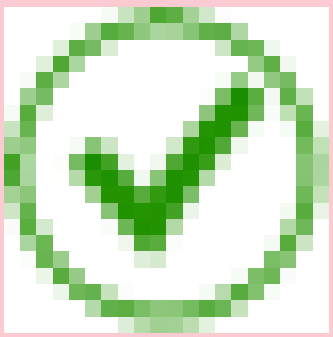
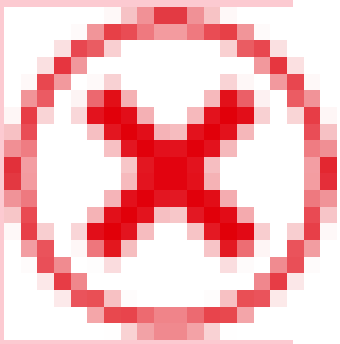
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
概要				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

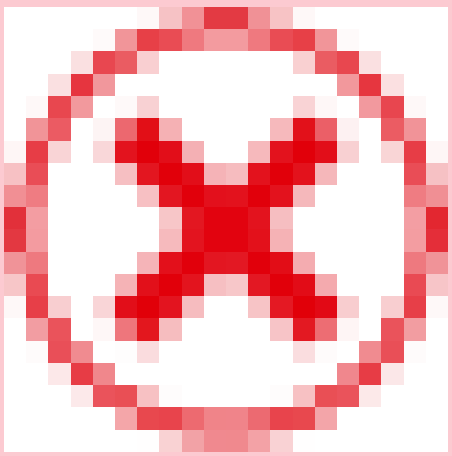
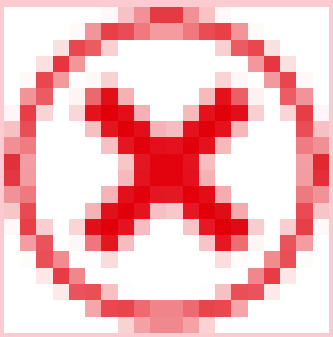
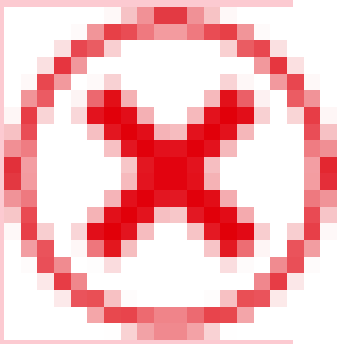
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
自分の承認				
修復タスク				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

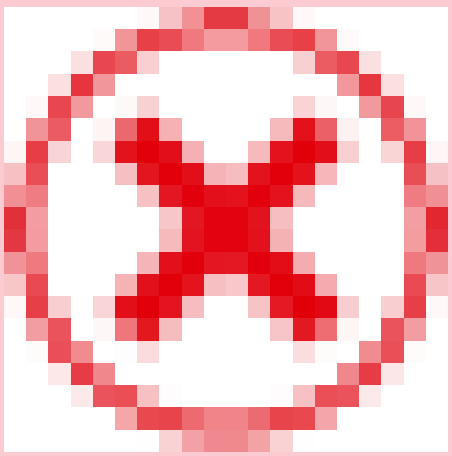
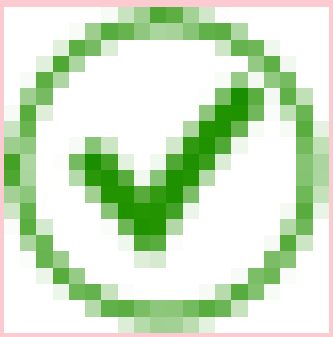
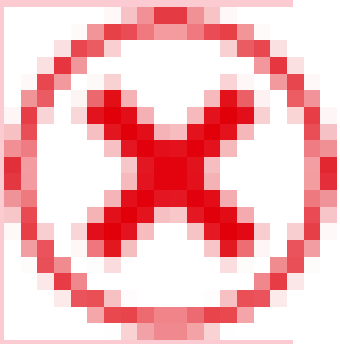
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
有効				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

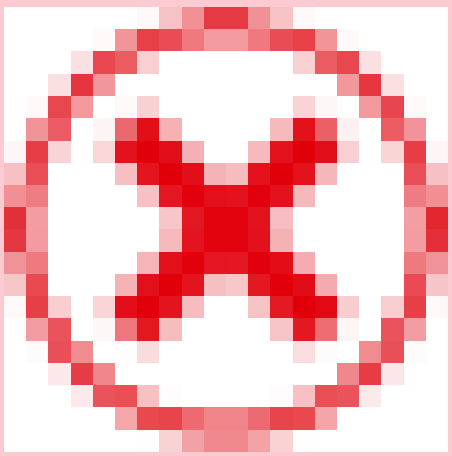
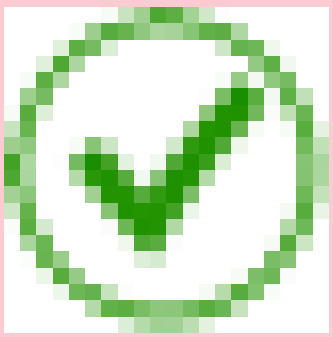
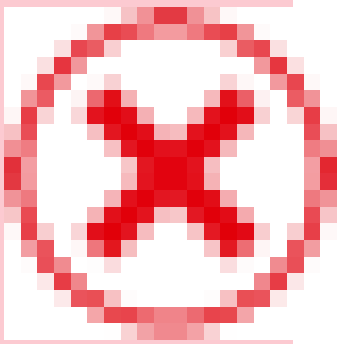
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
自分にアサイン済み				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

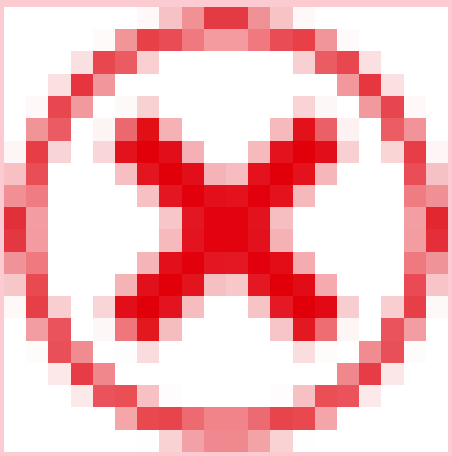
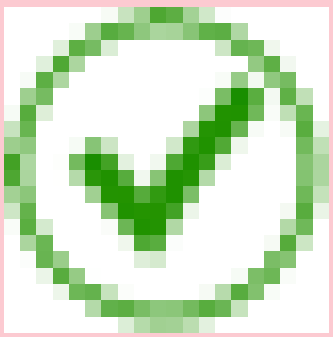
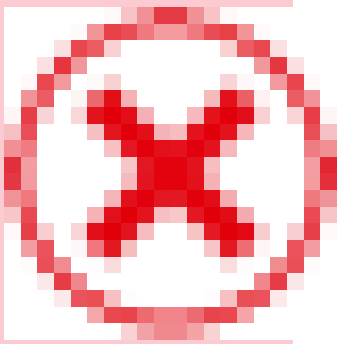
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
所属グループにアサイン済み				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

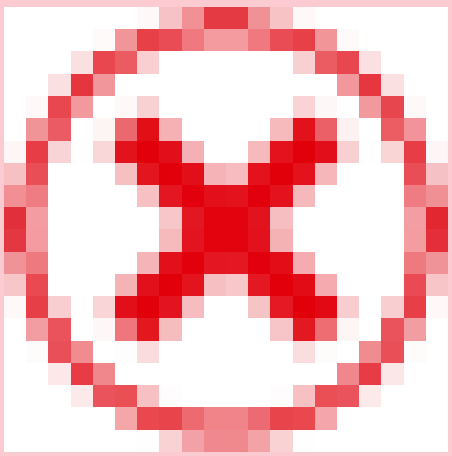
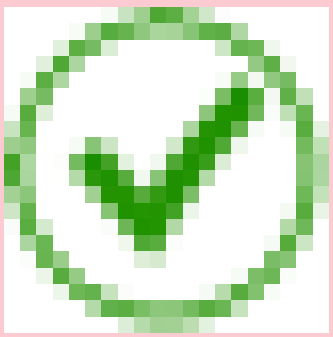
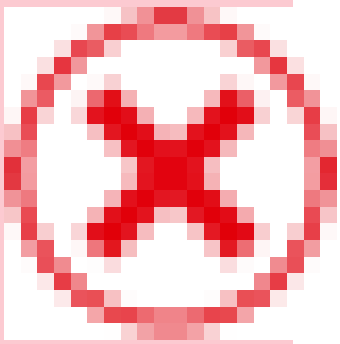
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
すべて				

脆弱性一致アイテム

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

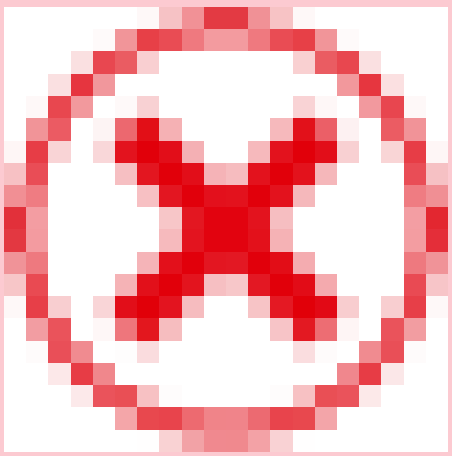
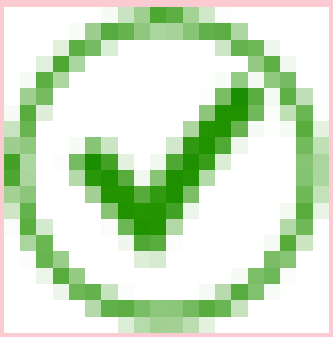
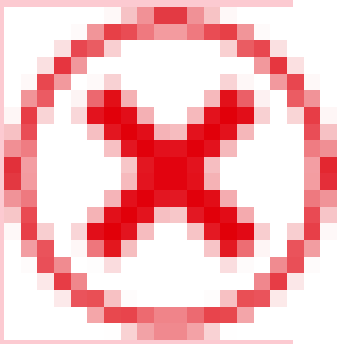
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
重大なリスク				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

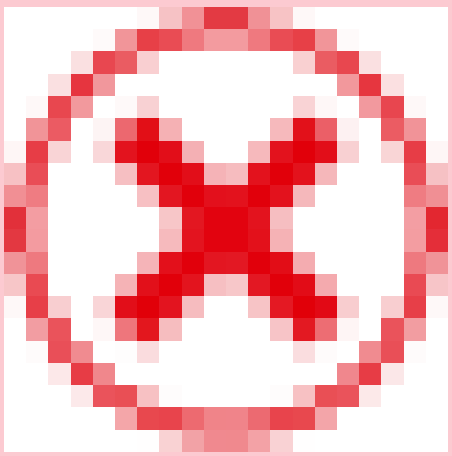
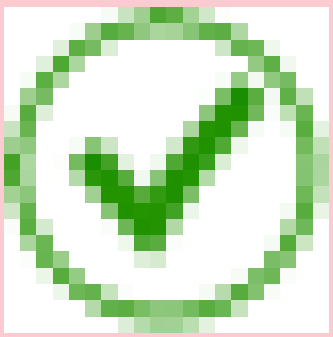
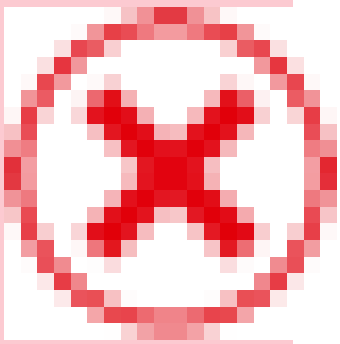
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
高リスク				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

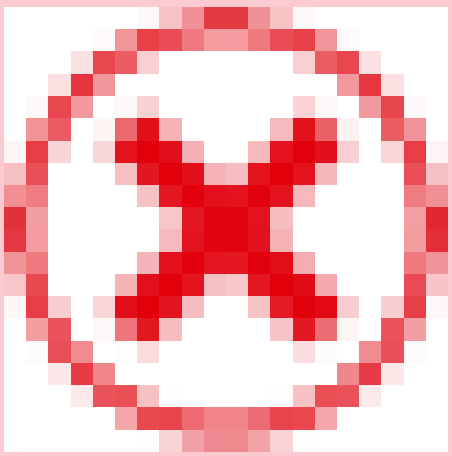
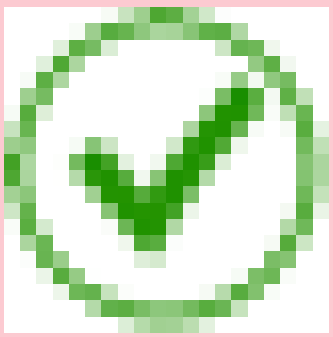
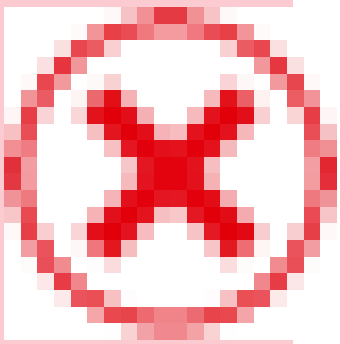
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
エクスプロイト可能				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

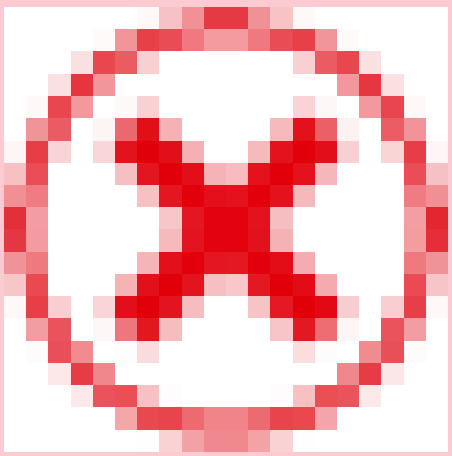
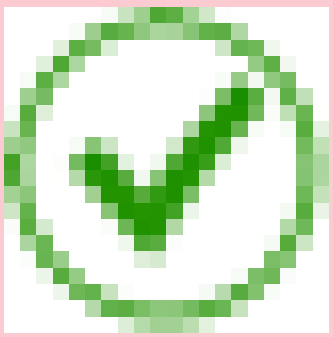
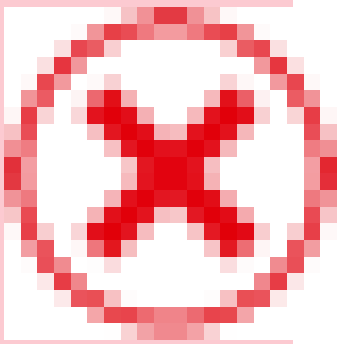
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
該当 CI 確認中				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

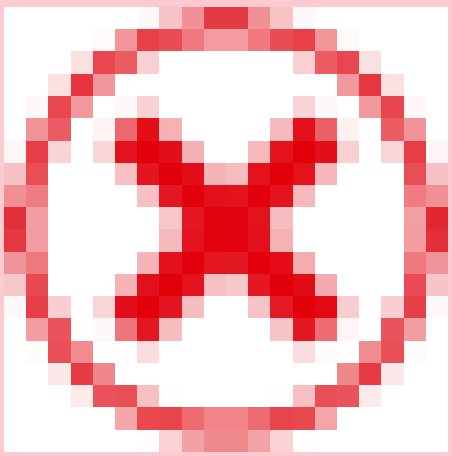
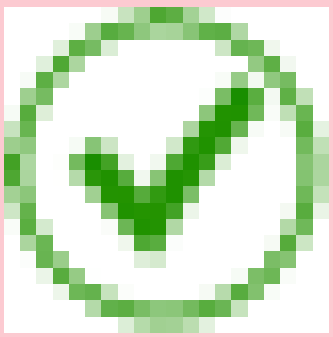
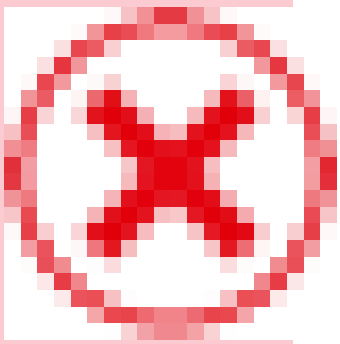
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
CI 不明				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

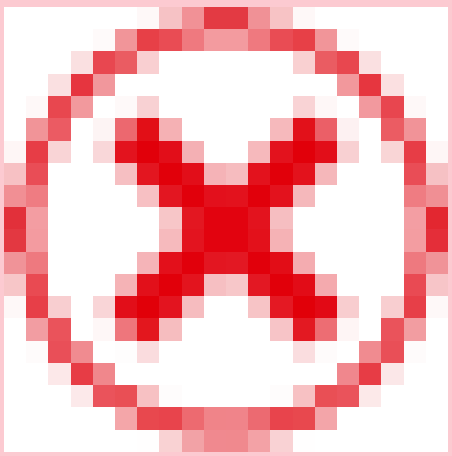
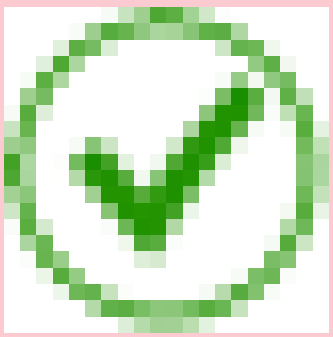
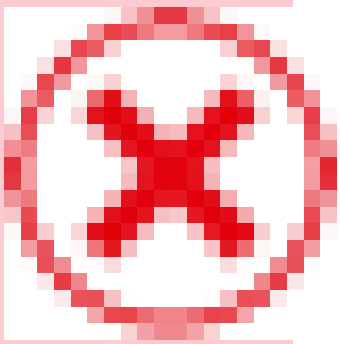
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
過去 90 日以内				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

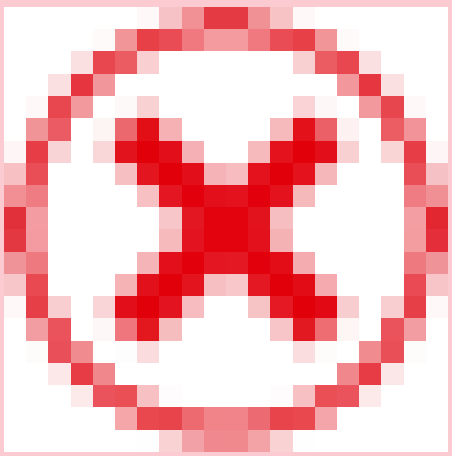
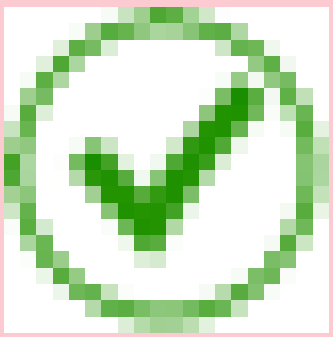
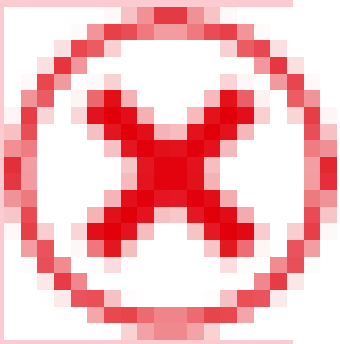
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
91 日以上前				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

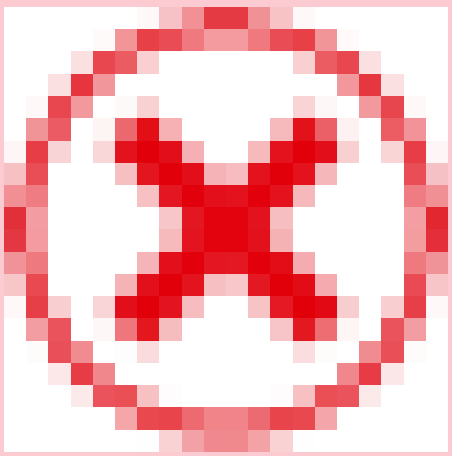
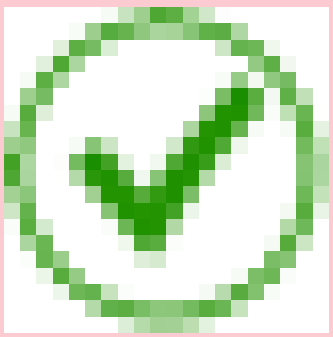
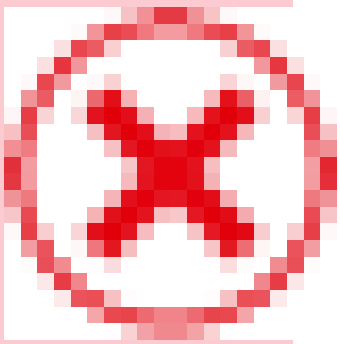
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
未アサイン				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

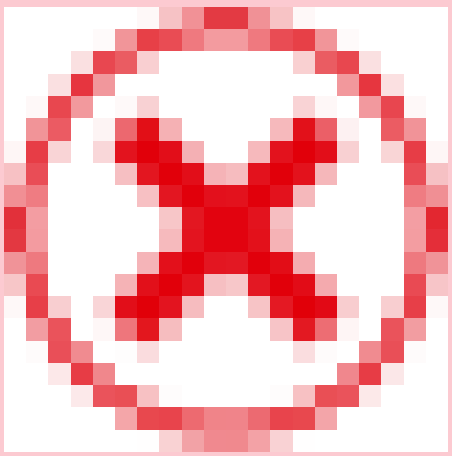
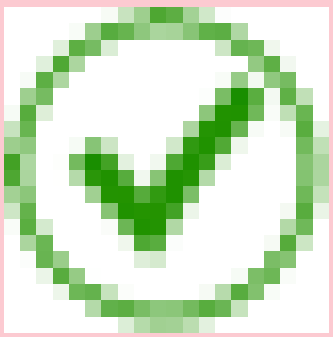
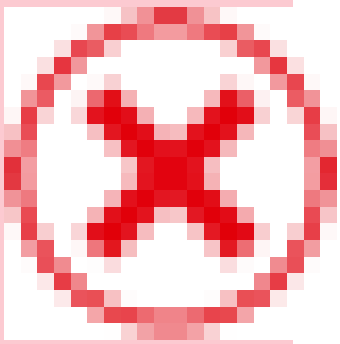
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
修復タスク未割り当て				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

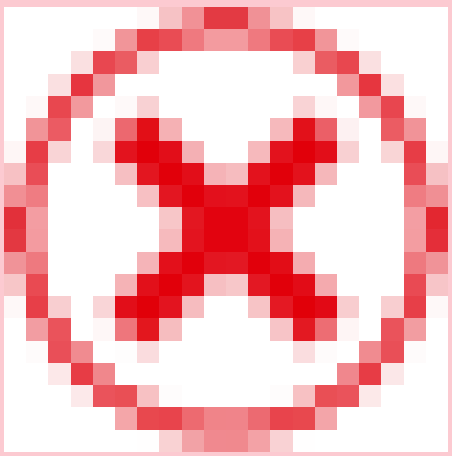
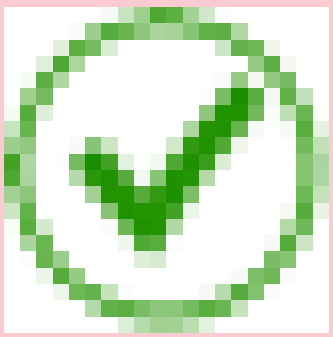
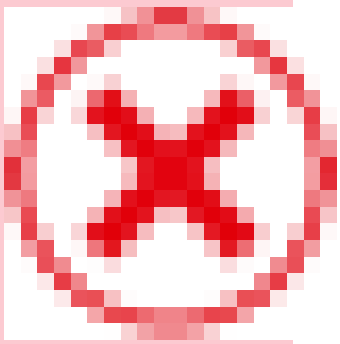
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
廃止				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

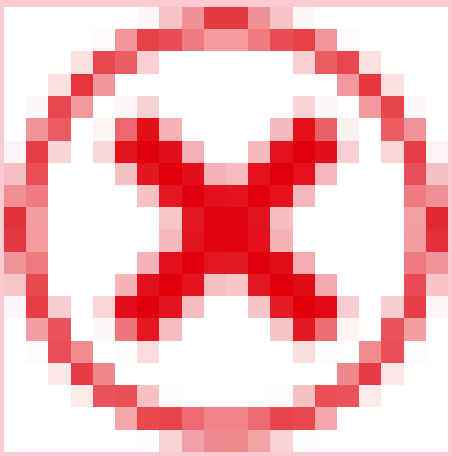
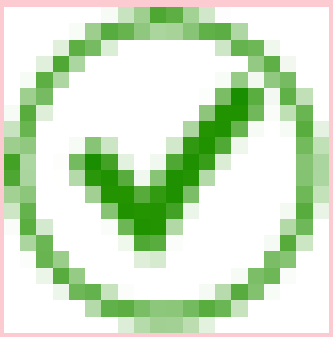
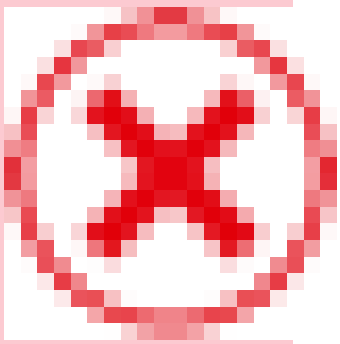
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
複数の保留				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

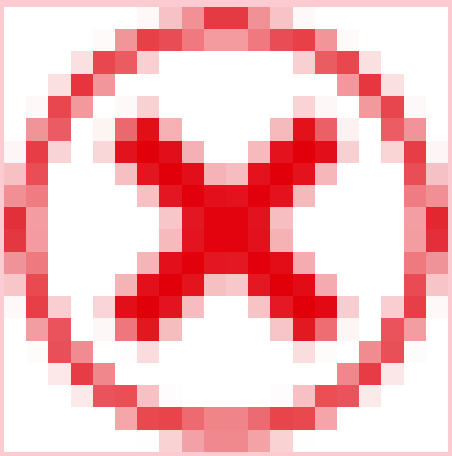
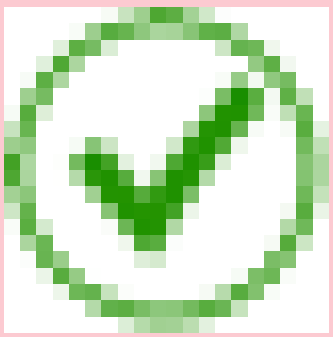
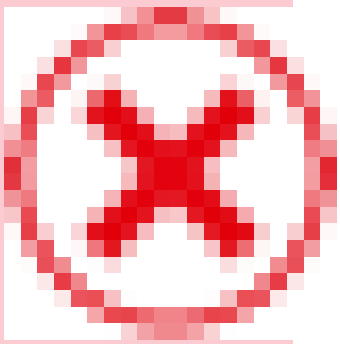
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
すべて				

ソリューション

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

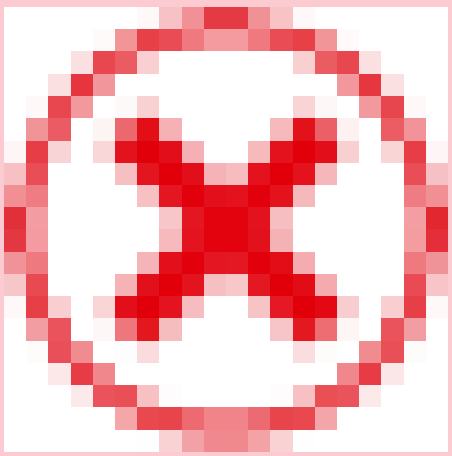
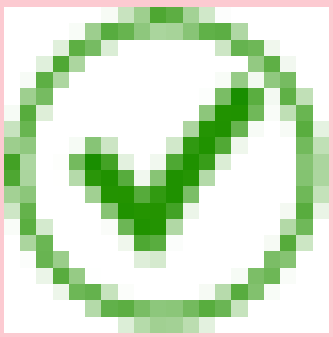
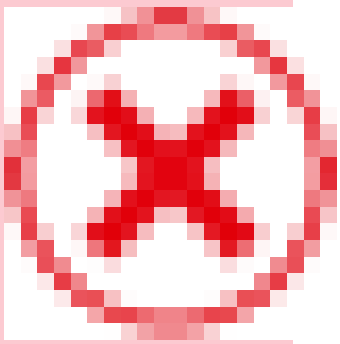
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
すべて				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

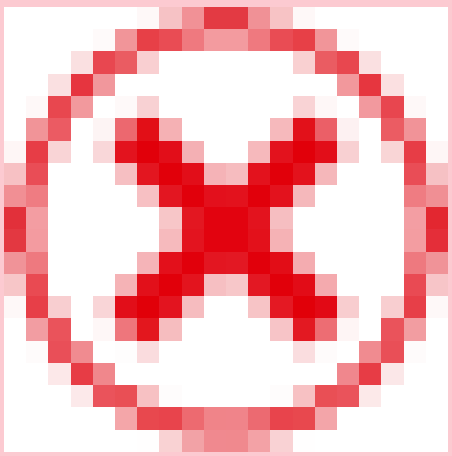
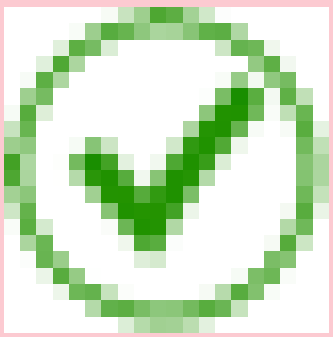
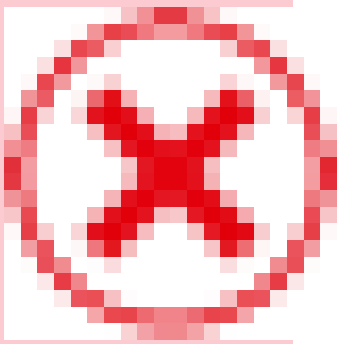
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
最高優先度				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

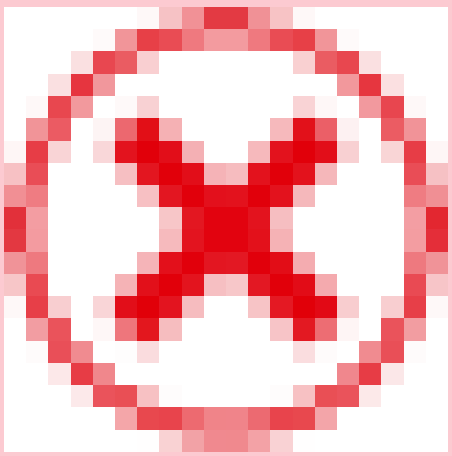
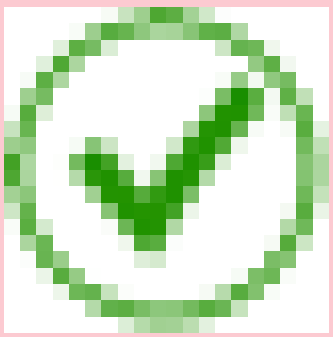
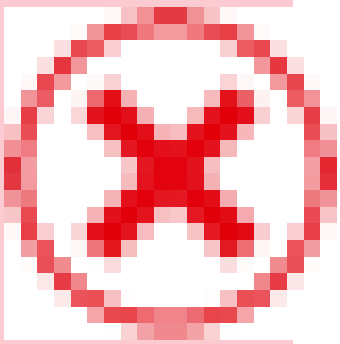
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
脆弱性一致アイテムを使用				

ライブラリ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

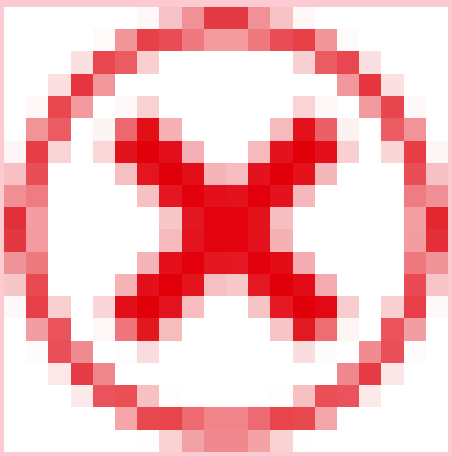
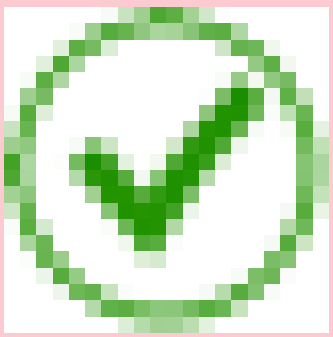
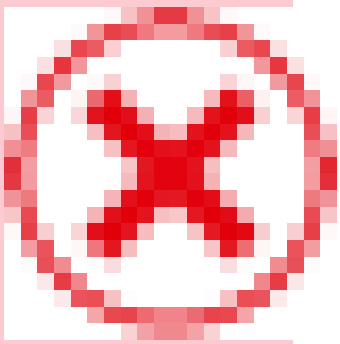
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
NVD				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

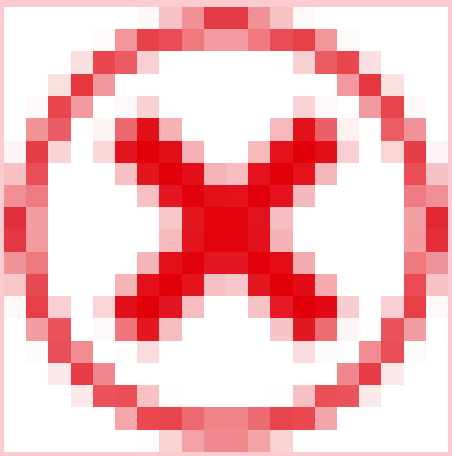
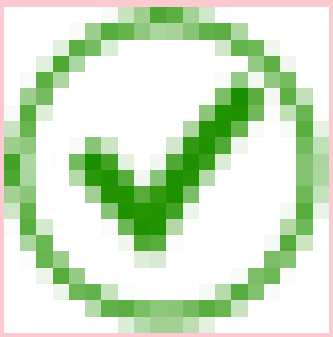
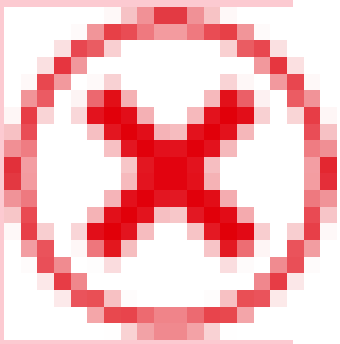
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
CWE				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

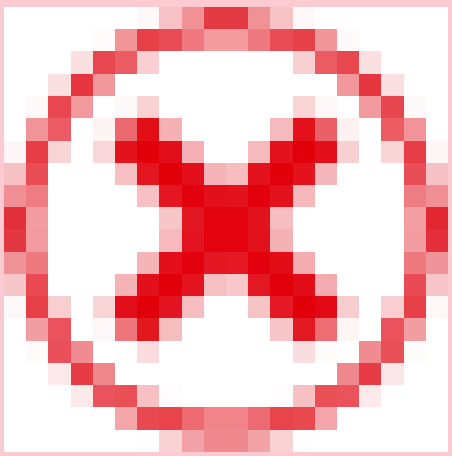
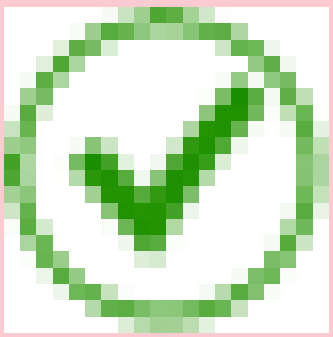
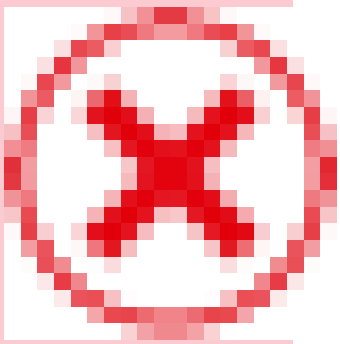
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
サードパーティ				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

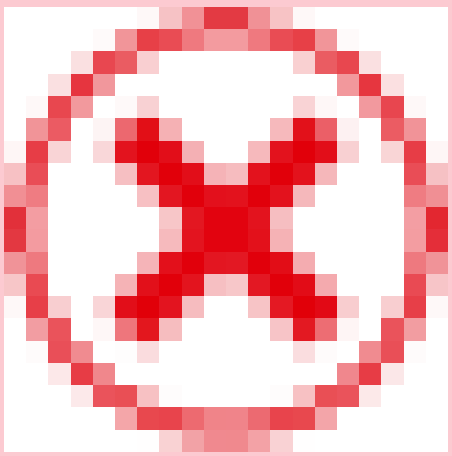
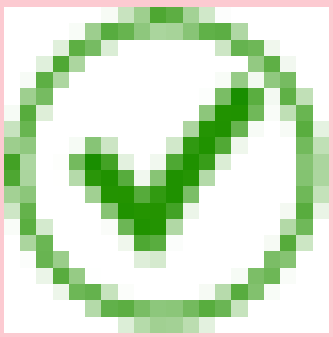
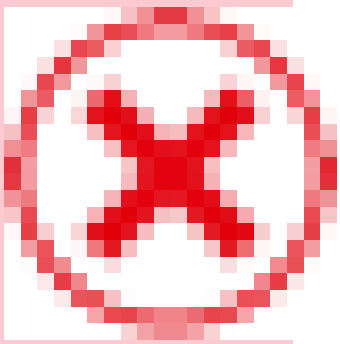
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
脆弱なソフトウェア				
脆弱性スキャン				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

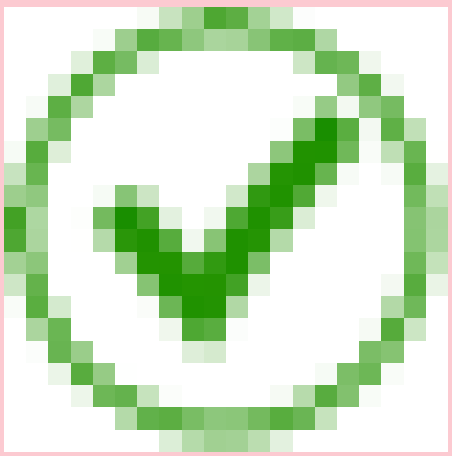
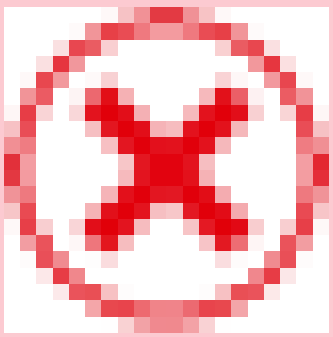
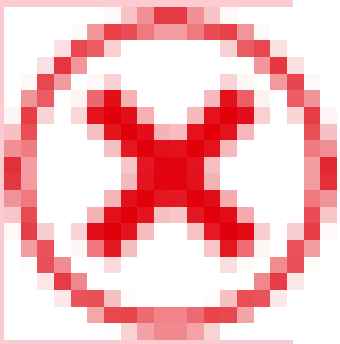
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
エクスポージャーアセスメント				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

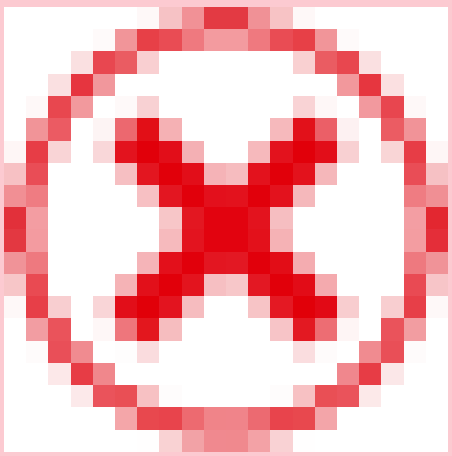
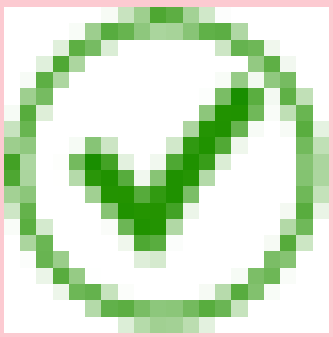
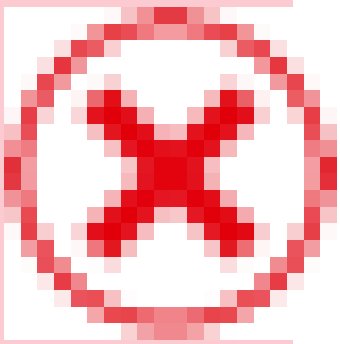
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
スキャン				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

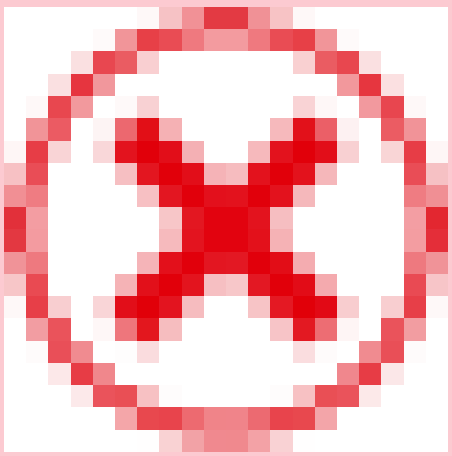
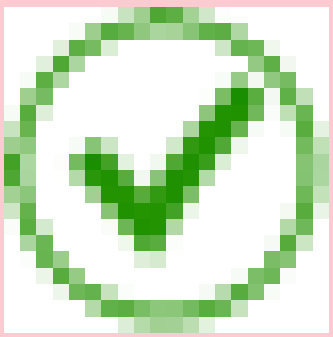
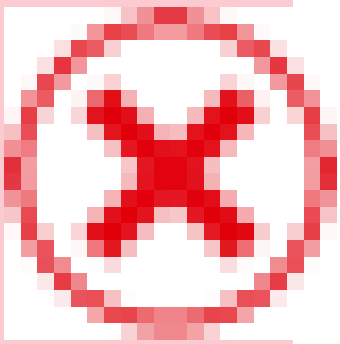
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
スキャナー				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

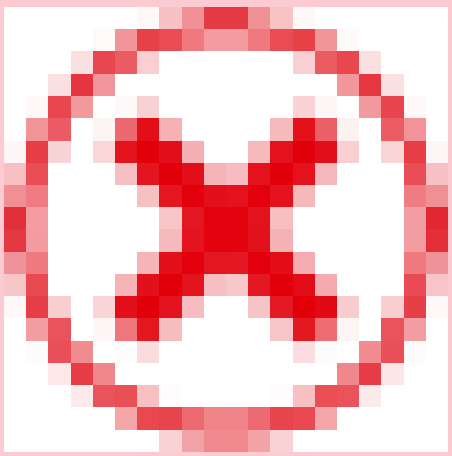
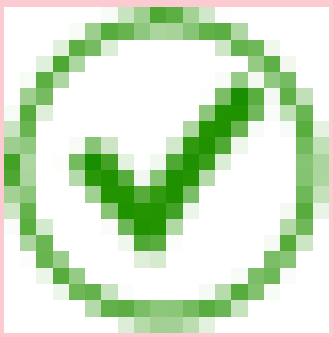
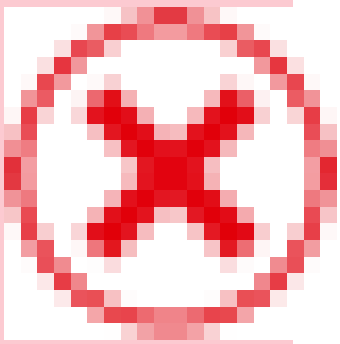
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
スキャンキュー				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

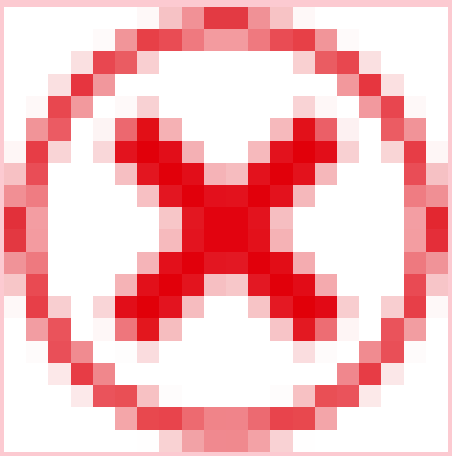
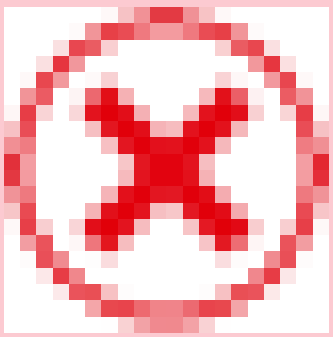
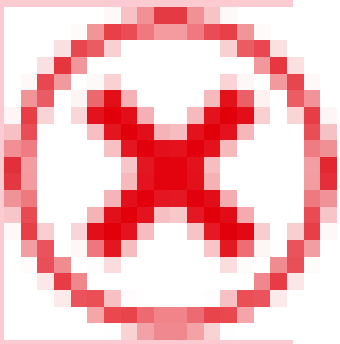
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
スキャナーレート制限				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

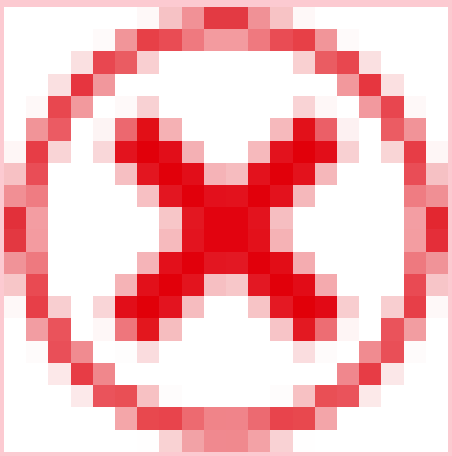
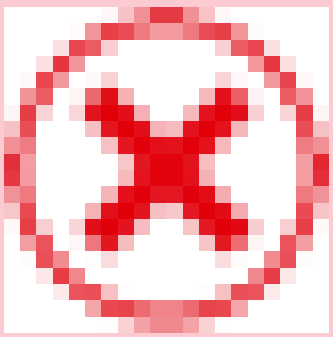
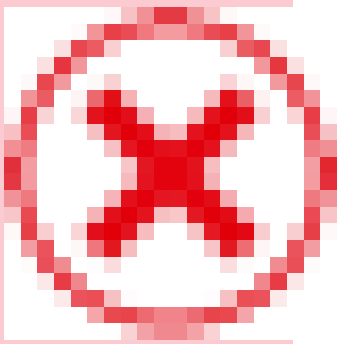
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
レート制限定義				
管理				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

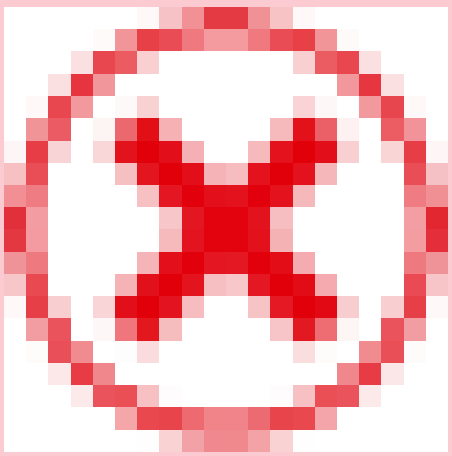
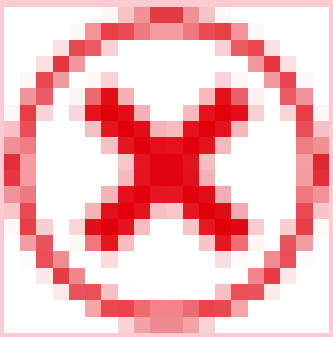
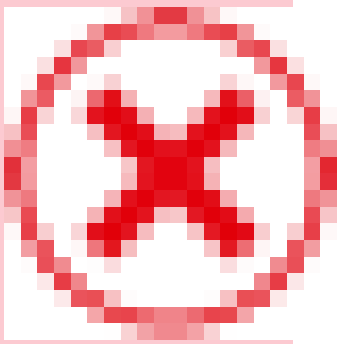
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
セットアップアシスタント				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

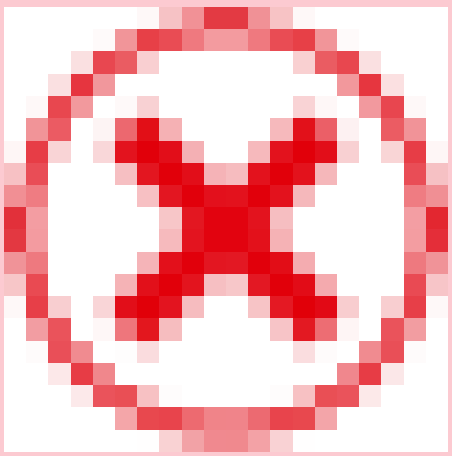
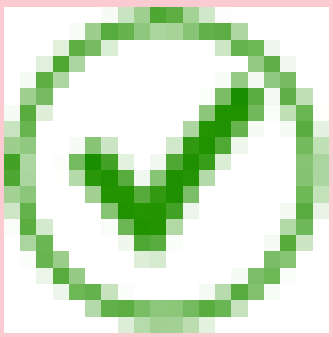
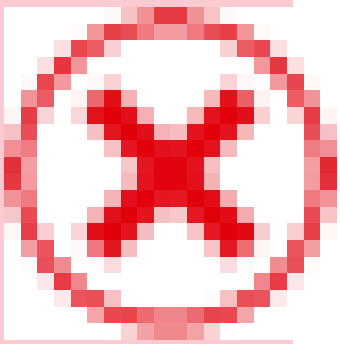
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
監視トピック				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

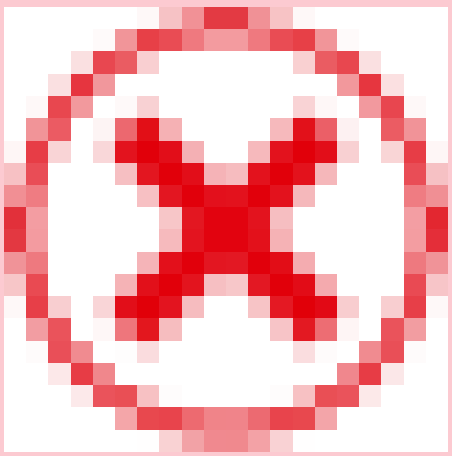
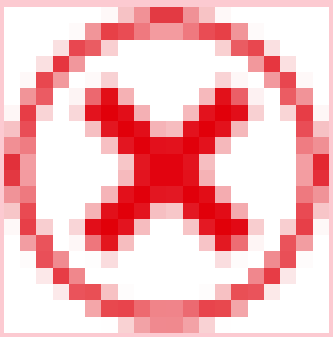
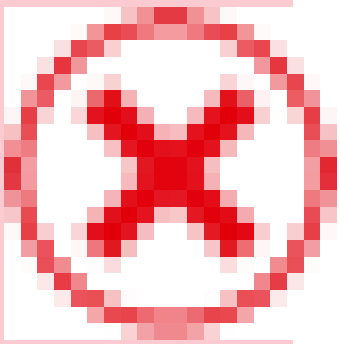
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
アサインルール				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

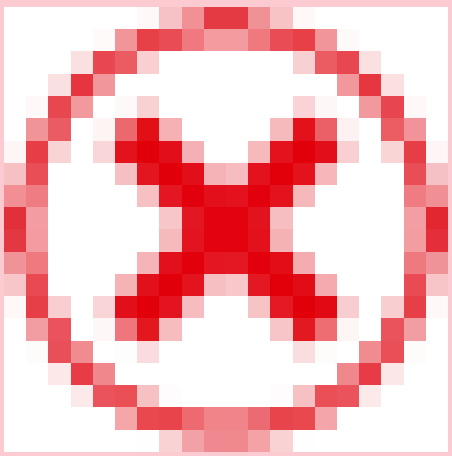
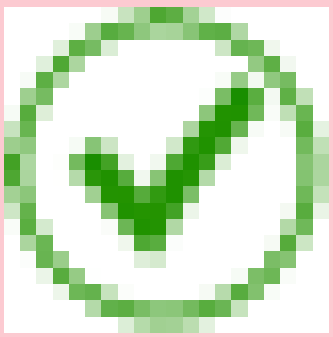
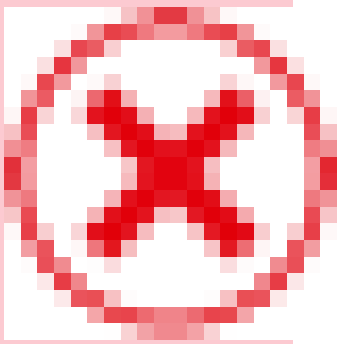
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
修復タスクルール				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

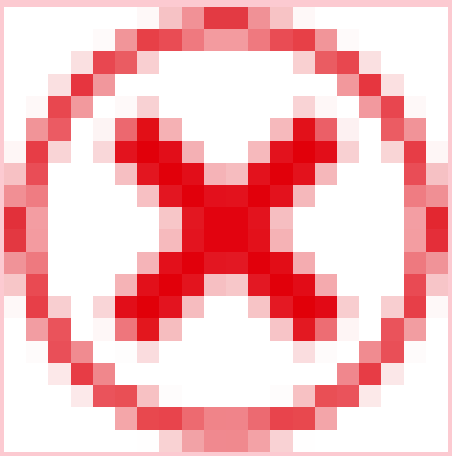
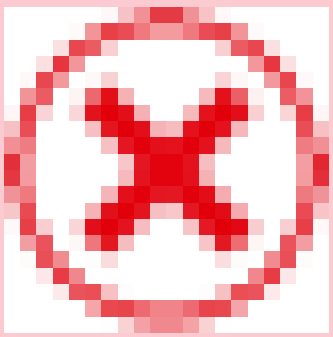
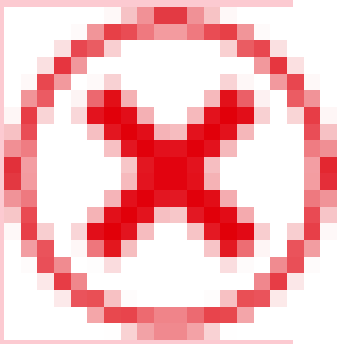
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
アサインの推奨				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

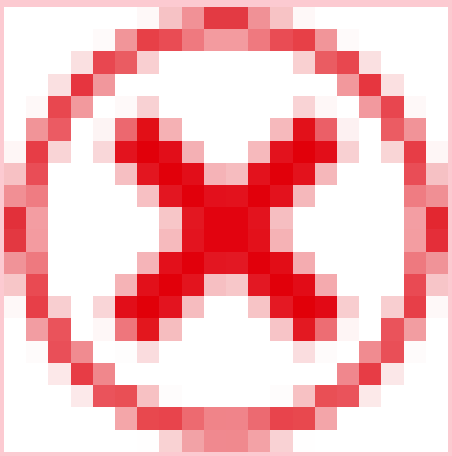
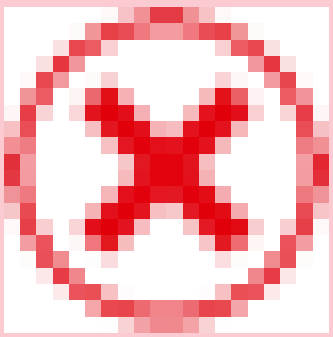
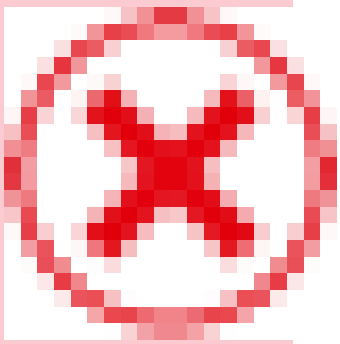
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
脆弱性算出				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

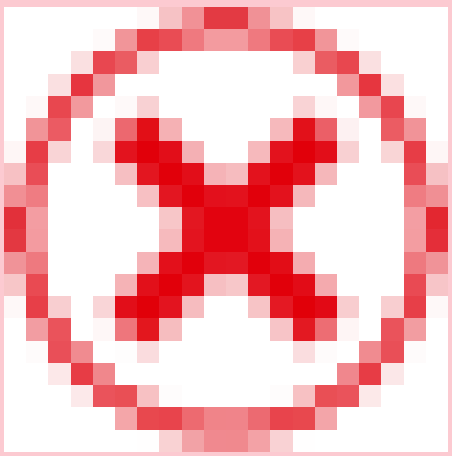
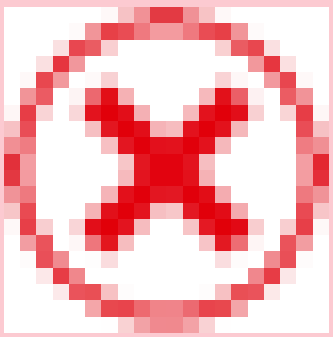
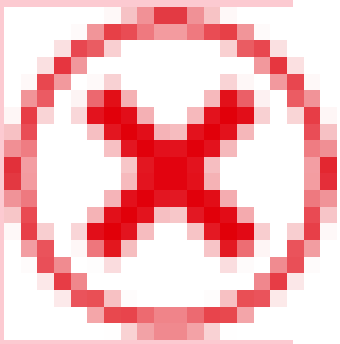
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
脆弱性ロールアップ算出				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

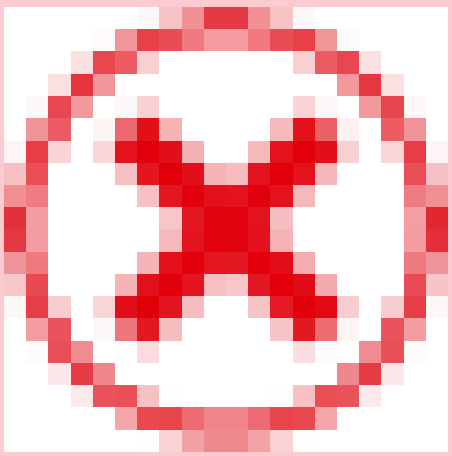
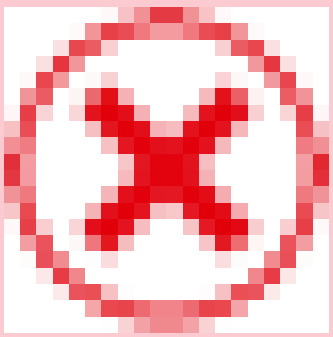
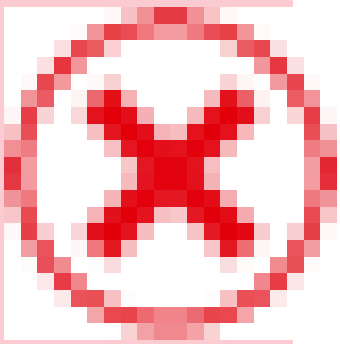
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
修復ターゲットルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

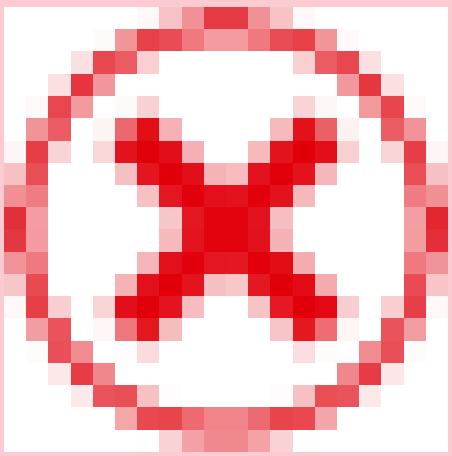
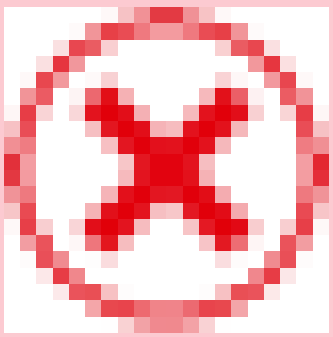
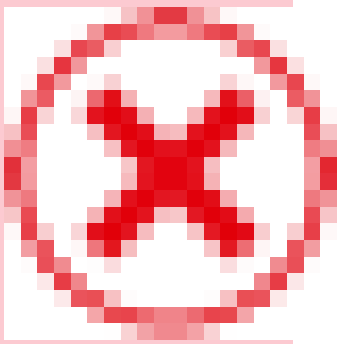
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
自動クローズ構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

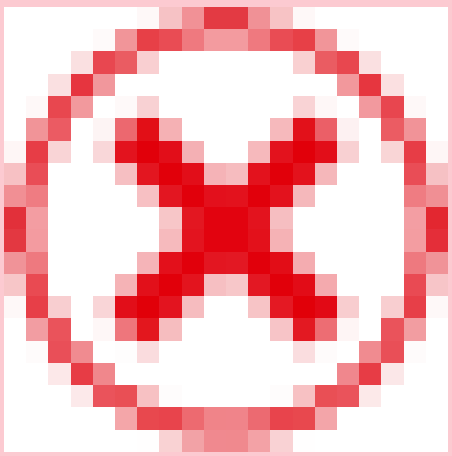
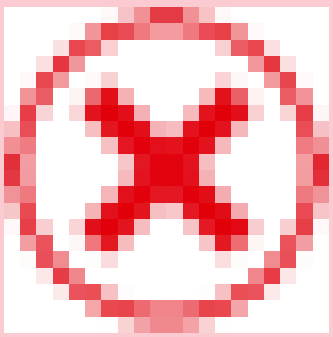
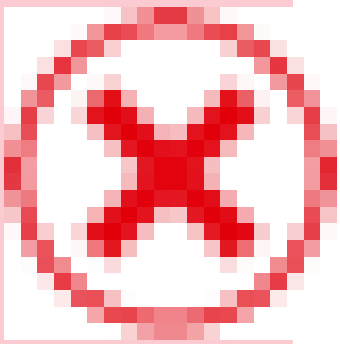
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
ルールの自動削除				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

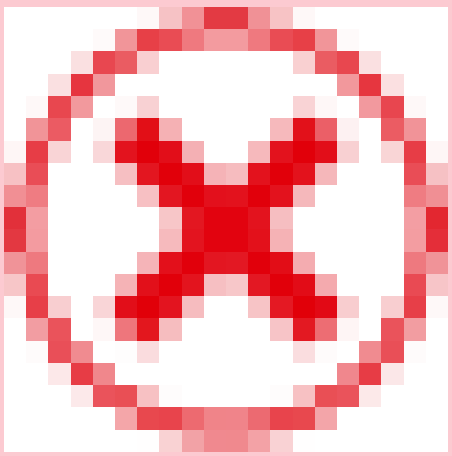
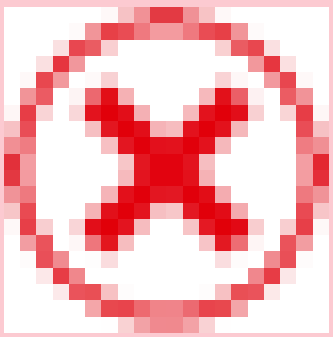
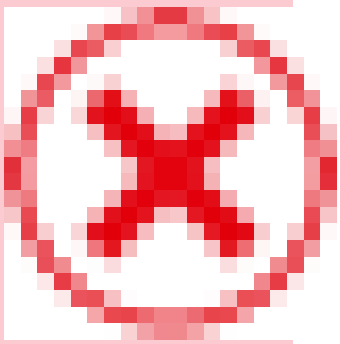
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
例外ルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

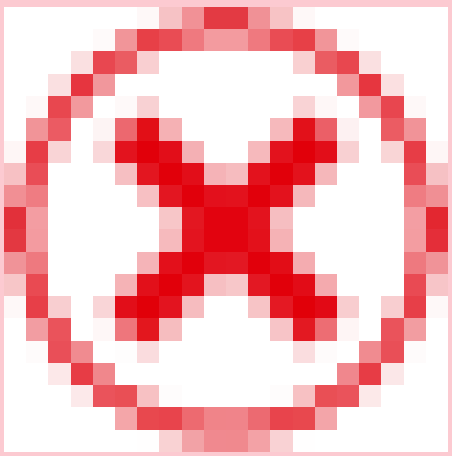
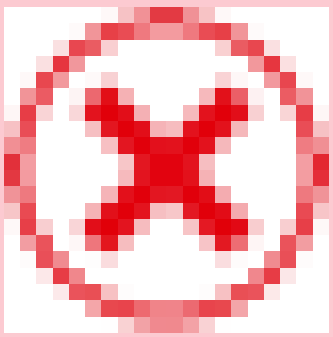
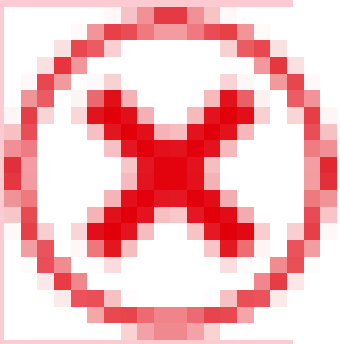
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
承認ルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

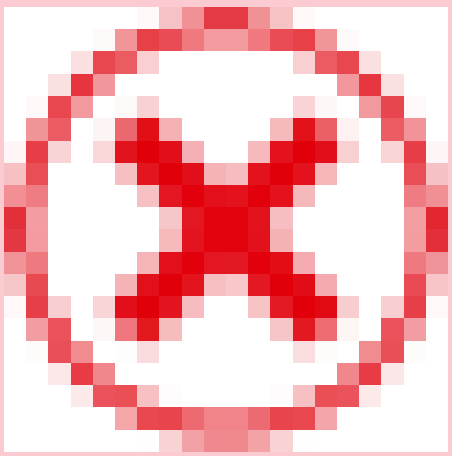
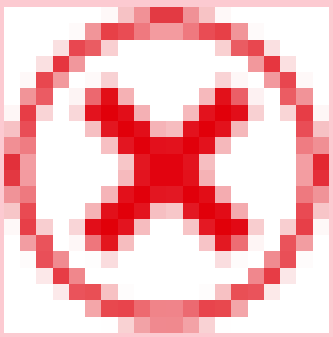
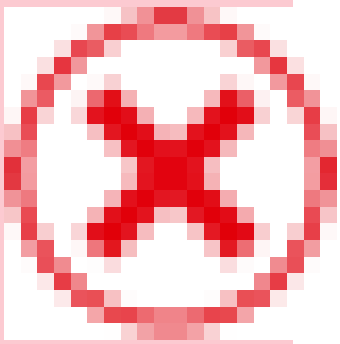
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
分類ルール				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

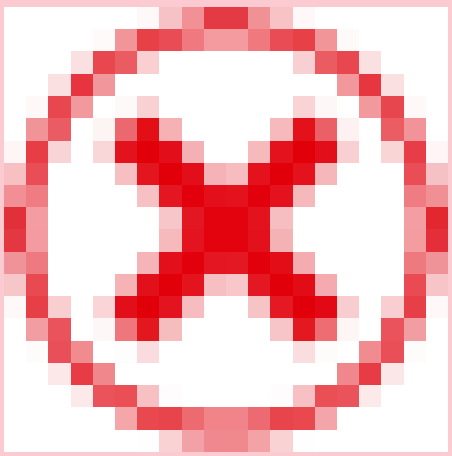
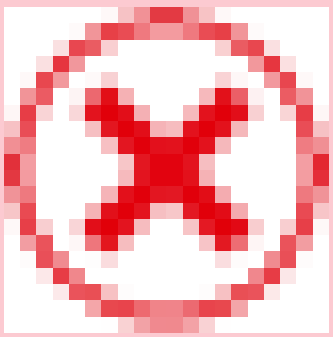
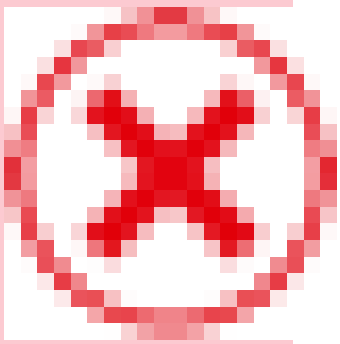
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
パフォーマンス構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

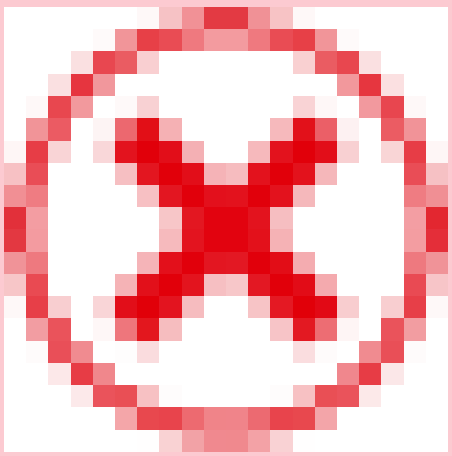
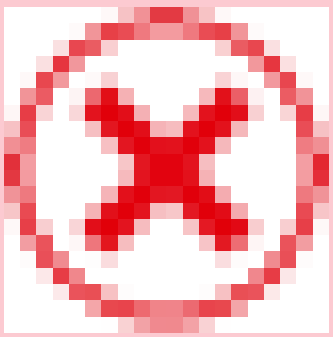
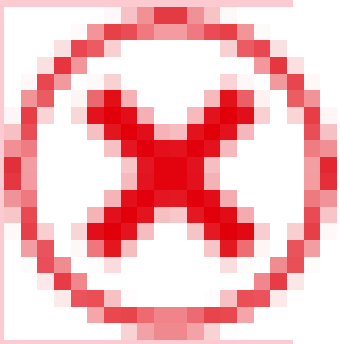
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
VI の粒度の構成				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

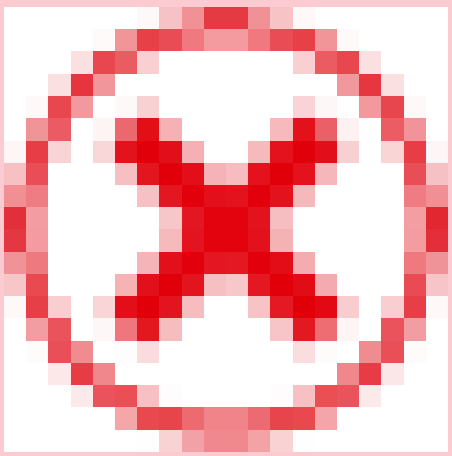
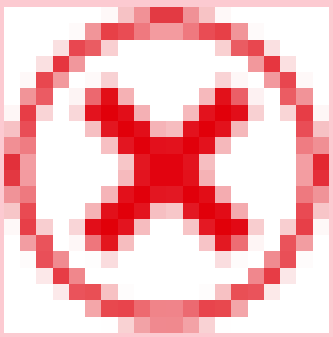
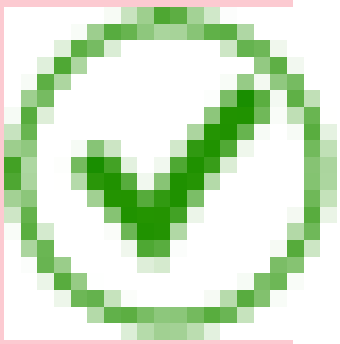
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
通知				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

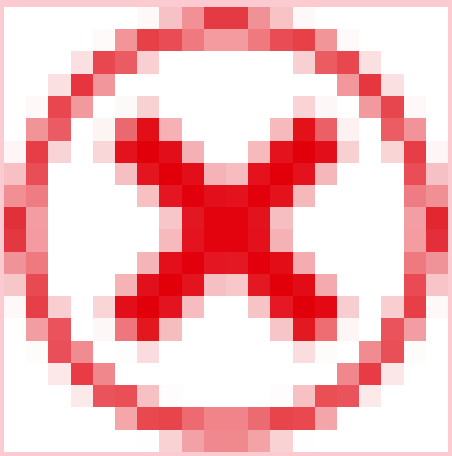
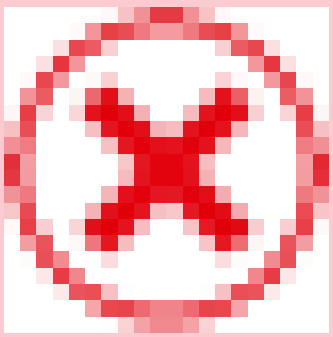
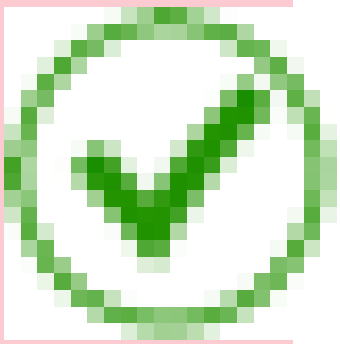
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
メールテンプレート				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

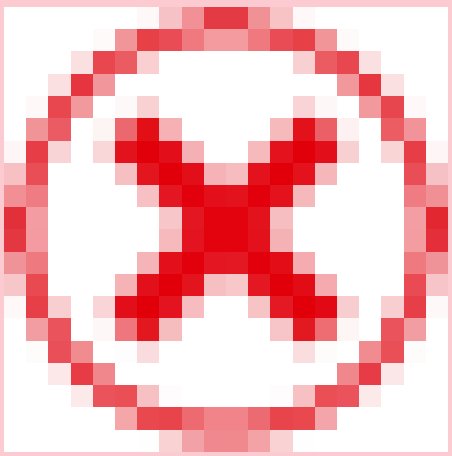
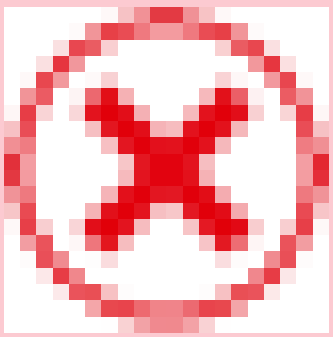
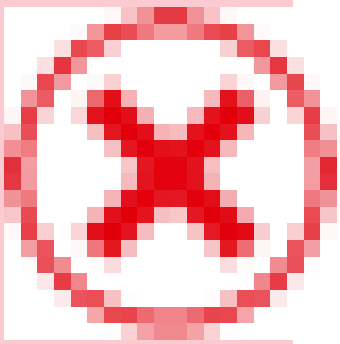
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
キューをインポート				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

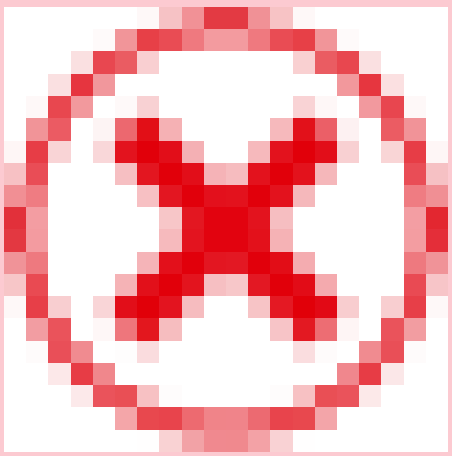
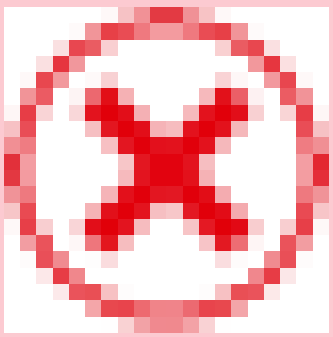
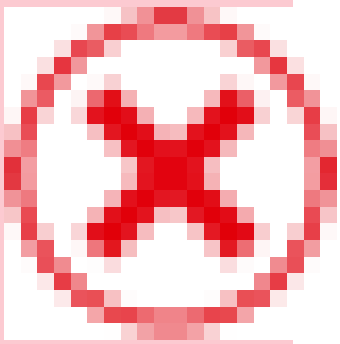
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
統合				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

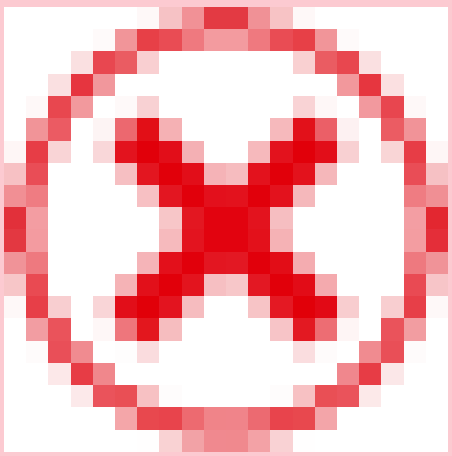
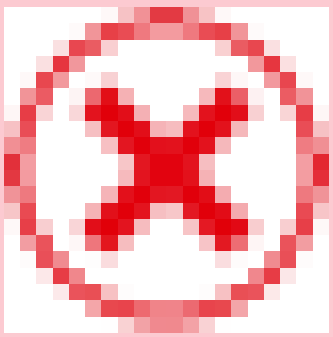
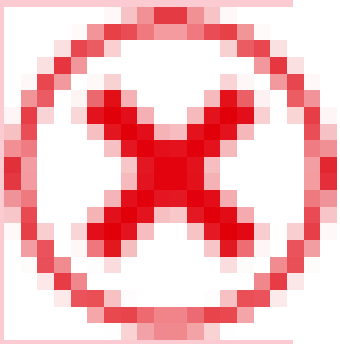
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
SLA 定義				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

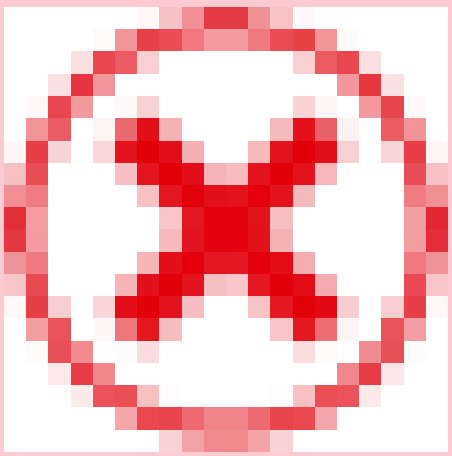
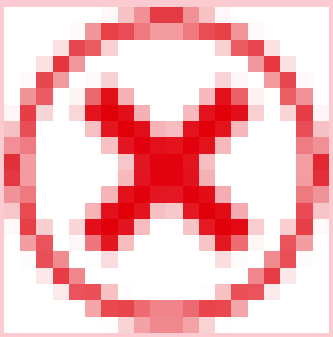
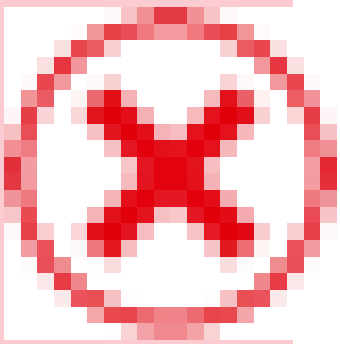
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
SAM NVD の構成				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

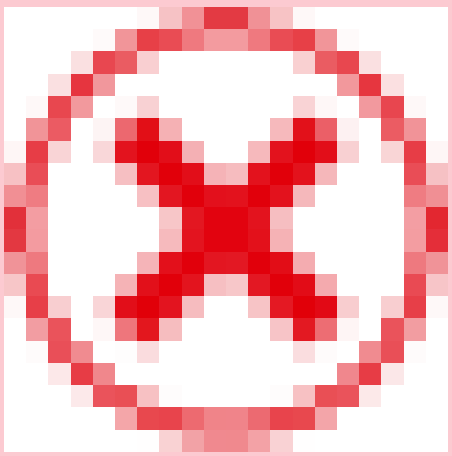
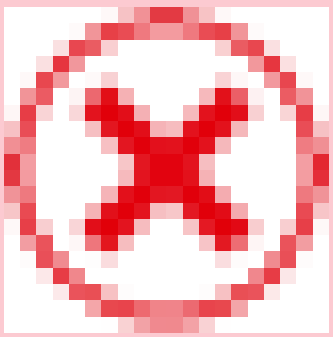
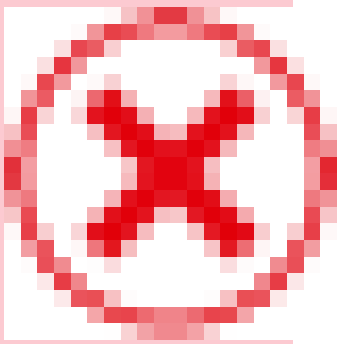
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
正規化された重大度マップ				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

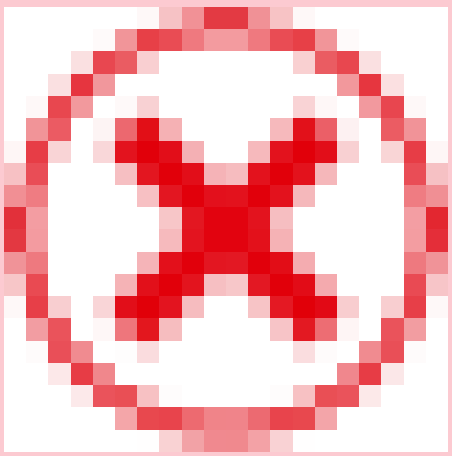
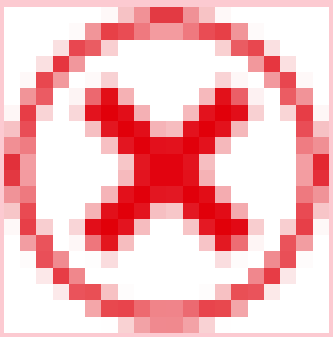
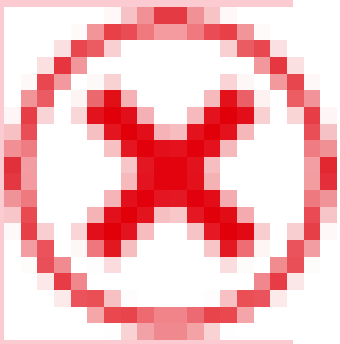
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
スキャン範囲構成				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

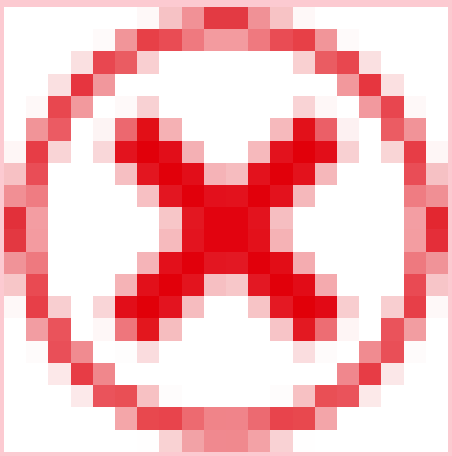
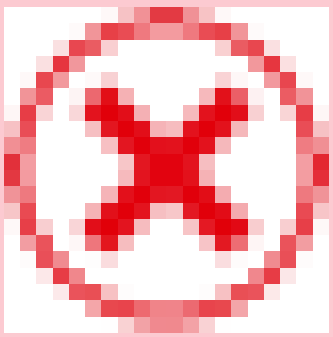
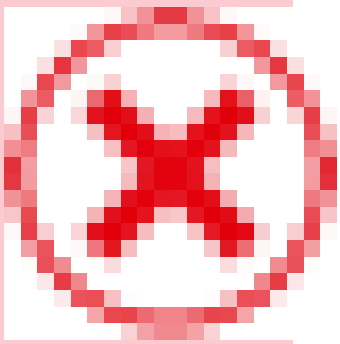
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
例外管理				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

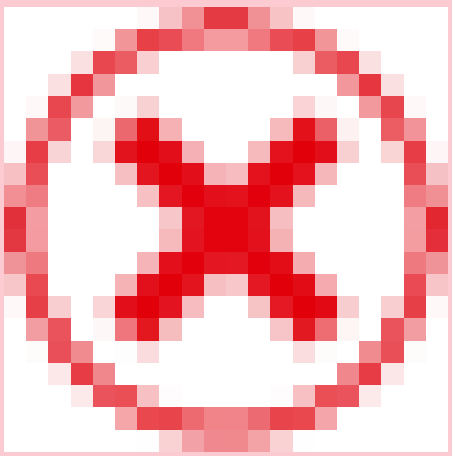
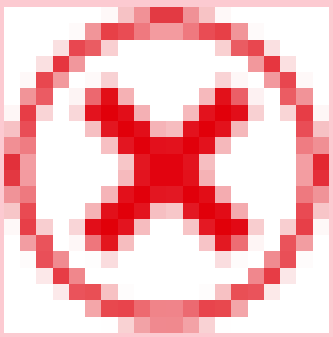
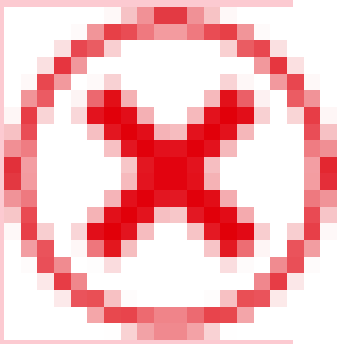
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
使用状況レポート				
診断				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_notifications、sn_vul.

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

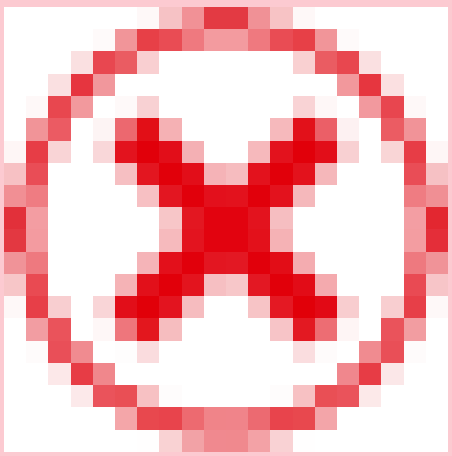
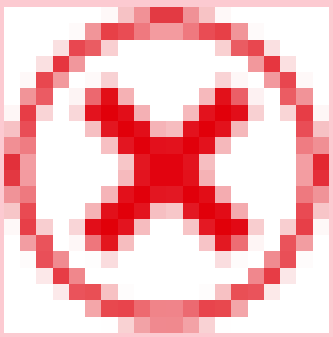
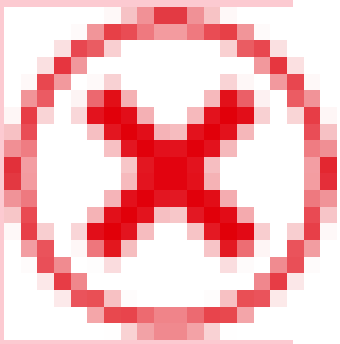
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul.man
チェック				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.r

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

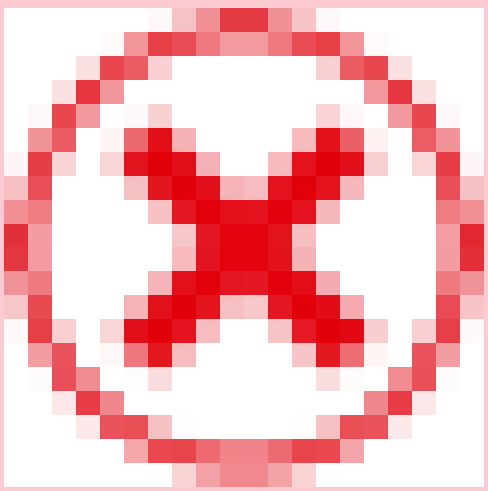
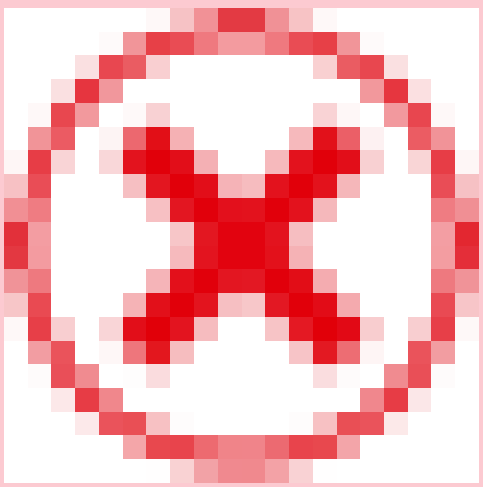
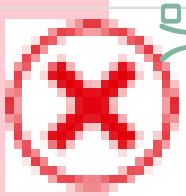
sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	n_vul.re
(メインアプリグループ)				
CISO ダッシュボード				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

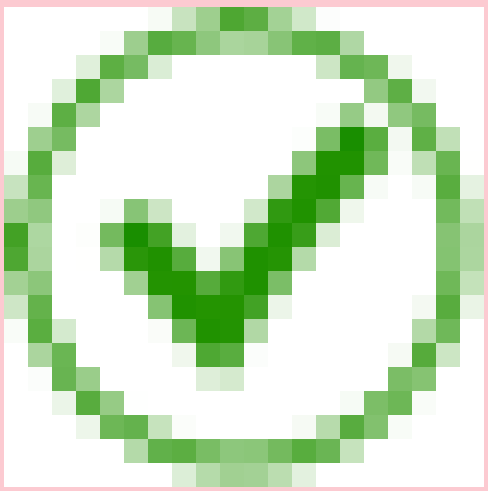
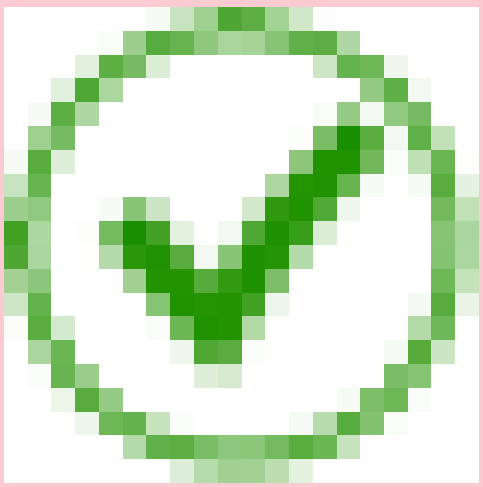
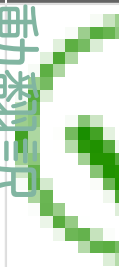
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
修復の概要				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
脆弱性マネージャーのワークスペース	✗	✗	✗	✗

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

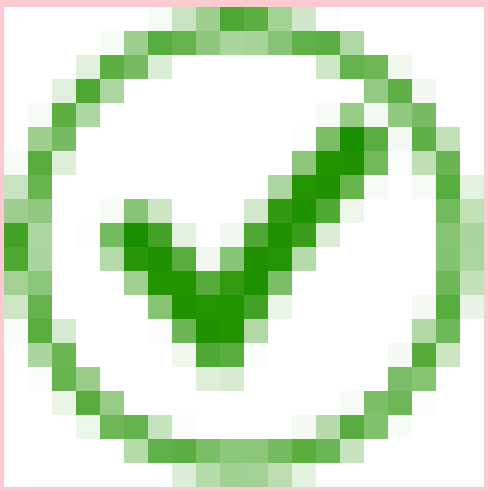
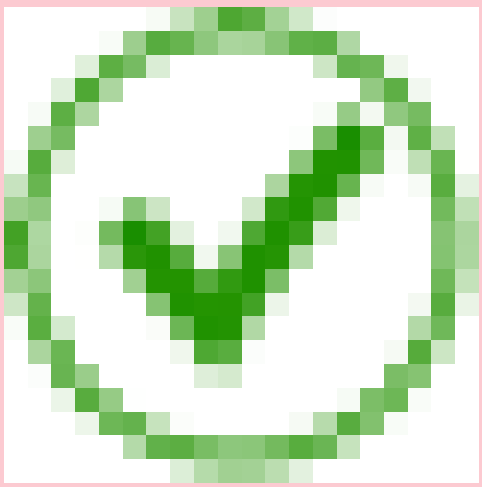
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	sn_vul.re
概要				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

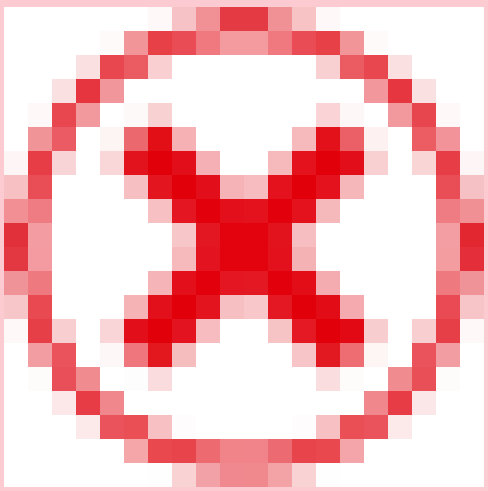
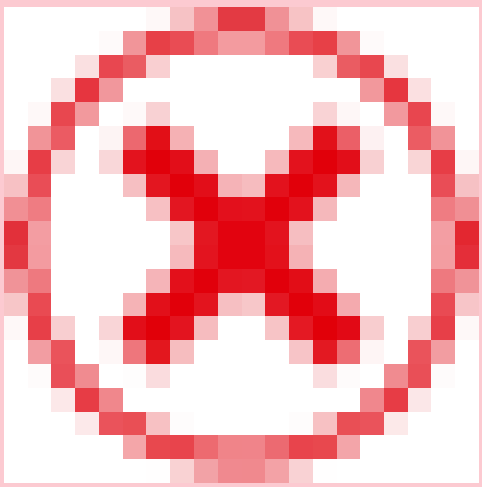
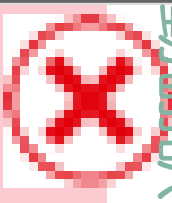
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
IT 修復ワークスペース				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

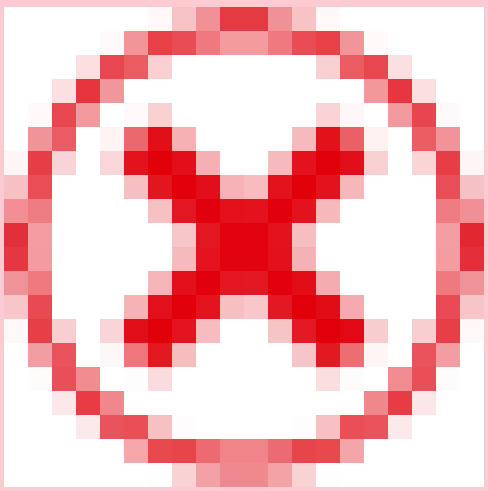
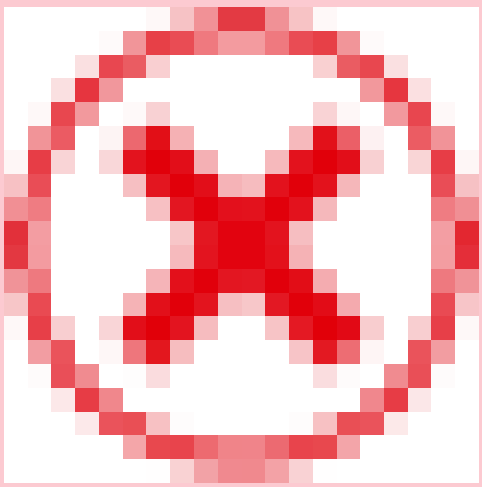
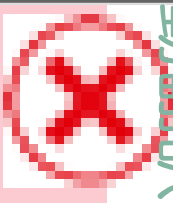
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	sn_vul.re
承認者の概要				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

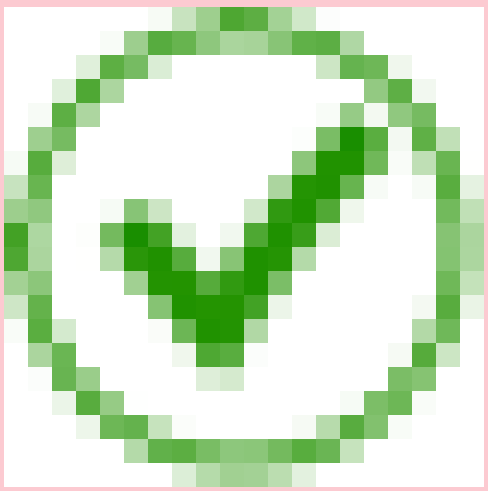
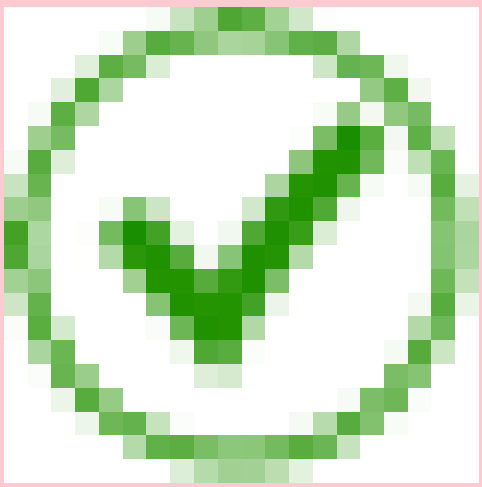
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	sn_vul.re
概要				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

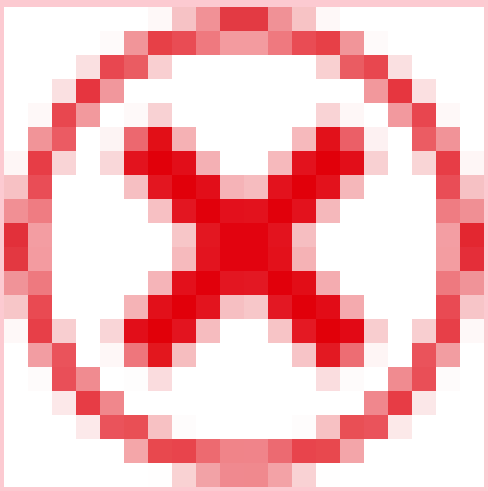
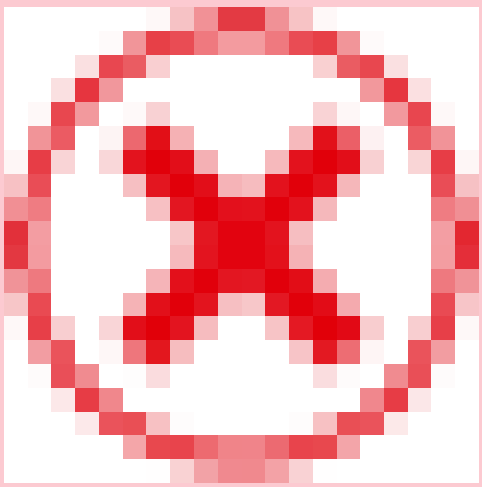
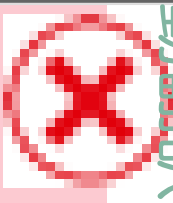
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
自分の承認				
修復タスク				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

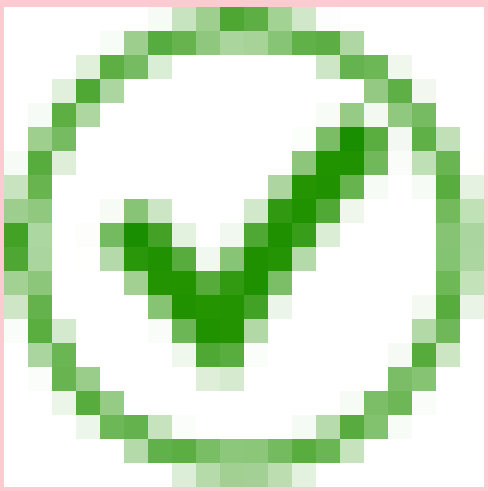
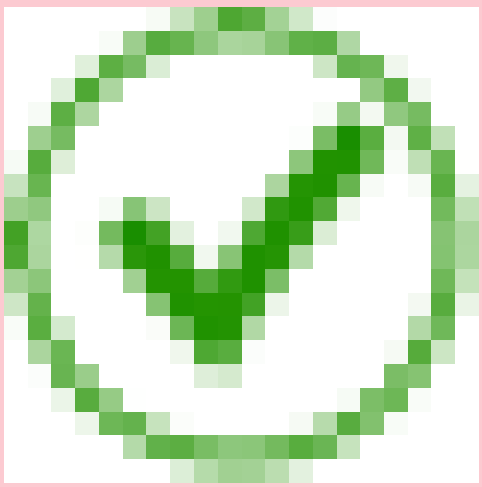
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	sn_vul.re
有効				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

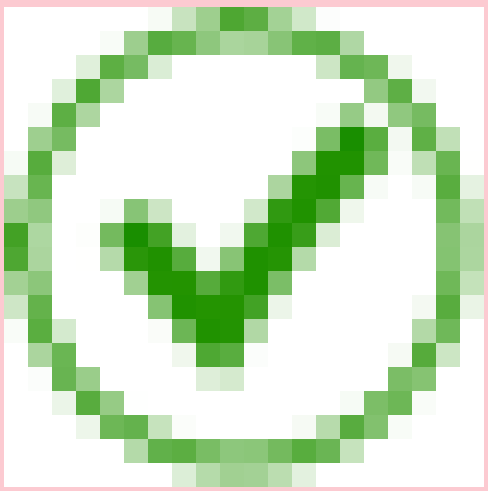
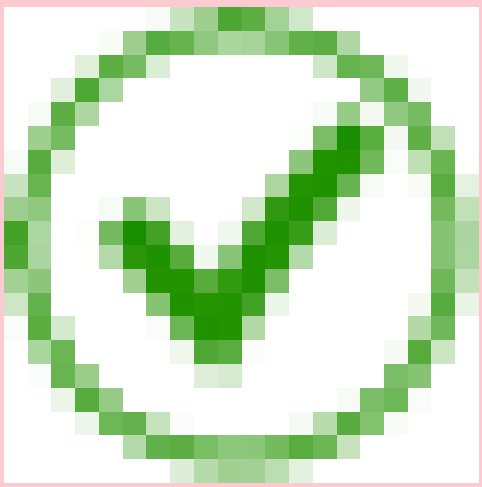
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
自分にアサイン済み				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

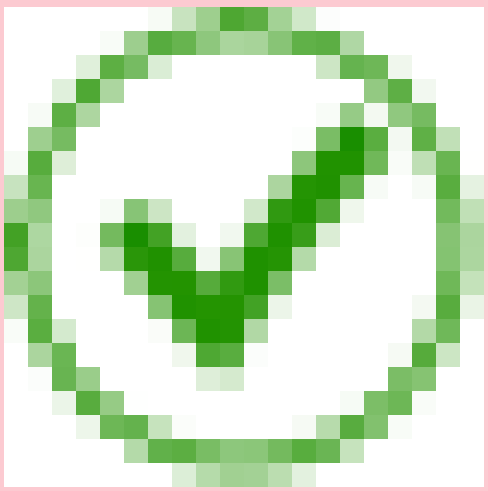
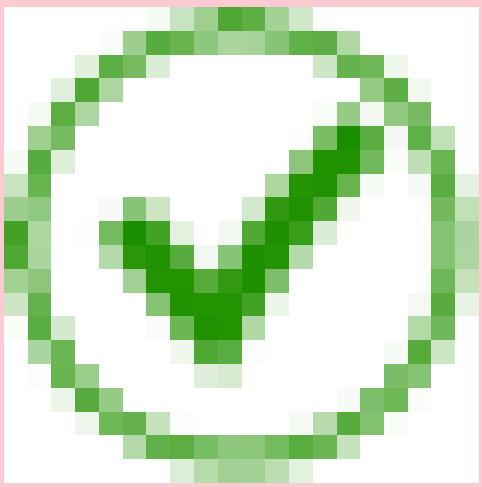
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
所属グループにアサイン済み				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

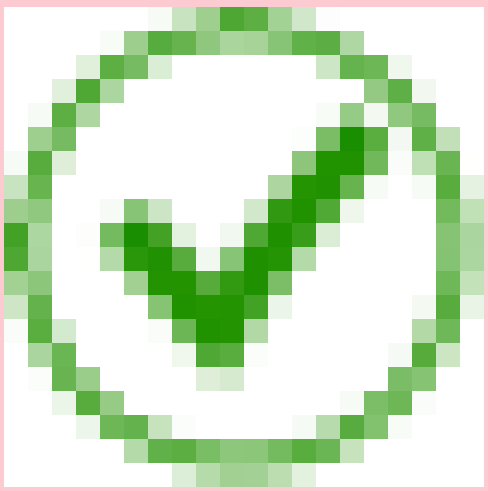
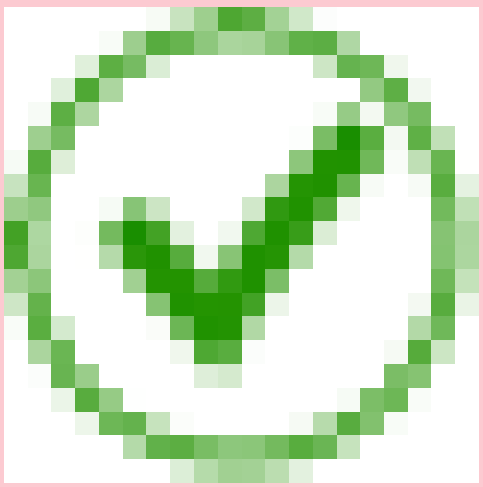
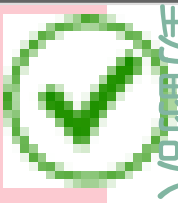
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	sn_vul.re
すべて				

脆弱性一致アイテム

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

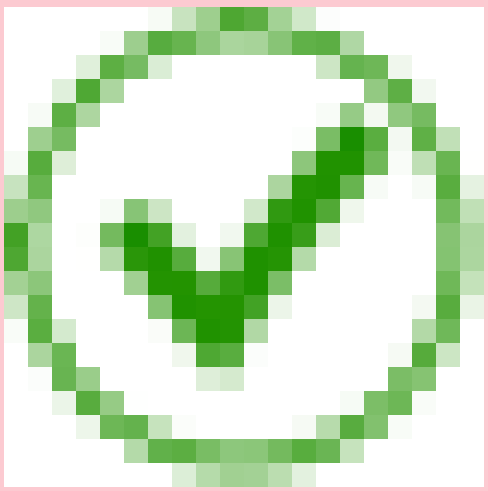
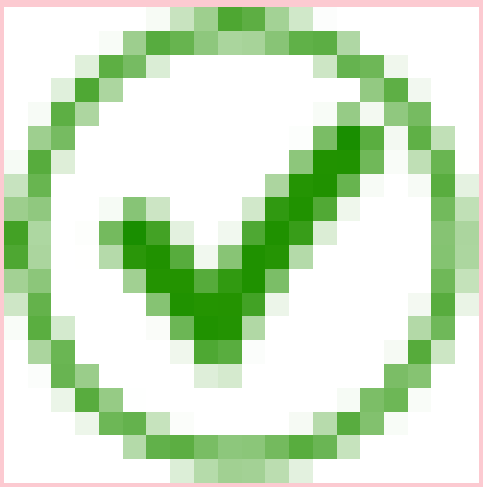
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	sn_vul.re
重大なリスク				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

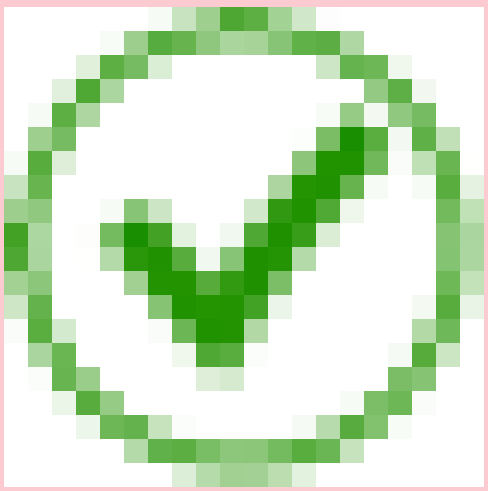
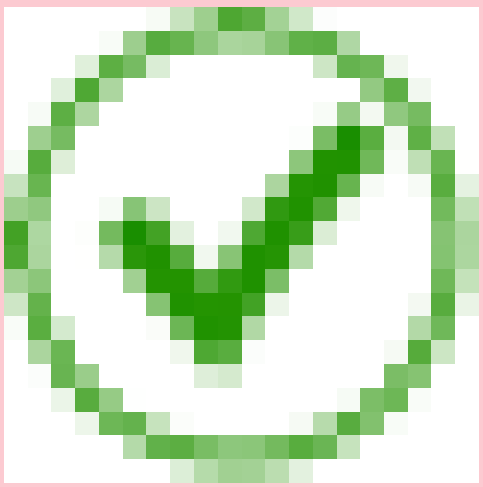
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
高リスク				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

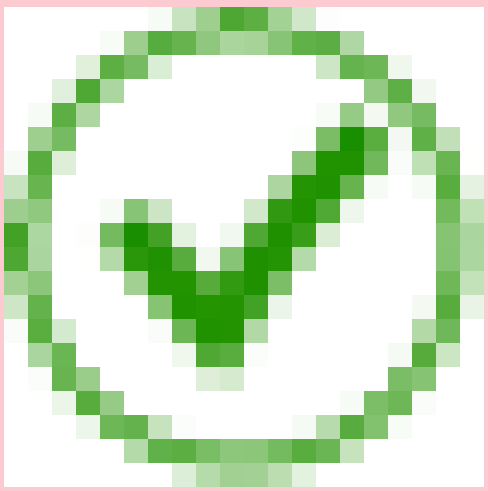
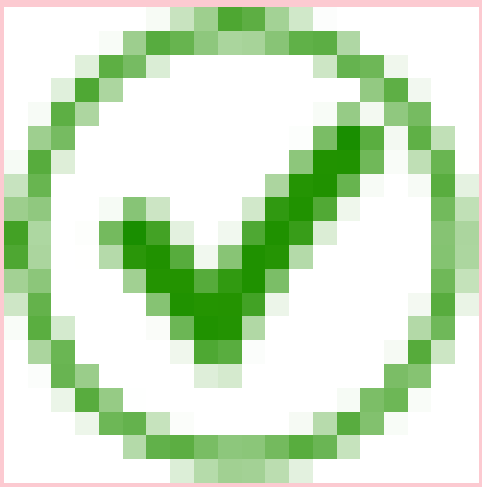
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
エクスプロイト可能				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

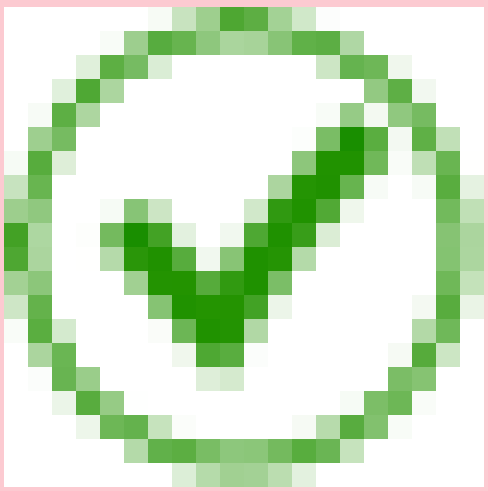
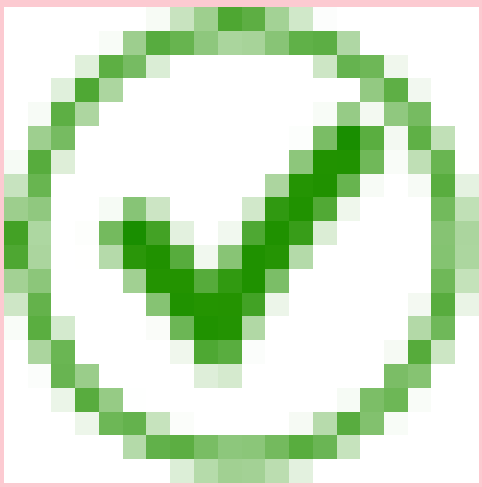
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	sn_vul.re
該当 CI 確認中				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

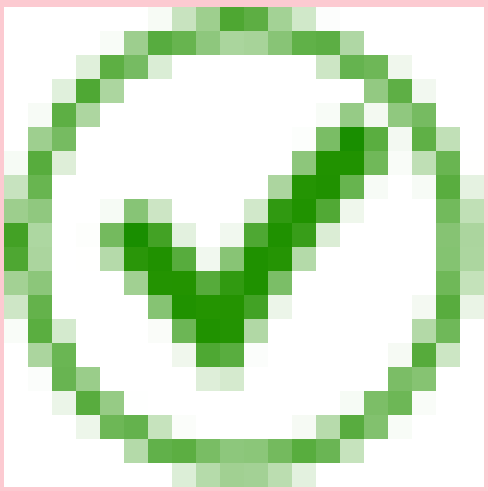
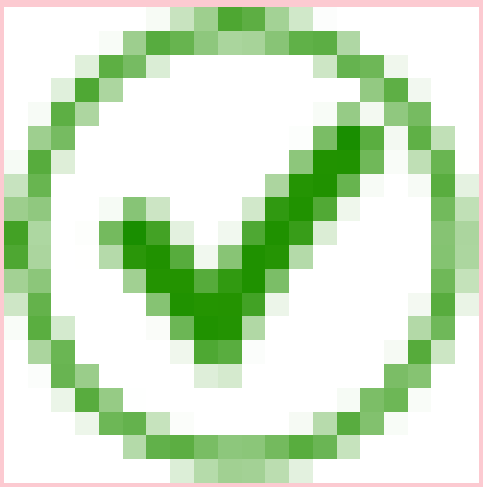
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	sn_vul.re
CI 不明				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

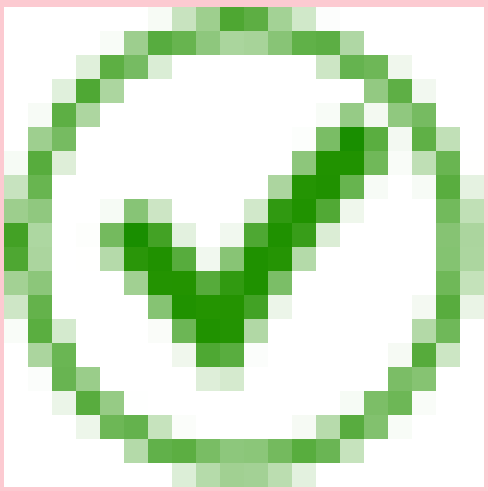
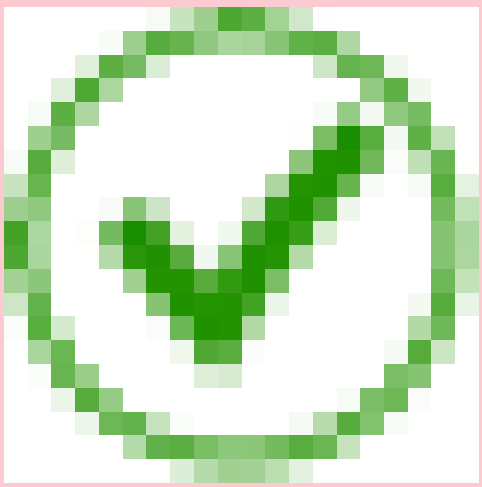
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	sn_vul.re
過去 90 日以内				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
91 日以上前	✓	✓	✓	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

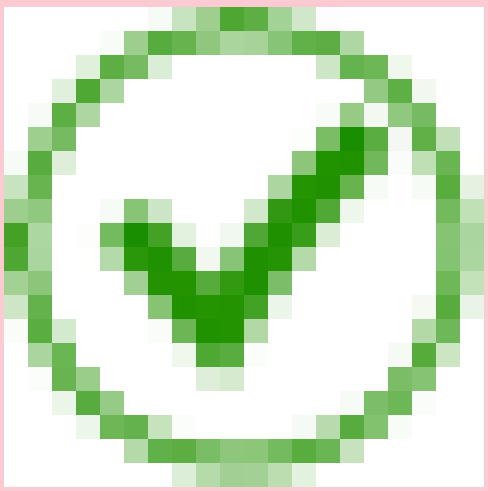
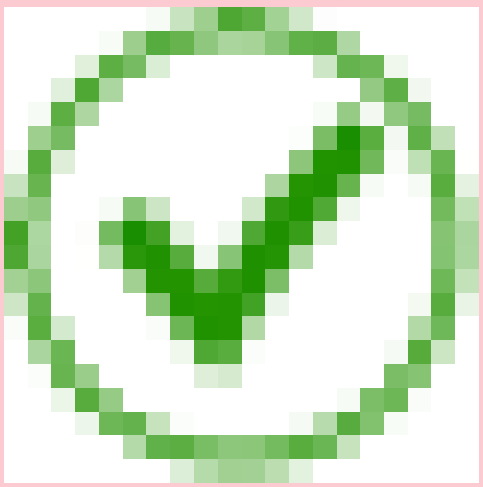
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
未アサイン				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

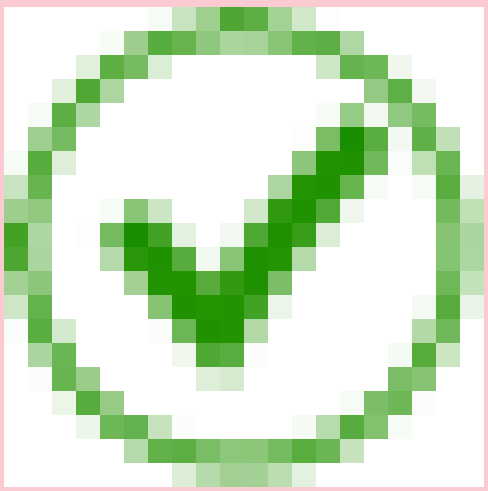
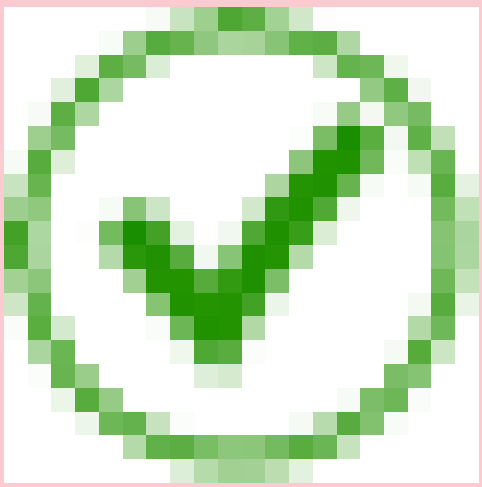
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	sn_vul.re
修復タスク未割り当て				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

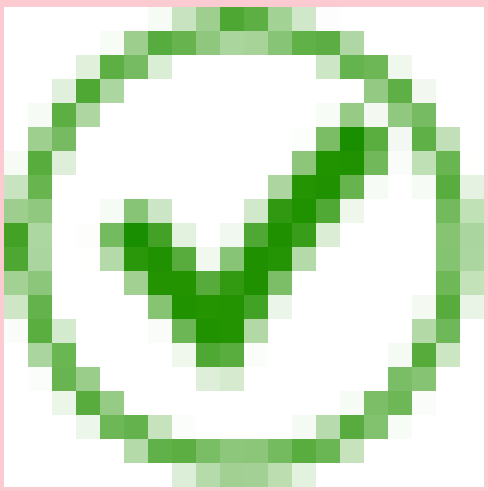
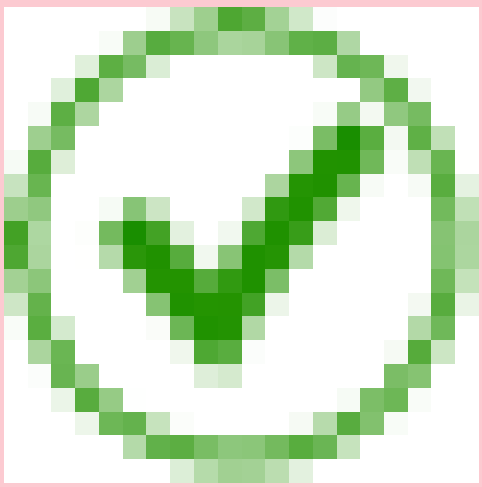
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
廃止				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

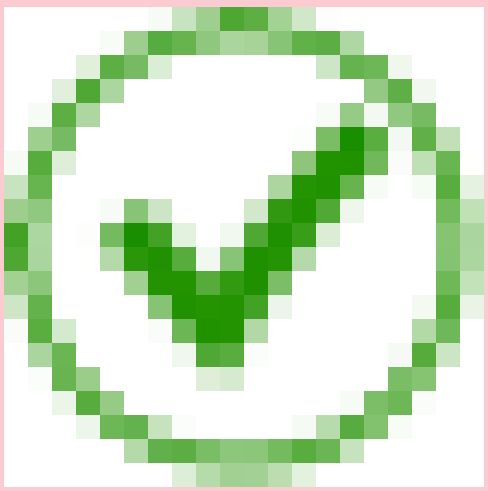
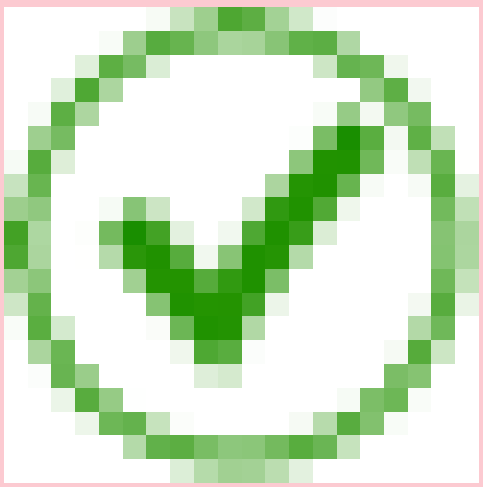
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
複数の保留				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

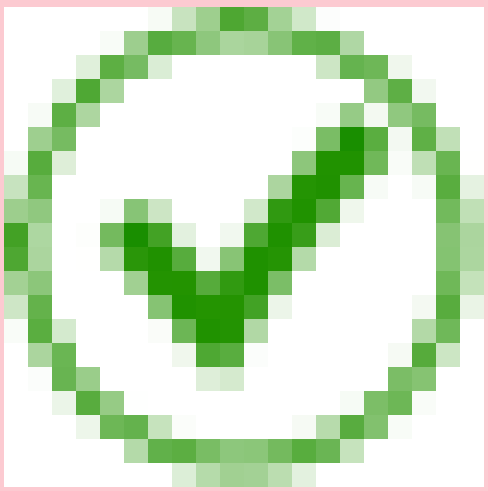
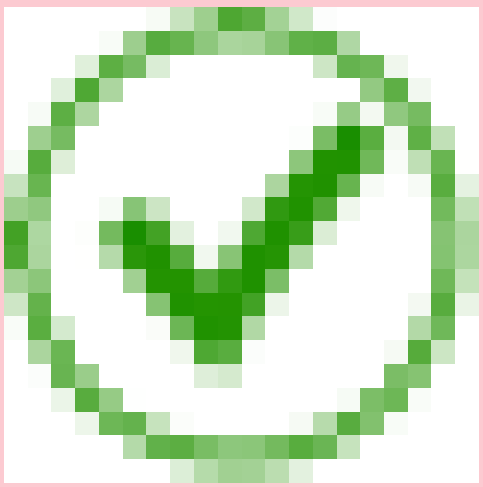
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
すべて				

ソリューション

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

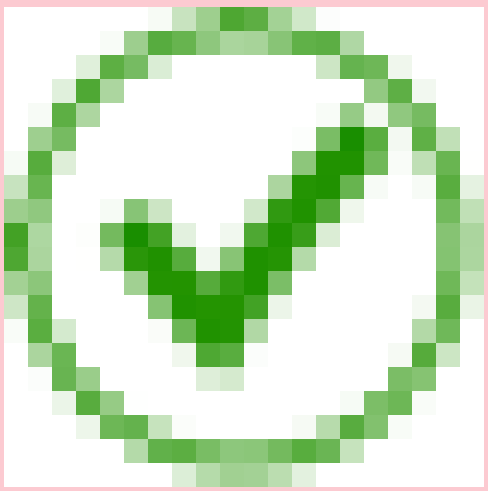
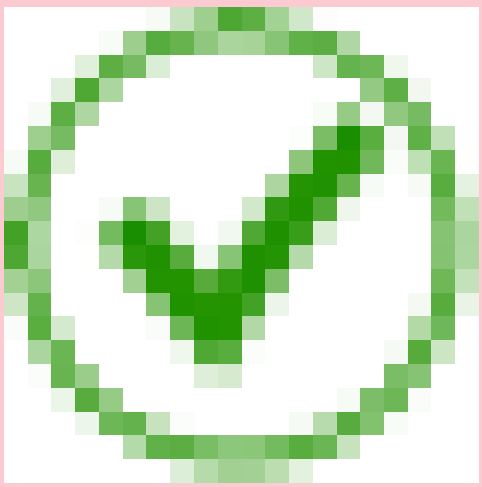
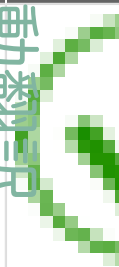
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
すべて				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

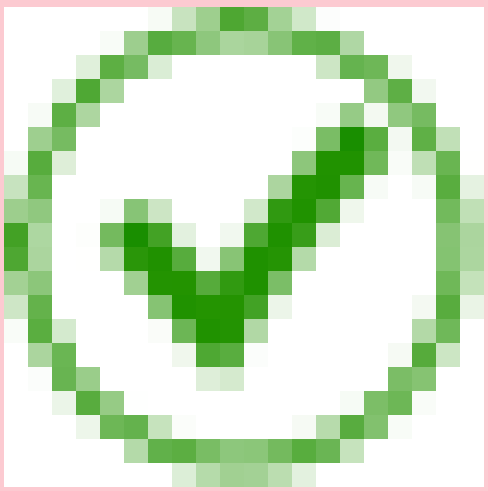
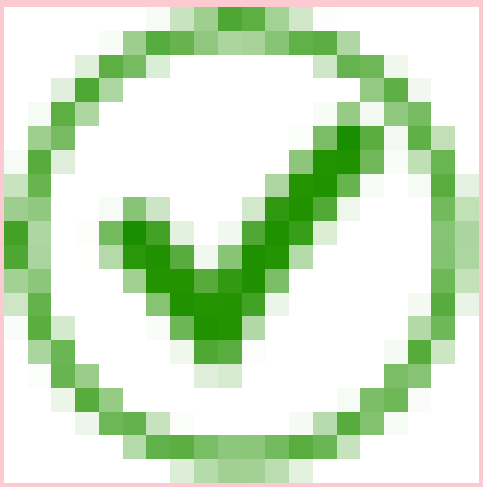
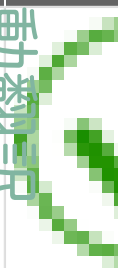
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
最高優先度				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

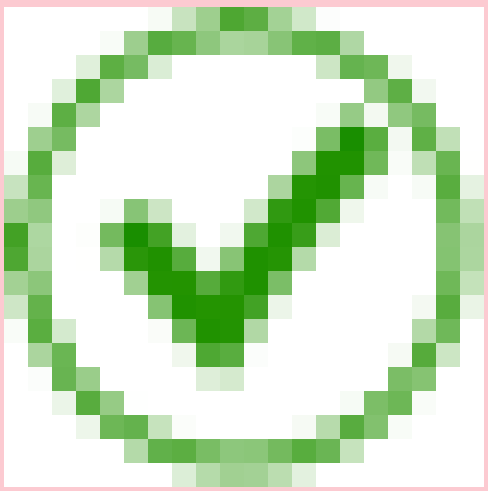
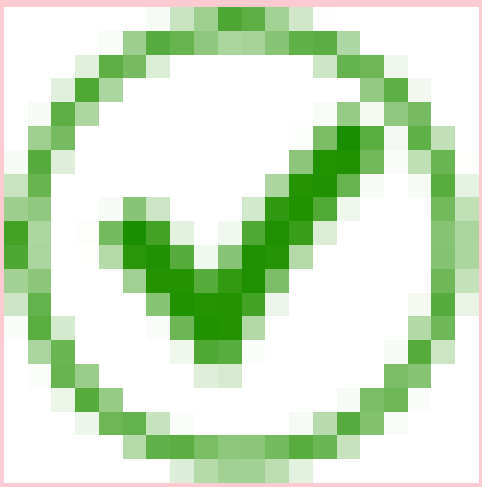
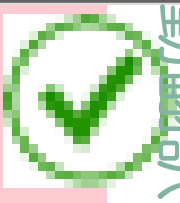
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
脆弱性一致アイテムを使用				

ライブラリ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

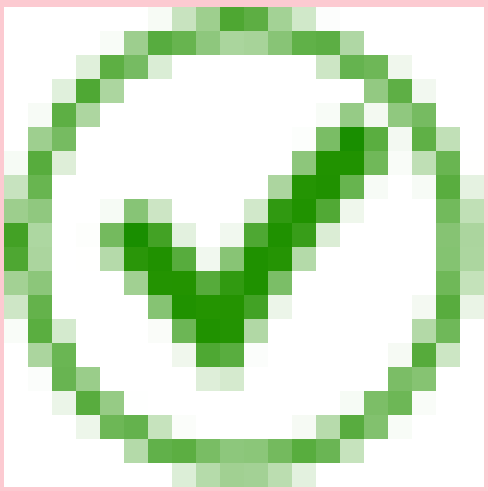
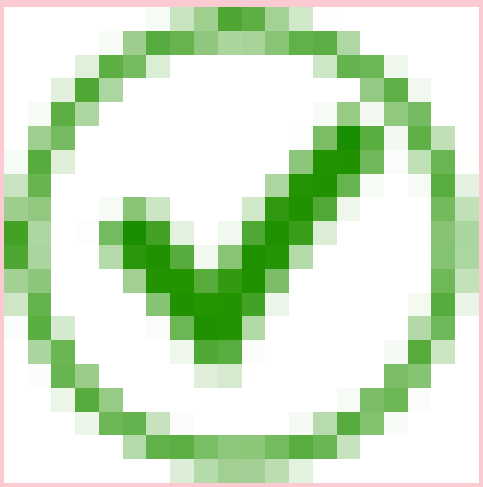
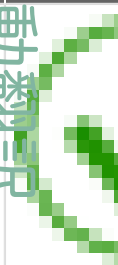
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
NVD				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

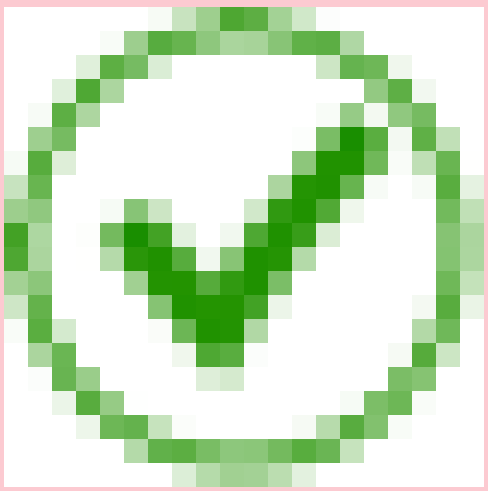
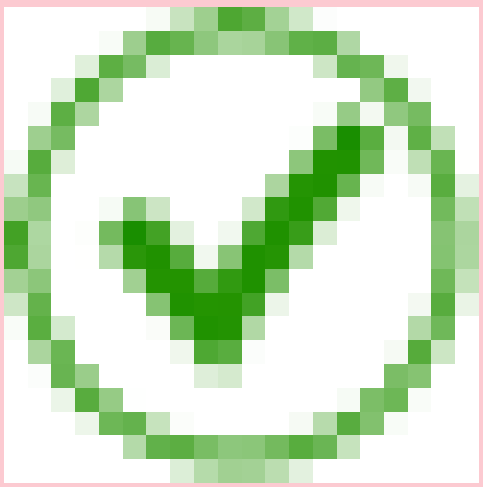
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
CWE				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

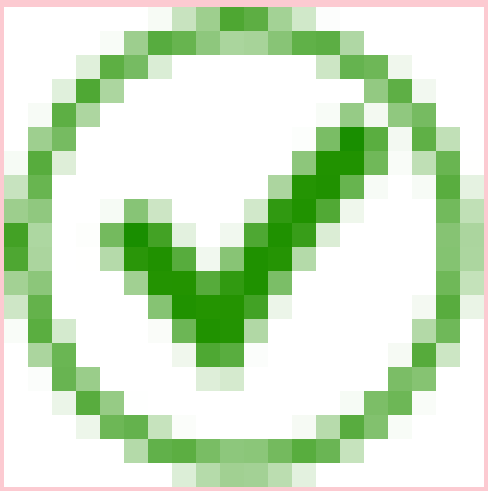
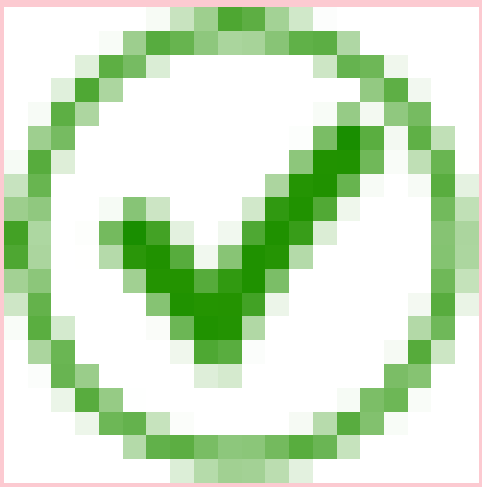
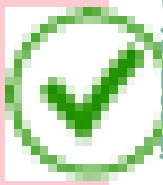
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
サードパーティ				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

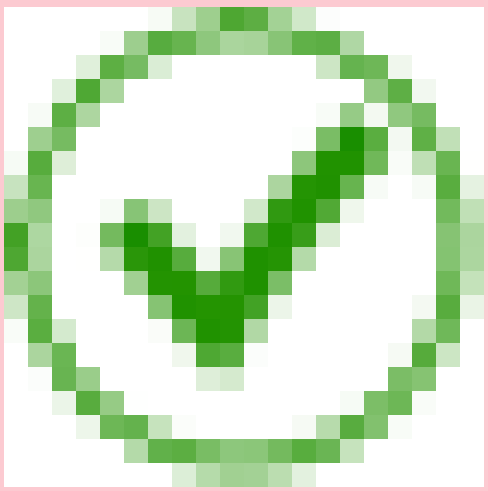
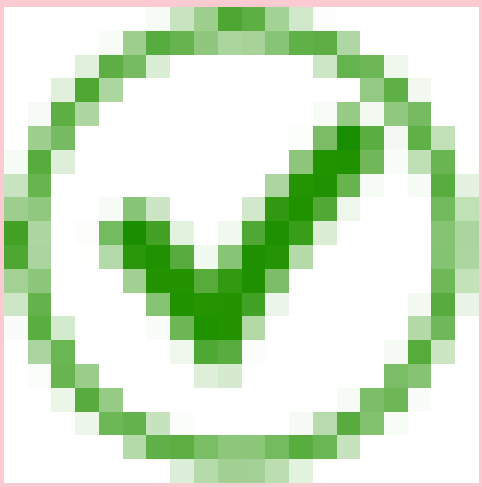
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
脆弱なソフトウェア				
脆弱性スキャン				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
エクスポージャーアセスメント	✗	✗	✗	✗

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

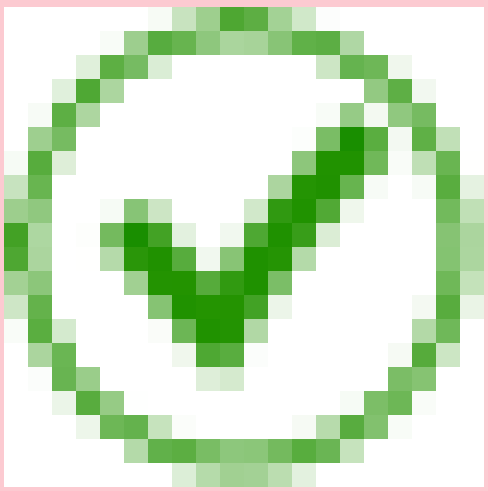
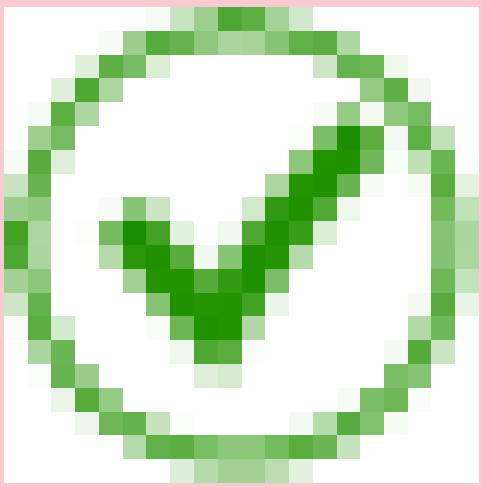
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
スキャン				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

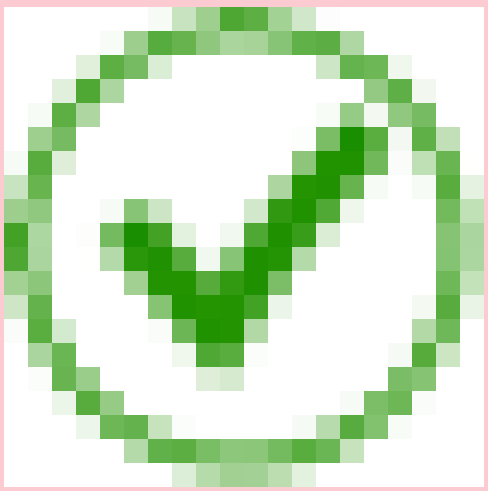
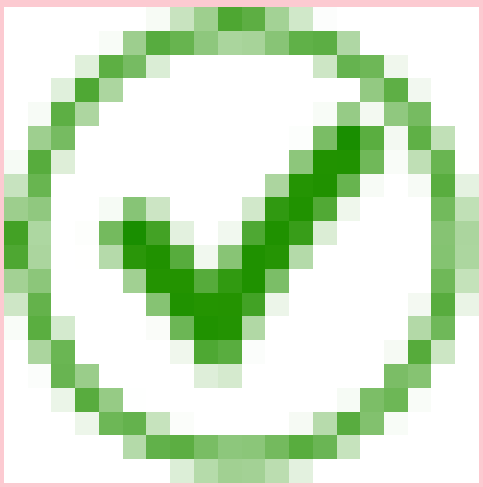
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
スキャナー				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

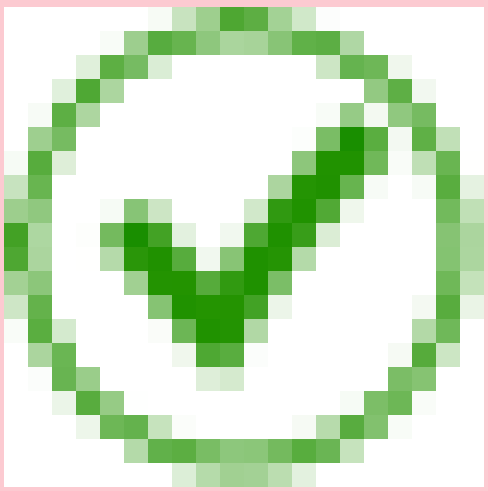
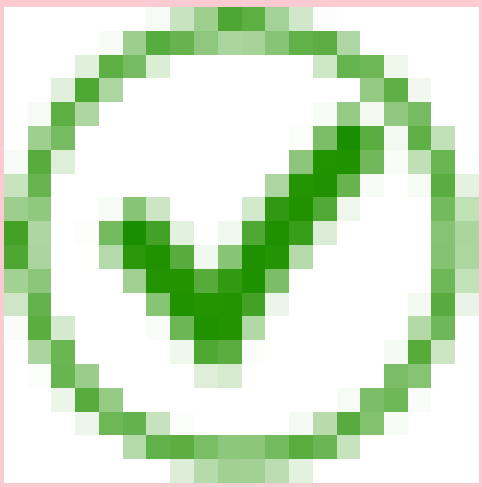
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	sn_vul.re
スキャンキュー				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

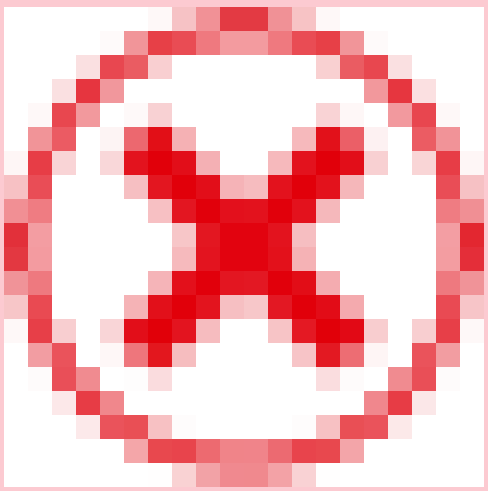
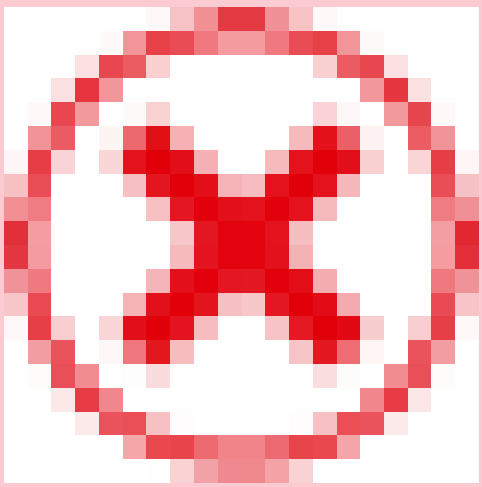
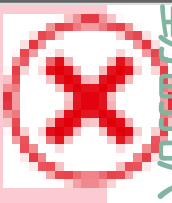
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
スキャナーレート制限				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

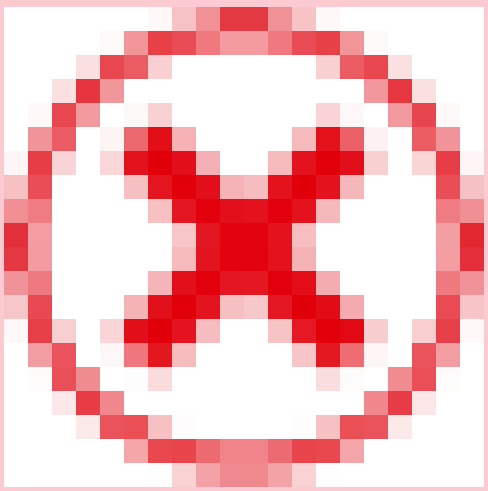
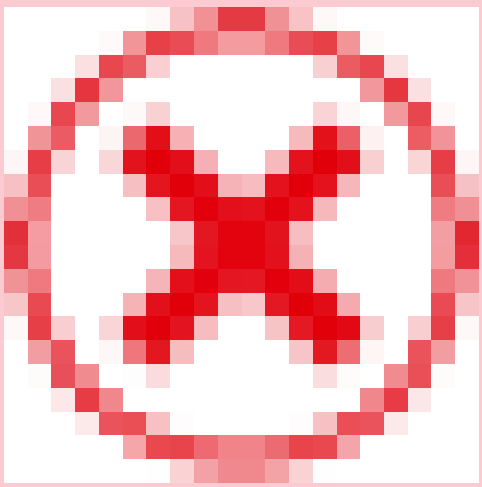
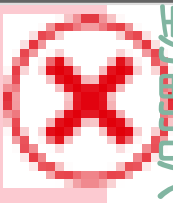
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
レート制限定義				
管理				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

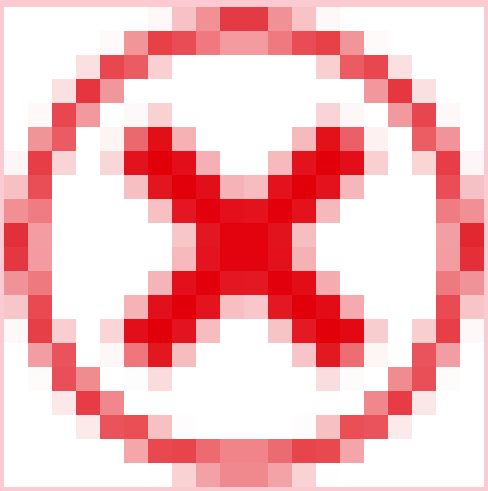
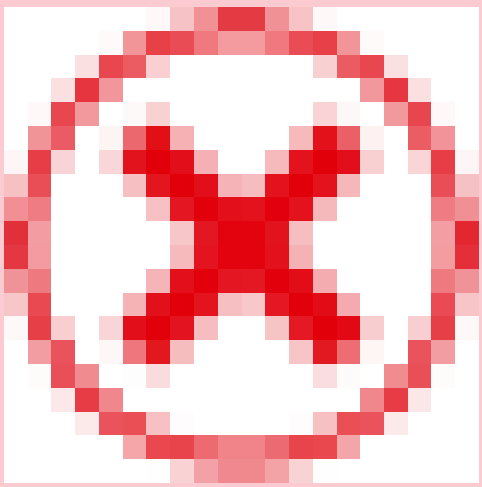
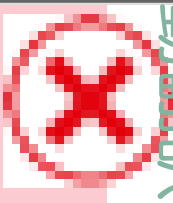
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
セットアップアシスタント				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

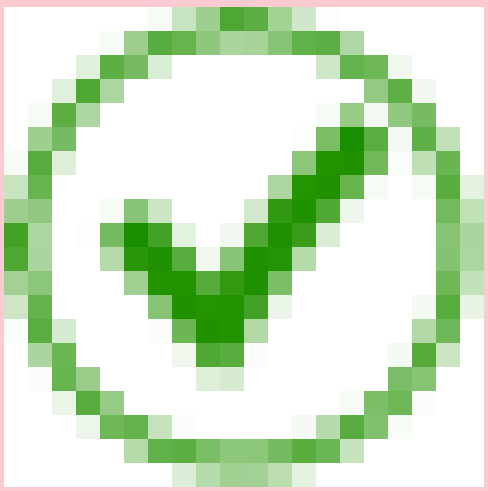
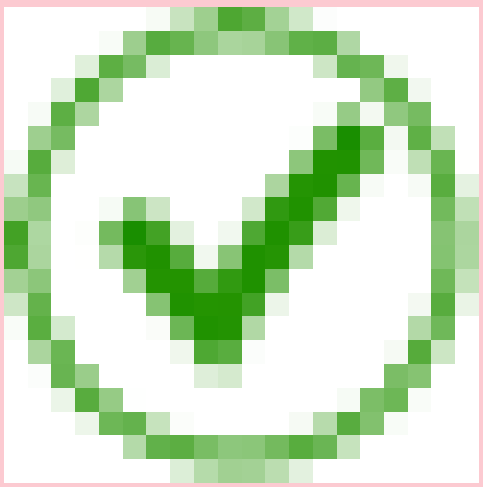
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
監視トピック				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

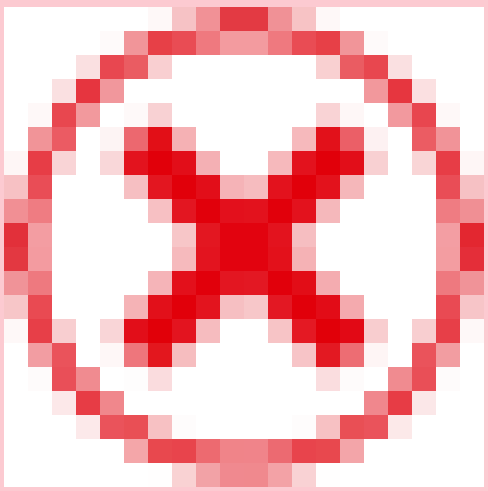
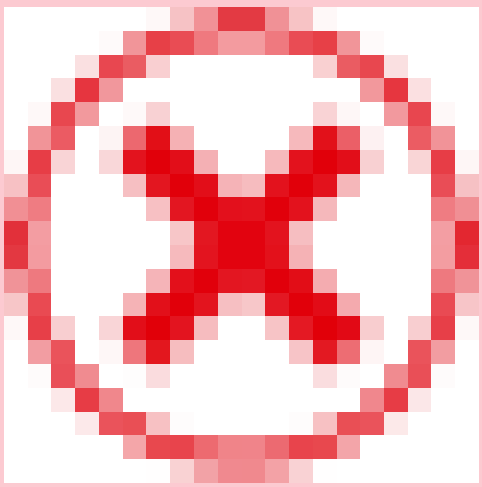
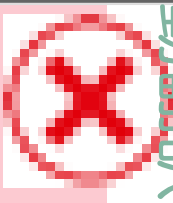
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
アサインルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

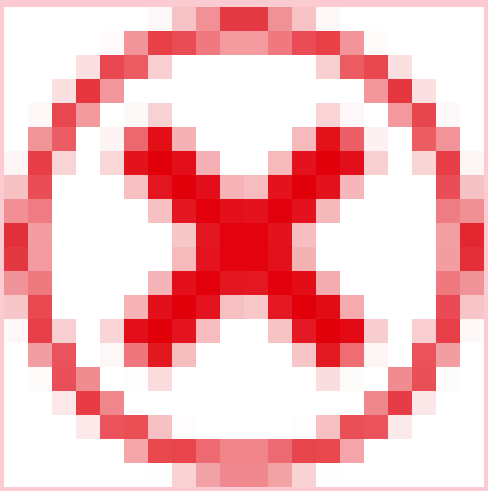
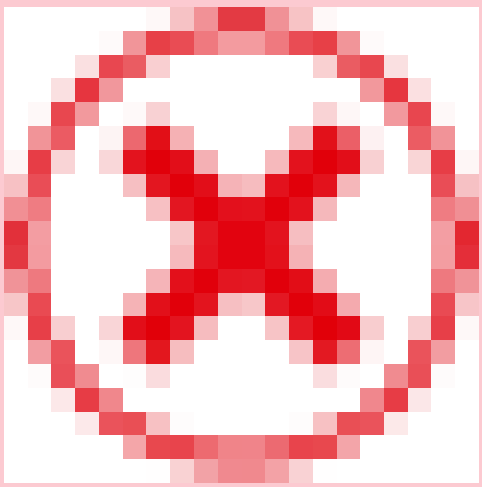
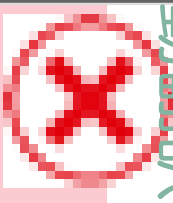
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
修復タスクルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

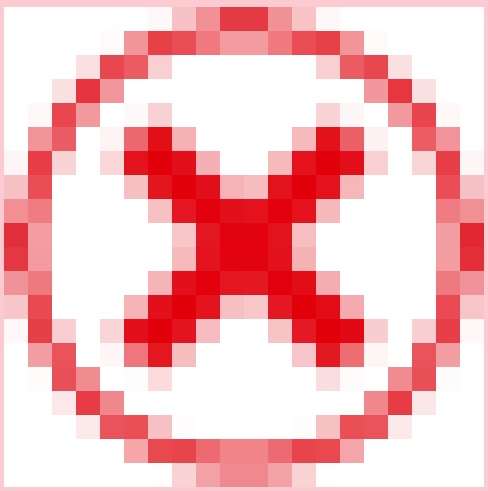
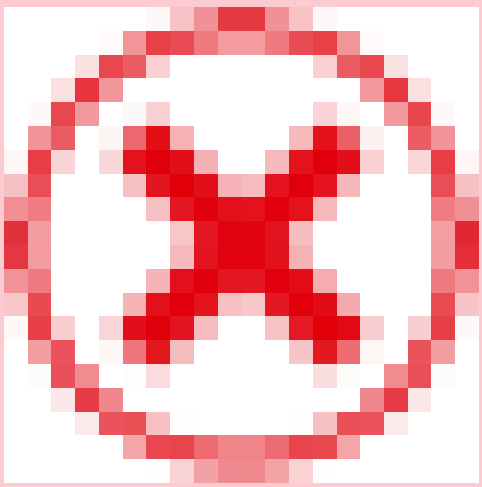
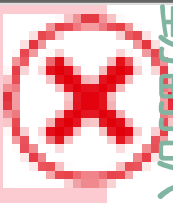
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
アサインの推奨				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

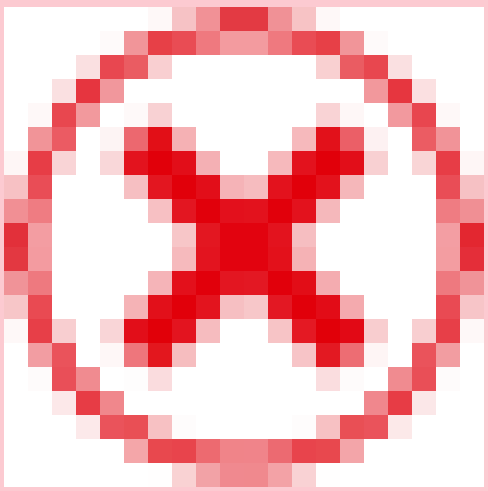
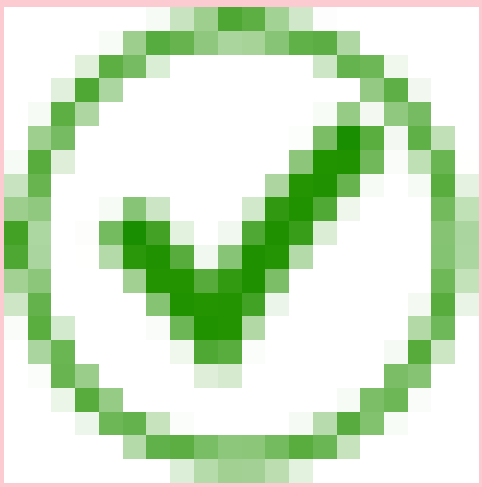
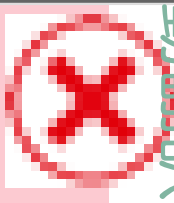
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	sn_vul.re
脆弱性算出				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

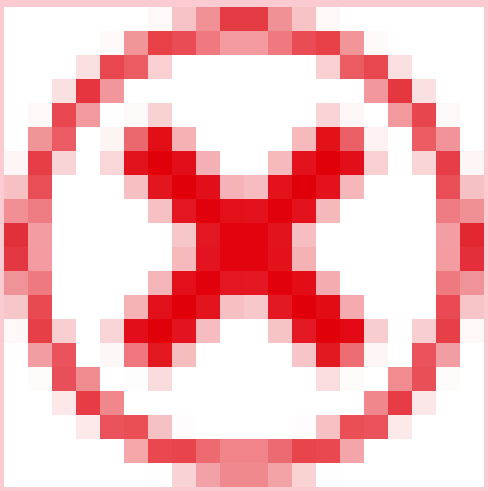
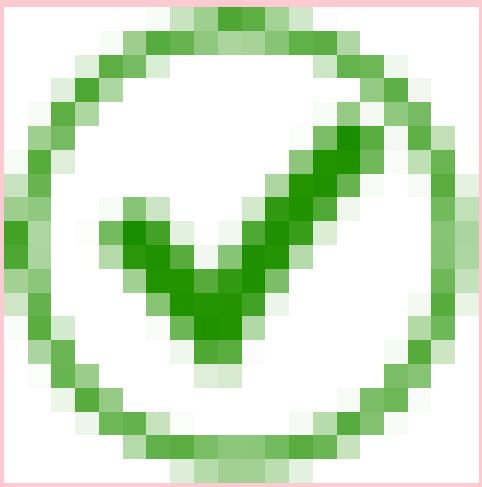
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	sn_vul.re
脆弱性ロールアップ算出				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

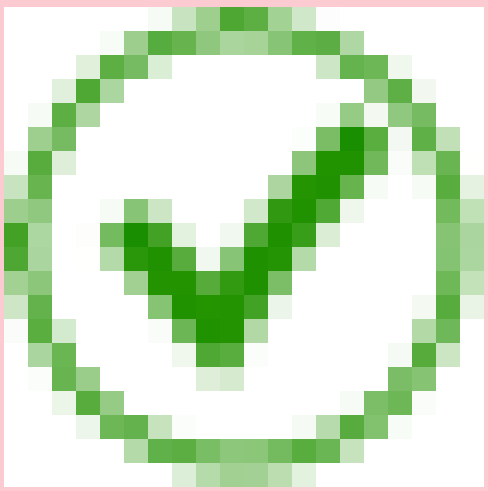
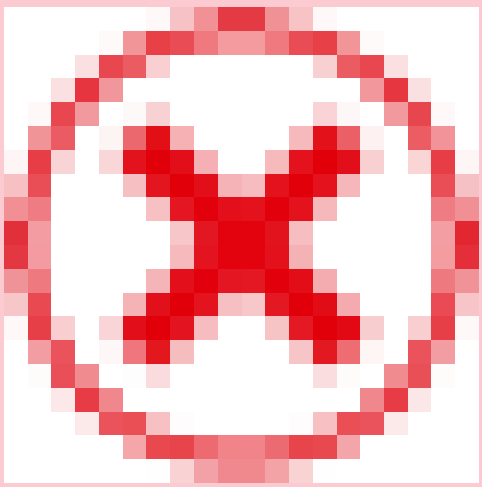
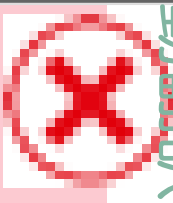
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	sn_vul.re
修復ターゲットルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

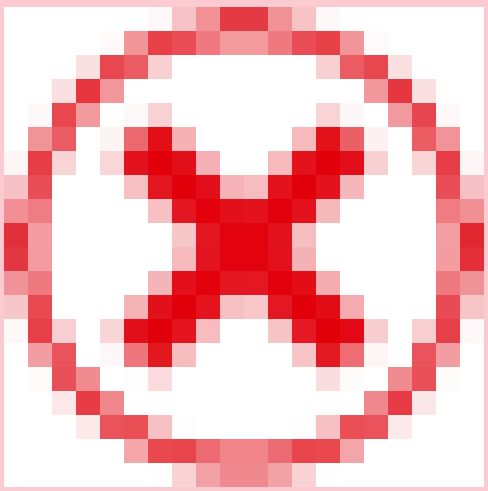
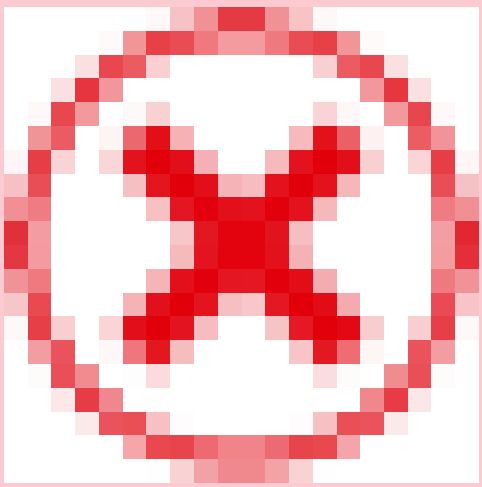
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_a	sn_vul.re
自動クローズ構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

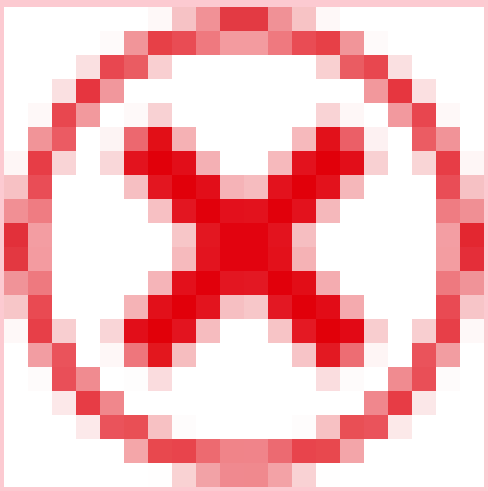
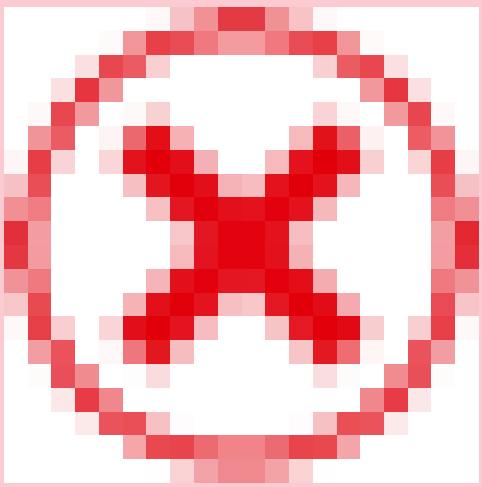
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
ルールの自動削除				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

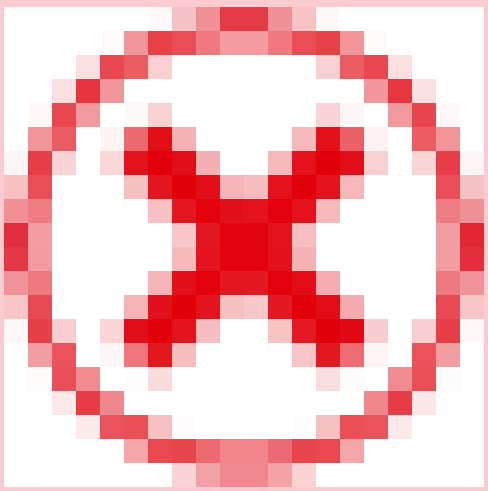
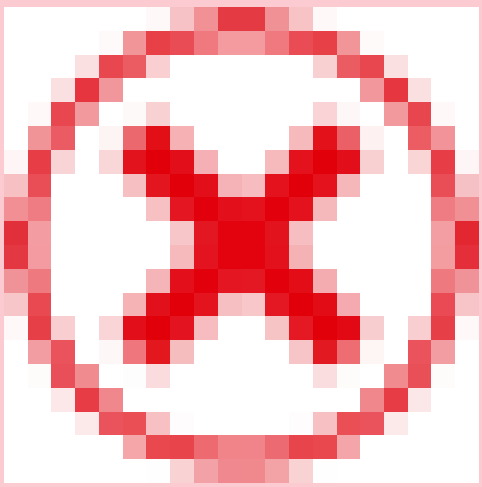
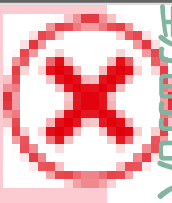
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
例外ルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

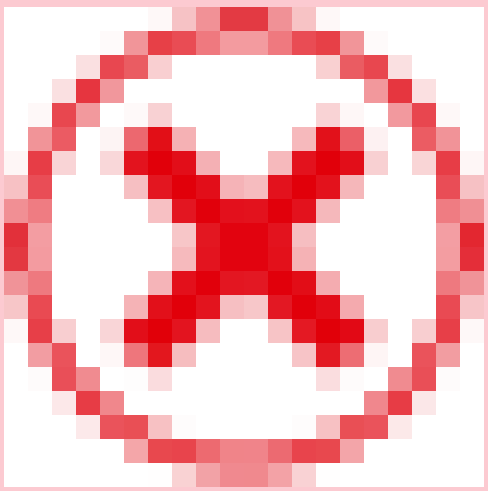
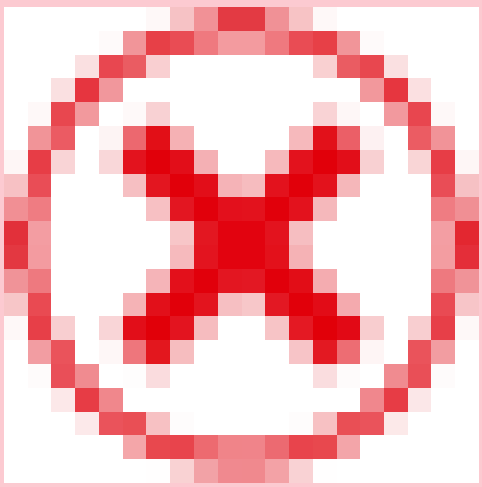
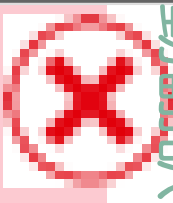
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
承認ルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

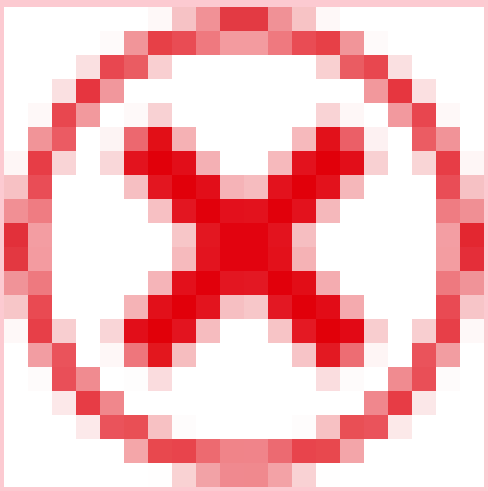
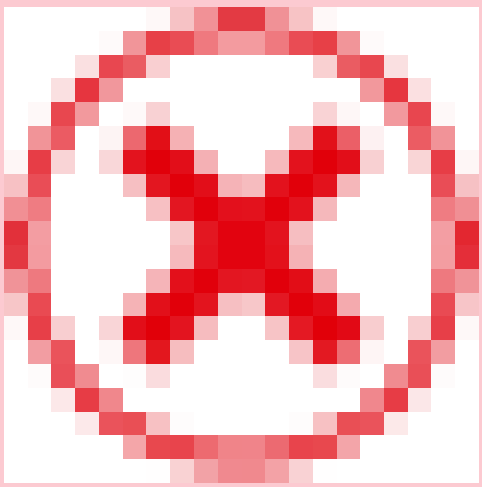
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
分類ルール				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

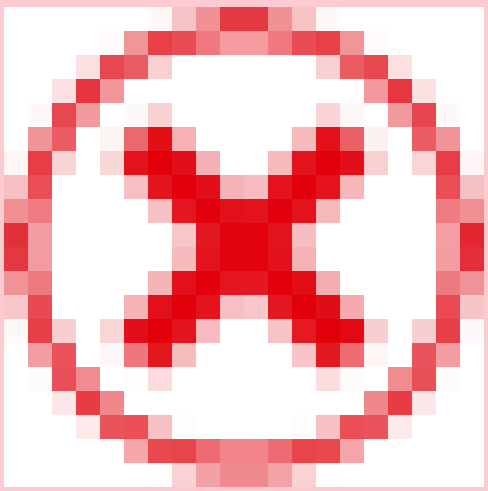
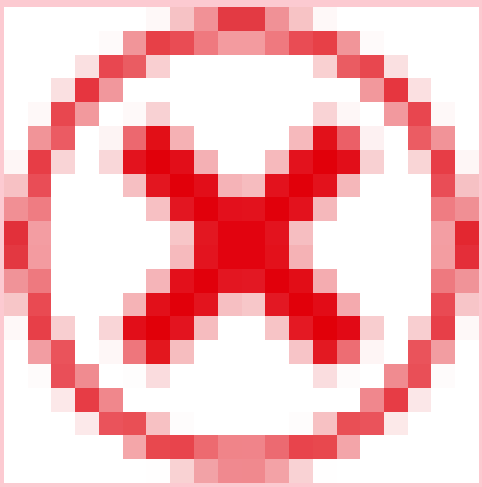
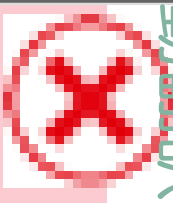
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
パフォーマンス構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

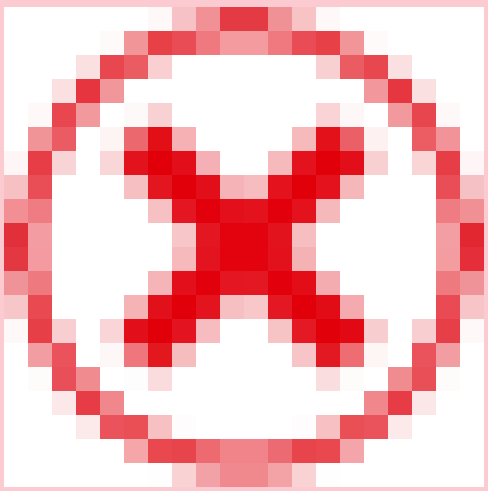
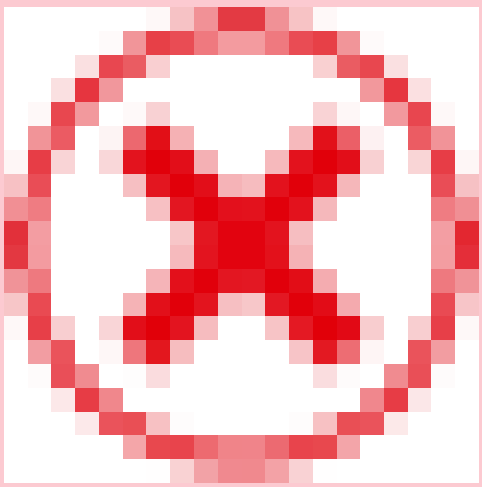
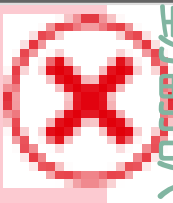
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
VI の粒度の構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

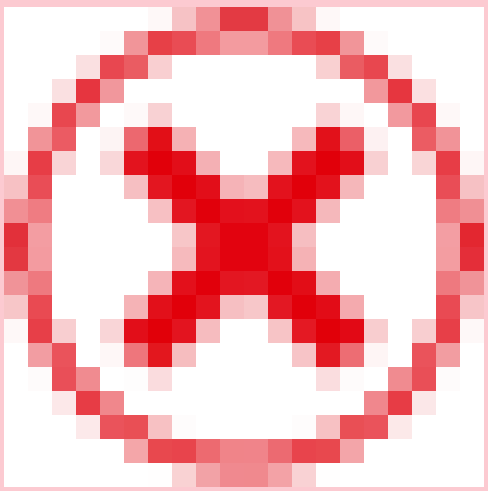
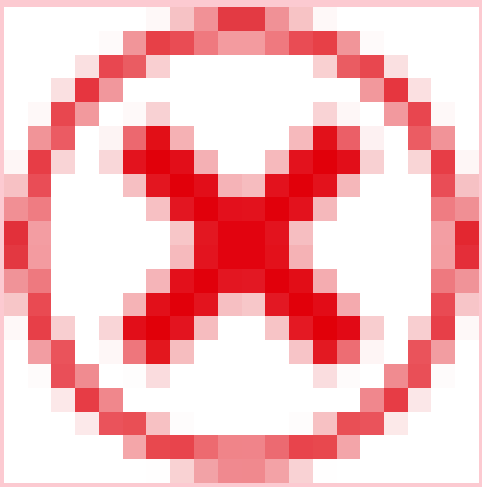
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
通知				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

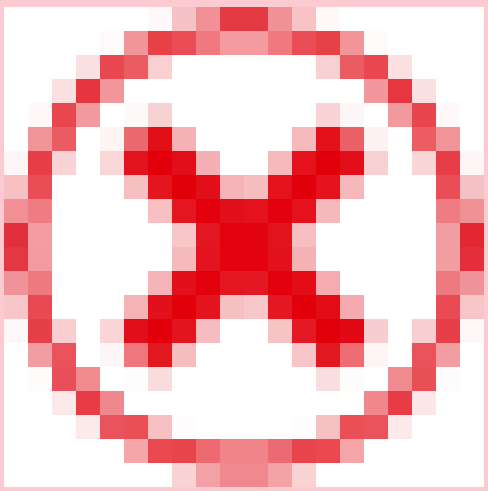
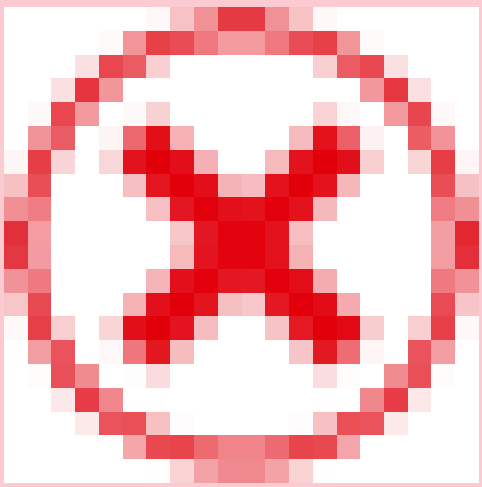
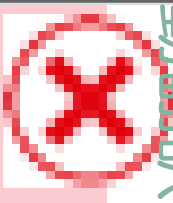
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
メールテンプレート				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

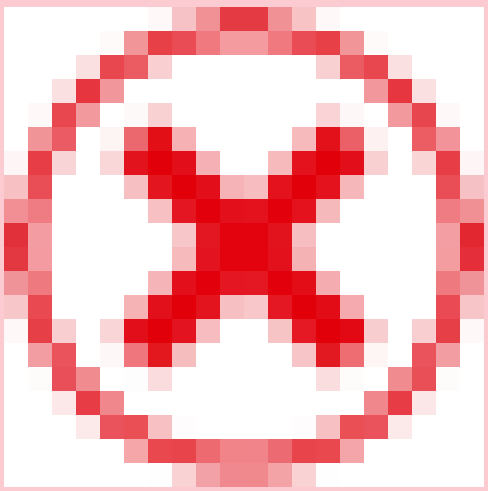
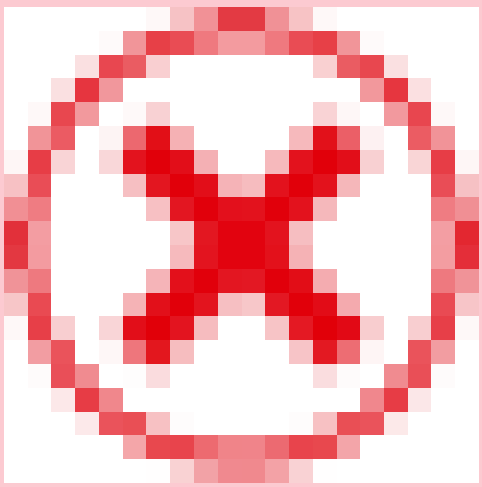
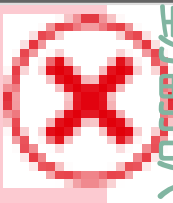
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
キューをインポート				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

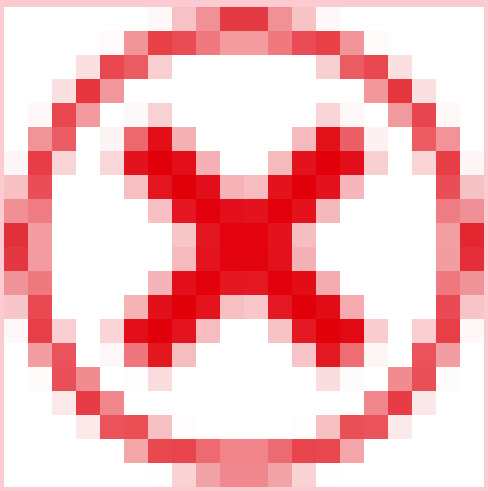
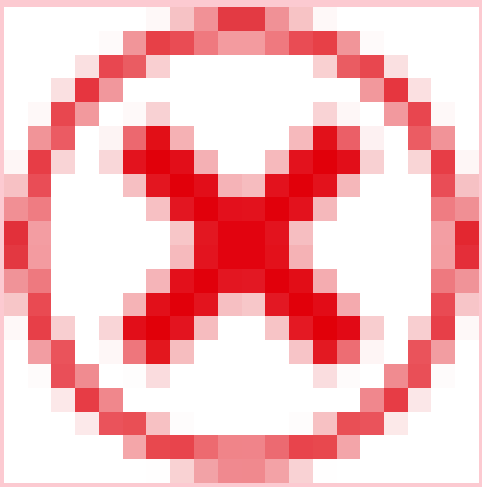
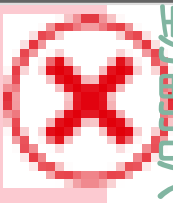
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
統合				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

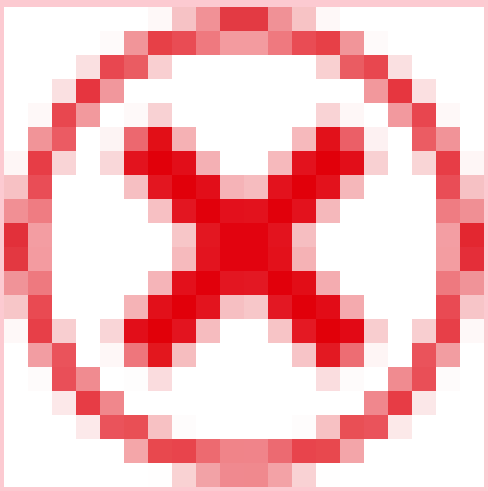
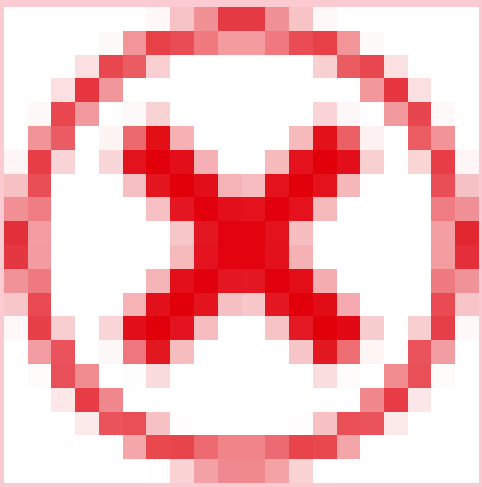
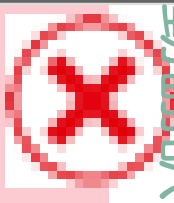
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
SLA 定義				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
SAM NVD の構成	✗	✗	✗	✗

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

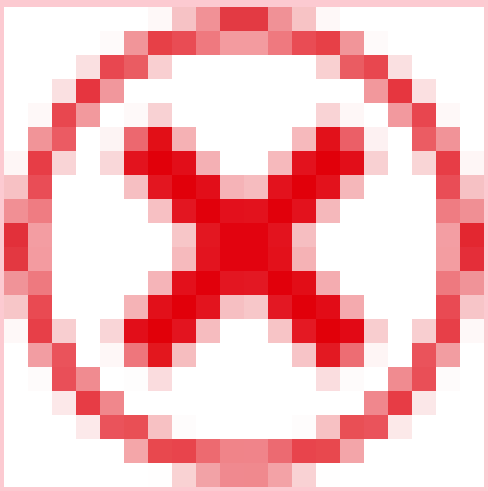
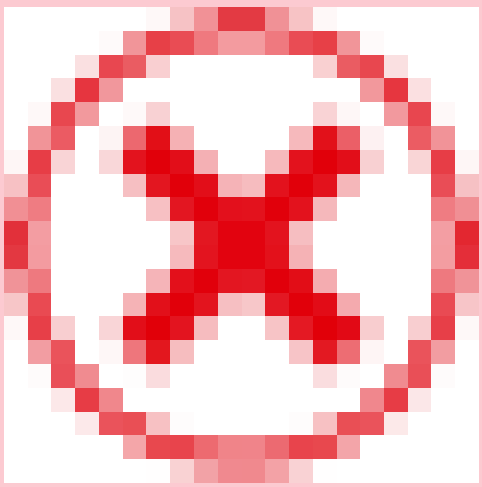
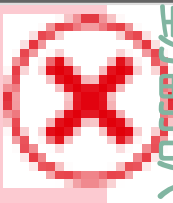
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
正規化された重大度マップ				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

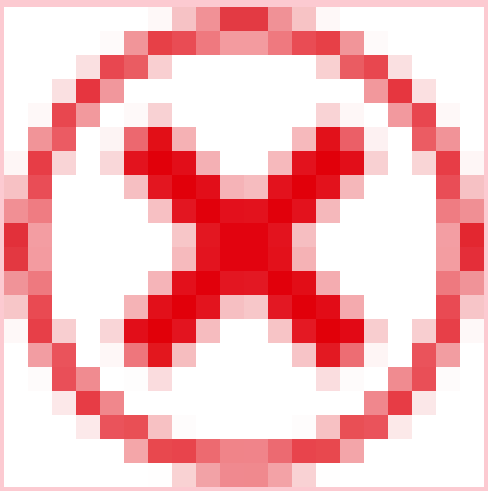
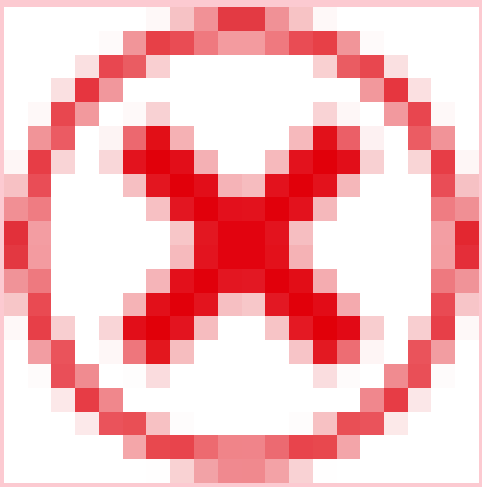
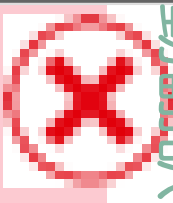
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
スキャン範囲構成				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

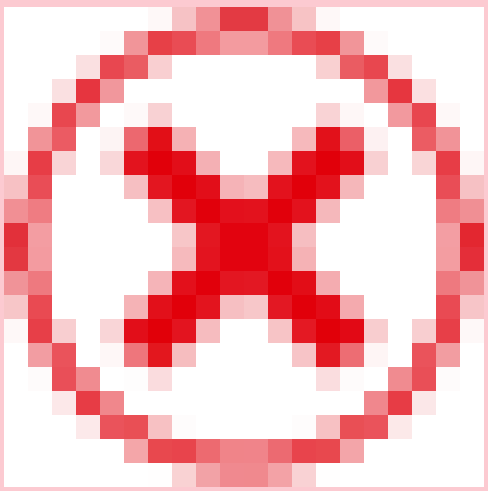
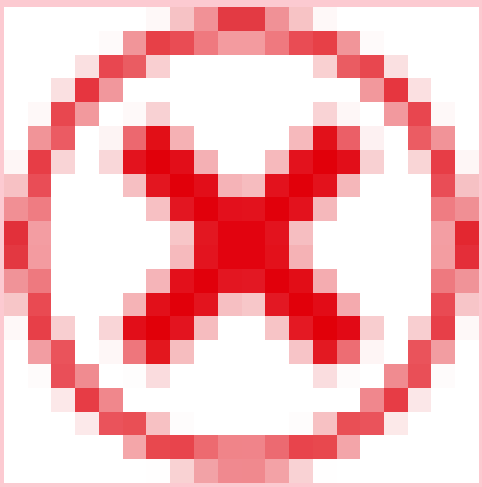
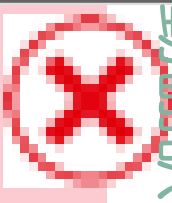
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
例外管理				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

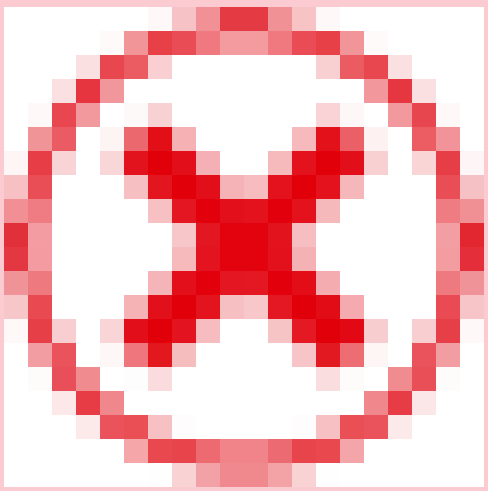
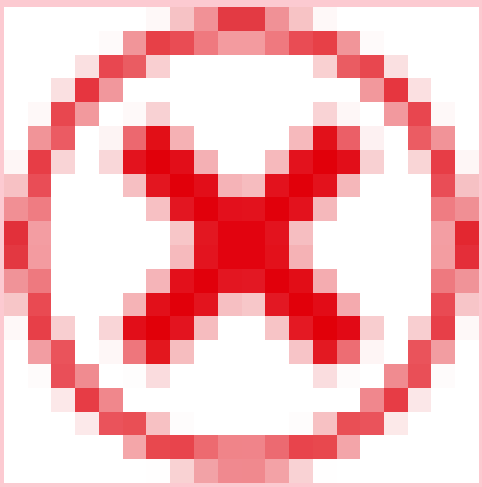
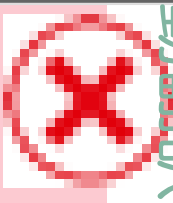
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_al	sn_vul.re
使用状況レポート				
診断				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_vul.read_all、sn_vu

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

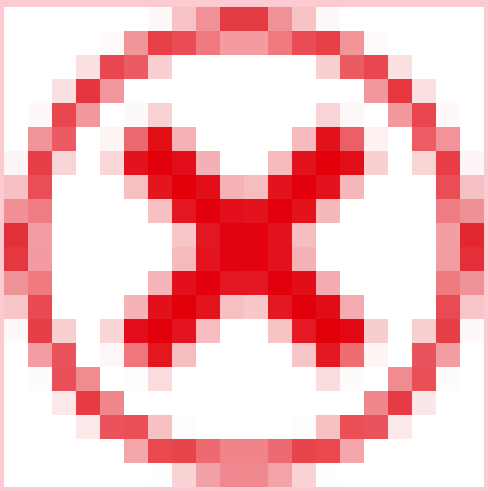
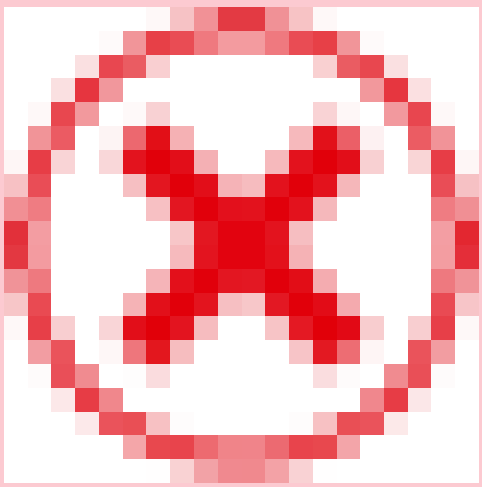
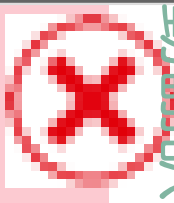
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_vul.re
チェック				

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unas

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

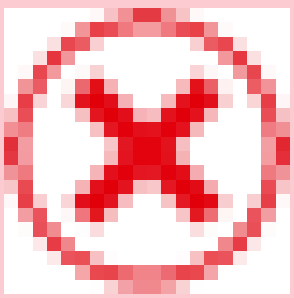
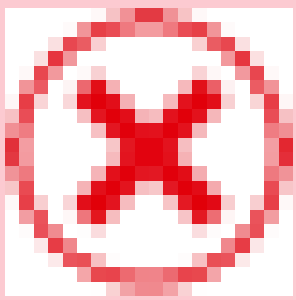
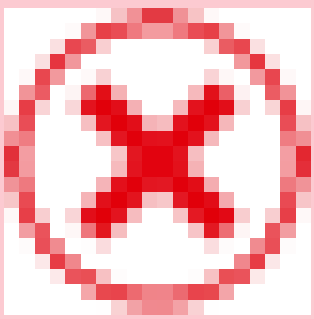
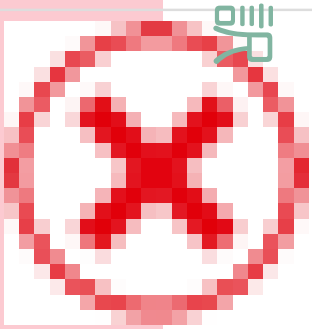
sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
(メインアプリグループ)					
CISO ダッシュボード					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

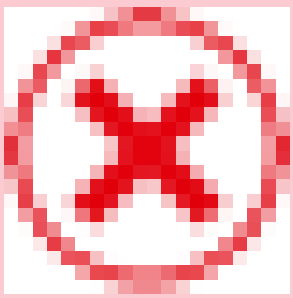
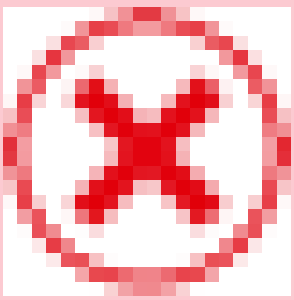
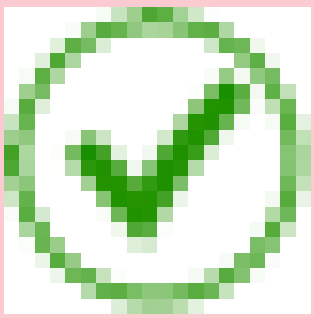
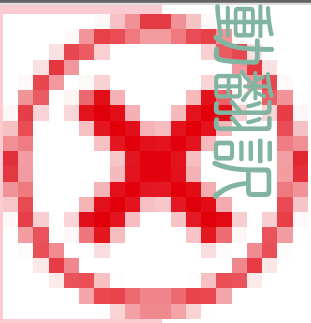
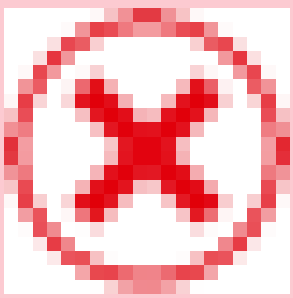
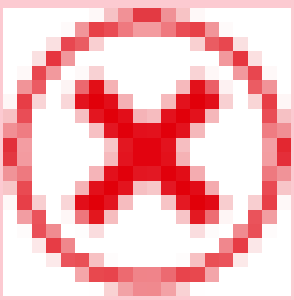
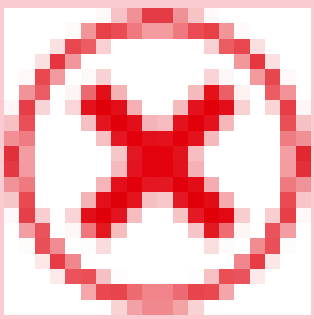
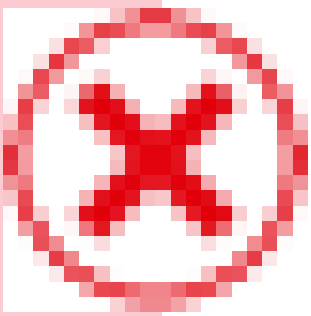
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
修復の概要					
脆弱性マネージャーのワークスペース					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

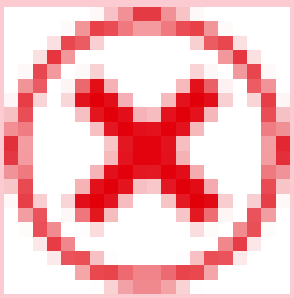
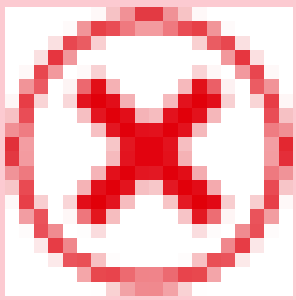
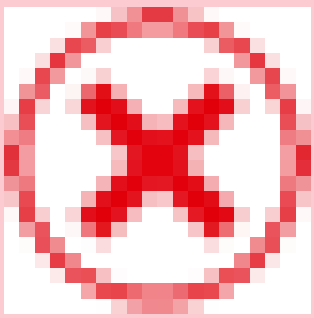
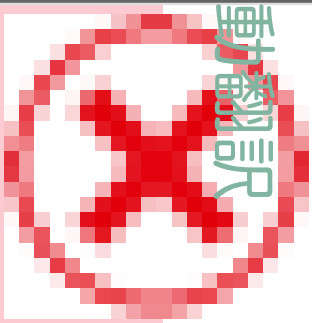
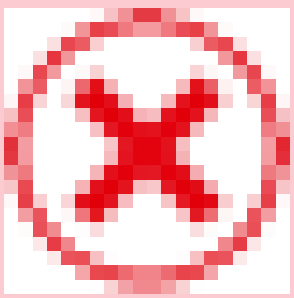
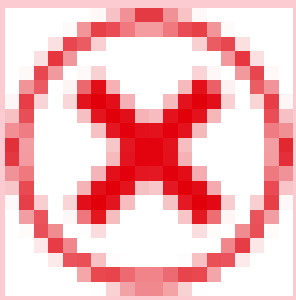
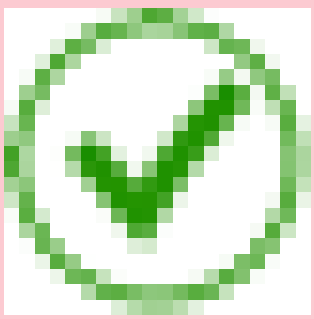
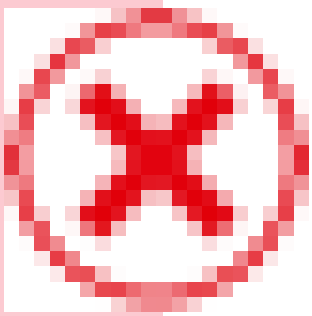
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
概要					
IT 修復ワークスペース					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

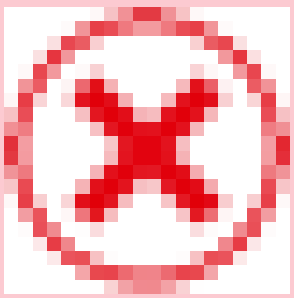
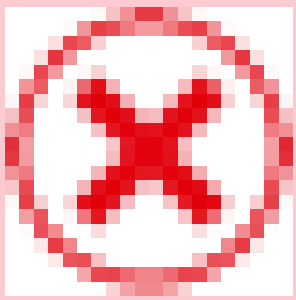
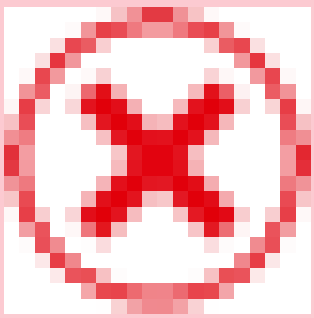
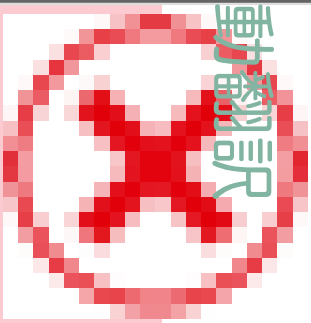
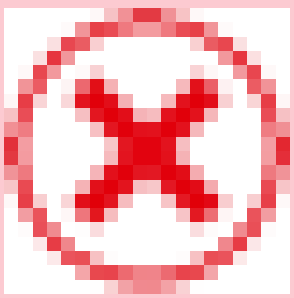
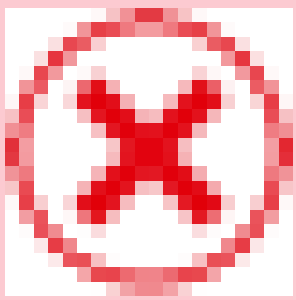
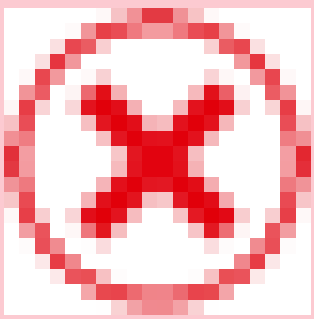
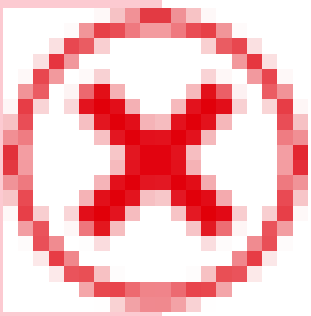
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
承認者の概要					
概要					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

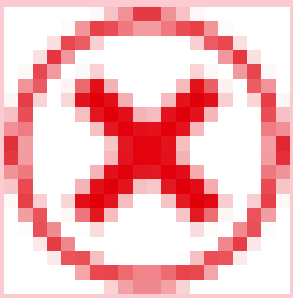
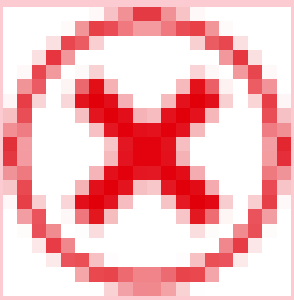
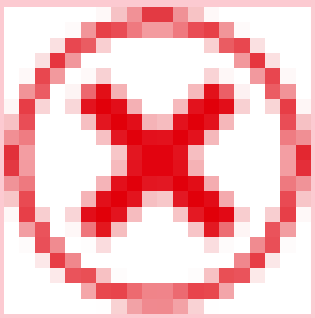
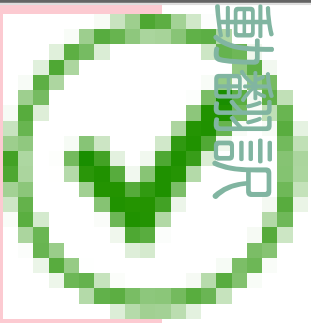
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
自分の承認					

修復タスク

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

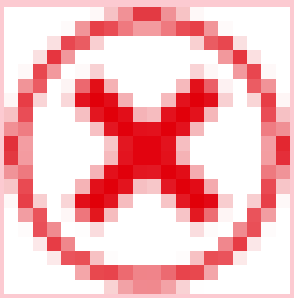
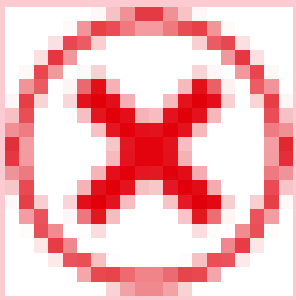
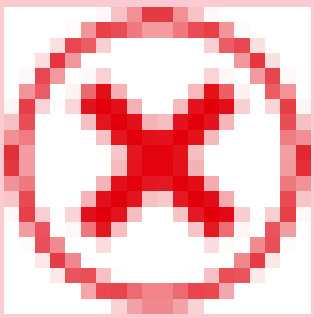
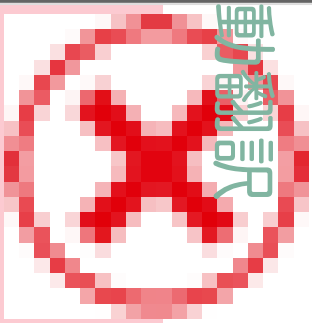
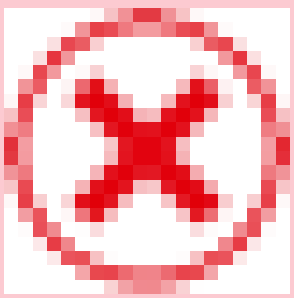
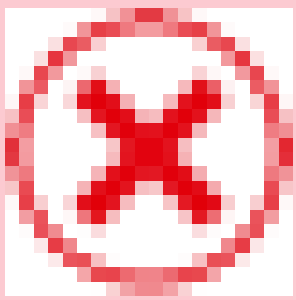
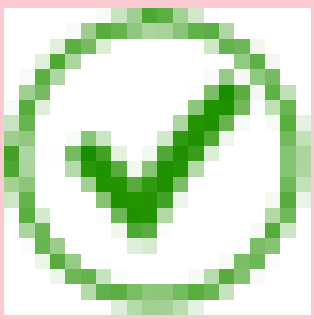
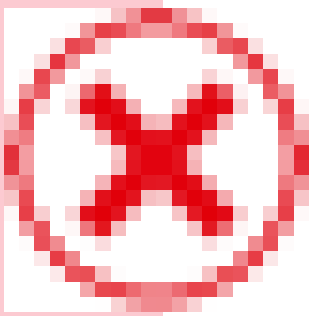
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
有効					
自分にアサイン済み					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

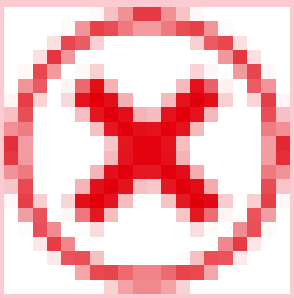
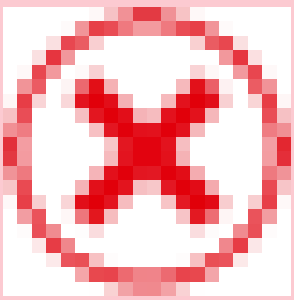
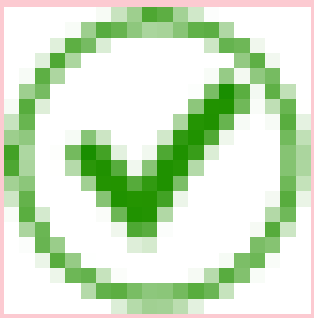
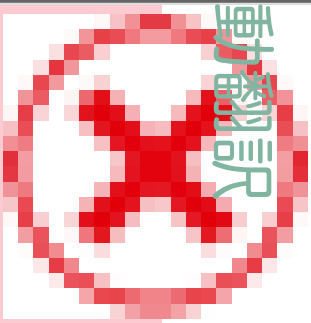
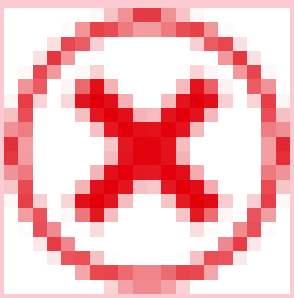
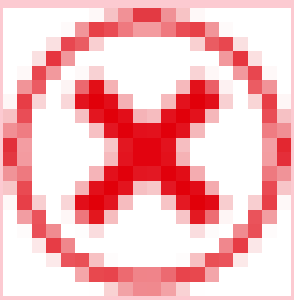
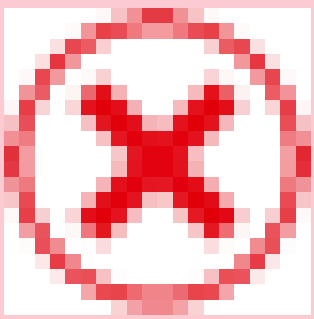
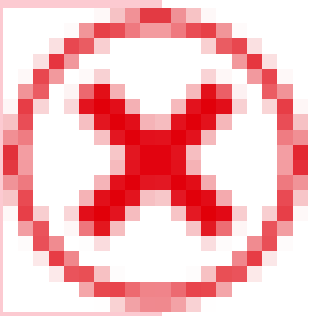
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
所属グループにアサイン済み					
すべて					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

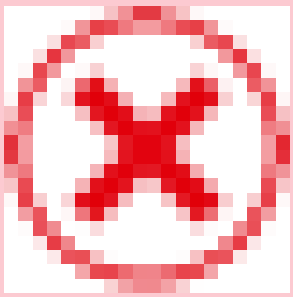
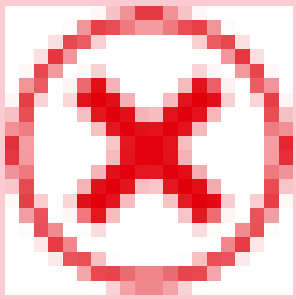
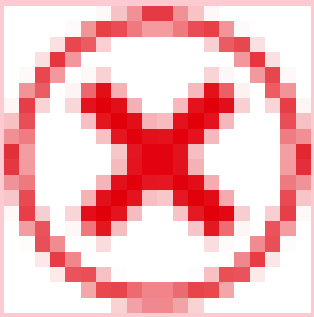
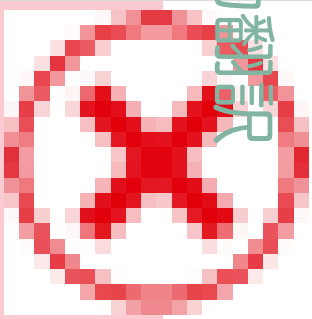
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
脆弱性一致アイテム					
重大なリスク					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

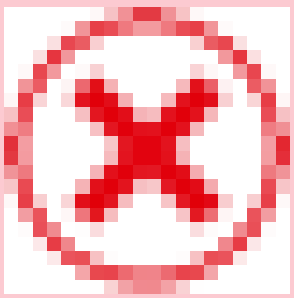
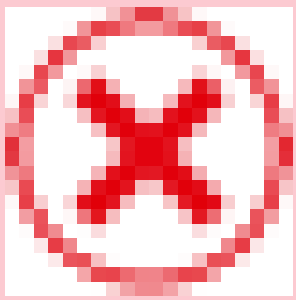
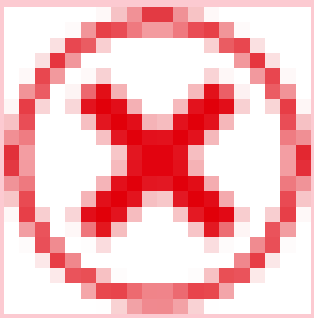
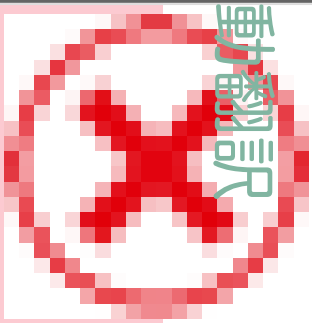
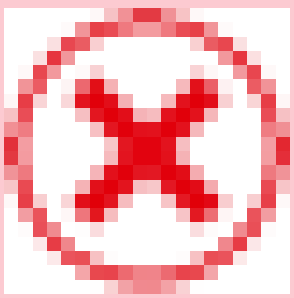
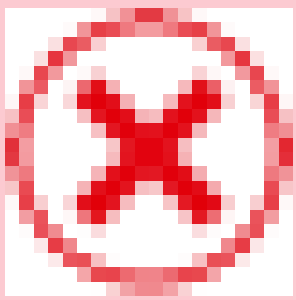
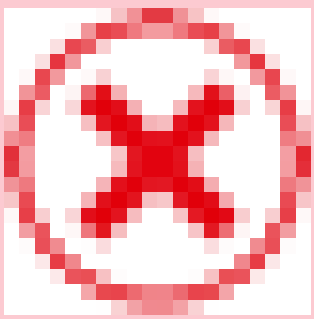
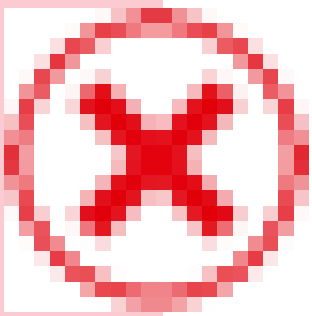
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
高リスク					
エクスプロイト可能					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

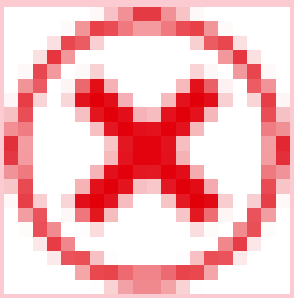
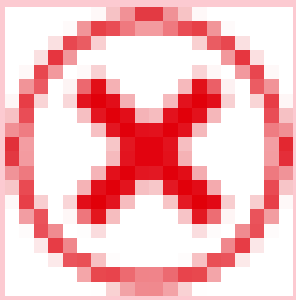
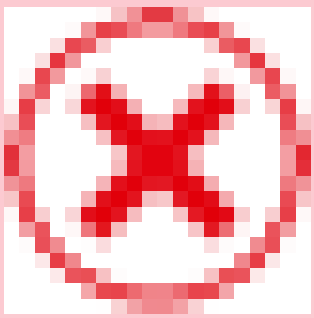
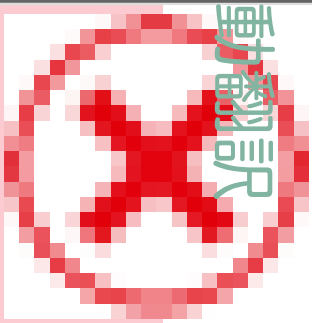
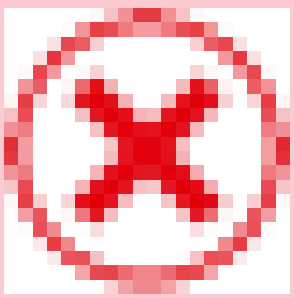
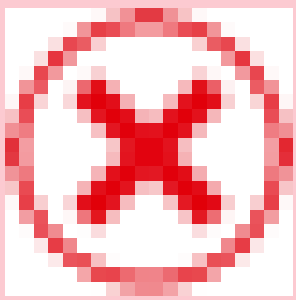
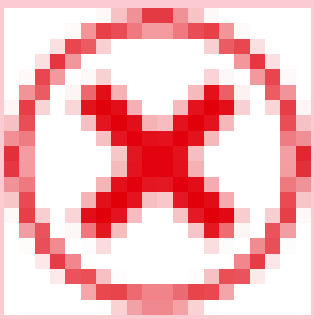
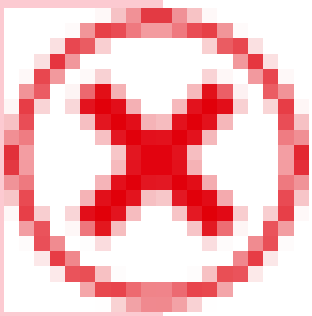
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
該当 CI 確認中					
CI 不明					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

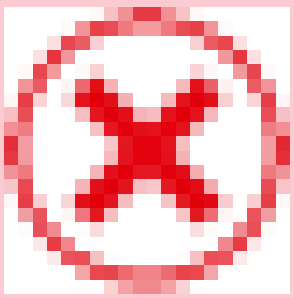
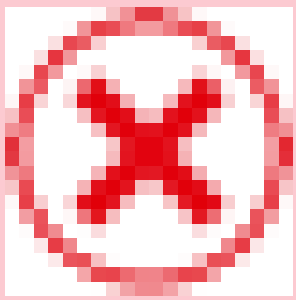
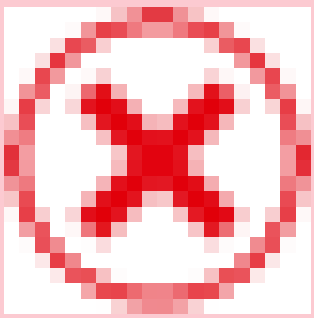
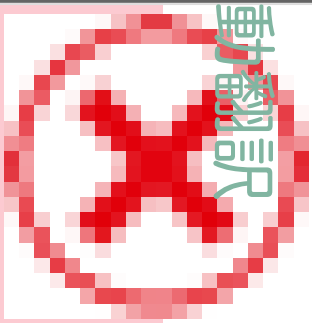
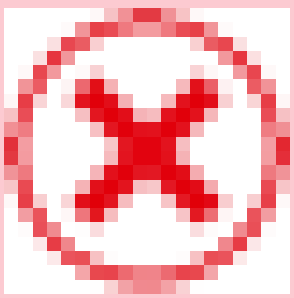
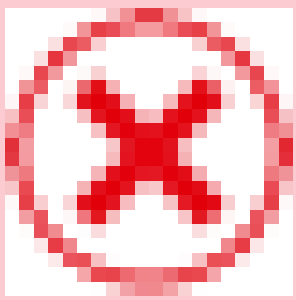
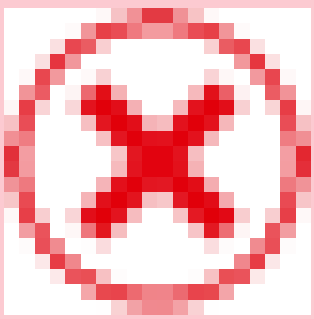
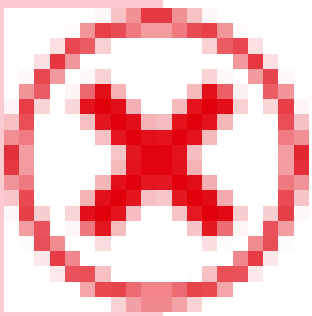
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
過去 90 日以内					
91 日以上前					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

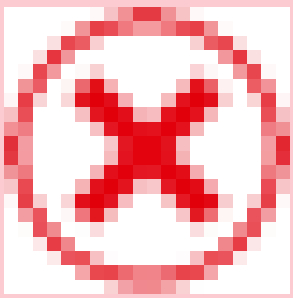
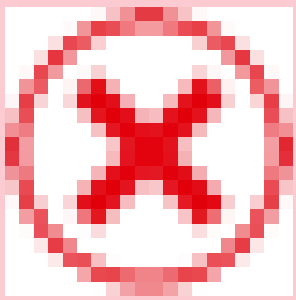
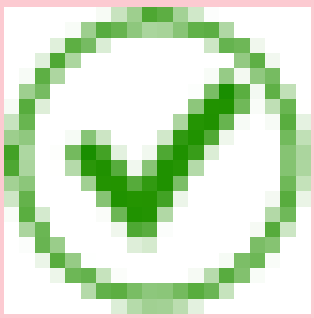
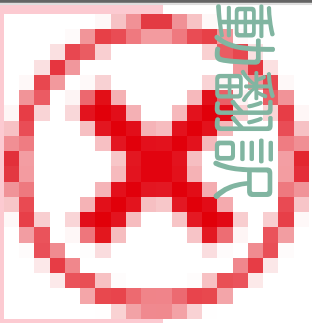
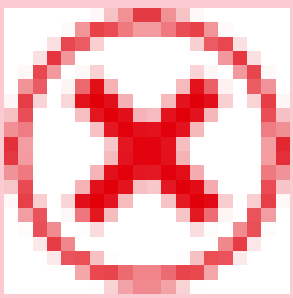
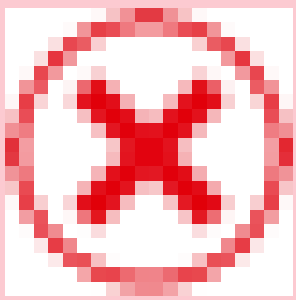
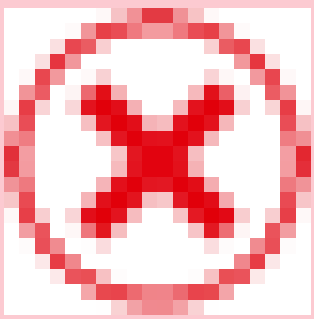
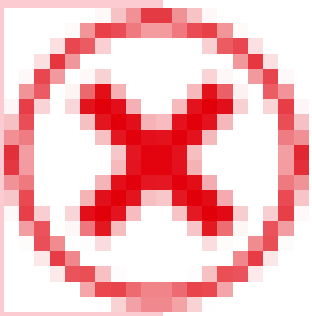
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
未アサイン					
修復タスク未割り当て					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

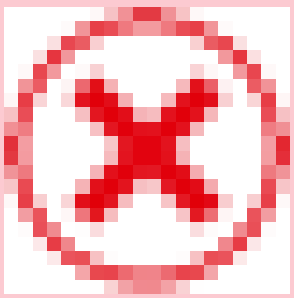
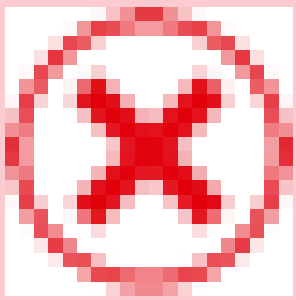
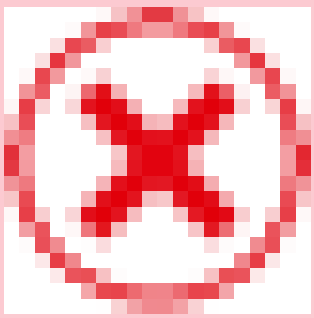
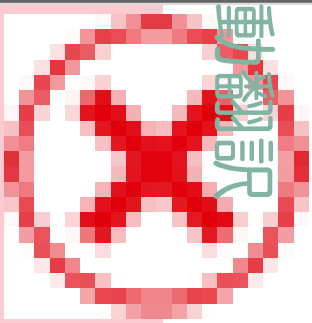
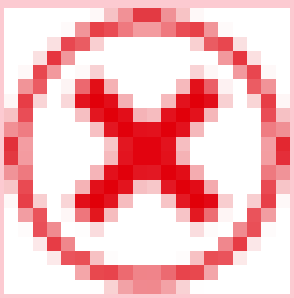
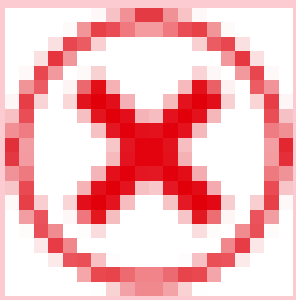
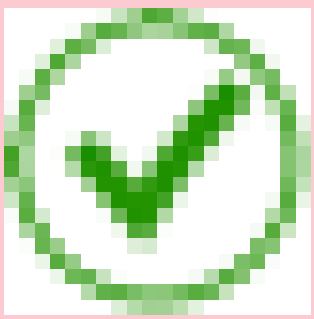
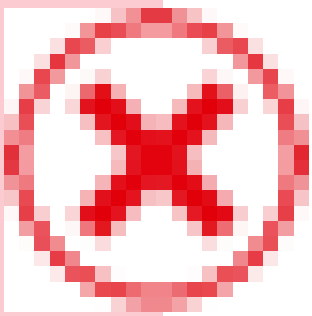
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
廃止					
複数の保留					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

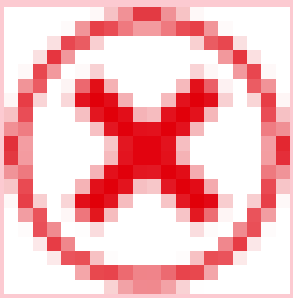
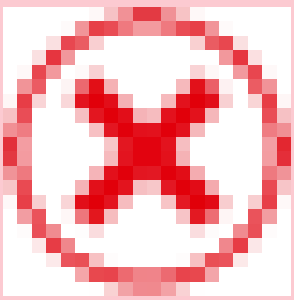
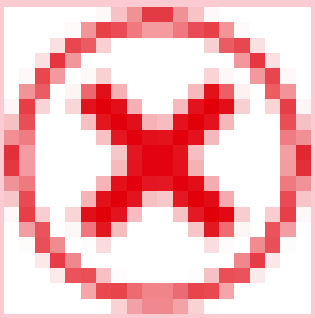
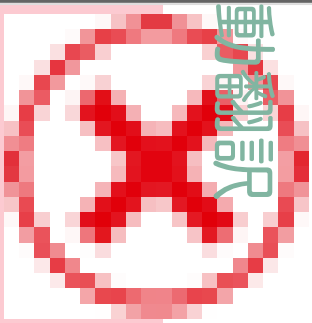
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
すべて					

ソリューション

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

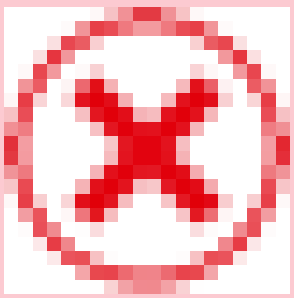
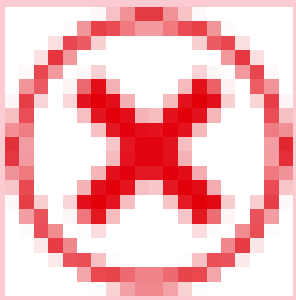
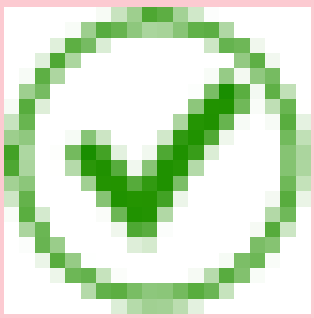
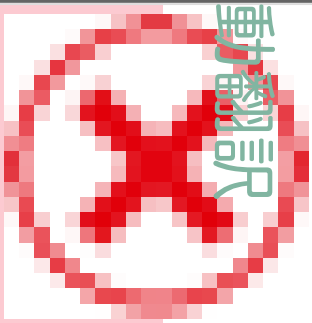
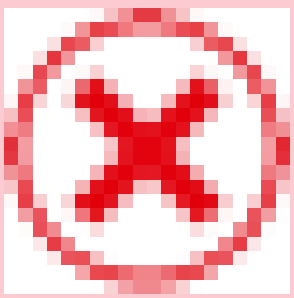
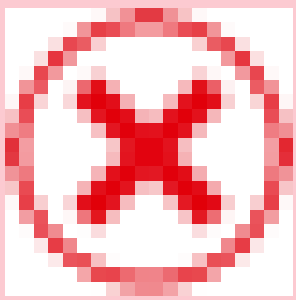
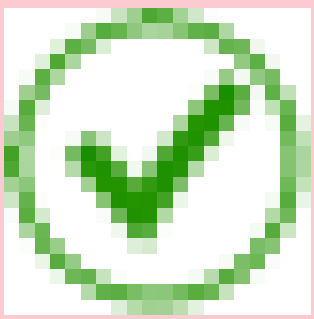
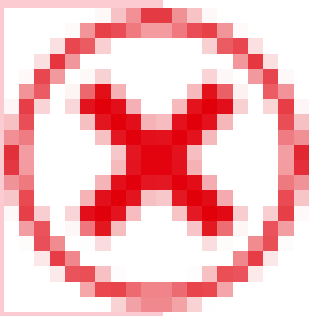
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
すべて					
最高優先度					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

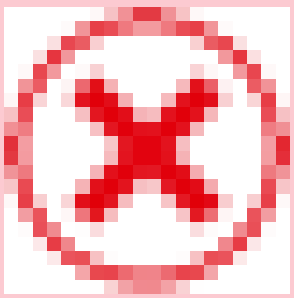
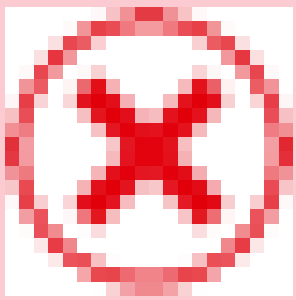
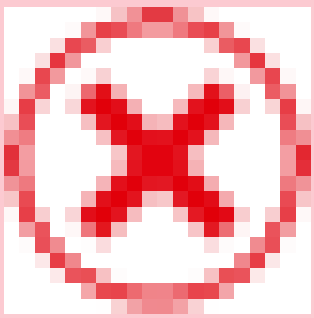
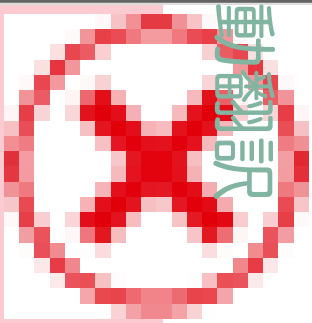
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
脆弱性一致アイテムを使用					

ライブラリ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

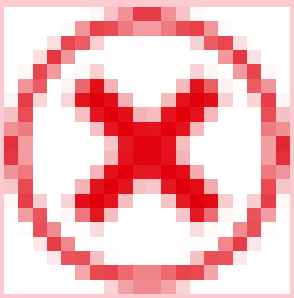
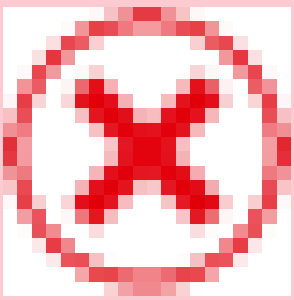
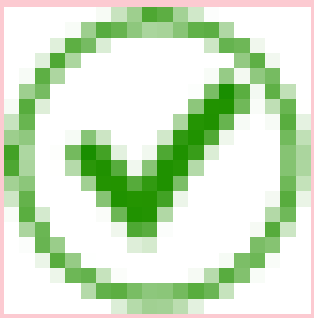
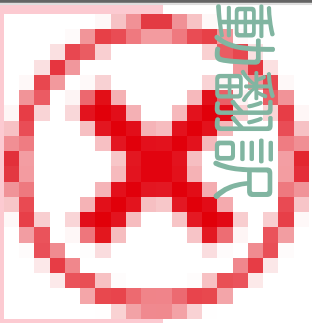
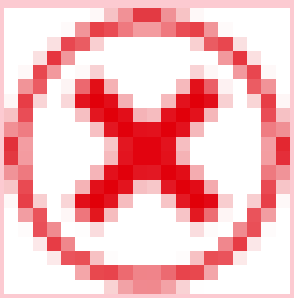
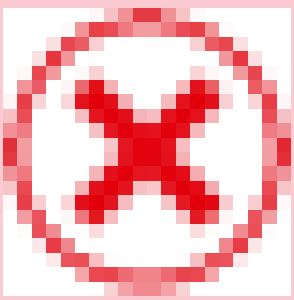
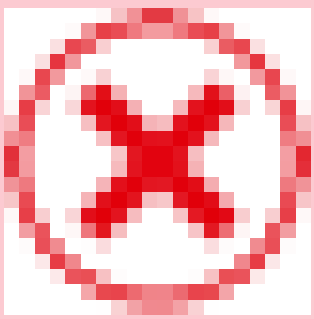
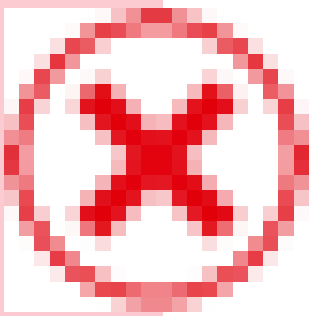
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
NVD					
CWE					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

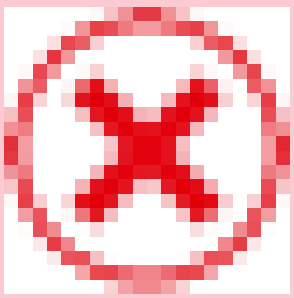
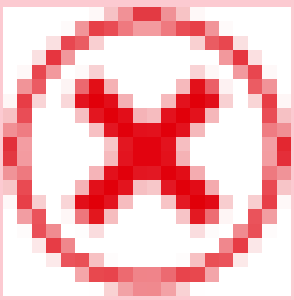
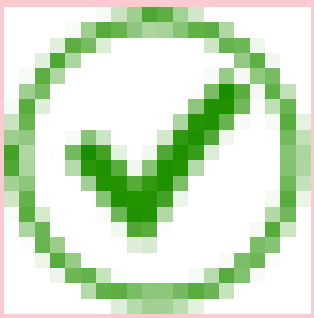
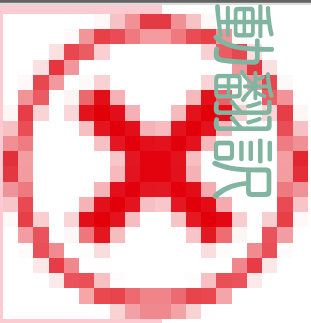
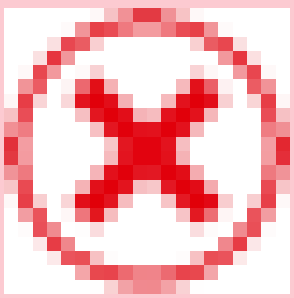
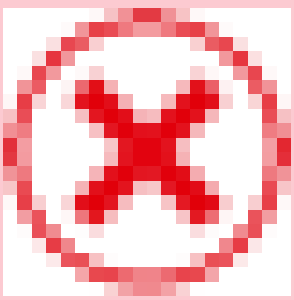
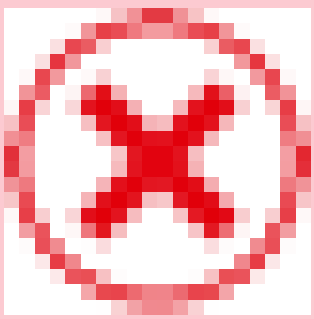
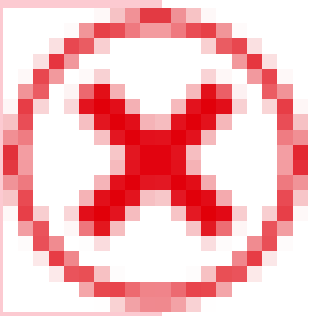
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
サードパーティ					
脆弱なソフトウェア					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

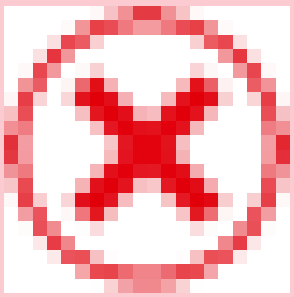
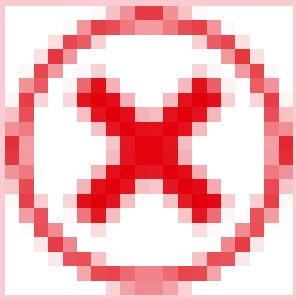
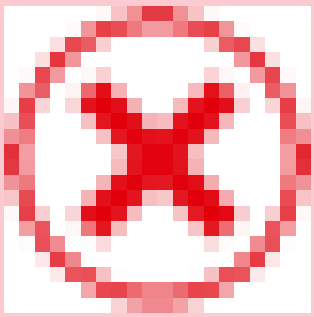
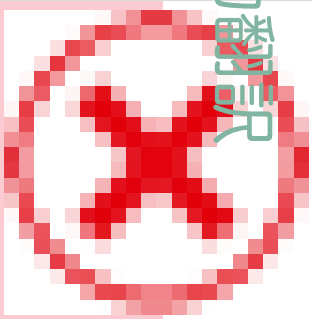
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
脆弱性スキャン					
エクスポージャーアセスメント					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

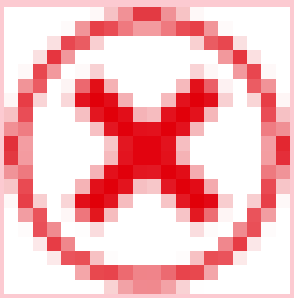
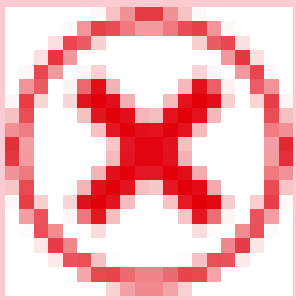
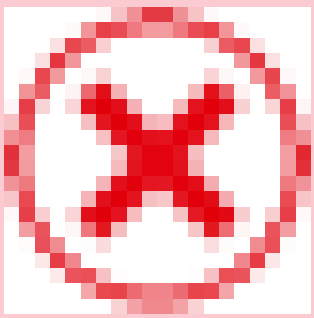
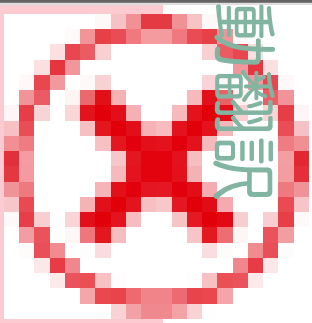
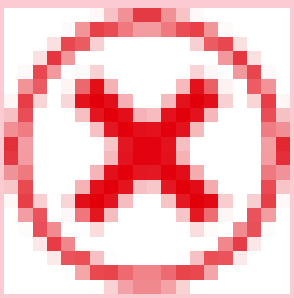
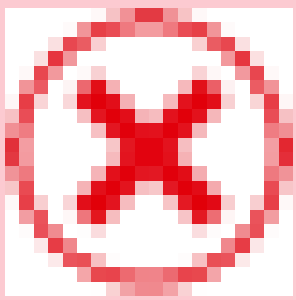
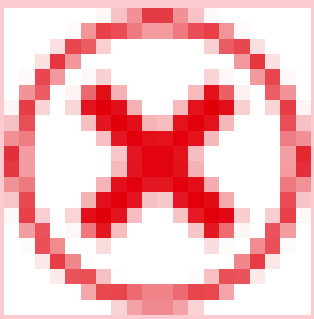
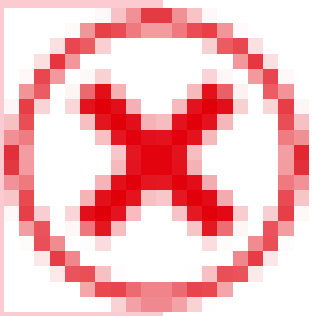
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
スキャン					
スキャナー					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

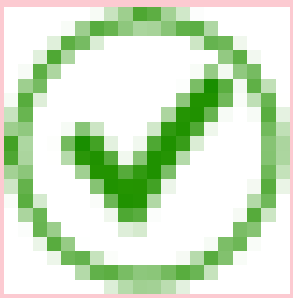
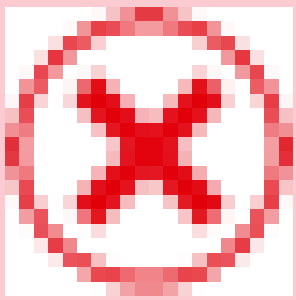
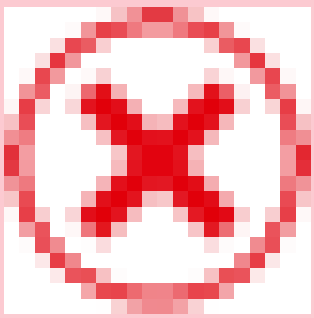
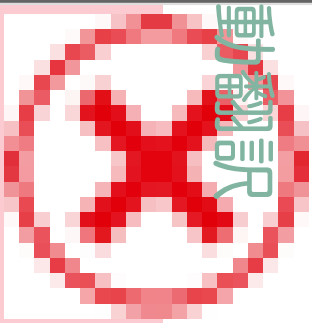
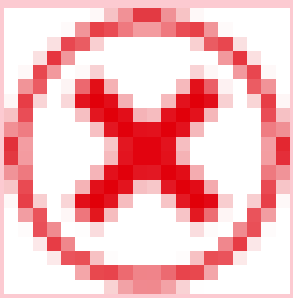
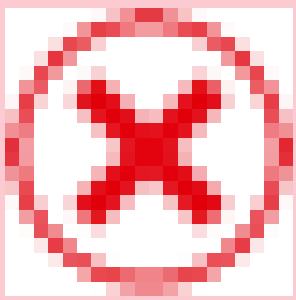
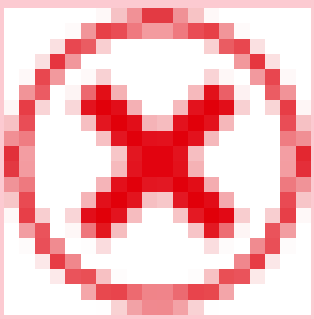
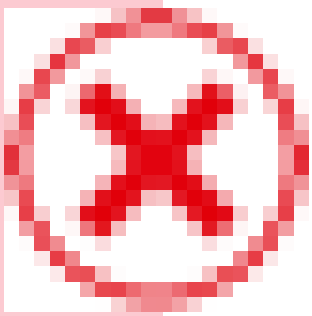
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
スキャンキュー					
スキャナーレート制限					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

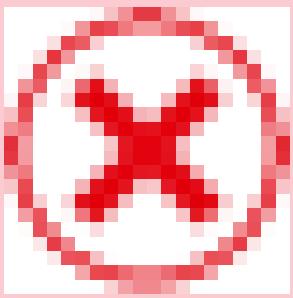
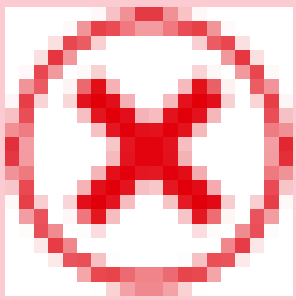
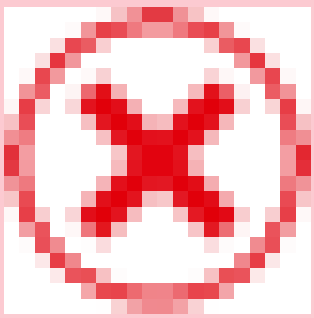
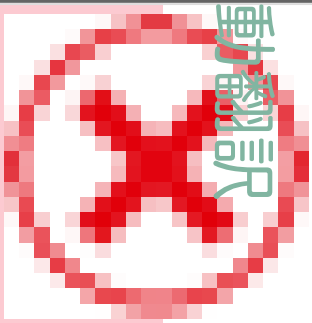
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
レート制限定義					

管理

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

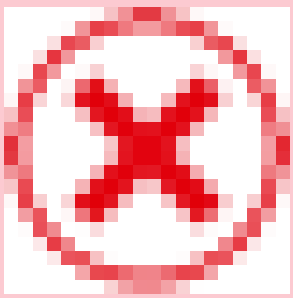
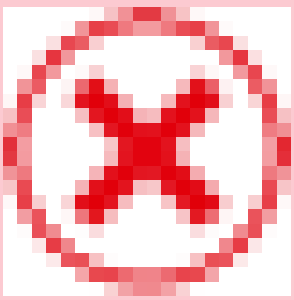
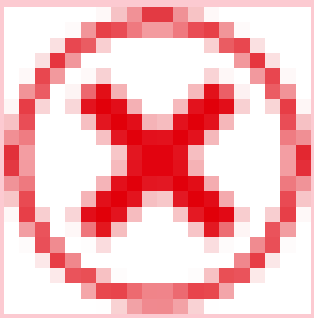
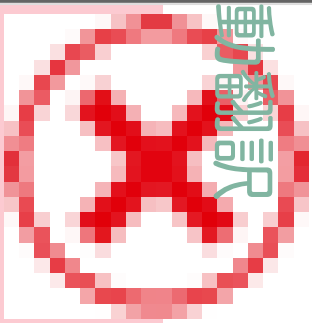
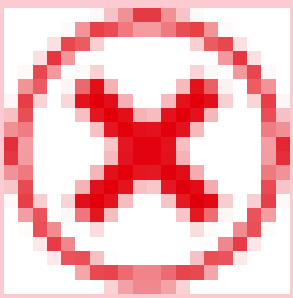
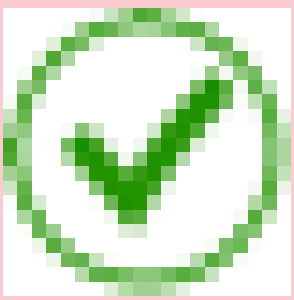
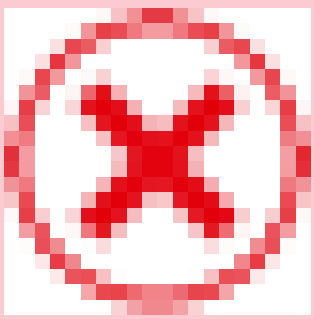
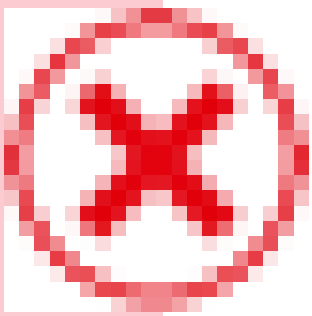
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
セットアップアシスタント					
監視トピック					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

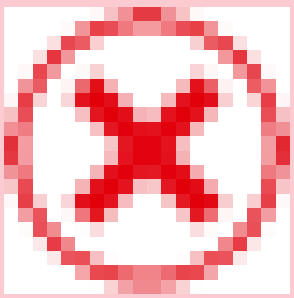
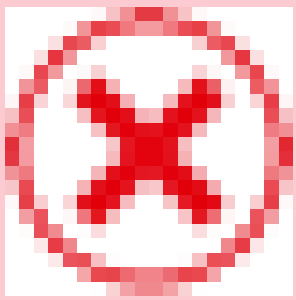
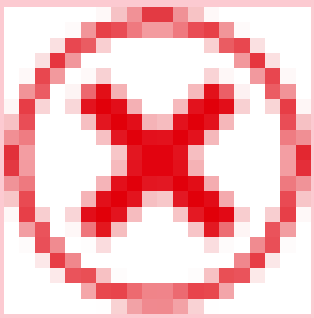
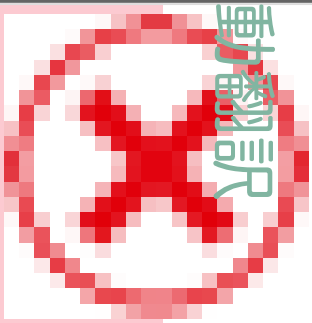
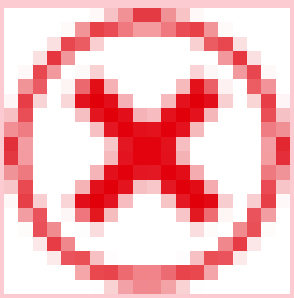
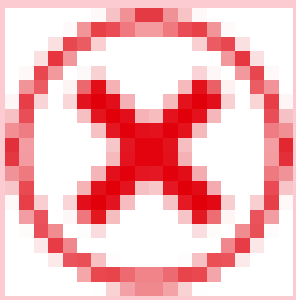
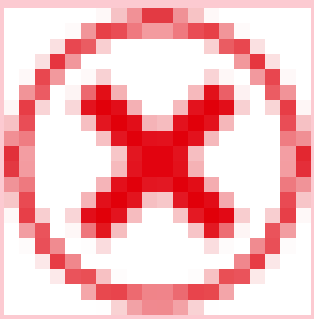
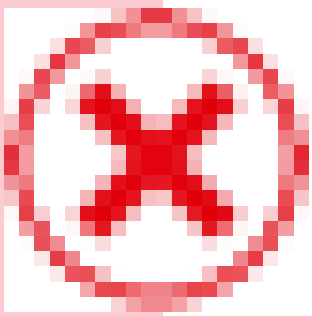
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
アサインルール					
修復タスクルール					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

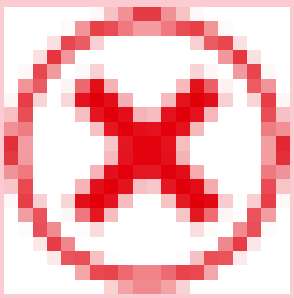
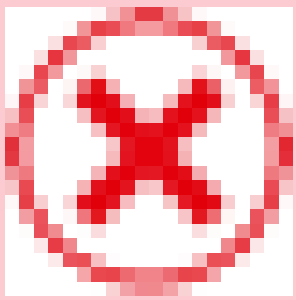
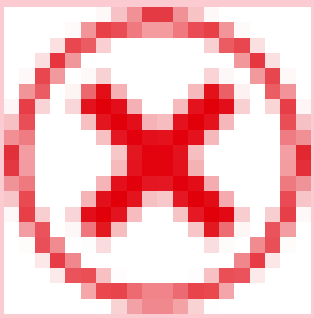
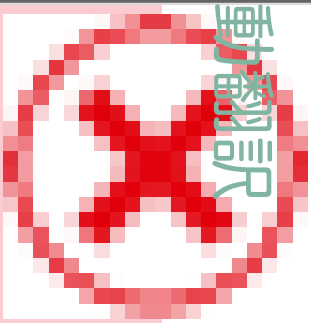
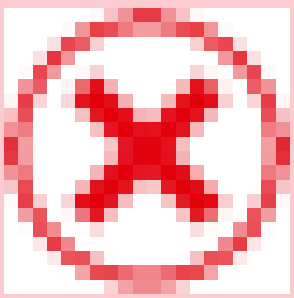
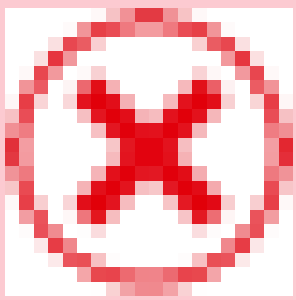
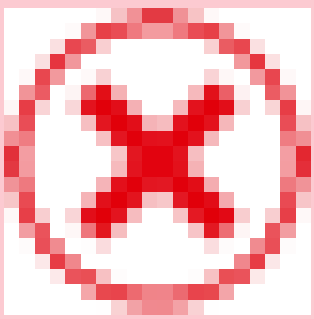
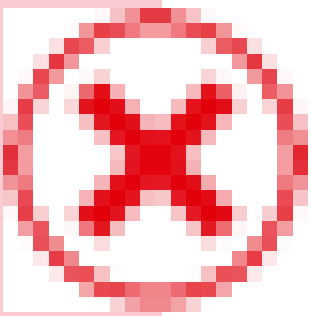
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
アサインの推奨					
脆弱性算出					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

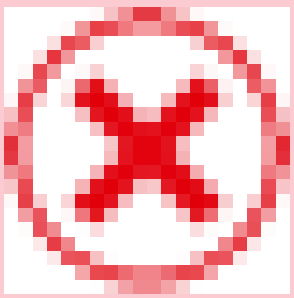
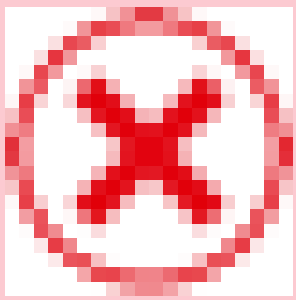
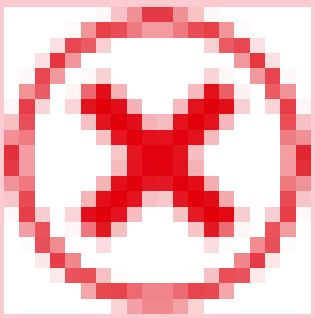
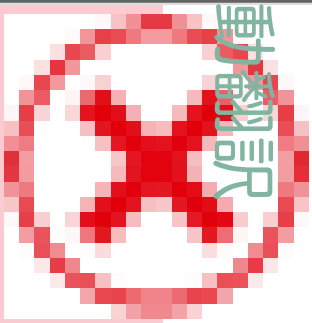
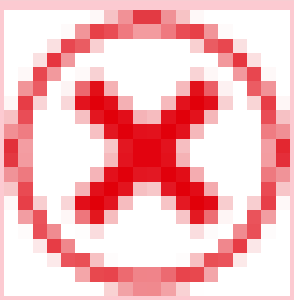
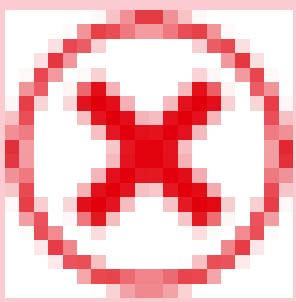
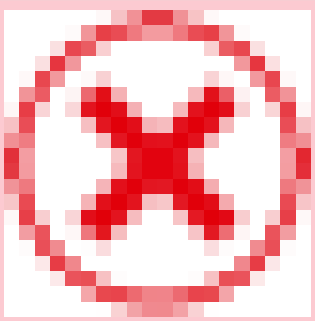
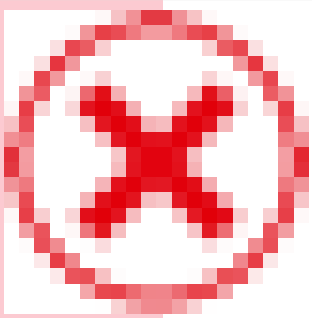
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
脆弱性ロールアップ算出					
修復ターゲットルール					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

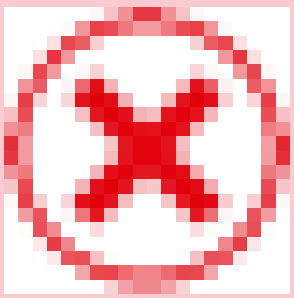
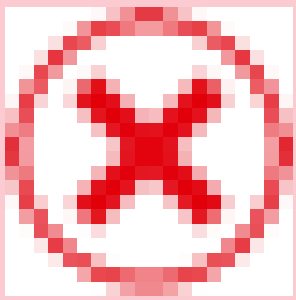
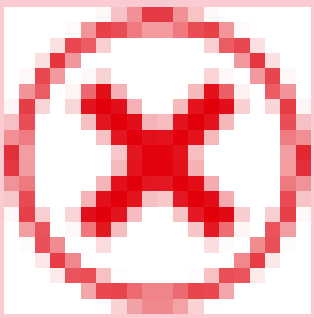
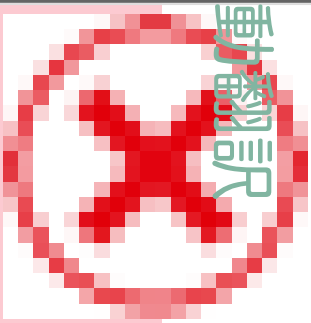
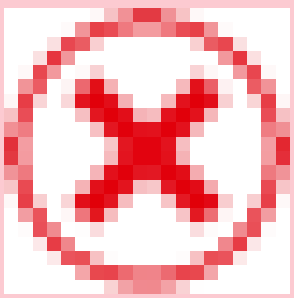
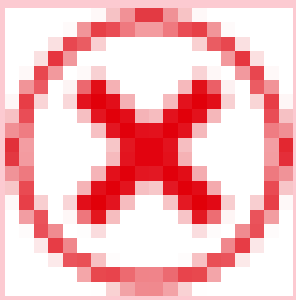
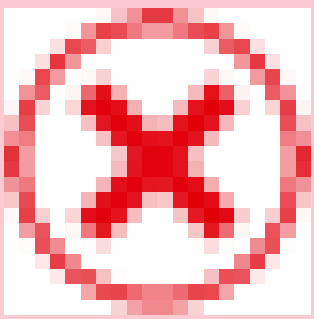
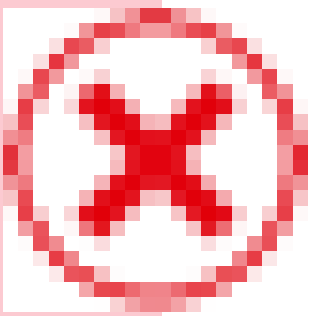
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
自動クローズ構成					
ルールの自動削除					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

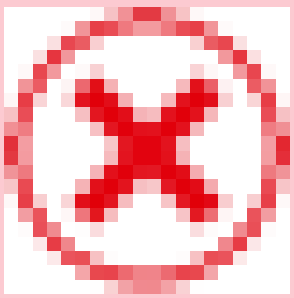
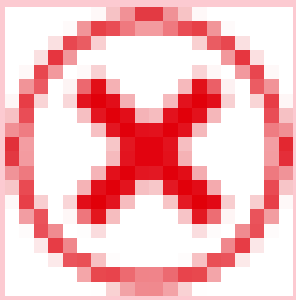
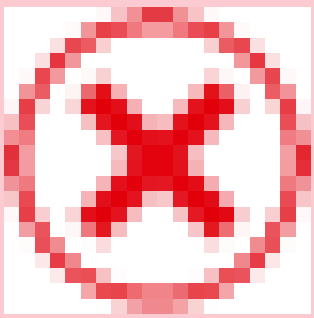
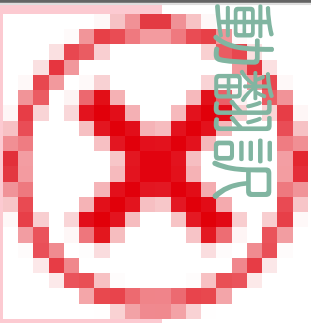
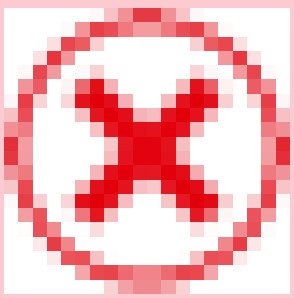
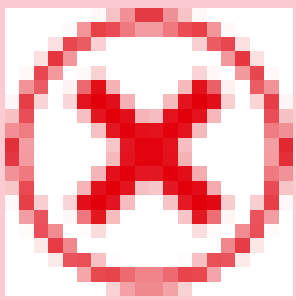
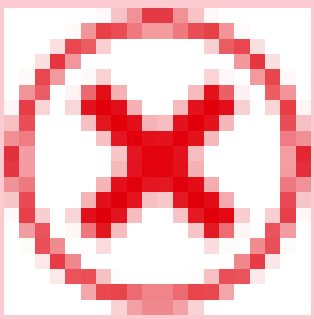
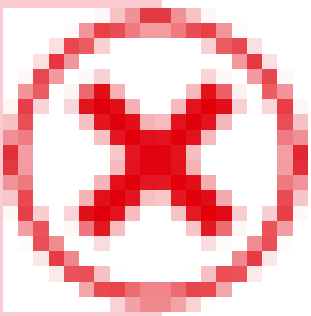
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
例外ルール					
承認ルール					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

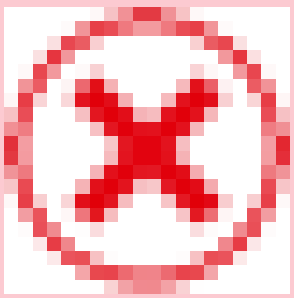
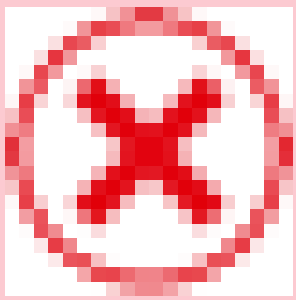
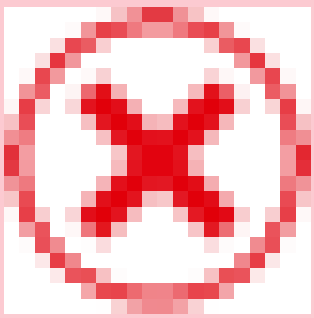
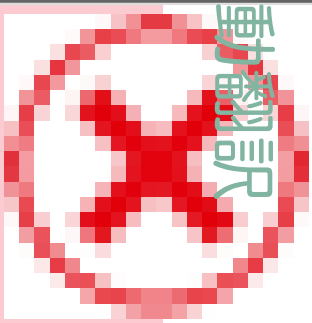
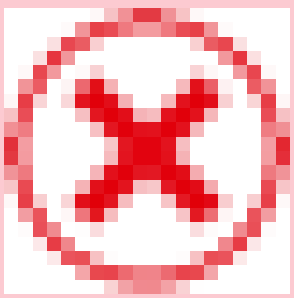
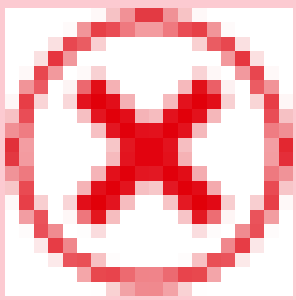
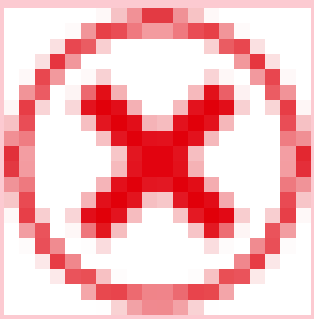
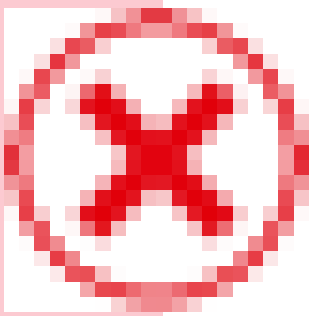
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
分類ルール					
パフォーマンス構成					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

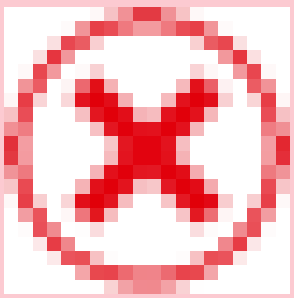
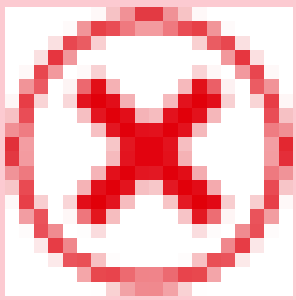
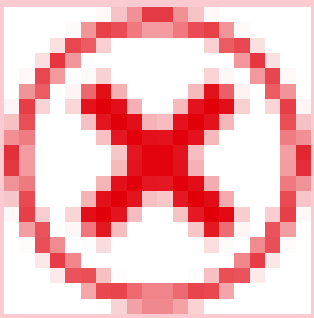
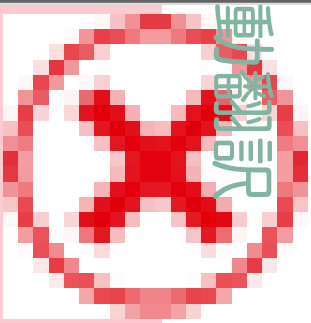
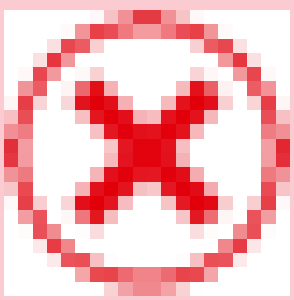
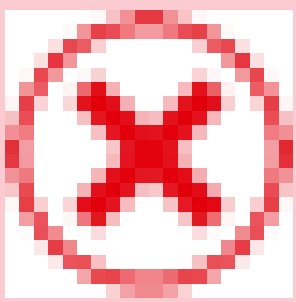
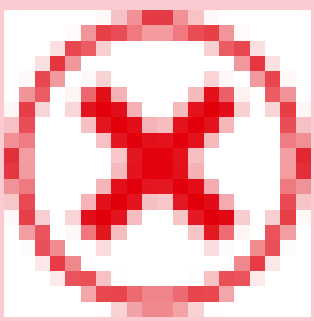
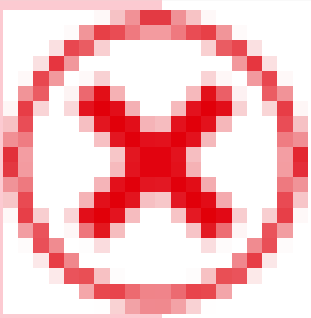
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
VI の粒度の構成					
通知					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

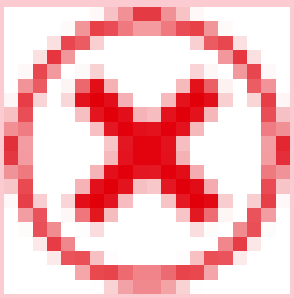
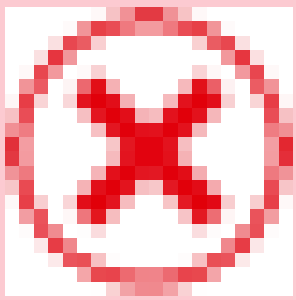
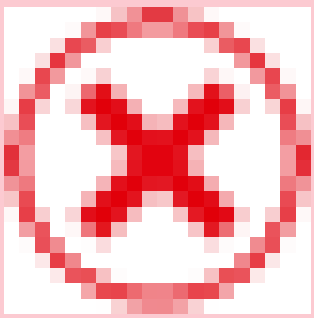
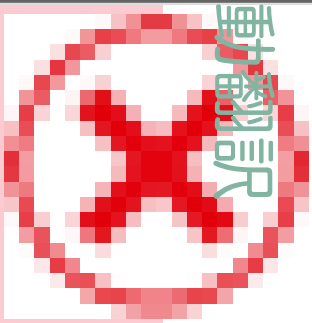
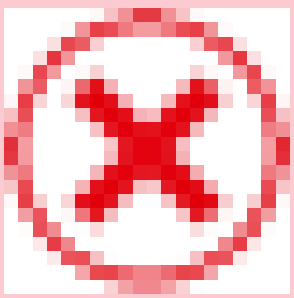
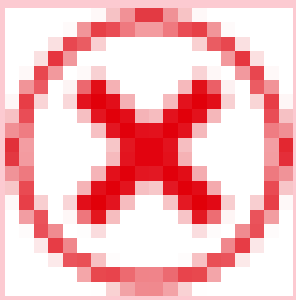
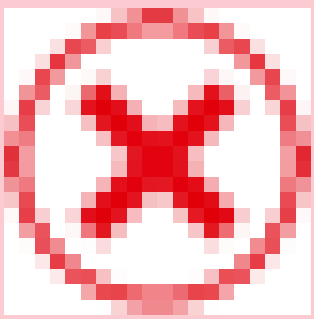
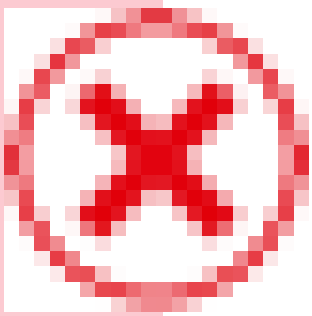
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
メールテンプレート					
キューをインポート					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

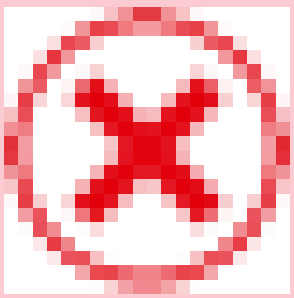
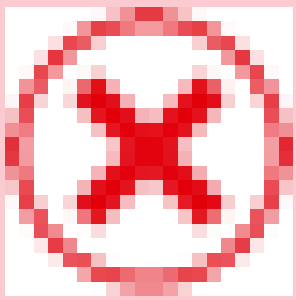
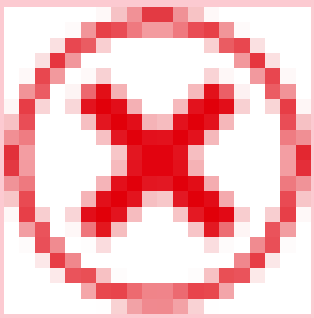
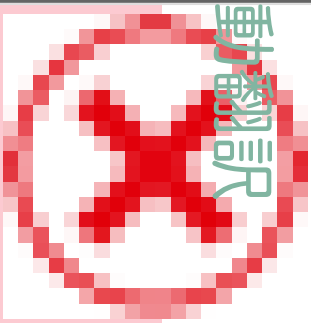
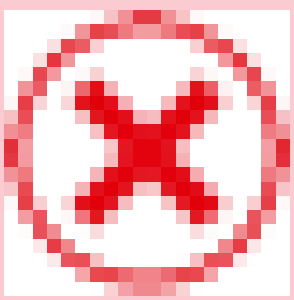
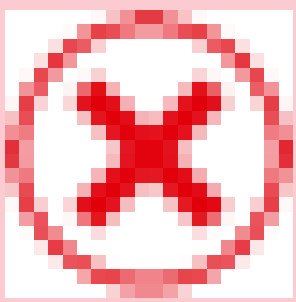
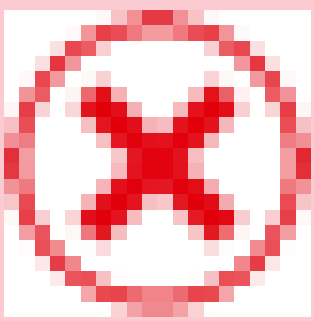
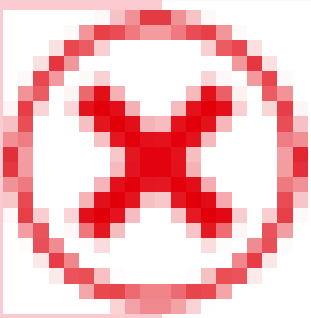
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
統合					
SLA 定義					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

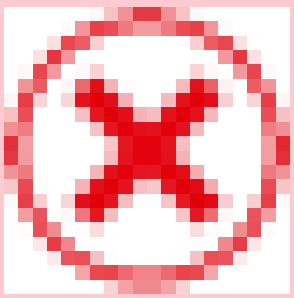
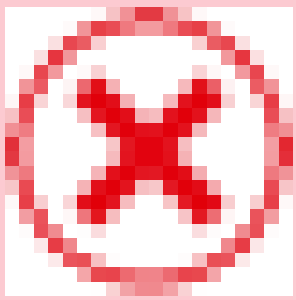
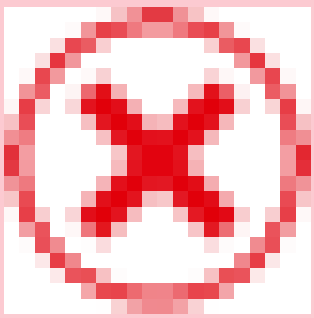
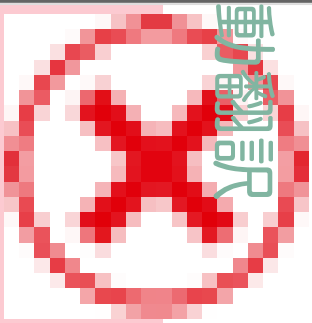
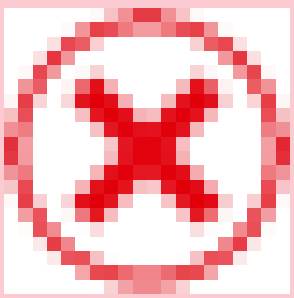
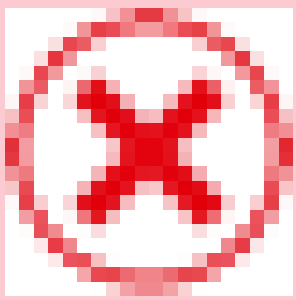
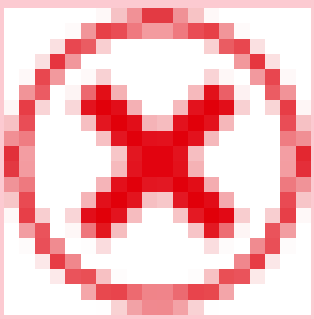
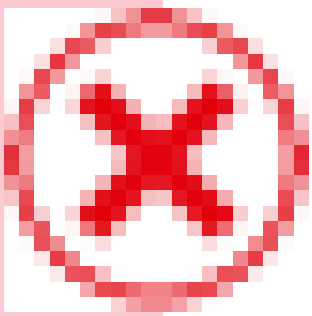
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
SAM NVD の構成					
正規化された重大度マップ					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

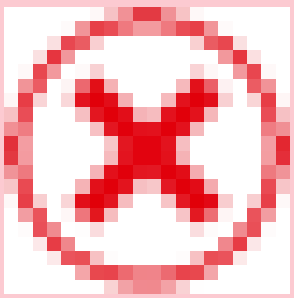
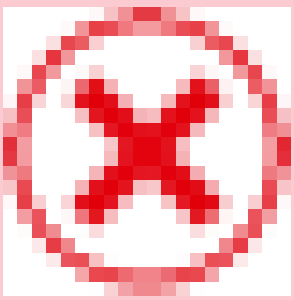
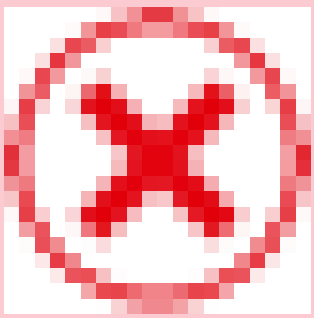
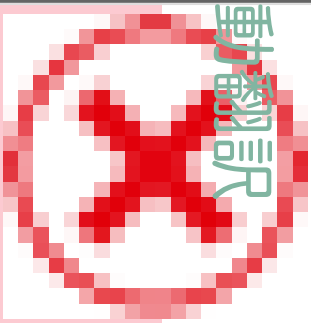
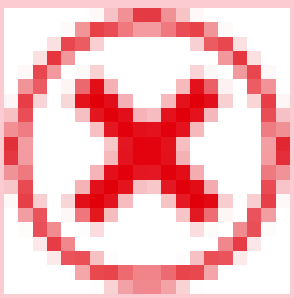
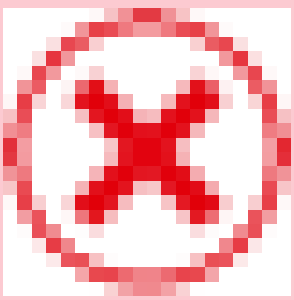
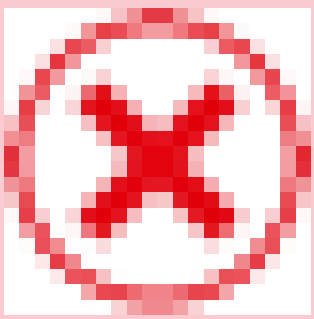
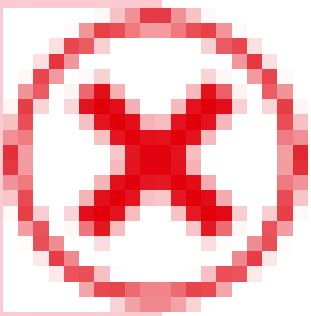
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
スキャン範囲構成					
例外管理					

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

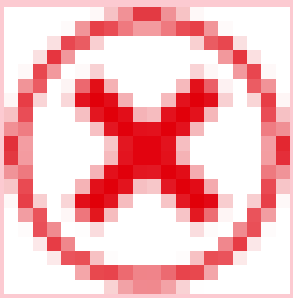
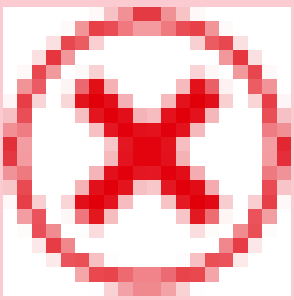
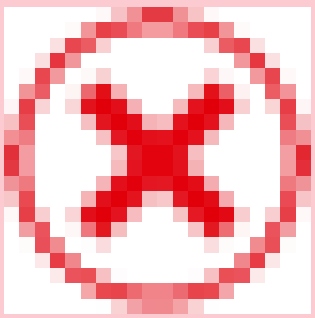
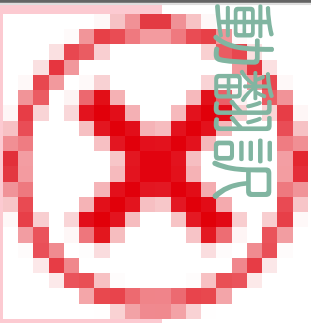
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
使用状況レポート					
診断					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：
sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.unassign_approver

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

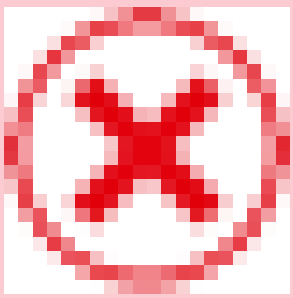
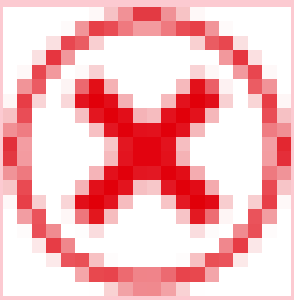
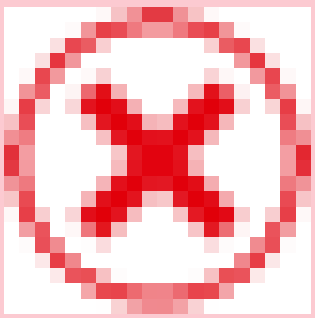
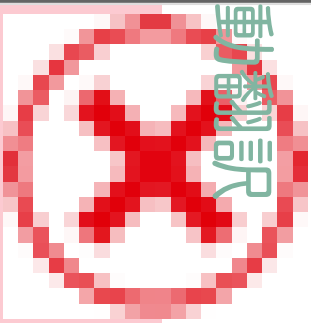
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

(続く)

モジュール	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver	sn
チェック					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

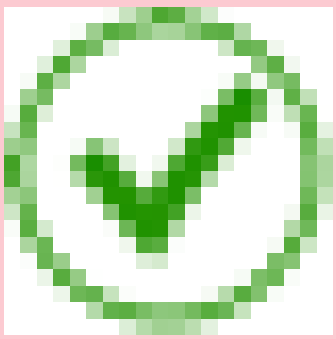
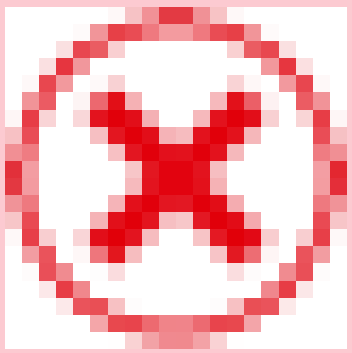
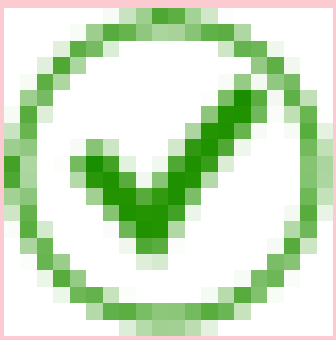
sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
(メインアプリグループ)		
CISO ダッシュボード		
修復の概要		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

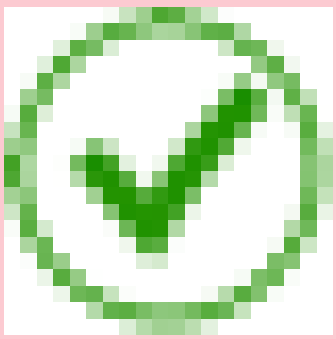
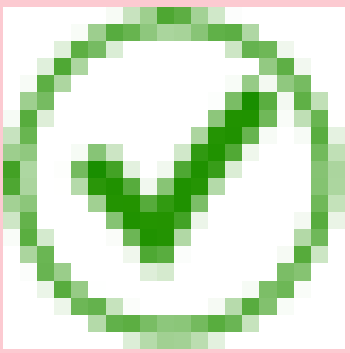
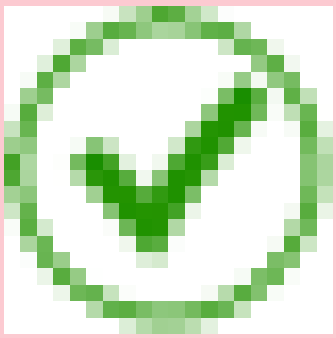
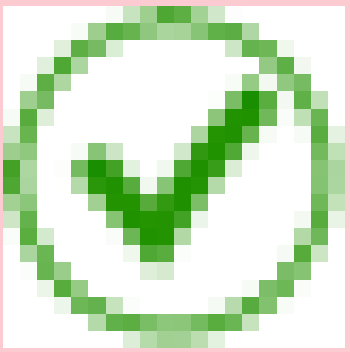
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
脆弱性マネージャーのワークスペース		
概要		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

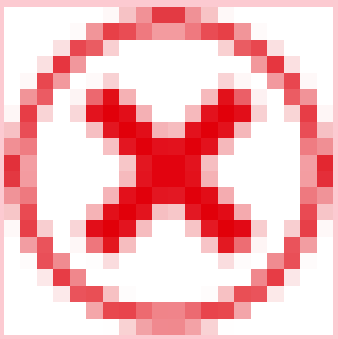
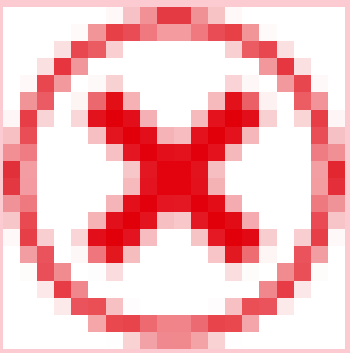
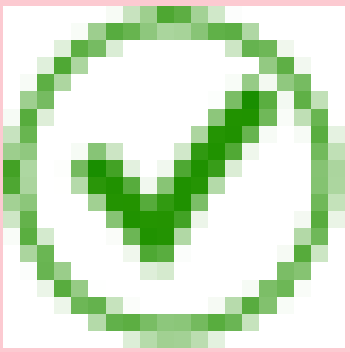
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
IT 修復ワークスペース		
承認者の概要		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

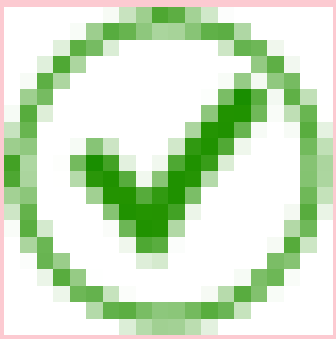
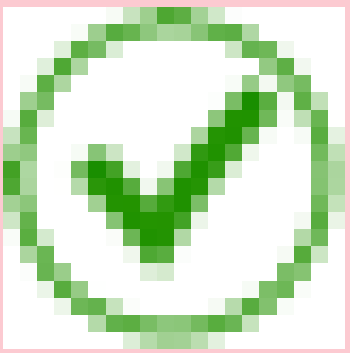
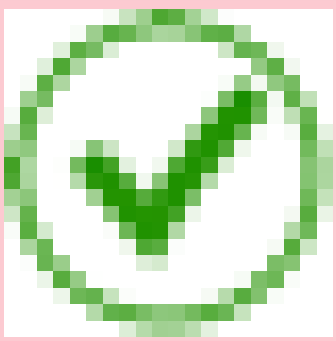
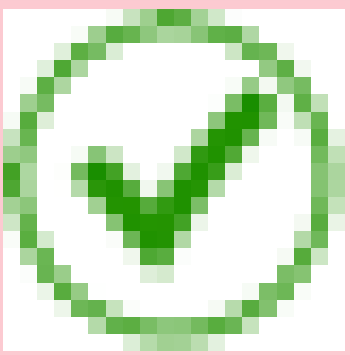
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
概要		
自分の承認		
修復タスク		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

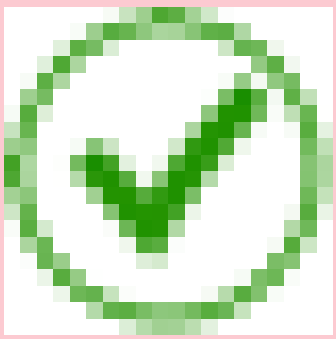
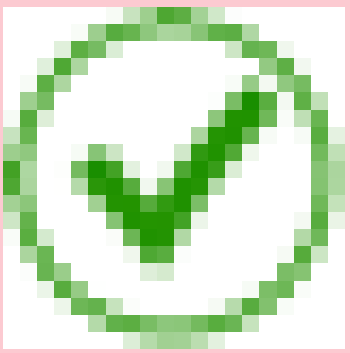
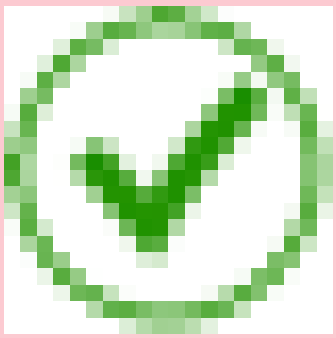
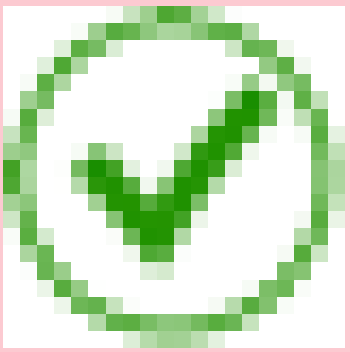
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
有効		
自分にアサイン済み		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

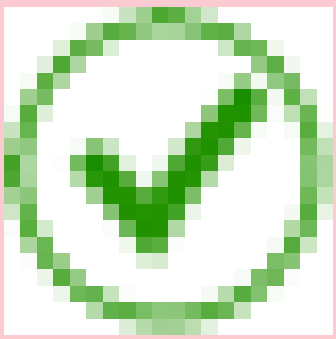
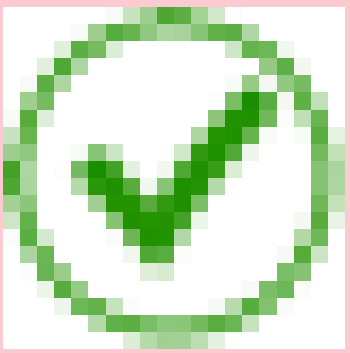
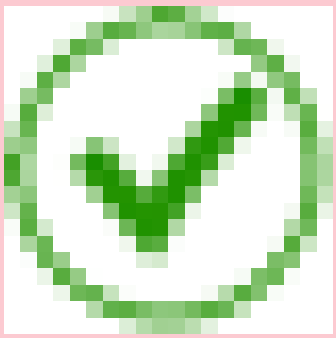
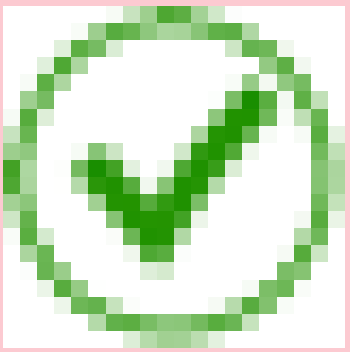
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
所属グループにアサイン済み		
すべて		
脆弱性一致アイテム		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

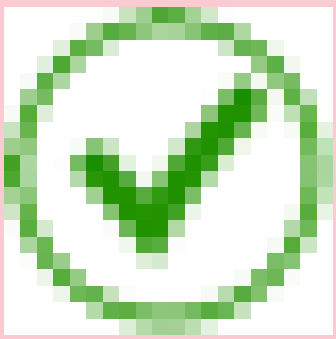
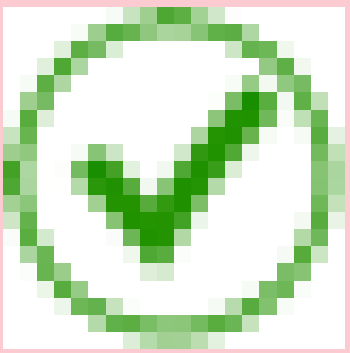
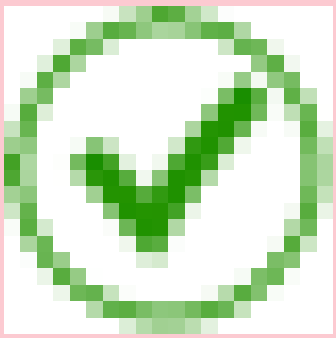
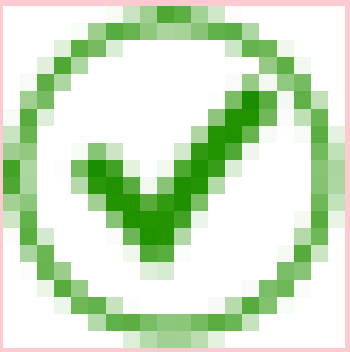
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
重大なリスク		
高リスク		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

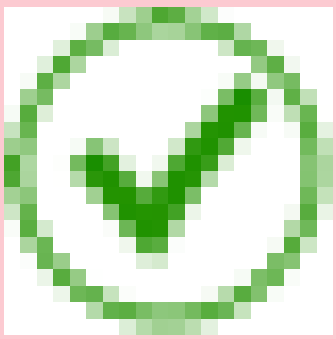
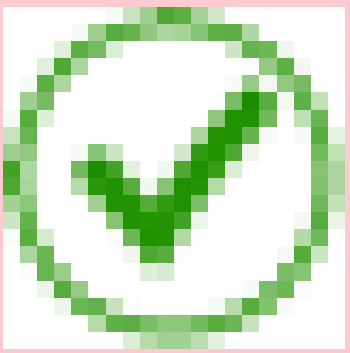
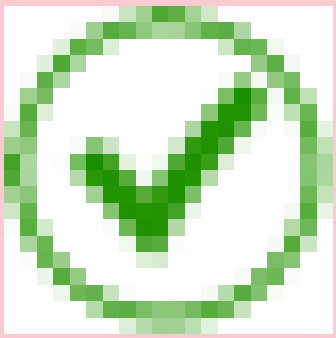
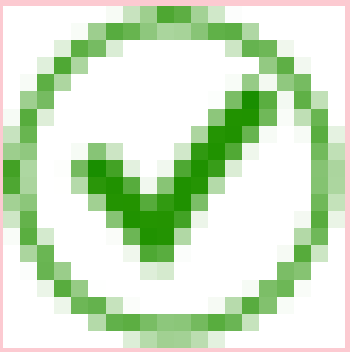
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
エクスプロイト可能		
該当 CI 確認中		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

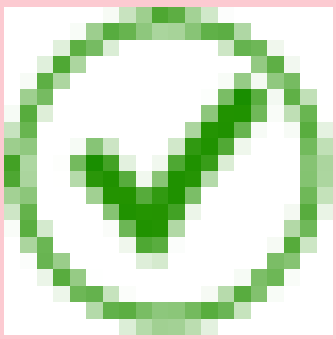
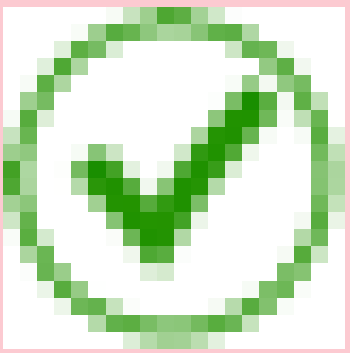
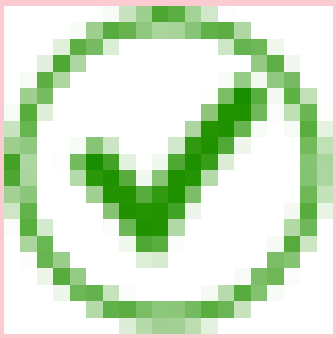
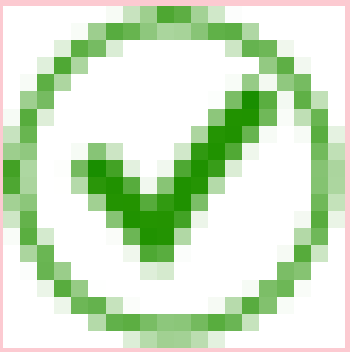
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
CI 不明		
過去 90 日以内		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

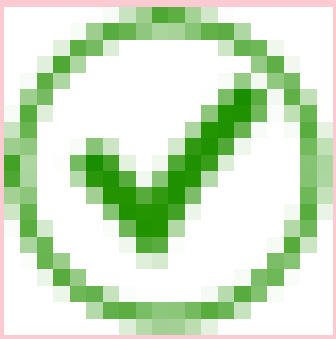
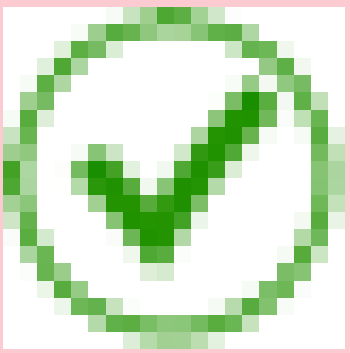
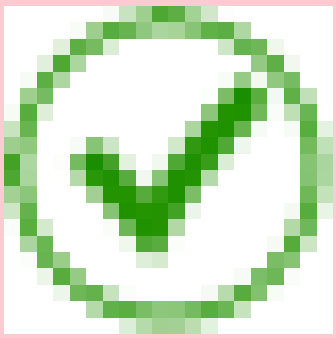
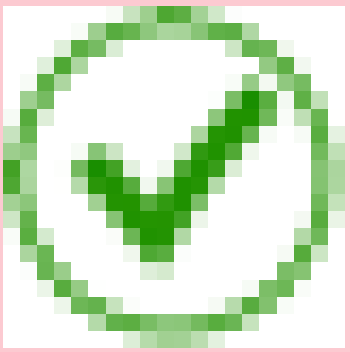
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
91 日以上前		
未アサイン		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

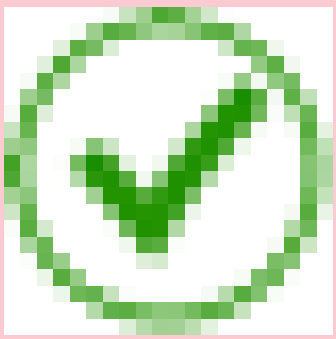
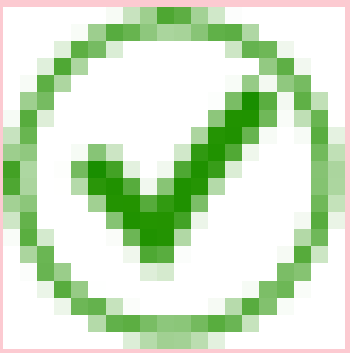
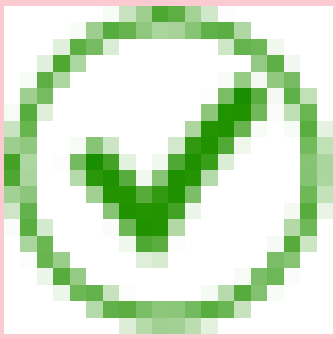
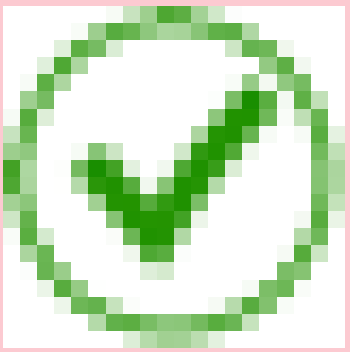
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
修復タスク未割り当て		
廃止		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

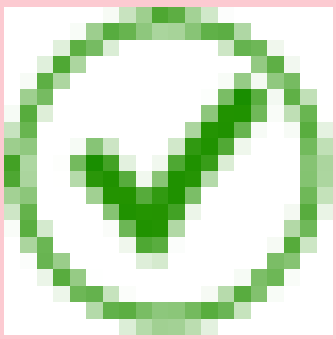
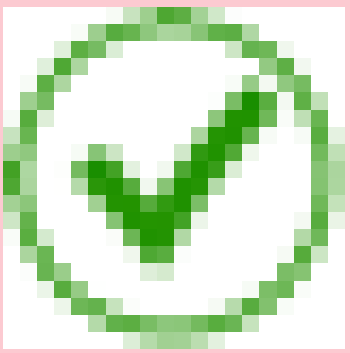
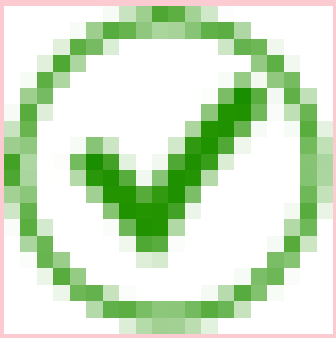
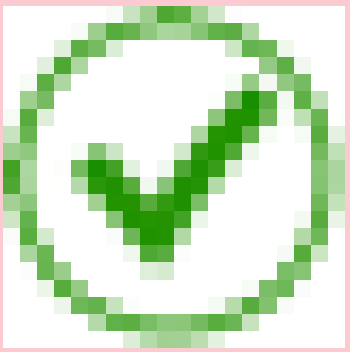
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
複数の保留		
すべて		
ソリューション		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

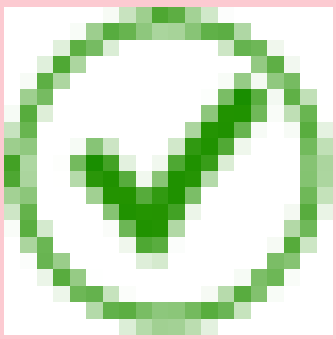
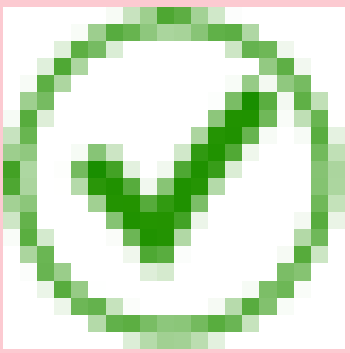
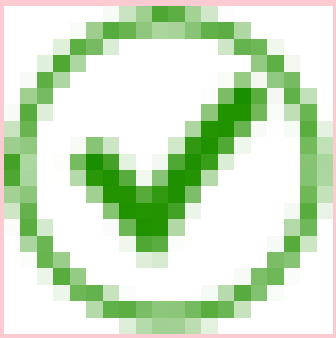
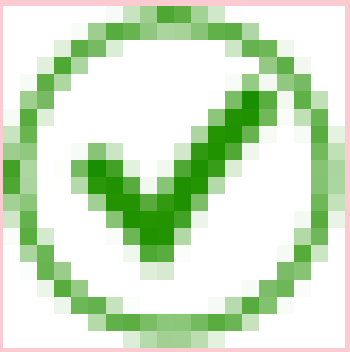
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
すべて		
最高優先度		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

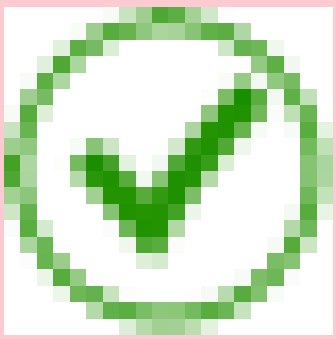
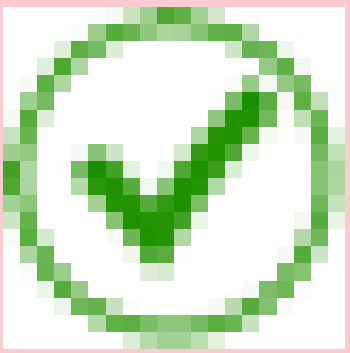
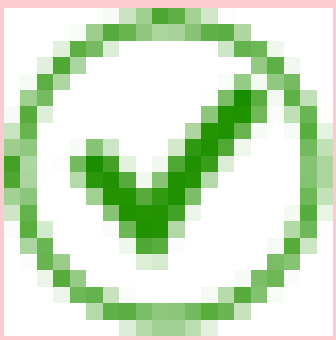
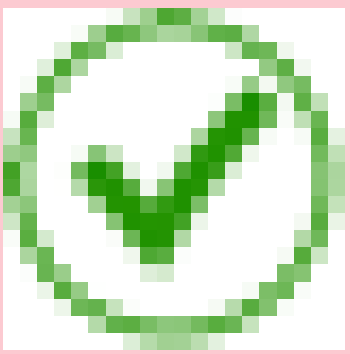
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
脆弱性一致アイテムを使用		
ライブラリ		
NVD		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

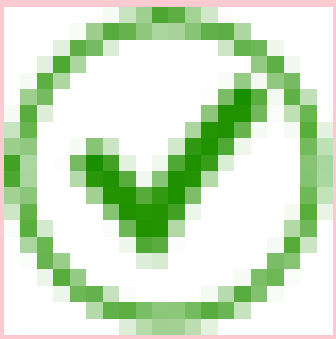
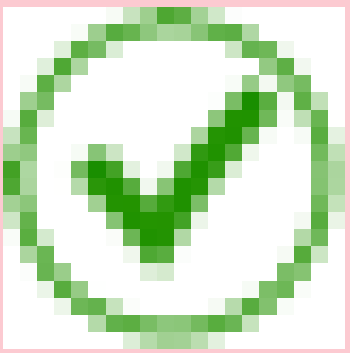
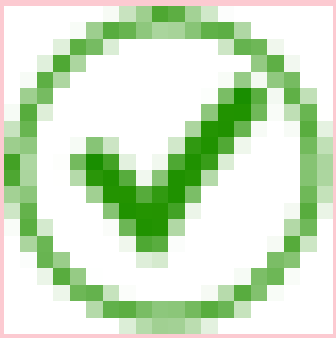
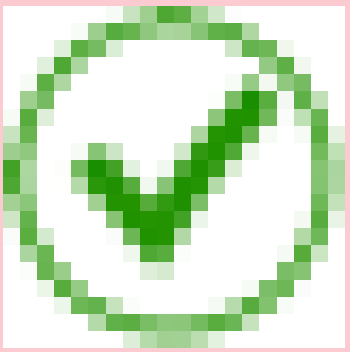
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
CWE		
サードパーティ		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

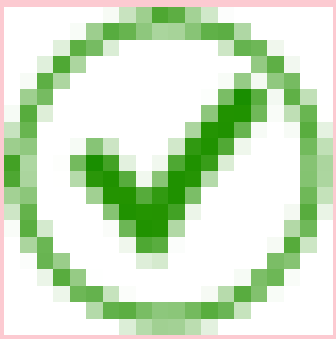
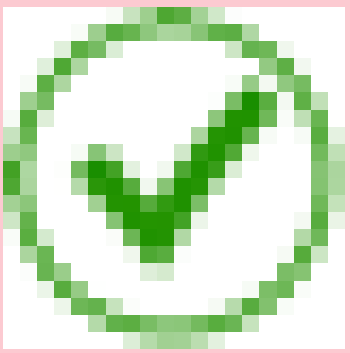
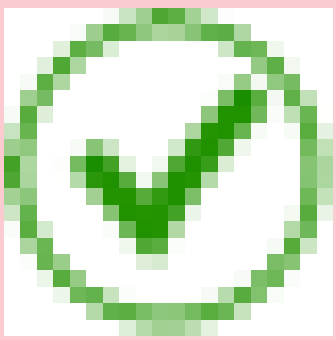
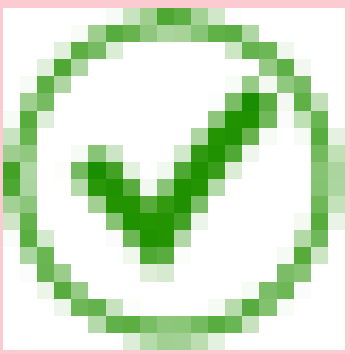
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
脆弱なソフトウェア		
脆弱性スキャン		
エクスポージャーアセスメント		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

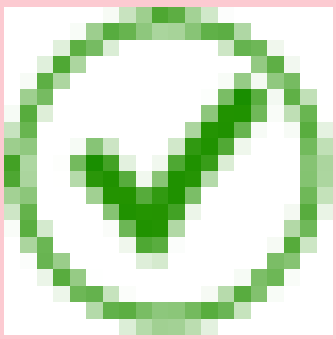
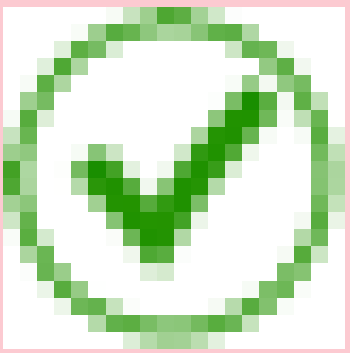
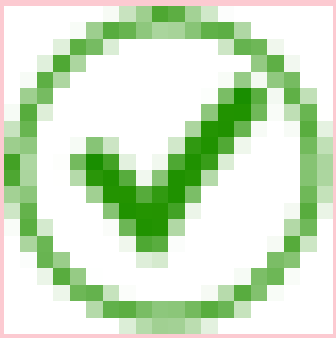
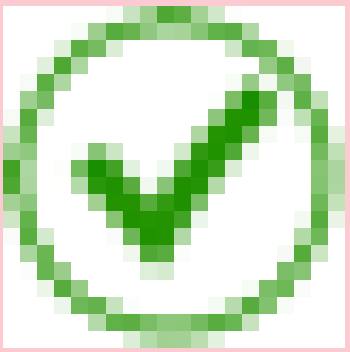
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
スキャン		
スキャナー		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

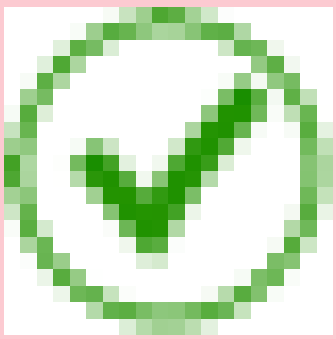
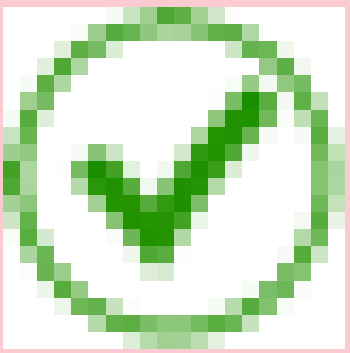
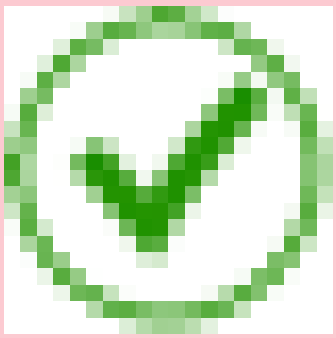
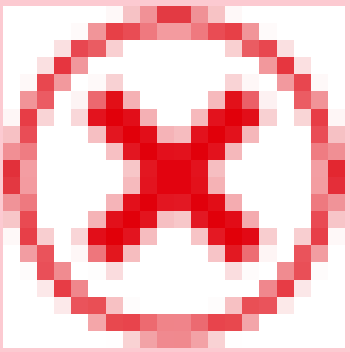
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
スキャンキュー		
スキャナーレート制限		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

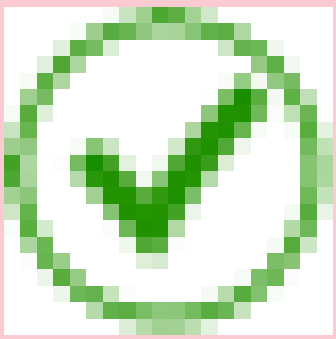
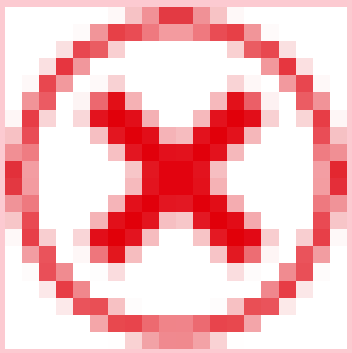
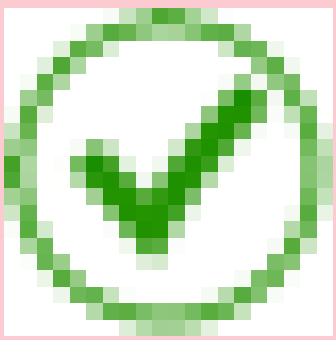
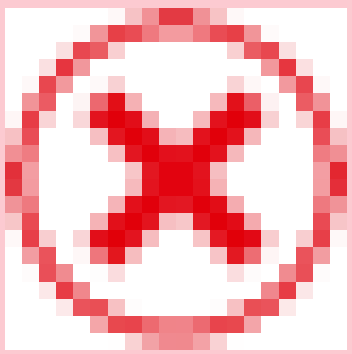
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
レート制限定義		
管理		
セットアップアシスタント		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

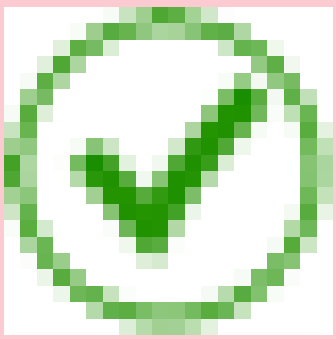
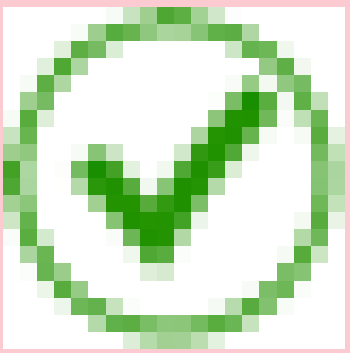
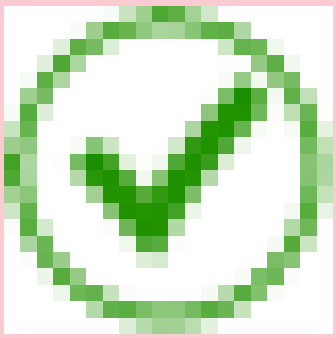
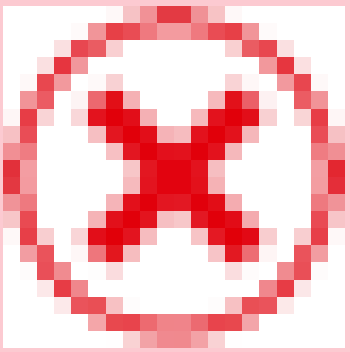
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
監視トピック		
アサインルール		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

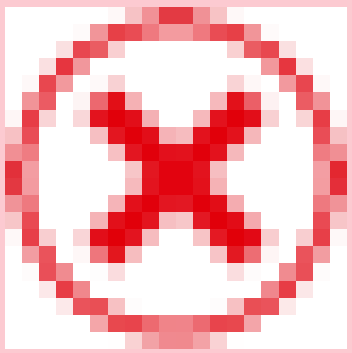
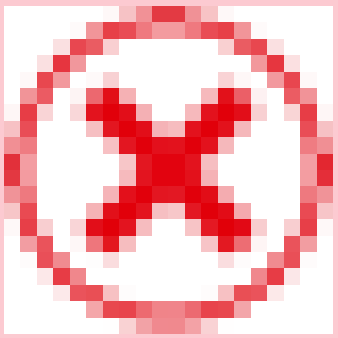
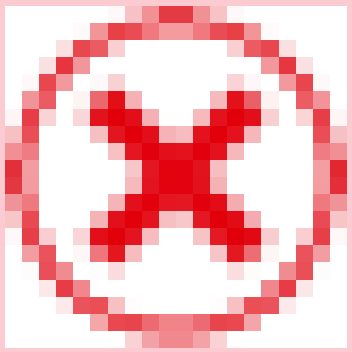
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
修復タスクルール		
アサインの推奨		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

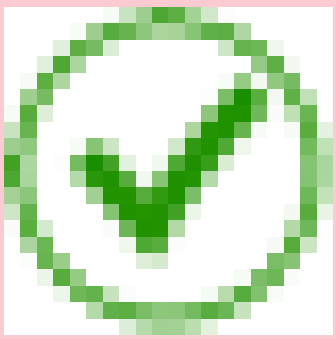
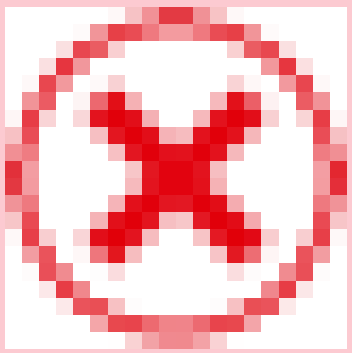
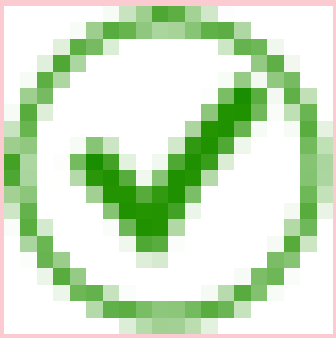
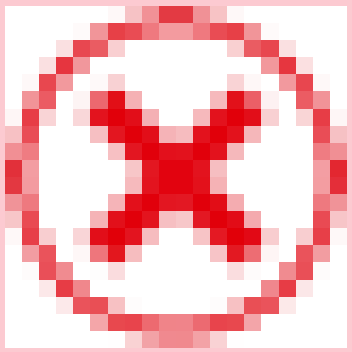
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
脆弱性算出		
脆弱性ロールアップ算出		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

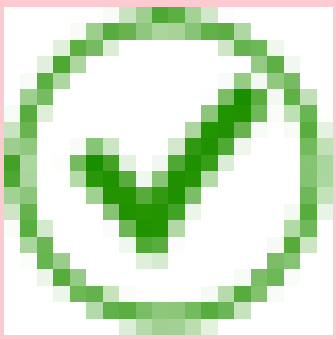
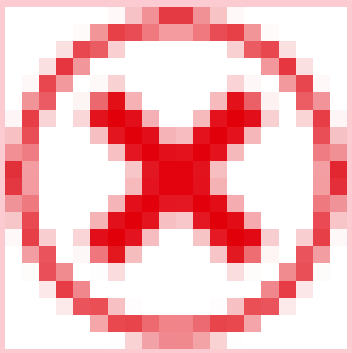
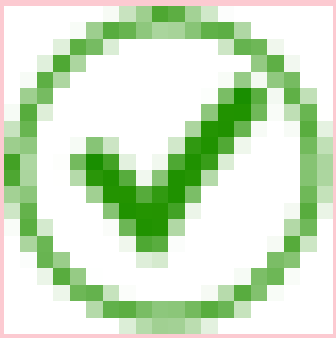
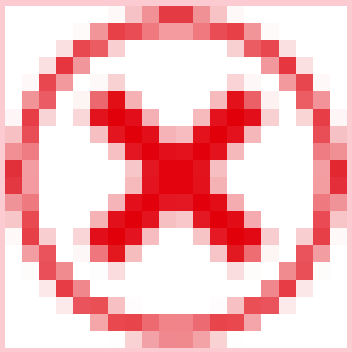
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
修復ターゲットルール		
自動クローズ構成		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

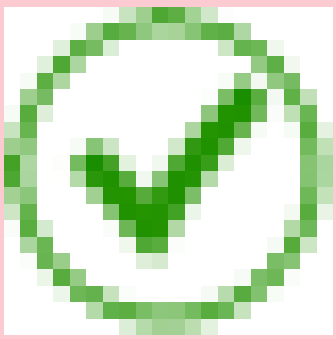
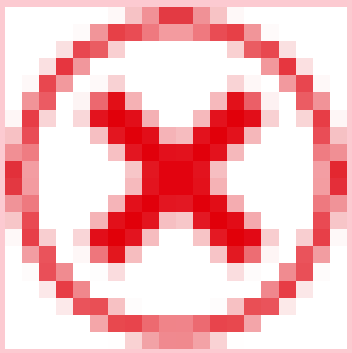
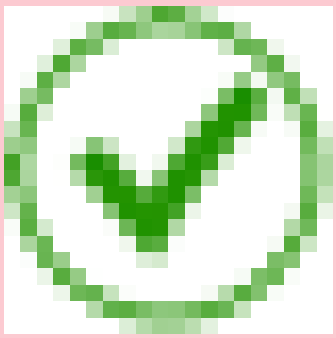
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
ルールの自動削除		
例外ルール		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

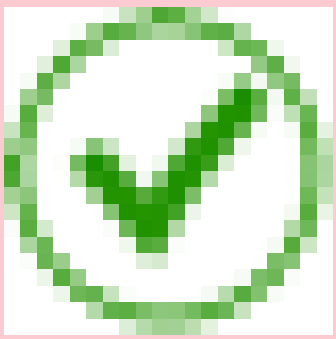
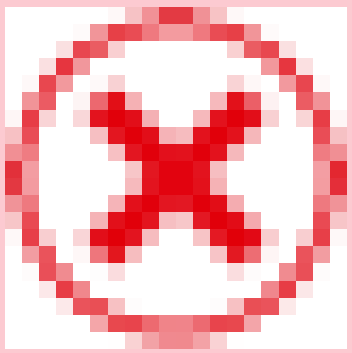
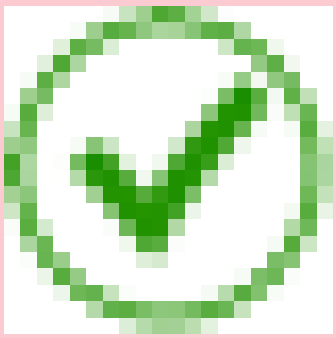
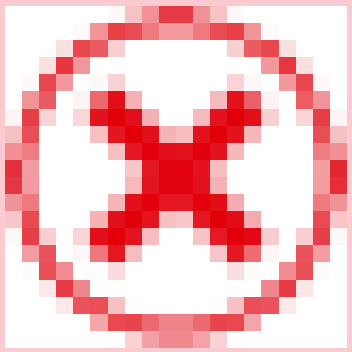
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
承認ルール		
分類ルール		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

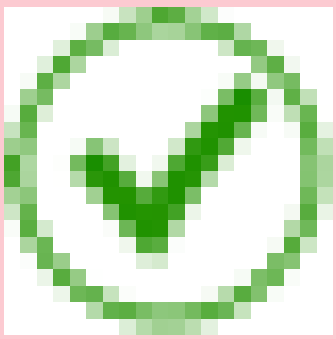
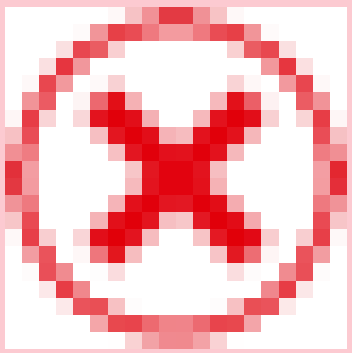
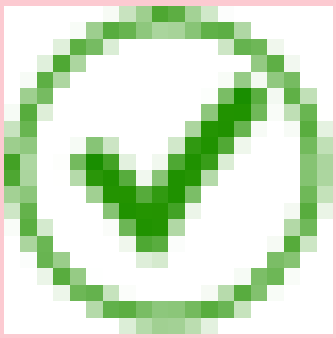
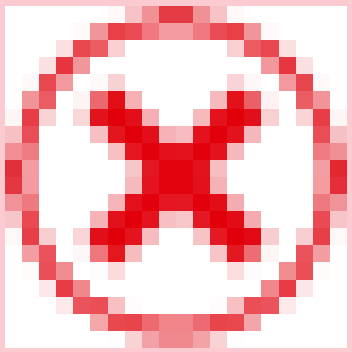
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
パフォーマンス構成		
VI の粒度の構成		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

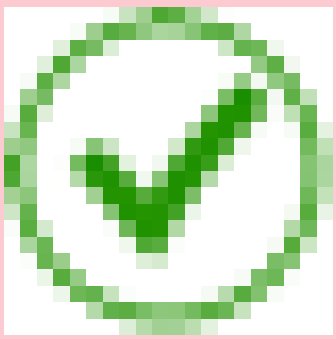
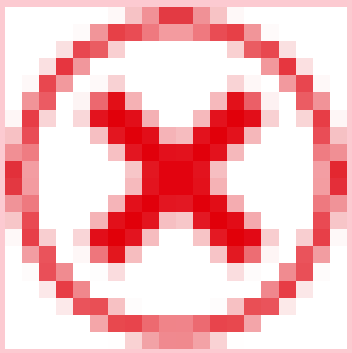
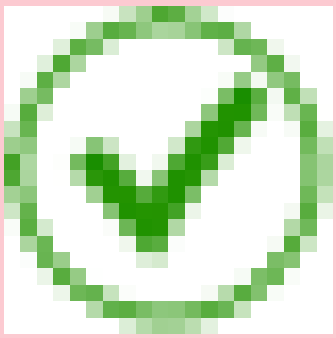
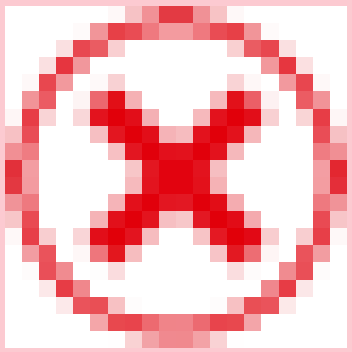
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
通知		
メールテンプレート		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

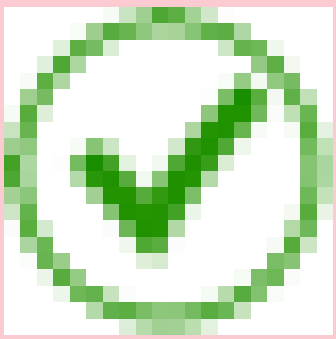
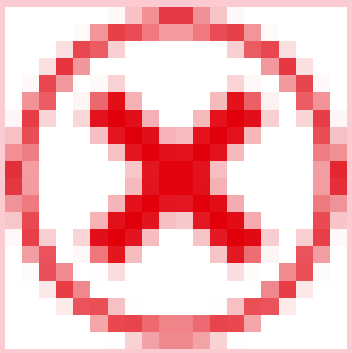
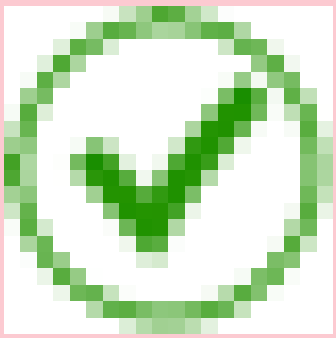
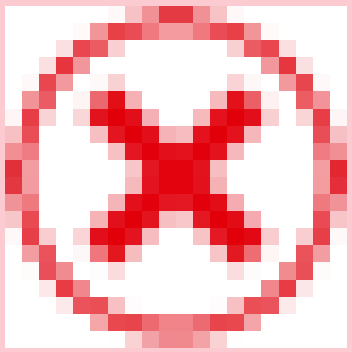
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
キューをインポート		
統合		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

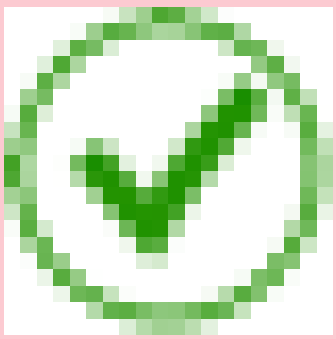
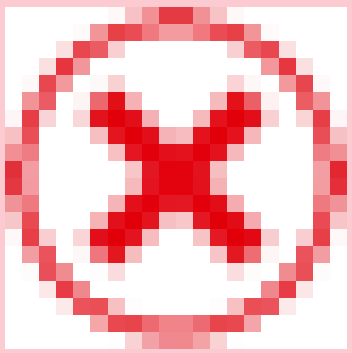
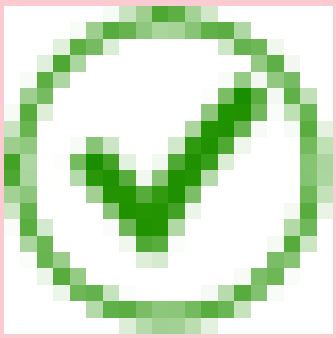
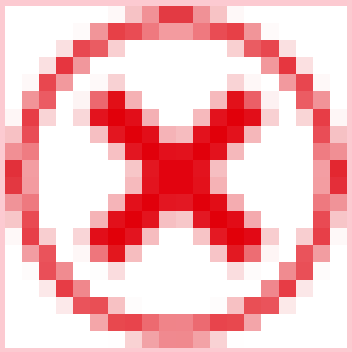
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
SLA 定義		
SAM NVD の構成		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

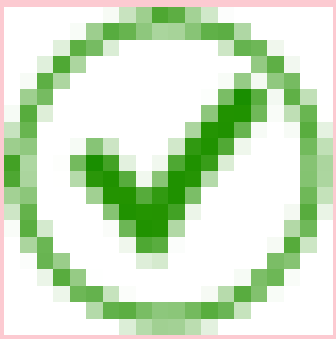
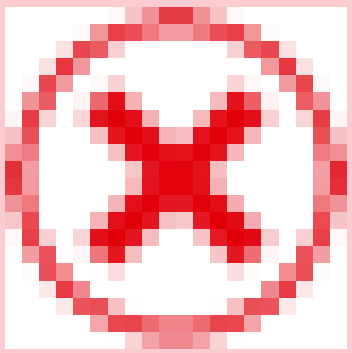
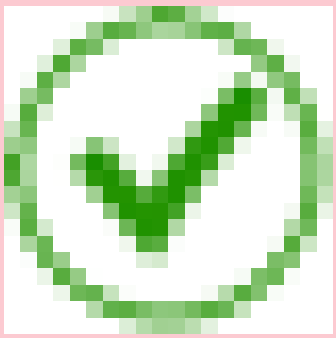
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
正規化された重大度マップ		
スキャン範囲構成		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

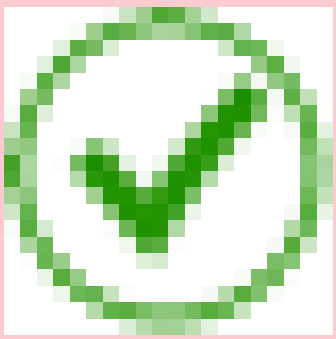
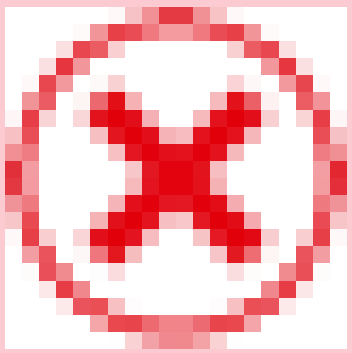
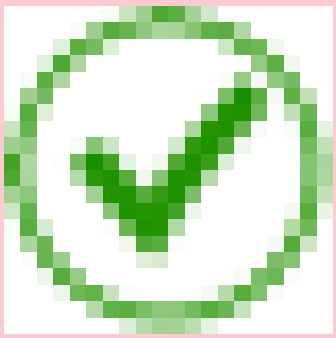
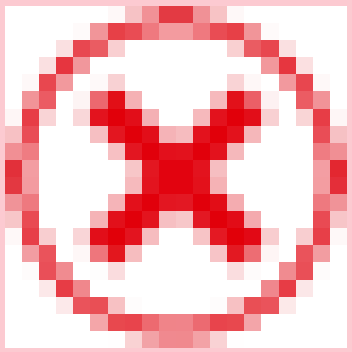
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
例外管理		
使用状況レポート		
診断		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセス：sn_vul.vulnerability_admin、sn_vul.vulnerability_analyst

その他のロールの情報：

sn_sec_cmn.manage_approval_rules、sn_vul.access_setup_assistant、sn_vul.ciso_read、

sn_vul.configure_nvd_integration、sn_vul.configure_scan_coverage_read、sn_vul.configu

sn_vul.exception_approver、sn_vul.false_
positive_approver、sn_vul.manage_assignment_recom_config、sn_vul.manage_assignme

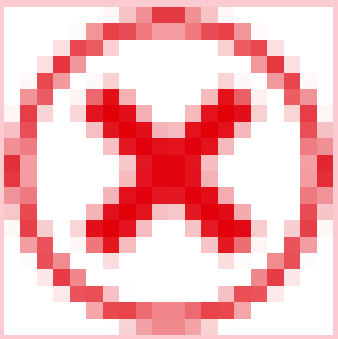
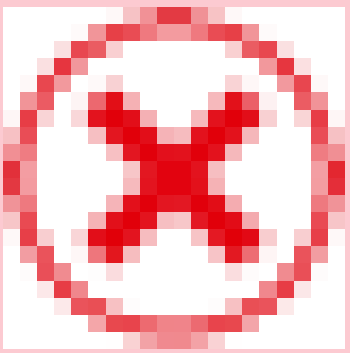
sn_vul.manage_auto_close_stale_vi、sn_vul.manage_auto_delete、sn_vul.manage_classifi
sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment、sn_vul.manage_group_rules、sn_vul.manage_noti

sn_vul.manage_remediation_target_rules、sn_vul.manage_risk_score_configuration、sn_v

sn_vul.read_integrations、sn_vul.read_watch_topic、sn_vul.remediation_owner、sn_vul.u

(続く)

モジュール	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
チェック		

[End]

セキュリティオペレーション の検索

画面ヘッダーの検索アイコンを使用すると、セキュリティオペレーション アプリケーションで情報をすばやく見つけることができます。Zing は、インスタンスのすべてのテキスト検索を実行するテキストのインデックス作成および検索用エンジンです。

始める前に

必要なロール：sn_si.read or higher

手順

1. 画面右上隅の検索アイコン (🔍) をクリックします。
2. 検索基準を入力し、**Enter** を押します。
   セキュリティインシデントレスポンス プラグインをアクティブ化している場合、入力した検索条件により、セキュリティインシデント、セキュリティインシデントレスポンス タスク、または

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティ要求で一致する簡単な説明テキスト、CI、IP アドレス、または URL が表示されます。脆弱性対応 または 脅威インテリジェンス プラグインをアクティブ化している場合、検索結果には脆弱性、脆弱性一致アイテム、脆弱性エントリー、観測事象、IoC、および攻撃モード/メソッドが含まれます。

関連情報

検索の概要

Zing テキスト検索

Security Operations Integration の参考文献

開発者様および ServiceNow パートナー様は、このセクションの情報を参考にして、開発ガイドライン、統合機能、ワークフローなどのサードパーティ統合の内部機能の理解にお役立てください。

ServiceNow セキュリティオペレーション 統合開発のガイドライン

ServiceNow プラットフォームは、外部システムとの統合を開発するためのいくつかのメカニズムを提供します。ServiceNow セキュリティオペレーション 製品スイートは、セキュリティを重視した外部システムとの統合プロセスを簡素化するための統合機能を追加します。

このガイドの概念のほとんどは、標準の ServiceNow 機能についてよく理解していることを前提としています。セキュリティオペレーション スイートと統合するには、少なくとも次の ServiceNow の概念に関する知識が必要です。

- スクリプトインクルード
- 受信/送信 Web サービス
- データソース
- インポートセット
- 変換マップ

テクノロジーパートナープログラム

テクノロジーパートナープログラムの資料に記載されているアプリケーション認定の要件またはガイドラインは、このガイドの情報より優先されます。このガイドは、テクノロジーパートナープログラムの資料に代わるものではなく、既存のドキュメントの補足としてのみ提供されます。

詳細については、テクノロジーパートナープログラムトレーニングコースのブログ投稿 を参照してください。

提供される ServiceNow 統合のタイプ

セキュリティオペレーション アプリケーション (セキュリティインシデントレスポンス、脅威インテリジェンス、および 脆弱性対応) は、他の ServiceNow アプリケーションとシームレスに統合して機能を拡張できます。

次の統合は セキュリティオペレーション ベースシステムで提供されます。

セキュリティインシデントレスポンス – イベント管理統合

イベント管理 アプリケーションの機能が セキュリティインシデントレスポンス をサポートするように拡張されました。セキュリティインシデントレスポンス イベント管理 サポートプラグインは、イベント管理 内のイベントの内容を自動的に解析して、セキュリティインシデントのフィールドに入力します。

対象となるユースケース：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティ情報と イベント管理 (SIEM) ツールからの イベント管理 システムでのセキュリティイベントの作成

提供される便利な機能：

- イベント管理機能：イベント相関、イベントルール、アラートルール
- 結果のセキュリティインシデントへの additional_information 値の自動マッピング

リソース：

セキュリティインシデントイベント管理サポートに関するドキュメント

イベント管理に関するドキュメント

セキュリティインシデントレスポンス - インポートセット API 統合

セキュリティインシデントレスポンス アプリケーションは、イベント管理 を使用してセキュリティ関連イベントをプッシュするだけでなく、セキュリティインシデントを直接作成できるインポートセット API を提供します。セキュリティインシデントインポートセットの REST エンドポイントは、http://localhost:8080/api/now/import/sn_si_incident_import です。

この統合テクニックは、a) イベント管理 がインストールされていない場合、または b) イベント管理 を使用するときに必要なイベント > アラート > セキュリティインシデントフローを経由せずに単にセキュリティインシデントを作成する場合に便利です。

対象となるユースケース：

SIEM ツールから直接セキュリティインシデントを作成する。

提供される便利な機能：

IP、NetBIOS、または完全修飾ドメイン名に基づくセキュリティインシデント作成時の自動 CI 照合。

リソース：

プラットフォームインポートセット API ドキュメント

セキュリティインシデント Web サービスインポートセットに関するドキュメント

脅威インテリジェンス - ルックアップソース統合

ルックアップソースを使用すると、外部のルックアップソースにデータを送信して、そのデータが悪意のあるものかどうかを判断できます。通常、そのデータは IP アドレス、URL、ファイル、またはファイルハッシュです。

対象となるユースケース：

外部ルックアップサービスで IP アドレス、URL、ファイル、またはハッシュを検索します。

提供される便利な機能：

- カタログアイテムとセキュリティインシデントからルックアップを要求する一貫した方法。
- コーディングをほとんど/まったく使用せずに提供されるレート制限およびスロットリング機能。
- ルックアップソースによって検出された問題に対するセキュリティ侵害のインジケーター (IoC) の観測可能エントリーの自動作成。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威インテリジェンス - 脅威ソース統合

脅威ソースは、外部の脅威インテリジェンスリポジトリからデータをプルする機能を提供します。このデータは、システム内に存在するさまざまなセキュリティ侵害のインジケーターテーブルにインポートされます。TAXII 収集と簡易ブロックリストがネイティブにサポートされています。新しい TAXII 収集 (または検出または収集管理サービスに基づくプロファイル) は、エントリーを追加するのと同じくらい簡単です。同様に、新しいシンプルな 1 列のブロックリストを追加するには、新しいレコードを入力し、ブロックリストの URL を指定します。より複雑なデータセットの場合は、URL を呼び出して応答を解析するカスタム統合を提供できます。

対象となるユースケース：

脅威インテリジェンスソースからデータを取得して IoC テーブルにロードします。

提供される便利な機能：

- コーディングなしで簡単なブロックリストと TAXII 収集をサポート。
- データを取得するための REST メッセージを実行するためのシンプルなメカニズム。
- 統合コンポーネントの再利用性のためのデータ取得/処理の分離。
- データソース (およびインポートセット/変換マップ) に返されるデータの受け渡しを処理するためのネイティブサポート。
- 後続の呼び出しにコンテキストを渡す機能により、統合ごとに複数のデータ要求をサポート(ページネーションされた呼び出し)。

リソース：

脅威のソースを定義する

脆弱性対応：スキャナー発動統合

脆弱性スキャナーの発動は、インスタンスからの脆弱性スキャンの呼び出しをサポートする軽量の統合エントリーポイントです。サードパーティの脆弱性スキャナーが非同期に呼び出され、構成アイテムまたは IP アドレスのスキャンがスケジュールされます。

対象となるユースケース：

CI (CI から派生したホスト情報を使用) または IP アドレスをスキャンするようにサードパーティスキャナーに要求します。

提供される便利な機能：

- スキャナー実装を定義するためのシンプルなフレームワーク。
- カタログアイテム、セキュリティインシデントおよび脆弱性一致アイテムからスキャンを要求する一貫した方法。
- スキャン発動の結果によるタスクの自動更新。

脆弱性対応：データ統合

脆弱性データ統合は、サードパーティの脆弱性システムから脆弱性データを取得することを目的としています。これらの統合から期待される出力は、脆弱性エントリーと脆弱性一致アイテムです。この統合により、サードパーティの脆弱性スキャナーが独立して機能し、インスタンス内で脆弱性を処理および追跡できます。

対象となるユースケース：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 脆弱性ライブラリの取得
- 脆弱性/CI のペアリングの取得
- CI と脆弱性管理システムの同期

提供される便利な機能：

- 統合コンポーネントの再利用性のためのデータ取得/処理の分離。
- データソース (およびインポートセット/変換マップ) に返されるデータの受け渡しを処理するためのネイティブサポート。
- 後続の呼び出しにコンテキストを渡す機能により、統合ごとに複数のデータ要求をサポート (ページネーションされた呼び出し)。

リソース：

脆弱性データ統合に関するドキュメント

セキュリティオペレーション 統合構成

ベースシステムに含まれる統合の多くは、セットアップをほとんどまたはまったく必要とせず、同じように動作します。ただし、Qualys クラウドプラットフォーム などの特定の統合では、統合を設定するために個別の手順が必要です。その他にも、さまざまなスキャンおよびルックアップタイプ、さまざまなレート制限をサポートする統合があります。

このセクションでは、サポートされている統合の違いについて説明し、必要に応じてその他のドキュメントを紹介します。

- Carbon Black 統合：Carbon Black API を使用して、セキュリティインシデントに関連するエンドポイントにクエリや操作を実行することで、セキュリティインシデントに対する調査および対応ができます。
- チェックポイントアンチボット - メールパーサー統合：チェックポイントアンチボットからメール通知を取得するメールパーサーを使用して、セキュリティインシデントを作成します。
- Elasticsearch インシデント拡張統合：ログを検索し、関連するサイティング情報をセキュリティインシデントに追加します。
- Have I been pwned? の統合：RESTful サービスを使用して、侵害されたアカウントのリスト (メールアドレスとユーザー名) をすばやく検索できます。
- HPE Security ArcSight ESM - メールパーサー統合：HPE ArcSight ESM からメール通知を取得するメールパーサーを使用して、セキュリティインシデントを作成します。
- HPE ArcSight Logger - インシデント拡張統合：ログを検索し、関連するサイティング情報をセキュリティインシデントに追加します。
- IBM QRadar - インシデント拡張統合：ログを検索し、関連するサイティング情報をセキュリティインシデントに追加します。
- McAfee ESM - メールパーサー統合：McAfee ESM からメール通知を取得するメールパーサーを使用して、セキュリティインシデントを作成します。
- McAfee ESM - インシデント拡張統合：ログを検索し、関連するサイティング情報をセキュリティインシデントに追加します。
- OPSWAT Metadefender 統合の概要：サードパーティの Metadefender スキャナーによって検出された脅威データを 脅威インテリジェンス アプリケーションへダウンロードし、追跡、優先順位付け、および解決できます。
- Palo Alto Networks - AutoFocus の統合：脅威インテリジェンスクラウドサービスである Palo Alto Networks AutoFocus を使用すると、セキュリティインシデント観測事象に関連するセッション情報を検索できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- Palo Alto Networks - Firewall の統合：Palo Alto Networks ファイアウォールを使用すると、ネットワーク、クラウド、およびエンドポイント全体で既知および不明な脅威を防止するためのファイアウォールをセットアップおよび管理できます。
- Palo Alto Networks - WildFire の統合：Wildfire 統合を使用すると、Wildfire でプログラムによって分析ジョブを照会し、シンプルな XML API インターフェイスを介して履歴結果を取得できます。
- Qualys 脆弱性統合の概要：Qualys クラウドプラットフォーム は 脆弱性対応 で使用されます。
- Splunk - インシデント拡張統合：ログを検索し、関連するサイティング情報をセキュリティインシデントに追加します。
- VirusTotal 統合：脅威インテリジェンス で使用されます。このルックアップソースを使用するには、VirusTotal Integration プラグインをアクティブにする必要があります。
- WhoisXML API 統合セットアップ：Whois ルックアップから適切に構造化され一貫性のあるデータを提供します。24 時間 365 日、いつでも正確な Whois データにアクセスできるようにします。

サードパーティ統合のアクティブ化と構成

サードパーティ統合用のプラグインをアクティブ化し、同じ画面から使用するように構成できます。

始める前に

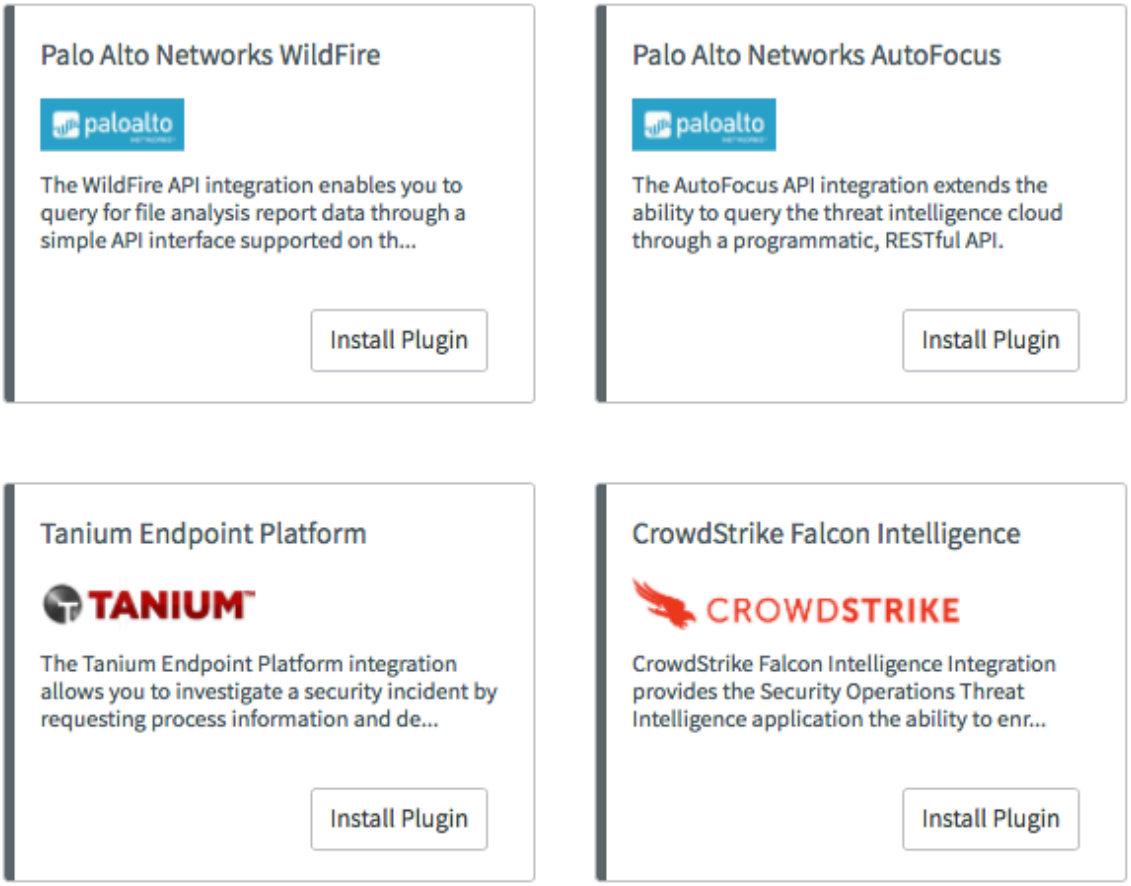
必要なロール：sn_sec_cmn.admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > 統合設定.
   以下のカードグループのように、利用可能なセキュリティ統合が一連のカードとして表示されます。任意のカードをポイントすると、統合の説明が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

2. 特定の統合のプラグインをインストールするには、[プラグインをインストール] をクリックします。

   a. [システムプラグイン] フォームでプラグインの詳細を確認し、[アクティブ化/アップグレード] 関連リンクをクリックします。

   b. [アクティブ化] をクリックします。
   アクティブ化が完了すると、[セキュリティ統合] 画面が再度開き、アクティブ化した統合のボタンのラベルが [構成] になります。

3. [構成] をクリックします。

   注:
   Qualys 脆弱性統合 を構成する場合は、「脆弱性対応 およびサポートされているアプリケーションのインストール」を参照してください。

4. **API** キーを入力します。
5. **[Submit]** をクリックします。

統合の作成

統合を作成し、関連する統合カードを [セキュリティ統合] 画面に追加できます。この手順は、サードパーティ統合を作成するパートナーを対象としています。

始める前に
必要なロール：sn_sec_cmn.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

対象者：サードパーティ統合を作成するパートナー。

手順

1. ナビゲーションフィルターで、「sn_sec_core_integration_item.list」と入力して **Enter** キーを押します。
2. [新規] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
名前	統合の名前。
プラグイン ID	統合を使用するためにアクティブ化する必要があるプラグイン。
順序	この統合カードが表示される順序を示します。
バナーテキスト	リンクをクリックし、統合カードに表示する画像またはロゴを選択し、**[OK]** をクリックします。
インストール	プラグインが既にインストールされているかどうかを示す読み取り専用フィールド。
構成可能	統合を構成できるかどうかを示します。
カテゴリ	統合カードのフィルタリングに使用されます。
簡単な説明	カードのツールヒントに表示される統合の説明。
説明	統合の詳細な説明。

4. フォームヘッダーを右クリックし、[保存] を選択します。
[統合と構成 **(Integration and Configurations)]** 関連リストが表示されます。この関連リストを使用して、統合の構成オプションを定義できます。これらのオプションは、関連する統合カードの [構成] ボタンをクリックすると表示されます。
5. [新規] をクリックします。
6. 必要に応じて、フォームのフィールドに入力します。

フィールド	説明
ラベル	統合アイテムの名前。
名前	統合を使用するためにアクティブ化する必要があるプラグイン。
統合	統合アイテムを定義する統合を表示します。
順序	統合アイテムが表示される順序を示します。
タイプ	リストから、フィールドのタイプを選択します。 ○ 文字列 ○ 整数 ○ 10 進数 ○ 日付

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ ブーリアン ○ パスワード ○ IPv4 ○ IPv6 ○ URL
値	タイプが選択されている関連の値を入力します。選択したタイプに無効な値が入力された場合、統合の実行時にレコードは取得されません。たとえば、URL タイプを選択して 12.32.23.10 の値を入力すると、レコードは取得されません。

7. [Submit] をクリックします。

統合を作成するためのヒント

これらのガイドラインに従うことで、独自の統合を作成する際に発生する可能性のある落とし穴を回避できます。

可能な限り **ServiceNow** プラットフォームの機能を使用する

セキュリティオペレーション アプリケーションに組み込まれた統合機能 (セキュリティインシデントレスポンス、脅威インテリジェンス、および 脆弱性対応) は、既存の ServiceNow プラットフォーム統合機能を拡張または簡素化することを主な目的としています。統合を作成する際に、プラットフォーム機能が存在する場合は必ず使用してください。「独自で作成する」のではなく、以下に示す一般的な ServiceNow 機能を使用できます。

- 送信 Web サービス：サードパーティシステムとのほとんどのインタラクションでは、Web サービス経由で通信されます。このような場合は、プラットフォームの送信 Web サービスを利用します (REST と SOAP がサポートされています)。
- データソース/インポートセット/変換マップ：データを処理して ServiceNow テーブルに挿入する場合、データソースと関連コンポーネントを使用するメカニズムが推奨されます。

可能な場合は常に **Security Operations Integration** フレームワークを使用する

セキュリティオペレーション 統合メカニズムは多くの一般的な問題を解決してきたため、統合ごとに基本機能を再実装する必要はありません。たとえば、脆弱性データと脅威ソースフレームワークは、複数のページを処理し、そのデータをデータソース/変換/インポートセットに渡すことをサポートしています。同様に、スキャンまたはルックアップソースフレームワークは、構成可能なレート制限機能を提供します。一般に、機能または一連の機能を実装する場合は、既存の セキュリティオペレーション 統合フレームワークがユースケースに対応しているかどうかを確認してください。対応している場合は、そのフレームワークを使用します。

必要に応じて既存の **Security Operations Integration** フレームワークを拡張する

セキュリティオペレーション 統合フレームワークで使用されるテーブルとスクリプトのほとんどは、将来のニーズに合わせて拡張できるように設計されています。統合の作成中にユースケースが発生した場合は、そのユースケースに合わせて統合テーブルまたはスクリプトを拡張します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

統合中に発生した問題について ServiceNow にフィードバックを提供する

統合は開発中またはテスト中であるため、問題が発生した場合は必ずフィードバックを提供してください。ワークアラウンドが必要な場合でも、カスタマーサービス & サポート 担当者は、将来の統合で問題を軽減する可能性のある今後のリリースで改善を提供できます。

妥当な負荷でのテスト

統合におけるよくある問題として、現実的な負荷を処理する機能がないことが挙げられます。各統合はスコープ対象のアプリケーションであるため、システムの安定性を確保するためにプラットフォームによる制限が増えます。これらの制限により、実行時間が長いジョブまたは API 呼び出しが終了する可能性があります。長時間実行されているプロセスや大量のデータを処理するプロセスが正常に処理されるようにするには、各呼び出しまたはプロセスにかかる時間を短縮します (通常は、API 要求をページネーションするか、大量のデータをチャンクします)。

統合のトラブルシューティング

これらのトラブルシューティングでは、統合を設定または実行する際に発生することがある一般的な問題を解決するのに役立ちます。

信頼できないまたは期限切れのサードパーティ SSL 証明書の置き換え

統合に SSL 接続が必要な場合は、サードパーティベンダーによって提供された証明書が ServiceNow でまだ信頼されていないか、有効期限が切れていることがあります。証明書を置き換えるか、新しい証明書を追加できます。

始める前に
必要なロール：sn_ti.write

手順

1. サードパーティベンダーから SSL 証明書を取得します。
   たとえば、次のように、Firefox ブラウザーの SSL エンドポイントから X.509 証明書 (PEM) をインポートできます。

   a. ブラウザーのアドレスバーにエンドポイント URL を入力します。
      例： https://<3rdparty>/。

   b. 住所のロックアイコンをクリックします。

   c. [詳細情報] をクリックし、[セキュリティ] タブをクリックします。

   d. [証明書を表示 **(View Certificate)**] をクリックし、[詳細] タブをクリックします。

   e. [エクスポート] をクリックして、PEM をローカルファイルシステムに保存します。

   f. 保存したファイルをテキストエディターで開き、内容をクリップボードにコピーします。
      -----BEGIN CERTIFICATE----- で始まり、 -----END CERTIFICATE----- で終わる必要があります。

2. 次のように移動する。 システム定義 > 証明書.
3. [新規] をクリックし、 統合の新規レコードを作成します 。
4. ダウンロードしてクリップボードにコピーした証明書を **[PEM** 証明書] に貼り付けます。
5. [保存] をクリックします。
   レコード内の他のフィールドは自動的に生成されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Integrations Capabilities Framework 2.0

新しい Integration Capabilities Framework 2.0 は、シンプルで一貫した方法で統合を実装できるように再設計されました。これにより、類似のタイプの統合 (例：観測事象の評判のルックアップ) で一貫したエクスペリエンスが保証されます。

新しいフレームワークには、フロー を使用して実装される機能があります。

拡張フレームワークの実装によるメリットは次のとおりです。

- 実装固有のロジックのないビジネスレベルのコンポーネントのみを含む機能フロー
- 柔軟性を最大限に高めるために、機能フローでさまざまな入力と形式を使用できるようになりました (例：観測事象参照、CI 参照、タスク、任意のテーブルまたは sys_id の組み合わせ)。
- 統合実行のレート制限またはスロットリングが簡単に構成できるようになりました (カスタムコードまたは実装ワークフローの変更を使用して、この操作を実行する必要はありません)。
- 拡張された監査および実行トラッキング機能により、レポートの質が向上し、トラブルシューティングが容易になりました。
- 実装ルーチンの重複を避けるために、高度なエラー処理関数が機能フローに組み込まれています。
- 機能または統合の条件付きトリガーを設定する機能。これにより、インシデントカテゴリに基づいて自動化を柔軟に自動起動できます。
- 統合に入力する前に、許可リストに入れられた観測事象をフィルタリングするデフォルトのフィルター条件がすべての機能に導入されました。

注:
この新しい機能フレームワークは、現在の機能フレームワークをアップグレードするものではありません。両方のフレームワークは並行して機能します。新しい機能フレームワークを活用する方法については、「インストールされた統合での新しい機能フレームワークの使用」および「新しい機能フレームワークとフローの使用」を参照してください。

サポートされる統合とコンポーネント

セキュリティインシデントレスポンスプラグインには、Integration Capabilities Framework 2.0 に記載されているすべての機能フローと、要件に応じて有効または無効にできる標準の高レベルのフィルターが含まれています。

注:
New York リリースで新しい機能統合フレームワークを使用する場合は、ServiceNow 統合ハブスターターパックインストーラープラグインをインストールする必要があります。インストールのサポートについては、カスタマーサポートにお問い合わせください。

サポートされているアプリケーションのバージョン

セキュリティインシデントレスポンス 10.0 以降では、次の統合がサポートされています。

アプリケーション	最低限必要なバージョン
Security Operations Hybrid Analysis 統合	10.0.0
Security Operations PhishTank 統合	10.0.0
Security Operations ThreatCrowd Integration	10.0.0
Security Operations CrowdStrike Intelligence Integration	10.0.0

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション	最低限必要なバージョン
Security Operations 'Have I been pwned?' Integration	10.0.0
Security Operations Metadefender Integration	10.0.0
Security Operations Recorded Future Integration	10.0.0
Security Operations VirusTotal Integration	10.0.0
Security Operations Reverse WhoIs Integration	10.0.0

セキュリティインシデントレスポンス 10.4 以降では、次の統合がサポートされています。

アプリケーション	最低限必要なバージョン
Security Operations RiskIQ 統合	10.0.0
Security Operations Shodan Integration	10.0.0
Security Operations WhoIs Integration	10.0.0
Security Operations Carbon Black Integration	10.3.1
Security Operations Splunk Search Integration	10.3.0
Security Operations ArcSight Logger Integration	10.3.0
Security Operations McAfee ESM Integration	10.3.0
Security Operations Elasticsearch Integration	10.3.0
Security Operations IBM QRadar Integration	10.3.1
Security Operations CrowdStrike Falcon Host	10.3.0

含まれるコンポーネント

新しい機能統合フレームワークには、次のコンポーネントが含まれています。

- 機能：現在の製品にワークフローとして存在する次のすべての機能は、フロー を使用して再設計されています。
  - ブロック要求：ファイアウォール、Web プロキシ、またはその他のコントロールポイントにおけるセキュリティインシデントに関連する観測事象をブロックするための方法を提供します。この機能は、インシデント応答の調査中に、識別された脅威を封じ込めるために使用されます。
  - メールの検索と削除：セキュリティ調査時にメールサーバーを検索し、必要に応じてサーバーからメールを削除する方法を提供します。
  - 構成アイテムを拡張：さまざまなソースからの追加情報で構成アイテムを拡張する一般的な方法を提供します。この機能は、インシデント応答の調査中に、セキュリティインシデントに関連するデータを拡張するために使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 観測事象を拡張：さまざまなソースからの追加情報で観測事象を拡張する一般的な方法を提供します。この機能は、インシデント応答の調査中に、識別された脅威を封じ込めるために使用されます。
- イベントの取り込み：統合ソースからセキュリティインシデントにイベントをマッピングしてセキュリティインシデントを作成する一般的な方法を提供します。
- ネットワーク統計情報を取得：エンドポイントまたはホストから、アクティブなネットワーク接続のリストを取得します。この機能は、調査中にインシデントの拡張に使用されます。
- 実行中のプロセスを取得：エンドポイントまたはホストから、実行中のプロセスのリストを取得します。この機能は、調査中にインシデントの拡張に使用されます。
- ホスト隔離：セキュリティインシデントに関連するエンドポイントまたはホストを隔離する方法を提供します。ホスト隔離は構成アイテム (CI) に対して実行されます。
- ウォッチリストに公開：セキュリティインシデントに関連付けられた観測事象を、セキュリティイベントを監視してアラートを生成するウォッチリストに追加する方法を提供します。この機能は、調査中にインシデント応答の一部として使用されます。
- サイティング検索：さまざまな SIEM または他のログストアで観測事象のインスタンスを検索します。この機能は、環境に悪意のある IoC が存在するかどうかを判断するために使用されます。
- 脅威のルックアップ：脅威インテリジェンスルックアップを実行して、特定の観測事象が既知のセキュリティ上の脅威に関連するかどうかを判断します。この機能は、調査中にインシデント応答の一部として使用されます。

- 新しいテーブル：
  - sn_sec_cmn_capability：機能とその機能を実装するフロー。
  - sn_sec_cmn_capability_implementation：機能のサービスを提供する実際の実装フロー。
  - sn_sec_cmn_capability_execution：実行時の機能の実行レコード。
  - sn_sec_cmn_capability_implementation_execution：実行時の機能実装の実行レコード。
  - sn_sec_cmn_filter_condition：実行時に機能または機能実装に適用できるフィルター条件。
- インクルードスクリプト：CapabilityProcessor：フレームワークのすべての処理コードを処理します。
- レート制限：[期間あたりの機能の最大同時要求数 (Capability Max Concurrent Req Per Period)]：並行実行できる統合の数を定義します。
- スケジュール済みジョブプロセス機能の実装:15 秒ごとに実行され、セキュリティ管理の [プロパティ] ページ (セキュリティインシデント > アドミニストレーション > プロパティ.
  - スケジュール済みジョブのプロセス機能実装の有効化または無効化：このジョブは、機能実装の実行フローを自動的にスケジュールおよび管理します。
  - 自動ルックアップまたは拡張の有効化または無効化：現在の機能フレームワークでセキュリティインシデントに観測事象が追加されたときに、自動脅威ルックアップまたは観測事象の拡張を実行するスケジュール済みジョブを有効または無効にする設定。
  - スケジュール済みジョブのセキュリティインシデント観測事象のルックアップの有効化または無効化：このジョブは、セキュリティインシデントに観測事象が追加された場合に、「脅威のルックアップ」または「観測事象を拡張」ジョブを自動的にスケジュールします。

新しい機能フレームワーク内の構成

このセクションでは、新しいフレームワークで利用可能な構成について説明します。

始める前に

必要なロール：sn_si.admin、flow_designer、action_designer

自動翻訳

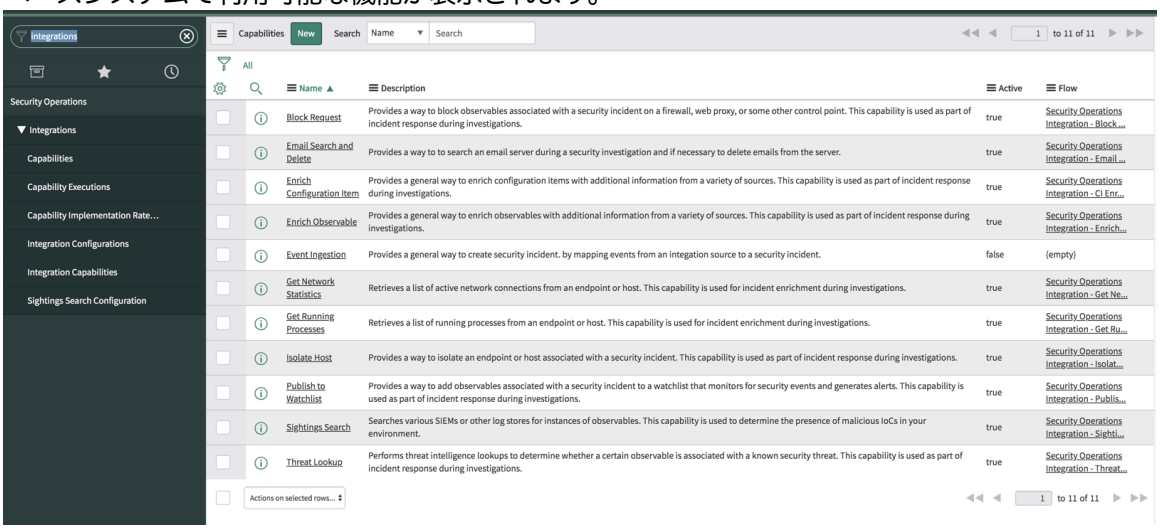
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > 統合 > 機能.

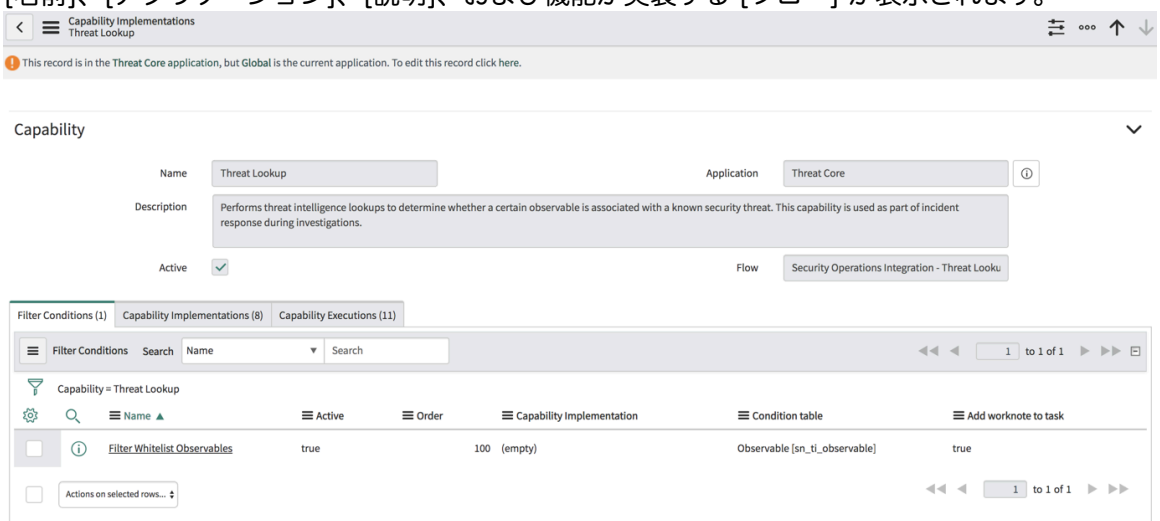
> **注:**
> バージョン 10.4：セキュリティインシデントレスポンス 10.4 以降、[機能] というメニュー名は [統合機能 (フロー)] に変更されました。

2. ベースシステムで利用可能な機能が表示されます。



> **注:**
>
> これらはベースシステムで提供される機能です。機能を使用することも、必要に応じてカスタマイズすることもできます。次の手順では、機能および機能に実装された統合の設定方法について説明します。

3. [名前] 列のリンクをクリックして機能を設定します。
[名前]、[アプリケーション]、[説明]、および機能が実装する [フロー] が表示されます。



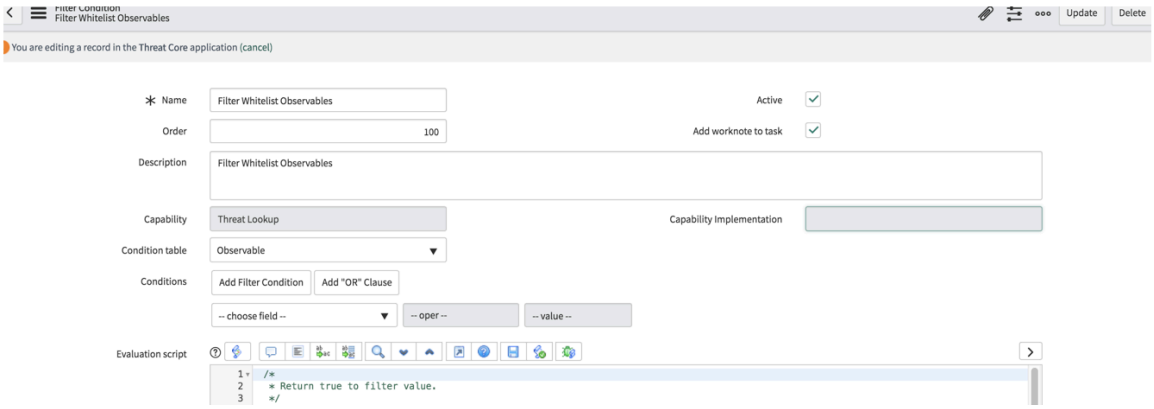
4. [アクティブ] チェックボックスを選択して、機能をアクティブ化します。

- 機能レベルのフィルター条件：統合機能がフローを実装すると、機能フローの起動前に、フローに関連付けられたフィルター条件が実行されます。たとえば、脅威のルックアップ機能には、上に示すように [許可リストに追加された観測事象をフィルター] 条件が含まれています。[名前] リンクをクリックしてフィルター条件を編集します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

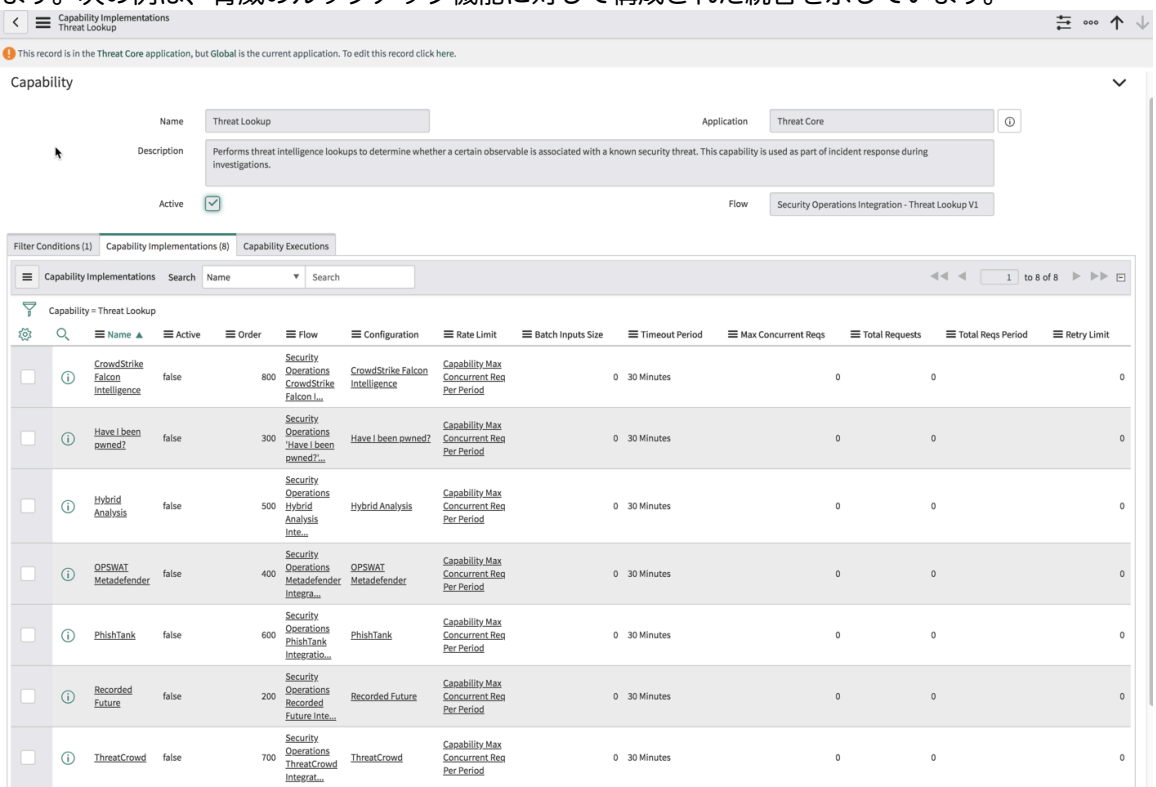
注:
[タスクに作業メモを追加] チェックボックスを選択して、使用するフィルター条件に関する情報を含む作業メモを追加します。



フィルター条件またはスクリプト、あるいはその両方の組み合わせを定義できます。上記の例では、スクリプトを使用してフィルター条件を定義しています。機能フローが実行されると、スクリプトは許可リストに追加された観測事象を検索し、それらをテーブルから削除します。

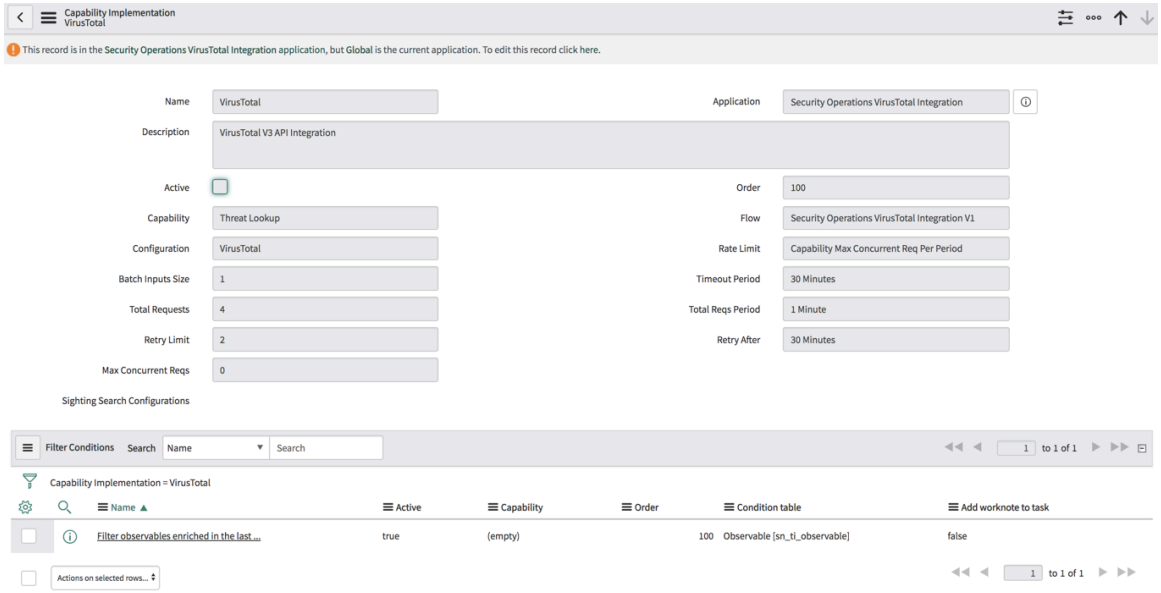
注:
ここで設定したフィルター条件は、[機能実装] タブで定義されたすべてのアクティブな統合に適用されます。

- 機能実装：[機能実装] タブをクリックします。機能に対して構成された実装 (統合) が表示されます。次の例は、脅威のルックアップ機能に対して構成された統合を示しています。



5. [名前] リンクをクリックして機能実装を表示します。
   [名前]、[アプリケーション]、[説明]、および機能が実装する [フロー] が表示されます。
6. [アクティブ] チェックボックスをクリックして、機能をアクティブ化します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



次の詳細を指定できます。

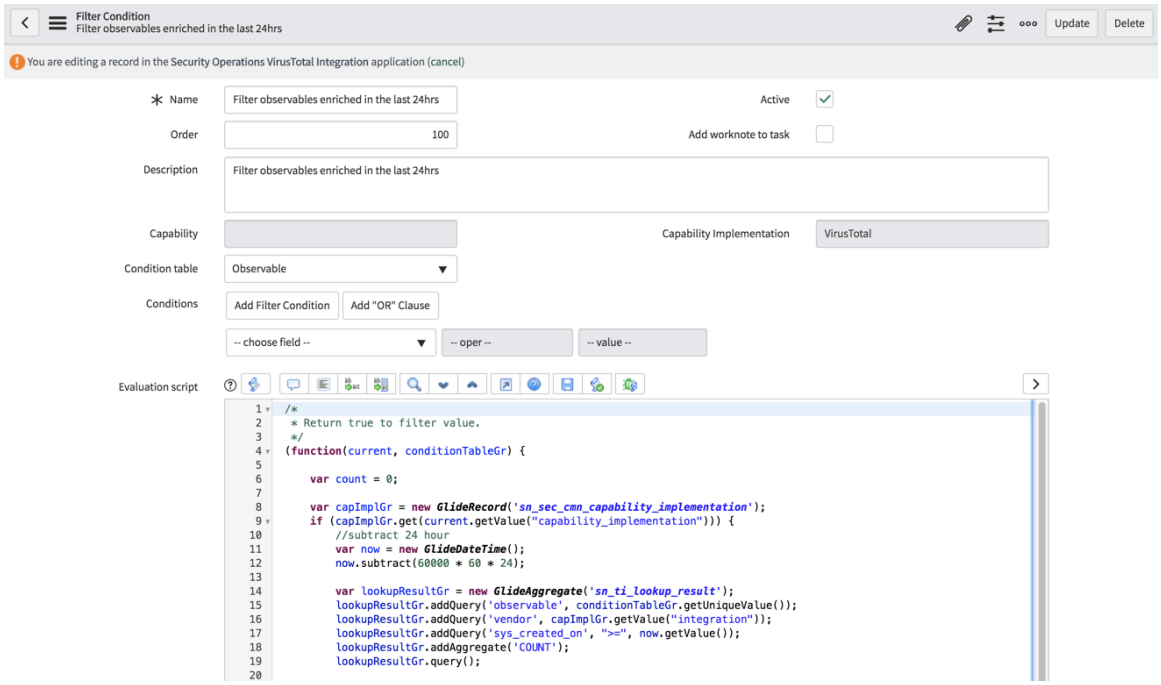
フィールド名	説明
有効	この統合を有効/無効にするには、このチェックボックスを選択します。 **注:** の統合タイルを使用してこの統合を構成する場合 セキュリティ オペレーション > 統合 > 統合構成ページでは、このフラグは自動的に [アクティブ] に設定されます。
順序	統合が実行される順序を示します。
機能	この統合によって実装される機能。
フロー	機能を実装するサブフロー。
構成	この機能の統合構成。 **注:** これは、最初はベースシステムで提供されるデフォルト構成に設定されます。[統合構成] ページの統合タイルを使用して統合を構成すると、この値は作成された新しい構成に自動的にリセットされます。
レート制限	実行時に実行できる (並列または時間単位あたりの) 統合の数を示します。
バッチ入力サイズ	各実行のバッチ入力サイズ。たとえば、サイティング検索統合の場合、生成されるクエリが大きくなりすぎないように、観測事象を 50 のバッチにグループ化することができます。ゼロは制限がないことを示します。
タイムアウト期間	機能実装フローがキャンセルされるまでの最大期間。ゼロはタイムアウト期間がないことを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド名	説明
要求合計	実装実行要求の合計数。このフィールドを [合計要件期間] フィールドとともに使用して、サービスへの要求数を制限できます。たとえば、この数を 1 分あたり 4 件の要求に制限できます。
合計要件期間	期間あたりの許可される実行要求の合計数。
再試行制限	失敗した実行要求に許可される再試行回数。この制限は、条件が満たされたときに実行要求を再試行するように統合で [再試行] フラグが設定されている場合に適用されます。 たとえば、一定期間そのサービスのライセンス制限を超えた場合、またはサービスがダウンしている場合に、再試行要求が行われます。
後で再試行	失敗した実行要求の再試行が試みられるまでの期間。
最大同時要求	同時実装実行要求の最大数。ゼロは制限がないことを示します。
サイティング検索構成	実行できるデフォルトのサイティング検索クエリ。

[フィルター条件] セクションの [名前] リンクをクリックして、実装に定義された条件を設定します。フィルター条件を追加または削除し、必要に応じてスクリプトを変更して、レコードを更新します。



インストールされた統合での新しい機能フレームワークの使用

このセクションでは、既存の統合に新しいフレームワークを使用する方法について説明します。

以下の手順を使用して、既にインストールおよび構成されている統合 (「サポートされる統合とコンポーネント」のサポートされている統合のリストを参照) で新しい機能フレームワークを使用できるようにします。

注:
セキュリティインシデントレスポンス 10.0.2 で利用可能な Integration Capability Framework 2.0 は、[脅威のルックアップ] および [観測事象を拡張] 機能の実装をサポートしています。他の機能の実装は将来のリリースで利用可能になる予定です。

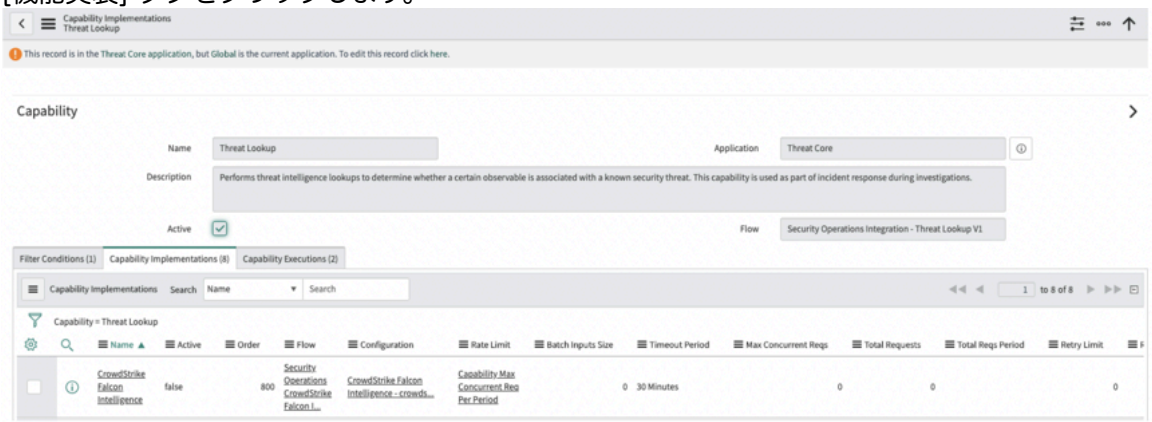
事前準備

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

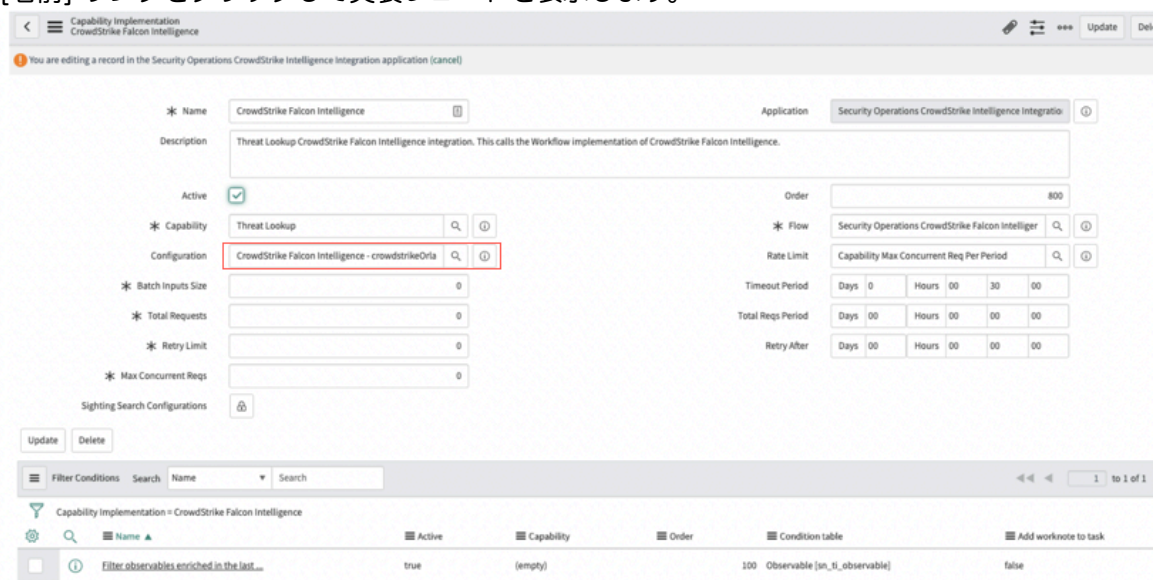
自動翻訳

- 必要なロール：sn_si.admin
- セキュリティインシデントレスポンス 10.0.2

1. 次のように移動する。 セキュリティオペレーション > 統合 > 機能.
2. [脅威のルックアップ] 機能をクリックします。
3. [機能実装] タブをクリックします。



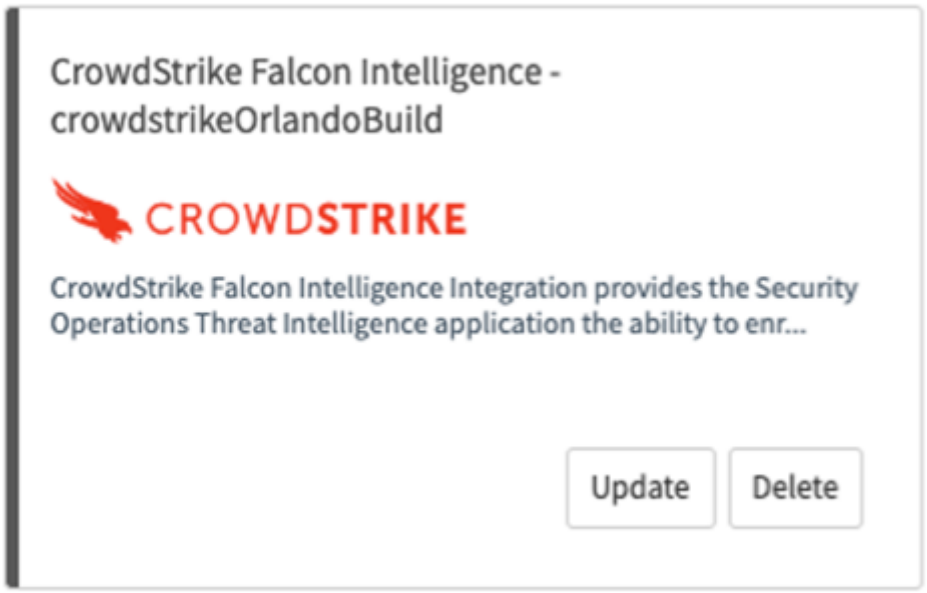
4. 4. 対象の統合の機能実装レコードを表示します (例：Crowdstrike Falcon Intelligence)。[アクティブ] 列の値は **[False]** である必要があります。
5. [名前] リンクをクリックして実装レコードを表示します。



6. [**Active** (有効)] チェックボックスをオンにします。
7. 実装レコードが正しい設定レコード (統合のためのタイル名) を指していることを確認します 統合設定 > 設定を表示 (はい)) を開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



8. 実装は、新しいフレームワークで使用できます。

> **注:**
> セキュリティインシデントレスポンス 10.0.2 とともにインストールされている場合、サポートされているすべての統合は、新しい統合機能フレームワークで自動的に有効になります。

新しい機能フレームワークとフローの使用

以下の手順を使用してフローを作成し、新しい機能フレームワークによって提供されるサブフローを呼び出します。

始める前に

- 必要なロール：sn_si.admin、flow_designer、action_designer
- サポートされている統合のいずれかをインストールします (「サポートされる統合とコンポーネント」を参照)

次の手順では、サンプルフローを作成し、新しい機能フレームワークによって提供されるサブフローのいずれかを呼び出す方法を説明します。

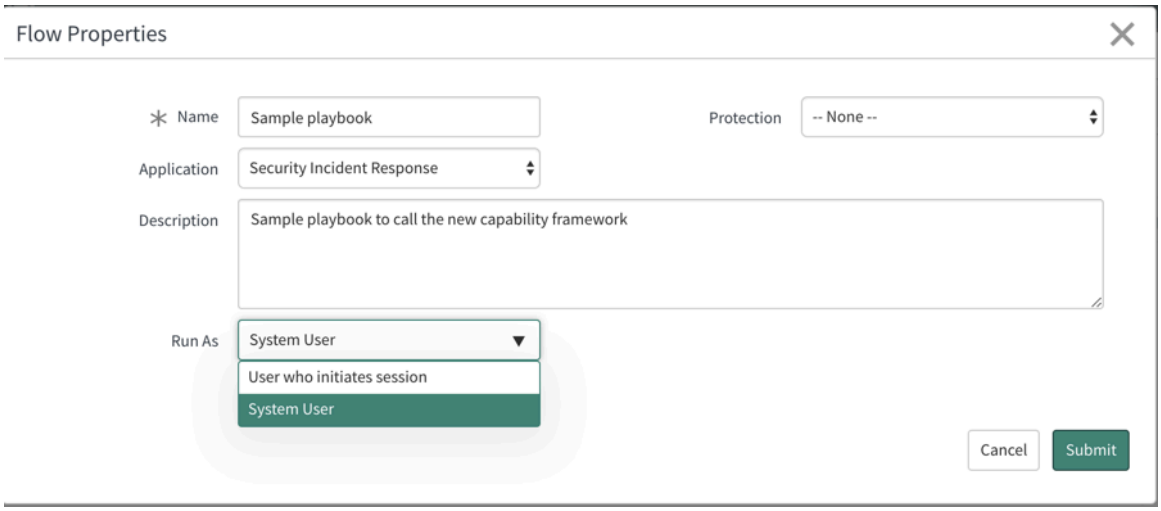
手順

1. 次のように移動する。 **All** (すべて) > **Flow Designer** > デザイナー.

2. [新規] をクリックして新しいフローを作成し、プロパティに必要な情報を入力します。

自動翻訳

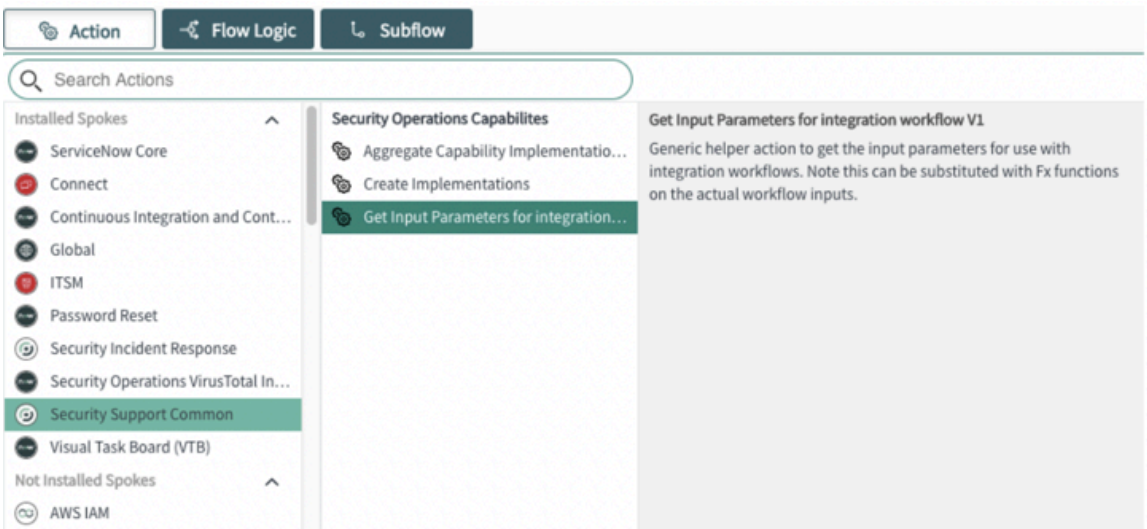
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
上の画像に示すように、[実行方法] 選択リストで [システムユーザー] を選択します。

3. フローのトリガー条件を選択します (一般的なトリガーは、特定のインシデントカテゴリのセキュリティインシデントレコードの作成です)。

4. フローのステップ 1 で、セキュリティインシデントから入力を取得するアクション (観測事象など) を選択します。
Security Support Common スポークを使用して、ベースシステムで提供されるアクションからアクションを選択できます。



5. ステップ 2 で、サブフロー (脅威のルックアップなど) を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. 選択したサブフローを以下に示すように設定します。

7. フローを保存して公開します。

統合機能フローのトラブルシューティング

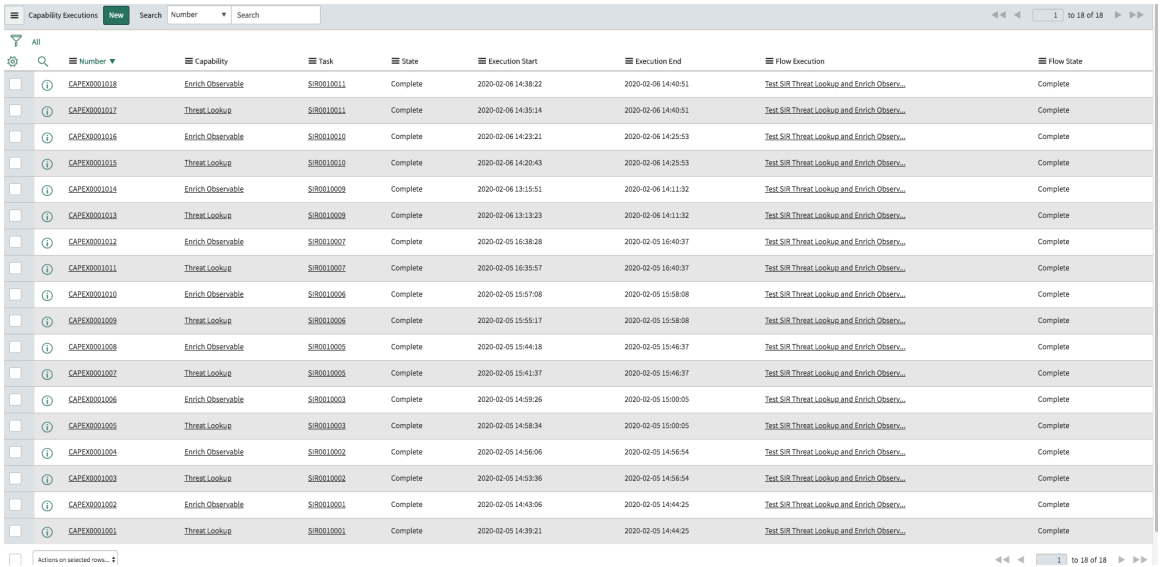
[機能実行] オプションは、実行された各機能に関する詳細情報を提供します。

注:
完了した実行は 30 日後にアーカイブされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. 次のように移動する。 セキュリティオペレーション > 統合 > 機能実行。.



2. [機能実行] のリンクをクリックして追加の詳細を表示します。

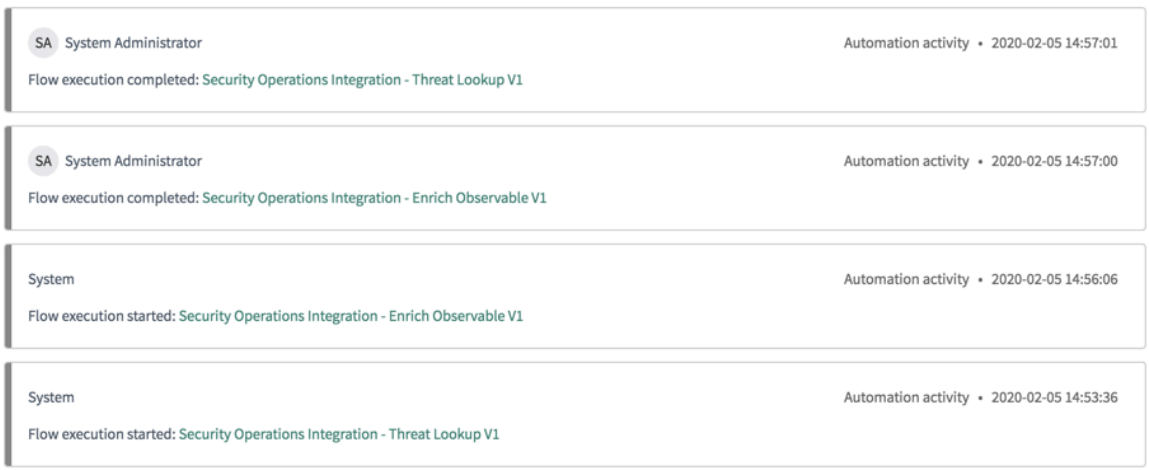
セキュリティインシデントレコードの作業メモ

観測事象がセキュリティインシデントに追加され、フローのトリガー条件が満たされると、「脅威のルックアップ」および「観測事象を拡張」サブフローが開始され、次の作業メモがセキュリティインシデントに追加されます。

- フロー実行が開始されました：Security Operations Integration - 観測事象 V1 を拡張
- フロー実行が完了しました：Security Operations Integration - 観測事象 V1 を拡張
- フロー実行が開始されました：Security Operations Integration – 脅威のルックアップ V1
- フロー実行が完了しました：Security Operations Integration – 脅威のルックアップ V1

これらの作業メモを表示するには、*sn_si.admin* または *sn_si.analyst*、*flow_designer*、および *action_designer* ロールを持つユーザーとしてログインします。

セキュリティインシデントレコードページに移動し、これらの作業メモをクリックしてフロー実行の詳細を表示します。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Security Operations とのサードパーティ統合のための REST API

セキュリティオペレーション ベースシステムには、顧客とパートナーが既存の セキュリティオペレーション 展開と簡単に統合できるようにする一連のスクリプト済み REST API が含まれています。この API を使用すると、システムの外部からデータを収集し (たとえば、VirusTotal からデータを受信するには Python スクリプトを使用)、インスタンスに送り返すことができます。

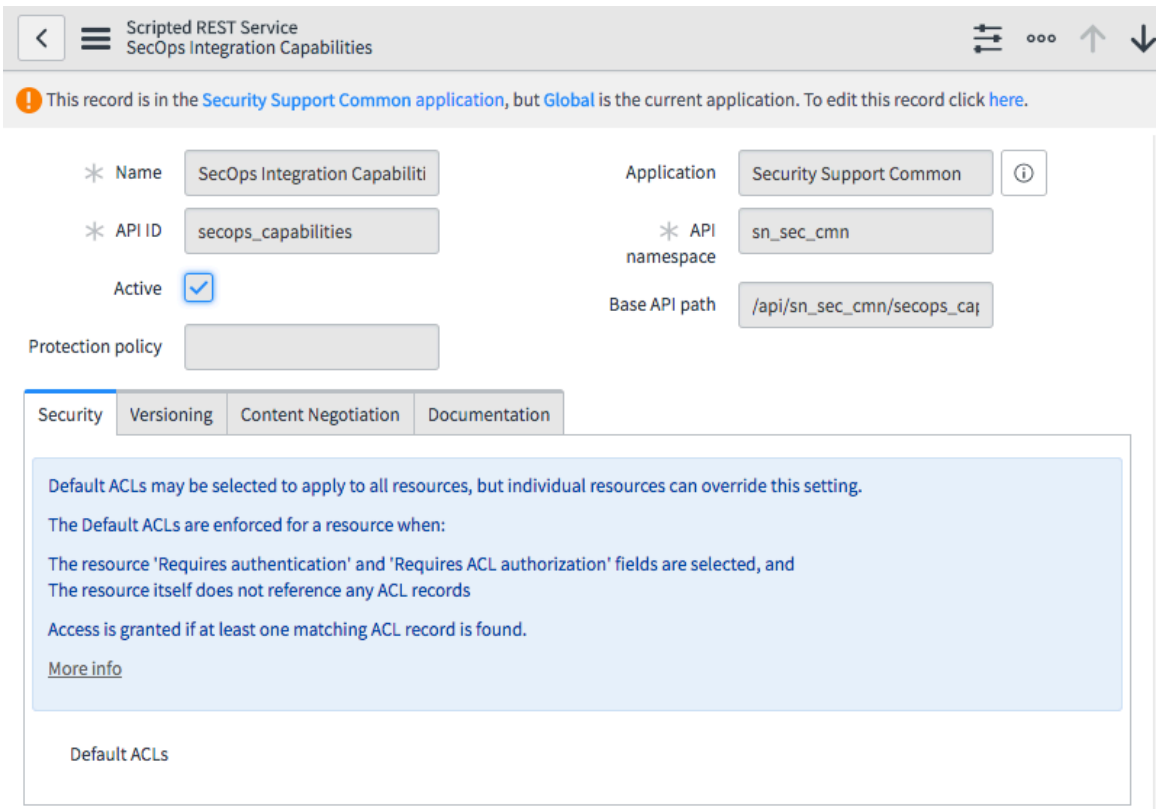
ほぼあらゆる言語 (たとえば Python) で記述されたスクリプトを API とともに使用して、顧客固有のプロセスを実行できます。スクリプトは、外部向けの HTTP Post 呼び出しが可能な言語で記述する必要があります。たとえば、Java アプリケーションがある場合は、java.net.HttpUrlConnection パッケージなどのライブラリを使用して HTTP 呼び出しをビルドし、JSON 文字列をメッセージの本文として渡す必要があります。

API は、システムの外部で収集されたデータ追加する目的でのみ使用されます。たとえば、VT Python スクリプトを入力して VT からデータを受信した場合、そのデータを SN インスタンスに送り返すことができます。

認証

API 定義内のすべての操作で、 スクリプト済み REST API 操作機能。アクセスするには、次に移動します: システム **Web** サービス > スクリプト化 **Web** サービス > スクリプト済み **REST API** **SecOps** 統合機能 API を見つけます。

スクリプト済み **REST** サービス



ユーザーとユーザーのドメインは、API のコンテキストですぐに利用できます。レコードは、ユーザー、確立する監査パス、実現しているドメインセパレーションに関連付けることができます。また、特定のユーザーとして認証されているため、 GlideRecordSecure を使用 して、データへの不正アクセスを防止できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

認証

セキュリティオペレーション アプリケーション外部のユーザーからレコード作成プロセスを保護するには、sn_sec_cmn.api_write ロールが必要です。このロールを持つユーザーのみが API にアクセスできます。

構成要求パラメーター

次の要求パラメーターを使用できます。

名前	デフォルト	説明
ignore_mandatory_fields	false	true に設定すると、必須フィールドに入力されていない場合でもレコードが保持されます。
include_wrap	false	true に設定すると、インスタンス提供のスクリプト済み REST API 用標準ラッパーが応答に含まれます。
simple_response	false	true に設定すると、操作が成功したかどうかのみが応答に含まれます。

エラー応答

次のエラー応答が発生する可能性があります。

エラーメッセージ	発生する条件	ソリューション
アクセス権が不十分です	ユーザーに sn_sec_cmn.api_write ロールがない場合。	ユーザーにロールを追加してください。
無効な投稿本文	要求本文が空または空のオブジェクトの場合。	API 定義に準拠します。
提供されたフィールドがありません	保持するよう指定されたデータフィールドが空の場合。	API 定義に準拠します。
必須フィールドがありません：x、y、z (Mandatory fields missing: x,y,z)	必須フィールドに入力されていない場合。	ターゲットテーブルのテーブル定義に従うか、**[ignore_mandatory_fields]** を true に設定してください。
レコードを保持できません	解析されたレコードを保持できない場合。	GlideRecord insert() が失敗しました。詳細な分析が必要です。
不明なエラー	既知のエラーパスに従わなかった場合。	詳細な分析が必要です。

CI 拡張のユースケース

サードパーティスクリプトを使用して、CI 拡張を構成アイテム拡張 [sn_sec_cmn_ci_enrichment_result] テーブルに書き込むことができます。拡張レコードは、サードパーティソースからのレコードに関する詳細情報を提供する既存の機能に基づいています。

以下に CI 拡張ユースケースのサンプル要求と応答を示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CI 拡張の作成要求


```
{
   "ignore_mandatory_fields": true,
   "payload": [
      {
         "configuration_item_id": "2dfd7c8437201000deeabfc8bcbe5d56",
         "data": [
             {
               "external_link": "http://www.servicenow.com",
               "vendor": "aafbf46ad72212007a6de294de6103a2",
               "data_type": null,
               "source": null,
               "name": null,
               "parent": null,
               "summary": "Found 1000 open vulnerabilities on the specified
               configuration item",
               "retrieval_date": "2017-09-05 08:56:28"
             }
          ]
      }
   ]
}
```


CI 拡張の作成応答


```
{
   "success": true,
   "status": "success",
   "payload": {
        "results": [
            {
                "sys_id": "2dfd7c8437201000deeabfc8bcbe5d56",
                "reference_url":
                "http://10.0.214.15:8080/nav_to.do?uri=cmdb_ci.do?sys_id=2dfd7c8437201000
                deeabfc8bcbe5d56",
                    "results": [
                        {
                            "sys_id": "4a8b92fb0b410300263a089b37673a33",
                            "reference_url":
                            "http://10.0.214.15:8080/nav_to.do?uri=sn_sec_cmn_ci_
                        enrichment_result.do?sys_id=4a8b92fb0b410300263a089b37673a33"}
                    ]
                }
            ],
            "domain": "global",
            "configuration_item_ids": [
            "2dfd7c8437201000deeabfc8bcbe5d56"
        ]
    }
}
```


自動翻訳

観測事象の拡張ユースケース

サードパーティスクリプトを使用して、観測事象拡張を観測事象拡張結果 [sn_ti_observable_enrichment_result] テーブルに書き込むことができます。拡張レコードは、サードパーティソースからのレコードに関する詳細情報を提供する既存の機能に基づいています。

以下に観測事象拡張ユースケースのサンプル要求と応答を示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

観測事象拡張の作成要求


```
"ignore_mandatory_fields": true,
  "payload": [
    {
      "observable_value": "http://www.google.com",
      "security_incident_ids": [
        "9424d4e10b110300263a089b37673a21"
      ],
      "enrichment_mapping_id": "9fa7d4590b622200263a089b37673a1d",
      "data": [{
        "vendor": "f15a46140b622200263a089b37673a7e",
        "summary": "Registrar:MarkMonitor, Inc., Registration Date:1997-09-15,
            Expiration Date:2020-09-14, Registrant country:UNITED STATES",
        "data_type": "json",
        "retrieval_date": "2017-08-30 10:35:02",
        "raw_data": "{\"WhoisRecord\":{\"administrativeContact\":{\"city\":
            \"Mountain View\",\"country\":\"UNITED STATES\",\"email\":
            \"dns-admin@google.com\",\"fax\":\"16506188571\",\"name\":
            \"DNS Admin\",\"organization\":\"Google Inc.\"}"
      }]
    }
  ]
}
```


観測事象拡張の作成応答


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "43bd3f210b510300263a089b37673ac6",
                "reference_url": "http://10.0.65.185:8080/sn_ti_observable.do?
                    sys_id=43bd3f210b510300263a089b37673ac6&sys_target=&XML",
                "results": [
                    {
                        "sys_id": "0bbd3f210b510300263a089b37673acc",
                        "reference_url": "http://10.0.65.185:8080/sn_ti_observable_
                            enrichment_result.do?sys_id=0bbd3f210b510300263a089b37673acc
                                &sys_target=&XML"
                    }
                ]
            }
        ],
        "domain": "global",
        "observable_ids": [
            "43bd3f210b510300263a089b37673ac6"
        ]
    }
}
```


自動翻訳

注:
既存のレコードを拡張するだけでなく、セキュリティオペレーション 拡張データマッピングを使用して、既存の拡張マッピングの **enrichment_mapping_id** と、それに対応する、マッピングプロセスで解析できる **raw_data** 文字列を渡すことで、テーブルに新しいレコードを追加することもできます。

脅威のルックアップのユースケース

サードパーティスクリプトを使用して、脅威のルックアップの結果を脅威のルックアップの結果 [sn_ti_lookup_result] テーブルに書き込むことができます。ルックアップレコードは、サードパーティソースからのレコードに関する詳細情報を提供する既存の機能に基づいています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

以下に脅威のルックアップのユースケースのサンプル要求と応答を示します。

脅威のルックアップの作成要求


```
{
"simple_response": false,
"include_wrapper": true,
  "ignore_mandatory_fields": false,
  "payload": [
    {
      "request_element_correlation_id": "1",
      "observable_value": "128.214.67.80",
      "data": [
        {
          "request_element_correlation_id": "2",
          "finding": "Malicious6",
          "source_engine": "VirusTotal API",
          "vendor": "aafbf46ad72212007a6de294de6103a2",
          "data_type": null,
          "source": null,
          "name": null,
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        },
        {
          "finding": "Malicious8",
          "source_engine": "VirusTotal API",
          "source_engine_version": "v2",
          "first_found": "2000-09-05 15:56:28",
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        }
      ]
    }
  ]
}
```


自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威のルックアップの作成応答


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "a0bddafb0b410300263a089b37673a93",
                "reference_url":
                    http://10.0.214.15:8080/nav_to.do?uri=sn_ti_observable.do?sys_id=
                        a0bddafb0b410300263a089b37673a93,
                    "request_element_correlation_id": "1",
                    "results": [
                        {
                            "sys_id": "24bddafb0b410300263a089b37673a95",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?sys
                            _id=24bddafb0b410300263a089b37673a95,
                    "request_element_correlation_id": "2",
                },
                {
                    "sys_id": "e8bddafb0b410300263a089b37673a96",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?
                            sys_id=e8bddafb0b410300263a089b37673a96
                            }
                        ]
                    }        ],
                "domain": "global",
                "observable_ids": [
                    "a0bddafb0b410300263a089b37673a93"        ]
    }
}
```


統合機能

統合機能 フレームワークは、サードパーティとの統合の相互運用性をサポートする一貫したアーキテクチャを提供します。この抽象化されたインターフェイスとデータモデルによって、統合はコアアプリケーションに対する変更の影響を受けず、類似するタイプの統合に対して一貫したエクスペリエンスが保証されます。

各統合機能は、統合機能 [sn_sec_cmn_integration_capability] テーブルに保持されます。統合機能フローは単独では実行できません。実装フローを開始する必要があります。機能の実装を提供するプラグインは、その実装を子テーブル (統合機能の実装 [sn_sec_cmn_integration_capability_implementation]) に追加します。

実装では、実行するフロー、関連する統合 (プラグイン ID)、および実装する機能を指定します。これらのフローは、並列フローランチャーを使用して並列に実行できます。ただし、ベースシステムでは順次実行がデフォルトです。必要に応じて実行順序を変更できます。

注:
利用可能な実装がない場合、機能アクションは製品メニューに表示されません。

Security Operations Integration - ブロック要求機能

ブロックアクション機能は、実装フローを使用して、ファイアウォール、Web プロキシ、またはその他のコントロールポイントにおけるセキュリティインシデントに関連する観測事象をブロックします。この機能は、インシデント応答の調査中に、識別された脅威を封じ込めるために使用されます。

ブロック要求機能には、ブロックする要求を実行するフロー Security Operations Integration - ブロック要求フロー があります。このフローは、観測事象のリストを受け入れ、実装機能を見つけて、設定されたフローに基づいて要求を実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
利用可能な実装がない場合、機能アクションは製品メニューに表示されません。

ブロック要求の実行

セキュリティインシデントに関連付けられた観測事象との通信をブロックします。

始める前に

必要なロール：sn_si.analyst

このタスクについて

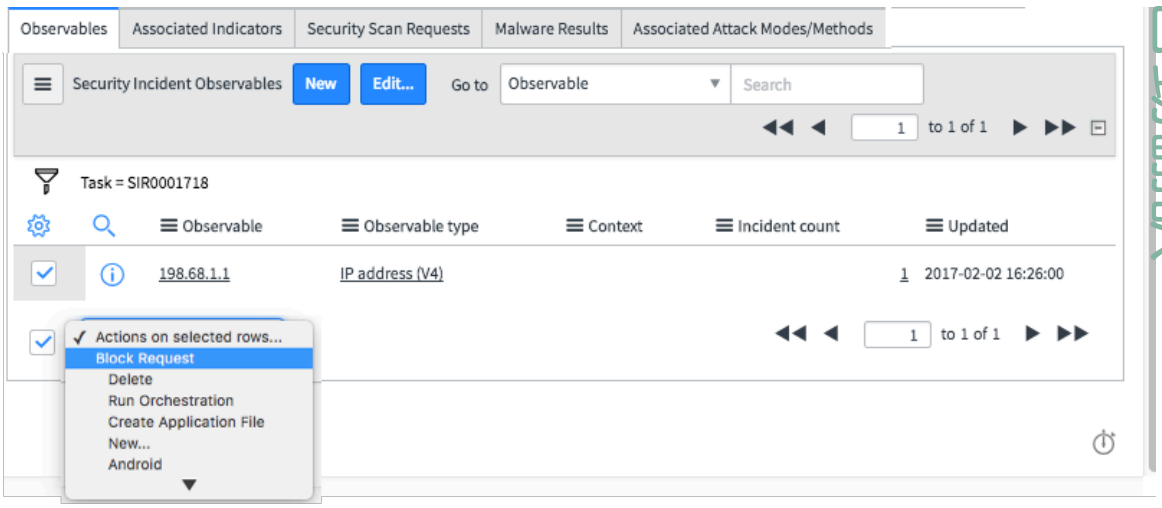
注:
利用可能な実装がない場合、機能アクションは製品メニューに表示されません。

[Security Operations Integration - ブロック要求] フローは、観測事象フォーム、またはセキュリティインシデントの [セキュリティインシデント観測事象] 関連リストからトリガーできます。

この例は、セキュリティインシデントからのブロック要求を示しています。

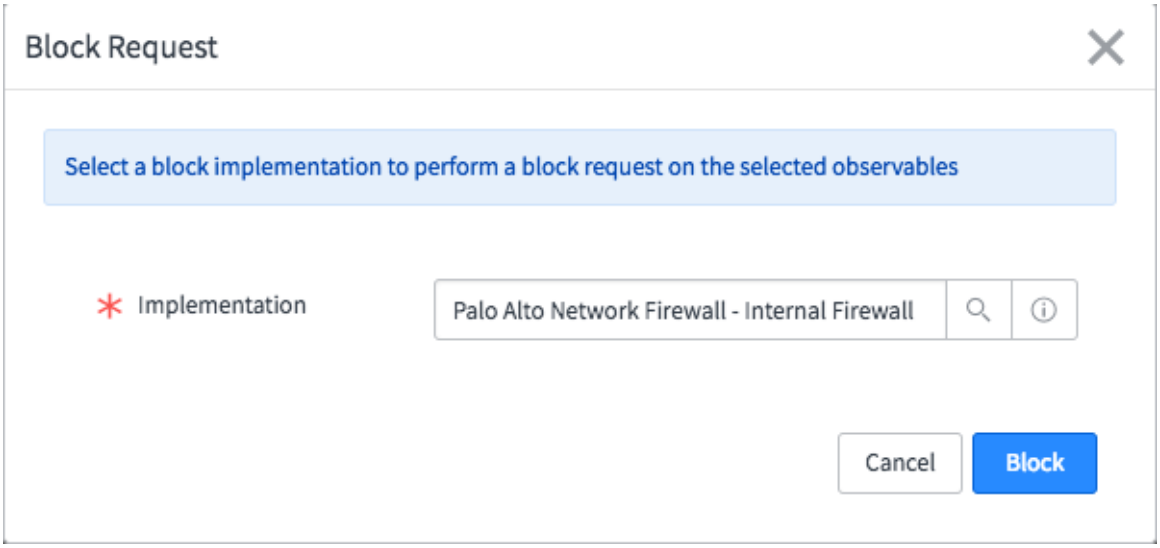
手順

1. セキュリティインシデントに移動します。
2. [関連リスト] タブから [観測事象] を選択します。
3. [選択した行のアクション...] ドロップダウンメニューで [ブロック要求] をクリックします。

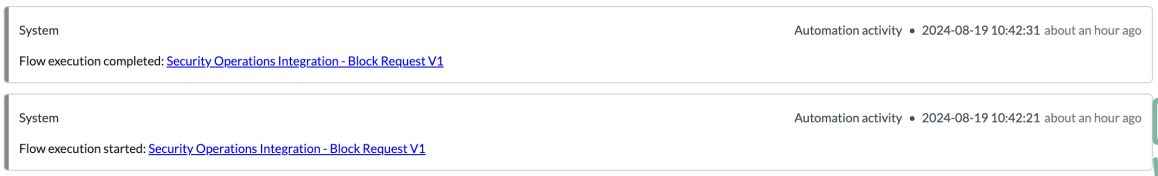


ダイアログボックスが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [実装] を選択します。
5. [ブロック] をクリックします。
   フロー実行の監査が [作業メモ] セクションに表示されます。



Security Operations Integration - ブロック要求フロー

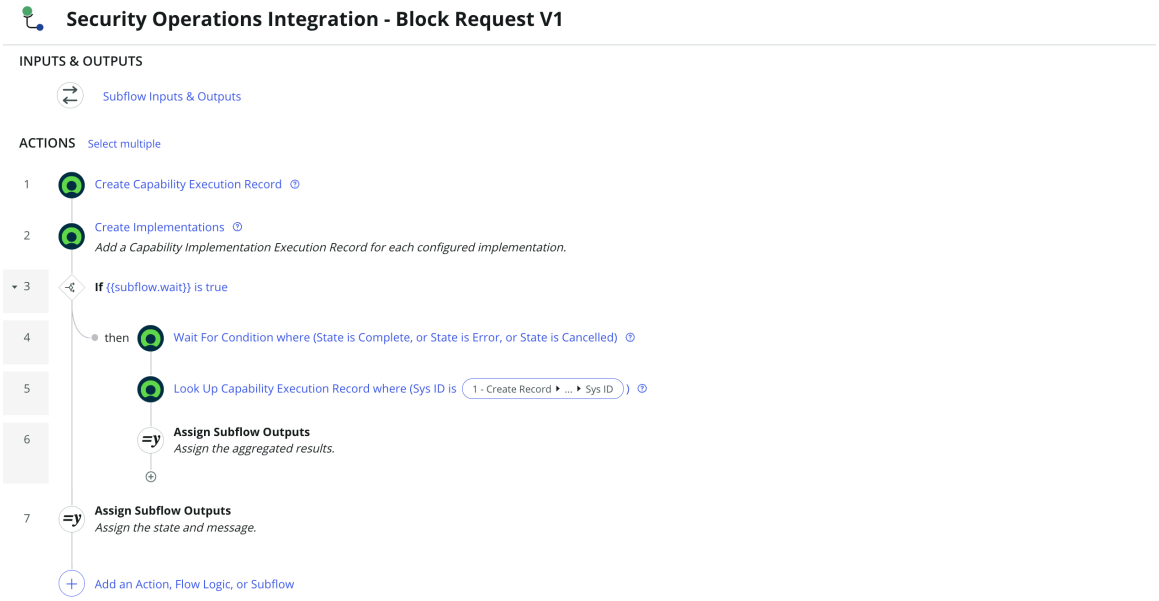
[Security Operations Integration - 要求のブロック] フローは、統合に依存しない高レベルのフローです。セキュリティインシデントに関連付けられた観測事象をブロックします。Palo Alto Networks - Firewallなどの統合を実行するために使用します。

[Security Operations Integration - ブロック要求] フローは、観測事象フォームでトリガーするか、セキュリティインシデントの [セキュリティインシデント観測事象] 関連リストからトリガーできます。リストのドロップダウンアクションメニューにあります。フォームでは関連リンクです。要求のブロックは、要求ブロック機能の実装がインストールされている場合にのみ使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ブロック要求



ここでは、このフローに固有のアクションについて説明します。他のアクションの詳細については、「 一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

Security Operations Integration - [メールの検索と削除] 機能

[メールの検索と削除] 機能は、メールサーバーの検索から脅威メールの件数を返します。オプションで、見つかった各メールの詳細を返すこともできます。メールの検索が完了したら、メールを削除できます。

[メールの検索と削除] 機能には、メールの検索と削除のプロセスを実行するフローが 1 つあります。

> **注:**
> 利用可能な実装がない場合、機能アクションは製品メニューに表示されません。また、[メールの検索と削除] 機能のアクティブな実装が 1 つもない場合、セキュリティインシデントの [メールの検索] 関連リンクは表示されません。

Security Operations Integration - メールの検索と削除フロー

[Security Operations Integration - メールの検索と削除] フローは、メールサーバーの検索から脅威メールの数を返し、オプションで見つかった各メールの詳細を返します。メールの検索が完了したら、メールを削除できます。

始める前に
必要なロール：sn_si.analyst

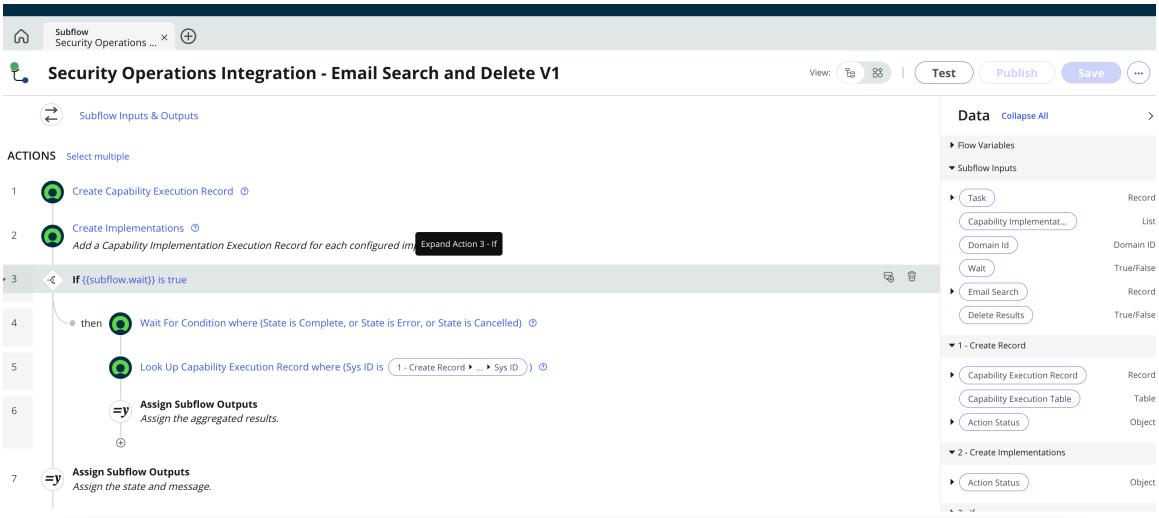
このタスクについて
検索クエリが完了するまで時間がかかる場合があります。カウントを受信した後、メールサーバーからメールを削除するには承認が必要です。

このフローは、セキュリティインシデントの [メール検索] フォームの [メールサーバーから削除] ボタンと [メールサーバーで検索] ボタンによってトリガーされます。詳細については、「フィッシングメールの検索と削除」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

メールの検索と削除



ここでは、このフローに固有のアクティビティについて説明します。他のアクティビティの詳細については、「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

フロープロセスアクティビティには次のものが含まれます。

[実行トラッキング開始 (メール検索)] アクション

[実行トラッキング:開始 (メール検索)] 機能の実行アクションは、トラッキングレコードを作成し、レコードのステータスを [開始] としてマークします。このアクションは、すべての機能と実装フローでそのステータスを追跡するために使用されます。

結果

このアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	実行トラッキングレコードが作成されました。
失敗	実行トラッキングレコードを作成できませんでした。

入力変数

アクションの初期動作が、入力変数によって決まります。

変数	説明
capabilityId	実行されている統合機能のシステム識別子。
implementationId	実行されている統合機能実装のシステム識別子。
taskId	フローに関連付けられたタスクのシステム識別子。
flowContextId	関連付けられたフローコンテキストレコードのシステム識別子。システムによって提供されます。
flowName	フローの名前。システムによって提供されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

変数	説明
parentCapabilityExcutionId	実装フローを開始した監査レコードのシステム識別子。Splunk や Elasticsearch などの統合機能の実装フローのみに必要です。
emailsearchId	メール検索 [sn_sec_cmn_email_search] テーブル内のメール検索レコードの sysid。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。

出力変数

変数	説明
capabilityExecutionId	実行トラッキングレコードのシステム識別子。

- [サポートされているセキュリティ機能を取得] アクション
- 機能トラッキング - 未実施アクションなし

Security Operations Integration - [CI を拡張] 機能

[CI を拡張] 機能を使用すると、セキュリティインシデントに関連する構成アイテム (CI) のデータを拡張できます。

[CI を拡張] 機能にはフロー Security Operations Integration - CI 拡張フロー があります。機能フローが実行されると、アクティブ化された実装の追加フローが実行されます。選択した CI に使用する拡張の実装を指定して実行するか、すべての実装を使用して拡張を実行することができます。

注:
この拡張データは、CI からのメモリダンプの実行など、特定の調査に固有の鑑識データであるため、CMDB に保存しておくタイプのデータではありません。代わりに、データは構成アイテム拡張 [sn_sec_cmn_ci_enrichment_result] テーブルに格納されます。

注:
利用可能な実装がない場合、機能アクションは製品メニューに表示されません。

Security Operations Integration - CI 拡張フロー

[Security Operations Integration - CI 拡張] フローを使用すると、セキュリティインシデントに関連付けられた構成アイテム (CI) のデータを拡張できます。

始める前に
必要なロール：sn_si.analyst

このタスクについて
このフローは、 セキュリティインシデントレスポンス から 2 つの方法でトリガーされます。

- [構成アイテム] タブ ([影響を受けるアイテム]] 関連リンクの下) から 1 つ以上の CI を選択し、[選択した行のアクション...] 選択リストから **[CI** 拡張を実行] を選択します。
- CI レコードを開き、**[CI** 拡張を実行] 関連リンクをクリックします。

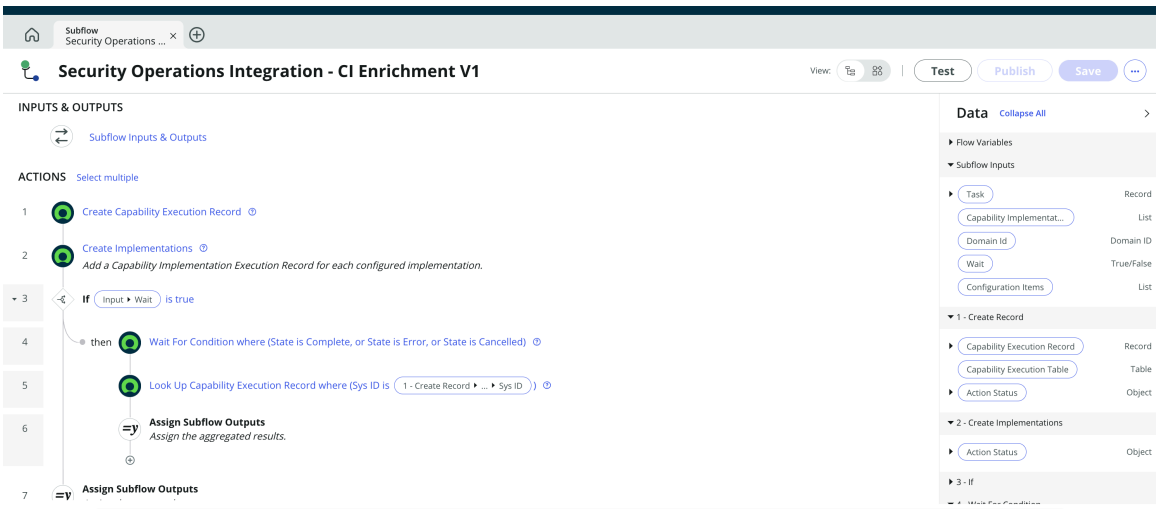
いずれの方法でも、選択した CI を拡張するために使用する実装を指定できます。関連する実装フローが実行され、拡張が実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
ベースシステムには、この機能の実装フローは含まれていません。CI を拡張するには、独自の実装 フロー を作成する必要があります。

CI 拡張



ここでは、このフローに固有のアクションについて説明します。他のアクションの詳細については、「 一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

フロープロセスアクションには次のものが含まれます。

- [実行トラッキング:フローを開始] アクション
- Security Operations Integration - CI 拡張フロー
- 機能トラッキング - 未実施アクションなし
- [サポートされているセキュリティ機能を取得] アクション

Security Operations Integration - [観測事象を拡張] 機能

[観測事象を拡張] 機能では、実装フローを使用して、さまざまなソースからの追加情報で観測事象を拡張できます。この機能は、インシデント応答の調査中に、識別された脅威を封じ込めるために使用されます。

[観測事象を拡張] 機能にはフロー [Security Operations Integration - 観測事象を拡張] フロー があります。機能フローが実行されると、アクティブ化された実装の追加フローが実行されます。選択した観測事象に使用する拡張の実装を指定して実行するか、サポートされる観測事象タイプに一致するすべての実装を使用して拡張を実行することができます。

注:
利用可能な実装がない場合、機能アクションは製品メニューに表示されません。

[Security Operations Integration - 観測事象を拡張] フロー

[Security Operations Integration：観測事象を拡張] サブフローでは、実装フローデザイナーを使用して、さまざまなソースからの補足情報で観測事象を拡張できます。

始める前に
必要なロール：sn_si.analyst

このタスクについて
このフローは、2 つの方法で セキュリティインシデントレスポンス または 脅威インテリジェンス からトリガーできます。

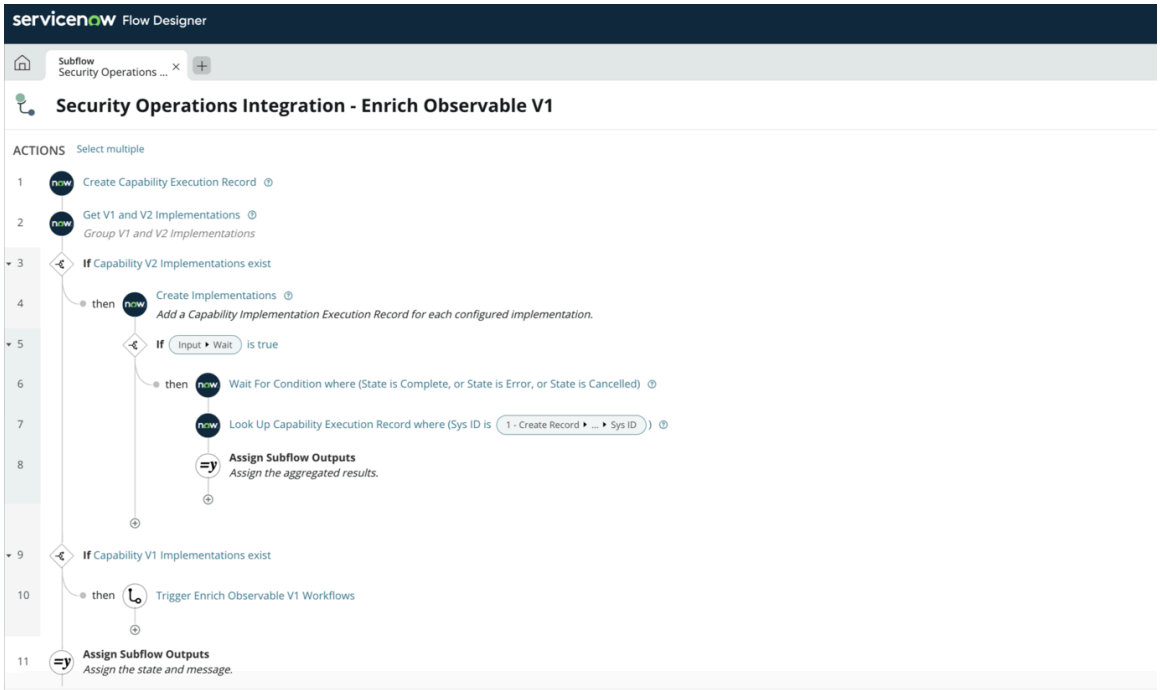
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [観測事象] リストから 1 つ以上の観測事象を選択し、[選択した行のアクション...] 選択リストから [観測事象の拡張を実行] を選択します。
- 観測事象レコードを開き、[観測事象の拡張を実行] 関連リンクをクリックします。

いずれの方法でも、選択した観測事象を拡張するために使用する実装を指定できます。関連する実装フローが実行され、拡張が実行されます。

観測可能項目を拡張



ここでは、このフローに固有のアクションについて説明します。他のアクションの詳細については、「 一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

フロープロセスアクションには次のものが含まれます。

- 機能トラッキング - 未実施アクションなし
- [サポートされているセキュリティ機能を取得] アクション機能トラッキング - 未実施アクションなし

Security Operations Integration - [ネットワーク統計情報を取得] 機能

[ネットワーク統計情報を取得] 機能は、ホストまたはエンドポイントから、アクティブなネットワーク接続のリストを取得します。調査中にインシデントの拡張に使用できます。この機能は、構成アイテムがセキュリティインシデントに追加されると自動的にトリガーされます。

[ネットワーク統計情報を取得] 機能には、1 つ以上の CI とタスクを受け入れるフロー、[Security Operations Integrations - ネットワーク統計情報を取得] フロー があります。フローは各実装と各 CI を反復処理し、実装フローを再度呼び出します。

注:
利用可能な実装がない場合、機能アクションは製品メニューに表示されません。

[Security Operations Integrations - ネットワーク統計情報を取得] フロー

[Security Operations Integrations - ネットワーク統計情報を取得] フローは、ホストまたはエンドポイントからアクティブなネットワーク接続のリストを取得します。

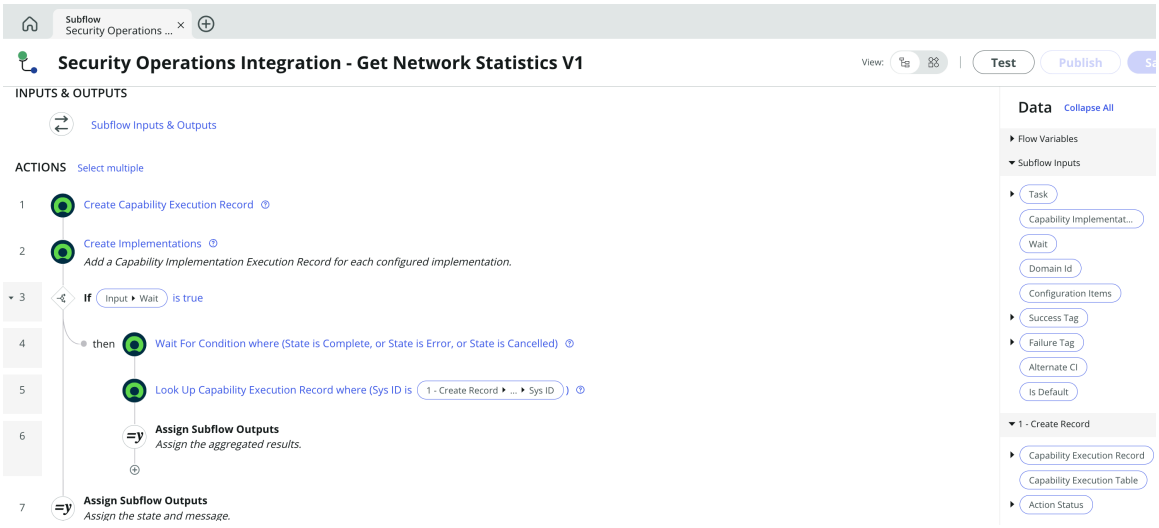
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：sn_si.analyst

このタスクについて
このフローは、構成アイテムがセキュリティインシデントに追加されると自動的に実行されます。

ネットワーク統計情報を取得



ここでは、このフローに固有のアクションについて説明します。他のアクションの詳細については、「 一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

フローアクションには次のものが含まれます。

- [機能 - CI の特定] アクティビティ
-

.

実行トラッキング:開始 (CI) フローアクション

[実行トラッキング:開始 **(CI)]** フローアクションは、構成アイテム (CI) で動作する セキュリティオペレーション 統合フローの監査プロセスを開始します。

[実行トラッキング **-** 開始 **(CI)]** フローアクションを任意の CI フローで使用して、監査でフローの進行状況の記録を開始できます。

結果

このフローアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	監査レコードが作成されます。

入力変数

フローアクションの初期動作が、入力変数によって決まります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

変数	説明
capabilityId	実行されている統合機能のシステム識別子。
isImpl	統合機能フローまたは統合機能実装フローのどちらに対して監査を実行するかを指定するフラグ。可能な値： • false - サイティング検索などの抽象統合機能フローの監査を示します。(デフォルト) • true - 統合機能の実装フローの監査を示します。たとえば、Splunk や Elasticsearch です。
taskId	フローに関連付けられたタスクのシステム識別子。

ciList	次の形式で目的のアクションを実行する 1 つ以上の構成アイテム (CI)：
	`["sysId", "sysId"]`
	または
	`"sysId"`
	フロー入力として使用されます。

flowContextId	関連付けられたフローコンテキストレコードのシステム識別子。システムによって提供されます。
flowName	フローの名前。システムによって提供されます。
parentCapabilityExcutionId	実装フローを開始した監査レコードのシステム識別子。Splunk や Elasticsearch などの統合機能の実装フローのみに必要です。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
capabilityExecutionId	監査レコードのシステム識別子。

フロープロセスアクションには次のものが含まれます。

- [サポートされているセキュリティ機能を取得] アクション
- 機能トラッキング - 未実施アクションなし

セキュリティインシデントレスポンス - ネットワーク統計情報を取得フロー

application **Security Incident Response** (セキュリティインシデントレスポンス) > ネットワーク統計情報を取得 フローは、[分析] ステータスのセキュリティインシデントに追加されたときに、影響を受ける Windows ベースのリソースのネットワーク統計情報を取得します。

始める前に
必要なロール：sn_si.analyst

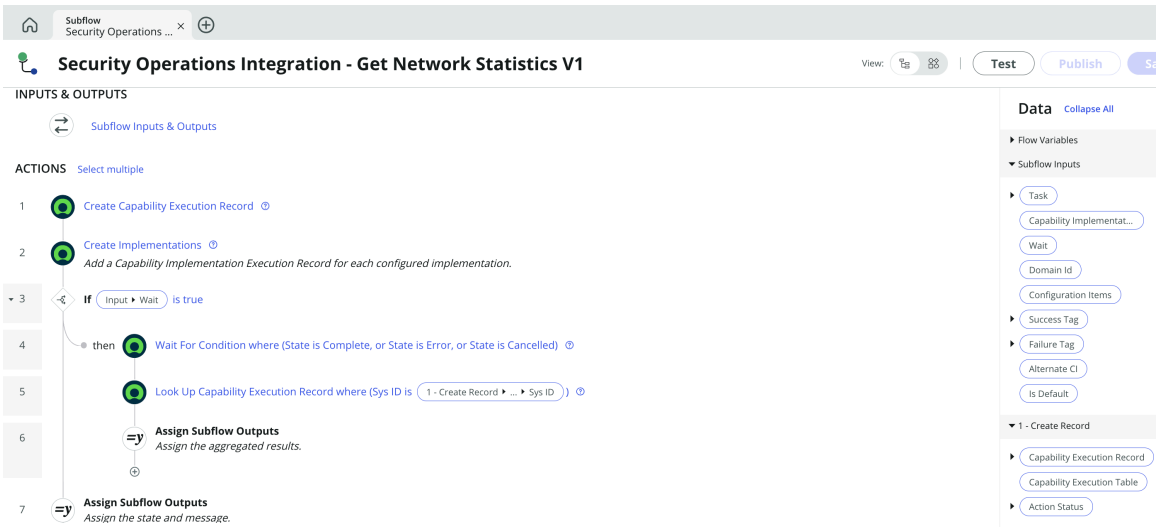
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
構成アイテムを含む新しいセキュリティインシデントの場合、ステータスが [分析] に変わるとフローが自動的に実行されます。

既存のセキュリティインシデントは、[分析] ステータスのときに新しい構成アイテムを追加すると自動的に更新されます。

ネットワーク統計情報を取得



フロープロセスアクションには次のものが含まれます。

[構成アイテム FQDN を取得] フローアクション

OS によるシェルスクリプトの決定

ステートメントが Powershell によって実行される場合

[実行トラッキング:フローを開始] アクション

netstat フローアクションを介してネットワーク統計情報を取得

機能トラッキング:失敗フローアクション

拡張データレコードフローアクションを作成

機能トラッキング:失敗フローアクション - 拡張 ID を返します。

機能トラッキング:フローアクションを完了

手順

1. 任意のセキュリティインシデントを開きます。
2. 必要に応じて [ステータス **(State)**] を [分析] に更新します。
3. 構成アイテム (コンピューター、サーバーなど) を追加します。
4. **[Update** (更新)] をクリックします。
   セキュリティインシデントレスポンスオーケストレーション でネットワーク統計情報を提供します。 関連リンク > セキュリティインシデントの拡張 学習します。詳細については、「セキュリティオペレーション 拡張データマッピング」を参照してください。

   ここでは、このフローに固有のアクションについて説明します。他のアクションの詳細については、「 一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Security Operations Integration - [実行中のプロセスを取得] 機能

「実行中のプロセスを取得」機能は、ホストまたはエンドポイントから、構成アイテム (CI) で実行中のプロセスのリストを取得します。この機能は、調査中にインシデントの拡張に使用されます。

[実行中のプロセスを取得] 機能には 実装 2 つのフローがあります。

- Security Operations Carbon Black 統合 - 実行中のプロセスを取得フロー
- Security Operations System Command Integration - 実行中のプロセスを取得フロー

> **注:**
> 利用可能な実装がない場合、機能アクションは製品メニューに表示されません。

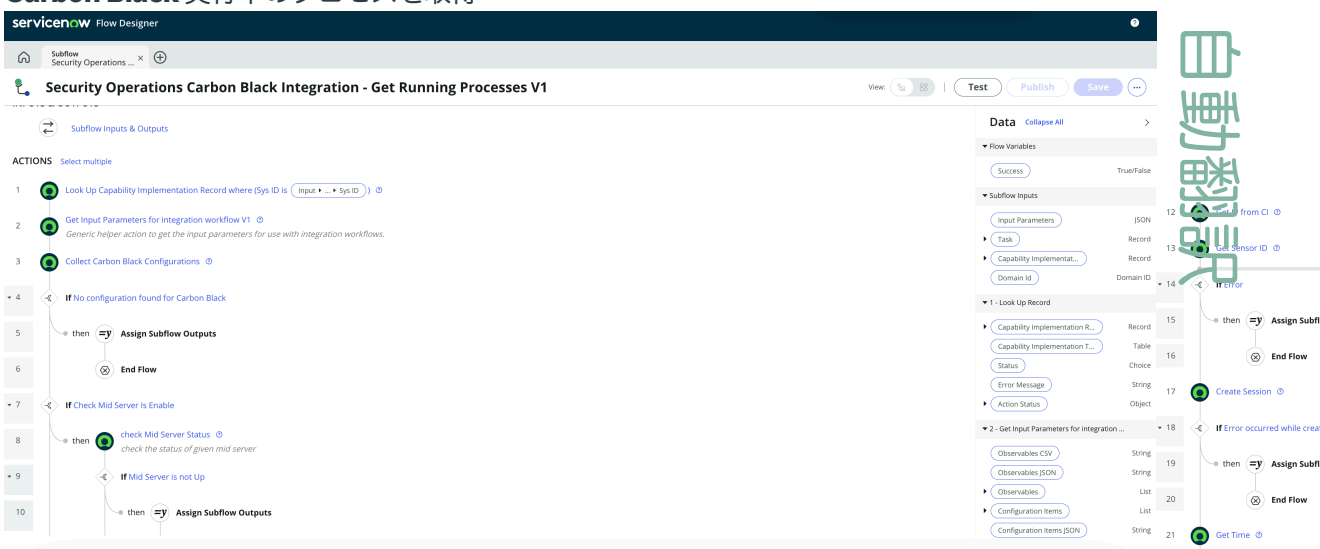
ここでは、このフローに固有のアクションについて説明します。他のアクションの詳細については、「 一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

Security Operations Carbon Black 統合 - 実行中のプロセスを取得フロー

[Security Operations Carbon Black 統合 - 実行中のプロセスを取得] は、[Security Operations Integration - 実行中のプロセスを取得] フローによって起動される Carbon Black 統合の実装です。

必要なロール：sn_si.analyst

Carbon Black 実行中のプロセスを取得



ここでは、このフローに固有のアクションについて説明します。他のアクションの詳細については、「 一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

[Carbon Black 設定の収集] フローアクション

[Carbon Black 設定の収集] フローアクションは、フローで使用する構成情報を収集します。

[Carbon Black 構成の収集] フローアクションは、フローで使用する Carbon Black 構成情報を収集します。

結果

このフローアクションの考えられる結果は次のとおりです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

結果

結果	説明
成功	構成に成功しました。
失敗	構成の検証中にエラーが発生しました。その他のエラー情報は、アクティビティ出力エラーで確認できます。

入力変数

このフローアクションの入力変数はありません。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
endpoint_base	サードパーティ統合 API のベース URL。
use_mid_server	REST アクティビティが MID サーバーを使用して Carbon Black とやり取りするかどうかを決定します。
api_token	サードパーティ統合 API キー。

MID サーバーステータスの確認

統合構成の **[MID** サーバーホスト] フィールドで識別された MID サーバーが稼働しているかどうかを判断します。フィールドが [任意] に設定されている場合、フローアクションは MID サーバーが稼働中であることを確認します。

[MID サーバーステータスの確認] フローアクションを任意のフローで使用して、フロー内で実行中の MID サーバーの存在を確認できます。

結果

このフローアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	セッションステータスが返されました。
失敗	セッションステータスエラー。その他のエラー情報は、フローアクション出力エラーで確認できます。

入力変数

フローアクションの初期動作が、入力変数によって決まります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

変数	説明
capabilityExecutionId	実行されている機能の ID。
flowName	実行中のフローの名前。
mid_server_host	統合構成で識別された MID サーバー。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
mid_server_live	統合構成の **[MID** サーバーホスト] フィールドで識別された MID サーバーが稼働しているかどうかを識別します。フィールドが [任意] に設定されている場合、フローアクションは MID サーバーが稼働中であることを確認します。

[センサー **ID** を取得] フローアクション

[センサー ID を取得] フローアクションは、フローで使用するセンサー識別子を収集します。

[センサー ID を取得] フローアクションを任意のフローで使用して、フローで使用するセンサー情報を収集できます。

結果

このフローアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	センサー識別子が見つかりました。
失敗	センサーが見つかりませんでした。その他のエラー情報は、フローアクション出力エラーで確認できます。

入力変数

フローアクションの初期動作が、入力変数によって決まります。

変数	説明
api_token	Carbon Black の API キー。
use_mid_server	REST アクティビティが MID サーバーを使用して Carbon Black とやり取りするかどうかを決定します。
endpoint_base	Carbon Black API のベース URL。
ci_ip_address	構成アイテムの IP アドレス。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
status_code	要求が成功したかどうかを判断します。失敗した場合は、HTTP エラーコードとメッセージを表示します。
アレイ要素タイプ	API 変数。
sensor_detail	JSON 形式の Carbon Black センサーの説明。

セッションフローアクションを作成

[セッションを作成] フローアクションは、フローで使用する Carbon Black セッションを確立します。

[セッションを作成] フローアクションを任意のフローで使用して、フロー内に Carbon Black セッションを作成できます。

結果

このフローアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	セッションが作成されました。
失敗	セッションが作成されませんでした。その他のエラー情報は、フローアクション出力エラーで確認できます。

入力変数

フローアクションの初期動作が、入力変数によって決まります。

変数	説明
api_token	Carbon Black の API キー。
endpoint_base	Carbon Black API のベース URL。
sensor_id	センサー識別子。
use_mid_server	REST アクティビティが MID サーバーを使用して Carbon Black とやり取りするかどうかを決定します。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数

変数	説明
status_code	要求が成功したかどうかを判断します。失敗した場合は、HTTP エラーコードとメッセージを表示します。
output	API 変数

セッションステータスのチェックフローアクション

フロー内の Carbon Black セッションのステータスを決定します。

[セッションステータスの確認] フローアクションを任意のフローで使用して、フロー内の Carbon Black セッションステータスを確認できます。

結果

このフローアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	セッションステータスが返されました。
失敗	セッションステータスエラー。その他のエラー情報は、フローアクション出力エラーで確認できます。

入力変数

フローアクションの初期動作が、入力変数によって決まります。

変数	説明
api_token	Carbon Black の API キー。
endpoint_base	Carbon Black API のベース URL。
session_id	セッション識別子。
use_mid_server	REST アクティビティが MID サーバーを使用して Carbon Black とやり取りするかどうかを決定します。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
status_code	要求が成功したかどうかを判断します。失敗した場合は、HTTP エラーコードとメッセージを表示します。
output	実行中の Carbon Black プロセスに関する情報

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コマンドプロセスフローアクションを作成

[コマンドプロセスを作成] フローアクションは、フローで使用する Carbon Black コマンドプロセスを作成します。

[コマンドプロセスを作成] フローアクションを任意のフローで使用して、フロー内に Carbon Black コマンドプロセスを作成できます。

結果

このフローアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	コマンドプロセスが作成されました。
失敗	コマンドプロセスが作成されませんでした。その他のエラー情報は、フローアクション出力エラーで確認できます。

入力変数

フローアクションの初期動作が、入力変数によって決まります。

変数	説明
api_token	Carbon Black の API キー。
endpoint_base	Carbon Black API のベース URL。
session_id	セッション識別子。
command_id	コマンド識別子。
use_mid_server	REST アクティビティが MID サーバーを使用して Carbon Black とやり取りするかどうかを決定します。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
status_code	要求が成功したかどうかを判断します。失敗した場合は、HTTP エラーコードとメッセージを表示します。
output	API 変数

コマンドステータスのチェックとプロセスフローアクションの取得

Carbon Black コマンドのステータスを確認し、フローで使用するプロセスを取得します。

[コマンドステータスの確認] および [プロセスフローの取得] アクションを任意のフローで使用して、Carbon Black コマンドステータスを確認し、フロー内のプロセスを取得できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

結果

このフローアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	コマンドステータスが返され、プロセスが作成されました。
失敗	コマンドステータスまたはプロセスエラー。その他のエラー情報は、フローアクション出力エラーで確認できます。

入力変数

フローアクションの初期動作が、入力変数によって決まります。

変数	説明
api_token	Carbon Black の API キー。
endpoint_base	Carbon Black API のベース URL。
session_id	セッション識別子。
command_id	コマンド識別子。
use_mid_server	REST アクティビティが MID サーバーを使用して Carbon Black とやり取りするかどうかを決定します。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
status_code	要求が成功したかどうかを判断します。失敗した場合は、HTTP エラーコードとメッセージを表示します。
output	API 変数

プロセスデータフローのマップアクション

[プロセスデータのマッピング] フローアクションは、フロー内の Carbon Black プロセスデータをマッピングします。

[プロセスデータのマッピング] フローアクションを任意のフローで使用して、Carbon Black プロセスをマッピングできます。

結果

このフローアクションの考えられる結果は次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

結果

結果	説明
成功	プロセスがマッピングされました。
失敗	プロセスがマッピングされませんでした。その他のエラー情報は、フローアクション出力エラーで確認できます。

入力変数

フローアクションの初期動作が、入力変数によって決まります。

変数	説明
affected_ci	影響を受けた構成アイテム。
Implementation_id	実装識別子。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
output	抽象ワークフローで使用される実行中のプロセスに関する書式設定済みの返されるデータ。
processes	アレイ内のプロセスのリスト。

機能トラッキング:フローアクションを完了

[機能トラッキング:完了] フローアクションは、フローが完了したときに監査レコードを更新します。

[機能トラッキング:完了] フローアクションを任意のフローで使用して、フローの完了を記録できます。

注:
[パラレルランチャー] コアフローアクションからの戻り値アレイには、実行されたすべての統合フローの結果のアレイが含まれており、実行トラッキングの正常な完了を促します。

結果

このフローアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	監査レコードのステータスが [完了] に更新されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

入力変数

フローアクションの初期動作が、入力変数によって決まります。

変数	説明
capabilityExecutionId	監査レコードのシステム識別子。このフィールドは、[監査の開始 (Begin auditing)] アクティビティの出力です。
flowName	フローの名前。システムによって提供されます。
message	完了メッセージ

出力変数

出力変数はありません。

セッションフローを閉じるアクション

フロー内の Carbon Black セッションを閉じます。

[セッションを閉じる] アクティビティを任意のフローで使用して、Carbon Black セッションを閉じることができます。

結果

このフローアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	セッションがクローズされました。
失敗	セッションがクローズされませんでした。その他のエラー情報は、フローアクション出力エラーで確認できます。

入力変数

フローアクションの初期動作が、入力変数によって決まります。

変数	説明
api_token	Carbon Black の API キー。
endpoint_base	Carbon Black API のベース URL。
session_id	セッション識別子。
use_mid_server	REST アクティビティが MID サーバーを使用して Carbon Black とやり取りするかどうかを決定します。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数

変数	説明
status_code	要求が成功したかどうかを判断します。失敗した場合は、HTTP エラーコードとメッセージを表示します。
output	API 変数

Security Operations System Command Integration - 実行中のプロセスを取得フロー

Security Operations System Command Integration - 実行中のプロセスを取得フローは、[分析] ステータスの Windows または UNIX ベースのセキュリティインシデントに構成アイテムを追加または更新すると、構成アイテムの実行中のプロセスを取得します。

始める前に
必要なロール：sn_si.analyst

このタスクについて
新しいセキュリティインシデントの場合、選択した構成アイテムを含むインシデントを送信すると、ステータスが自動的に [分析] に変わると、フローが自動的に実行されます。[ドラフト] ステータスのままだった場合は実行されません。

既存のセキュリティインシデントは、[分析] ステータスのときに新しい構成アイテムを追加すると自動的に更新されます。

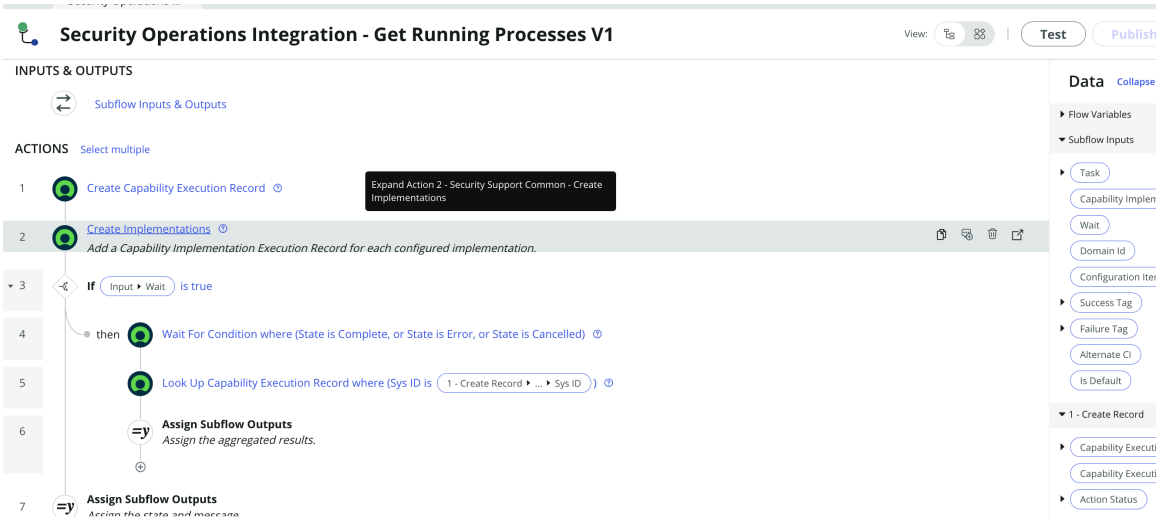
フロープロセスアクションには次のものが含まれます。

- [構成アイテム FQDN を取得] フローアクション
- [OS によるシェルスクリプトの確認] アクティビティ
- [実行トラッキング:フローを開始] アクション
- PowerShell を介して実行中のプロセスを取得
- [シェルスクリプトを実行] アクティビティ
- 機能トラッキング:失敗フローアクション
- [MID スクリプトからシェルスクリプトを抽出する] アクティビティ
- 結果を結合して、値をアレイで返します。
- 拡張データレコードフローアクションを作成
- 機能トラッキング:フローアクションを完了

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

実行中のプロセスを取得



手順

1. 任意のセキュリティインシデントを開きます。
2. 必要に応じて [ステータス **(State)**] を [分析] に更新します。
3. 構成アイテム (コンピューター、サーバーなど) を追加します。
4. **[Update** (更新)] をクリックします。
   セキュリティインシデントレスポンスオーケストレーション で実行中のプロセスの情報を提供 関連リンク > セキュリティインシデントの拡張学習します。詳細については、「セキュリティオペレーション 拡張データマッピング」を参照してください。

   ここでは、このフローに固有のアクションについて説明します。他のアクションの詳細については、「 一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

[結果の結合] アクティビティ

[結果の結合] ワークフローアクティビティは、ワークフローで使用するサードパーティ統合の結果を結合します。

[結果を結合] アクティビティを任意のワークフローで使用して、ワークフローで MID サーバーシェルスクリプトを実行できます。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	結果が結合されました。
失敗	結合されませんでした。その他のエラー情報は、アクティビティ出力エラーで確認できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

変数	説明
inputA	結果セット A
inputB	結果セット B
Implementation_id	実装識別子。
affected_ci	構成アイテム

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
result	結果セット A または結果セット B (どちらに入力されたかに基づく)。

[シェルスクリプトを実行] アクティビティ

[シェルスクリプトを実行] ワークフローアクティビティは、ワークフロー内で MID サーバーシェルスクリプトを実行します。

[シェルスクリプトを実行] アクティビティを任意のワークフローで使用して、ワークフローで MID サーバーシェルスクリプトを実行できます。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	シェルスクリプトが見つかりました。
失敗	シェルスクリプトが見つかりませんでした。その他のエラー情報は、アクティビティ出力エラーで確認できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

変数	説明
target	ターゲット CI の IP または完全修飾ドメイン名 (FQDN)。
scriptValue	Unix システムで実行される文字列値としてのスクリプト。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
response	生の出力。実行中のプロセスデータ。

[MID スクリプトからシェルスクリプトを抽出する] アクティビティ

[MID スクリプトからシェルスクリプトを抽出する] ワークフローアクティビティは、ワークフローで使用する MID サーバーシェルスクリプトをプルします。

[MID スクリプトからシェルスクリプトを抽出する] アクティビティを任意のワークフローで使用して、ワークフローに含める MID サーバーシェルスクリプトを抽出できます。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	シェルスクリプトが見つかりました。
失敗	シェルスクリプトが見つかりませんでした。その他のエラー情報は、アクティビティ出力エラーで確認できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

変数	説明
sysId	システム識別子

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
scriptValue	Unix システムで実行される文字列値としてのスクリプト。

[PowerShell を介して実行中のプロセスを取得] アクティビティ

[PowerShell を介して実行中のプロセスを取得] ワークフローアクティビティは、PowerShell を使用して実行中のプロセスを収集し、ワークフローで使用します。

[PowerShell を介して実行中のプロセスを取得] ワークフローアクティビティを任意のワークフローで使用して、ワークフローに含めるプロセスを取得できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	プロセスが見つかりました。
失敗	プロセスが見つかりません。その他のエラー情報は、アクティビティ出力エラーで確認できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

変数	説明
target	ターゲット CI の IP または完全修飾ドメイン名 (FQDN)。
processingScript	ECC スクリプトは Windows ベースのシステムで実行されます。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
response	生の出力。実行中のプロセスデータ。

Security Operations - 実行中のプロセスを取得フロー

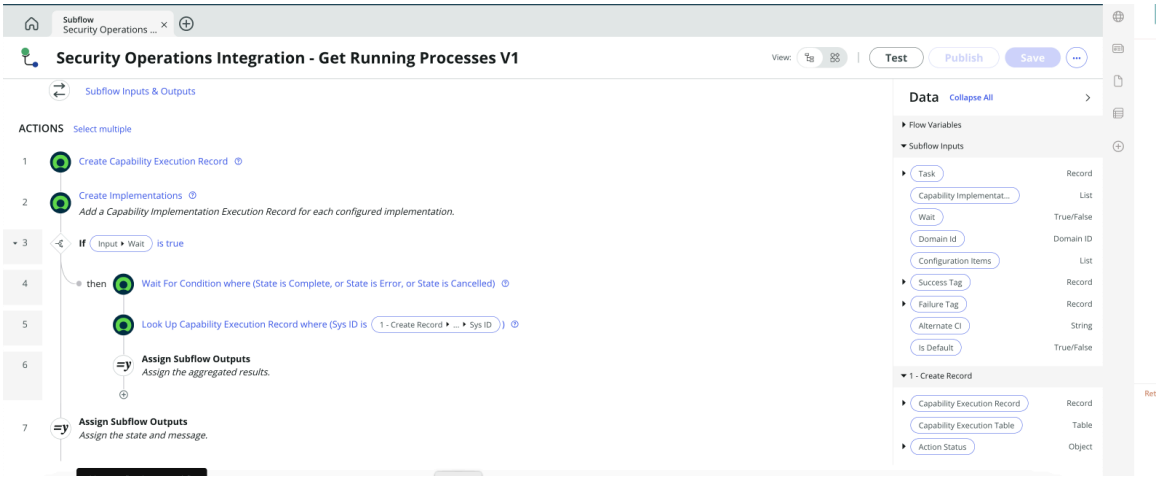
[Security Operations - 実行中のプロセスを取得] フローは、統合に依存しない高レベルのフローです。ホストから構成アイテム (CI) で実行中のプロセスのリストを取得します。Carbon Black などの統合を実行する場合や、Windows ベースのセキュリティインシデントを処理する場合に使用します。

必要なロール：sn_si.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

実行中のプロセスを取得



ここでは、このフローに固有のアクティビティについて説明します。他のアクティビティの詳細については、「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

Security Operations Integration - [ホストを隔離] 機能

[ホストを隔離] 機能は、他のデバイスへのシステム接続を制限します。ホスト隔離は構成アイテム (CI) に対して実行されます。

[ホストを隔離] 機能には、1 つ以上の CI とオプションで実装を受け入れるフロー[Security Operations - ホストを隔離] フローがあります。使用する実装を指定してホストを隔離することも、すべての実装を使用してフローでホストの隔離を試みることもできます。

注:
機能、フロー、 Security Operations Carbon Black 統合 - ホスト隔離削除フロー と統合されていませんが、隔離されたホストとの通信を復元するためのオーケストレーションで使用できます。

注:
利用可能な実装がない場合、機能アクションは製品メニューに表示されません。

ホスト隔離の実行

[ホストを隔離] では、他のデバイスとのシステム接続を制限します。

始める前に
必要なロール：sn_si.analyst

このタスクについて

注:
利用可能な実装がない場合、機能アクションは製品メニューに表示されません。

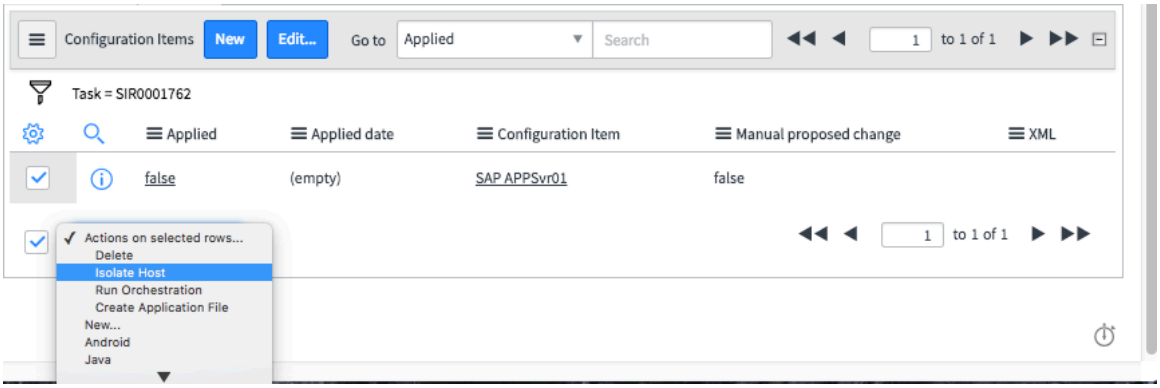
[Security Operations Integration - ホストまたはエンドポイントを隔離] フローは、セキュリティインシデントの関連リストからトリガーできます。

手順

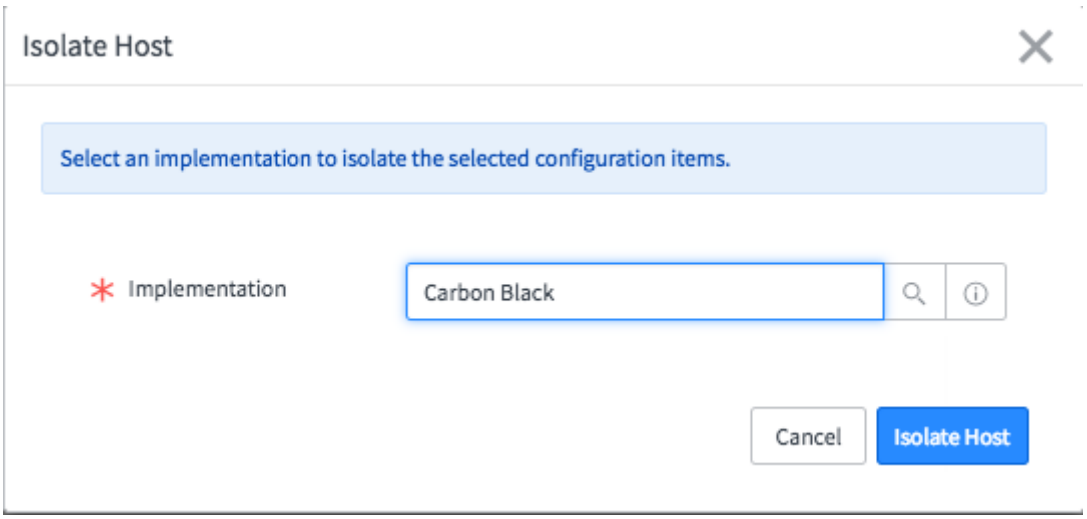
1. セキュリティインシデントに移動します。
2. [関連リスト] タブから [構成アイテム] を選択します。
3. [選択した行のアクション...] ドロップダウンメニューで [ホストを隔離] をクリックします。

自動翻訳

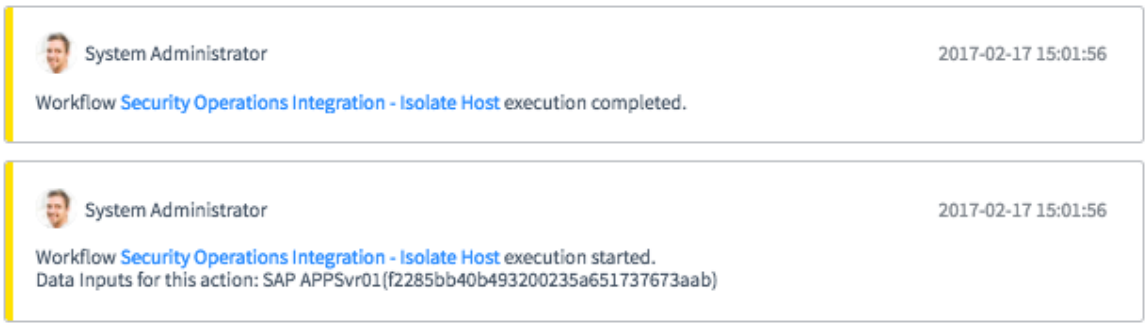
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



ダイアログボックスが表示されます。



4. [実装] を選択します。
5. [ホストを隔離] をクリックします。
   フロー実行の監査が [作業メモ] セクションに表示されます。



[Security Operations - ホストを隔離] フロー

「Security **Operations** - ホストを隔離」フローは、統合に依存しない高レベルのフローです。構成されたクエリを使用して、構成アイテムのセットを検索します。Carbon Black などの統合を実行するために使用します。

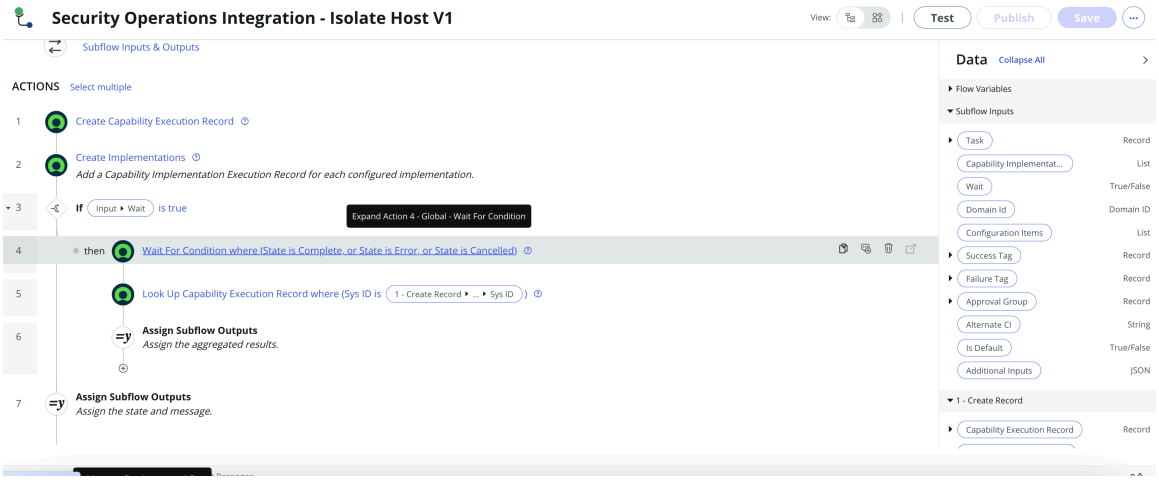
始める前に
必要なロール：sn_si.analyst

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
このフローは、セキュリティインシデント関連リストの [構成アイテム] タブからトリガーされます。

ホストを隔離



ここでは、このフローに固有のアクティビティについて説明します。他のアクティビティの詳細については、「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

[Security Operations Carbon Black 統合 - ホストを隔離] フロー

[Security Operations Carbon Black 統合 - ホストを隔離] は、[Security Operations Integration - ホストを隔離] フローによって起動される Carbon Black 統合の実装です。

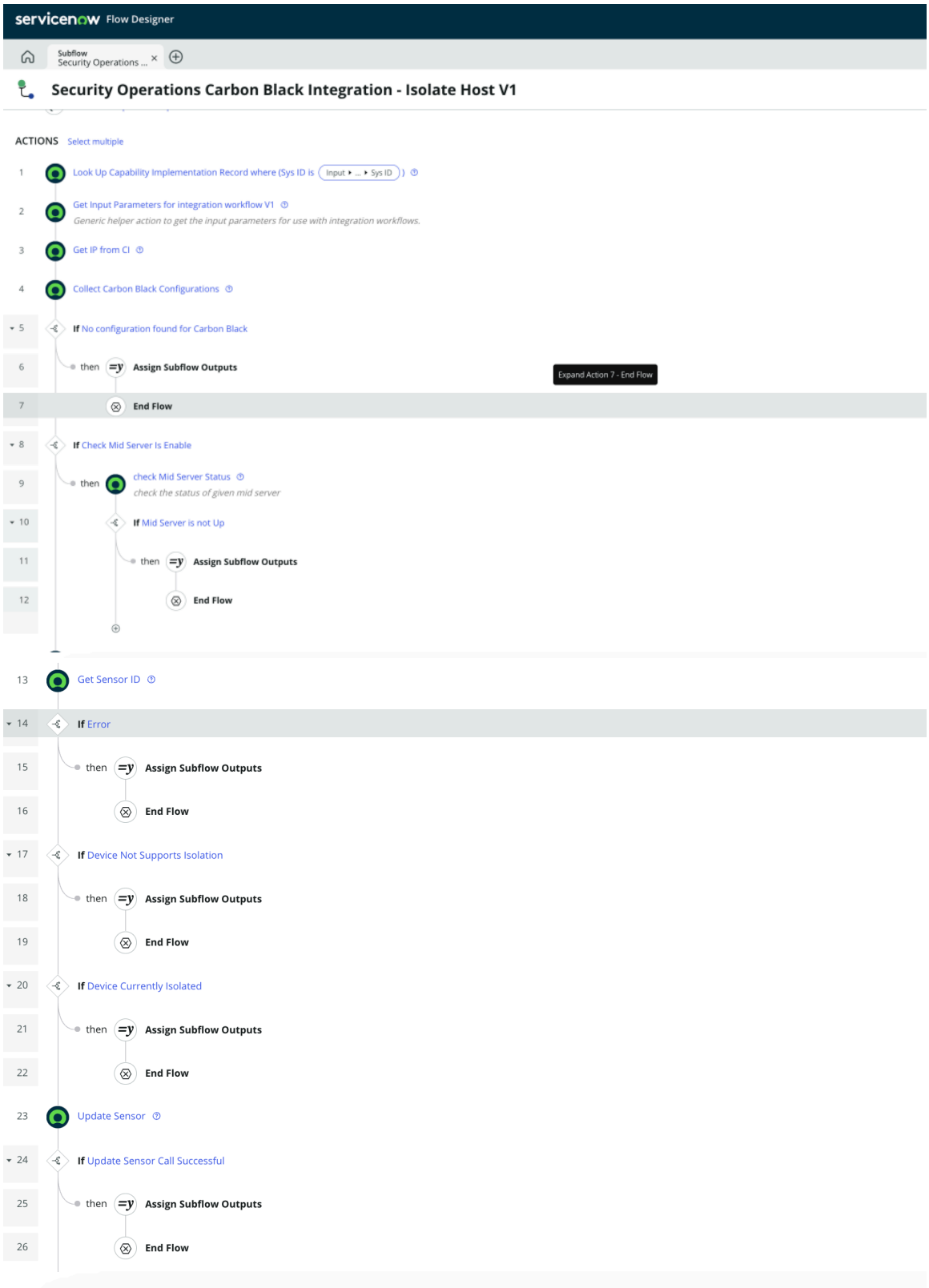
始める前に
必要なロール：sn_si.analyst

このタスクについて
フロープロセスアクティビティには次のものが含まれます。

- 実行トラッキング:開始 (CI) フローアクション
- CI から IP を取得
- Carbon Black 設定の収集
- 機能トラッキング:失敗フローアクション
- センサー ID を取得
- [ネットワーク分離を有効に設定する] アクティビティ
- センサーの更新 ：ホストの隔離結果を返します。
- 機能トラッキング:フローアクションを完了

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



ここでは、このフローに固有のアクティビティについて説明します。他のアクティビティの詳細については、「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

[センサー **ID** を取得] フローアクション

[センサー ID を取得] フローアクションは、フローで使用するセンサー識別子を収集します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[センサー ID を取得] フローアクションを任意のフローで使用して、フローで使用するセンサー情報を収集できます。

結果

このフローアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	センサー識別子が見つかりました。
失敗	センサーが見つかりませんでした。その他のエラー情報は、フローアクション出力エラーで確認できます。

入力変数

フローアクションの初期動作が、入力変数によって決まります。

変数	説明
api_token	Carbon Black の API キー。
use_mid_server	REST アクティビティが MID サーバーを使用して Carbon Black とやり取りするかどうかを決定します。
endpoint_base	Carbon Black API のベース URL。
ci_ip_address	構成アイテムの IP アドレス。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
status_code	要求が成功したかどうかを判断します。失敗した場合は、HTTP エラーコードとメッセージを表示します。
アレイ要素タイプ	API 変数。
sensor_detail	JSON 形式の Carbon Black センサーの説明。

[ネットワーク分離を有効に設定する] アクティビティ

[ネットワーク分離を有効に設定する] ワークフローアクティビティは、ネットワーク分離を有効にします。

[ネットワーク分離を有効に設定する] ワークフローアクティビティを任意のワークフローで使用して、ネットワーク分離を有効にできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	ネットワーク分離が有効になりました。
失敗	ネットワーク分離を有効にできません。その他のエラー情報は、アクティビティ出力エラーで確認できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

変数	説明
sensor_detail	JSON 形式の Carbon Black センサーの説明。
disable	ホストを隔離するかどうかを決定するか、ホスト隔離を削除します。 True = 分離を無効にする False = 分離が有効

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
sensor_detail	JSON 形式の Carbon Black センサーの説明。

[センサーの更新] アクティビティ

[センサーの更新] ワークフローアクティビティは、センサーを更新してホストまたはエンドポイントを隔離します。

[センサーの更新] アクティビティを任意のワークフローで使用して、ホストまたはエンドポイントを隔離できます。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	センサーが更新されました。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

結果 (続く)

結果	説明
失敗	センサーを更新できません。その他のエラー情報は、アクティビティ出力エラーで確認できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

変数	説明
api_token	Carbon Black の API キー。
use_mid_server	REST アクティビティが MID サーバーを使用して Carbon Black とやり取りするかどうかを決定します。
endpoint_base	Carbon Black API のベース URL。
sensor_id	センサー識別子。
sensor_detail	JSON 形式の Carbon Black センサーの説明。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
status_code	要求が成功したかどうかを判断します。失敗した場合は、HTTP エラーコードとメッセージを表示します。

自動翻訳

Security Operations Carbon Black 統合 - ホスト隔離削除フロー

[Security Operations Carbon Black 統合 - ホスト隔離削除] フローは、Carbon Black システム内の指定されたホストまたはエンドポイントとの通信のブロックを解除します。

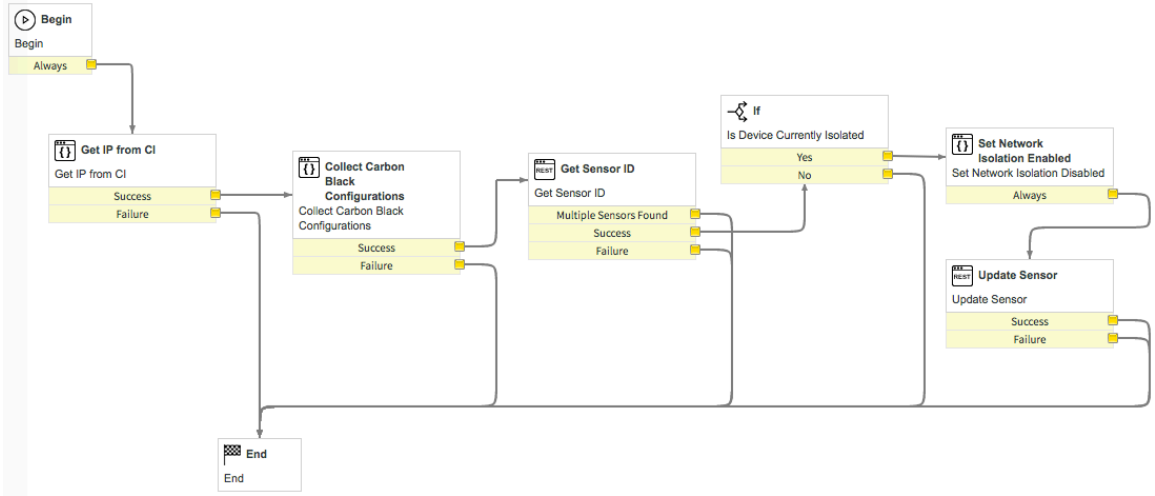
始める前に
必要なロール：sn_si.analyst

このタスクについて
このフローは機能の一部ではなく、実行するにはカスタムオーケストレーションが必要です。
フロープロセスアクティビティには次のものが含まれます。

- [CI から IP を取得] アクティビティ
- 成功した場合 - [Carbon Black 設定の収集] フローアクション
- [センサー ID を取得] フローアクションセンサー ID を取得
- デバイスが隔離をサポートしており、デバイスが隔離されていない場合は 無効にします。
- [センサーの更新] アクティビティ - ホスト隔離の結果を返します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Carbon Black 統合 - ホスト隔離削除



Security Operations Integration - [ウォッチリストに公開] 機能

[ウォッチリストに公開] 機能は、セキュリティインシデントに関連する観測事象とインジケーターを、セキュリティイベントをモニタリングしてアラートを生成するサードパーティのウォッチリストに追加します。この機能は、調査中にインシデント応答の一部として使用されます。

注:
利用可能な実装がない場合、機能アクションは製品メニューに表示されません。

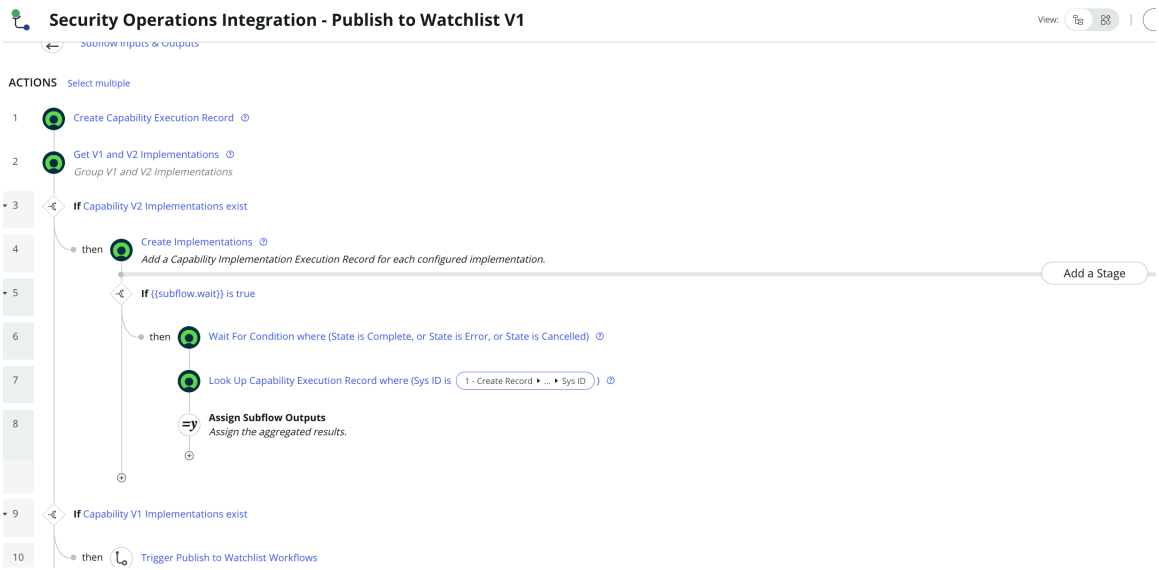
Security Operations Integration - ウォッチリストに公開フロー

「Security **Operations Integrations -** ウォッチリストに公開」フローは、統合に依存しない高レベルのフローです。機能をサポートするサードパーティのウォッチリストに観測事象を追加します。統合を実行するために使用します。

始める前に
必要なロール：sn_si.analyst

このタスクについて
このフローは、統合が利用可能な場合にのみ表示され、実行されます。これは、セキュリティインシデントの [観測事象] または [関連するインジケーター] タブからトリガーされます。

ウォッチリストに公開



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ここでは、このフローに固有のアクティビティについて説明します。他のアクティビティの詳細については、「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

Security Operations Integration - [サイティング検索] 機能

[サイティング検索] 機能は一連の観測事象を受け入れ、サイティング検索をサポートする統合を検索して、これらの検索を実行します。

サイティング検索機能には、サイティング検索を実行するワークフロー Security Operations Integration - サイティング検索フロー があります。このワークフローは、観測事象のリストを受け入れ、実装機能を検索し、[サイティング検索構成] に基づいてクエリを作成し、設定されたワークフローに基づいて検索を実行します。検索が完了すると、サイティングが見つかったかどうか、見つかった場合はその件数を含むメモがインシデント作業メモに追加されます。

サイティング検索構成を表示するには、次に移動します: セキュリティオペレーション > 統合 > サイティング検索構成.

注:
利用可能な実装がない場合、機能アクションは製品メニューに表示されません。

サイティング検索設定レコードの作成

複数のサイティング検索設定レコードを作成し、複数のログストアを照会したり、検索パラメーターを変更したりするときに使用します。

始める前に
必要なロール：sn_si.admin

- CIM アドオンが Splunk インスタンスにインストールされている必要があります。
- 保存された検索とインプレースクエリは、Splunk Integration でのみサポートされています。

このタスクについて
サイティング検索設定レコードを作成して、Splunk エンタープライズログストアで保存済みの検索 を呼び出すこともできます。

注:
検索構成クエリは、Splunk 共通情報モデル (CIM) に準拠するために Splunk ログデータに依存しています。

保存済みの検索構成を使用して、次のことができます。

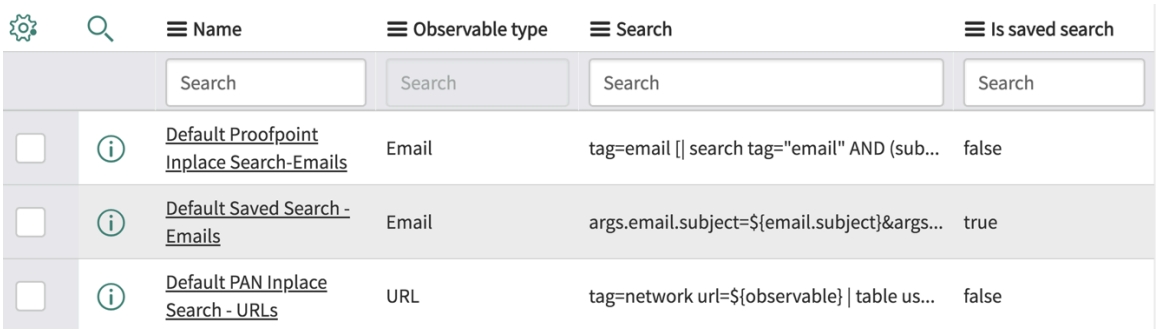
- 複数のイベントレコードを組み合わせたカスタム検索の作成
- 設計効率に優れ、効果的な検索
- Splunk の保存済みの検索でパラメーター化された入力を使用

ベースシステムには、次の画像に示すサンプル構成が含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

保存済みの検索の構成



	Name	Observable type	Search	Is saved search
	Search	Search	Search	Search
	Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
	Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
	Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

この保存済みの検索とインプレース構成クエリはサンプルクエリです。パラメーターは、お使いの環境に合わせて適宜置き換えてください。必要に応じて、保存済みの検索構成を追加で作成します。保存済みの検索構成を定義するときに、検索クエリの名前とパラメーターは、Splunk インスタンスで定義した保存済みの構成と一致させる必要があります。名前とパラメーターが同じでない場合、サイティング検索を実行しても正確な結果が表示されない可能性があります。

注:
Splunk インスタンスで、[検索、レポート、およびアラート (Searches, Reports, and Alerts)] ページに移動し、保存済みの検索クエリを見つけます。[権限 **(Permissions)]** リンクをクリックして [権限 (Permissions)] ページに移動します。[すべてのアプリ **(All Apps)]** ラジオボタンを選択し、[全員 **(Everyone)]** の [読み取り権限 **(Read Permission)]** オプションを有効にします。これにより、保存済みの検索クエリの [共有 (Sharing)] 列の値が [プライベート (Private)] から [アプリ (App)] に変更されます。これが設定されていない場合、保存済みの検索クエリが何も結果を返さない可能性があります。

保存済みの検索構成が Splunk インスタンスで定義した構成と一致するかどうかを確認するには、次の手順を実行します。

1. 次のように移動する。 設定 > 検索、レポート、およびアラート.
2. [アプリコンテキスト] を [すべて] に変更します。

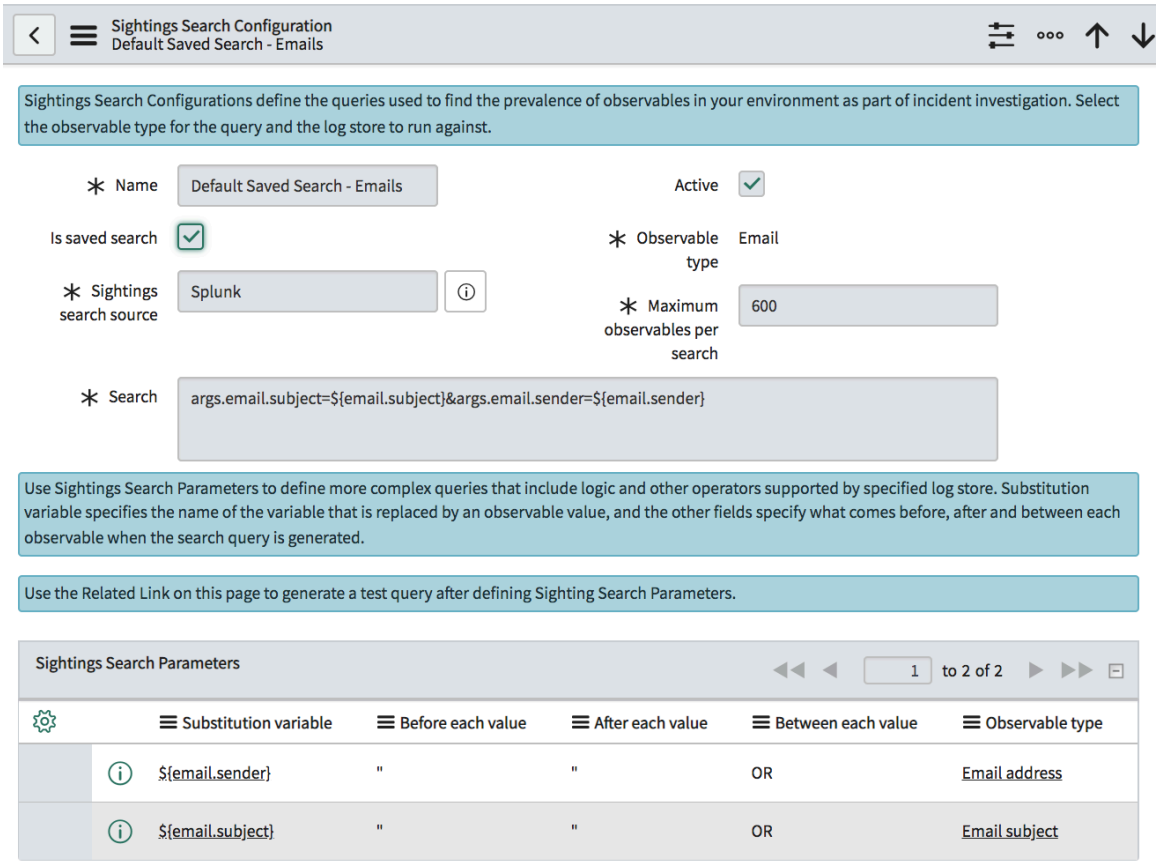
   検索レポートのリストが表示されます。
3. 保存済みの検索クエリがリストに存在することを確認します。

たとえば、[サイティング検索構成] フォームには、メールアドレスとメール送信者が検索パラメーターとして含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[サイティング検索構成] フォーム



Splunk インスタンスで、同じ「Default Saved Search - Emails (デフォルトの保存済みの検索 - メール)」という名前で、同じ検索パラメーター (メールアドレスとメールの件名) の保存済みの検索を定義します。名前と検索パラメーターが同じでない場合、サイティング検索で正確な結果が生成されない可能性があります。

手順

1. 次のように移動する。 セキュリティオペレーション > 統合 > サイティング検索構成 をクリックし、新しいレコードを作成します (フィールドの説明についてはテーブルを参照)。

[サイティング検索構成] フォーム

フィールド	説明
名前	構成の名前。
保存された検索	このオプションを選択すると、保存された検索構成が作成されます。
サイティング検索ソース	サイティング検索のソース。ソースとして Splunk ログストアを選択します。
有効	保存済みの検索ステータスのオプション。サイティング検索に使用できるのは、アクティブな検索構成だけです。
観測可能タイプ	[観測事象タイプ] には、IP、ハッシュ値、URL、ドメイン名などの任意の観測事象タイプを指定できます。
検索あたりの最大観測事象の数	検索から返される観測事象の最大数。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
検索	デフォルトの検索文字列は `$(observable)` ですが、Splunk ログストアでサポートされているパラメーターを指定することで、独自の検索クエリを定義できます。

2. **[Submit]** をクリックします。

タスクの結果
これでサイティング検索設定レコードを作成できました。

次のタスク
検索クエリを定義した後、[サイティング検索テストクエリを生成] をクリックし、観測事象値のリストを指定して、この保存済みの検索構成に基づいてテストクエリを生成します。

サイティング検索の実行

時間の経過に伴う脅威のまん延を判断したり、修復または根絶作業をテストしたりします。セキュリティインシデントから、個別または複数の観測事象と検索対象の日付範囲を選択できます。結果は [セキュリティインシデント観測事象] 関連リストに含まれます。

始める前に
必要なロール：sn_si.analyst

このタスクについて
サイティング検索機能には、サイティング検索を実行するフロー Security Operations Integration - サイティング検索フロー があります。このフローは、観測事象のリストを受け入れ、実装機能を検索し、サイティング検索構成に基づいてクエリを作成し、構成されたフローに基づいて検索を実行します。

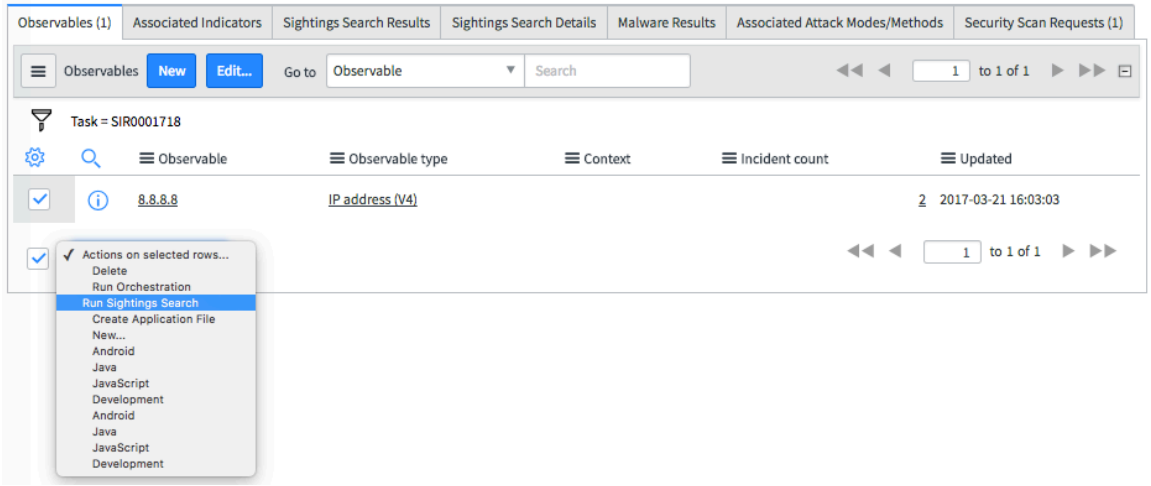
> **注:**
> アクティブな実装を構成する必要があります。サイティング検索は、Elasticsearch、Splunk、McAfee ESM、HPE ArcSight Logger、および QRadar インシデント拡張をサポートしています。実装を使用できない場合、[サイティング検索を実行] などの機能アクションは製品メニューに表示されません。

手順

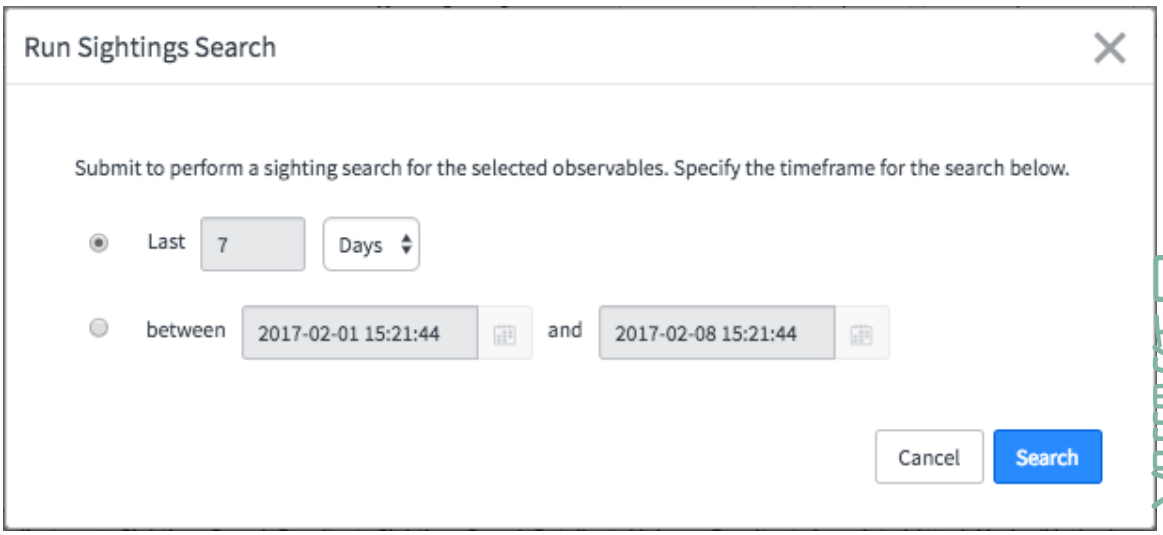
1. セキュリティインシデントに移動します。
2. **[IoC** を表示] 関連リンクをクリックします。
3. [関連リスト] タブから [観測事象] を選択します。
4. サイティング検索を実行する観測事象を選択します。
5. [選択した行のアクション...] ドロップダウンメニューで [サイティング検索を実行] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[サイティング検索を実行] ダイアログボックスが開きます。



自動翻訳

注:
ダイアログボックスに入力された値は、この実行の機能構成値を上書きします。

6. データを検索する日数または日付範囲を選択します。

オプション	説明
前の	検索するインシデントの作成までの時間数または日数。 デフォルトは 7 日です。制限は 99 時間または日です。
次の間	検索する日付の範囲。デフォルトの日付は次のとおりです。 インシデントが作成された日時。 インシデントのオープンの 7 日前の日時。

注:
[前の] は、検索するインシデントの作成までの時間数または日数です。デフォルトは 7 日です。制限は 99 時間または日です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. [検索] をクリックします。
サイティング検索レコードが作成されます。集計および関連するサイティングデータは、[サイティング検索結果] タブおよび [サイティング検索の詳細] タブの下に表示されます。

> **注:**
> サイティング検索結果データは、生データを含むように構成された実装の場合を除き、トラステッドセキュリティサークル と共有できます。

サイティング検索結果

結果	説明
数値	サイティング検索の識別子。
観測事象数	クエリで検索される観測事象の数。
内部発生回数	内部発生回数の数。
外部発生回数	外部発生回数の数(脅威共有から受信)。
一致する構成アイテム	環境内で見つかった各観測事象について、cmdb 内の既存のレコードと一致した構成アイテムの数。
開始日の範囲	サイティングの検索を開始する時間。
終了日の範囲	サイティングの検索を終了する時間。
更新日時	最後の変更の日時。

注：サイティング検索に使用する実装が生データを含むように構成されており、少なくとも 1 つのサイティングが見つかった場合、生データサンプルを含む添付ファイルがセキュリティインシデントの先頭に表示されます。

サイティング検索の詳細

詳細	説明
サイティング検索	サイティング検索の識別子。
観測事象	クエリによって検索された観測事象。
観測可能タイプ	クエリによって検索された観測事象のタイプ。
内部発生回数	内部発生回数の集計数。
外部発生回数	外部発生回数の集計数(脅威共有から受信)。
更新日時	最後の変更の日時。

Security Operations Integration - サイティング検索フロー

Security Operations Integration - サイティング検索 フローは、統合に依存しない高レベルのフローです。構成設定されたクエリを使用して、機能をサポートする構成済みの統合に基づいて、一連の観測事象を検索します。Splunk や Elasticsearch などの統合を実行するために使用します。

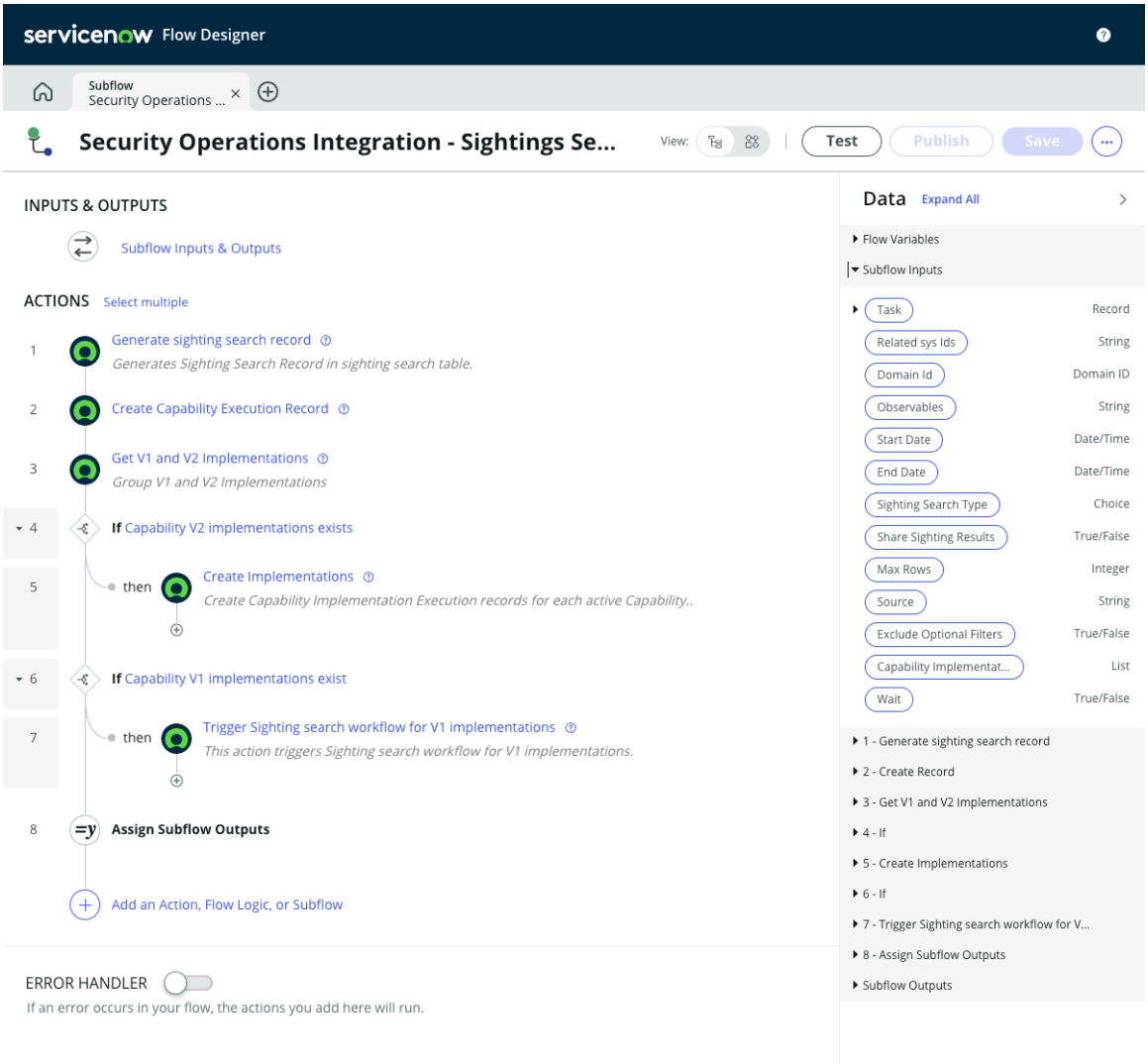
始める前に
必要なロール：sn_si.analyst

このタスクについて
セキュリティインシデントに観測事象が添付されている場合、[セキュリティインシデント観測事象] タブの [選択した行のアクション...] ドロップダウンメニューで [サイティング検索を実行] をクリックすると、このフローがトリガーされます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

サイティング検索



自動翻訳

ここでは、このフローに固有のアクティビティについて説明します。他のアクティビティの詳細については、「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

[サイティング検索 - 観測事象を決定] アクティビティ

[サイティング検索 - 観測事象を決定] ワークフローアクティビティは、ワークフローに含める観測事象を決定します。

[サイティング検索 - 観測事象を決定] アクティビティを任意のワークフローで使用して、ワークフローに含める観測事象を決定できます。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	観測事象が見つかりました。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

結果 (続く)

結果	説明
失敗	観測事象が見つかりませんでした。その他のエラー情報は、アクティビティ出力エラーで確認できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

変数	説明
task_sys_id	タスク識別子 (セキュリティインシデントを観測事象にマッピング)
観測事象	IP アドレス、ハッシュ、URL、ドメイン名。
workflow_current_sys_id	現在のレコードのシステム識別子。task_sys_id、観測事象入力が利用できない場合にのみ使用されます。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
観測事象	フィルター済み観測事象

[永続的な観測事象の発生] アクティビティ

[永続的な観測事象の発生] ワークフローアクティビティは、サードパーティ統合から観測事象を取得します。

[永続的な観測事象の発生] アクティビティを任意のワークフローで使用して、サードパーティ統合で見つかった観測事象を取得できます。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	観測事象が取得されました。
失敗	観測事象を収集中にエラーが発生しました。その他のエラー情報は、アクティビティ出力エラーで確認できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

変数	説明
sightingsResponse	
taskId	タスク識別子。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
response	

[観測事象発生クエリを取得] アクティビティ

[観測事象発生クエリを取得] を取得クエリ] ワークフローアクティビティは、統合構成からクエリを取得します。

[観測事象発生クエリを取得] アクティビティを任意のワークフローで使用し、[パラレルフローランチャー] を使用して指定された実装に送信するクエリを取得できます。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	クエリが見つかりました。
失敗	クエリの取得中にエラーが発生しました。その他のエラー情報は、アクティビティ出力エラーで確認できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

変数	説明
観測事象	フィルター済み観測事象のリスト。
capabilities	サポートされている機能のリスト。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数

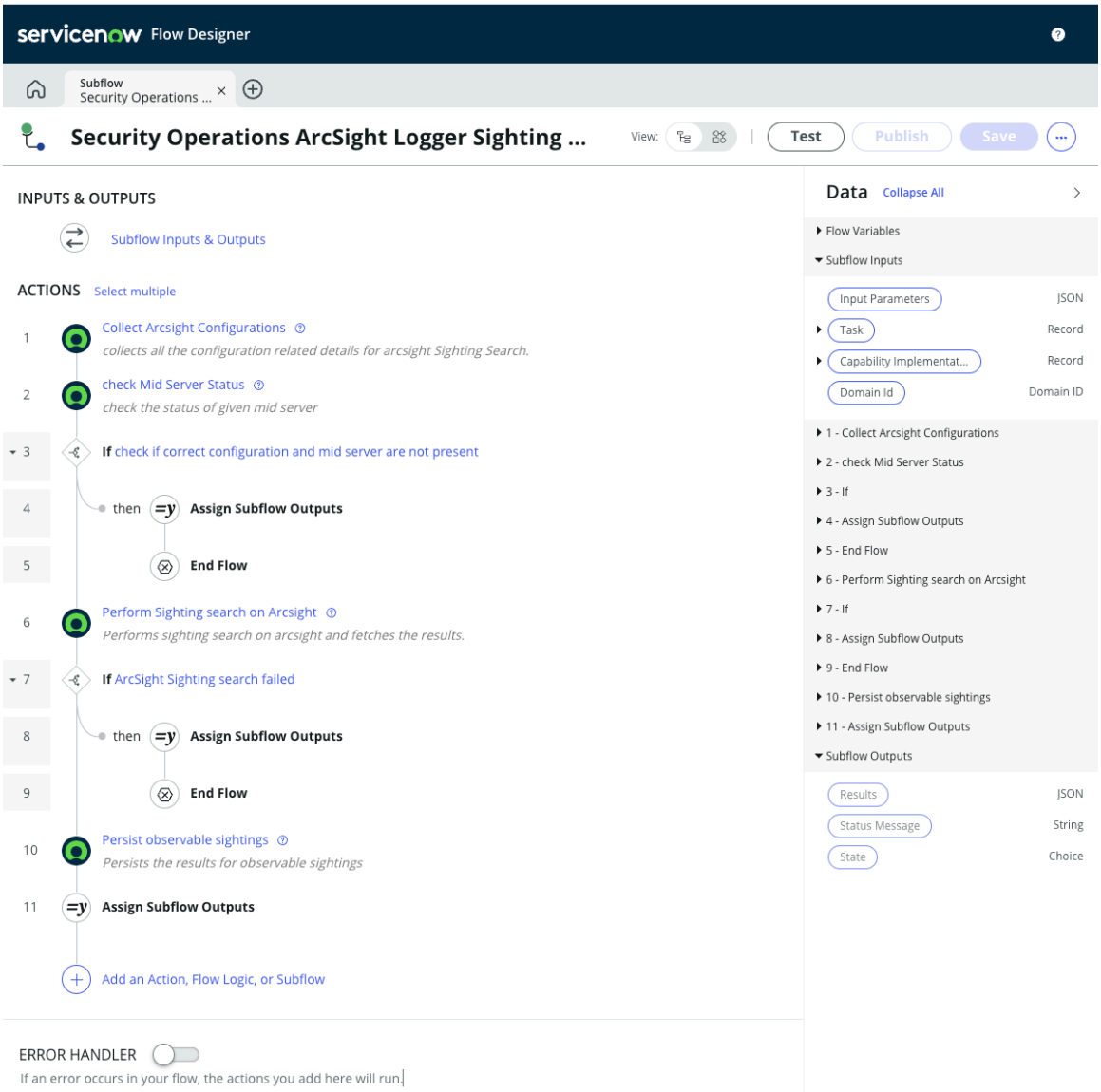
変数	説明
クエリ	検索文字列。
queryCount	実行するクエリの数。

Security Operations - Arcsight Logger サイティング検索フロー

[Security Operations - ArcSight Logger サイティング検索] フローは、[**Security Operations Integration -** サイティング検索] フローによって起動される Splunk 統合の実装です。

必要なロール：sn_si_analyst

ArcSight Logger サイティング検索



ここでは、このフローに固有のアクティビティについて説明します。他のアクティビティの詳細については、「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

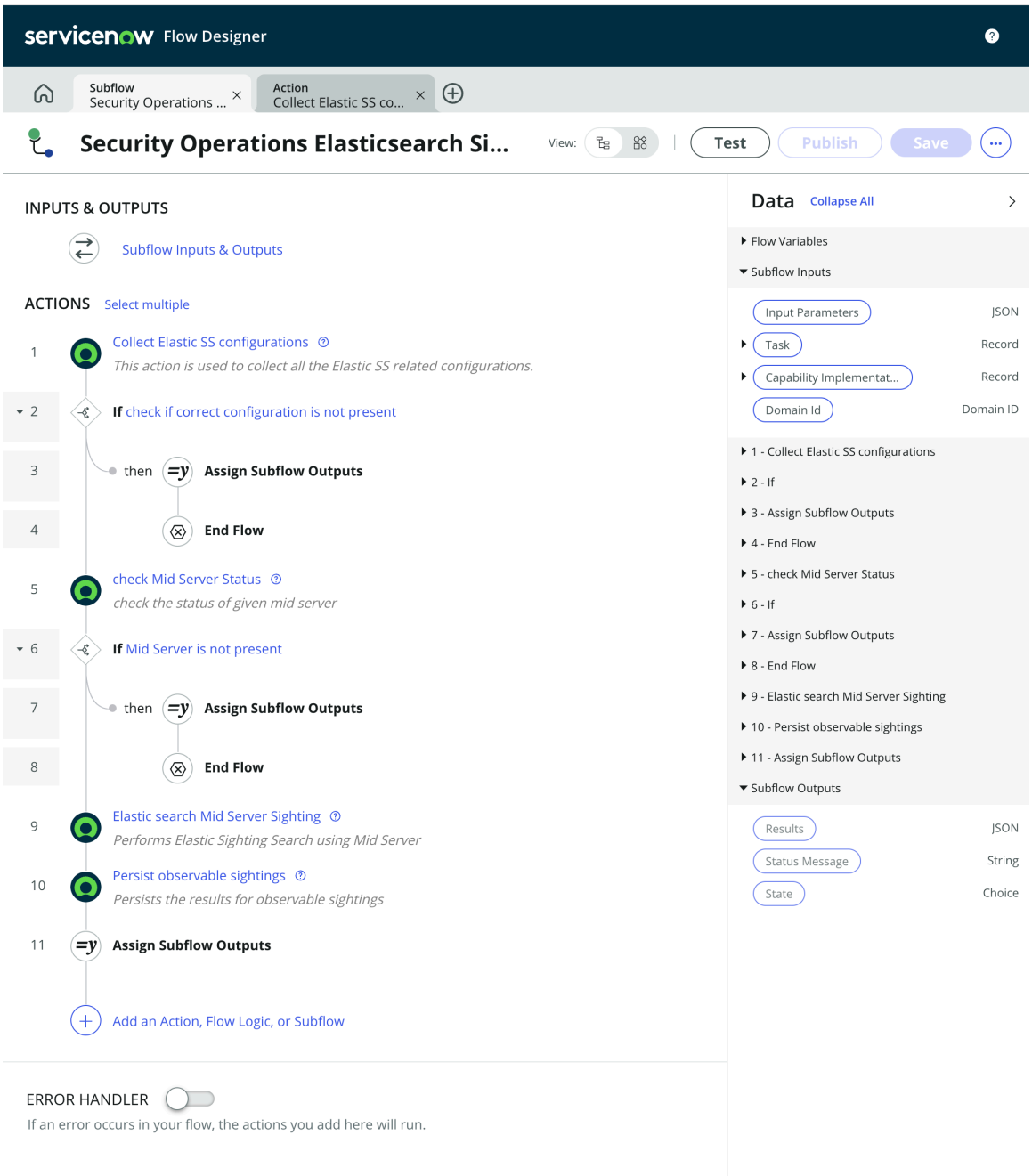
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Security Operations - Elasticsearch サイティング検索フロー

[Security Operations - Elasticsearch サイティング検索] フローは、[Security Operations Integration - サイティング検索] フローによって起動される Elasticsearch 実装です。

必要なロール：sn_si.analyst

Elasticsearch サイティング検索



ここでは、このフローに固有のアクティビティについて説明します。他のアクティビティの詳細については、「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

Security Operations - McAfee ESM サイティング検索フロー

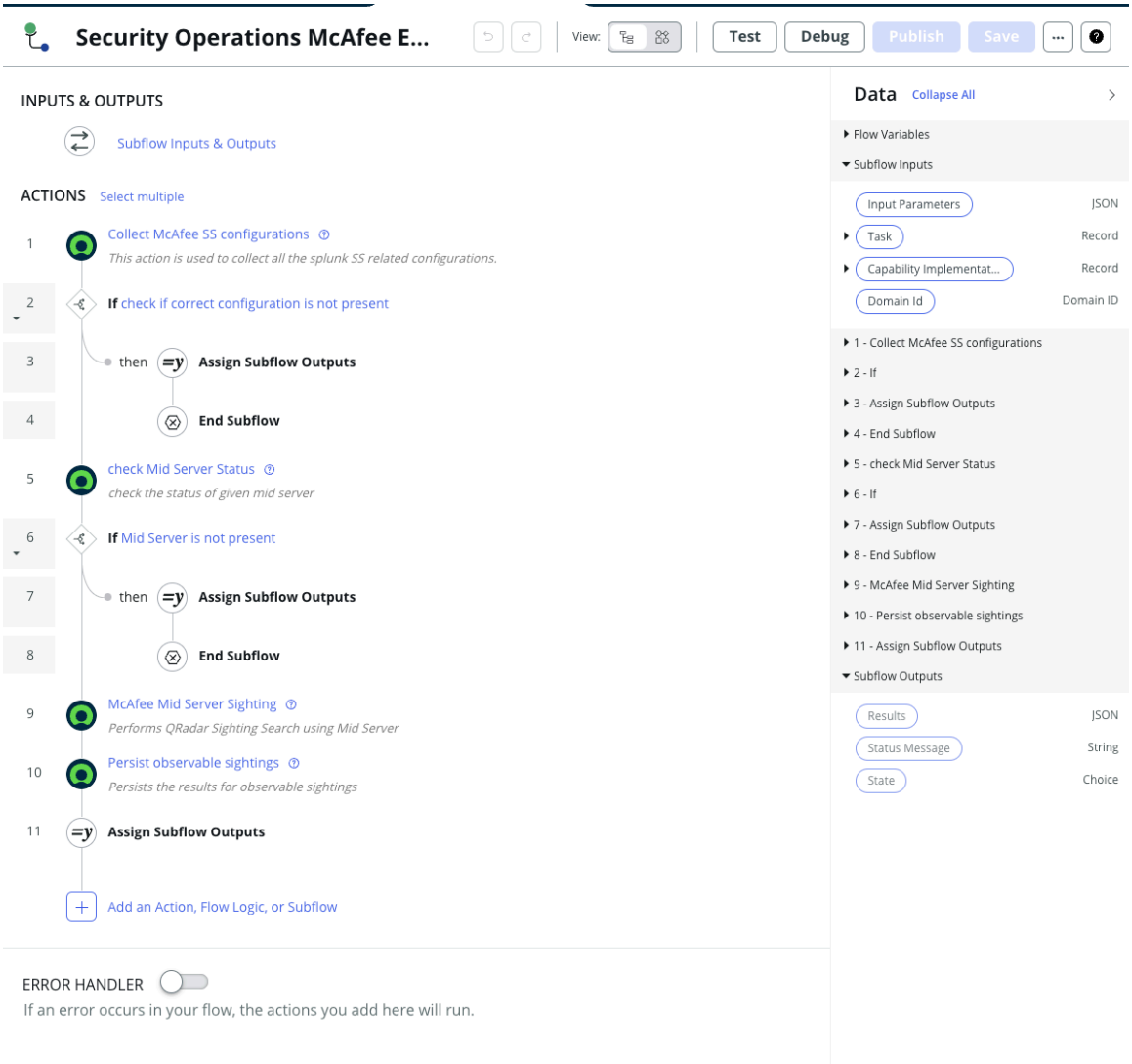
[Security Operations - McAfee ESM サイティング検索] フローは、[Security Operations Integration - サイティング検索] フローによって起動される McAfee サイティング検索の実装です。

必要なロール：sn_si_analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

McAfee ESM サイティング検索



自動翻訳

ここでは、このフローに固有のアクティビティについて説明します。他のアクティビティの詳細については、「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

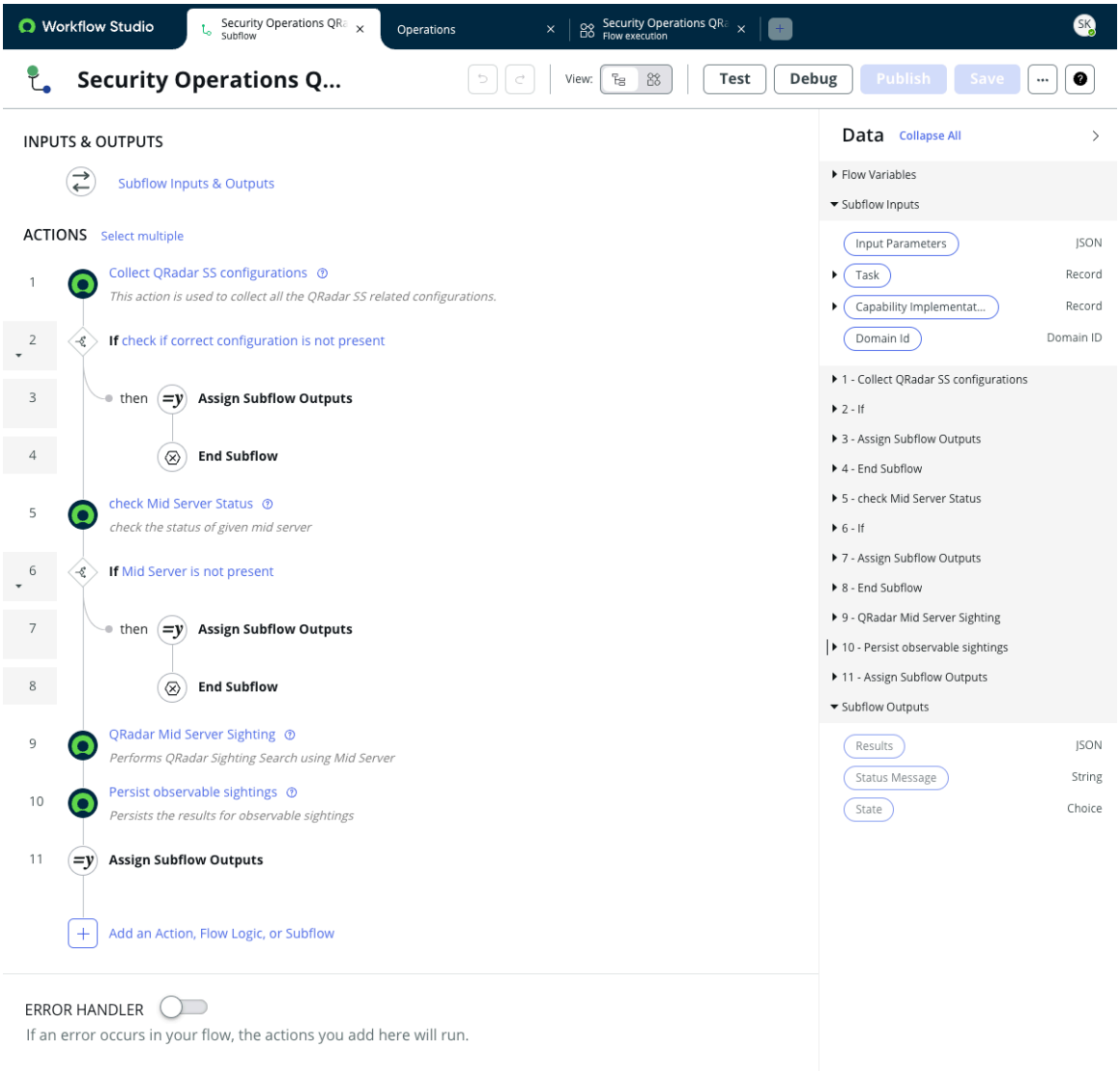
Security Operations - QRadar サイティング検索フロー

[Security Operations - QRadar サイティング検索] フローは、[**Security Operations Integration -** サイティング検索] フローによって起動される IBM QRadar 統合の実装です。

必要なロール：sn_si_analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

QRadar サイティング検索



ここでは、このフローに固有のアクティビティについて説明します。他のアクティビティの詳細については、「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

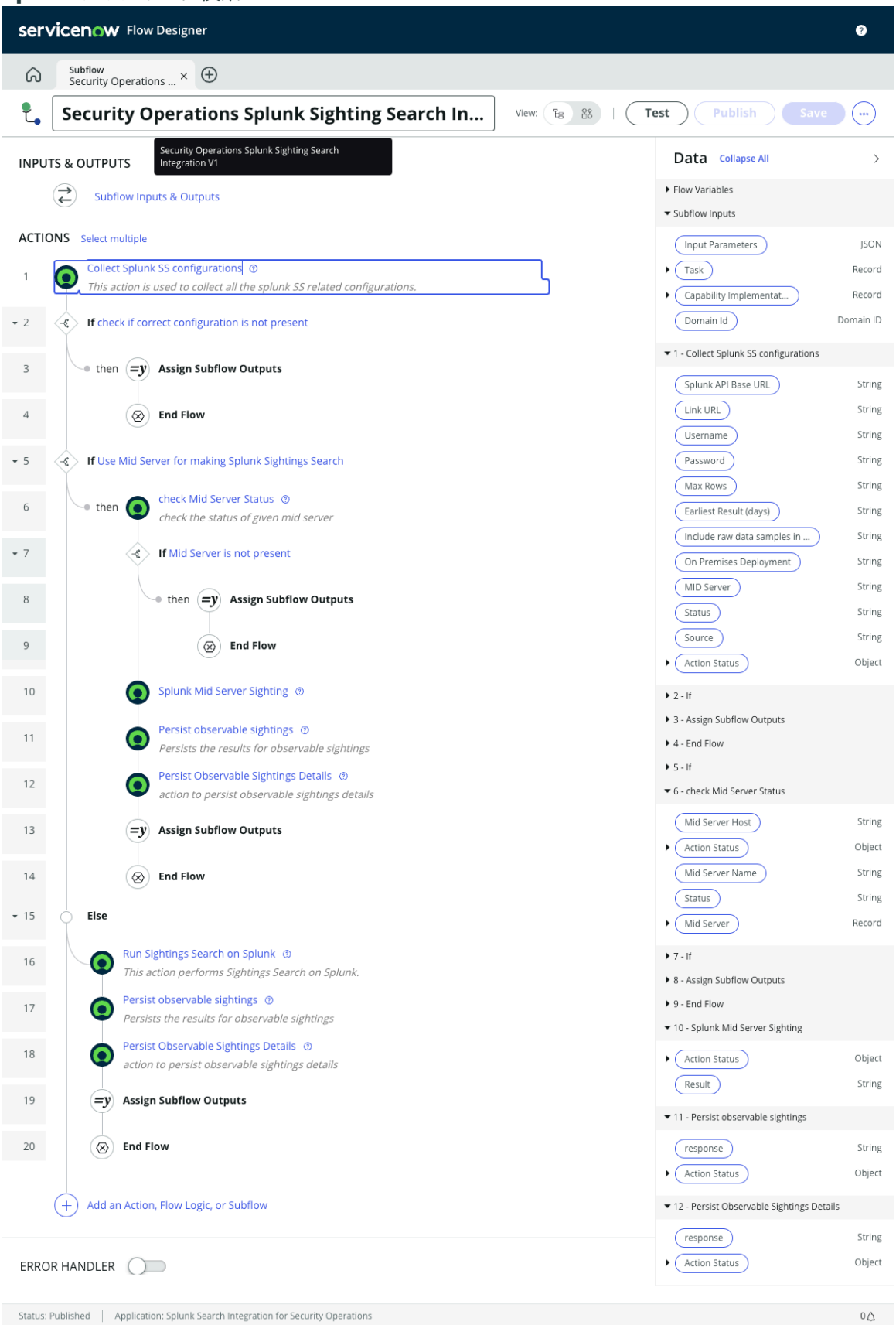
Security Operations Integration - Splunk サイティング検索フロー

[Security Operations - Splunk サイティング検索] フローは、[**Security Operations Integration -** サイティング検索] フローによって起動される Splunk 統合の実装です。

必要なロール：sn_si_analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Splunk サイティング検索



ここでは、このフローに固有のアクティビティについて説明します。他のアクティビティの詳細については、「一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サイティング検索結果の表示

内部および外部の悪意のあるインジケーターのサイティング検索結果を確認できます。

始める前に

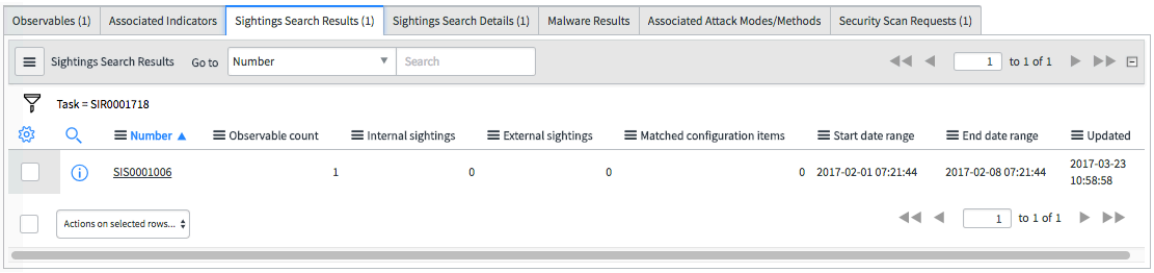
必要なロール：sn_si.analyst

このタスクについて

.

手順

1. セキュリティインシデントに移動します。
2. **[IoC** を表示] 関連リストグループの [サイティング検索結果] タブを選択し、サイティング検索のリストを表示します。



> **注:**
> このデータは トラステッドセキュリティサークル と共有できます。

サイティング検索結果

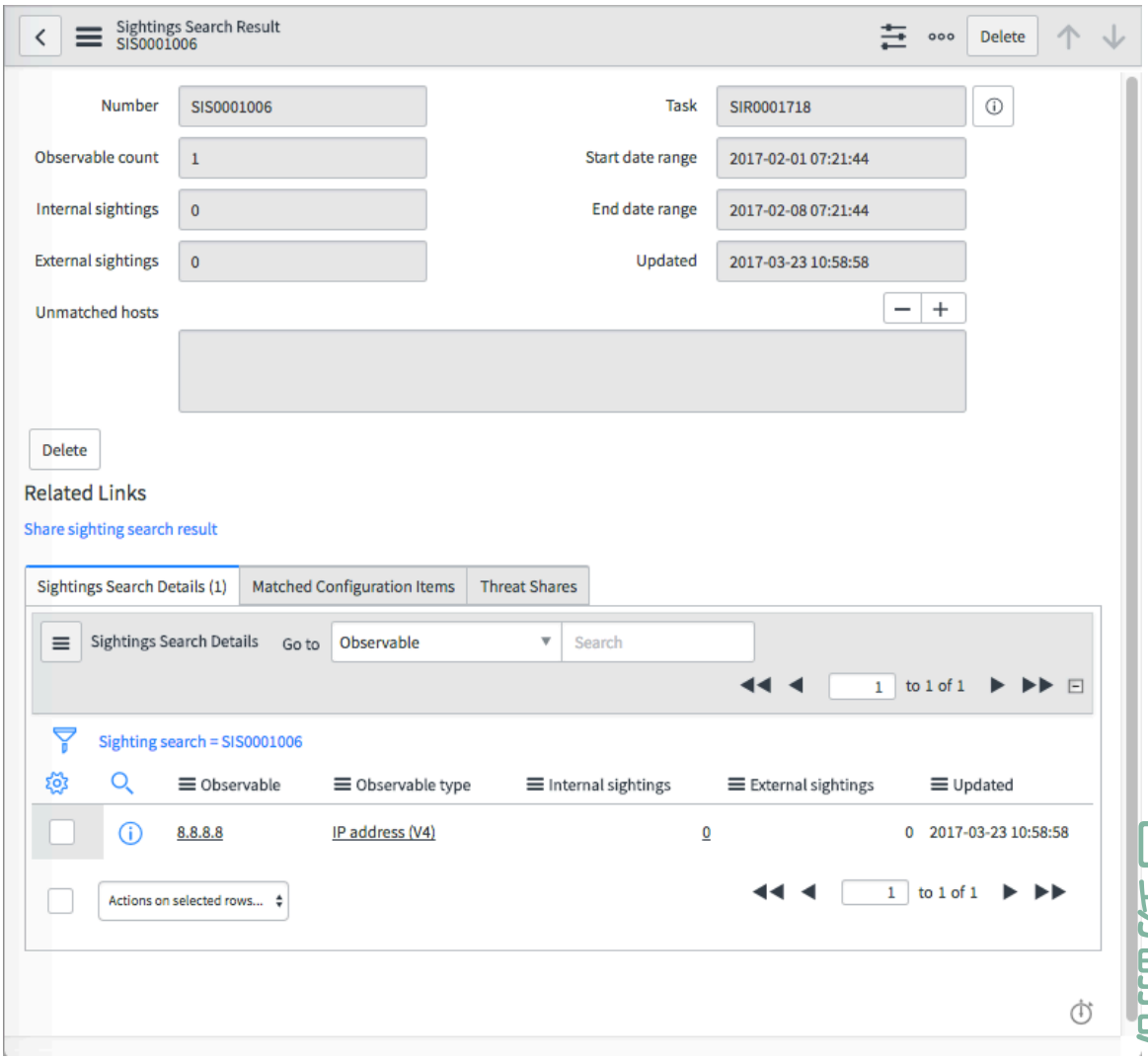
結果	説明
数値	サイティング検索の識別子。
観測事象数	検索される観測事象の数。
内部発生回数	内部発生回数の集計数。
外部発生回数	外部発生回数の集計数(脅威共有から受信)。
一致する構成アイテム	cmdb の既存のレコードに一致する構成アイテムの集計数。
開始日の範囲	サイティングの検索を開始する時間。
終了日の範囲	サイティングの検索を終了する時間。
更新日時	最後の変更の日時。

単一の検索の詳細を表示するには、次の手順を実行します。

3. [サイティング検索結果] リストで [サイティング検索] をクリックします。
[サイティング検索結果] フォームが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[サイティング検索結果] フォーム

詳細	説明
数値	内部サイティング検索の識別子。
観測事象数	このクエリで検索される観測事象の数。
内部発生回数	この検索の内部発生回数の数。
外部発生回数	この検索の外部発生回数の数(トラステッドセキュリティサークル から受信)。
一致しないホスト	cmdb のどのレコードとも一致しなかった、この検索の潜在的な構成アイテムのリスト。
タスク	セキュリティインシデントタスク識別子。
開始日の範囲	サイティング検索が開始された時間。
終了日の範囲	サイティング検索が停止された時間。
更新日時	最後の変更の日時。
サイティング検索の詳細	タイプ、サイティングの数、変更日。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細	説明
一致する構成アイテム	cmdb の既存のレコードに一致する構成アイテムの数。CI とサイティングを一覧表示します。
脅威共有	トラステッドセキュリティサークル と共有される脅威のリスト。

サイティング検索結果の共有

特定の検索に関連付けられたローカルのサイティングの詳細または結果を Trusted Security Circle と共有できます。

始める前に

必要なロール：sn_si.analyst

このタスクについて

共有は、次のセキュリティインシデントレスポンスの [プロパティ] を使用して自動化できます。

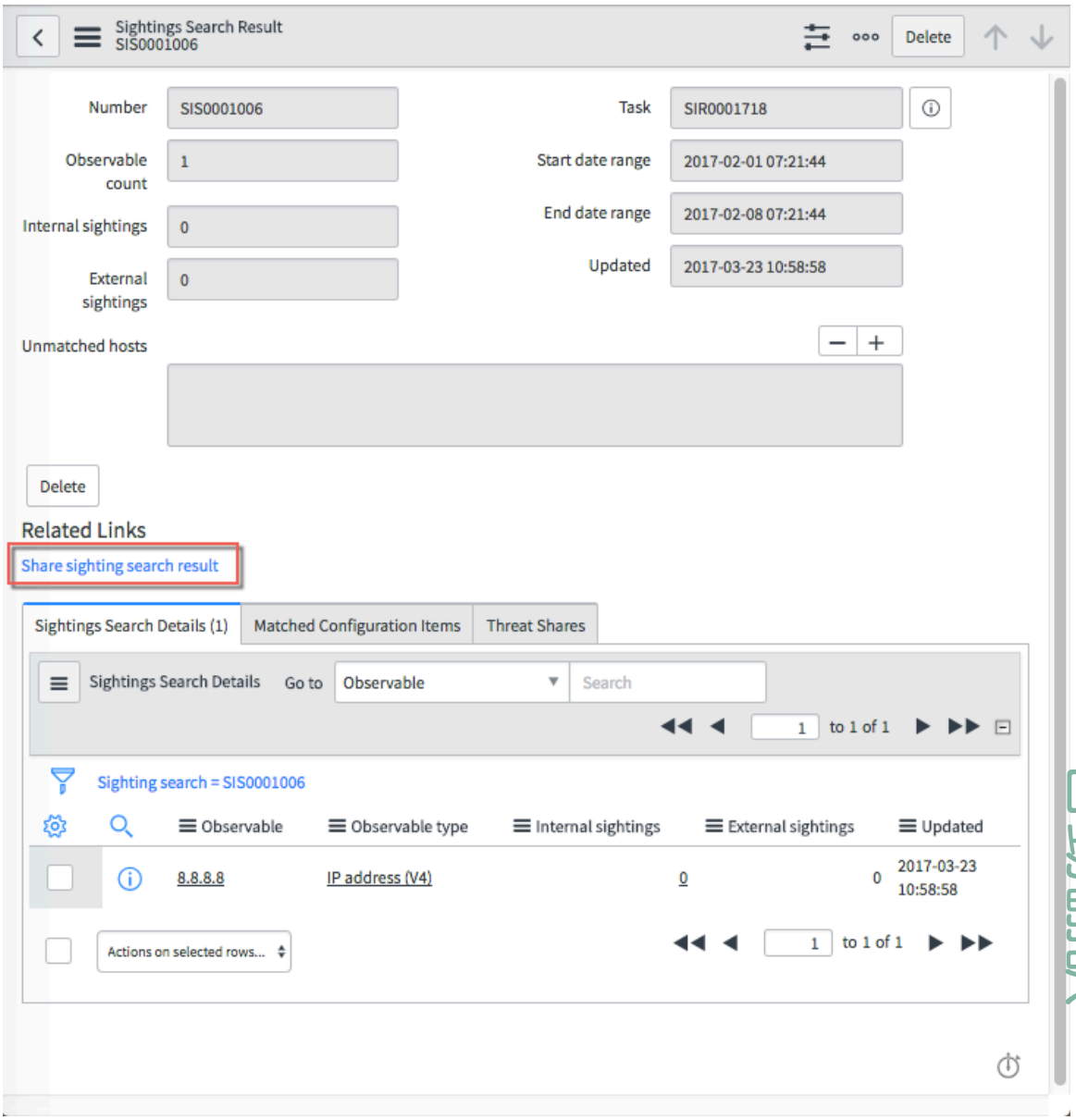
- サイティング検索の結果をデフォルトの ServiceNow の信頼できるサークルと自動的に共有する
- サイティング検索結果を自動的に共有するときに、ローカルサイティングのない観測事象を含める
- 信頼できるサークルから脅威共有を受信した場合は常にローカルサイティングで応答する

手順

1. セキュリティインシデントに移動します。
2. **[IoC** を表示] 関連リストをクリックし、[サイティング検索結果] タブを選択してサイティング検索のリストを表示します。
3. サイティング検索結果をクリックします。

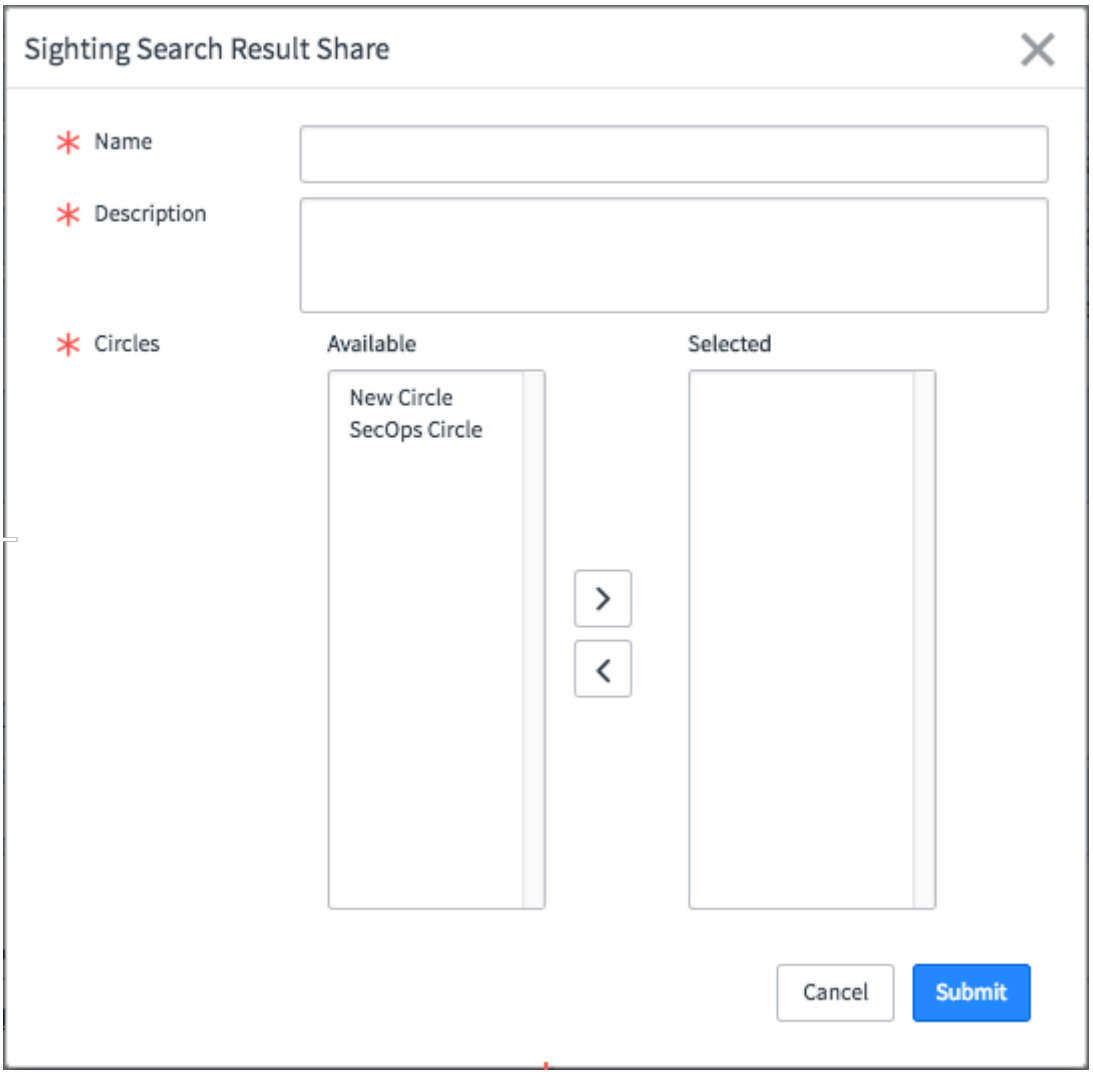
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [サイティング検索結果] フォームで、[サイティング検索の共有 **(Share Sightings Search)]** 関連リンクをクリックします。
[サイティング検索結果の共有 (Share Sightings Search)] ダイアログボックスが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

5. この観測事象共有レコードの名前を入力します。
6. 共有する観測事象の説明を入力します。
7. 観測事象を共有するサークルを選択します。
8. **[Submit]** をクリックします。
   観測事象は、指定された信頼できるサークルと共有されます。

セキュリティインシデントからの観測事象の共有

セキュリティインシデントレスポンス のセキュリティインシデントから信頼できるサークルのメンバーと観測事象を共有できます。

始める前に

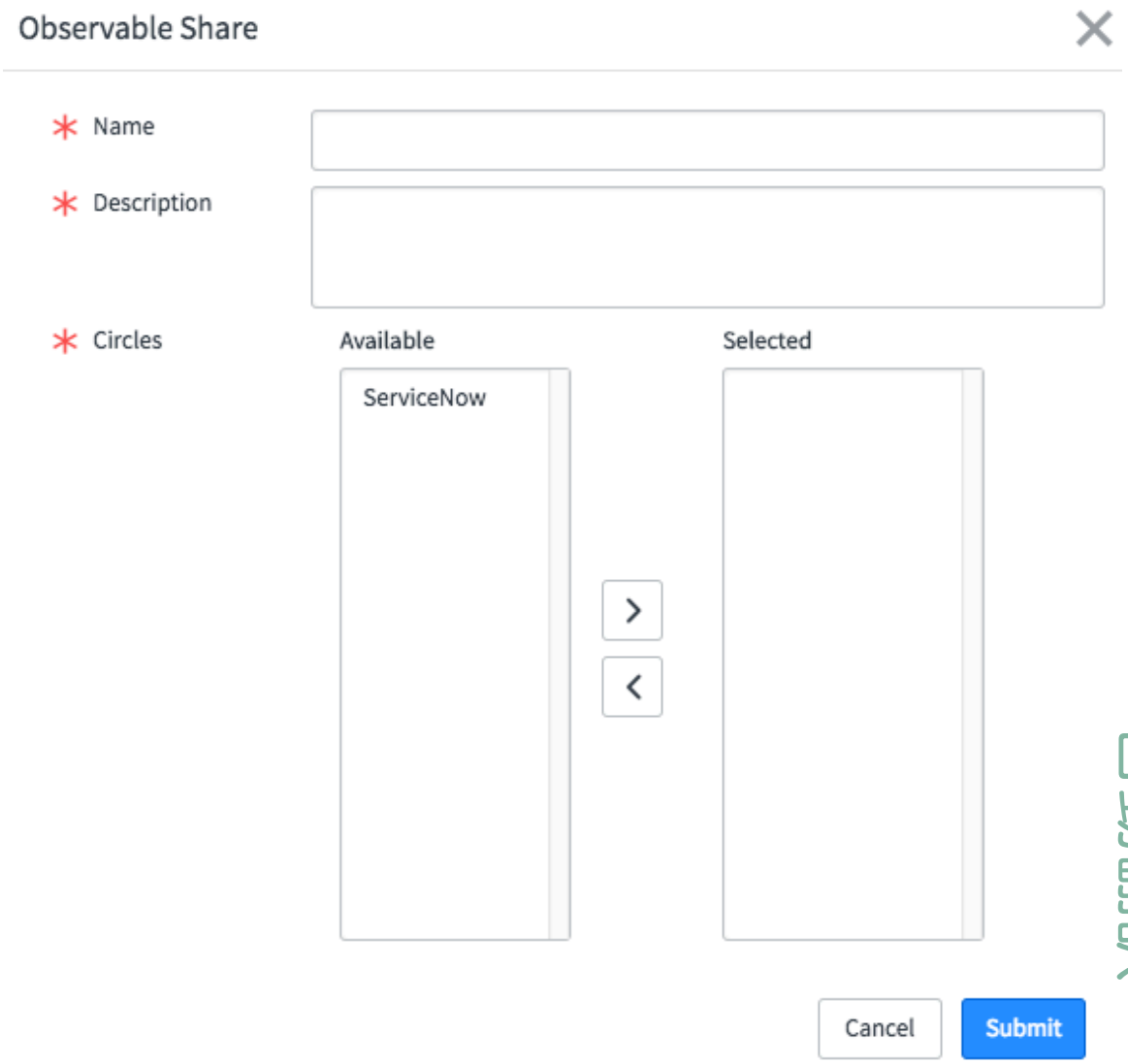
必要なロール：sn_si.analyst

手順

1. セキュリティインシデントに移動します。
2. **[IoC** を表示] 関連リストグループから [観測事象] タブを選択します。
3. 観測事象をクリックします。
4. [観測事象] フォームで、[観測事象の共有] 関連リンクをクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[観測事象の共有] ダイアログボックスが表示されます。



5. この脅威共有レコードの名前を入力します。
6. 選択した観測事象の説明を入力します。
7. 観測事象を共有するサークルを選択します。
8. **[Submit]** をクリックします。
   観測事象は、指定された信頼できるサークルと共有されます。
9. [脅威共有] タブをクリックすると、脅威共有レコードを表示できます。
10. 共有されている観測事象にサイティングが含まれている場合は、サイティングも共有され、[サイティング] タブをクリックして表示できます。

サイティング検索の詳細の表示

すべてのサイティング検索の集計の詳細を確認します。

始める前に

必要なロール：sn_si.analyst

このタスクについて

.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. セキュリティインシデントに移動します。
2. **[IoC を表示]** 関連リストグループの [サイティング検索の詳細] タブを選択し、サイティング検索のリストを表示します。

> **注:**
> このデータは トラステッドセキュリティサークル と共有できます。

サイティング検索の詳細

詳細	説明
観測事象	クエリで検索されるすべての観測事象のリスト。
観測可能タイプ	
内部発生回数	すべての検索の内部発生回数の数。
外部発生回数	すべての検索の外部発生回数の数(脅威共有から受信)。
サイティング検索	サイティング検索の識別子。
更新日時	最後の変更の日時。

[Security Operations Integration - 脅威のルックアップ] 機能

[脅威のルックアップ] 機能は、脅威インテリジェンスのルックアップを実行し、1 つ以上の観測事象が既知のセキュリティ脅威に関連するかどうかを判断します。

[脅威のルックアップ] 機能にはワークフロー Security Operations Integration - 脅威のルックアップフロー があります。機能ワークフローが実行されると、アクティブ化された実装の追加のワークフローが実行されます。選択した観測事象に使用するルックアップの実装を指定して実行するか、すべての実装を使用してルックアップを実行することができます。

> **注:**
> 利用可能な実装がない場合、機能アクションは製品メニューに表示されません。

Security Operations Integration - 脅威のルックアップフロー

[Security Operations Integration - 脅威のルックアップ] 機能フローは、利用可能な脅威のルックアップ実装にアクセスし、それぞれに関連付けられた実装フローを実行して、選択した観測事象の脅威のルックアップを実行します。

始める前に
必要なロール：sn_ti.write

このタスクについて
このフローは次の方法でトリガーできます。

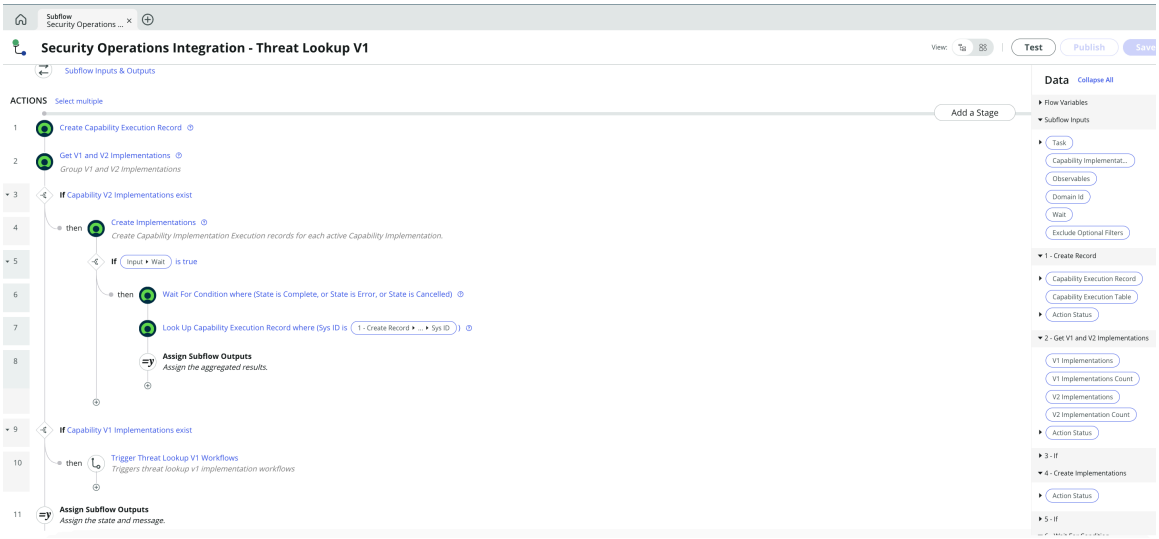
- [観測事象] リストから 1 つ以上の観測事象を選択し、[選択した行のアクション...] 選択リストから [脅威のルックアップを実行] を選択します。
- 観測事象レコードを開き、[脅威のルックアップを実行] 関連リンクをクリックします。
- セキュリティインシデントの [観測事象] 関連リストからトリガーします。

いずれの方法でも、選択した観測事象を拡張するために使用するルックアップ実装を指定できます。関連する実装フローが実行され、ルックアップが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威情報ルックアップ



ここでは、このフローに固有のアクションについて説明します。他のアクションの詳細については、「 一般的な Security Operations 統合フローとオーケストレーションアクティビティ」を参照してください。

フロープロセスアクションには次のものが含まれます。

- [サポートされているセキュリティ機能を取得] アクション
- 機能トラッキング - 未実施アクションなし

フローの実行順序を変更する

統合機能の実装では、実行するフローを指定します。ベースシステムでは、フローは実装で指定された順序で順番に実行されます。順序は必要に応じて変更することができます。

始める前に

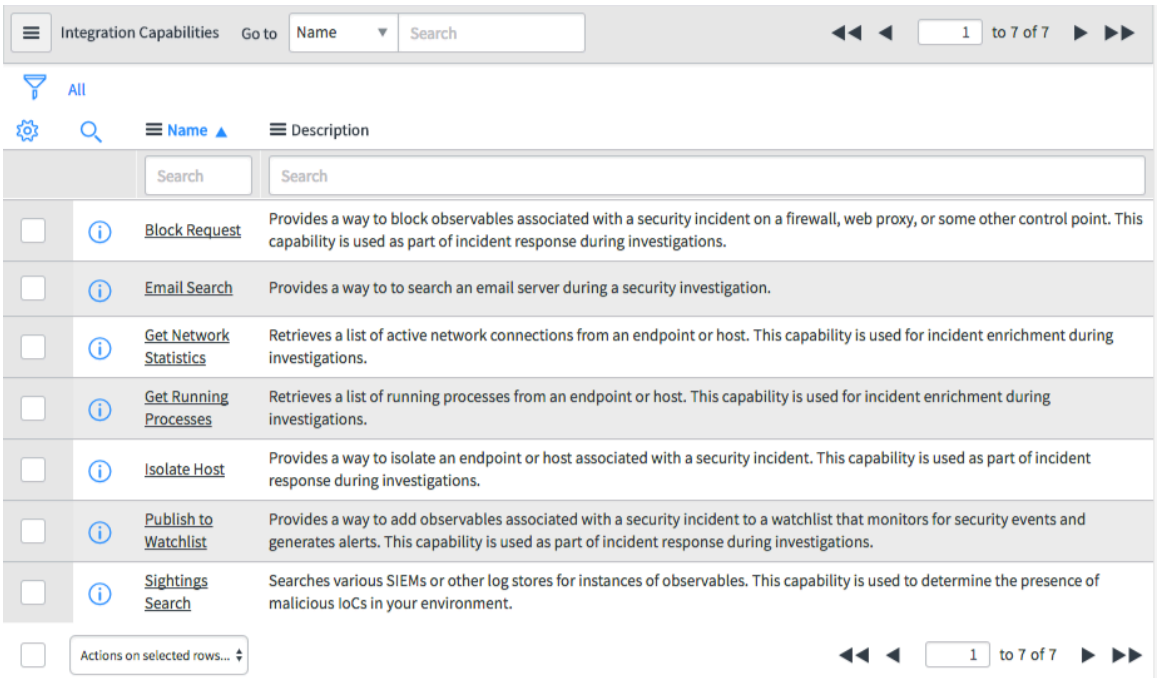
必要なロール：sn_sec_cmn.write

自動翻訳

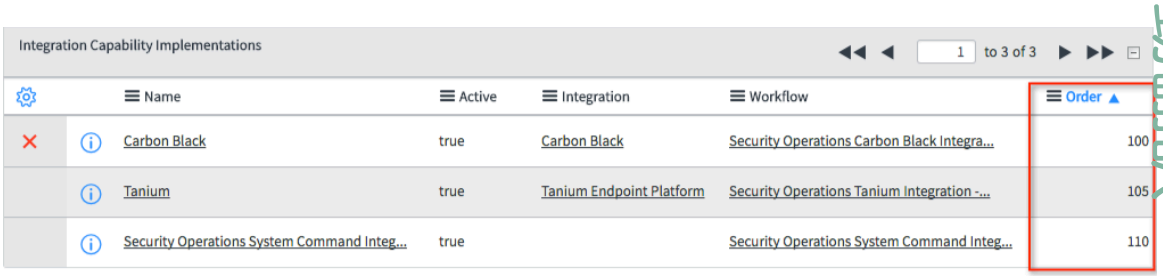
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

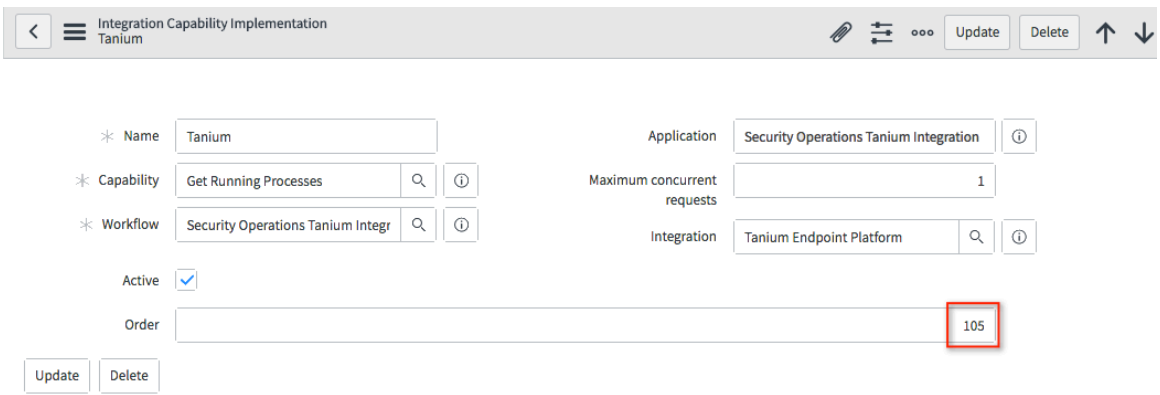
1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > 統合 > 統合機能.



2. 実行順序を変更する統合機能を選択します。



3. 変更する実装を選択します。



4. [順序] を大きい数値または小さい数値に変更します。
数値が小さいほど、実行の優先度が高くなります。

5. **[Submit]** をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

一般的な Security Operations 統合フローとオーケストレーションアクティビティ

サードパーティ統合に関連するフローの多くには、同じアクティビティが含まれています。たとえば、処理の開始と完了のアクティビティです。

[実行トラッキング:フローを開始] アクション

[実行トラッキング:開始] フローアクションは、観測事象で動作する セキュリティオペレーション 統合フローの監査プロセスを開始します。

[実行トラッキング:フローを開始] アクションを任意のフローで使用して、監査でフローの進行状況の記録を開始できます。

結果

このフローアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	監査レコードが作成されます。

入力変数

フローアクションの初期動作が、入力変数によって決まります。

変数	説明
capabilityId	実行されている統合機能のシステム識別子。
isImpl	統合機能フローまたは統合機能実装フローのどちらに対して監査を実行するかを指定するフラグ。可能な値： • false - サイティング検索などの抽象統合機能フローの監査を示します。(デフォルト) • true - 統合機能の実装フローの監査を示します。たとえば、Splunk や Elasticsearch です。
taskId	フローに関連付けられたタスクのシステム識別子。
observableList	目的のアクションを実行する 1 つ以上の観測事象 SysID。 フロー入力として使用されます。
flowContextId	関連付けられたフローコンテキストレコードのシステム識別子。システムによって提供されます。
flowName	フローの名前。システムによって提供されます。
parentCapabilityExcutionId	実装フローを開始した監査レコードのシステム識別子。Splunk、Elasticsearch、VirusTotal などの統合機能の実装フローのみに必要です。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数

変数	説明
capabilityExecutionId	監査レコードのシステム識別子。

- [サポートされているセキュリティ機能を取得] アクション
- 機能トラッキング - 未実施アクションなし

機能トラッキング:フローアクションを完了

[機能トラッキング:完了] フローアクションは、フローが完了したときに監査レコードを更新します。

[機能トラッキング:完了] フローアクションを任意のフローで使用して、フローの完了を記録できます。

注:
[パラレルランチャー] コアフローアクションからの戻り値アレイには、実行されたすべての統合フローの結果のアレイが含まれており、実行トラッキングの正常な完了を促します。

結果

このフローアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	監査レコードのステータスが [完了] に更新されます。

入力変数

フローアクションの初期動作が、入力変数によって決まります。

変数	説明
capabilityExecutionId	監査レコードのシステム識別子。このフィールドは、[監査の開始 (Begin auditing)] アクティビティの出力です。
flowName	フローの名前。システムによって提供されます。
message	完了メッセージ

出力変数

出力変数はありません。

機能トラッキング:失敗フローアクション

[機能トラッキング:失敗] フローアクションは、監査レコードに失敗を記録します。

[機能トラッキング - 失敗] フローアクションを任意のフローで使用して、失敗条件を記録できます。

結果

このフローアクションの考えられる結果は次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

結果

結果	説明
成功	監査レコードのステータスは [エラー] に設定され、エラーを示すメッセージが記録されます。

入力変数

フローアクションの初期動作が、入力変数によって決まります。

変数	説明
capabilityExecutionId	監査レコードのシステム識別子。これは、[監査の開始 (Begin auditing)] アクティビティの出力です。
errorMessage	失敗の理由を示すメッセージ。
flowName	フローの名前。システムによって提供されます。

出力変数

出力変数はありません。

[機能 - CI の特定] アクティビティ

[機能 - CI の決定] ワークフローアクティビティは、ワークフローに含める構成アイテム (CI) を決定します。

[機能 - CI の決定] アクティビティを任意のワークフローで使用して、ワークフローに含める CI を決定できます。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	構成アイテムが見つかりました。
失敗	CI が見つかりませんでした。その他のエラー情報は、アクティビティ出力エラーで確認できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

変数	説明
task_sys_id	タスク識別子 (セキュリティインシデントを CI にマッピング)
cis_affected	構成アイテム

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
cis_affected	フィルター済み CI
task_sys_id	タスク識別子 (セキュリティインシデントを CI にマッピング)

拡張データレコードフローアクションを作成

[拡張データレコードを作成] フローアクションは、フローで使用する拡張レコードを作成または更新します。

[拡張データレコードを作成] フローアクションを任意のフローで使用して、フロー内の拡張レコードを更新できます。

結果

このフローアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	拡張レコードが更新されました。
失敗	拡張レコードは更新されませんでした。その他のエラー情報は、フローアクション出力エラーで確認できます。

自動翻訳

入力変数

フローアクションの初期動作が、入力変数によって決まります。

変数	説明
task_id	タスク識別子。
コンテンツ	生のコンテンツ (実行中のプロセスデータ)
enrichment_mapping_id	拡張マッピング識別子
ci_id	構成アイテムの識別子。
reference_value	未使用

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数

変数	説明
result	enrichmentUtils スクリプトを使用して、GlideRecords が作成されました。

[構成アイテム **FQDN** を取得] フローアクション

application **Security Common** オーケストレーション > 構成アイテム **(CI)** の **FQDN** を取得 フローアクションは、構成アイテムの完全修飾ドメイン名 (FQDN) を取得します。このフローアクションにより、調査と修復のプロセスを迅速化できます。

[構成アイテム FQDN を取得] フローアクションを任意のフローで使用して、構成アイテムの完全修飾ドメイン名 (FQDN) を取得できます。

入力変数

フローアクションの初期動作が、入力変数によって決まります。

入力変数

変数	説明
cmdb_ci.id [文字列]	構成アイテムレコードのシステム識別子 (sys_id)。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。

出力変数

変数	説明
fqdn [文字列]	構成アイテムの完全修飾ドメイン名 (FQDN)。

その他の注意事項

構成アイテムの [fqdn] フィールドに値を入力する必要があります。

[観測事象の決定] アクティビティ

[観測事象の決定] ワークフローアクティビティは、ワークフローに含める観測事象を決定します。

[観測事象の決定] アクティビティを任意のワークフローで使用して、ワークフローに含める観測事象を決定できます。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	観測事象が見つかりました。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

結果 (続く)

結果	説明
失敗	観測事象が見つかりませんでした。その他のエラー情報は、アクティビティ出力エラーで確認できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

変数	説明
task_sys_id	タスク識別子 (セキュリティインシデントを観測事象にマッピング)
観測事象	IP アドレス、ハッシュ、URL、ドメイン名。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
観測事象	フィルター済み観測事象

[サポートされているセキュリティ機能を取得] アクション

[サポートされている機能を取得] フローアクションは、要求された機能をサポートするアクティブな統合の名前と数を取得します。

[サポートされている機能を取得] アクションを任意のフローで使用して、サポートされている機能を特定できます。

結果

このアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	機能をサポートする統合が見つかりました。
失敗	機能をサポートするアクティブな統合を検索中にエラーが発生しました。その他のエラー情報は、アクション出力エラーで確認できます。

入力変数

アクションの初期動作が、入力変数によって決まります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

変数	説明
capabilityName	機能の名前。
taskId	フローに関連付けられたタスクのシステム識別子。
ドメイン ID	フローに関連付けられたドメインのシステム識別子。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。

出力変数

変数	説明
supportedCapabilities	機能をサポートする統合のリスト。
capabilityCount	機能をサポートする統合の数。

機能トラッキング - 未実施アクションなし

[機能トラッキング - 未実施] フローアクションは、統合機能の実装が見つからない場合にエラーレコードを作成します。

「機能トラッキング - 未実施」アクションを任意の抽象統合機能フローで使用して、構成された機能実装が利用できない場合にエラー条件を処理できます。

結果

このアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	実行トラッキングレコードのステータスは [エラー] に設定され、エラーを示すメッセージが記録されます。

入力変数

アクションの初期動作が、入力変数によって決まります。

変数	説明
capabilityExecutionId	監査レコードのシステム識別子。実行トラッキングを開始するために使用されるアクションからの出力。
flowName	フローの名前。システムによって提供されます。

出力変数

出力変数はありません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンプライアンス検索アクションを作成

[コンプライアンス検索を作成] アクションは、定義された検索クエリを使用して、指定された Exchange サーバー内のメールのコンプライアンス検索を作成し、作成されたコンプライアンス検索の名前を返します。

入力変数

アクションの初期動作が、入力変数によって決まります。

変数	説明
search_query	すべてのメールボックスで Exchange Server のメールを検索するために使用される必須の検索クエリ。
Exchange の場所 (exchange Location)	定義された場所全体を検索するために使用される必須の場所フィールド。値は次のとおりです。 • すべて • 特定のメールボックスの名前
targetId	Exchange Server が配置されている必須のターゲットホスト識別子フィールド。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。

出力変数

変数	説明
response	作成されたコンプライアンス検索の名前。

終了条件

このアクションの可能な終了条件は次のとおりです。

終了条件

変数	説明
検索の作成に失敗しました (Search Creation Failed)	Exchange サーバーの例外により検索の作成に失敗したとき。
検索が正常に作成されました (Search Created Successfully)	検索の作成に成功したとき。
解析エラーのため検索の作成に失敗しました (Search Creation Failed due to a Parsing Error)	解析の問題で検索の作成に失敗したとき。
エラー	フローアクションで例外が発生した場合。

[CI から IP を取得] アクティビティ

このワークフローアクティビティは、構成アイテム (CI) に関連付けられた IPV4 アドレスを決定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[CI から IP を取得] アクティビティを任意のワークフローで使用して、CI の IPv4 アドレスを取得できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

入力変数

変数	説明
ci_sys_id [文字列]	構成アイテムのシステム識別子。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
ip_addr [文字列]	IPv4 アドレス。IP アドレスを特定できない場合、この値は空になります。

終了条件

このアクティビティの考えられる結果は次のとおりです。

条件

条件	説明
成功	IPv4 アドレスが返されました。
失敗	IPv4 アドレスを特定できませんでした。

netstat フローアクションを介してネットワーク統計情報を取得

[Security Common オーケストレーション - netstat でネットワーク統計情報を取得] フローアクションは、Windows ベースシステム上の影響を受けるリソースのネットワーク統計情報を取得します。このフローアクションにより、調査と修復のプロセスを迅速化できます。

[netstat を介してネットワーク統計情報を取得] フローアクションを任意のフローで使用して、Windows ベースのシステムからネットワーク統計情報を取得できます。マシンは、**-a** および **-o** パラメーターを含む **netstat** コマンドで照会されます。出力データを拡張するために、**get-process** コマンドも呼び出されます。

結果

このフローアクションの考えられる結果は次のとおりです。

結果

結果	説明
成功	ネットワーク統計情報が JSON 形式で取得されました。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

結果 (続く)

結果	説明
失敗	ネットワーク統計情報の取得中にエラーが発生しました。その他のエラー情報は、フローアクション出力エラーで確認できます。

入力変数

変数	説明
target [文字列]	ターゲットシステムの完全修飾ドメイン名 (FQDN) または IP アドレス。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
response [文字列]	ターゲットシステムで現在実行中のプロセスを表す JSON 文字列。 JSON データには次のものが含まれます。 pid プロセス識別子。 local _port ネットワークトランザクション用のローカルポート。 state TCP 接続のステータス。 注: UDP 接続の場合、このフィールドは null です。 local_address ローカルの完全修飾ドメイン名 (FQDN) または IP アドレス。 remote_address リモートの完全修飾ドメイン名 (FQDN) または IP アドレス。 protocol TCP または UDP。 remote_port ネットワークトランザクションのリモートポート。 path プロセスの実行可能ファイルのパス。 hash プロセスの実行可能ファイルのハッシュ値。ハッシュは、PowerShell V4 以降の場合は SHA-256 です。それ以外の場合、ハッシュは MD5 です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

制限

MID サーバーは PowerShell をサポートしている必要があります。

SHA-256 ハッシュには PowerShell V4 が必要です。

[WMI を介して実行中のプロセスを取得] アクティビティ

[実行中のプロセスを取得] ワークフローアクティビティは、Windows ベースシステムで構成アイテムの実行中のプロセスを取得します。このアクティビティにより、調査と修復のプロセスを迅速化できます。

[WMI を介して実行中のプロセスを取得] ワークフローアクティビティを任意のワークフローで使用して、Windows ベースシステムで実行中のプロセスを取得できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

入力変数

変数	説明
target [文字列]	ターゲットシステムの完全修飾ドメイン名 (FQDN) または IP アドレス。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
response [文字列]	ターゲットシステムで現在実行中のプロセスを表す JSON 文字列。 JSON データには次のものが含まれます。 pid プロセス識別子。 name プロセスの名前 また、利用可能な場合： オーナー プロセスオーナーの名前。 owner_sid プロセスオーナーのシステム識別子。 owner_domain プロセスオーナーのドメイン。 path プロセスの実行可能ファイルのパス。 hash

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数 (続く)

変数	説明
	プロセスの実行可能ファイルのハッシュ値。ハッシュは、PowerShell V4 以降の場合は SHA-256 です。それ以外の場合、ハッシュは MD5 です。

制限

MID サーバーは **PowerShell** をサポートしている必要があります。

SHA-256 ハッシュには PowerShell V4 が必要です。

コンプライアンス検索ステータスのチェックアクション

[コンプライアンス検索ステータスのチェック(Check Compliance Search Status)] アクションは、Exchange サーバーで作成されたコンプライアンス検索のステータスを確認し、ステータスが完了の場合は、コンプライアンス検索で見つかったメール検索に関する情報を返します。

入力変数

アクションの初期動作が、入力変数によって決まります。

変数	説明
targetId	Exchange Server が配置されている必須のターゲットホスト識別子フィールド。
searchName	Exchange サーバーで作成されたコンプライアンス検索の必須名。

出力変数

出力変数には、後続のアクションで使用できるデータが含まれています。

出力変数

変数	説明
response	コンプライアンス検索のステータスと、コンプライアンス検索で Exchange サーバーで見つかったメールの数が含まれます。

終了条件

このアクションの可能な終了条件は次のとおりです。

終了条件

変数	説明
検索中 (Search In Progress)	コンプライアンス検索のステータスが進行中のとき。
検索完了 - 脅威メールが見つかりません (Search Complete - No Threat Emails Found)	コンプライアンス検索のステータスが完了で、コンプライアンス検索の一部としてメールが検出されていないとき。
検索完了 - 脅威メールが見つかりました (Search Complete - Threat Emails Found)	コンプライアンス検索のステータスが完了で、コンプライアンス検索の一部としてメールが検出されているとき。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

終了条件 (続く)

変数	説明
ステータスの確認中にエラーが発生しました (Error Checking Status)	Exchange サーバーの例外によりステータスのチェックに失敗した場合。
エラー	フローアクションで例外が発生した場合。

[タスク作業メモを更新] アクティビティ

[Security Common オーケストレーション **-** タスク作業メモを更新] ワークフローアクティビティは、タスクレコードの [アクティビティ] セクション (作業メモ) を更新します。これは情報のログ記録に便利です。

[タスク作業メモを更新] アクティビティを任意のワークフローで使用して、任意のタスクレコードの作業メモを更新できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

入力変数

変数	説明
task_id [文字列]	タスクレコードのシステム識別子 (sys_id)。
content [文字列]	タスクの作業メモに書き込まれるデータ。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
result [文字列]	更新が成功したかどうかを示します。

[セキュリティインシデントに対するルックアップ情報をロールアップ] アクティビティ

[セキュリティインシデントに対するルックアップ情報をロールアップ] アクティビティは任意のワークフローで使用が可能で、脅威のルックアップから情報をコレクションし、タスク作業メモにコンテンツのサマリーと元のセキュリティインシデントの ID を出力できます。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	ルックアップレポートのサマリーがセキュリティインシデントにロールアップされました。
失敗	元のタスクとルックアップサマリーレポートが空です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

入力変数

変数	説明
scanID[文字列]	ルックアップ識別子

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
sild[文字列]	セキュリティインシデント識別子
response [文字列]	ルックアップ結果のサマリー (IoC 値、結果、障害の原因、ルックアップ参照など)。

[ルックアップ結果によるセキュリティインシデントの更新 **(Update security incident with lookup results)**] ワークフロー

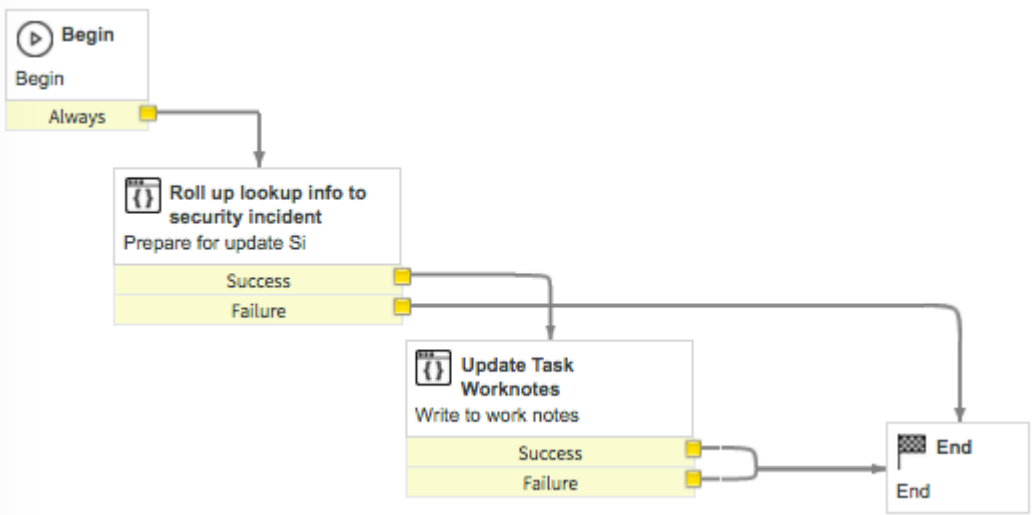
[ルックアップ結果によるセキュリティインシデントの更新 **(Update security incident with lookup results)**] ワークフローでは、ルックアップ結果で既存のセキュリティインシデントを更新します。

始める前に
必要なロール：sn_si.basic

このタスクについて
このワークフローは、[結果] フィールドが [失敗] に変わるタイミングを監視するルックアップテーブルのビジネスルールによってトリガーされます。

ワークフロープロセスアクティビティには次のものが含まれます。

- [セキュリティインシデントに対するルックアップ情報をロールアップ] アクティビティ
- [タスク作業メモを更新] アクティビティ



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[許可リストに追加された観測事象をフィルター] アクティビティ

[許可リストに追加された観測事象をフィルター] ワークフローアクティビティは、無視できる観測事象を観測事象のリストから削除します。このアクティビティにより、調査と修復のプロセスを迅速化できます。

[許可リストに登録された観測事象をフィルター] アクティビティを任意のワークフローで使用して、アクションを実行する前に観測事象をフィルタリングできます。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	フィルターリストが作成されました。
失敗	観測事象をフィルタリング中にエラーが発生しました。その他のエラー情報は、アクティビティ出力エラーで確認できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

変数	説明
観測事象	利用可能な観測事象のリスト。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
filteredObservables	フィルター済み観測事象。

[コンテンツを添付ファイルとしてレコードに書き込み] アクティビティ

このアクティビティは、入力から渡されたコンテンツを書き込み、指定された添付ファイルを所定のレコードに作成します。

[コンテンツを添付ファイルとしてレコードに書き込み] アクティビティを任意のワークフローで使用して、コンテンツを作成してレコードに添付できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

入力変数

変数	説明
tablename [文字列]	レコードのテーブル名。この入力フィールドは必須です。
sysid [文字列]	タスクレコードのシステム識別子 (sys_id)。この入力フィールドは必須です。
payload	添付ファイルとして書き込まれるプレーンテキストコンテンツ。この入力フィールドは必須です。
ファイル名	添付ファイル名。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

出力変数

変数	説明
result [文字列]	更新が成功したかどうかを示します。

[CI から IP を取得] アクティビティ

[CI から IP を取得] フローアクティビティは、フローで使用する IP アドレスを構成アイテム (CI) から収集します。

[CI から IP を取得] アクティビティを任意のフローで使用して、フローで使用する構成アイテム (CI) の IP アドレスを収集できます。

結果

このアクティビティの考えられる結果は次のとおりです。

結果

結果	説明
成功	IP アドレスが見つかりました。
失敗	IP アドレスが見つかりませんでした。その他のエラー情報は、アクティビティ出力エラーで確認できます。

入力変数

アクティビティの初期動作が、入力変数によって決まります。

変数	説明
ci_sys_id	構成アイテムの識別子。

出力変数

出力変数には、後続のアクティビティで使用できるデータが含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

出力変数

変数	説明
ip_addr	IP アドレス。

セキュリティオペレーション ワークフロートリガー

セキュリティオペレーション ワークフロートリガーには、テーブルの条件が含まれています。条件が満たされると、ワークフロートリガーレコードに添付されたすべてのワークフローが実行されます。

セキュリティオペレーション ワークフロートリガーの作成

テーブルの条件が含まれるワークフロートリガーを作成します。

始める前に
セキュリティオペレーション には、ベースシステムに複数のワークフロートリガーが含まれています。

アクティブなセキュリティインシデントの構成アイテムの変更

統合を使用して、構成アイテムの変更に応じて CI 関連データを拡張します。

脆弱性グループの再スキャン

グループをクローズ/無視するときに 脆弱性のスキャンワークフロー を使用して、脆弱性グループを再スキャンします。

脆弱性一致アイテムの再スキャン

アイテムをクローズ/無視するときに 脆弱性一致アイテムのスキャンワークフロー を使用して、脆弱性一致アイテムを再スキャンします。

必要なロール：

- 読み込み：sn_sec_cmn.read
- 作成または更新：sn_sec_cmn.write
- 削除：sn_sec_cmn.admin

手順

1. 次のように移動する。 **All** (すべて) > セキュリティオペレーション > ユーティリティ > ワークフロートリガー.
2. [**New**] をクリックします。
3. 必要に応じて、フォームのフィールドに入力します。

ワークフロートリガー

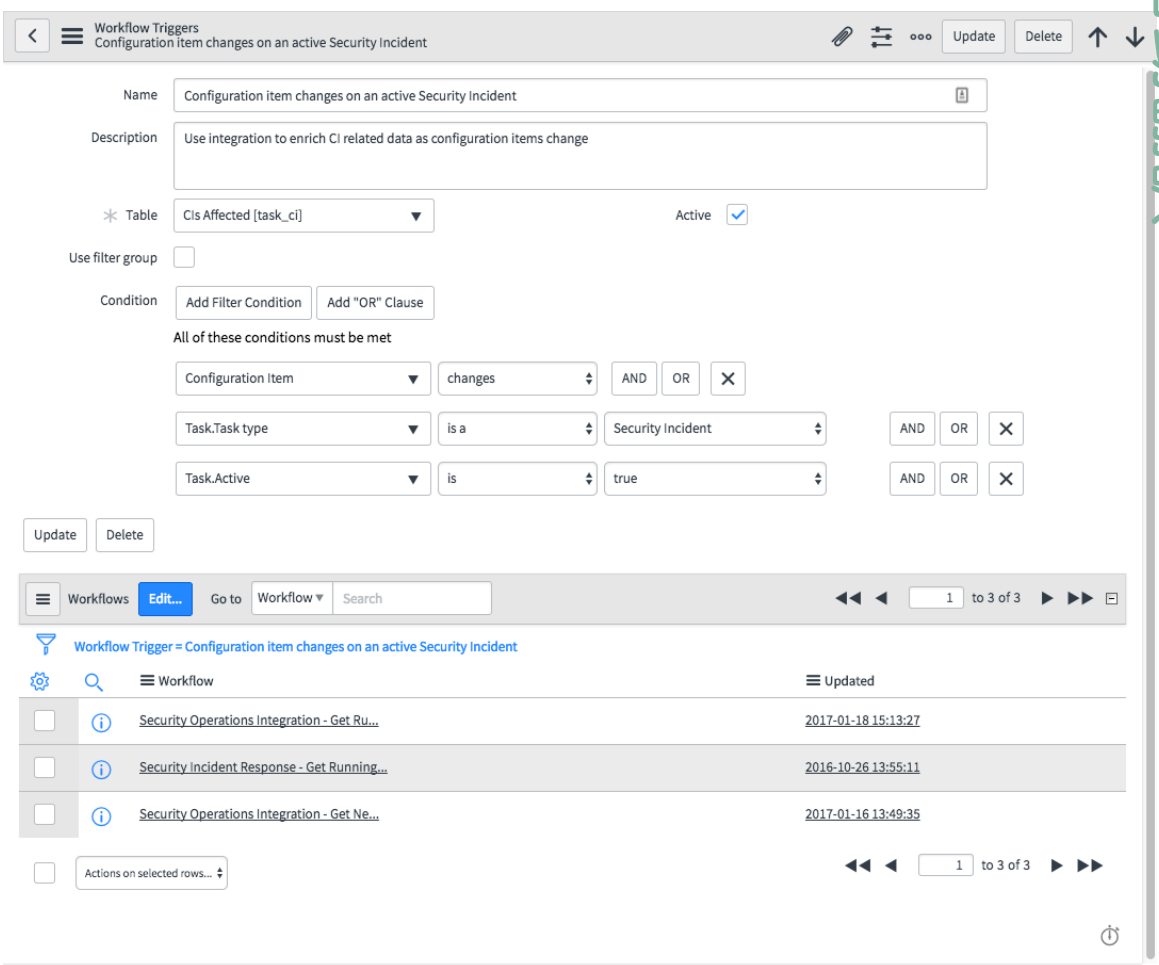
フィールド	説明
名前	ワークフロートリガーの名前。
説明	ワークフロートリガーの説明を入力します。
テーブル	ワークフロートリガーを含むテーブル。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	[フィルターグループを使用] チェックボックスをオンにしてフィルターグループを選択した場合、このフィールドは、選択したフィルターグループに関連付けられたテーブルにデフォルトで設定されます。
条件	次を使用： 条件ビルダー で、ワークフロートリガーの基準を定義します。 [フィルターグループを使用] チェックボックスをオンにしてフィルターグループを選択した場合、[条件] フィールドは表示されません。
有効	このワークフロートリガーをアクティブ化するには、このチェックボックスをオンにします。
フィルターグループを使用	事前定義フィルターグループを使用するか、または新しいフィルターグループを作成してワークフロートリガー基準を定義する場合は、このチェックボックスをオンにします。
フィルターグループ	ワークフロートリガーの定義に使用するフィルターグループを選択します。 このフィールドは、[フィルターグループを使用] チェックボックスが選択されている場合にのみ表示されます。

4. 入力が完了したら、フォームヘッダーを右クリックし、[保存] を選択します。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[ワークフロー] タブが表示されます。すべてのフィルター条件またはフィルターグループ条件が満たされたときに実行されるワークフローが含まれています。

5. ワークフローを追加するには、次の手順を実行します。
   a. [ワークフロー] タブで、[編集] をクリックします。
   b. 必要に応じて条件ビルダーを使用して選択するワークフローを見つけるか、スラッシュバケットを使用してワークフローを選択し、ワークフローリストに移動します。
   c. [保存] をクリックします。
   選択したワークフローが追加されます。
6. [更新] をクリックします。

Security Operations オーケストレーション

ユーザーは、セキュリティオペレーションオーケストレーション のアクティビティパックとワークフローを使用して、Windows または UNIX ベースのシステムと環境からデータを取得して操作できます。

セキュリティオペレーションオーケストレーション では、手動プロセスをなくして、インシデントを修正するためのコンテキスト情報を取得することで、時間を節約します。セキュリティオペレーション 製品には、各プラグインに付属しアクティブ化されている標準のアクティビティパックとワークフローがあります。

標準オファリング セキュリティオペレーション 製品では利用できない追加のオーケストレーションアクティビティを作成してアクセスするには、フルオーケストレーションライセンスを購入します。

- セキュリティインシデントレスポンスオーケストレーション ワークフロー：
  - セキュリティインシデントレスポンス - ネットワーク統計情報を取得フロー
  - Security Operations System Command Integration - 実行中のプロセスを取得フロー
  - IoC 変更のためのルックアップ要求の作成 (Create Lookup Request for IoC Changes) ワークフロー
  - Security Operations Integration - メールの検索と削除フロー
- 脅威インテリジェンスオーケストレーション ワークフロー：
  - [脅威インテリジェンス - IoC ルックアップを実行 (Run IoC Lookup)] ワークフロー
  - [ルックアップ結果によるセキュリティインシデントの更新 (Update security incident with lookup results)] ワークフロー
- 脆弱性対応オーケストレーション ワークフロー：
  - 脆弱性のスキャンワークフロー
  - 脆弱性一致アイテムのスキャンワークフロー

[store-future: BEGIN review]

セキュリティオペレーション のシナリオと例

ServiceNow® セキュリティオペレーション 製品については、いくつかのシナリオを学ぶことで簡単に理解できます。これらのシナリオは、製品で使用できる機能を表しています。シナリオは、これらの製品の機能と柔軟性についての理解を深めることを目的としています。

[End]
[store-future: BEGIN review]

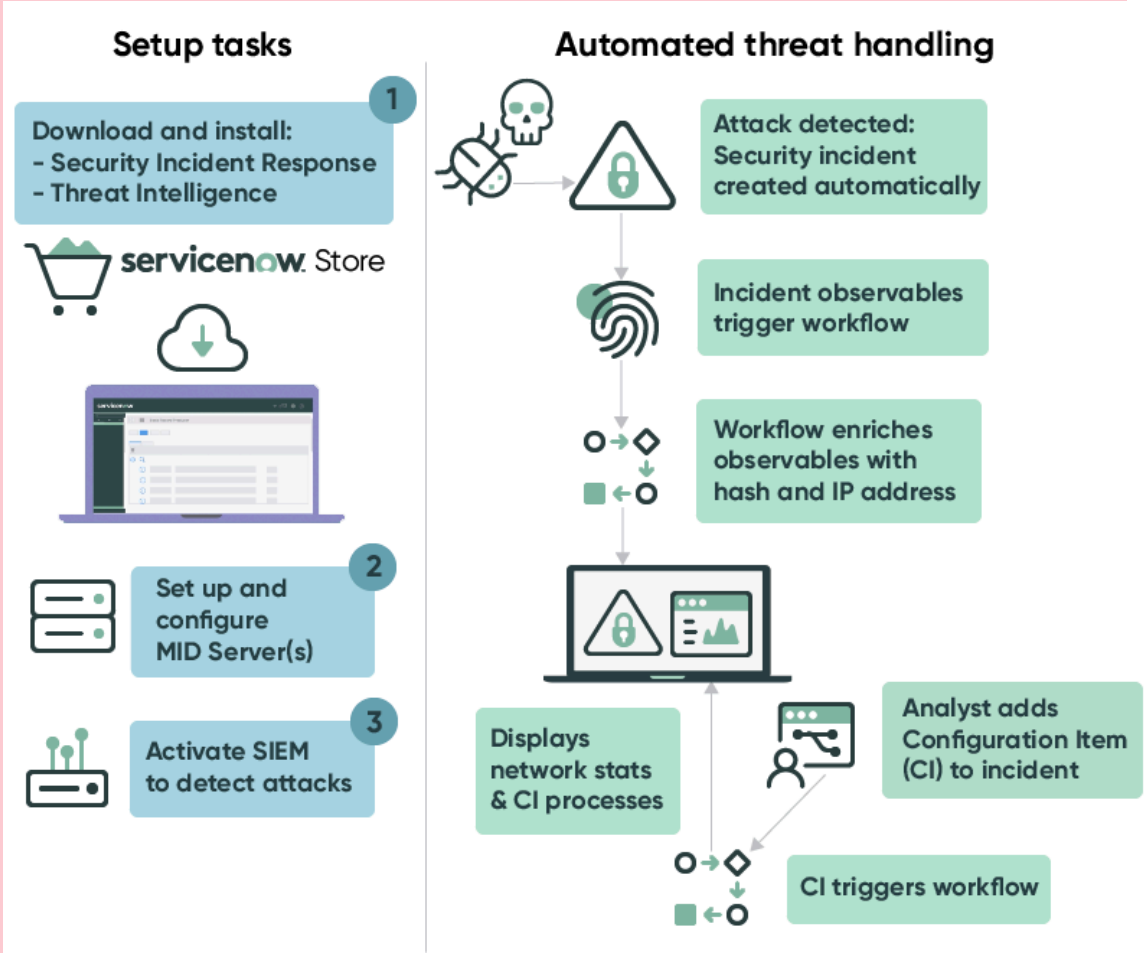
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動化を使用した脅威の分析時間の短縮

セキュリティインシデントのトリアージと分析は、脅威への対応プロセスから誤検出を排除し、セキュリティ脅威を識別、封じ込め、除去するのに最善の方法を決定するために必要なステップです。

トリアージには、脅威の原因と影響を手作業で探し出すステップを含めることができます。多くのステップを自動化することで、脅威の分析と封じ込めに必要な時間と労力を大幅に削減できます。ServiceNow セキュリティオペレーション ソフトウェアで自動化をセットアップすると、さまざまなタイプの自動化を実行できます。たとえば、観測事象がセキュリティインシデントに追加されたときに、観測事象データを自動的に拡張できます。あるいは、CMDB 内の CI がセキュリティインシデントに追加されたときに、実行中のプロセスを表示したり、ネットワーク統計情報を取得したりすることができます。以下に示すプロセスにより、脅威分析の貴重な時間を節約できます。



このシナリオでは、会社が脅威の検出に使用しているセキュリティ情報およびイベント管理 (SIEM) ツールによって悪意のあるファイルが検出されました。セキュリティオペレーション と SIEM の統合により、遭遇した脅威のタイプに基づいてセキュリティインシデントが自動的に作成されます。悪意のあるファイルに観測事象がすでに含まれている場合、またはセキュリティアナリストが事後に期限切れでない新しい観測事象を追加した場合は、観測事象レコードを拡張するワークフローが自動的にトリガーされます。ワークフローによって観測事象がスキャンされ、ファイルの送信者のハッシュと IP アドレスがセキュリティインシデントに追加されます。

トリアージ中に、アナリストは、会社の CMDB に含まれる構成アイテム (CI) が侵入の被害を受けていることを確認できる場合があります。その場合、アナリストは CI をセキュリティインシデントに追加します。セキュリティインシデントが保存されると、他の 2 つのワークフローが実行され、CI に関連するネットワーク統計情報と実行中のプロセスがセキュリティインシデントに即座に追加されます。

[End]

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威インテリジェンス 自動化の準備

脅威インテリジェンス 自動化を脅威への対応プロセスで使用する前に、いくつかの予備セットアップ手順を完了する必要があります。セットアップが完了すると、ワークフローはユーザーの支援がほとんどまたはまったくない状態で自動的に実行されます。

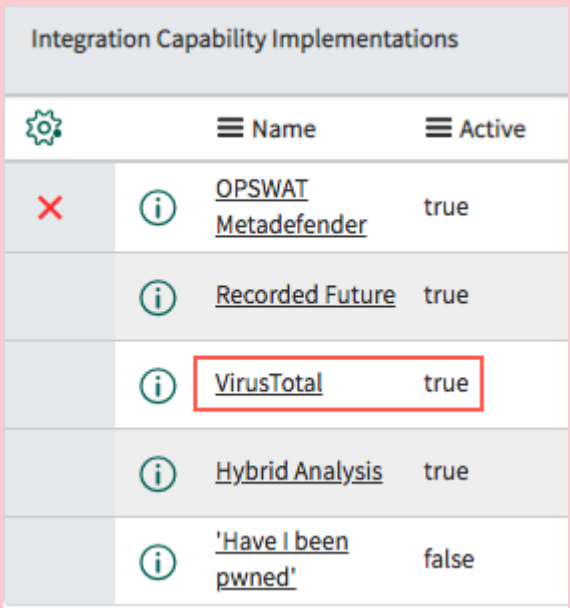
始める前に
必要なロール：admin

手順

1. をダウンロードする セキュリティインシデントレスポンス AND 脅威インテリジェンス アプリケーションから ServiceNow Store.
2. 1 つ以上の MID サーバーをインストールし、それぞれのサービス認証情報を設定します。
3. MID サーバーが稼働している場合は、使用している統合機能の実装 (VirusTotal など) が脅威のルックアップ機能で有効であることを確認します。
   脅威のルックアップ機能は、脅威情報ルックアップを実行し、1 つ以上の観測事象が既知のセキュリティ上の脅威に関連するかどうかを判断します。

   a. 次のように移動する。 セキュリティオペレーション > 統合 > 統合機能.

   b. [脅威のルックアップ] をクリックし、[統合機能の実装] 関連リストまで下にスクロールします。



   c. 使用する実装を見つけて、[アクティブ] 列に **[true]** が表示されていることを確認します。

   d. 実装が有効になっていない場合は、実装の [名前] をクリックし、[アクティブ] チェックボックスをオンにして、[更新] をクリックします。

観測事象データを自動的に拡張

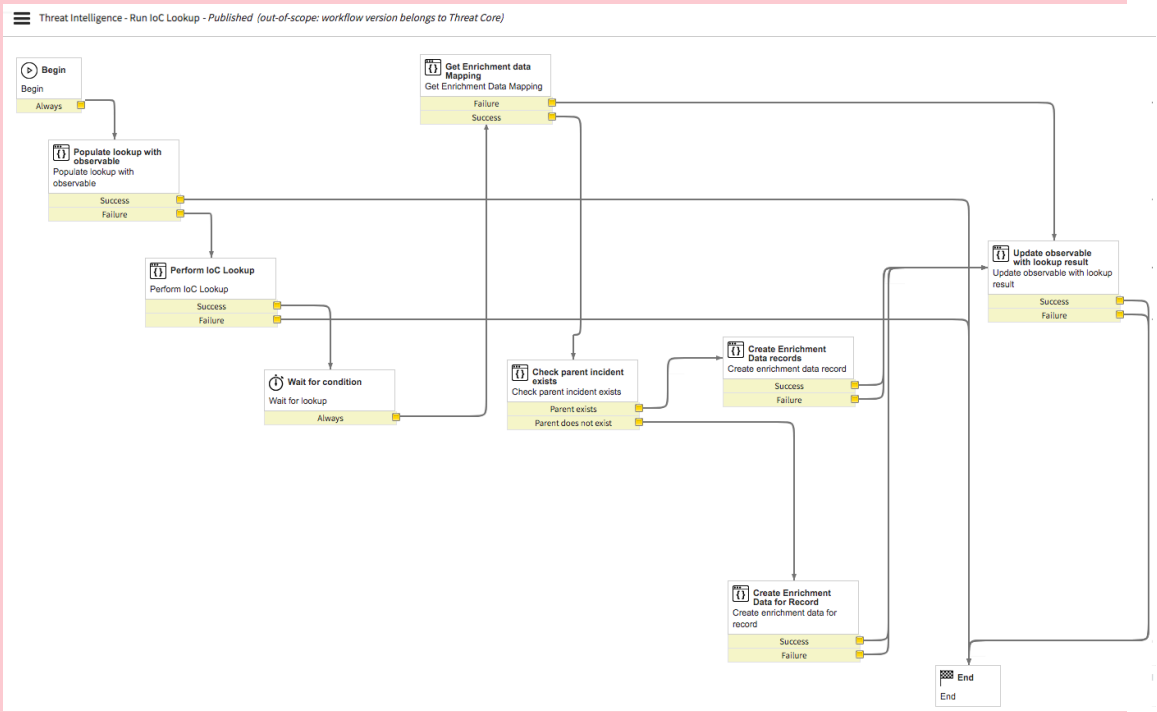
脅威インテリジェンス 自動化の準備を行い、新規または期限切れでないセキュリティ侵害のインジケーター (IoC) をセキュリティインシデントに追加すると、[脅威インテリジェンス - IoC ルックアップを実行 (Run IoC Lookup)] ワークフローが自動的に実行されます。

このワークフローアクティビティは、ユーザーの介入なしで不審なファイルのハッシュや送信元 IP アドレスなどの情報を IoC から抽出します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

観測事象データを自動的に拡張



注:
セキュリティインシデントにすでに添付されている観測事象を 1 つ以上選択し、[選択した行のアクション] 選択リストから [脅威のルックアップを実行] を選択して、ルックアップを手動で実行することもできます。

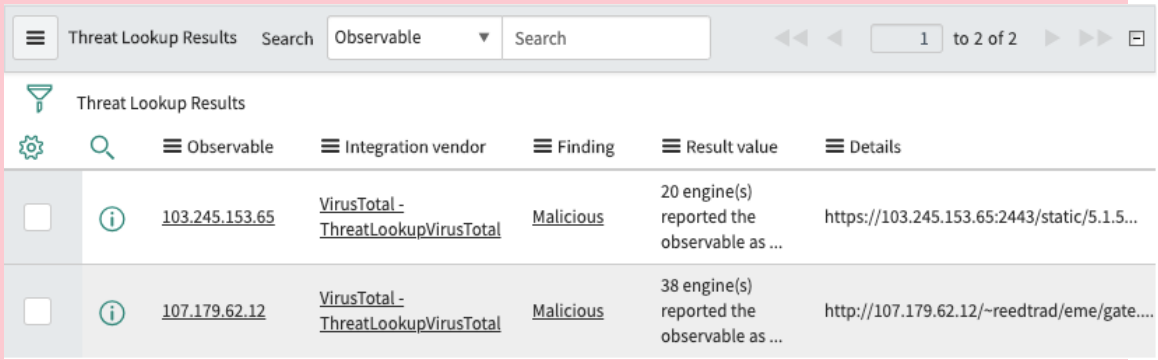
ワークフローは次のアクティビティを実行します。

1. [観測事象をルックアップに入力] アクティビティは、入力としてアクティビティに提供されたルックアップの値とタイプに一致するルックアップに対して、既存の観測事象の検索を試行します。
   a. 入力に一致する観測事象が見つかった場合、**[IoC ルックアップを実行 (Run IoC Lookup)]** アクティビティによって、レコードの ScanID でルックアップが実行されます。
   b. 観測事象が見つかり、期限切れになっていない場合、ルックアップは実行されず、セキュリティインシデントのルックアップ結果は、観測事象からの情報で更新されます。詳細については、「観測事象アクティビティをルックアップに入力する」を参照してください。
2. IoC ルックアップが実行されると、最初に次の 4 つのアクティビティが拡張データマップから情報を取得します。拡張データマッピングは、XML、JSON、またはプロパティファイルから ServiceNow レコードにデータを変換します。次に、親セキュリティインシデントが存在するかどうかを確認します。存在する場合、観測事象が作成され、拡張されます。存在しない場合は、既存の観測事象が拡張されます。詳細については、「[ルックアップ結果によって観測事象を更新] アクティビティ」を参照してください。
   - 拡張データマッピングの取得
   - 親インシデントの存在を確認
   - 拡張データレコードを作成
   - レコード用の拡張データを作成
3. データの拡張が完了すると、[ルックアップ結果によって観測事象を更新] アクティビティがセキュリティインシデント内の観測事象を更新し、[脅威のルックアップの結果] 関連リストに結果を書き込みます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

脅威のルックアップの結果



ネットワーク統計情報と実行中のプロセスの自動取得

CMDB にある完全修飾 Windows ドメイン名 (FQDM) を持つ構成アイテム (CI) をセキュリティインシデントに追加すると、追加のワークフローが実行され、ネットワーク統計情報と実行中のプロセスが提供されます。

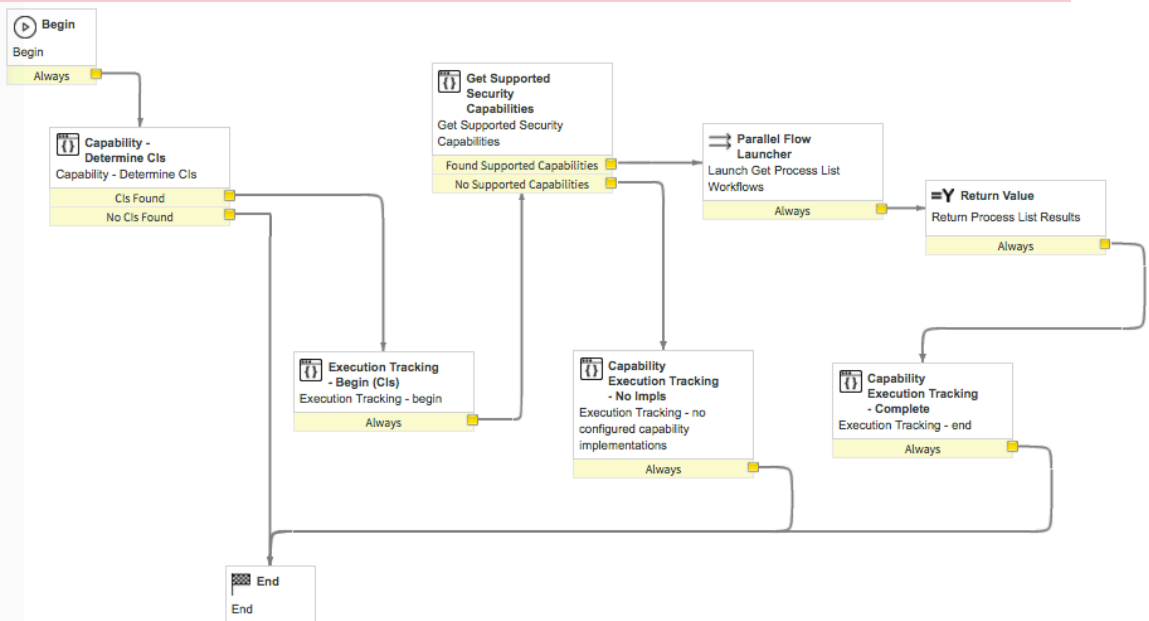
始める前に
必要なロール：admin

手順

1. Discovery モジュールを使用して、CMDB に Windows ドメイン名を入力します。

> **注:**
> ServiceNow ディスカバリー モジュールに登録しない場合は、CMDB を手動で入力するか、サードパーティのディスカバリータイプの製品を使用する必要があります。

2. CI をセキュリティインシデントに追加します。
   次の 2 つのワークフローが並行して実行されます。
   - Security Operations - 実行中のプロセスを取得フロー：このワークフローは、ホストから構成アイテム (CI) で実行中のプロセスのリストを取得します。Carbon Black などの統合を実行する場合や、Windows ベースのセキュリティインシデントを処理する場合に使用します。

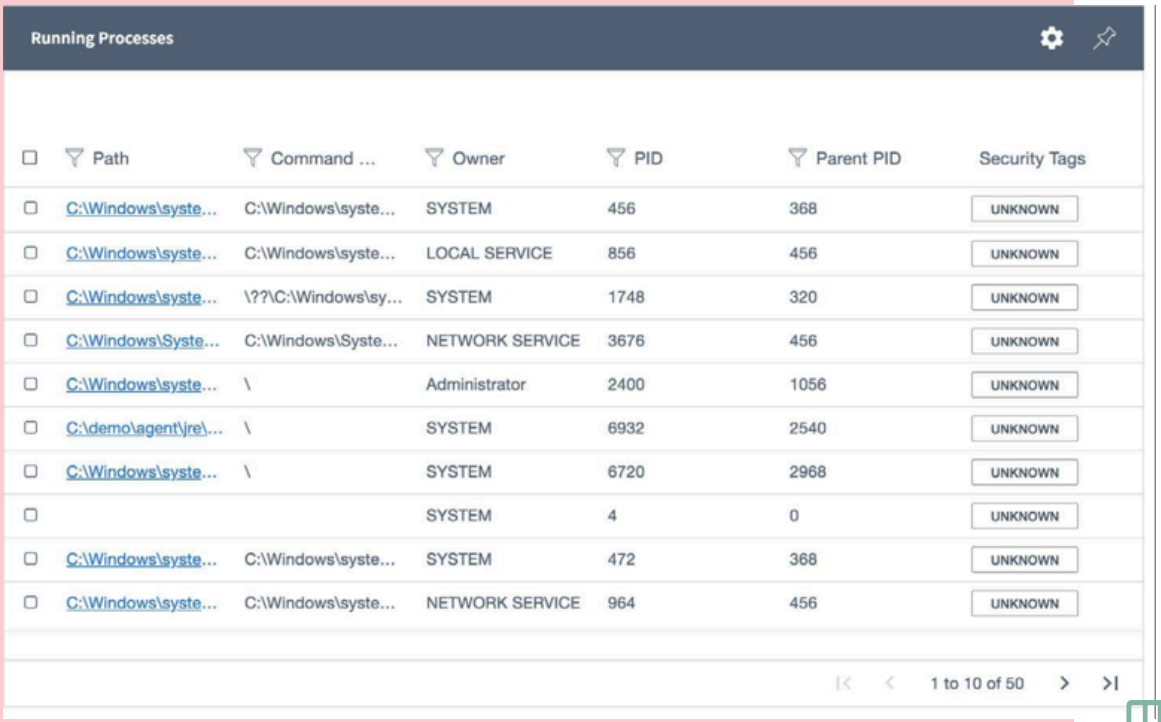


自動翻訳

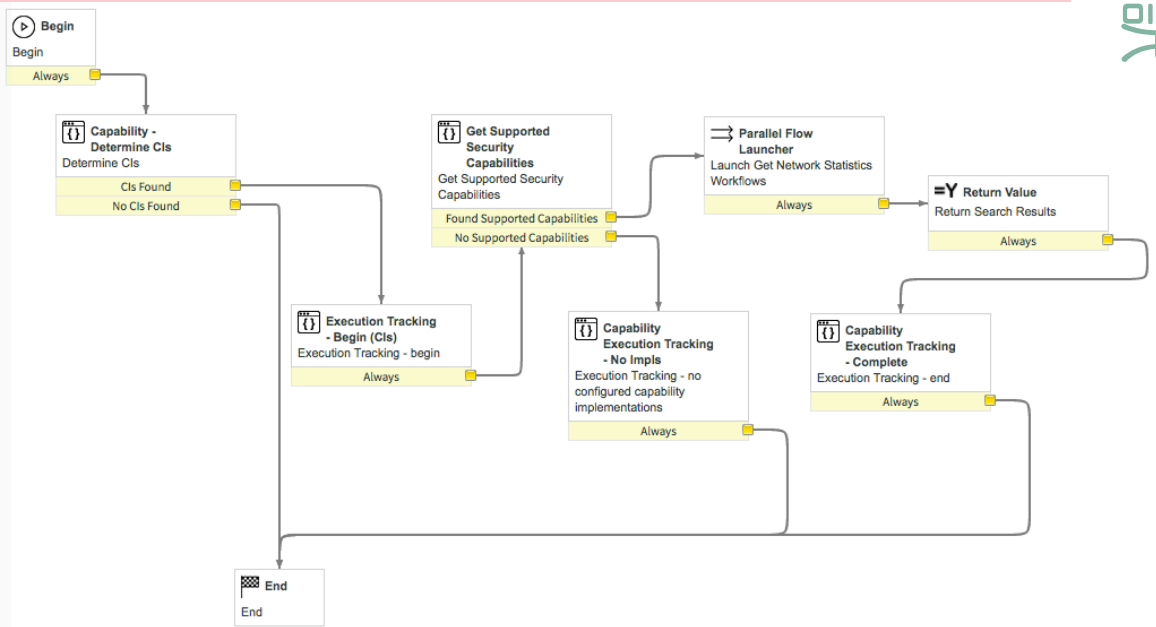
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ワークフローが完了すると、実行中のプロセスがセキュリティインシデントの [実行中のプロセス] 関連リストに表示されます。

実行中のプロセス



- [Security Operations Integrations - ネットワーク統計情報を取得] フロー：このワークフローでは、ホストまたはエンドポイントから、アクティブなネットワーク接続のリストを取得します。時期



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ワークフローが完了すると、セキュリティインシデントの [ネットワーク統計] 関連リストにネットワーク統計情報が表示されます。

ネットワーク統計

Workflow Activity History Search Started Search 1 to 8 of 8

Context = Security Operations Integration - Get Network Statistics

Started	Activity	State	Ended	Result	Fault Description
2019-05-13 13:28:38	Execution Tracking - begin	Finished	2019-05-13 13:28:38		
2019-05-13 13:28:38	Get Supported Security Capabilities	Finished	2019-05-13 13:28:38		
2019-05-13 13:28:39	Execution Tracking - end	Finished	2019-05-13 13:28:39		
2019-05-13 13:28:39	End	Finished	2019-05-13 13:28:39		
2019-05-13 13:28:39	Return Search Results	Finished	2019-05-13 13:28:39		
2019-05-13 13:28:38	Determine CIs	Finished	2019-05-13 13:28:38		
2019-05-13 13:28:38	Launch Get Network Statistics Workflows	Finished	2019-05-13 13:28:39	success	
2019-05-13 13:28:38	Begin	Finished	2019-05-13 13:28:38		

注目度の高い脆弱性を優先

一般にネットワークが攻撃されたときに考えるのは、「リスクエクスポージャーがあったことをどのように判断するか？」ですが、さらに重要なのは「最初に対処すべきシステムをどのように判断するか？」です。

2018 年初めに、2 つの重大な脆弱性、「**Meltdown**」と「**Spectre**」が発見されました。

注目度の高い脆弱性を優先

悪意のあるプログラムは、Meltdown と Specter を悪用して、他の実行中のプログラムのメモリに格納されている秘密情報にアクセスできる可能性があります。世界中の約 30 億台のシステムがこれらの脆弱性の影響を受ける可能性があり、ハードウェアとソフトウェアの両方のプロバイダーが急いで顧客にパッチを提供しようとしました。

脆弱性対応 のスキャンデータを使用した脅威のランキング

セキュリティオペレーション 脆弱性対応 アプリケーションには、脆弱性スキャンを実行するさまざまな手段が用意されています。セキュリティインシデントレスポンス アプリケーションがアクティブ化されている場合、セキュリティインシデントカタログ、セキュリティインシデントレコード、またはセキュリティスキャン要求からスキャンを開始することもできます。

使用するサードパーティ統合によっては、脆弱性データがスキャンされ、API を使用して 脆弱性対応 アプリケーションにインポートされます。その後、ServiceNow 構成管理データベース (CMDB) 内の資産と照合されます。結果の脆弱性一致アイテムには、脆弱性の重大度や影響を受ける資産の重要性など、複数の要因に基づいてリスクスコアが割り当てられます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リスクスコア

All Open Incidents

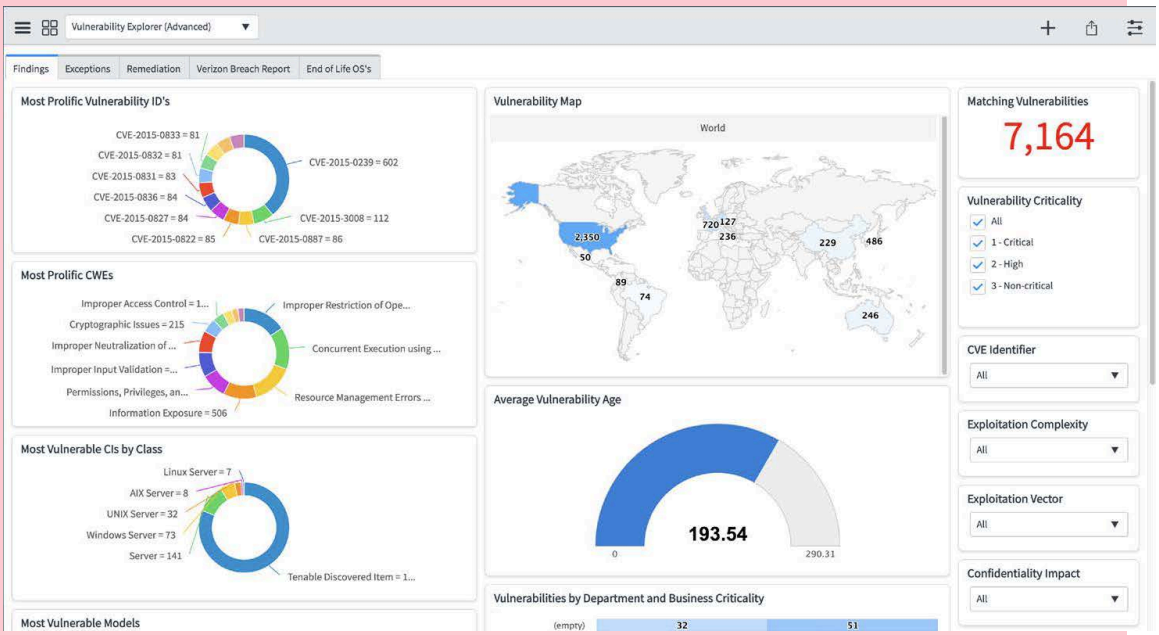
Search all incident columns

Create Incident

Number	Risk Score	Short Description	Category	Source
SIR0001774	89	DNS attack: zone transfer	Unauthorized access	Phone
SIR0001756	89	online gambling (policy breach)	Policy violation	Phone
SIR0001736	89	Email Malware in HQ	Malicious code act...	Alert
SIR0001742	82	USB drive found in server port	Criminal activity/i...	Email
SIR0001784	82	DNS redirect	Unauthorized access	Phone
SIR0001770	72	Database moved	Unauthorized access	Phone
SIR0001776	69	Sensitive data exposure (breach)	Unauthorized access	Phone
SIR0001761	65	email open relay	Unauthorized access	Phone

リスクスコアは構成可能で、迅速な優先順位付けを可能にします。脆弱性に関するすべての情報 (何であるか、どのように悪用されたか、脅威を修正する方法など) は、脆弱性情報データベース (NVD) から 脆弱性対応 に自動的に取り込まれるため、手作業で調査する必要はありません。ソリューションの構成可能なダッシュボードには、組織の全体的な脆弱性エクスポージャーがすぐに表示されます。

VR ダッシュボード



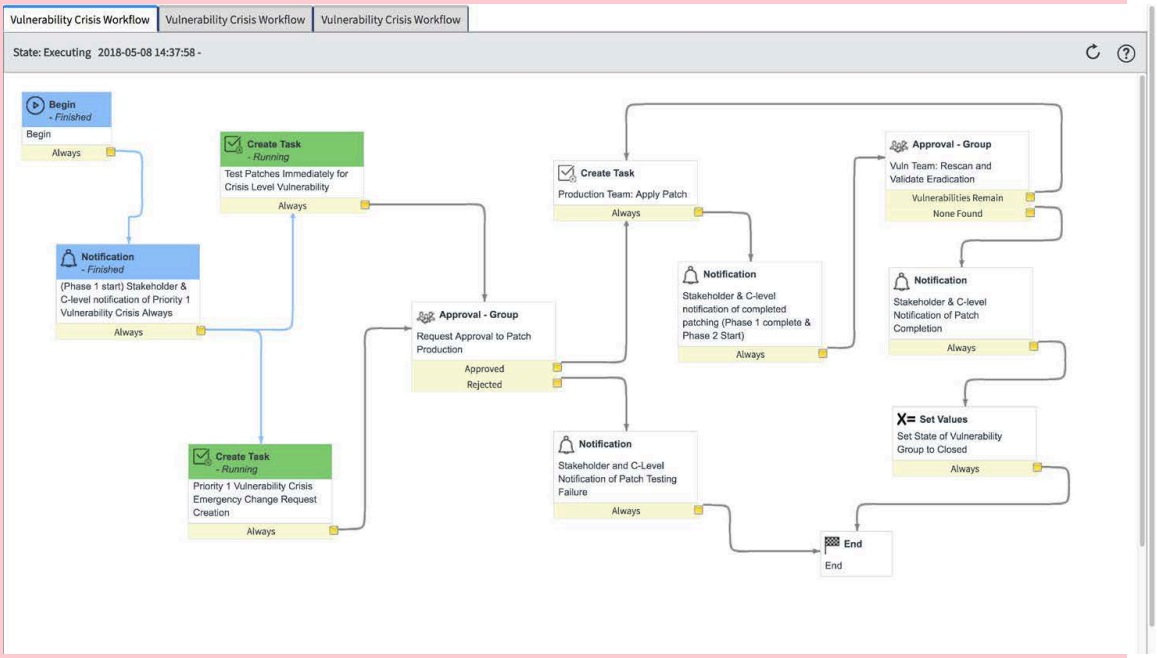
次のステップの自動化

最も重大な脆弱性一致アイテムを特定して優先順位を付けると、セキュリティオペレーション ワークフローによって次のいくつかのステップが自動化されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ステータスエンコーディングワークフロー



ビジネスクリティカルな脆弱性一致アイテムについては、自動パッチ適用を承認する要求が送信され、適切なオーナーに通知されます。これにより、オンコールアナリストを検索したり、アイテムを「重要」と見なすかどうかを自分で判断したりする必要がなくなります。

パッチが承認されて適用が完了すると、修正を確認するために 2 回目のスキャンが自動的に実行されます。優先順位付け、ワークフロー、および自動化を使用して、最も重要なアイテムが最初に処理されます。

自動翻訳

セキュリティオペレーション および **ServiceNow Store**

Madrid 以降は、すべての セキュリティオペレーション アプリケーションとサポートされている統合機能が ServiceNow Storeからダウンロードできます。それによって、新しい機能や更新された機能をより迅速に取得できます。セキュリティオペレーション アプリケーションを使用する前に、アプリケーションのエンタイトルメントがあること (すなわち使用するための有効なライセンスがあること) を確認し、ServiceNow Storeからアプリケーションをダウンロードして有効化する必要があります。

ダウンロード可能 セキュリティオペレーション なアプリケーションのリストは次のとおりです。アプリケーションは今後も増えていきます。

- セキュリティインシデントレスポンス (およびサポートされる統合機能)
- 脆弱性対応 (およびサポートされる統合機能)
- 脅威インテリジェンス (およびサポートされる統合機能)
- コンフィグレーションコンプライアンス
- トラステッドセキュリティサークル
- Data Loss Prevention Incident Response

ServiceNow Storeから Security Operations および GRC アプリケーションをダウンロードする方法については、この 5 分間の動画をご覧ください。 この 5 分間の動画では ServiceNow Store から Security Operations および GRC アプリケーションをダウンロードする方法を説明します

セキュリティオペレーション アプリケーションと統合機能を取得するために使用するプロセスは、初めてアプリケーションをダウンロードしているのか、以前に ServiceNow Storeからインストール

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

したアプリケーションを更新しているのか、またはあるファミリリリースから次のファミリリリースにアップグレードしているのかによって異なります。

ServiceNow Store からのアプリケーションの初回ダウンロード

ServiceNow Store からアプリケーションを初めてダウンロードする場合は、いくつかの簡単なステップを実行します。ServiceNow Store で実行するステップと、インスタンスで実行するステップがあります。

ServiceNow Store を使用すると、コア製品とアプリケーションをダウンロードできます。製品には、グループとしてライセンスされる 1 つ以上のアプリケーションが含まれています。たとえば、セキュリティインシデントレスポンス は製品です。このプロセスには次のステップが含まれます。

必要なロール：admin

- ServiceNow Store で、アプリケーションとその依存アプリケーションに対するエンタイトルメント (またはライセンス) があることを確認する必要があります。

  注:
  このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。非本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

- 最後に、アプリケーションをアクティブ化し、インスタンスで実行します。

注:
以前のバージョンの Rome 以降のリリースでは、コアアプリケーションをアクティブ化すると、依存関係プラグインが自動的にアクティブ化されます。たとえば、 脆弱性対応 アプリケーションをアクティブ化すると、 脆弱性対応 Dependencies プラグインも有効になります。詳細については、「ServiceNow Store アプリケーションのアクティブ化」を参照してください。

セキュリティオペレーション 製品またはアプリケーションのエンタイトルメントの取得

セキュリティオペレーション アプリケーションのインストールの最初の手順は、アプリケーションまたは製品およびその関連アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認することです。

始める前に
必要なロール：admin
エンタイトルメントを実行する個人には、Now Support アカウントと、検討中のインスタンスのアプリケーションを要求する権限が必要です。

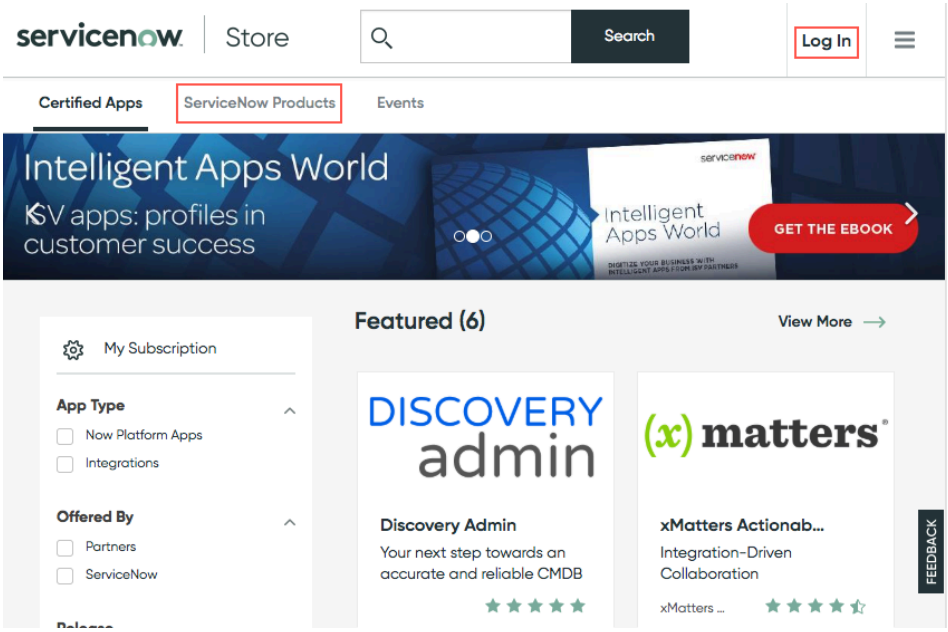
注:
このプロセスは、本番インスタンスにダウンロードしたアプリケーションにのみ適用されます。準本番インスタンスまたは開発インスタンスにアプリケーションをダウンロードする場合は、エンタイトルメントの取得は必要ありません。「ServiceNow Store アプリケーションのアクティブ化」に進みます。

自動翻訳

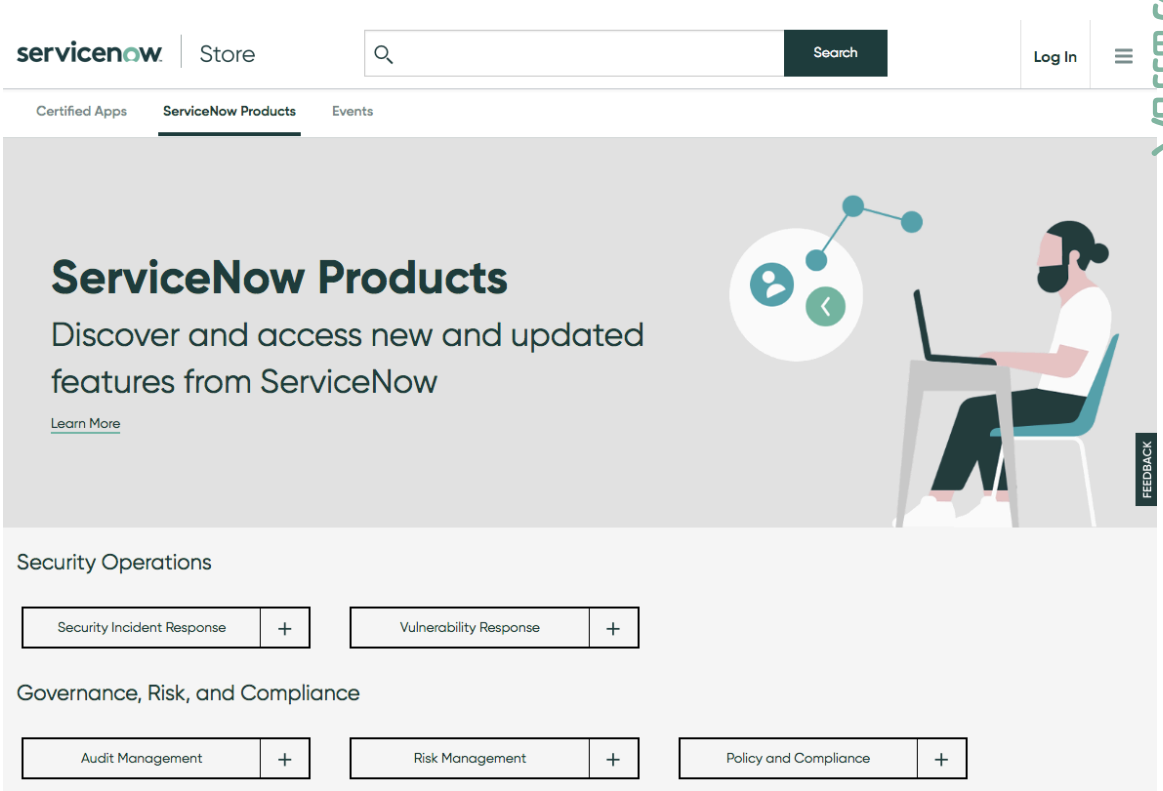
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. に移動します ServiceNow Store .



2. [ログイン] をクリックし、HI の認証情報を使用してログインします。
3. **[ServiceNow** 製品] タブをクリックして、利用可能なすべての ServiceNow製品を表示します。統合とその他のタイプのコンテンツが [認定アプリ **(Certified Apps)]** タブに表示されます。



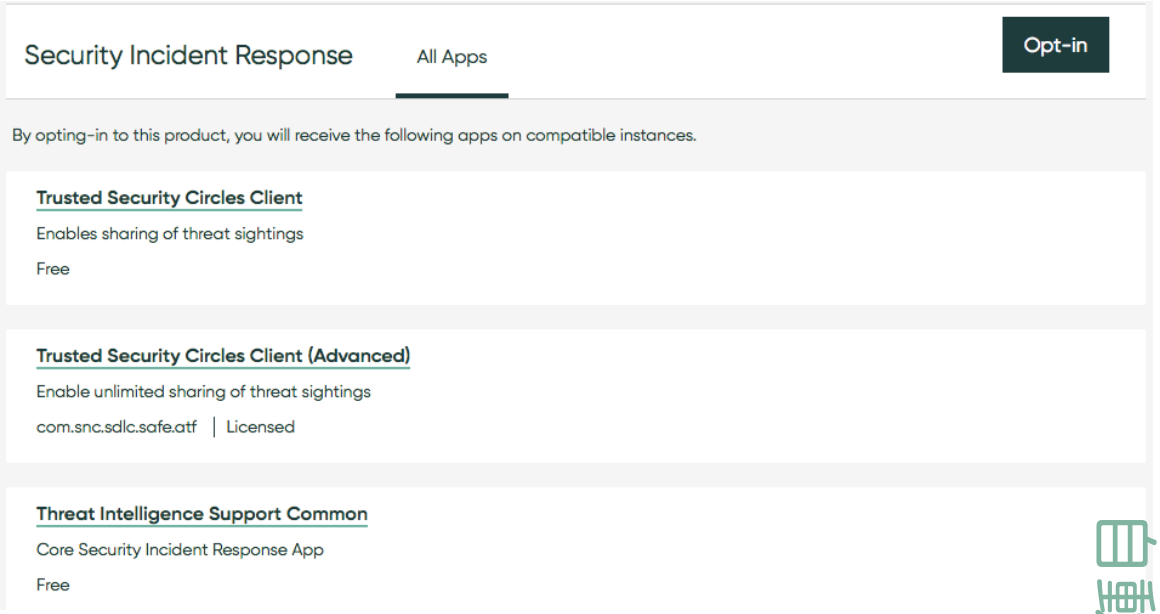
注:
この例では、セキュリティインシデントレスポンス 製品のエンタイトルメントを取得していることを前提とします。

自動翻訳

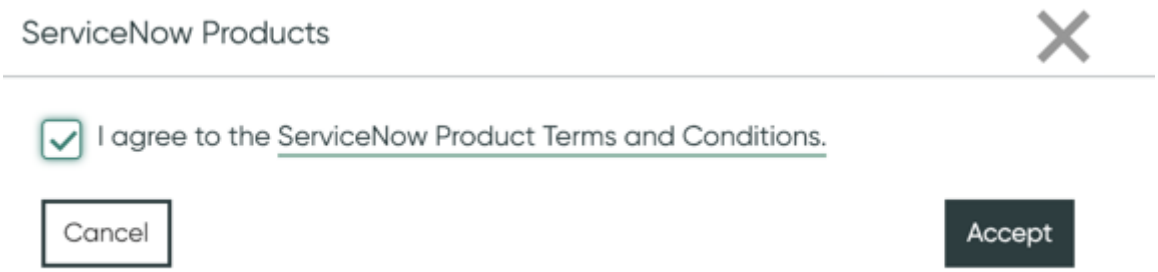
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. エンタイトルメントを取得する製品名の横にあるプラス (+) 記号をクリックします。
エンタイトルメントを取得している製品に関連付けられているすべてのアプリケーションが一覧表示されます。コア製品のエンタイトルメントを取得すると、その下にリストされているアプリケーションについてもエンタイトルメントを取得します。

   注:
   製品名をクリックすると、製品とその関連アプリケーションに関する詳細情報が表示されます。



5. [オプトイン] をクリックして、一覧表示されている製品とアプリケーションのエンタイトルメントがあることを確認します。
ServiceNowの契約条件を読んで同意するように求められます。



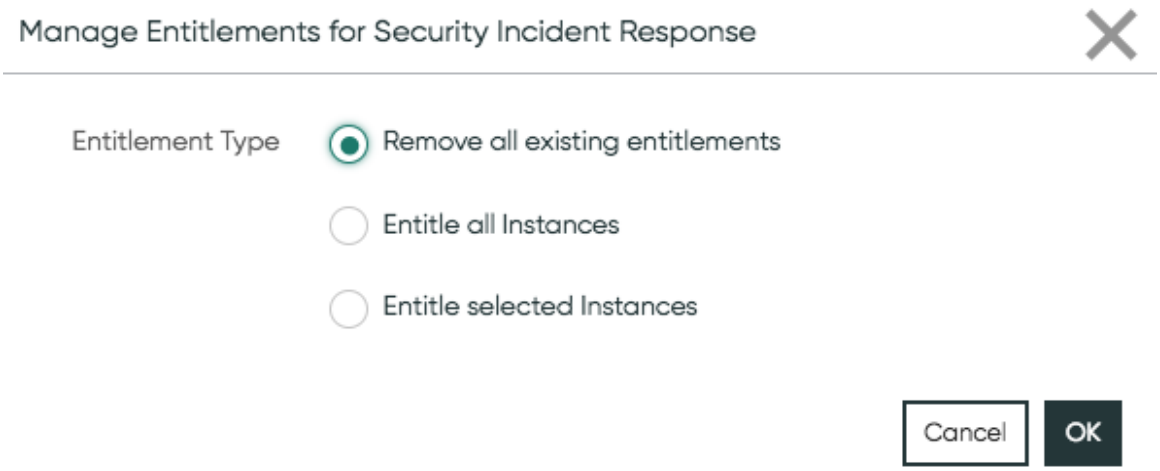
6. チェックボックスをオンにし、[受け入れ] をクリックします。
7. 製品名の横にチェックマークが表示され、[エンタイトルメントの管理 (Manage Entitlements)] ボタンが表示されます。

   このチェックマークは、ユーザーが製品とその関連アプリケーションに登録されていることを示します。エンタイトルメントを管理します。これは、この製品および後でインストールする他の製品に対する 1 回限りのプロセスです。

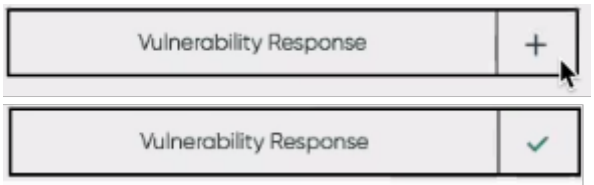
8. オプション: [エンタイトルメントの管理 **(Manage Entitlements)]** をクリックして、エンタイトルメントが付与されているアプリケーションの影響を受けるインスタンスを変更できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



9. ServiceNow の契約条件に同意し、エンタイトルメントを管理した後には、1 回クリックするだけで他の製品にエンタイトルメントを付与できます。



> **注:**
> 製品をアクティブ化する準備ができました。

ServiceNow Store アプリケーションのアクティブ化

アプリケーションにエンタイトルメントが付与されたら、その依存関係プラグインをアクティブ化し、アプリケーションをアクティブ化する必要があります。このプロセスは、準本番インスタンスにダウンロードしたアプリケーションにも適用されます。

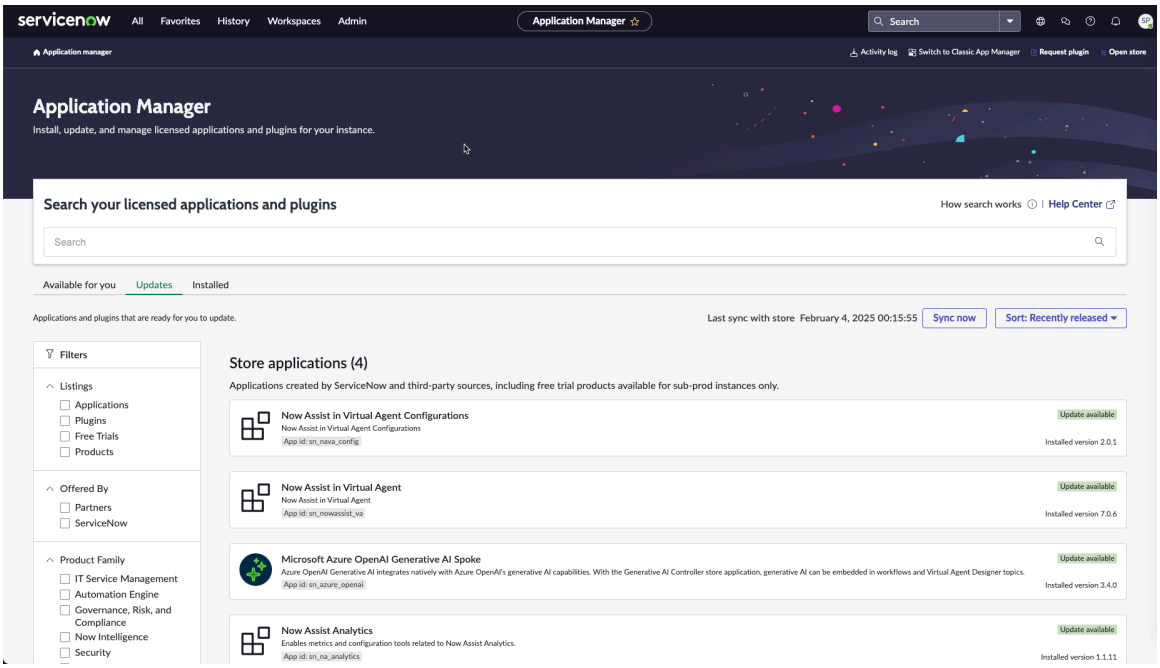
始める前に
必要なロール：admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

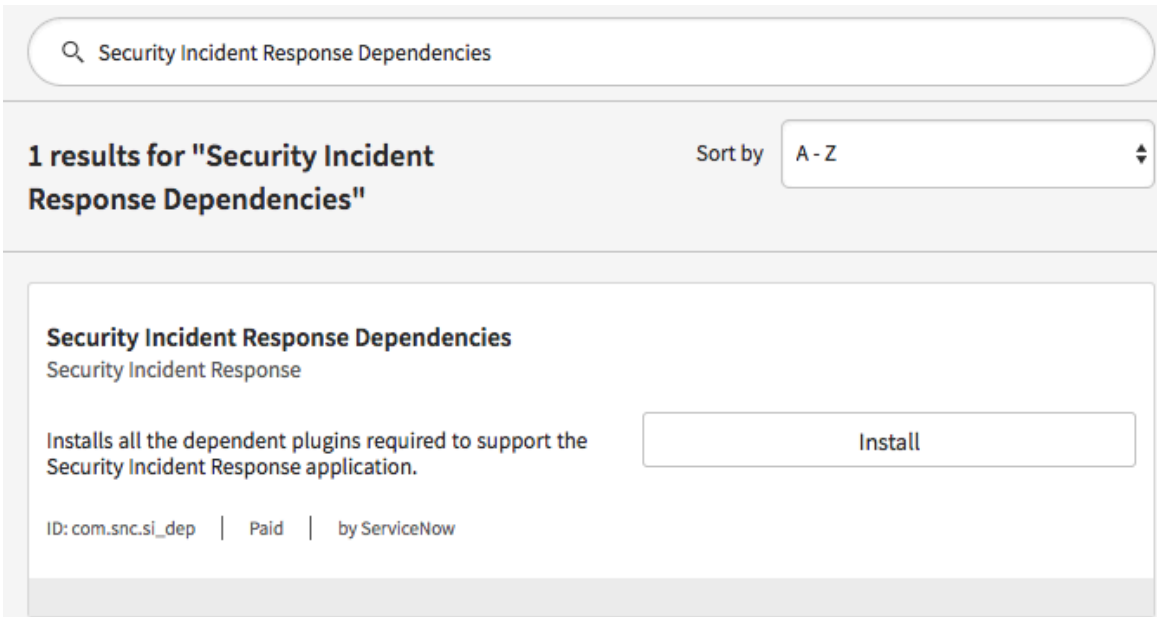
手順

1. 次のように移動する。 システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて).



> **注:**
> Orlando 以降では、コアアプリケーションをアクティブ化すると、依存関係プラグインが自動的にアクティブ化されます。たとえば、 脆弱性対応 アプリケーションをアクティブ化すると、 脆弱性対応 Dependencies プラグインも有効になります。したがって、ステップ 2 ～ 5 はオプションです。

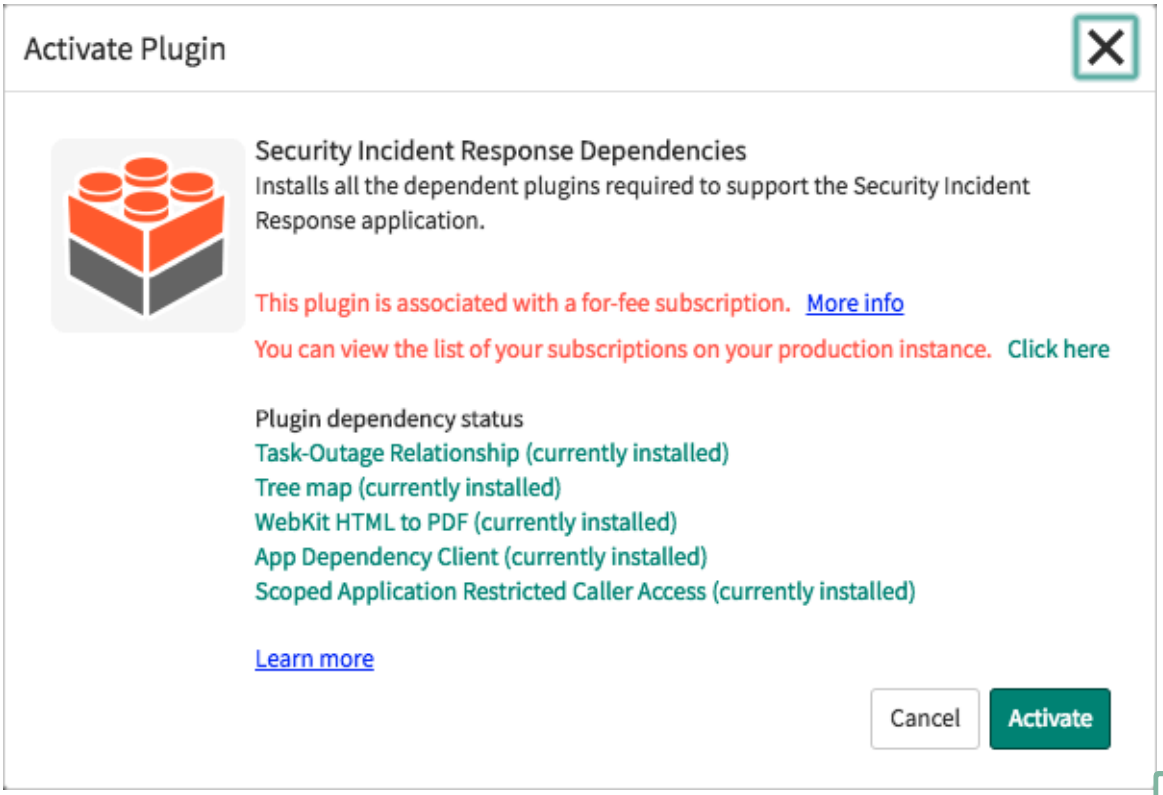
2. アクティブ化するアプリケーションの依存関係プラグインを検索します。
たとえば、セキュリティインシデントレスポンス をアクティブ化する場合は、セキュリティインシデントレスポンス Dependencies プラグインを見つけます。



3. [インストール] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[プラグインをアクティブ化] ダイアログボックスが表示されます。



4. [プラグインをアクティブ化] ダイアログボックスで、[アクティブ化] をクリックします。
5. アクティブ化が完了したら、[フォームを閉じてリロード] をクリックします。
6. アクティブ化するコア製品を探し、デモデータをロードする場合は [デモデータと共にインストール] チェックボックスをオンにし、[インストール] をクリックします。
   アプリケーションはインスタンスに自動でインストールされます。

   注:
   [デモデータと共にインストール] チェックボックスをオンにしないと、後でアプリケーションマネージャーからデモデータをインストールできません。初期インストール後にデモデータをインストールまたは再インストールする方法については、HI ナレッジベース記事「Work around to install demo data if application is already installed (アプリケーションが既にインストールされている場合にデモデータをインストールする方法) [KB0722909]」を参照してください。

セキュリティオペレーション 統合のインストール

ServiceNow のすべての統合を ServiceNow Storeで利用できます。セキュリティインシデントレスポンスなどのコアアプリケーションは、ストアの **[ServiceNow** 製品] タブに表示されます。統合アドオンは、[認定アプリ **(Certified Apps)]** タブに表示されます。

始める前に
必要なロール：admin
ストアのインストールには、検討中のインスタンスのアプリケーションを要求するために Now Support アカウントと権限が必要です。

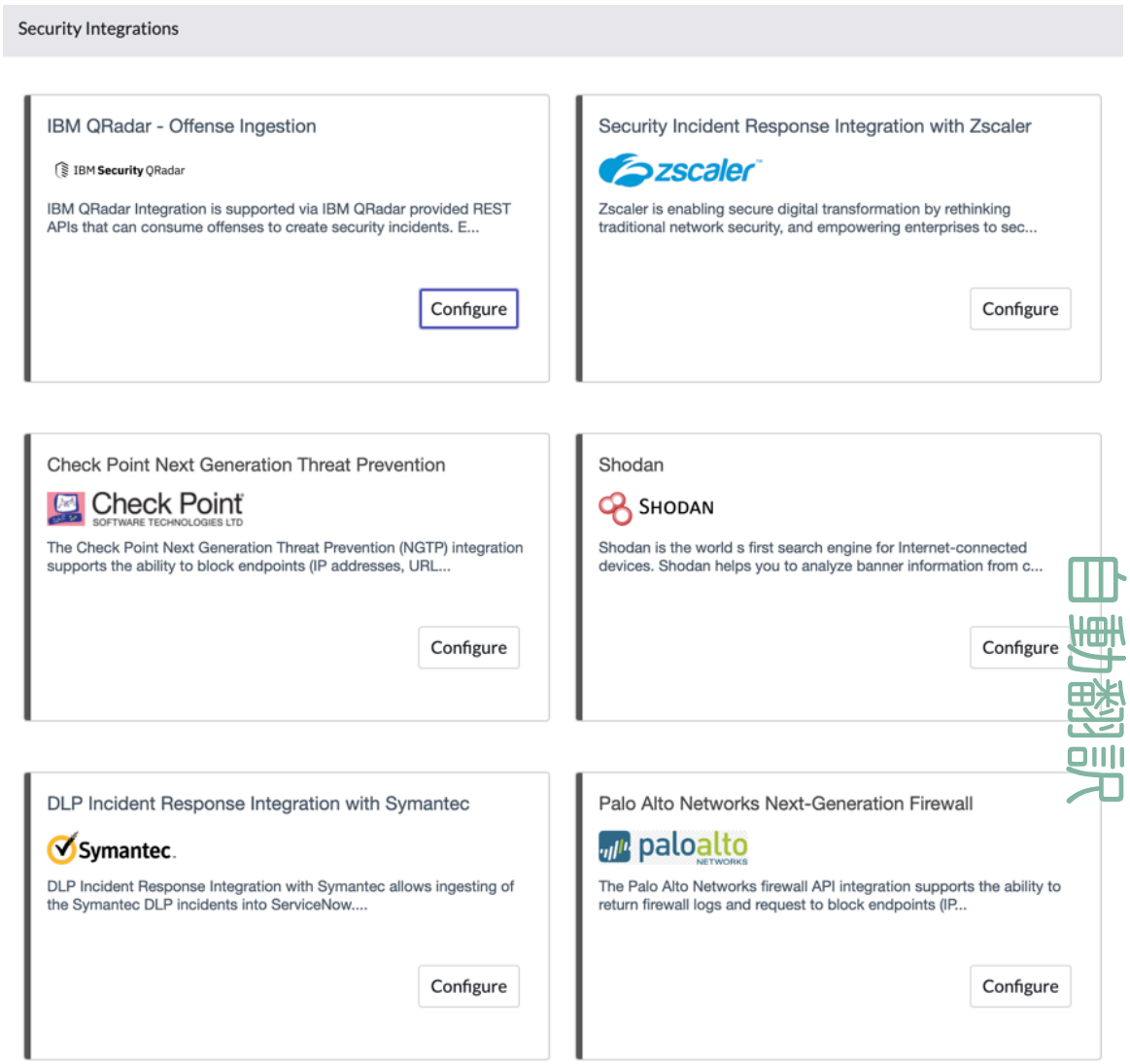
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 セキュリティオペレーション > 統合 > 統合設定 ServiceNow Store から アプリケーションをインストールした後。
   統合の構成タイルが表示されます。

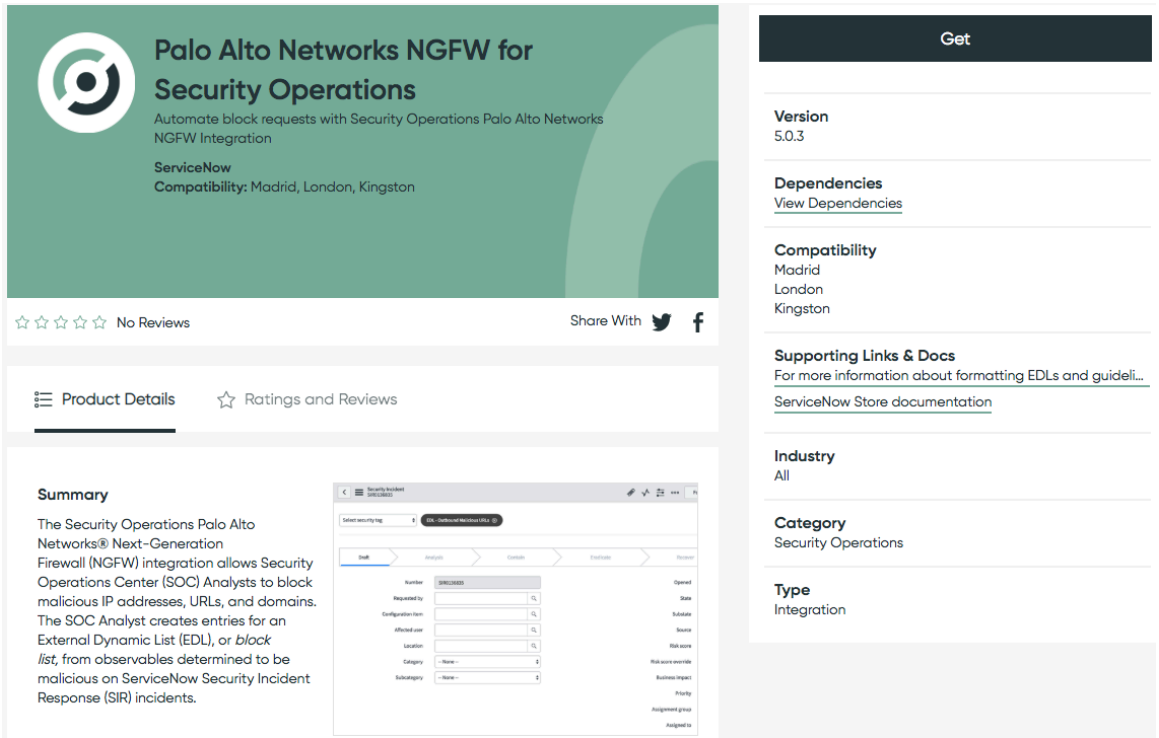
   注:



2. インストールする統合を見つけて、[構成] をクリックします。
   選択した統合が ServiceNow Store に表示されます。

自動翻訳

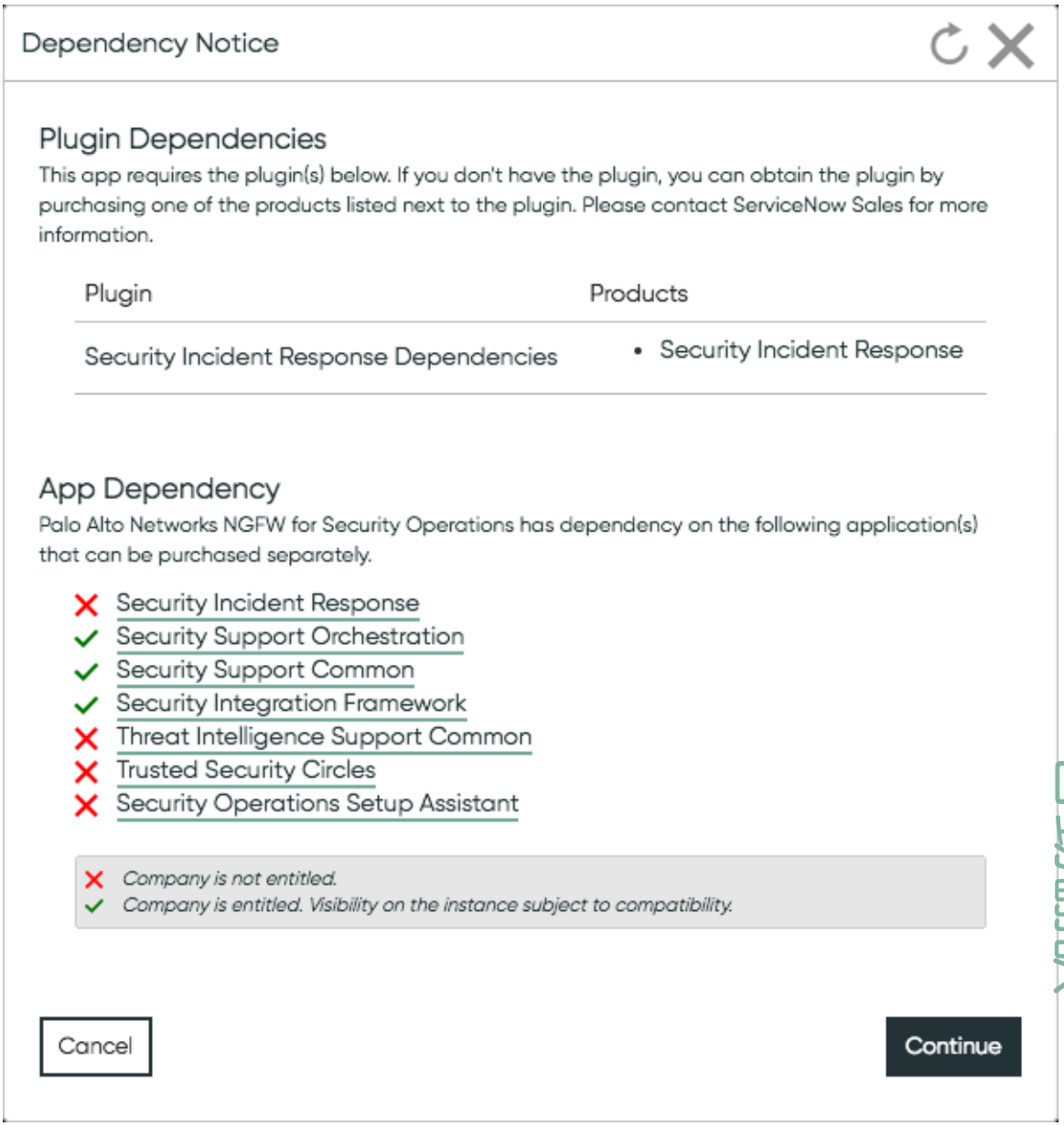
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. [依存関係を表示] をクリックし、リストされているアプリの依存関係を確認します。

自動翻訳

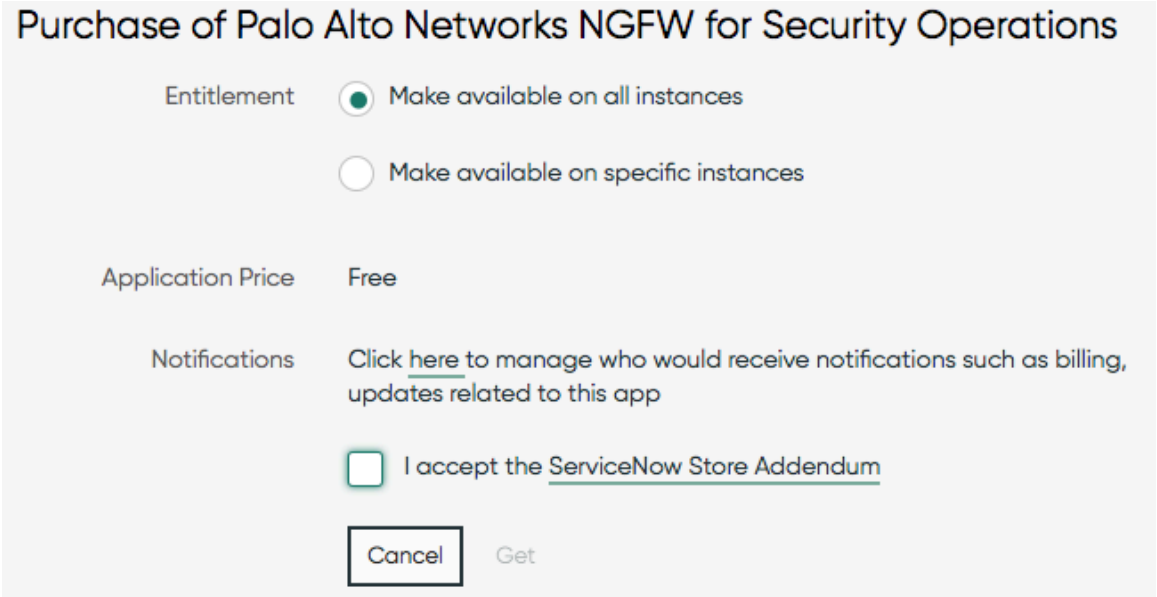
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. 統合に セキュリティインシデントレスポンス などのコアアプリケーションの依存関係があり、会社がまだエンタイトルメントを取得していない場合：
   a. 次の手順に従ってエンタイトルメントを取得し、依存関係プラグインをダウンロードし、アプリケーションをアクティブ化します。
   b. この手順に戻ります。
   c. [続行] をクリックします。
5. [取得] をクリックします。
   ServiceNow 契約条件が表示されます。
6. [続行] をクリックします。
   次のような購入画面が開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



7. 統合を利用可能にするインスタンスを特定し、通知を管理し、**[ServiceNow** ストアの補遺 **(ServiceNow Store Addendum)]** チェックボックスをオンにします。
8. [取得] をクリックします。

   注:
   購入するアプリケーションをダウンロードする場合は、[購入] をクリックします。ベンダーからの事前承認が必要なアプリケーションをダウンロードする場合は、[アプリを要求] をクリックします。

9. インスタンス名と要求の理由を入力し、[要求] をクリックします。
   詳細なインストール手順が記載されたメールが送信されます。
10. 次のように移動する。 システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて).
    インストール可能なアプリケーションのリストが表示されます。
11. アプリケーションを見つけて選択し、[インストール] をクリックします。
    統合はインスタンスに自動でインストールされます。

以前に **ServiceNow Store** からダウンロードしたアプリケーションの更新

以前にアプリケーションを ServiceNow Store からダウンロードしていて新バージョンが入手可能な場合、インスタンスで更新できます。

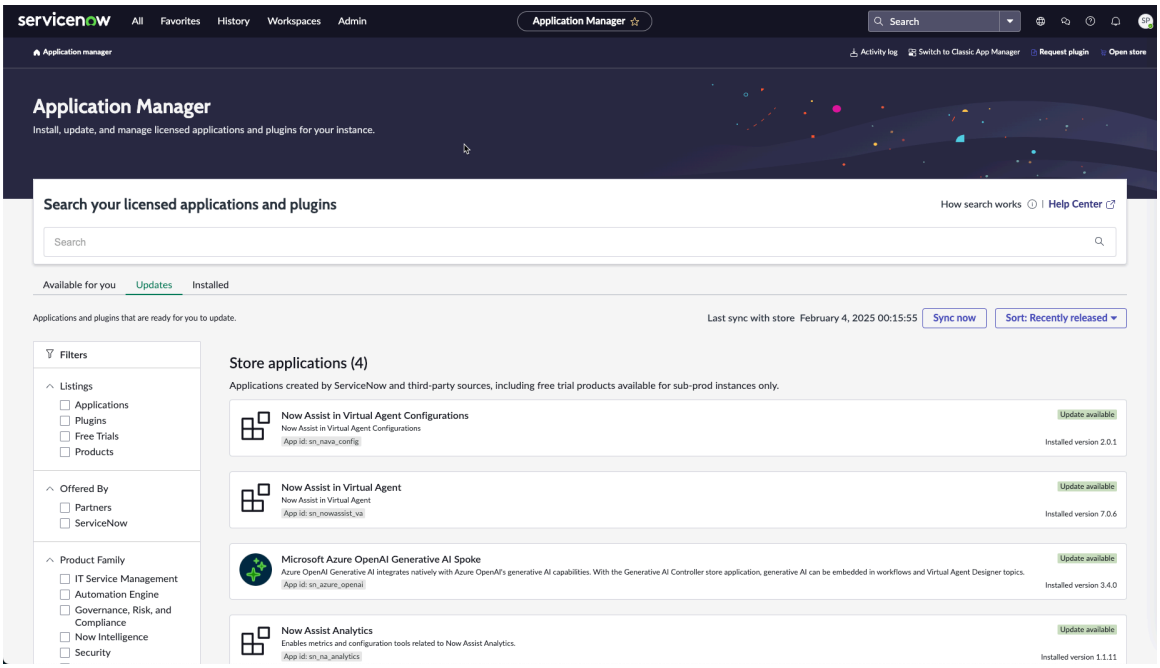
始める前に
必要なロール：admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のように移動する。 システムアプリケーション > 利用可能なすべてのアプリケーション > **All** (すべて).



2. 更新するアプリケーションを検索します。
3. アップグレード先のバージョンを選択し、[更新] をクリックします。
   アプリケーションはインスタンスへ自動的にインストールされます。

インスタンスの次のファミリリリースへのアップグレード

現在、いずれかのファミリリリース (London など) を実行していて、次のリリースにアップグレードする場合は、ServiceNow Store からアプリケーションを取得する必要はありません。プラットフォームが必要な最低バージョンに更新されると、アプリケーションが自動的に更新されます。

始める前に
必要なロール：admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。